INSTITUTO BRASILEIRO DE ENSINO, PESQUISA E DESENVOLVIMENTO
PROGRAMA DE PÓS-GRADUAÇÃO *STRICTU SENSU* EM DIREITO
DOUTORADO EM DIREITO CONSTITUCIONAL

DANIEL BASTOS MARWELL

DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS NO CAMPO PENAL:
A UTILIZAÇÃO DOS BANCOS DE DADOS NA POLÍCIA CIVIL DO DISTRITO FEDERAL.

BRASÍLIA
2024

DANIEL BASTOS MARWELL

DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS NO CAMPO PENAL: A UTILIZAÇÃO DOS BANCOS DE DADOS NA POLÍCIA CIVIL DO DISTRITO FEDERAL.

Tese de Doutorado desenvolvida no Programa de Pós-Graduação *Stricto Sensu* em Direito, sob a orientação do professor Ademar Borges de Sousa Filho, apresentado para obtenção do Título de Doutor em Direito Constitucional.

BRASÍLIA

2024

Código de catalogação na publicação – CIP

M391d Marwell, Daniel Bastos

Direito fundamental à proteção de danos no campo penal: a atualização nos bancos de dados na Polícia Civil do Distrito Federal / Daniel Bastos Marwell. — Brasília: Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa, 2024.

366 f.: il.

Orientador: Prof. Dr. Ademar Borges de Sousa Filho.

Tese (Doutorado Acadêmico em Direito Constitucional) — Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa – IDP, 2025.

1. Direitos fundamentais. 2. Proteção de dados - Brasil. 3. Polícia Civil do Distrito Federal. I.Título

CDDir 341.27

Elaborada por Pollyana da Silva Marra – CRB 1/3704

DANIEL BASTOS MARWELL

DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS NO CAMPO PENAL:
A UTILIZAÇÃO DOS BANCOS DE DADOS NA POLÍCIA CIVIL DO DISTRITO FEDERAL.

Tese de Doutorado apresentada ao Programa de Pós-Graduação *Stricto Sensu* em Direito IDP, como requisito para obtenção do título de Doutor em Direito Constitucional.

Data da defesa: 19/12/2024.

BANCA EXAMINADORA

Prof.(a) Dr.(a) Ademar Borges de Sousa Filho
Orientador(a)
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa

Prof.(a) Dr.(a) Carolina Costa Ferreira
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa
Membro Interno

Prof.(a) Dr.(a) Beatriz Vargas Ramos Gonçalves de Rezende
Universidade de Brasília
Membro Externo

Prof.(a) Dr.(a) Claudio Pereira de Souza Neto
Universidade Federal Fluminense
Membro Externo

INSTITUTO BRASILEIRO DE ENSINO DESENVOLVIMENTO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM DIREITO
DOUTORADO EM DIREITO CONSTITUCIONAL

Ata de Defesa de Tese

Discente: DANIEL BASTOS MARWELL
Registro Acadêmico: 2014945
Orientador(a): Prof. Dr. Ademar Borges de Sousa Filho
Co-Orientador(a) (se houver:)

Título da Tese:

DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS NO CAMPO PENAL: A UTILIZAÇÃO DOS BANCOS DE DADOS N POLÍCIA CIVIL DO DISTRITO FEDERAL.

Resultado:

Após a apresentação da Tese e arguição do(a) candidato(a) a banca examinadora decidiu pela Aprovação

Observações:

Sem observações.

Assinaturas da Banca Examinadora

Prof. Dr. Ademar Borges de Sousa Filho	Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP
Profa. Dra. Carolina Costa Ferreira	Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP
Profa. Dra. Beatriz Vargas Ramos Gonçalves de Rezende	Universidade de Brasília - UnB
Prof. Dr. Cláudio Pereira de Souza Neto	Universidade Federal Fluminense - UFF

19/12/2024 2:00pm

Para Adriana, com muito Amor. Parceira de vida. Fonte de inspiração.

Aos meus filhos Emanuela e João Pedro. Obrigado por todo amor e carinho. A parceria de vocês foi fundamental para a conclusão deste trabalho.

O problema fundamental em relação aos direitos do homem, hoje, não é tanto o de justifica-los, mas o de protege-los.
(BOBBIO, Norberto).

Não pensem vocês que são suas mentes brilhantes ou suas ideias inspiradas que conduzem suas vidas. São seus hábitos. Os hábitos possuem uma enorme capacidade de aprisionar o agir humano. Que cultivemos os bons, porque os maus hábitos nos escravizam dolorosamente.

(YOGANANDA, Paramahansa)

Ninguém pode construir em teu lugar as pontes que precisarás passar, para atravessar o rio da vida – ninguém, exceto tu, só tu. Existem, por certo, atalhos sem números, e pontes, e semideuses que se oferecerão para levar-te além do rio; mas isso te custaria a tua própria pessoa; tu te hipotecarias e te perderias. Existe no mundo um único caminho por onde só tu podes passar. Onde leva? Não perguntes, segue-o!

(NIETZSCHE, Friedrich)

Que ninguém se engane, só se consegue a simplicidade através de muito trabalho.
(LISPECTOR, Clarisse)

AGRADECIMENTOS

O que antes era um sonho, tornou-se realidade que custo a acreditar. Este Doutorado foi cursado durante um período de muitas transformações pessoais e profissionais, todas muito positivas e que me fizeram crescer. Dizem que os momentos de maior adversidade são aqueles que mais nos fortalecem. Antes de tudo, é preciso agradecer a Deus. Sem essa Força Divina, nada disso teria ocorrido. *Prepara-se o cavalo para o dia da batalha, porém do Senhor vem a vitória (Provérbios 21:31).*

À minha esposa, Adriana. Presente de Deus e parceira de vida que abraçou o meu sonho como se fosse o Dela. Sem a sua ajuda, nada disso seria possível. Eu jamais teria alcançado esse objetivo de vida sem o seu pleno e irrestrito apoio. Você me inspira a cada dia. *"Tudo de bom que você me fizer... Faz minha rima ficar mais rara... O que você faz me ajuda a cantar... Põe um sorriso na minha cara... Meu amor, você me dá sorte... Meu amor, você me dá sorte... Meu amor, você me dá sorte na vida...".* Obrigado por tudo. Amo muito você.

Aos meus filhos, Emanuela e João Pedro. Vocês são o meu combustível. Vocês são o ar que respiro. Vocês me motivam a ser uma pessoa cada vez melhor. Tenho muito orgulho de ter sido escolhido por Deus para ser o Pai de vocês. Uma das coisas que eu mais gosto de fazer na vida é estar na companhia de vocês. Obrigado pela ajuda e pela compreensão dos finais de semana dedicados a esse projeto. Sem a ajuda de vocês, a realização desse sonho não teria sido possível. Papai ama muito vocês.

Aos meus Pais, Francisco Marwell e Rosária Marwell, por tudo o que sempre fizeram por mim. Eu jamais teria chegado até aqui se não fossem os ensinamentos recebidos.

Aos amigos, por toda compreensão e pelos convites negados. Apesar de um período de ausência, senti a energia de cada um de vocês na torcida para que tudo desse certo.

Ao Professor Ademar, por todo apoio. Durante o início do curso de Doutorado no IPD, tive a honra de ter sido aluno do Professor Ademar. Naquele momento, apesar de ainda não ter tido contato com todos os outros professores, e possíveis orientadores, tive a iniciativa de convidar o Professor Ademar para ser o meu orientador, o que foi aceito de imediato. Mesmo com uma vida tão corrida, o Professor Ademar sempre foi muito solícito e prestativo. Homem sábio, de enorme conhecimento jurídico e muita humildade. Ao logo de todo o período de pesquisa, passou-me diversos *insights* que foram extremamente importantes para a confecção deste trabalho. Foi um privilégio tê-lo como orientador.

À Professora Carolina, à Professora Beatriz e ao Professor Cláudio, por terem me dado a honra de participarem das bancas de qualificação e defesa e por terem feito contribuições muito valiosas para a tese.

Às Professoras Laura Schertel, Heloisa Estellita e ao Professor Georges Abboud, pelo ensino, apoio e inspiração.

A todos os amigos da Divisão de Controle de Denúncias da Polícia Civil do Distrito Federal – DICOE/PCDF, que me auxiliaram nas permutas dos plantões para que eu pudesse conciliar o trabalho com as aulas no Doutorado.

Aos Diretores da DICOE/PCDF, Josafá e Monteiro, por todo apoio de sempre.

Aos amigos Alexandre e Alexander;

Aos amigos Ricardo Guedes da Cunha e Leonardo Flávio Ribeiro de Resende.

Ao IDP, por ter proporcionado toda estrutura necessária para o processo de aprendizagem.

À Polícia Civil do Distrito Federal.

SUMÁRIO:

LISTA DE ABREVIATURAS A SIGLAS

ABIN	Agência Brasileira de Inteligência
ADI	Ação Direta de Inconstitucionalidade
ADO	Ação Direta de Inconstitucionalidade por Omissão
ADPF	Arguição de Descumprimento de Preceito Fundamental
AIR	Análise de Impacto Regulatório
ANPD	Autoridade Nacional de Proteção de Dados
ARE	Análise em Recurso Extraordinário
BNPG	Banco Nacional de Perfil Genético
BNDES	Banco Nacional de Desenvolvimento Econômico e Social
CBF	Confederação Brasileira de Futebol
CDFUE	Carta dos Direitos Fundamentais da União Europeia
CEDH	Convenção Europeia dos Direitos do Homem
CIDH	Corte Interamericana de Direitos Humanos
CNJ	Conselho Nacional de Justiça
CNMP	Conselho Nacional do Ministério Público
CNPD	Comissão Nacional de Proteção de Dados
CPI	Comissão Parlamentar de Inquérito
CPP	Código de Processo Penal
DIOPI	Diretoria de Operações Integradas e de Inteligência
DPD	Diretiva de Proteção de Dados
DPO	Oficial de Proteção de Dados
ECA	Estatuto da Criança e do Adolescente
ENCCLA	Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro
ENISP	Estratégia Nacional de Inteligência de Segurança Pública
EUROJUST	Agência Europeia em Cooperação para Justiça Criminal
FBI	*Federal Bureal of Investigation*
FGV	Fundação Getúlio Vargas
GDPR	Regulamento Geral de Proteção de Dados da União Europeia
GPS	*Global Positioning System* (Sistema Global de Posicionamento)
HC	Habeas Corpus
IBGE	Instituto Brasileiro de Geografia e Estatística
IMEI	*International Mobile Equipment Identy*

IP	*Internet Protocol*
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados
LGPD Penal	Anteprojeto Penal da Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
MP	Medida Provisória
MJSP	Ministério da Justiça e Segurança Pública
OAB	Ordem dos Advogados do Brasil
OCDE	Organização para Cooperação e Desenvolvimento Econômico
OMS	Organização Mundial da Saúde
ONU	Organização das Nações Unidas
PAD	Processo Administrativo Disciplinar
PCDF	Polícia Civil do Distrito Federal
PDSI	Plano Diretor de Segurança da Informação
PGR	Procuradoria Geral da República
PL	Projeto de Lei
PNISP	Política Nacional de Inteligência de Segurança Pública
PNSPDS	Política Nacional de Segurança Pública e Defesa Social
RE	Recurso Extraordinário
RESP	Recurso Especial
RGPD	Regulamento Geral de Proteção de Dados
RHC	Recurso Ordinário Constitucional
RMS	Recurso Ordinário em Mandado de Segurança
SEI	Sistema Eletrônico de Informações
SEOPI	Secretaria de Operações Integradas
SISBIN	Sistema Brasileiro de Inteligência
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
SUSP	Sistema Único de Segurança Pública
TCU	Tribunal de Contas da União
TJUE	Tribunal de Justiça da União Europeia
UE	União Europeia

RESUMO:

A compreensão da proteção de dados no ordenamento jurídico brasileiro é de fundamental importância para os estudiosos do direito. Esse tema vem ganhando cada vez mais repercussão nacional, principalmente após o advento da Lei número 13.709/2018, denominada **Lei Geral de Proteção de Dados (LGPD)**. Essa Lei tem como principal objetivo seguir uma tendência mundial que visa proteger direitos fundamentais de liberdade e de privacidade, concedendo a qualquer cidadão o direito pleno ao controle sobre os seus dados pessoais. Além disso, a referida legislação protege o cidadão, pessoa natural, dando-lhe liberdade para decidir se o seu dado pessoal pode ou não ser utilizado por uma pessoa de direito público ou privado. A Lei Geral de Proteção de Dados Brasileira, por sua vez, foi inspirada no diploma normativo da União Europeia de 2018, denominado GDPR (*General Data Protection Regulation*). Qual a necessidade de desenvolver um estudo que relacione a Lei Geral de Proteção de Dados com o banco de dados das Polícias Judiciárias Brasileiras? Essa indagação será respondida durante a confecção deste trabalho, onde também será possível compreender o Anteprojeto da Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública e de investigação e repressão de investigações penais, também conhecida como "LGPD Penal". A principal temática do objeto de estudo é saber a medida certa para a aplicação da proteção de dados na persecução penal, sem violar o direito fundamental da proteção de dados.

Palavras-chave: Proteção de Dados, Privacidade, Regulação, Persecução Penal, Ponderação de Bens, Razoabilidade, Proporcionalidade.

ABSTRACT:

Understanding data protection in the Brazilian legal system is of fundamental importance for legal scholars. This topic has been gaining more and more national repercussion, especially after the advent of Law number 13,709/2018, called the General Data Protection Law (LGPD). This Law's main objective is to follow a global trend that aims to protect fundamental rights of freedom and privacy, granting any citizen the full right to control over their personal data. Furthermore, the aforementioned legislation protects citizens, natural persons, giving them the freedom to decide whether or not their personal data can be used by a person governed by public or private law. The Brazilian General Data Protection Law, in turn, was inspired by the 2018 European Union normative diploma, called GDPR (General Data Protection Regulation). What is the need to develop a study that relates the General Data Protection Law with the Brazilian Judicial Police database? This question will be answered during the preparation of this work, where it will also be possible to understand the Draft Personal Data Protection Law for the exclusive purposes of State security, national defense, public security and investigation and repression of criminal investigations, also known as "LGPD Penal". The main theme of the study object is knowing the right measure for applying data protection in criminal prosecution, without violating the fundamental right to data protection.

keywords: Data Protection, Privacy, Regulation, Criminal Prosecution, Weighting of Assets, Reasonability, Proportionality.

RESUMEN:

Comprender la protección de datos en el sistema legal brasileño es de fundamental importancia para los juristas. Este tema viene ganando cada vez más repercusión nacional, especialmente después de la aparición de la Ley número 13.709/2018, denominada Ley General de Protección de Datos (LGPD). Esta Ley tiene como principal objetivo seguir una tendencia global que pretende proteger los derechos fundamentales de libertad y privacidad, otorgando a cualquier ciudadano el pleno derecho al control sobre sus datos personales. Además, la mencionada legislación protege a los ciudadanos, personas físicas, dándoles la libertad de decidir si sus datos personales pueden ser utilizados o no por una persona de derecho público o privado. La Ley General de Protección de Datos brasileña, a su vez, se inspiró en el diploma normativo de la Unión Europea de 2018, denominado GDPR (Reglamento General de Protección de Datos). ¿Cuál es la necesidad de desarrollar un estudio que relacione la Ley General de Protección de Datos con la base de datos de la Policía Judicial brasileña? Esta pregunta será respondida durante la elaboración de este trabajo, donde también será posible comprender el Proyecto de Ley de Protección de Datos Personales para fines exclusivos de la seguridad del Estado, defensa nacional, seguridad pública y la investigación y represión de investigaciones criminales, también conocida como "LGPD Penal". El tema principal del objeto de estudio es conocer la medida adecuada para aplicar la protección de datos en el proceso penal, sin vulnerar el derecho fundamental a la protección de datos.

Palabras clave: Protección de Datos, Privacidad, Regulación, Persecución Penal, Ponderación Patrimonial, Razonabilidad, Proporcionalidad.

1 INTRODUÇÃO

1.1 Objeto de Pesquisa

A compreensão da proteção de dados no ordenamento jurídico brasileiro no contexto da conformação das relações jurídicas e sociais contemporâneas é de fundamental importância para os estudiosos do direito. O tema vem ganhando cada vez mais repercussão nacional, principalmente após o advento da Lei número 13.709/2018, denominada **Lei Geral de Proteção de Dados (LGPD)**. Essa Lei tem como principal objetivo seguir uma tendência mundial que visa proteger direitos fundamentais de liberdade e de privacidade, concedendo a qualquer indivíduo o direito pleno ao controle sobre os seus dados pessoais. Além disso, a referida legislação protege o indivíduo, pessoa natural, dando-lhe liberdade para decidir se o seu dado pessoal pode ou não ser utilizado por uma pessoa de direito público ou privado. A LGPD foi inspirada no diploma normativo da União Europeia de 2018, denominado GDPR (*General Data Protection Regulation*). Qual a necessidade de desenvolver um estudo que relacione a Lei Geral de Proteção de Dados com o direito penal e os bancos de dados das Polícias Judiciárias Brasileiras? A resposta para essa questão não é tão simples e durante a leitura deste trabalho será possível entender que o tema precisa ser debatido no âmbito do Direito Penal e do Direito Processual Penal, sob o prisma do Direito Constitucional.

A legislação brasileira que dispõe sobre proteção de dados pessoais aborda os direitos do titular dos dados, o tratamento de dados pessoais pelo Poder Público, menciona a transferência internacional de dados e faz referência aos agentes de tratamento de dados, definindo a função do controlador, do operador e do encarregado pelo tratamento de dados. A Lei Geral de Proteção de Dados, portanto, traz questões muito relevantes à segurança, o sigilo, boas práticas e a governança no tratamento de dados pessoais. Como toda legislação que tenha o escopo de mudar uma cultura, a fiscalização e às sanções administrativas não foram deixadas de lado.

A proteção dos dados pessoais já constava na Constituição Federal, mais especificamente no Título II, que trata dos Direitos e Garantias Fundamentais. O Inciso X é taxativo ao dizer que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente da sua violação. Além disso, os Incisos XI, XII, LV e IX também trazem essa previsão. A grande questão a ser debatida neste estudo está situada no artigo 4º, inciso II, alínea *a* da referida Lei

Geral de Proteção de Dados, consta que não se aplica o tratamento de dados pessoais quando realizado para fins exclusivos de segurança pública.

A temática principal do objeto de estudo é demonstrar a necessidade de regulamentação da utilização de dados pessoais no âmbito da investigação policial. Além disso, é necessário saber a medida certa para a utilização da ponderação de bens e do princípio da proporcionalidade diante de aparente confronto entre a investigação criminal e a preservação do direito fundamental da proteção de dados pessoais. Estudiosos de diversos países alegam que o Estado não pode manter uma vigilância constante dos seus cidadãos, sob a justificativa de que essa prática só pode ser utilizada para o combate do terrorismo, do tráfico de drogas e de outros crimes mais graves.

O fato é que o debate precisa ser feito de forma que o legislativo assuma o seu papel de protagonista para regulamentar a real necessidade de proteger o cidadão de qualquer ameaça que viole o direito fundamental de proteção de dados, diante de investigação que envolva a apuração de crimes, sejam eles graves ou não. A utilização dos dados também deve ser regulamentada, já que pode ser compreendida como parte integrante de um dos pilares[1] de um

[1]Os 10 pilares de um sistema de compliance: 1. Suporte da alta administração: antes de tudo, é importante destacar que não adianta tentar implantar um programa de compliance sem a adesão total dos diretores da empresa. A alta administração deve apoiar e se envolver no planejamento e na execução das ações. Da mesma forma, é preciso contar com um profissional especializado em compliance, que será o responsável pela implantação de todo o projeto. 2. Avaliação de riscos: a avaliação de riscos, também chamada de mapeamento de riscos de compliance (compliance risk assessment – cra), é uma das etapas mais importantes da implantação de um programa de integridade. Isso porque é nela que se conhece todos os riscos potenciais e seus impactos para que a organização alcance seus objetivos. Afinal, cada empresa está sujeita a problemas diferentes, de acordo com seu tamanho, mercado de atuação e cultura organizacional. 3. Código de conduta e políticas de compliance: outro dos pilares de um programa de compliance é a adoção de um código de conduta ética. Ele traz todas as políticas a serem adotadas na empresa, não apenas para manter a conformidade com as leis, como também garantir uma cultura de integridade e valorização de comportamentos éticos. 4. Controles internos: a empresa deve criar mecanismos de controle para assegurar que os riscos sejam minimizados, tanto no nível interno quanto no externo. Os próprios registros contábeis e financeiros são usados para transparecer a realidade do negócio. 5. Treinamento e comunicação: o programa de compliance deve fazer parte da cultura de toda a empresa. Para isso, além da adesão da alta administração**,** os colaboradores precisam entender os objetivos, as regras e o papel de cada um para que ele seja bem-sucedido. Para isso, é fundamental investir em treinamentos e na comunicação interna. 6. Canais de denúncia: uma vez que estejam conscientes sobre a importância do compliance, os colaboradores precisam de canais de denúncia ativos para alertar sobre violações ao código de conduta. Ou seja, deve-se manter e-mails, telefones e outras formas de comunicação à disposição dos colaboradores. 7. Investigações internas: feita uma denúncia, a empresa precisa investigar qualquer indício de comportamento antiético e ilícito que tenha sido noticiado. Em seguida, deve-se tomar as providências necessárias, com as devidas correções e, conforme o caso, punições. 8. Due diligence: o programa de compliance não pode ficar restrito ao comportamento da organização. Fornecedores, representantes, distribuidores e outros parceiros devem ser submetidos a uma rigorosa due diligence. Ou seja, é importante avaliar o histórico de cada um deles antes de se estabelecer uma relação contratual. 9. Auditoria e monitoramento: o penúltimo dos pilares de um programa de compliance trata, exatamente de sua manutenção. Ele deve ser contínuo, avaliando sempre se está sendo bem executado e se as pessoas estão, de fato, comprometidas com as normas**,** se cada um dos pilares está funcionando como o esperado.: 10. Diversidade e inclusão: após mais de 7 anos ensinando compliance de acordo com uma metodologia exclusiva baseada em 9 pilares do programa de

eficiente sistema de *compliance*. Cabe ressaltar que tanto a Lei Geral de Proteção de Dados (LGPD) quanto o Regulamento Geral de Proteção de Dados Europeu (GDPR) excluem a sua aplicação em casos de tratamento de informações em investigações criminais ou persecuções penais.

1.2 O problema teórico

Como regulamentar a utilização dos dados pessoais armazenados nos bancos de dados das polícias judiciárias brasileiras? A questão que merece ser debatida sob o espectro constitucional, já que recentemente a proteção de dados passou a ser considerada um direito fundamental, conforme previsto na proposta de EC 17/2019, foi estabelecido que cabe somente à União a fiscalização e a proteção de dados pessoais, acumulando a competência exclusiva para legislar sobre o tema.

Apenas a título de exemplo, é cediço que algumas polícias judiciárias brasileiras são responsáveis pela emissão de carteiras de identidade, o que já acontece na Polícia Civil do Distrito Federal. Quando não é feito dessa forma, as Secretarias de Segurança Pública são as responsáveis pela emissão do referido documento, o que alimenta os bancos de dados das Polícias e das Secretarias de Segurança Pública. Além disso, os bancos de dados também são alimentados quando qualquer cidadão procura uma Delegacia de Polícia para confeccionar uma Ocorrência Policial de acidente de trânsito sem vítima ou o extravio de algum documento. Embora os referidos registros sejam de natureza administrativa, os dados fornecidos pelos indivíduos podem eventualmente ser utilizados pelas polícias na investigação de futuros delitos.

1.3 Perguntas a serem respondidas

A pergunta central em questão é: as policiais judiciárias brasileiras podem utilizar os dados que constam nos seus próprios bancos de dados para investigar a autoria de delitos sem que exista legislação específica regulamentado o tema? A pergunta central gera outras questões que também precisam ser respondidas. Caso os órgãos de persecução penal aleguem a

---

compliance, a lec passa agora a tratar também de diversidade e inclusão como o seu 10º pilar**,** como uma forma de prestigiar um tema tão importante e capaz de transformar positivamente o ambiente corporativo no brasil. Não há compliance sem respeito e igualdade. Lec | [infográfico] os 10 pilares de um programa de compliance. Disponível em: <https://lec.com.br/os-10-pilares-de-um-programa-de-compliance/>. Acesso em: 24 abr. 2023.

necessidade de utilização dos dados em face da ponderação de bens e do princípio da proporcionalidade, em que circunstâncias isso seria permitido? A apuração de um crime de menor potencial ofensivo, como é o caso dos crimes contra a honra, justificaria a restrição de um direito fundamental? Que tipos de crimes justificariam a aplicação da ponderação de bens? O cidadão precisa ser informado sobre a utilização dos seus dados? Quais providências devem ser adotadas pelo Governo brasileiro, para que dados pessoais de investigados sejam respeitados durante o procedimento de investigação?

Embora diversas novas tecnologias utilizadas pelas policias para a investigação criminal também mereçam atenção dos legisladores[2], o objetivo deste trabalho não será responder essas questões. O foco desta pesquisa é tão somente a análise dos dados pessoais utilizados no dia a dia pelas policiais judiciárias brasileiras, na apuração dos crimes mais simples, também conhecidos como crimes de menor potencial ofensivo, aos crimes mais complexos, tais como os crimes hediondos.

Os dados pessoais obtidos através de provedores da internet, por exemplo, embora sejam de extrema importância para a investigação criminal, não estão inseridos no objeto deste trabalho. Os dados pessoais em questão, repita-se, são aqueles dados acumulados ao longo dos anos pelas polícias judiciárias brasileiras e que os cidadãos sequer desconfiam que estão sendo utilizados em um contexto de investigação de crimes. Os dados estão disponíveis aos servidores das polícias e podem ser utilizados sem autorização judicial, não havendo limites claros para que esses dados sejam acessados e processados para fins de apuração de crimes.

Percebe-se, portanto, que enquanto diversos estudiosos se preocupam com a utilização irregular de dados obtidos com o avanço da tecnologia, a preocupação deste autor, no entanto, é com a utilização daqueles dados que poucas pessoas se importam, por não imaginarem que estejam disponíveis e facilmente acessados por todos aqueles que participam de uma investigação criminal.

[2]Câmara dos Deputados. Comissão promove debate sobre o uso de ferramentas de reconhecimento facial no combate ao crime. Fonte: Agência Câmara de Notícias. Disponível em: https://www.camara.leg.br/noticias/1058042-comissao-promove-debate-sobre-o-uso-de-ferramentas-de-reconhecimento-facial-no-combate-ao-crime/. Acesso em 22 de nov. 2024.

A proposta de Emenda à Constituição que inseriu a proteção de dados como direito fundamental pode servir para regulamentar a utilização dos bancos dados, estabelecendo parâmetros e normas que visem coibir abusos e a má utilização dos sistemas dos órgãos públicos da segurança pública, que são alimentados pelos próprios titulares dos dados. A proteção de dados foi elevada ao mesmo patamar dos outros direitos fundamentais previstos no Artigo 5º da Constituição Federal.

A elevação da proteção de dados pessoais ao *status* de direito fundamental refletirá diretamente na atuação da atividade policial e no serviço público de um modo geral, porque o vazamento ou o mau uso do banco de dados pode ser considerada uma conduta grave, ocasionando severas responsabilizações. O Artigo 4º da Lei Geral de Proteção de Dados trouxe exceções à aplicação da lei, apresentando a utilização de dados no contexto das investigações criminais e de temas ligados à segurança pública, à defesa nacional e à segurança de Estado. A temática precisa de uma criteriosa regulamentação, sob pena do Estado ter acesso ilimitado e irrestrito de dados pessoais, bem como eterna possibilidade de visualização irrestrita.

Percebe-se, portanto, um problema vinculado aos limites da utilização dos bancos de dados das Polícias Judiciárias brasileiras. O objetivo deste trabalho também é fazer uma análise das normas legislativas e decisões judiciais, apontar caminhos para determinar limites, de acordo com parâmetros constitucionais.

1.4 Metodologia da pesquisa

A metodologia utilizada foi a da análise documental. Foram pesquisados livros, projetos de lei, teses e decisões judiciais. O método comparativo, porém, também se faz presente, já que em diversos momentos do texto o sistema jurídico brasileiro foi comparado a sistemas jurídicos de outros países. O método indutivo foi necessário para, a partir da análise de um protocolo da Polícia Civil do Distrito Federal, refletir sobre possíveis implicações na fiscalização dos bancos de dados das Polícias Judiciárias Brasileiras. Por esse motivo, será possível aferir a alternância das três metodologias. A descrição do protocolo para utilização de dados pessoais na Polícia Civil do Distrito Federal terá o objetivo de identificar o problema, levantar dados, analisar contexto atual com suas variáveis e possíveis soluções. Por fim, também foi feita uma entrevista semiestruturada com a Professora Heloisa Estellita, que fez parte da comissão de juristas que

elaborou o Anteprojeto Penal de Proteção de Dados para a Persecução Penal e Segurança Pública (LGPD Penal).

1.5 Importância do tema para os Direitos Constitucional, Penal e Processo Penal Brasileiros

No início do ano de 2022, o Congresso Nacional promulgou a Emenda à Constituição que tornou a proteção de dados pessoais em direito fundamental, transformando-o em cláusula pétrea, ou seja, que não pode ser alterada nem mesmo por Proposta de Emenda à Constituição, já que os direitos fundamentais previsos em nossa Constituição Federal são considerados valores inerentes a todo ser humano. Conforme será possível aferir adiante, o direito à proteção de dados já era previsto de forma implícita em nossa Carta Magna, que resguardava o direito à intimidade e à vida privada.

Conforme será possível aferir no decorrer do presente estudo, há uma omissão legislativa no tratamento de dados pessoais para fins penais, além da inexistência de trabalhos sobre bancos de dados das polícias judiciárias brasileiras, daí a importância do tema para o ordenamento jurídico brasileiro. Pretende-se, portanto, fazer uma abordagem diretiva sobre o tema, com base em princípios constitucionais, uma vez que tanto o Poder Judiciário quanto o Poder Legislativo terão a missão de suprir as lacunas existentes na utilização dos bancos de dados para fins penais.

1.6 Organização da Tese

O trabalho não tem o objetivo de abordar todos os artigos da Lei Geral de Proteção de Dados e do Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Persecução Penal. O principal intuito do estudo é sugerir a regulamentação da utilização de dados pessoais no Direito Penal e aferir em que circunstâncias o princípio fundamental da proteção de dados pode ser mitigado, diante de eventual utilização de informações armazenadas nos bancos de dados das polícias judiciárias brasileiras, para apuração dos mais variados tipos de delitos.

O estudo em questão foi elaborado levando em consideração a possibilidade de mudanças no Anteprojeto Penal de Proteção de Dados, antes da sua transformação em lei. Todo o trabalho, portanto, foi elaborado com base no direito fundamental da proteção de dados, expresso no Artigo 5º da nossa Constituição Federal. Atualmente, o que existe é um vácuo

legislativo por ausência de uma norma que regulamente a proteção de dados no âmbito da persecução penal. É provável que até a implementação de legislação específica, tenhamos decisões judiciais que resolvam essa omissão legislativa de forma provisória, porque, conforme já mencionado acima, é preciso estabelecer os parâmetros que devem ser utilizados para o acesso aos dados dos bancos de dados das Polícias Judiciárias brasileiras, de forma que o direito fundamental da proteção de dados sofra uma restrição mínima.

Para melhor compreensão do tema, será necessário discorrer sobre a revolução tecnológica ocorrida ao longo dos últimos 25 anos, o que nos permitirá compreender o caminho percorrido até a elaboração do Anteprojeto Penal de Proteção de Dados Pessoais para fins Penais. A abordagem das causas que motivaram a implementação da proteção de dados em solo brasileiro será de fundamental importância para entendimento do assunto. Assim, no capítulo 2, denominado "General data Protection Regulation – GDPR", será abordado o General Data Protection Regulation – GDPR, que serviu de referência para a implantação da Lei Geral de Proteção de Dados do Brasil. A análise da proteção de dados sob o prisma europeu será estudada, bem como a influência do referido Regulamento na Lei Geral de Proteção de Dados Brasileira. Embora se trate de um regulamento europeu, a análise de alguns tópicos da legislação deve ser observada para percepção da nossa atual legislação. Além disso, serão analisados quais os pressupostos para aplicação desse regulamento europeu.

No capítulo 3 será feita uma análise na Lei Geral de Proteção de Dados Brasileira, observando os principais objetivos da LGPD. Cabe salientar que o objetivo do estudo, conforme mencionado acima, não é aferir todos os artigos da legislação. Serão abordados, tão somente, os artigos que possam ter alguma relação com o Anteprojeto Penal de Proteção de Dados, bem como os artigos que tenham relação com o tratamento de dados pelo poder público. Aqui será debatida uma questão fundamental para o objeto do estudo, que é a utilização da LGPD na persecução penal diante da ausência de uma matéria específica que regulamente o tema.

O capítulo 4 terá como foco a Diretiva 2016/680 da União Europeia, que foi a legislação elaborada única e exclusivamente para a proteção de dados pessoais na persecução penal. Diferentemente do que ocorreu na Europa, quando a Diretiva entrou em vigor no mesmo dia do regulamento Europeu (GDPR), aqui no Brasil ocorreu um longo estudo para posterior elaboração do Anteprojeto Penal de Proteção de Dados. O estudo da Diretiva será relevante para compreensão de alguns pontos do Anteprojeto. Será feita uma abordagem do tratamento

de dados pessoais levando em consideração o direito fundamental da proteção de dados pessoais, o que influenciará diretamente no futuro das investigações criminais no Brasil.

O capítulo 5 será dedicado ao Anteprojeto Penal de Proteção de Dados, que atualmente se encontra parado no Congresso Nacional, à espera de algum parlamentar que o apresente na forma de Projeto de Lei. Serão estudados os fundamentos do Anteprojeto diante da atuação dos órgãos de persecução penal. O principal objetivo do capítulo será tentar demonstrar a necessidade e a urgência de regulamentação da proteção de dados na esfera penal.

No capítulo 06, o foco será o direito à privacidade e à proteção de dados na Constituição Federal. Embora seja recente a previsão do direito fundamental à proteção de dados pessoais, outras normas jurídicas já regulamentavam a privacidade e a proteção de dados no ordenamento jurídico brasileiro. Conforme será possível observar, o direito à proteção de dados pessoais foi reconhecido no julgamento da ADI 6.387, antes de ser incorporado ao texto constitucional, por intermédio da Emenda Constitucional número 115/2022.

Por fim, no capítulo 07, proponho uma análise de descrição do protocolo na utilização de dados pessoais, com a implementação de estratégias para o tratamento de dados armazenados pela Polícia Civil do Distrito Federal. Será feita uma análise da ponderação de bens jurídicos, a ser realizada pelo legislador e pelo judiciário, para aferir a proporcionalidade diante de eventual violação ao direito fundamental da proteção de dados pessoais. Será demonstrada a importância do armazenamento consciente de dados pessoais pelas policiais judiciárias brasileiras, bem como a necessidade da utilização desses dados como forma de prevenção e combate ao crime, desde que a prática seja devidamente autorizada por lei ou por decisão judicial. Por fim, será feita uma reflexão sobre as melhores estratégias para o tratamento de dados pessoais no direito penal, de forma que seja possível apresentar um modelo para a regulamentação do manuseio de dados pessoais na persecução penal.

Ao logo do estudo, proponho ao leitor uma análise crítica da proteção de dados no direito penal, visando estabelecer um modelo de regulação que seja mais apropriado e com mínimo de intervenção nos direitos fundamentais, principalmente no que diz respeito à privacidade e à proteção de dados pessoais. Acredito que o trabalho despertará a atenção dos estudiosos do direito e de outras áreas para a regulamentação do uso de dados pessoais pelas polícias judiciárias.

O objetivo do trabalho, portanto, não é estudar todos os artigos da Lei Geral de Proteção de Dados Pessoais e do Anteprojeto Penal de Proteção de Dados Pessoais para Persecução Penal e Segurança Pública. A pretensão aqui será abordar a questão da proteção de dados para fins penais, através da utilização dos bancos de dados das polícias judiciárias brasileiras, mais especificamente da Polícia Civil do Distrito Federal, o que será feito através da análise de protocolo.

Ao final do estudo, pretendo esclarecer se atualmente há proteção suficiente aos dados pessoais armazenados e se o acesso aos bancos de dados das Polícias Judiciárias Brasileiras, quando utilizados para a prevenção e investigação de crimes, viola ou não a proteção de dados pessoais. A questão nos faz refletir sobre a temática da proteção de dados para fins penais, porque conforme será visto ao longo deste trabalho, os órgãos jurisdicionais do Brasil e da Europa reconhecem, em algumas circunstâncias, a importância e a necessidade da garantia do direito fundamental à segurança pública para assegurar o pleno exercício de outros direitos fundamentais.

2 GENERAL DATA PROTECTIONON REGULATION – GDPR

O avanço da tecnologia nos trouxe avanços positivos e negativos em diversas áreas de nossas vidas. Com um toque na tela do celular, abrimos o despertador para programar o alarme que nos acordará no dia seguinte, olhamos o clima e aferimos que roupa será mais apropriada para usarmos durante o dia, pedimos um transporte, que através da geolocalização nos permite acompanhar o trajeto do motorista até parar em frente à porta de nossas casas, efetuamos pagamentos de contas sem sair de casa e conversamos por horas com pessoas queridas através de uma chamada de vídeo, mesmo estando a milhas de distância.

Segundo Manoel Castells, o mundo está há décadas em um acelerado processo de transformação estrutural. De acordo com o autor, a sociedade em que estamos vivendo atualmente desenvolveu-se em redes, o que faz com que as conexões das tecnologias digitais passem a ser determinantes nos dias de hoje. A revolução tecnológica foi estruturada com base em informações que transformaram o nosso modo de pensar, de produzir, de consumir, de negociar, de administrar, de viver, de morrer, de fazer guerra e de fazer amor[3].

Percebe-se, portanto, a existência de uma revolução tecnológica ainda em pleno crescimento, onde a informação através dos meios digitais impacta diariamente a nossa forma de viver, pensar e se manifestar. Sob o ponto de vista do objeto desse estudo, é possível afirmar que a referida transformação também afeta diretamente o processo penal e, consequentemente a investigação criminal. As mudanças invadem as nossas rotinas sem nos pedir licença e exige de nós uma postura adequada aos tempos atuais.

É bem verdade que a velocidade com que as transformações ocorrem não é a mesma velocidade que utilizamos para nos preparar para essas transformações. No que diz respeito ao tema em questão, será necessária uma análise acurada dos elementos probatórios na investigação criminal, principalmente no que diz respeito à proteção de dados, levando-se em conta o prisma constitucional.

Diariamente são feitos inúmeros acessos aos bancos de dados das polícias judiciárias brasileiras, com a principal intenção de produzir provas e de identificar autores de crimes. Embora a prática seja necessária para a persecução penal, é preciso que a utilização dos bancos

[3]CASTELLS, Manuel. A SOCIEDADE EM REDE. Rio de Janeiro: Paz e Terra, 2021, p. 18.

de dados esteja em plena consonância com preceitos constitucionais. Necessário fazer essas observações, porque sob o prisma constitucional é necessário observar a validade das provas que estão sendo colhidas no decorrer da investigação de um crime.

As primeiras notícias sobre o conceito de privacidade surgiram com a queda do sistema feudal, no mesmo momento em que ocorreram as transformações sociais, econômicas e políticas que chegaram com a Revolução Industrial, no final do Século XIX, especialmente na Europa. Naquela ocasião, quem possuía recursos financeiros construía suas próprias casas e se isolava dos demais, passando a usufruir de uma certa privacidade. Esse tipo de privilégio era destinado tão somente aos senhores feudais e aos membros das igrejas.

A privacidade não era considerada um direito fundamental propriamente dito, mas um privilégio daqueles que possuíam uma melhor condição financeira, o que os diferenciava das demais pessoas. No século XIX, diante da ascensão da burguesia, a privacidade passou a ser um valor existencial, passando a ser vista como o direito de estar só, ou como mencionou Danilo Doneda, "(...) tomando como garante de isolamento e da solidão(...)[4]".

A tecnologia, porém, também gerou alguns transtornos, uma vez que nossos dados pessoais passaram a ser cada vez mais expostos com facilidade. Até pouco tempo atrás, quase não se falava sobre proteção de dados no Brasil. O tema só começou a aparecer em solo brasileiro com o avanço das tecnologias mencionadas acima. Danilo Doneda foi um dos primeiros autores a mencionar a proteção de dados no Brasil, tendo como principal parâmetro a nossa Constituição Federal. Depois disso, conforme será possível aferir ao logo deste trabalho, essa visão já foi superada, porque diversos outros autores também seguiram o mesmo pensamento, sob a alegação de que a proteção de dados estava inserida, de forma implícita, inserida no direito fundamental à privacidade.

O que deve ser destacado é que o direito fundamental à privacidade está diretamente ligado à segurança de dados, conforme será demonstrado adiante. A privacidade se refere ao direito que qualquer pessoa tem para controlar suas informações pessoais, decidindo como as

[4]DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. In: TEPEDINO, Gustavo (Org.). Temas de direito civil. Rio de Janeiro: Renovar, 2000, p. 37-54.

informações serão compartilhadas e utilizadas por terceiros. Trata-se de um aspecto essencial da liberdade individual e da autonomia.

Para Danilo Doneda, em 1960 o tema "privacidade" possuiu um grande impacto nos Estados Unidos, também por conta da revolução tecnológica mencionada anteriormente. De acordo com o autor, vários foram os motivos que contribuíram para uma inflexão da tendência de "proteção de dados"[5]. Um modelo de Estado liberal se transmudava para o *welfare state* (mudança do relacionamento entre o cidadão e o Estado), consequência de movimentos sociais e das reivindicações da classe trabalhadora, o que ocasionou um crescimento do fluxo de informações, consequência do desenvolvimento tecnológico, ao qual correspondia a uma capacidade técnica cada vez maior de recolher, processar e utiliza a informação.

Quando se fala em privacidade, não se pode deixar de lado o artigo de Samuel Warren e Louis Brandeis. Os autores fizeram um ensaio denominado "O Direito à Privacidade" que se tornou fundamental para marcar o início das discussões sobre o direito à privacidade nos Estados Unidos. O ensaio foi escrito pelos referidos autores para abordar a privacidade das pessoas, em detrimento de fotografias registradas por parte da mídia sensacionalista. Warren e Brandeis alegaram que as pessoas possuíam o direito de serem "deixadas em paz" e de controlarem a divulgação de informações pessoais sobre si mesmas. O principal argumento do ensaio foi o de fortalecer a tutela da privacidade em casos de violação dos direitos do indivíduo, trazendo à tona o direito do ser humano à proteção da esfera privada[6].

Canotilho[7] sempre defendeu que o Estado de Direito deve ser um garantidor das liberdades individuais, protegendo os cidadãos dos arbítrios dos Poderes Públicos, defendendo que o direito à privacidade pode ser subdividido em outros dois direitos. O primeiro direito seria o direito a impedir o acesso de estranhos a informações sobre a vida privada e familiar; o segundo seria o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem.

---

[5]DONEDA, Danilo Cesar Maganhoto. Da privacidade à proteção de dados pessoais: Elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Thompson Reuters Brasil, 2020, p, 440/454.

[6]WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. Harvard Law Review, v. 4, n.5., Dec. 15,1890. Disponível em: http://links.jstor.org/sici?sici=0017811x%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C. Acesso em 25 abr. 2024.

[7]CANOTILHO, José Joaquim; MOREIRA; Vital. Constituição da República Portuguesa anotada. 1. Ed. Brasileira. Revista dos Tribunais, 2007.

De acordo com Laura Schertel Mendes, no ensaio de Warren e Brandeis "a proteção à privacidade teve um caráter fortemente individualista, em seus primórdios, com a sua feição do direito a ser deixado só (*right to be let alone*)"[8]. Priorizando a importância e a necessidade de equilibrar a liberdade de expressão e o direito à privacidade, Brandeis e Warren discutiram a "fotografia instantânea", que à época foi uma inovação para o jornalismo americano, o que fez com que jornais passassem a publicar fotografias e declarações das pessoas sem obter o seu consentimento.

Warren e Brandeis argumentavam que:

> A imprensa está ultrapassando em todas as direções os limites óbvios do decoro e da decência. A fofoca não é mais o recurso dos ociosos e dos viciosos, mas tornou-se um comércio, que é praticado com diligência e descaramento. Para satisfazer um gosto lascivo, os detalhes das relações sexuais são divulgados nas colunas dos jornais diários. Para ocupar os indolentes, coluna após coluna está cheia de fofocas ociosas, que só podem ser obtidas por intrusão no círculo doméstico. (...)" – Trecho do ensaio. (Tradução nossa)[9].

Os Autores sugeriram que a privacidade pudesse ser tutelada no Direito Norte Americano[10], embora os direitos autorais já fossem garantidos pelo ordenamento jurídico, sendo denominados como *"bem jurídico passível de controle pelo seu titular".* Visando alcançar o mesmo status para o direito à privacidade, Warren e Brandeis o conceituaram como *"(...) Controle das Informações ligadas à esfera íntima (...)"*, tornando-os conhecidos como os idealizadores da "privacidade".

Já em 1960, diante do avanço da tecnologia, também denominada de sociedade da informação, a privacidade deixou de ser o *"direito de ser deixado só"* e passou a ser protegida com a finalidade da busca pelo livre desenvolvimento da personalidade humana[11]. A partir

[8]MENDES, Laura Schertel. Privaciade, proteção de dados e defesa do consumidor. São Paulo: Saravia, 2014, p.28.
[9]LAURENTTIS, Lucas de. Enciclopédia Jurídica da PUC-SP. Proteção de Dados Pessoais. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/557/edicao-1/protecao-de-dados-pessoais. Acesso em 27 de out. 2024.
[10]WARREN, Samuel; BRANDEIS, Loius D. The Right to Privacy. In: Harvard Law Review, Vol.4, nº 05 (Dec. 15, 1890). p. 193-220.
[11]BAIÃO, Kelly C. Sampaio; GONÇALVES, Kalline Carvalho. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. Civilistica.com. Rio de Janeiro. Ano 03, nº 02, (jul. – dez.2014). [Com.25 abril 2018]. Disponível em: http://civilista.com/agarantia-da-privacidade-na-sociedade-tecnologica-um-imperativo-a-concretizacao-do-principio-da-dignidade-da-pessoa-humana/>. Acessado em 25 de abril de 2024.

disso, em 1965, o direito à privacidade foi reconhecido pela Suprema Corte dos Estados Unidos, no caso *Griswold x Connecticut*[12].

Durante o ano de 1879, o Estado de Connecticut aprovou uma lei que proibia o uso de qualquer droga, dispositivo médico ou outro instrumento para promover a contracepção[13]. Um ginecologista da Escola de Medicina Yale, C. Lee Buxton, abriu uma clínica de controle de natalidade em New Havem, em conjunto com Estelle Griswold. Eles foram presos e condenados por violarem a lei, ocasião em que suas condenações foram confirmadas pelos Tribunais Estaduais Superiores. Não conformados com as decisões que lhes condenaram, os réus decidiram contestar a constitucionalidade do Estatuto da Décima Quarta Emenda perante a Suprema Corte.

O principal questionamento feito para a Suprema Corte foi indagar se a Constituição Americana protegia o direito à privacidade conjugal contra as restrições estatais à capacidade de um casal ser aconselhado sobre a utilização de métodos contraceptivos, demonstrando que o direito à privacidade poderia ser visto sob vários aspectos da declaração universal de direitos, o que impedia que os Estados tornassem ilegal a vedação de uso de métodos contraceptivos para casais casados.

A Suprema Corte decidiu, por maioria de 7 a 2, que a Constituição Americana, de fato, protegia o direito à privacidade no casamento contra restrições estaduais sobre a escolha de um casal em ser aconselhado para a utilização de métodos contraceptivos. Foi frisado que embora a Constituição não protegesse explicitamente um direito geral à privacidade, as várias garantias dentro da Declaração de Direitos criavam penumbras ou zonas que estabeleciam um direto à privacidade. Ficou demonstrado que a lei de Connecticut conflitava com o exercício desse direito, o que fez com que a Suprema Corte a considerasse nula e sem efeito. Com o reconhecimento da inconstitucionalidade da lei do Estado de Connecticut, conferiu-se status constitucional à privacidade, que foi justamente o que Warren e Brandeis buscaram anos antes, quando escreveram o já mencionado artigo[14].

---

[12]Cornell Law School. **Griswold v Connecticut.** Disponível em: https://www.law.cornell.edu/wex/griswold_v_connecticut_(1965). Acessado em 25 de abril de 2024.
[13] *Ibid.*
[14] *Ibid.*

Em Portugal, a temática do direito à privacidade demorou um pouco mais para ser abordada. José Joaquim Gomes Canotilho e Vital Moreira[15] afirmam que o direito à privacidade consiste no direito à reserva da intimidade da vida privada e familiar, dividindo-se em dois direitos menores. O primeiro seria o direito de impedir o acesso de estranhos a informações sobre a vida privada e familiar e o segundo seria o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem.

No contexto Brasileiro, o direito à privacidade foi incorporado ao ordenamento jurídico pela Constituição de 1988, no Artigo 5º Inciso X[16], e no Artigo 21 do nosso Código Civil de 2002[17]. Cabe ressaltar que outros direitos fundamentais derivam do direito à privacidade. Podemos citar como exemplo a inviolabilidade do domicílio, a inviolabilidade de correspondência, bem como o sigilo das comunicações, todos previstos no Artigo 5º da Constituição Federal.

Segundo Orlando Gomes, em 1957 os direitos da personalidade já estavam previstos em alguns ordenamentos jurídicos, tais como o japonês, o grego e o egípcio. No ano de 1966, foi previsto no Artigo 17 do Pacto Internacional sobre Direitos Civis e Políticos[18], que "Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, ne de ofensas ilegais às suas honra e reputação"[19]. O pacto foi um instrumento por meio do qual os Estados partes das Nações Unidas que o aderiram e o ratificaram, assumiram o compromisso de respeitar e garantir a todos os indivíduos que se achem em seus territórios e que estejam sujeitos às suas jurisdições.

---

[15]CANOTILHO, José Joaquim Gomes; MOREIRA, Vital. Constituição da República Portuguesa Anotada. Vol. I. Coimbra: Coimbra Editora, 2007, p.467-468.

[16]BRASIL. Artigo 5º Inciso X da Constituição Brasileira de 1988: Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no país a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) "Inciso X: São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação"(...). Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acessado em 25 abr. 2024.

[17]BRASIL. Artigo 21 do Código Civil Brasileiro: A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 26 de abr. 2024.

[18]Pacto Internacional sobre Direitos Civis e Políticos. Disponível em: https://www.gov.br/mdh/pt-br/navegue-por-temas/atuacao-internacional/relatorios-internacionais-1/pacto-internacional-sobre-direitos-civis-e-politicos#:~:text=Instrumento%20por%20meio%20do%20qual,alguma%20por%20motivo%20de%20ra%C3%A7a%2C. Acesso em: 29 abr. 2024.

[19]GOMES, Orlando. Introdução ao direito civil. Rio de Janeiro: Forense Editora, 2019, p. 106. *E-book.*

Nos dias de hoje, a Declaração Universal dos Direitos Humanos de 1948[20] faz previsão do Direito à Intimidade em seu Artigo 12. A mesma previsão pode ser vista em diversas outras declarações e convenções pelo mundo. Os Estados Unidos, desde o já mencionado artigo "*Right to Pracy*" de Samuel Dennis Warren e Louis Dembitz Brandeis, passaram a respeitar mais a intimidade[21], o que influenciou diversas decisões judiciais na Suprema Corte Americana.

A doutrina alemã adotou a teoria das esferas, que sugere a divisão da privacidade e da intimidade em três esferas[22]. A primeira foi denominada de *esfera íntima*, por ser de âmbito mais interno e intangível da liberdade humana. Seriam os assuntos mais secretos e reservados, que não devem ser de conhecimento de outras pessoas, devido ao nível de sua confidencialidade. A segunda foi chamada de *esfera privada ampla*, de âmbito privado, mas que não pertence à esfera mais interna. Como exemplos, podemos citar os assuntos compartilhados com pessoas de nossa confiança, e não a todas as pessoas. Percebe-se que na segunda esfera, a proteção é menos intensa que na esfera íntima. Por fim, a terceira foi definida como *esfera social*, que não é englobada pelas esferas anteriores, porque trata-se de questões relacionadas a notícias e informações que a pessoa deseja excluir do conhecimento de terceiros.

Sobre a última esfera, podemos citar o exemplo de um indivíduo, ex presidiário, que está prestes a ser contratado. Embora todos tenham o direito de recomeçar suas vidas, geralmente através da reintegração ao convívio social por meio da ressocialização, o que é um dever do Estado, é bem provável que esse candidato à vaga não queira que o futuro empregador tenha acesso aos seus antecedentes criminais. As informações do candidato, portanto, fazem parte da terceira esfera, a social, porque o empregador pode ter o direito de saber se a pessoa que está contratando já praticou algum delito.

Inclusive, a exigência de antecedentes criminais como exigência para vaga de emprego possui relação com o objeto do presente estudo, porque, de alguma forma, a utilização de informações que constam nos bancos de dados das Policiais Judiciárias Brasileiras, atinge uma

[20]Declaração Universal dos Direitos Humanos. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 29 de abr de 2024.
[21]*Ibid.*
[22]MARQUES, Andrea Neves Gonzaga. Direito à Intimidade e Privacidade. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2010/direito-a-intimidade-e-privacidade-andrea-neves-gonzaga-marques. Acesso em 29 de abr. 2024.

dessas esferas. Até que ponto as informações podem ser utilizadas em uma investigação policial, sem que o direito fundamental à proteção de dados seja violado?

O Tribunal Superior do Trabalho entendeu que a exigência de antecedentes criminais para a contratação de empregados é ilegal, salvo nas seguintes situações: quando a exigência está prevista em lei, como no caso de vigilantes, por exemplo ou quando a exigência é justificada pela natureza do cargo ou pelo grau de confiança necessário, como para motoristas de carga, cuidadores de idosos, bancários, entre outros[23]. Caso a empresa exija a certidão de antecedentes criminais sem uma justificativa plausível, o candidato ao emprego pode ter direito a uma indenização por danos morais[24].

Sobre o direito à privacidade, Gilmar Ferreira Mendes e Paulo Gustavo Gonet Branco ressaltam que:

> Estar submetido ao constante crivo da observação alheia dificulta o enfrentamento a novos desafios. A exposição diuturna dos nossos erros, dificuldades e fracassos à crítica e à curiosidade permanentes de terceiros, e ao ridículo público mesmo inibiria toda tentativa de autossuperação. Sem a tranquilidade emocional que se pode aferir da privacidade, não há muito menos como o indivíduo pode se autoavaliar, medir perspectivas e traçar metas[25].

Percebe-se, portanto, que ao longo dos anos o direito à privacidade deixou de ser analisado sob o ponto de vista da individualidade, resguardando o direito de o indivíduo permanecer sozinho, para se transformar em um direito fundamental coletivo, que atinge toda a sociedade e que serve de desdobramento para outros direitos fundamentais. Para Danilo Doneda, isso se deve ao reconhecimento do direito à privacidade como como espécie de direito fundamental, com a sua consequente funcionalização, permitindo desdobrá-lo em uma série de direitos subjetivos, tais como o direito à vida privada e à vida familiar, mas também à proteção dados pessoais[26].

---

[23]TST, RR-1269-65.2017.05.-7.0032, Sétima Turma, Rel. Min. Renato de Lacerda Paiva, J, 20.01.2021, DJe .29.01.2021.
[24]*Ibid.*
[25]MENDES, Gilmar Ferreira; Branco, Paulo Gustavo Gonet. Curso de Direito Constitucional. 11. Ed. São Paulo: Saravia, 2016, p. 255.
[26]DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019.

A tutela dos dados pessoais ultrapassa uma proteção individual, como é tradicionalmente aquela conferida ao direito à privacidade, apresentando também uma "dimensão coletiva", através do reconhecimento dos dados pessoais como instrumento apto ao controle político dos indivíduos e suscetível de uso para discriminar grupos minoritários[27].

Vários aspectos do direito à privacidade sempre foram protegidos e valorizados pelas sociedades. No entanto, até determinado período, a tutela conferida não era respaldada pela noção de privacidade. Segundo Doneda, a mudança só começou a ocorrer no século XVII, com a formação do Estado-nação e o fim do feudalismo, ocasião em que ocorreu o reconhecimento de uma esfera particular de atuação, livre das interferências do Estado[28].

Ainda de acordo com o autor, talvez em nenhum outro país esses fatores tenham sido tão presentes no século XIX quanto nos Estados Unidos da América. Conforme será possível aferir adiante, não foi por acaso que a discussão sobre o *right to privacy* surgiu nos EUA, com o artigo de Warren e Brandeis, de 1890, intitulado *"The right to privacy"*[29].

As revoluções burguesas deram um novo passo ao intensificarem o ideal individualista, enquanto as revoluções industriais forneceram meios materiais para permitir o isolamento das pessoas, através de moradias menores e urbanas, com núcleos familiares reduzidos e protegidos da curiosidade alheia por novas técnicas[30]. Percebe-se, portanto, que no decorrer dos anos a privacidade se transformou em proteção de dados pessoais e direito fundamental.

Um fato curioso é que a cada ano, com o avanço da era digital, fica mais complexo resguardar de forma ampla o direito fundamental em questão. Apenas a título de exemplo, segundo consta no site da ONU – Organização das Nações Unidas, em todo o mundo existem aproximadamente 5,3 bilhões de usuários de internet, ou seja, mais da metade das pessoas que habitam o globo terrestre[31]. Isso significa dizer que uma grande parte desses usuários expõem

[27]DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019.
[28]*Ibid.*
[29]*Ibid.*
[30]*Ibid.*
[31]Organização das Nações Unidas. Crescimento da internet desacelera e 2,7 bilhões ficam fora da rede. Disponível em: https://news.un.org/pt/story/2022/09/1801381. Acesso em 26 de abril de 2024.

suas vidas e, consequentemente, sua privacidade, o que merece ser refletido sobre a forma como utilizamos a internet nos dias de hoje.

Com o intuito de utilizar estratégias mais eficientes para captar clientes, empresas de grande porte começaram a fazer uso dos dados abertos da internet. A utilização da *big data*[32] serve para analisar o histórico de pesquisas, o nome e o comportamento dos consumidores. As empresas alegam que a prática serve para melhorar a relação com o cliente, otimizando tempo e garantindo mais assertividade no atendimento.

Até chegarmos ao que está sendo debatido nos dias atuais, um longo caminho foi percorrido. Embora o tema central do objeto de estudo esteja vinculado à proteção de dados no âmbito da atividade policial, é preciso passar pelos principais pontos que regulamentam a proteção de dados no Brasil e no exterior. Por esse motivo, é necessário mencionar a importância que o *General Data Protection Regulation* teve para que hoje estejamos debatendo o tema deste trabalho, que é a análise do impacto do Anteprojeto Penal de Proteção de Dados Pessoais no direito penal e nos bancos de dados das Polícias Judiciárias brasileiras[33].

O GDPR é o Regulamento Geral de Proteção de Dados na União Europeia que estabelece regras sobre a privacidade e a proteção de dados de cidadãos da União Europeia e do Espaço Econômico Europeu. O Regulamento foi criado para proteger os direitos dos cidadãos europeus em relação ao uso dos seus dados pessoais por empresas ou outras organizações. Ele define as obrigações das empresas em relação à coleta, armazenamento, processamento e compartilhamento de dados pessoais, além de definir as penalidades nos casos em que ocorram violações a esses direitos.

O GDPR entrou em vigor em maio de 2018 e se aplica a todas as empresas que processam dados pessoais dos cidadãos da União Europeia, independentemente do local onde a empresa esteja localizada. O Regulamento também estabelece os direitos dos cidadãos no que

[32]Trecsson Business Scholl. O que é big data? Conceitos, Definição, Exemplos. Big data é um volume gigante (mas gigante mesmo) de dados que vão sendo coletados sistematicamente de várias fontes e que podem ser usados - a depender de seu objetivo - para tomadas de decisões de negócios, para escolhas estratégicas ou para sugestão de ação para um determinado usuário. É desta forma que o serviço de streaming consegue entender o seu gosto por determinados filmes, séries, músicas, ou qualquer outra coisa.Disponível em: https://www.trecsson.com.br/blog/tecnologia-e-ciencia-de-dados/o-que-e-big-data. Acesso em 01 de out. 2024.
[33]*Ibid.*

diz respeito aos seus próprios dados pessoais, dando-lhes a possibilidade de acessar, corrigir e excluir esses dados.

Há muitos anos percebe-se que a União Europeia preocupa-se com a questão da proteção de dados, o que resultou na implementação do Regulamento. O GDPR passou a vigorar, de fato, em 25 de maio de 2018, 24 meses depois da sua publicação. Até a sua efetiva publicação, ocorreram logos debates e contribuições, quem contaram com a participação de diversos especialistas das mais variadas áreas. O texto definitivo levou 4 anos para ser aprovado, o que fez com que diversos pontos importantes fossem minuciosamente incluídos na legislação que hoje se tornou uma referência para vários países[34].

Além da proteção de dados dos cidadãos europeus, os legisladores também se preocuparam com a proteção de dados dos países que de alguma forma se relacionam com países que compõe o bloco da União Europeia. Um dos pontos mais importantes do GDPR, porém, foi a padronização da proteção de dados em todos os países da União Europeia.

O que deve ser destacado é que o GDPR revogou a Diretiva 95/46/CE[35], que serviu de base para a atual legislação, porque previa um sólido texto sobre proteção de dados, o que englobava princípios, direitos e deveres dos titulares de dados. A Diretiva 95/46/CE foi aprovada no dia 24 de outubro de 1995, mas só entrou em vigor três anos depois. Um ponto que merece destaque foi o fato de, à época da sua vigência, fazer constar a exigência para que cada país membro da União Europeia tivesse uma agência ou comissário de proteção de dados. No caso do comissário de proteção de dados, havia outra exigência. A de que um agente estatal supervisionasse a aplicação dos princípios e leis de proteção à privacidade individual.

Diferentemente da Diretiva 05/46/CE, o GDPR fez a previsão de aplicação imediata a todos os países da União Europeia, sem a necessidade de uma legislação complementar para regulamentar a questão. Isso fez com que todos os países da União Europeia mantivessem o mesmo patamar mínimo de proteção de dados, o que foi um grande diferencial, porque a legislação anterior foi promulgada em um período onde a informatização de dados estava em

[34] *Ibid.*
[35] Diretiva 95/46/CE. Disponível em < https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em 26 dez. 2023.

um estágio prematuro, fazendo com que cada um dos países integrantes da União Europeia tivesse que editar normas internas para que a norma fosse de fato aplicada.

Após breve estudo sobre a evolução das normas europeias que tratam sobre proteção de dados, é possível aferir que o GDPR foi um verdadeiro marco, não só para os países da União Europeia, mas também para outros países do mundo, inclusive o Brasil. Além da União Europeia, os Estados Unidos também se tornaram eficientes quando o assunto é proteção de dados pessoais. Uma das principais diferenças entre os países da União e Europeia e os Estados Unidos é que no país americano não há uma única legislação, como o GDPR, mas normas esparsas que visam proteger dados pessoais. Nos Estados Unidos, a proteção de dados é regulada pelo *Privacy Act* de 1974[36], o qual estabelece um código de práticas para reger a coleta, manutenção, uso e disseminação de informações sobre indivíduos.

O *General Data Protection Regulation*, exige o preenchimento dos seguintes requisitos para o tratamento de dados pessoais[37]: Consentimento do Titular dos Dados: O GDPR exige que o consentimento para coleta e processamento de dados pessoais seja dado de forma clara e inequívoca; Direitos dos Titulares dos Dados: A regulamentação confere aos indivíduos uma série de direitos, incluindo o direito de acessar seus dados pessoais, o direito de retificar dados incorretos, o direito de ser esquecido (ou seja, de ter seus dados apagados), e o direito à portabilidade dos dados; Responsabilidade e Transparência: As organizações são obrigadas a adotar medidas adequadas para proteger dados pessoais e devem ser capazes de demonstrar a conformidade com a GDPR, o que inclui manter registros detalhados das atividades de processamento de dados; Notificações de Violação de Dados: O GDPR exige que a divulgação de dados notificados às autoridades reguladoras e, em certos casos, aos indivíduos afetados, geralmente dentro de 72 horas após a organização ter conhecimento da violação; Penalidades por não Conformidade: Organizações que não cumprem o GDPR podem enfrentar prejuízos graves, quem podem chegar a 4% do faturamento anual global da empresa ou 20 milhões de euros, o que acaba sendo ainda maior e Alcance Extraterritorial: O GDPR não se aplica apenas às empresas sediadas na União Europeia, mas também às empresas fora da EU, mas que processam dados de indivíduos localizados na UE.

[36]Justice.Gov. Privacy Act of 1974. Disponível em < https://www.justice.gov/opcl/privacy-act-1974#:~:text=The%20Privacy%20Act%20of%201974%2C%20as%20amended%2C%205%20U.S.C.,of%20records%20by%20federal%20agencies.>. Acesso em 01 jan. 2024.

[37]General Data Protection Regulation – GDPR. Disponível em < https://gdpr-info.eu/>. Acesso em 13 nov. 2023.

Por esse motivo, o *General Data Protection Regulation* é considerado até hoje a norma jurídica mais rigorosa no mundo quando o tema é a proteção de dados, o que o tornou uma referência para diversos outros países, incluindo o Brasil, fazendo com que a Europa seja apontada como baliza e *standard* em matéria de proteção de dados[38].

2.1 Proteção de Dados sob o prisma Europeu

O Regulamento Geral sobre a Proteção de Dados da União Europeia, eu seu artigo 4.0, conceitua dados pessoais como sendo a informação relativa a uma pessoa singular identificada ou identificável (titular dos dados). Ainda de acordo com o regulamento[39], é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

A proteção de dados é um direito fundamental na União Europeia, o que faz com que os países do bloco sejam vistos como referência para os demais países de outros continentes. A proteção de dados visa garantir a preservação da vida privada e a segurança de dados pessoais de todos os cidadãos europeus, promovendo confiança no ambiente digital, incentivando o desenvolvimento econômico e a inovação tecnológica[40].

Conforme já mencionado anteriormente, as principais regras da União Europeia em matéria de proteção de dados são o Regulamento Geral sobre a Proteção de Dados (RGPD) e a Diretiva 680/2016 (UE)[41], que dispõe sobre a Proteção de Dados para fins penais. O RGPD

[38]Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia / Viviane Nóbrega Maldonado, Renato Opice Blum, coordenadores. 3ª ed. São Paulo: Thompson Reuters Brasil, 2021.
[39]General Data Protection Regulation – GDPR. Disponível em < https://gdpr-info.eu/>. Acesso em 13 nov. 2023.
[40]Proteção de Dados na UE. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pt. Acesso em 27 de out. 2024.
[41]DIRETIVA (UE) 2016/ 680 DO PARLAMENTO EUROPEU E DO CONSELHO - de 27 de abril de 2016 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas aut oridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/ 977/ JAI do Conselho. [s.d.]. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=HU>. Acessado em 01 de out. 2024.

estabelece requisitos pormenorizados para o recolhimento, o armazenamento e a gestão de dados pessoais, bem como os direitos e deveres dos titulares dos dados, dos responsáveis pelo tratamento e dos subcontratantes. A Diretiva sobre a Proteção de Dados entrou em vigor em 2016 e protege os dados pessoais das vítimas, testemunhas e suspeitos de crimes quando são utilizados por autoridades responsáveis pela aplicação do direito penal, como as autoridades policiais ou judiciárias.

A União Europeia também possui um Comité Europeu para a Proteção de Dados[42], que é um órgão independente, responsável por assegurar a aplicação coerente das regras da União Europeia em matéria de proteção de dados. Além disso, o Comitê Europeu emite orientações e recomendações sobre questões relacionadas à proteção de dados. Cada país da União Europeia tem uma autoridade nacional de proteção de dados, que é responsável por supervisionar o cumprimento das regras da UE em matéria de proteção de dados no seu território e por cooperar com as outras autoridades nacionais de proteção de dados.

O Comitê Europeu para Proteção de Dados[43] disponibiliza, ainda, orientações gerais, tais como diretrizes, recomendações e boas práticas, para tornar mais claro tudo o que está especificado no RGPD. Outra prática relevante é a adoção de conclusões para garantir que o RGPD seja interpretado da mesma forma por todas a entidades reguladoras nacionais, como, por exemplo, nos casos que envolvam dois ou mais países. Além disso, o Comitê aconselha a Comissão Europeia sobre questões relativas à proteção de dados e qualquer proposta de nova legislação da União Europeia que seja de especial importância para a proteção dos dados pessoais, incentivando as autoridades nacionais de proteção de dados a colaborarem e a partilharem informações e boas práticas.

Qualquer cidadão que não tenha os seus dados devidamente protegidos[44], pode entrar em contato diretamente com a instituição que violou os dados pessoais, acionar a autoridade nacional de seu país ou submeter o assunto a um tribunal nacional. As autoridades nacionais de proteção de dados realizam investigações e aplicam sanções sempre que necessário.

---

[42]European Union. Comitê Europeu para Proteção de Dados. Disponível em: <https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-board-edpb_pt. >. Acesso em 01 jan. 2024.

[43] *Ibid.*

[44]European Union. A proteção de dados ao abrigo do RGPD. Disponível em: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_pt.htm. Acesso em 27 de out. 2024.

Um dos principais instrumentos de proteção dos direitos fundamentais na Europa, a Carta de Direitos Fundamentais da União Europeia[45], preceitua em seu Artigo 8º que todas as pessoas têm direito à proteção de dados de caráter pessoal que lhes digam respeito. O referido dispositivo legal também destaca que os dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei.

A temática é levada tão a sério na União Europeia, que o *European Data*[46], portal europeu de dados, disponibiliza relatórios anuais sobre dados pessoais. O site conta com diversos documentos e resultados de investigações de outras instituições, compartilhando histórias de sucesso quando o assunto é a proteção de dados pessoais.

Apenas a título de exemplo, no ano de 2020 o *European Data* divulgou relatório sobre o resultado do impacto econômico de dados abertos[47], o que gerou aumento positivo na economia da União Europeia. O estudo permitiu estimar o crescimento da economia em diversos setores e possibilitou prever a possibilidade de salvamento de vidas, de tempo economizado, de benefícios ambientais e de melhoria de serviços.

Percebe-se, portanto, que a legislação europeia de proteção de dados é uma referência para outros países. O que deve ser destacado, porém, é que o marco legal europeu buscou impor o seu padrão cultural para outros países que possuem hábitos diferentes, como é o caso do Reino Unido, que utiliza a sua própria Lei Geral de Proteção de Dados[48]. O principal objetivo do GDPR foi influenciar os países membros da União Europeia a terem patamar mínimo de proteção de dados, mantendo a soberania de cada um desses países.

---

[45]Carta de Direitos Fundamentais da União Europeia. Artigo 8º. Proteção de dados pessoais. 1 - Todas as pessoas tem direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2 - Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas tem o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3 - O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12012P/TXT. >. Acesso em 02 jan. 2024.

[46]European Data. Disponível em: <https://data.europa.eu/pt/publications/overview. >. Acesso em 02 jan. 2024.

[47]Impacto do Valor Econômico dos Dados Abertos. Disponível em: < https://data.europa.eu/pt/publicacoes/open-data-impact. >. Acesso em 02 jan. 2024.

[48]UK ETA. A lei de proteção de dados do Reino Unido pode alterar a forma como a ETA armazena os dados. Disponível em: https://uk-eta.com.br/a-lei-de-protecao-de-dados-do-reino-unido-pode-alterar-a-forma-como-a-eta-armazena-os-dados/. Acesso em 28 de out. 2024.

O *General Data Protection Regulation* se tornou uma norma geral de proteção de dados para toda a União Europeia, mas cada país teve autonomia para regulamentar determinados temas de acordo com os aspectos locais, como por exemplo a proteção de dados pessoais para fins penais[49]. Embora exista essa liberdade, o GDPR estabeleceu alguns parâmetros que são considerados fundamentais, tais como licitude, equidade, transparência, limitação da finalidade, minimização de dados, precisão, limitação de armazenamento, integridade, confiabilidade e prestação de contas.

Os debates sobre proteção de dados em solo Europeu, no entanto, começaram bem antes da entrada em vigor do atual *General Data Protection Regulation* (GDPR). Para Guilherme Guidi[50], no começo do século XIX na França, os tribunais relutavam em reconhecer um direito subjetivo à proteção da intimidade e tratavam o assunto como uma situação excepcional. Os tribunais franceses só falaram do direito à privacidade de forma incidental, em uma decisão de 1958, no caso Felix c O´Connell[51].

Somente em 1970 ocorreu a modificação do Artigo 9º do Código Civil Francês para introduzir um direito ao respeito da vida privada[52], o que fez com que os tribunais passassem a deferir diversas decisões sobre direito à privacidade. Ainda de acordo com Guilherme Guidi[53], na Itália a questão do direito à privacidade começou a chamar atenção em 1971, com o caso Fiat. Naquele ano foi tornada pública a informação de que a Fiat, fabricante de veículo, estava utilizando, desde 1948, dados pessoais fornecidos pela polícia, pelos militares e pelo serviço secreto italiano, para selecionar seus empregados. Esse fato foi marcante porque fomentou o início de debates sobre privacidade e dados pessoais no cenário legislativo do país, o que fez com que outros países vizinhos também se preocupassem com o mesmo tema.

[49]Agência Brasil. Legislação de proteção de dados já é realidade em outros países. Disponível em: https://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises. Acesso em 28 de 0ut. 2024.
[50]GUIDI, Guilherme Berti de Campos. Proteção de Dados Pessoais: A composição de Sistemas pelo Direito Internacional. 2021. 215f. Tese (Doutorado). Faculdade de Direito. Programa de Pós-Graduação. Área de concentração: Direito Internacional. Universidade de São Paulo. São Paulo.
[51]O´Connell, Felix C. The Rigth To Privacy. Disponível em: https://www.cambridge.org/core/books/abs/right-to-privacy/felix-c-oconnell/86C0D205334505A29DD621208909355C. Acesso em 23 de set. 2024.
[52]FERNANDES, Milton, Proteção Civil da Intimidade. São Paulo: Saraiva, 1977.
[53]*Ibid.*

Se formos comparar os sistemas de proteção de dados dos Estados Unidos e da União Europeia, será possível aferir diferenças. Enquanto a União Europeia concentra a regulamentação da proteção de dados no GDPR, nos Estados Unidos essa abordagem é mais fragmentada, porque, conforme já mencionado anteriormente, várias leis federais e estaduais regulamentam diversos tipos de dados pessoais. Apenas a título de exemplo, a lei *Health Insurance Portability and Accountability* (HIPAA)[54] protege informações sobre saúde de pacientes; a *Childen's Online Privacy Protection Rule* (COPPA)[55] protege a privacidade das crianças on line; e o *Califórnia Consumer Privacy Act* (CCPA)[56], lei de privacidade do consumidor da Califórnia, que oferece aos residentes da Califórnia direitos sobre seus dados pessoais.

O GDPR, portanto, é uma lei de abrangência no âmbito da União Europeia que se aplica a todas as empresas que tenham contato com dados pessoais dos cidadãos que residem em um dos Estados da União Europeia. Conforme mencionado alhures, nos Estados Unidos a legislação é setorial e varia de Estado para Estado. O GDPR exige consentimento explícito para o tratamento de dados pessoais, ao passo que algumas leis dos Estados Unidos admitem o consentimento implícito. Por fim, o GDPR permite o direito ao esquecimento, enquanto nos Estados o esquecimento pode variar de lei para lei.

2.2 Influência do General Data Protection Regulation – GDPR, na elaboração da Lei Geral de Proteção de Dados Brasileira – LGPD

O *General Data Protection Regulation* – GDPR, já mencionado acima, é um regulamento da União Europeia que estabelece regras sobre privacidade e proteção de dados de cidadãos da União Europeia e do espaço econômico europeu. A Lei Geral de Proteção de Dados – LGPD é uma lei brasileira que busca fornecer a todos um efetivo controle dos seus dados pessoais. As duas legislações têm o mesmo objetivo, ou seja, buscam proteger os direitos dos cidadãos em relação aos seus dados pessoais, incluindo o direito de saber quais dados estão sendo coletados, como eles estão sendo usados e com quem estão sendo compartilhados.

---

[54]U.S. Departament of Health and Human Services. Health Insurance Portability and Accountability – HIPAA. Disponível em: https://www.hhs.gov/hipaa/index.html. Acesso em 23 de set. 2024.

[55]Federal Trade Commission. Childen's Online Privacy Protection Rule – COPPA. Disponível em: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa. Acesso em 23 de set. 2024.

[56]IBM. Califórnia Consumer Privacy Act - (CCPA). Disponível em: https://www.ibm.com/br-pt/topics/ccpa-compliance. Acesso em 23 de set. 2024.

Até agosto de 2018, o Brasil era um dos poucos países com uma das maiores economias do mundo[57] que não possuía uma legislação para proteger dados pessoais. As principais normas que regulamentavam a privacidade de dados no Brasil eram o Marco Civil da Internet, o Código Civil e o Código de Defesa do Consumidor. O Brasil, portanto, foi uma das últimas democracias da América Latina a ter uma legislação sobre proteção de dados pessoais. Devido à pressão comercial pela manutenção das relações com os países da União Europeia, o Brasil se empenhou na implementação da atual Lei Geral de Proteção de Dados. Abaixo será possível perceber que a LGPD é quase uma cópia da GDPR.

Embora haja muitas similaridades entre a LGPD e o GDPR, os dois dispositivos possuem diferenças importantes. O GDPR, por exemplo, é a vanguarda do direito de privacidade de dados pessoais e possui amplitude a todo cidadão membro da União Europeia, enquanto a LGPD brasileira tem influência direta do GDPR, não só pela sua característica vanguardista, mas também por questões comerciais . O GDPR e a LGPD, portanto, diferem em relação à base legal para o processamento de dados, já que a LGPD inclui a realização de estudos de pesquisa e a proteção de classificações de crédito. O consentimento para tratamento de dados pessoais no GDPR deve ser prévio, livre, informado e específico, o que também ocorre na LGPD.

Necessárias as observações acima, porque o tema central do trabalho aqui desenvolvido é a análise da proteção de dados no Direito Penal, mais especificamente nos bancos de dados das Policiais Judiciárias brasileiras, onde será analisada a ponderação de bens diante de eventual conflito entre o direito fundamental da proteção de dados versus a necessidade de apuração de um determinado tipo penal. Não é possível compreender a temática sem antes analisar, ainda que superficialmente, os instrumentos legais que motivaram o debate, bem como os pressupostos para a aplicação do *General Data Protection Regulation*.

2.3 Pressupostos Para a Aplicação da General Data Protection Regulation – GDPR

Diante de tudo o que foi mencionado até aqui, é possível perceber que a Europa pode ser considerada atualmente como *standard* na temática de proteção de dados em todo o mundo. O regulamento, apesar de atento à proteção e ao direito à privacidade dos cidadãos, não pode

[57]CNN Brasil. Brasil ao grupo das 10 maiores economias do mundo após alta do PIB. Disponível em: https://www.cnnbrasil.com.br/economia/macroeconomia/brasil-volta-ao-grupo-das-10-maiores-economias-do-mundo-apos-alta-do-pib/. Acessado em 24 de mai. 2024.

ser utilizado como padrão para criar uma regulamentação que prejudique a atividade dos órgãos de persecução penal, que do mesmo modo que toda a sociedade, também se beneficiou com o avanço de novas tecnologias.

Quando se fala em regulação, é preciso ter mente a busca pelo equilíbrio diante de interesses contrapostos, o que abrange dicotomia entre o público e o privado ou entre a privacidade e proteção de dados pessoais. O grande desafio de qualquer lei é demonstrar que alguns interesses são complementares, e não contrapostos. Na Europa, antes da entrada em vigor do *General Dara Protection Regulation*, alguns Estados já disciplinavam a questão da proteção de dados, cujo principal foco era o controle do processamento de dados efetuado por órgãos públicos e por grandes empresas.

Embora o GDPR tenha feito menção à autodeterminação informativa[58], definido como o direito que cada indivíduo tem de controlar e proteger seus dados pessoais, o conceito surgiu em um *case* da Alemanha, conhecido como "caso do censo", julgado em 1983[59]. Na época, a Alemanha já passava por uma intensa discussão pública a respeito da Lei Geral de Proteção de Dados Federal, tendo em vista que ainda não existia uma opinião formada sobre o tema. A repercussão contra a norma legal fez com que mais de 1.600 ações fossem ajuizadas em desfavor da Lei do Censo, ocasião em que 4 foram escolhidas para serem levadas ao Tribunal.

A Lei do Censo determinou o processo de recenseamento de toda a população alemã, impondo a coleta de dados sobre profissão, moradia e local de trabalho, para fins meramente estatísticos. O objetivo da lei foi aferir o crescimento populacional e sua composição demográfica e social sob a perspectiva econômica. O conceito da autodeterminação informativa tem sido fundamental até os dias de hoje, principalmente pelo fato de estar relacionado ao direito à privacidade e à autonomia das pessoas em relação às suas próprias informações.

A decisão da Suprema Corte da Alemanha, portanto, estabeleceu um marco na proteção de dados pessoais na Europa[60], reconhecendo, pela primeira vez, que todo cidadão alemão teria direito à autodeterminação informacional, o que lhe permite decidir sobre a coleta e o uso dos

[58]MENDES, Laura S. F. Autodeterminação informativa: a história de um conceito. Rev. de Ciências Jurídicas Pensar, v. 25, n. 4, 2020. Disponível em: <https://periodicos.unifor.br/rpen/article/view/10828/pdf>. Acesso em 28 de out. 2024.
[59]*Ibid.*
[60]*Ibid.*

seus dados pessoais, estabelecendo parâmetros para a proteção de dados pessoais. Antes da Lei do Censo, porém, no ano de 1975 o Estado de Hesse, também na Alemanha, sancionou a primeira Lei de Proteção de Dados no mundo[61].

Segundo Nuno Saldanha, a realidade da globalização da economia europeia, não só na questão dos dados pessoais, associada à descoberta de que os dados pessoais possuem um valor econômico intrínseco, têm levado as organizações a fazerem grandes investimentos no tratamento de dados de vários consumidores europeus[62]. A nova realidade dos dados com valor econômico e a ausência de fronteiras digitais levou os Estados Membros da União Europeia a decidirem que estava na hora de adotar uma legislação mais apropriada aos novos tempos, com apenas um único regulamento europeu.

O GDPR, portanto, considera a proteção de dados um direito fundamental, independente da nacionalidade ou local de residência, cujo objetivo é a harmonização e a defesa dos direitos e liberdade das pessoas, garantindo uma livre circulação de dados pessoais entre os Estados da UE. Na Europa, um regulamento, diferentemente de uma Diretiva, é de aplicação direta no sistema jurídico dos diferentes Estados-Membros, já que uma vez aprovada, entra em vigor imediatamente[63].

A implementação de uma Diretiva depende da existência de uma lei, ou seja, para que governos, empresas e particulares possam recorrer a uma diretiva, esta deve ter sido objeto de transposição para o direito nacional[64]. Posteriormente, a Comissão Europeia notifica os Estados-Membros sobre a Diretiva aprovada e os países passam a ter um prazo para que a Diretiva seja incorporada à legislação de cada país. A prática pode criar novas leis ou modificar as que já existem, para adaptá-las à Diretiva. O que deve ser destacado é que cada Estado Membro deve seguir um prazo determinado para incorporar a Diretiva à legislação do país, que pode ser punido pela Comissão Europeia caso nada seja feito.

---

[61]BENNET, Colin. Regulating privacy: data Protection and public policy in Europe and the United States. Ithaca, Nova Iorque: Cornell University, 1992, p. 95.
[62]SALDANHA, Nuno. Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar? Lisboa: Fca, 2018, p. XV.
[63]União Europeia. Tipos de Legislação. Disponível em https://european-union.europa.eu/institutions-law-budget/law/types-legislation_pt. Acesso em 28 de out. 2024.
[64]EUR-Lex. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE). Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em 28 de out. 2024.

Isso faz com que o GDPR estabeleça alguns pressupostos necessários para a sua aplicação. São eles:

> Estar na UE ou lidar com dados de cidadãos da UE: A GDPR se aplica a todas as empresas que estão localizadas na União Europeia (UE) ou que oferecem bens ou serviços aos cidadãos da UE, independentemente de onde estejam localizadas. Isso significa que a lei tem um alcance global e afeta muitas empresas que operam fora da UE;
> Ter dados pessoais de usuários: A GDPR define dados pessoais como qualquer informação que possa identificar direta ou indiretamente uma pessoa física. Isso inclui nome, endereço, e-mail, número de telefone, identificadores online, dados biométricos, dados de saúde, dados de localização, preferências, opiniões, etc. A lei protege os direitos e liberdades dos usuários em relação ao tratamento desses dados.
> Ter uma base legal para o tratamento de dados: A GDPR exige que as empresas tenham uma base legal para coletar, armazenar, processar, compartilhar ou transferir dados pessoais de usuários. As bases legais podem ser: consentimento, contrato, interesse legítimo, obrigação legal, interesse público ou vital. As empresas devem informar aos usuários qual é a base legal para cada finalidade de tratamento de dados e respeitar os princípios da GDPR, como minimização de dados, limitação de finalidade, precisão, segurança, etc;
> Cumprir os direitos dos usuários: A GDPR concede aos usuários uma série de direitos sobre seus dados pessoais, como o direito de acesso, retificação, exclusão, portabilidade, oposição, limitação, etc. As empresas devem atender aos pedidos dos usuários dentro de um prazo razoável (geralmente um mês) e sem custo. As empresas também devem facilitar o exercício desses direitos, por exemplo, fornecendo mecanismos simples e transparentes para os usuários gerenciarem suas preferências e consentimentos[65].

Os pressupostos demonstram o interesse do Parlamento Europeu em se preocupar com a evolução tecnológica, fazendo com que a proteção de dados pessoais seja mais sólida e eficiente. Isso também abrange uma base legal para tratamento de dados, onde as instituições, públicas ou privadas, coletam, processam e armazenam dados pessoais, visando sempre um interesse legítimo. Outros aspectos também devem ser observados, tais como o consentimento informado, a finalidade limitada, a minimização de dados, a precisão de dados, a limitação de armazenamento, a segurança e proteção e, principalmente, os direitos dos titulares dos dados.

Através da implementação do GDPR, a União Europeia obrigou que diversos países do mundo inteiro criassem legislações para o tratamento de dados pessoais em plena sintonia com o que preceitua o regulamento europeu. Por esse motivo, a nossa Lei Geral de Proteção de

[65]EUR-Lex. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE). Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em 28 de out. 2024.

Dados é tão parecida com o GDPR. Inclusive, a similaridade da LGPD com o GDPR não foi reproduzida na relação do Anteprojeto Penal de Proteção de Dados com a Diretiva 680/2016, conforme será possível aferir em capítulo específico.

3 LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

Durante muitos anos não se falou em tratamento de dados pessoais no Brasil, até que nos anos 2000 alguns autores passaram a defender a existência dos dados pessoais. Danilo Doneda foi um dos percursores do direto à proteção de dados pessoais no Brasil, sustentando que esse direito seria extraído dos dispositivos previstos no Artigo 5º da nossa Constituição Federal[66]. Posteriormente, o Marco Civil da Internet, em 2015, foi a primeira norma que abordou o direito à proteção de dados pessoais[67].

Além do direito à inviolabilidade da intimidade e da vida privada, o Marco Civil da Internet também garantiu a inviolabilidade e sigilo de fluxo de comunicações pela internet e a inviolabilidade e sigilo das comunicações privadas e armazenadas[68]. Mais que estabelecer as

[66]DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. In: TEPEDINO, Gustavo (Org.). Temas de direito civil. Rio de Janeiro: Renovar, 2000.

[67]Tribunal de Justiça do Distrito Federal e Territórios. Marco Civil da Internet. A referida lei prevê como princípios que regulam o uso da internet no Brasil, enumerados no artigo 3º, dentre outros, o princípio da proteção da privacidade e dos dados pessoais, e asseguram, como direitos e garantias dos usuários de internet, no artigo 7º, a inviolabilidade e sigilo do fluxo de suas comunicações e inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial. O artigo 10º, § 1º, que trata de forma específica da proteção aos registros, dados pessoais e comunicações privadas, é bem claro quanto à possibilidade de fornecimento de dados privados, se forem requisitados por ordem de um juiz, e diz que o responsável pela guarda dos dados será obrigado a disponibilizá-los se houver requisição judicial. Caso o responsável se recuse a fornecer os dados solicitados pelo juiz, poderá responder pelo crime de desobediência, previsto no artigo 330 do Código Penal. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet#:~:text=O%20Marco%20Civil%20da%20Internet,da%20internet%20no%20Brasil. Acessado em 29 de out. 2024.

[68]BRASIL. Marco Civil da Internet. Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização; V - manutenção da qualidade contratada da conexão à internet; VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade; VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as

inviolabilidades, o Marco Civil da Internet fez a previsão expressa da proteção de dados pessoais como princípio para a utilização da internet no Brasil. Posteriormente, no ano de 2018 foi editada a Lei número 13.708/2018, Lei Geral de Proteção de Dados – LGPD, que foi o ponto de partida para falarmos do tema deste trabalho, que é a utilização, para fins penais, dos dados armazenados nos bancos de dados das Polícias Judiciárias Brasileiras.

Nos mesmos moldes do que acontece na Europa com o *General Data Protection Regulation*, a Lei Geral de Proteção de Dados regula, no Brasil, o tratamento de dados pessoais por empresas e entidades[69]. A legislação tem como principal objetivo a garantia, a privacidade e a segurança de determinadas informações, exigindo consentimento para coleta e impondo penalidades para eventuais violações. A LGPD se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: a operação de tratamento seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou os dados pessoais objeto do tratamento tenham sido coletados no território nacional[70].

A Lei Geral de Proteção de Dados define dados pessoais como qualquer informação que possa identificar direta ou indiretamente uma pessoa física, incluindo nome, endereço, e-mail, número de telefone, identificadores online, dados biométricos, dados de saúde, dados de localização, preferências, opiniões, etc. As empresas que não cumprem as regras da LGPD enfrentam consequências legais, incluindo multas pesadas. A multa pode ser de até 2% do faturamento bruto da empresa no Brasil no seu último exercício, limitada a R$ 50 milhões por

---

hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais; XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet; XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 29 de out. 2024.

[69]BRASIL. Lei Geral de Proteção de Dados - LGPD. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 13 nov. 2023.

[70]BRASIL. Lei Geral de Proteção de Dados - LGPD. Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 29 out. 2024.

infração[71]. Além disso, a LGPD permite que as autoridades de proteção de dados tomem medidas corretivas, como advertências, multas diárias, bloqueio ou eliminação de dados, suspensão parcial ou total do funcionamento do banco de dados, suspensão do exercício da atividade de tratamento de dados pessoais, e proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Os dados pessoais mencionados acima são todas as informações relacionadas à pessoa natural identificada ou identificável, como nome, sobrenome, data de nascimento, CPF, RG, CNH, carteira de trabalho, passaporte, título de eleitor, matrícula do servidor, e-mail, endereço, salário do servidor no portal da transparência e número de telefone[72].

Os dados pessoais são chamados de anonimizados, quando estão vinculados a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis no momento do seu tratamento[73]. Os dados pessoais sensíveis são dados pessoais sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Os dados são sensíveis porque possuem um potencial discriminatório, colocando os titulares de dados em situação de maior vulnerabilidade.

Os titulares dos dados pessoais são pessoas naturais, pessoas identificadas ou identificáveis, independentemente da sua nacionalidade ou do local da sua residência. É a pessoa natural a qual se referem os dados pessoais que são objeto de tratamento. A Lei Geral de Proteção de Dados prevê aos titulares de dados pessoais os seguintes direitos[74]: autodeterminação informativa; confirmação da existência de tratamento; acesso aos dados;

---

[71]Autoridade Nacional de Proteção de Dados – ANPD. Sanções Administrativas: o que muda após 1º de agosto de 2021? Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/sancoes-administrativas-o-que-muda-apos-1o-de-agosto-de-2021. Acesso em 29 de out. 2024.

[72]Ministério da Ciência, Tecnologia e Inovações – MCTI. Qual a diferença entre dados pessoais e dados sensíveis? Disponível em: https://www.gov.br/lncc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/campanha-lgpd/qual-a-diferenca-entre-dados-pessoais-e-dados-sensiveis. Acesso em 29 de out. 2024.

[73]Serpro. O que são dados anonimizados, segundo a LGPD? Disponível em: https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-anonimizados-lgpd#:~:text=E%20o%20que%20anonimiza%C3%A7%C3%A3o%20tem,desvincula%C3%A7%C3%A3o%20dele%20a%20essa%20pessoa. Acesso em 29 de out. 2024.

[74]Autoridade Nacional de Proteção de Dados – ANPD. Papel da ANPD, direitos dos titulares e função da ouvidoria. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/acoes-e-programas/programas-projetos-acoes-obras-e-atividades/semana-da-protecao-de-dados-2022/semana-da-protecao-de-dados-pessoais-2022-papel-da-anpd-direitos-dos-titulares-e-funcao-da-ouvidoria. Acesso em 29 de out. 2024.

correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei; portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa de acordo com a regulamentação da autoridade nacional; observados os segredos comercial e industrial; Eliminação dos dados tratados com o consentimento do titular, salvo as hipóteses previstas no art. 16 da LGPD; revogação do consentimento a qualquer momento, nos termos do §5º do art. 8º; obter informações sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

Os principais atores da Lei Geral de Proteção de Dados podem ser definidos da seguinte forma: Titular: pessoa natural a quem pertencem os dados pessoais; Controlador: pessoa natural ou jurídica, pública ou privada, a quem competem as decisões referentes ao tratamento de dados pessoais (As Polícias Judiciárias Brasileiras funcionarão como controlas de dados, sempre que ocorrer uma investigação policial); Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da lei em todo o território nacional; Encarregado: pessoal natural indicada pelo controlador, que atua como canal de comunicação entre o controlador, os titulares dos dados e as Autoridade Nacional de Proteção de Dados e Operador: pessoal natural ou jurídica de direito público ou provado, que realiza o tratamento de dados pessoais em nome do controlador (escopo eminentemente executório)[75].

A compreensão dos conceitos elencados é de extrema importância para o que será debatido no momento em que for abordado o Anteprojeto Penal da Lei Geral de Proteção de Dados. O principal foco da GDPR, da LGPD e do referido Anteprojeto é o tratamento dos dados[76], que pode ser entendido como toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, transferência, difusão ou extração.

[75]BRASIL. Lei Geral de Proteção de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 29 de out. 2024.
[76]Autoridade Nacional de Proteção de Dados – ANPD. Guia orientativo. Tratamento de Dados Pessoais pelo Poder Público. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 29 de out. 2024.

O tratamento de dados pessoais deve ser fiel ao cumprimento dos seguintes princípios estabelecidos pela própria Lei Geral de Proteção de Dados: Princípio da finalidade: o tratamento dos dados deve utilizar propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; Princípio da Adequação: deve ocorrer a compatibilidade do tratamento de dados com as finalidades informadas ao titular, de acordo com o contexto do tratamento; Princípio da necessidade: o tratamento dos dados pessoais deve ser limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; Princípio do livre acesso: é garantido aos titulares de dados a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; Princípio da qualidade dos dados: os titulares de dados devem ter a garantia de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; Princípio da transparência: os titulares de dados pessoais devem receber informações claras, precisas e facilmente acessíveis sobre a realização do tratamento, observados os segredos comercial e industrial; Princípio da Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; Princípio da não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; Princípio da Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; Princípio da responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

A LGPD aborda, tão somente, o tratamento de dados pessoais, não fazendo abordagem aos dados de pessoa jurídica, documentos sigilosos ou confidências, patentes, bem como outros documentos que não estejam vinculados à pessoa natural identificada ou identificável. Do mesmo modo que o regulamento europeu, a Lei Geral de Proteção de Dados também se preocupa em tutelar direitos fundamentais, merecendo destaque o direito à privacidade, que será amplamente debatido nesse estudo.

3.1 Objetivos e Fundamentos da Lei Geral de Proteção de Dados – LGPD

O recente avanço da tecnologia fez com que a população mundial passasse a virtualizar praticamente quase todos os atos da vida comum, o que gerou uma certa exposição de dados pessoais e, consequentemente, uma certa preocupação por parte do próprio titular dos dados e das empresas que armazenam os dados. Por esse motivo, a Lei Geral de Proteção de Dados surgiu para proteger os dados dos cidadãos. A proteção se deve ao fato de os dados pessoais estarem vinculados a vários direitos fundamentais previstos na Constituição de 1988, tais como direito à liberdade, à privacidade e à dignidade da pessoa humana.

A Lei Geral de Proteção de Dados funciona como uma diretriz, para regular e guiar a forma a melhor forma para proteger os dados dos cidadãos. A legislação, portanto, protege os titulares dos dados pessoais e traz segurança jurídica para os profissionais responsáveis pelo tratamento de dados pessoais. Conforme será mencionado em capítulo específico, o tema ganhou ainda mais importância depois que a proteção de dados pessoais foi elevada ao patamar de direito fundamental, previsto no Artigo 5º da Constituição Federal de 1988, conforme Emenda Constitucional número 115, de 10/02/2022[77].

A LGPD, portanto, define os seguintes fundamentos para o tratamento de dados pessoais: respeito à privacidade; inviolabilidade da intimidade; da honra e da imagem; desenvolvimento econômico, tecnológico e à inovação; direitos humanos, live desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais; autodeterminação informativa; liberdade de expressão, de informação, de comunicação e de opinião; livre iniciativa, livre concorrência e a defesa do consumidor.

De acordo com a Lei Geral de Proteção de Dados, apenas as pessoas naturais são titulares de dados pessoais. A legislação, porém, se aplica e deve ser observada por todos aqueles que realizam o tratamento de dados, seja pessoa física ou pessoa jurídica, com finalidade econômica, pública ou privada. A LGPD também não se aplica ao tratamento de dados pessoais que sejam: Realizados por pessoa natural para fins exclusivamente particulares e não econômicos; Para fins exclusivamente artísticos, jornalísticos ou acadêmicos; Realizados

[77]BRASIL. Emenda Constitucional número 115 de 2022 - Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: < https://legis.senado.leg.br/norma/35485358. >. Acesso em 04 jan. 2024.

para fins exclusivo de segurança nacional, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais; Provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequados de acordo com a lei.

Trazendo os fundamentos para o âmbito das Polícias Judiciárias Brasileiras, é possível afirmar que são titulares de dados: os próprios servidores das instituições policiais; o cidadão que faz um registro de ocorrência policial ou uma identidade; e o autor de crimes.

3.2 Tratamento de Dados pelo Poder Público – Órgãos de Persecução Penal

O tratamento de dados pessoais pelo poder público talvez seja considerado um dos temas mais complexos da Lei Geral de Proteção de Dados. Foi justamente a importância dessa discussão que motivou a Autoridade Nacional de Proteção de Dados a elaborar um Guia Orientativo para o Tratamento de Dados Pessoais pelo Poder Público[78]. O Guia estabeleceu diversas diretrizes que devem ser seguidas pelos agentes de tratamento que atuam no Poder Público.

No próprio Guia consta que o termo "Poder Público" é definido pela Lei Geral de Proteção de Dados de forma ampla, o que inclui todos os órgãos ou entidades dos entes federativos (União, Estados, Distrito Federal e Municípios), além dos três Poderes (Legislativo, Executivo e Judiciário), o que não exclui os Tribunais de Contas e os Ministérios Públicos. Isso demonstra, portanto, que todas as entidades e órgãos públicos devem observar o que está previsto na Lei Geral de Proteção de Dados, com exceção do que está descrito no Artigo 4º da referida Lei.

O Artigo 4º é de extrema importância, porque aborda o principal tema deste trabalho, que é o tratamento de dados nos bancos de dados das Polícias Judiciárias Brasileiras. Conforme consta no Artigo 4º da Lei número 13.709/2018[79] (LGPD), "essa lei não será aplicada ao

[78]Autoridade Nacional de Proteção de Dados. Guia Orientativo – Tratamento de Dados Pessoais pelo Poder Público. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf >. Acesso em 11 dez. 2023.

[79]BRASIL. Lei Geral de Proteção de Dados - LGPD. Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins

tratamento de dados pessoais quando realizado para fins exclusivos de segurança pública, defesa nacional, segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais".

A exclusão, porém, não afasta a responsabilidade do Poder Público ou dos Agentes Públicos quando realizam o tratamento de dados pessoais[80]. O Artigo 28 do Decreto-Lei número 4.657/1942[81] (Lei de Introdução às Normas do Direito Brasileiro), é bem claro quando preceitua que *o agente público responderá pessoalmente por suas decisões ou opiniões técnicas em caso de dolo ou erro grosseiro*, demonstrando que todo Agente Público pode ser responsabilizado civil, administrativamente e criminalmente em caso de tratamento de dados inadequado, o que abrange consultas pessoais que não tenham fins permitidos por lei, alteração de dados, inclusão de dados inverídicos e principalmente vazamento de dados.

Um dos problemas mais comuns que envolvem servidores lotados em unidades policiais é a utilização de dados pessoais para fins próprios ou para o favorecimento de terceiros[82]. Conforme previsto no Artigo 7º da Lei Geral de Proteção de Dados[83], o tratamento de dados

---

exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c)segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei. § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo. § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais. § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 13 nov. 2023.

[80]Senado Federal. Punições pelo uso indevido de dados pessoais. A partir deste domingo (01/08/2021) entram em vigor os artigos 52, 53 e 54 da Lei Geral de Proteção de Dados (LGPD). Esses dispositivos tratam das multas e demais sanções administrativas que a Autoridade Nacional de Proteção de Dados (ANPD) poderá aplicar a qualquer "agente de tratamento de dados" que infringir normas da LGPD, a Lei 13.709/2018. Tanto os órgãos públicos, quanto as empresas privadas, poderão receber sanção pelo uso incorreto dos dados pessoais do cidadão. Fonte: Agência Senado. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/07/29/punicoes-pelo-uso-indevido-de-dados-pessoais-comecam-a-valer-no-domingo. Acesso em 29 de out. 2024.

[81]BRASIL. Lei de Introdução às Normas do Direito Brasileiro – LINDB. Disponível em <https://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm>. Acesso em 12 dez. 2023.

[82]Correio Braziliense. PF cumpre mandado de busca contra delegado acusado de vazar informações. Disponível em: <https://www.correiobraziliense.com.br/brasil/2023/10/5133295-pf-cumpre-mandado-de-busca-contra-delegado-acusado-de-vazar-informacoes.html>. Acesso em 12 dez. 2023.

[83]BRASIL. Lei Geral de Proteção de Dados - LGPD. Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 13 nov. 2023.

pessoais somente poderá ser realizado mediante consentimento do titular. O referido dispositivo legal enumera diversas outras hipóteses em que o tratamento pode ser realizado sem o consentimento.

Apesar da previsão expressa já mencionada acima, ou seja, a de que a Lei Geral de Proteção de Dados não será aplicada aos casos que envolvam a atividade policial, não se podem deixar de lado as situações previstas nos casos em que o consentimento do titular de dados pessoais deve ser dispensado. Polícias Judiciárias são instituições que fazem parte do Poder Público, e na ausência de uma legislação específica, os fundamentos e princípios[84] da Lei Geral de Proteção de Dados podem ser utilizados para resolver questões que eventualmente tenham como destino o Judiciário.

O primeiro ponto diz respeito à ausência do consentimento quando necessário para a proteção da vida ou da incolumidade física do titular ou de terceiros. A questão merece uma reflexão, porque parte do trabalho exercido pelas Polícias Judiciárias utiliza dados que foram adquiridos ao longo dos anos, quando os bancos de dados dessas instituições começaram a ser informatizados. Independente do contexto, a visão de quem trabalha com investigação criminal é a de que qualquer tipo de delito deve ser investigado, porque pode gerar risco à incolumidade física do titular dos dados ou de terceiros.

Um simples crime de ameaça pode se transformar em morte. Da mesma forma, uma perturbação da tranquilidade também pode resultar em crime mais grave[85]. Embora esteja inserida dentro do contexto de "Poder Público", a atividade policial deve ser vista com mais cuidado quando o assunto é a proteção de dados pessoais. Além das exceções mencionadas acima, outra hipótese de tratamento que dispensa o consentimento do titular de dados é a utilizada, quando necessário, para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção de dados pessoais.

---

[84]Ministério Público Federal. Fundamentos e Princípios da LGPD. Disponível em: https://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd/fundamentos-e-principios. Acesso em 28 de out. 2024.

[85]Globo.com. Justiça condena a 48 anos de prisão Guarda Municipal de Belém que matou casal de vizinhos por causa de som alto. Disponível em: https://g1.globo.com/pa/para/noticia/2023/12/11/justica-condena-a-48-anos-de-prisao-guarda-municipal-de-belem-que-matou-casal-de-vizinhos-por-causa-de-som-alto.ghtml. Acesso em 12 dez. 2023.

Percebe-se, portanto, que, via de regra, conforme preceitua a Lei Geral de Proteção de Dados, a autorização do titular é fundamental para o tratamento de dados. A autorização pressupõe aceitar ou recusar que os dados sejam tratados, sem deixar de lado a possibilidade de revogação do consentimento a qualquer momento. Importante fazer essa observação, porque o objeto de estudo deste trabalho analisa eventual mitigação do consentimento do titular de dados pessoais, quanto o tratamento dos dados for efetuado por uma instituição policial.

Embora o Brasil ainda não possua essa legislação específica para tratamento de dados pessoais no âmbito da atividade policial, já é possível perceber que o tema vem ganhando cada vez mais notoriedade, uma vez que há inúmeras decisões judiciais[86] sobre o aparente conflito entre o direito à privacidade e proteção de dados diante do dever da polícia na apuração de investigações policiais.

Cabe salientar, no entanto, que o GDPR também faz uma exceção ao mencionar que a sua aplicação não deve ser feita no tratamento de dados pessoais para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou da execução de sanções penais, já que a referida previsão foi disciplinada na Diretiva 680/2016.

O Artigo 144 da nossa Constituição Federal[87] assegura que a segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio. É justamente por esse motivo que se levanta a questão da mitigação de alguns direitos fundamentais, como a privacidade e a proteção de dados por exemplo, para que os órgãos de persecução penal possam garantir a segurança e a incolumidade das pessoas, conforme previsão constitucional acima.

[86]Superior Tribunal de Justiça. Os precedentes do STJ nos primeiros quatro anos de vigência da Lei Geral de Proteção de Dados Pessoais. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/27102024-Os-precedentes-do-STJ-nos-primeiros-quatro-anos-de-vigencia-da-Lei-Geral-de-Protecao-de-Dados-Pessoais.aspx. Acesso em 31 de out. 2024.

[87]BRASIL. Constituição Federal. Capítulo III. Da Segurança Pública. Artigo 144: A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos: I - polícia federal; II - polícia rodoviária federal; III - polícia ferroviária federal; IV - polícias civis; V - polícias militares e corpos de bombeiros militafederal, estaduais e distrital. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 07 de jun. 2024.

Durante o ano de 2022, o Tribunal de Contas da União verificou um alto risco à privacidade de dados pessoais coletados pelo governo[88]. Na ocasião, o TCU fez uma auditoria para avaliar as ações governamentais e os riscos à proteção de dados pessoais. A análise abrangeu 382 organizações, que aferiu iniciativas governamentais para providenciar a adequação à Lei Geral de Proteção de Dados, bem como as medidas implementadas para o cumprimento das exigências estabelecidas em Lei.

Embora não exista uma Lei Penal de Proteção de Dados pessoais, os órgãos de persecução penal não podem descartar os princípios existentes na atual Lei Geral de Proteção de Dados que está vigente. A finalidade, adequação, necessidade, transparência, livre acesso, qualidade, segurança, prevenção, não discriminação e responsabilização e prestação de contas devem ser respeitados[89].

A auditoria do Tribunal de Contas da União pode servir de parâmetro para que em um futuro próximo as instituições policiais façam à devida adequação à legislação penal de proteção de dados que por ventura venha a surgir. Foi constato pelo TCU[90] que de todos os órgãos públicos que não fazem tratamento de dados pessoais, 17,8% estavam em um nível inexpressivo de adequação à Lei Geral de Proteção de Dados, 58,9 estavam em um nível inicial, 20,04% estavam em um nível intermediário e 2,9% em nível aprimorado. De acordo com o Tribunal, o diagnóstico apresentou uma situação de alto risco à privacidade dos cidadãos que possuíam dados pessoais coletados e tratados pela Administração Pública Federal. Como já se passaram dois anos desde a data dessa auditoria, é possível que esses números tenham se tornado mais expressivos.

3.3 Utilização da Lei Geral de Proteção de Dados – LGPD, diante da ausência de Lei Geral Penal de Proteção de Dados

Conforme já mencionado, o Artigo 4º[91] da Lei Geral de Proteção de Dados é bem claro quando menciona que a legislação não se aplica ao tratamento de dados pessoais realizados para

[88]Tribunal de Contas da União. TCU verifica risco alto à privacidade de dados pessoais coletados pelo governo. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/tcu-verifica-risco-alto-a-privacidade-de-dados-pessoais-coletados-pelo-governo.htm. Acesso em 29 de ago. 2024.
[89]ARAS, Vladimir. Aplicabilidade da LGPD às atividades de segurança Pública e Persecução Penal. Jota. Disponível em: https://www.jota.info/artigos/aplicabilidade-da-lgpd-as-atividades-de-seguranca-publica-e-persecucao-penal. Acesso em 25 de nov. 2024.
[90] *Ibid.*
[91]BRASIL. Artigo 4º da Lei Geral de Proteção de Dados. Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado

fins exclusivos de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais. Isso tem gerado alguns conflitos, porque algumas empresas privadas, principalmente às de telefonia, estão utilizando a LGPD para não repassar informações de usuários às polícias e ao Ministério Público[92].

A questão foi objeto de análise do Ministério Público Federal, que elaborou um estudo técnico[93] sobre a Lei Geral de Proteção de Dados Pessoais e o poder requisitório do Ministério Público. O referido estudo técnico fez uma exposição dos fundamentos técnicos e jurídicos sobre a inexistência de incompatibilidade entre a Lei Federal número 13.709 de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD) e o referido poder requisitório.

Nesse sentido, é preciso estabelecer a distinção entre as normas de competência e as normas de autorização. As normas de competência são aquelas que delimitam quais órgãos ou entidades possuem autoridade para tomar decisões ou realizar determinadas ações. As normas de competência são fundamentais para garantir a organização e a divisão de responsabilidades dentro de um sistema jurídico ou administrativo. As normas de autorização, no entanto, estabelecem os procedimentos e requisitos necessários para que uma atividade ou ação seja

---

para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei. § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo. § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais. § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais. § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. Disponível em < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 12 jan. 2024.

[92] Supremo Tribunal Federal. Norma que autoriza MP e polícia a requisitar de telefônicas dados cadastrais de investigados é válida, decide STF. Disponível em: https://noticias.stf.jus.br/postsnoticias/norma-que-autoriza-mp-e-policia-a-requisitar-de-telefonicas-dados-cadastrais-de-investigados-e-valida-decide-stf/. Acesso em 31 de out. 2024.

[93]BRASIL. Lei Geral de Proteção de Dados Pessoais e o poder requisitório do Ministério Público. Disponível em <https://www.mpf.mp.br/pgr/arquivos/2023/2023-11-estudo%20tecnico%20dados%20pessoais.pdf>.Acesso em 12 jan. 2024.

legalmente permitida. As normas de autorização podem ser aplicadas em diversos contextos, como na concessão de licenças, permissões e aprovações para atividades específicas[94].

Para o Ministério Público, o seu poder de requisição não foi alterado com a vigência da Lei Geral de Proteção de Dados. Essa legislação apenas implementou contornos procedimentais, delimitando a forma como os dados pessoais devem ser tratados. A Lei Geral de Proteção de Dados, inclusive, não fez qualquer distinção para o tratamento de dados pessoais efetuado por órgãos integrantes da Administração Pública.

O ponto a ser debatido nesse contexto é que a Lei Geral de Proteção de Dados, por não fazer a distinção entre o tratamento de dados pessoais, equiparou os órgãos de persecução penal ao demais órgãos públicos, o que foi inapropriado. Se a própria LGPD fez a previsão de afastamento de sua incidência ao tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou investigação e repressão de infrações penais, como pode equiparar esses órgãos ao mesmo regramento dos demais entes da Administração Pública?

Já que a Lei Geral de Proteção de Dados excluiu o tratamento de dados no âmbito da segurança pública, equiparando as instituições policiais ao mesmo patamar dos demais órgãos públicos, quando esse tratamento for feito para fins não criminais, é possível afirmar que, diante da ausência de uma legislação específica, a LGPD pode ser aplicada ao tratamento de dados para fins penais?

Percebe-se, portanto, que a interpretação inapropriada da Lei Geral de Proteção de Dados pode trazer diversos prejuízos para a atividade policial e para o processo penal de forma geral. Conforme será possível aferir adiante, a proteção de dados pessoais deve ser respeitada principalmente pelo fato de ter se tornado um direito fundamental previsto na Constituição Federal de 1988[95]. Ocorre que os direitos fundamentais das vítimas de crimes também devem ser observados. Por outro lado, é preciso ressaltar que essa ponderação cabe ao legislador e ao judiciário, e não ao intérprete da lei.

---

[94]NERY, Nina. O compartilhamento de dados financeiros no sistema antilavagem de dinheiro brasileiro. São Paulo: Thompson Reuters Brasil, 2024.

[95]BRASIL. Constituição Federal de 1988. LXXIX – é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 19 jan. 2024.

Diante da omissão legislativa, empresas prestadoras de serviço de telefonia fazem uso, ilegalmente, da Lei Geral de Proteção de Dados[96], para mitigar o poder requisitório do Ministério Público e da Polícias Judiciárias, que necessitam de alguns dados pessoais para garantir, em tempo hábil, que não ocorram prejuízos para a investigação criminal e para a persecução penal. O que deve ser destacado é que as mesmas empresas que recusam o fornecimento de dados a quem por direito deveria obtê-los, não impede que criminosos tenham acesso aos mesmos dados, utilizando-os para praticarem os mais variados tipos de delitos, sendo o estelionato o mais recorrente.

O poder de requisição do Ministério Público e das Polícias Judiciárias deve ser observado de acordo com os parâmetros legais, uma vez que alguns tipos de atos processuais necessitam de autorização judicial, tendo em vista a cláusula de reserva de jurisdição[97], já que certos atos ou decisões devem ser reservados exclusivamente ao Poder Judiciário. Isso visa,

[96]Câmara dos Deputados. Empresas de internet e de telecomunicações negam repasse de dados de usuários. Fonte: Agência Câmara de Notícias. Disponível em: https://www.camara.leg.br/noticias/412182-empresas-de-internet-e-de-telecomunicacoes-negam-repasse-de-dados-de-usuarios/. Acesso em 31 de out. 2024.

[97]STF. RE 593727, Rel. Min. Cézar Peluso, Tribunal Pleno, J. 18.05.2015, DJe 08.09.2015. Recurso extraordinário representativo da controvérsia. Constitucional. Separação dos poderes. Penal e processual penal. Poderes de investigação do Ministério Público. 2. Questão de ordem arguida pelo réu, ora recorrente. Adiamento do julgamento para colheita de parecer do Procurador-Geral da República. Substituição do parecer por sustentação oral, com a concordância do Ministério Público. Indeferimento. Maioria. 3. Questão de ordem levantada pelo Procurador-Geral da República. Possibilidade de o Ministério Público de estado-membro promover sustentação oral no Supremo. O Procurador-Geral da República não dispõe de poder de ingerência na esfera orgânica do Parquet estadual, pois lhe incumbe, unicamente, por expressa definição constitucional (art. 128, § 1º), a Chefia do Ministério Público da União. O Ministério Público de estado-membro não está vinculado, nem subordinado, no plano processual, administrativo e/ou institucional, à Chefia do Ministério Público da União, o que lhe confere ampla possibilidade de postular, autonomamente, perante o Supremo Tribunal Federal, em recursos e processos nos quais o próprio Ministério Público estadual seja um dos sujeitos da relação processual. Questão de ordem resolvida no sentido de assegurar ao Ministério Público estadual a prerrogativa de sustentar suas razões da tribuna. Maioria. 4. Questão constitucional com repercussão geral. Poderes de investigação do Ministério Público. Os artigos 5º, incisos LIV e LV, 129, incisos III e VIII, e 144, inciso IV, § 4º, da Constituição Federal, não tornam a investigação criminal exclusividade da polícia, nem afastam os poderes de investigação do Ministério Público. Fixada, em repercussão geral, tese assim sumulada: "O Ministério Público dispõe de competência para promover, por autoridade própria, e por prazo razoável, investigações de natureza penal, desde que respeitados os direitos e garantias que assistem a qualquer indiciado ou a qualquer pessoa sob investigação do Estado, observadas, sempre, por seus agentes, as hipóteses de reserva constitucional de jurisdição e, também, as prerrogativas profissionais de que se acham investidos, em nosso País, os Advogados (Lei 8.906/94, artigo 7º, notadamente os incisos I, II, III, XI, XIII, XIV e XIX), sem prejuízo da possibilidade – sempre presente no Estado democrático de Direito – do permanente controle jurisdicional dos atos, necessariamente documentados (Súmula Vinculante 14), praticados pelos membros dessa instituição". Maioria. 5. Caso concreto. Crime de responsabilidade de prefeito. Deixar de cumprir ordem judicial (art. 1º, inciso XIV, do Decreto-Lei nº 201/67). Procedimento instaurado pelo Ministério Público a partir de documentos oriundos de autos de processo judicial e de precatório, para colher informações do próprio suspeito, eventualmente hábeis a justificar e legitimar o fato imputado. Ausência de vício. Negado provimento ao recurso extraordinário. Maioria. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&queryString=PRINC%C3%8DPIO%20CONSTITUCIONAL%20DA%20RESERVA%20DE%20JURISDI%C3%87%C3%83O&sort=_score&sortBy=desc. Acesso em 31 de out. 2024.

justamente, a proteção de direitos fundamentais, com o intuito de evitar a ocorrência de arbitrariedades. Reserva legal, portanto, não deve ser confundida com reserva de jurisdição.

Como exemplos clássicos de matérias com reserva de jurisdição, podemos mencionar a busca domiciliar, que só pode ocorrer, via de regra, com o mandado de busca e apreensão; a interceptação telefônica e a decretação de prisão preventiva ou temporária. Apesar da existência da cláusula de reserva de jurisdição, algumas leis mencionam a requisição de dados cadastrais no processo penal.

A Lei número 12.683/20212[98], que alterou a Lei número 9.613/98, para tornar mais eficiente a persecução penal nos crimes de lavagem de dinheiro, menciona que:

> Artigo 17 – B: A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito.

Posteriormente, a Lei número 12.965/2014[99], Marco Civil da Internet, referendou que a qualificação pessoa, filiação e endereço, na forma da lei, podem ser acessados pelas autoridades administrativas que detenham competência legal para a requisição. Na sequência, a Lei número 13.344/2016[100] inovou ao permitir o acesso a dados e informações cadastrais de vítimas e não somente dos suspeitos. A requisição, portanto, foi limitada à prática dos crimes estabelecidos pela própria Lei.

> Art. 11. O Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), passa a vigorar acrescido dos seguintes arts. 13-A e 13-B:
> "Art. 13-A. Nos crimes previstos nos arts. 148 , 149 e 149-A , no § 3º do art. 158 e no art. 159 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal) , e no art. 239 da Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente) , o membro do Ministério Público ou o delegado de polícia poderá requisitar, de quaisquer órgãos do poder público ou de empresas da iniciativa privada, dados e informações cadastrais da vítima ou de suspeitos.
> Parágrafo único. A requisição, que será atendida no prazo de 24 (vinte e quatro) horas, conterá:
> I - o nome da autoridade requisitante;

[98]BRASIL. Lei número 12.683/2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12683.htm. Acesso em 15 mai. 2024.
[99]Marco Civil da Internet. Lei número 12.965/2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acessado em 05 de mai. 2024.
[100]BRASIL. Lei número 13.344/2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13344.htm. Acessado em 15 de mai. 2024.

> II - o número do inquérito policial; e
> III - a identificação da unidade de polícia judiciária responsável pela investigação."
> "Art. 13-B. Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso.

Com a entrada em vigor do Decreto número 8.771/2016[101], que regulamentou o Marco Civil da Internet, a autoridade policial e o Ministério Público passaram, após indicação de fundamentação legal de competência expressa para o acesso e a motivação para o motivo de acesso, a ter acesso aos dados cadastrais. O mesmo Decreto estabeleceu como dados cadastrais a filiação, o endereço, a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário. Cabe ressaltar que, visando preservar o uso desnecessário de dados, o Decreto estabeleceu que os pedidos devem especificar os indivíduos cujos dados estão sendo requeridos e as informações desejadas, sendo vedados pedidos coletivos que sejam genéricos ou inespecíficos.

Um dos maiores avanços do Decreto foi a introdução de uma concepção mais ampla de endereço, quando menciona que dado pessoal pode ser considerado como dado relacionado à pessoal natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estiverem relacionados a uma pessoa. Já o tratamento de dados pessoais foi definido como toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração[102].

---

[101]BRASIL. Decreto número 8.771/2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acessado em: 15 de mai. 2024.

[102]BRASIL. Decreto número 8.771/2016. Art. 14. Para os fins do disposto neste Decreto, considera-se: I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acessado em: 15 de mai. 2024.

Aqui é preciso abrir um parêntese para reforçar a importância da necessidade de regulamentação na utilização dos bancos de dados utilizados pelas Policias Judiciárias brasileiras. Antes de o Decreto trazer a definição de tratamento de dados pessoais, as instituições policiais já faziam a coleta, produção, recepção e utilização dos dados. Embora a prática não tenha nenhum contorno de ilicitude ou ilegalidade, nos dias atuais, cada vez mais, é preciso implementar uma fiscalização adequada, para que os dados possam ser acessados de forma controlada e utilizados com o objetivo previsto para o determinado caso concreto.

A definição do dado locacional prevista pelo Decreto é de extrema importância para o dia a dia da atividade policial, tendo em vista que diariamente crimes graves são praticados, o que exige imediatismo da atuação policial, sob pena de não se conseguir dar uma resposta efetiva para solução do litígio criminal. O dado locacional[103], além dos identificadores eletrônicos, pode ser compreendido como a geolocalização[104].

Diante da celeuma jurídica, no dia 18 de abril de 2024 o Supremo Tribunal Federal – STF, dispensou autorização para o Ministério Público e as polícias acessarem dados controlados por operadoras de telefonia que atuem no Brasil, nos casos em que a polícia precise acessar informações sobre suspeitos e vítimas de sequestro, tráfico de pessoas, redução análoga à de escravo. Cabe salientar que para os Ministros, as informações se restringem aos dados cadastrais, tais como qualificação pessoal, filiação e endereço[105].

O que deve ser destacado é que as operadoras de telefonia eram contra o acesso aos dados sem autorização judicial, o que motivou o ajuizamento da ADI 5642, que questionou a validade dos Artigos 13-A e 13-B do Código de Processo Penal, incluídos pela Lei número 13.344/2016. As referidas normas fizeram a previsão de que os Membros do Ministério Público e os delegados de polícia possam investigar crimes relacionados ao tráfico de drogas, pedindo informações sobre vítimas ou suspeitos diretamente aos órgãos do poder público e às empresas privadas, dispensando a autorização judicial.

---

[103]*Ibid.*
[104]Geolocation. O que é geolocalização? Disponível em: https://www.geolocation.com/pt/index. Acesso em 31 de out. 2024.
[105]STF, ADI 5642, Tribunal Pleno, Rel. Min. Edson Fachin, J. 29.04.2024, DJe 19.09.2024.

O Artigo 13-A do Código de Processo Penal prevê que os dados encontrados em cadastros, tais como nome, filiação e endereço, sejam entregues diretamente aos órgãos de investigação. Já o Artigo 13-B do CPP trata sobre as informações que ajudem a achar vítimas ou suspeitos, como a localização do sinal de celular ou internet, por exemplo. Via de regra, nesses casos os dados só podem ser entregues aos órgãos de persecução penal por ordem judicial. Ocorre que se o juiz não analisar o pedido de acesso aos dados em até 12 horas[106], o Ministério Público e a Polícia podem exigir a sua entrega, sem que seja necessária a ordem judicial.

O maior questionamento na ADI 5462, foi se os Membros do Ministério Público e os Delegados de Polícia que investiguem crimes relacionados ao tráfico de pessoas poderiam exigir informações pessoais e dados de localização das vítimas e suspeitos sem autorização judicial. Na ocasião, o STF entendeu que os Artigos 13-A e 13-B do Código de Processo Penal autorizavam a entrega dos dados de cadastro e localização diretamente aos membros do Ministério Público e Policiais, mas não permitia que essas autoridades tivessem acesso ao conteúdo das mensagens e ligações feitas por vítimas ou suspeitos[107].

Ainda de acordo com a decisão do STF, não se aplica a regra constitucional que trata do sigilo das comunicações telefônicas previsto no Inciso XII do artigo 5º da Constituição Federal, que só pode ser quebrado por ordem judicial. O entendimento que prevaleceu foi o de que os crimes relacionados ao tráfico de pessoas são considerados graves e precisam ser investigados de forma rápida, tendo em vista a existência de risco iminente da vítima, além do risco de que ela seja levada para fora do país. Diante disso, a proteção constitucional à intimidade e à vida

[106]BRASIL. Código de Processo Penal. Art. 13-B. Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso. § 4º *Não havendo manifestação judicial no prazo de 12 (doze) horas*, a autoridade competente requisitará às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso, com imediata comunicação ao juiz. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em 31 de out. 2024.

[107]1ª Tese: É constitucional norma que permite, mesmo sem autorização judicial, que delegados de polícia e membros do Ministério Público requisitem dados e informações cadastrais da vítima ou dos suspeitos em investigações sobre os crimes de cárcere privado, redução a condição análoga à de escravo, tráfico de pessoas, sequestro relâmpago, extorsão mediante sequestro e envio ilegal de criança ao exterior (CPP/1941, art. 13-A). 2ª Tese: É constitucional norma que possibilita, mediante autorização judicial (mesmo que posterior), a requisição da disponibilização imediata de sinais, informações e outros dados que viabilizem a localização da vítima ou dos suspeitos daqueles mesmos delitos (CPP/1941, art. 13-B). STF, ADI 5642, Tribunal Pleno, Rel. Min. Edson Fachin, J. 29.04.2024, DJe 19.09.2024.

privada deve ser relativizada, ou mitigada, em favor do interesse da sociedade em dar solução para esses crimes, o que validou as regras mencionadas acima, determinando, com ressalvas, a entrega de informações sobre vítimas e suspeitos à autoridades que conduzam as investigações, mesmo sem ordem judicial.

O Supremo Tribunal Federal declarou constitucionais os dispositivos que autorizam Delegados de Polícia e membros do Ministério Público a requisitarem dados cadastrais a operadoras de celular, mesmo sem autorização judicial, prevalecendo o voto do Relator, Ministro Edson Fachin. Os dados devem ser utilizados exclusivamente em investigações sobre os crimes de cárcere privado, redução à condição análoga à de escravo, tráfico de pessoas, sequestro-relâmpago, extorsão mediante sequestro e envio ilegal de criança ao exterior. Na mesma decisão, também por maioria, o STF validou a regra que permite a requisição, mediante autorização judicial, às empresas prestadoras de serviços de telecomunicações e/ou telemática para que disponibilizem imediatamente sinais, informações e outros dados que permitam a localização da vítima ou dos suspeitos desses mesmos delitos. Caso a autorização judicial não seja concedida em um prazo de 12 horas, as autoridades podem pedir os dados referentes a sinal diretamente às empresas, conforme previsto na lei, com imediata comunicação ao juiz. Os Ministros Marco Aurélio e Rosa Weber votaram em sentido contrário, sob a alegação de que a lei afrontava a privacidade dos dados previstos em nossa Constituição Federal[108]. Para os Ministros, a única forma de acesso aos dados pessoais é mediante autorização judicial[109].

[108]*Ibid.*

[109]Em seu voto, o Ministro Edson Fachin sustentou que "Essas alterações legislativas e os debates judiciais demonstram que, na era digital, são no mínimo discutíveis a aplicação do conceito de "dados cadastrais" para definir o alcance dos poderes de requisição sem mandado judicial por parte das autoridades policiais e do Ministério Público. Por isso, apesar de a redação legislativa contida no art. 13-A do Código de Processo Penal limitar-se a "dados e informações cadastrais", expressão consagrada na jurisprudência deste Tribunal, é preciso não colocá-la acima da própria proteção constitucional, isto é, não se deve interpretar a expressão de modo a tornar ineficaz a proteção constitucional. Como advertem Dennys Antonialli e Jacqueline de Souza Abreu (Brazil and the Treasure Trove's Tales: A Study on the Evolution and Popularization of Phones and Law Enforcement Access to Communications. In: FELSBERGER, Stefanie; SUBRAMANIAN, Ramesh. Mobile Technology and Social Transformation. Abingdon: Routledge, 2021, tradução livre): "Na prática, essas autoridades [delegados de polícia e membros do Ministério Público] utilizam esses dispositivos legais [que lhes atribuem o poder de requisição de dados cadastrais] para justificar a requisição de dados a empresas de telefonia em todos os casos; e a questão só é levada às cortes para revisão se uma empresa se recusar a cumprir. A falta de qualquer critério formal ou material para o fornecimento de informações deixa esses procedimentos ainda mais discricionários". Por tudo isso, este Tribunal não pode aceitar acriticamente a utilização da expressão "dados e informações cadastrais" para reconhecer como legítima toda e qualquer interferência no direito à privacidade, já que a atual capacidade de produção e análise de dados, ainda que mais simples e públicos, pode trazer significativos impactos. STF, ADI 5642, Tribunal Pleno, Rel. Min. Edson Fachin, J. 29.04.2024, DJe 19.09.2024.

A evolução legislativa demonstra um avanço considerável na compreensão da proteção de dados no Brasil. O grande problema é falta de regulamentação para o tratamento de dados pessoais que são utilizados na persecução penal, como os dados existentes nos bancos de dados das polícias judiciárias brasileiras. Apenas a título de exemplo, a Lei número 13.964/2019[110], que aperfeiçoou a legislação penal e processual, também conhecida como pacote anticrime, implementou um pacote de medidas cujo objetivo foi endurecer a legislação penal no combate a crimes graves e à impunidade. A legislação aumentou a pena em determinados crimes, restringiu benefícios processuais e introduziu novas práticas no sistema de justiça criminal.

O Artigo 12 do pacote anticrime traz um modelo que pode servir de base para incentivar o debate sobre a regulamentação dos bancos de dados utilizados pelas polícias judiciárias brasileiras. O referido Artigo autorizou, pelo Ministério da Justiça e Segurança Pública, a criação do Banco Nacional Multibiométrico e de Impressões Digitais. O banco tem como objetivo o armazenamento de dados de registros biométricos, de impressões digitais, de íris, face e voz colhidos em investigações criminais ou por ocasião de identificação criminal, para subsidiar investigações federais, estaduais ou distritais.

No Parágrafo 5º do mesmo Artigo 12, consta que poderão integrar o Banco Nacional Multibiométrico e de Impressões Digitais, ou com ele interoperar, os dados de registros constantes em quaisquer bancos de dados geridos por órgãos dos Poderes Executivo, Legislativo e Judiciário das esferas Federal, Estadual e Distrital, inclusive pelo Tribunal Superior Eleitoral e pelos Institutos de Identificação.

O pacote anticrime faz uma ressalva, quando afirma que nos casos de banco de dados de identificação de natureza civil, administrativa ou eleitoral, a integração ou o compartilhamento dos registros do Banco Nacional Multibiométrico e de Impressões Digitais será limitado às impressões digitais e às informações necessárias para identificação do seu titular. Percebe-se que o banco de dados possui mais informações que os bancos de dados das polícias judiciárias, porque é um banco de dados unificado, composto por órgãos de várias esferas do poder público. A diferença, no entanto, reside no fato de que o acesso aos dados deve ser feito através de autorização judicial, nos casos de inquérito policial ou ação penal.

[110]BRASIL. Lei número 13.964/2019. Pacote Anticrime. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acessado em 18 de mai. 2024.

Em outras palavras, enquanto o Banco de Dados da Polícia Civil do Distrito Federal é alimentado com dados inseridos tão somente no Distrito Federal, o Banco Nacional Multibiométrico é a união dos dados recebidos pelas políticas de todos os Estados brasileiros. Além disso, conforme mencionado acima, a exigência de autorização para acesso aos registros do Banco Nacional Multibiométrico é dispensada no acesso ao banco de dados da Polícia Civil do Distrito Federal, por ausência de legislação que regulamente o tema.

De início, parece que o Banco de Dados Multibiométrico com informações de diversos órgãos pode gerar uma intervenção ilegítima acentuada ao direito fundamental à proteção de dados. Ocorre que a exigência de autorização judicial e a necessidade de instauração de inquérito policial ou ação penal afastam a referida impressão. Nos bancos de dados das polícias judiciárias, diante da ausência de norma legal e do devido monitoramento, o acesso aos dados é ilimitado e pode ser feito em qualquer circunstância, sem autorização judicial e sem a necessidade de instauração de inquérito policial ou ação penal. Basta a mera suspeita, ou até mesmo a sua ausência, para que os responsáveis pela investigação policial façam as consultas da forma que acharem mais conveniente.

Os dados constantes no banco de dados terão caráter sigiloso, e aquele que permitir ou promover sua utilização para fins diversos do previsto na própria lei ou em decisão judicial, responderá civil, penal e administrativamente. Na mesma linha de raciocínio, foi vedada a comercialização, total ou parcial, da base de dados em questão[111]. Por fim, a exclusão dos perfis

[111]BRASIL. Lei número 13.964/2019. Pacote Anticrime. "Art. 7º-A. A exclusão dos perfis genéticos dos bancos de dados ocorrerá: I - no caso de absolvição do acusado; ou II - no caso de condenação do acusado, mediante requerimento, após decorridos 20 (vinte) anos do cumprimento da pena.". "Art. 7º-C. Fica autorizada a criação, no Ministério da Justiça e Segurança Pública, do Banco Nacional Multibiométrico e de Impressões Digitais. § 1º A formação, a gestão e o acesso ao Banco Nacional Multibiométrico e de Impressões Digitais serão regulamentados em ato do Poder Executivo federal. § 2º O Banco Nacional Multibiométrico e de Impressões Digitais tem como objetivo armazenar dados de registros biométricos, de impressões digitais e, quando possível, de íris, face e voz, para subsidiar investigações criminais federais, estaduais ou distritais. § 3º O Banco Nacional Multibiométrico e de Impressões Digitais será integrado pelos registros biométricos, de impressões digitais, de íris, face e voz colhidos em investigações criminais ou por ocasião da identificação criminal. § 4º Poderão ser colhidos os registros biométricos, de impressões digitais, de íris, face e voz dos presos provisórios ou definitivos quando não tiverem sido extraídos por ocasião da identificação criminal. § 5º Poderão integrar o Banco Nacional Multibiométrico e de Impressões Digitais, ou com ele interoperar, os dados de registros constantes em quaisquer bancos de dados geridos por órgãos dos Poderes Executivo, Legislativo e Judiciário das esferas federal, estadual e distrital, inclusive pelo Tribunal Superior Eleitoral e pelos Institutos de Identificação Civil. § 6º No caso de bancos de dados de identificação de natureza civil, administrativa ou eleitoral, a integração ou o compartilhamento dos registros do Banco Nacional Multibiométrico e de Impressões Digitais será limitado às impressões digitais e às informações necessárias para identificação do seu titular. § 7º A integração ou a interoperação dos dados de registros multibiométricos constantes de outros bancos de dados com o Banco Nacional Multibiométrico e de Impressões Digitais ocorrerá por meio de acordo ou convênio com a unidade gestora. § 8º Os dados constantes do Banco Nacional Multibiométrico e de Impressões Digitais terão caráter sigiloso, e aquele que permitir ou promover

genéticos do banco de dados ocorrerá no caso de absolvição do acusado, ou no caso de condenação do condenado, mediante requerimento após decorridos 20 anos do cumprimento da pena[i].

Outro banco de dados do Governo Federal de âmbito nacional, instituído pelo Decreto nº 7.950/2013[112], é o Banco Nacional de Perfis Genéticos (BNPG)[113], que conta com mais de 175.503 perfis cadastrados e já auxiliou mais de 4.500 investigações em todo o país[114]. A maior parte dos registros é ligada às pessoas envolvidas em casos de crimes violentos e de abuso sexual. Para Ronaldo Caieiro, coordenador da Rede Integrada de Bancos de Perfis Genéticos do Ministério da Justiça e Segurança Pública "os dados possibilitam a resolução de muitos crimes. Se trata de uma ferramenta eficiente para resolver crimes, afinal, as informações cadastradas no banco, apontam autorias de crimes sem solução, comprovam a inocência de suspeitos e interligam um caso com outras investigações das demais esferas policiais"[115].

O Banco Nacional de Perfis Genéticos também auxilia na localização de pessoas desaparecidas e conta com a participação de todas as 27 unidades da federação. Vestígios, como fios de cabelo, sangue e outros materiais biológicos são coletados no local do crime ou no corpo de vítima e em exames realizados nas vítimas nos Institutos Médicos Legais. A coleta, inclusive, é feita em condenados por crimes graves e hediondos. A partir de Lei número 2.654/2012[116], foi determinada a obrigação de identificação do perfil genético de condenados por crime com violência de natureza grave, como homicídios, latrocínio, sequestro e estupro, ou em casos que sejam determinados pelo juiz.

---

sua utilização para fins diversos dos previstos nesta Lei ou em decisão judicial responderá civil, penal e administrativamente. § 9º As informações obtidas a partir da coincidência de registros biométricos relacionados a crimes deverão ser consignadas em laudo pericial firmado por perito oficial habilitado. § 10. É vedada a comercialização, total ou parcial, da base de dados do Banco Nacional Multibiométrico e de Impressões Digitais. § 11. A autoridade policial e o Ministério Público poderão requerer ao juiz competente, no caso de inquérito ou ação penal instaurados, o acesso ao Banco Nacional Multibiométrico e de Impressões Digitais." Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acessado em 18 de mai. 2024.

[112]BRASIL. Decreto nº 7.950, de 12 de março de 2013. Institui o Banco Nacional de Perfis Genéticos e a Rede Integrada de Bancos de Perfis Genéticos. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7950.htm#:~:text=%C2%A7%201%C2%BA%20O%20Banco%20Nacional,destinadas%20%C3%A0%20apura%C3%A7%C3%A3o%20de%20crimes. Acesso em 25 de nov. 2024.

[113]Governo Federal. Banco Nacional de Perfis Genéticos (BNPG). Disponível em: https://www.gov.br/pt-br/noticias/justica-e-seguranca/2022/12/banco-nacional-de-perfis-geneticos-conta-com-mais-de-175-mil-perfis-cadastrados. Acesso em 25 de set. 2024.

[114] *Ibid.*

[115] *Ibid.*

[116]BRASIL. Lei número 12.654/2012. Altera as Leis nºs 12.037, de 1º de outubro de 2009, e 7.210, de 11 de julho de 1984 - Lei de Execução Penal, para prever a coleta de perfil genético como forma de identificação criminal, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12654.htm. Acesso em 31 de out. 2024.

Embora possa parecer um excelente instrumento na identificação de autores de crimes, a obrigatoriedade de fornecer material genético na forma da do Artigo 9º-A da Lei de Execução Penal[117] já foi questionada no Supremo Tribuna Federal[118]. Em sede de execução penal, o Ministério Público do Estado de Minas Gerais requereu a identificação de condenado por meio de colheita de material genético – DNA. O juízo indeferiu o pedido, alegando ser inconstitucional a submissão obrigatória à identificação do perfil genético mediante destruição de DNA, porque não se pode forçar o indivíduo a entregar material que, eventualmente possa ser desfavorável.

De acordo com o STF[119], os limites dos poderes do Estado de colher material biológico de suspeitos ou condenados por crimes, de traçar o específico perfil genético, de armazenar os perfis em bancos de dados e de fazer o uso dessas informações são objeto de discussão em diversos sistemas jurídicos. Nesse caso específico, analisado pelo Supremo Tribunal Federal, o recorrente foi condenado por crimes praticados com violência contra a pessoa e por crimes hediondos e se negou a incluir seu perfil genético em bancos de dados, sob a alegação de violação de direitos de personalidade e de prerrogativa de não se autoincriminar. Atualmente o Tema tramita no STF sob o número 905, tendo sido taxado como de repercussão geral, aguardando julgamento.

O STJ, por sua vez, entendeu, em setembro de 2024[120], que o preso não pode se negar a fornecer material genético para banco de DNA. A Sexta Turma do Superior Tribunal de Justiça negou Habeas Corpus a um condenado que não queria fornecer material biológico para armazenamento no banco de perfis criminais, conforme preceitua o Artigo 9ª-A da Lei de Execução Penal.

---

[117]BRASIL. Lei de Execução Penal. Art. 9º-A. O condenado por crime doloso praticado com violência grave contra a pessoa, bem como por crime contra a vida, contra a liberdade sexual ou por crime sexual contra vulnerável, será submetido, obrigatoriamente, à identificação do perfil genético, mediante extração de DNA (ácido desoxirribonucleico), por técnica adequada e indolor, por ocasião do ingresso no estabelecimento prisional. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7210.htm. Acesso em 25 de set. 2024.

[118]BRASIL. Supremo Tribunal Federal. EXECUÇÃO PENAL – PERFIL GENÉTICO – EXAME – DNA – ENTREGA DE MATERIAL – OBRIGATORIEDADE – IMPOSIÇÃO NA ORIGEM – RECURSO EXTRAORDINÁRIO – REPERCUSSÃO GERAL CONFIGURADA. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/verPronunciamento.asp?pronunciamento=6410103. Acesso em 25 de set. 2024.

[119]*Ibid.*

[120]STJ, HC 879757 GO, Sexta Turma, Rel. Min. Sebastião Reis Júnior, J. 20.08.2024, DJe 03.10.2024.

Antes de chegar ao STJ, o Tribunal local não concedeu o Habeas Corpus, sob a justificativa de que o material biológico não serviria para a produção de prova no processo que já havia sido concluído contra o paciente, podendo ser utilizada, tão somente em eventuais futuros processos, até mesmo como prova de inocência. A defesa alegou que a coleta forçada de material biológico seria uma ofensa à dignidade da pessoa humana e à intimidade, além de violar os princípios da autonomia da vontade da presunção de inocência e da vedação à não autoincriminação.

O Relator no STJ, Ministro Sebastião Reis Júnior[121], afirmou que, não havendo crime em apuração, o fornecimento do perfil genético não ocasiona produção de prova contra o apenado. "Não há que falar em obrigatoriedade de produção de provas de crime ainda não ocorrido, futuro e incerto"[122], disse Sebastião Júnior. O Relator também frisou que o direito de não produzir provas contra si tem limitações no ordenamento jurídico brasileiro, apontando como exceções a desobediência diante de ordem de parada de policiamento ostensivo e autoatribuição de falsa identidade.

Para Sebastião Reis Júnior[123], a obrigatoriedade do fornecimento do material biológico constitui um procedimento de classificação, individualização e identificação do indivíduo, e a negativa de se submeter à coleta seria o mesmo que recusar o fornecimento de impressões digitais nos procedimentos papiloscópicos dos institutos de identificação. Também explicou que a utilização do material genético como prova de fatos anteriores à determinação de seu fornecimento poderia violar o princípio que veda a autoincriminação, o que não foi discutido no caso do julgamento em questão. Conforme mencionado acima, repita-se, o Tema 905 do Supremo Tribunal Federal, que discute a exigência de perfil genético, encontra-se pendente de julgamento.

Ainda sobre os bancos de dados, o Supremo Tribunal Federal invalidou Lei do Estado do Tocantins que criou cadastro de usuários de drogas[124]. A Lei foi declarada inconstitucional porque além de usurpar competência privativa da União para legislar sobre matéria penal e

[121] *Ibid.*
[122] *Ibid.*
[123] *Ibid.*
[124] STF, ADI 6561 TO, Tribunal Pleno, Rel. Min. Edson Fachin, J. 13.10.2020, DJe 28.10.2020.

processual penal, também viola os princípios da dignidade da pessoa humana, da presunção de inocência e o direito à intimidade.

Nos autos da ADI 6561 TO, o Procurador Geral da República alegou que a lei estadual usurpava a competência privativa da União para legislar sobre matéria penal e processual penal, além de violar os princípios da dignidade da pessoa humana, da presunção de inocência e o direito à intimidade. Para Augusto Aras, a norma instituiu uma espécie de lista de antecedentes criminais cujo objetivo é tornar conhecidas, no meio policial, as pessoas que já foram detidas com substâncias entorpecentes. "*Não se recuperam pessoas lançando-as em cadastro que poderá trazer mais exclusão e estigmatização*", alegou[125].

O Ministro Fachin destacou em seu voto que que o cadastro de usuários de drogas se assemelha ao extinto rol de culpados, de que tratava o Artigo 393, inciso I, do CPC, que armazenava informações sobre condenações criminais transitadas em julgado. Ainda de acordo com Fachin, por se tratar de matéria tipicamente processual, é reservada à União legislar privativamente sobre o tema[126].

O Relator observou que há, na esfera federal, legislação própria, como a Lei número 11.343/06, que institui o Sisnad – Sistema Nacional de Políticas Públicas sobre drogas, voltado para a prevenção e o tratamento do usuário ou dependente de drogas, bem como plano individual de tratamento. Além disso, a sistematização dos dados, por sua vez, é tratada na esfera federal, por intermédio do Decreto número 5.912/06, que institui o Observatório Brasileiro de Informações sobre drogas. "*A gestão dessas informações, portanto, compete à União, não podendo os Estados criarem um cadastro próprio*", conclui Fachin[127].

Para Fachin, o cadastro revela um desvalor dos usuários e tem um viés de seletividade e higienização social incompatível com o Estado de Direito democrático e os direitos fundamentais dos cidadãos. Não há previsão de formas de controle prévio à inclusão da pessoa no cadastro, tão pouco comunicação e consentimento do interessado, exigindo-se, para sua exclusão, laudo médico e informação oficial sobre a não reincidência. Por fim, acrescentou que

[125]*Ibid.*
[126]STF, ADI 6561 TO, Tribunal Pleno, Rel. Min. Edson Fachin, J. 13.10.2020, DJe 28.10.2020.
[127]*Ibid.*

não há um protocolo claro de proteção e tratamento desses dados, que são alimentados com informações de caráter reservado[128].

Seguindo caminho diametralmente oposto, o Congresso Nacional aprovou a criação do cadastro de condenados por crimes sexuais[129]. O texto, que foi encaminhado para sanção presidencial, prevê que nome completo e número de CPF estejam disponíveis para consultar quem já foi autor dos crimes de estupro; registro não autorizado da intimidade sexual; estupro de vulnerável e favorecimento da prostituição ou de outra forma de exploração sexual de criança ou adolescente ou de vulnerável; e mediação para servir a lascívia de outrem, favorecimento da prostituição ou outra forma de exploração sexual, casa de prostituição e rufianismo.

Atualmente os denominados processos de crimes contra a dignidade sexual tramitam em sigilo, o que não acontecerá mais com a criação do cadastro. Caso os réus sejam absolvidos em instâncias superiores, os dados voltam a ser sigilosos. A consulta ao cadastro só será possível a partir do trânsito em julgado da sentença condenatória, ou seja, quando não houver mais possibilidade para recursos. Os dados ficarão disponíveis para acesso público por dez anos após o cumprimento integral da pena. Dados das vítimas, detalhes do caso e provas continuam sob sigilo.

No Distrito Federal, foi publicada a Lei número 7.547/2024, que criou o cadastro de condenados por crimes sexuais praticados contra crianças e adolescentes, permitindo que qualquer cidadão acesse informações de identificação e fotos de condenados. Conforme consta o texto da lei, o cadastro deverá ser disponibilizado em site oficial, possibilitando o acesso a qualquer cidadão do nome completo do condenado, data de nascimento, número de CPF e RG, foto, características físicas e histórico de crimes. Os integrantes das Polícias Civil e Militar, conselheiros tutelares, membros do Ministério Público e do Poder Judiciário terão acesso ao conteúdo integral do cadastro, além de outras informações, tais como filiação e endereço atualizado do condenado. As demais autoridades podem ter acesso ao cadastro a critério do

[128] *Ibid.*

[129] Senado Federal. Congresso aprova criação de cadastro de condenados por crimes sexuais. Disponível em: https://www12.senado.leg.br/tv/programas/noticias-1/2024/10/aprovada-criacao-do-cadastro-de-pedofilos-e-predadoressexuais#:~:text=Nesta%20quarta%2Dfeira%20(30),a%20preven%C3%A7%C3%A3o%20contra%20novos%20crimes. Acesso em 31 de out. 2024.

Poder Executivo. A normativa ressalva que, na hipótese de reabilitação, deve haver exclusão imediata do cadastro[130].

Apenas a título de exemplo, a criação de bancos de dados no Brasil não é recente. Em 1977, o Deputado José Faria Lima, durante discurso na Câmara dos Deputados, mencionou que o Brasil estava entre os dez maiores usuários de computadores no mundo e que em um mundo tecnológico, a informação é tão vital como a água e luz[131]. Enquanto foi Deputado, Faria Lima, que à época foi o representante da Câmara dos Deputados no Centro de Processamento de Dados do Senado (Prodasen), promoveu a integração das bases de dados entre as casas e a adoção de sistemas informáticos para organização do fluxo de trabalho legislativo.

Ciente da importância do armazenamento de informações para o Estado brasileiro, Faria Lima apresentou, no dia 08 de novembro de 1977, o Projeto de Lei número 4.365/1977[132], que tratava sobre o "Registro Nacional de Banco de Dados", estabelecendo normas de proteção da intimidade contra o uso indevido de dados arquivados em dispositivos eletrônicos de processamento de dados. Apesar dos vários argumentos, Faria Lima não conseguiu convencer o Congresso Nacional a legislar sobre dados pessoais.

O § único do Artigo 6º do Projeto de Lei em questão sugeriu que os bancos de dados operados pela Polícia, Órgãos de informações e Segurança das Forças Armadas e Serviço Nacional de Informações seriam registrado em separado, sem acesso ao público. Com a sugestão da criação do Registro Nacional de Banco de Dados, Faria Lima alegou que todos os bancos de dados existentes deveriam ter informações sobre o proprietário do banco de dados, pessoas responsáveis pela administração, local onde estaria situada a operação, características técnicas do bando de dado e finalidade do tratamento dos dados.

---

[130]DISTRITO FEDERAL. Lei número 7.547, de 23 de julho de 2024. Institui o Cadastro Distrital de Pessoas Condenadas por Crimes contra a Dignidade Sexual, e dá outras providências. Disponível em: https://www.cl.df.gov.br/-/lei-cria-cadastro-de-condenados-por-crimes-sexuais-contra-criancas-e-adolescentes#:~:text=A%20Lei%207.547%2F2024%2C%20que,de%20condenados%20por%20esses%20crimes . Acesso em 25 de nov. 2024.

[131]ZANATTA, Rafael Augusto Ferreira. A proteção coletiva dos dados pessoais no Brasil: a defesa de direitos entre autoritarismo e democracia. 2022. 356f. Tese (Doutorado). Instituto de Energia e Ambiente. Programa de Pós-Graduação em Ciência Ambiental. Universidade de São Paulo. São Paulo.

[132]BRASIL. Câmara dos Deputados. Projeto de Lei número 4.365/1977. Disponível em:https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=220936&fichaAmigavel=nao. Acesso em 23 de set. 2024.

Além disso, o Projeto de Lei também sugeriu que os dados poderiam ser excluídos a qualquer momento, desde que julgada inconveniente a divulgação ao público destas informações, por lesar os interesses de uma ou várias pessoas, ou que sua disseminação não atenda aos interesses do público em geral. O que mais chamou atenção no Projeto de Lei foi a visão do Parlamentar, que já vislumbrava a importância que os dados pessoais teriam com o avanço da tecnologia, em uma época onde pouquíssimas pessoas tinham acesso a sistemas informatizados.

Seguindo a cronologia legislativa sobre esse registro de dados, podemos mencionar a Lei número 12.850/2013[133], que no Artigo 10-A, § 1°, Incisos I e II define dados de conexão e dados cadastrais. Os primeiros são informações referentes a hora, data, início, término, duração, endereço de protocolo de internet (IP) utilizado e terminal de origem da conexão. Já os segundos são informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão. Cabe salientar que os conceitos sobre dados, ainda incipiente na legislação brasileira, foram extraídos do artigo 190-A do Estatuto da Criança e do Adolescente, Lei de 1990[134].

Percebe-se, portanto, que durante os últimos anos os dados pessoais passaram por transformações digitais e conceituais. Isso não aconteceu com a legislação brasileira, que parece não ter acompanhado a evolução tecnológica. Por esse motivo, apesar da ausência de uma Lei Penal de Proteção de Dados, os princípios da nossa Lei Geral de Proteção de Dados devem ser respeitados, com ressalvas, já que empresas detentoras de dados não podem utilizar a LGPD para omitir informações às polícias e ao Ministério Público, principalmente quando um crime esteja acontecendo ou na iminência de acontecer.

Nesse cenário, tem-se que a criação de um banco de dados penal no Brasil envolve diversas considerações legais e regulamentares. A Lei Geral de Proteção de Dados por exemplo,

[133]BRASIL. Lei número 12.850/2013 (Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm>. Acessado em: 18 de Mai. 2024.
[134]BRASIL. Lei número 8.069/90. Estatuto da Criança e do Adolescente. Art. 190-A. § 2 º Para efeitos do disposto no inciso I do § 1 º deste artigo, consideram-se: I – dados de conexão: informações referentes a hora, data, início, término, duração, endereço de Protocolo de Internet (IP) utilizado e terminal de origem da conexão; II – dados cadastrais: informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão. Disponível em https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em 31 de out. 2024.

estabelece as diretrizes para o tratamento de dados pessoais, incluindo os dados sensíveis como os penais. Por sua vez, a Lei nº 12.654/2012, que alterou a Lei de Execução Penal e a Lei de Identificação Criminal, permite a coleta de material biológico para a obtenção de perfis genéticos e a criação de um banco de dados nacional de perfis genéticos. A Comissão de Constituição e Justiça (CCJ) da Câmara dos Deputados aprovou o Projeto de Lei número 3.705/2019, que cria um banco de dados de criminosos a ser compartilhado por órgãos de segurança pública de todo o país, visando melhorar a eficiência das investigações criminais e a prevenção de crimes[135].

Conforme preceitua Nina Nery, não há dúvida de que, em hipóteses excepcionais, a proteção de indivíduos e da sociedade demandará uma intervenção estatal em esferas originalmente invioláveis, mas a legitimidade dessa atuação está condicionada à observância de um limite formal, que assegura que os direitos fundamentais estejam submetidos à reserva do legal, exigindo que qualquer intervenção nesses direitos dependa de uma autorização expressamente prevista em lei. "Qualquer intromissão do Estado em direitos individuais que não esteja legalmente autorizada deve ser considerada uma violação ilícita", conclui a autora[136].

O reconhecimento de que os direitos fundamentais criam um espaço de proteção de proteção contra intervenções do Estado deve vir acompanhado da noção de que não há direitos absolutos. Essa máxima, no entanto, não pode levar à própria negação desses mesmos direitos, de modo que, independentemente das circunstâncias do caso concreto, a intromissão nessa esfera de proteção dependerá de uma justificação especial[137]. Os problemas envolvendo o discurso de que não há direitos absolutos surgem justamente quando o argumento passa a ser invocado para justificar os compartilhamentos de dados de forma indiscriminada, o que acaba ganhando força quando associado a argumentos eficientistas[138].

---

[135]Câmara dos Deputados. CCJ aprova criação de banco de dados nacional de criminosos. Disponível em: https://www.camara.leg.br/noticias/764790-ccj-aprova-criacao-de-banco-de-dados-nacional-de-criminosos/. Acesso em 25 de nov. 2024.
[136]NERY, Nina. O compartilhamento de dados financeiros no sistema antilavagem de dinheiro brasileiro. São Paulo: Thompson Reuters Brasil, 2024. p.99.
[137]GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. O direito de proteção de dados no processo penal e na segurança pública. Rio de Janeiro: Marcial Pons, 2021.
[138]NERY, Nina, op.cit., 2024, p, 98.

O Ministério Público do Estado da Bahia acionou as quatro maiores operadoras de telefonia do Brasil[139], por compartilharem indevidamente dados pessoais de clientes do Estado. A Ação Civil Pública em questão reforçou que informações compartilhadas de modo indevido têm contribuído para fraudes e para o incômodo aos consumidores, que recebem diversas e inconvenientes ligações telefônicas ao longo do dia. Percebe-se, portanto, que a Lei Geral de Proteção de Dados não pode ser utilizada para embaraçar o trabalho dos órgãos de persecução penal, que também devem ser responsabilizados por quaisquer violações aos dados recebidos.

A recorrente recusa de informações sobre dados às polícias e ao Ministério Público pode ter motivado a elaboração do Projeto de Lei número 1.239/2024[140], que obriga às operadoras a fornecerem à polícia dados sobre celulares irregulares habilitados, com o intuito de permitir a localização dos aparelhos e dos chips em casos quanto estiverem envolvidos em crimes de furto, roubo, latrocínio ou em atividades criminosas. De acordo com a proposta, as operadoras terão um prazo de 36 horas para fornecer as informações, contanto a partir do recebimento do pedido documentado.

---

[139]Ministério Público do Estado da Bahia. MP aciona Vivo, Tim, Oi e Claro por compartilhamento indevido de dados pessoais. Disponível em: https://www.mpba.mp.br/noticia/60732. Acesso em 25 nov. 2024.

[140]BRASIL. Projeto de Lei número 1.239/2024. Disponível em: https://www.camara.leg.br/noticias/1054261-PROJETO-OBRIGA-OPERADORAS-A-FORNECEREM-A-POLICIA-DADOS-SOBRE-CELULARES-IRREGULARES-HABILITADOS. Art. 1º As operadoras de telefonia móvel são obrigadas a fornecer às autoridades de Segurança Pública os dados necessários para localizar telefones celulares e cartões SIM que tenham sido objeto de furto, roubo, latrocínio ou utilização em atividades criminosas. § 1º O fornecimento dos dados será realizado mediante solicitação fundamentada das autoridades policiais. § 2º Os dados fornecidos devem incluir as informações solicitadas pelas autoridades policiais, bem como outras informações essenciais para identificar a localização geográfica do dispositivo. § 3º Os dados devem ser enviados às autoridades solicitantes de forma confidencial, utilizando meios técnicos adequados para garantir a segurança e integridade das informações, e devem ser acessíveis apenas à autoridade policial competente. Parágrafo único. Para a implementação e execução da Estratégica, o Poder Executivo poderá criar um Comitê Gestor composto por representantes dos órgãos de segurança pública nacionais, com a finalidade de coordenar as ações, estabelecer metas e avaliar os resultados alcançados. Art. 2º As diretrizes da Estratégia incluem: a) criação de um banco de dados nacional de celulares roubados, acessível às autoridades, para registro e compartilhamento de informações sobre aparelhos furtados ou roubados; b) estabelecimento de procedimentos padronizados para bloqueio e rastreamento de celulares roubados, para agilidade e eficácia na recuperação dos dispositivos; c) incentivo ao uso de tecnologias de segurança para identificação e recuperação de aparelhos, além da implementação de sistemas de criptografia e autenticação para proteção de dados pessoais; e d) realização de campanhas de conscientização sobre os riscos do roubo de celulares, orientando os cidadãos sobre medidas preventivas de segurança, como o uso de senhas, biometria e aplicativos de rastreamento. Art. 3º As operadoras de telefonia móvel serão responsáveis por: a) bloquear imediatamente o IMEI de celulares roubados reportados pelos usuários, em conformidade com as instruções das autoridades competentes; b) colaborar com as autoridades na identificação e localização de aparelhos adquiridos, fornecendo informações precisas e atualizadas sobre a situação dos dispositivos; c) manter registros atualizados de celulares bloqueados e compartilhar essas informações com os órgãos competentes, relacionados ao combate ao comércio ilegal de aparelhos. Art. 4º As operadoras têm prazo de 36 horas para fornecer as informações, contadas a partir do recebimento do pedido documentado. Art. 5º O descumprimento do disposto nesta Lei configurará ato de desobediência e obstrução à Justiça, a ser punido na forma da legislação correspondente. Art. 6º Esta Lei entra em vigor no prazo de 30 (trinta) dias após a sua publicação. Acessado em: 18 de mai. 2024.

Pelo texto do PL em questão, as operadoras de telefonia móvel serão responsáveis pelo bloqueio imediato do IMEI (número de registro) de celulares roubados, por colaborar com as autoridades na identificação e localização de aparelhos habilitados, fornecendo informações precisas e atualizadas sobre a situação dos dispositivos e também serão obrigadas a manterem os registros atualizados de celulares bloqueados, compartilhando informações com os órgãos competentes.

O Projeto também esclarece que o envio dos dados deverá ser feito de maneira a manter o sigilo e a integridade das informações, que só poderão ser acessadas pela autoridade policial competente. Por fim, o Projeto previu a criação de um comitê gestor nacional, com representantes dos órgãos de segurança pública, para coordenar as ações, estabelecer metras e avaliar os resultados alcançados, incluindo a criação de um banco de dados nacional de celulares roubados[141].

Conforme pode ser observado, cada vez mais a temática da proteção de dados vem ganhando relevância na área penal. Isso ficou evidente no julgamento da ADF 722[142], que analisou a utilização, por parte do Ministério da Justiça, de dados pessoais para a investigação sigilosa em desfavor de opositores do Governo, denominados "dossiês antifascistas". O Plenário do Supremo Tribunal Federal julgou inconstitucionais os atos do Ministério da Justiça, reiterando que as atividades de inteligência devem respeitar o regime democrático, sem perseguir opositores.

Na ocasião, o Ministério da Justiça produziu relatórios através da utilização e do compartilhamento de informações sobre a vida pessoal, as escolhas pessoais e políticas e as práticas cívicas de pessoas identificadas como integrantes de um movimento político denominado antifascismo, que dentro dos limites da legalidade exerciam seus direitos de livre expressão, reunião e associação.

Na Arguição de Descumprimento de Preceito Fundamental, a Rede Sustentabilidade questionou investigação sigilosa que foi aberta contra um grupo de 579 servidores federais e estaduais de segurança, além de três professores universitários que foram identificados como integrantes do movimento antifascismo. Chegou ao conhecimento do referido partido político

[141] *Ibid.*
[142] STF, ADPF 722, Tribunal Pleno, Rel. Carmén Lúcia, J. 16.05.2022, DJe 22.06.2022.

que a Secretaria de Operações Integradas do Ministério da Justiça havia produzido um dossiê com nomes, endereços, fotografias e contas de redes sociais de pessoas que faziam parte do movimento e que utilizavam as suas contas virtuais para deferir palavras contra o governo, sem que os envolvidos tivessem conhecimento dessa prática. Posteriormente, o dossiê foi distribuído, na forma de relatório, para as administrações públicas federais e estaduais.

A Relatora, Ministra Carmem Lúcia, votou pela procedência do pedido, sob o fundamento de que o serviço de inteligência é necessário para fins de segurança pública e segurança nacional e para a garantia de cumprimento eficiente dos deveres do Estado, mas não pode ser desempenhado fora de estritos limites constitucionais e legais, sob pena do comprometimento da democracia em sua instância mais central, que é a de garantia dos direitos fundamentais. A Ministra também reiterou que "as atividades de inteligência devem respeitar o regime democrático, no qual não se admite a perseguição de opositores e o aparelhamento político do Estado. O histórico de abusos relatados quanto ao serviço de inteligência acentua a imperiosidade do efetivo controle dessa atividade"[143], concluiu.

Ainda de acordo com a Ministra[144], é imprescindível que a coleta de dados, a produção de informações e o seu compartilhamento entre os órgãos do Sistema Brasileiro de Inteligência estejam estritamente vinculados ao interesse público. Carmem Lúcia afirmou que

> "o uso da máquina estatal para a colheita de informações de servidores com postura política contrária ao governo caracteriza desvio de finalidade e afronta aos direitos fundamentais de livre manifestação do pensamento, de privacidade, reunião e associação. É no debate político que a democracia é exercida com o vigor de sua essência"[145].

Nunes Marques foi o único Ministro que divergiu, por considerar que não houve comprovação dos atos do Ministério que tenham violado garantias constitucionais, mas somente relatórios cujo objetivo era a segurança pública e prevenir atos que poderiam gerar tumultos, agressões físicas e depredação ao patrimônio público e privado.

Embora exista uma ausência de um regramento geral na regulamentação do uso de dados pessoais por parte dos órgãos de persecução penal, recorrentemente o tema chega ao judiciário,

---

[143] *Ibid.*
[144] *Ibid.*
[145] *Ibid.*

demonstrando urgência na elaboração de uma Lei que defina os parâmetros legais. Além dos exemplos já mencionados acima, na ADO 84[146] a Procuradoria Geral da República questionou a falta de regulamentação de monitoramento secreto de tablets e telefones celulares, feita por órgãos e agentes públicos através de softwares espiões. Na ocasião, a PGR solicitou ao Supremo Tribunal Federal a criação de regras provisórias até que o Congresso Nacional edite lei sobre o tema.

Na Ação Direta de Inconstitucionalidade por Omissão, a PGR alegou que novas ferramentas tecnológicas vêm sendo utilizadas por serviços de inteligência e órgãos de repressão estatais para vigilância remota e invasiva de dispositivos móveis, sob pretexto de combate ao terrorismo e ao crime organizado. Ainda de acordo com a Procuradoria Geral da República, apesar de avanços na legislação para proteger a intimidade, a vida privada e a inviolabilidade do sigilo das comunicações pessoais, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais (LGPD), ainda não há uma regulamentação sobre programas de infiltração virtual remota.

Para a Procuradoria Geral da República, os instrumentos podem ser eficazes no combate à criminalidade, mas sua utilização deve observar os direitos fundamentais à intimidade e à vida privada e a inviolabilidade do sigilo das comunicações pessoais, com autorização judicial prévia para obtenção dos dados pessoais dos investigados. Conforme mencionado acima, a PGR solicitou ao Supremo Tribunal Federal a implementação de regras provisórias a serem estabelecidas e que tenham como objetivo a proteção dos direitos fundamentais à intimidade, à privacidade e à inviolabilidade do sigilo das comunicações pessoais e dados, até que o Congresso Nacional aprove lei sobre o assunto[147].

Percebe-se que, apesar da Procuradoria Geral da República também ser um órgão de persecução penal, fica evidente a preocupação com o grau de intervenção nos direitos fundamentais. Essa tem sido uma tendência nos últimos anos, o que pode se tornar mais evidente depois que a proteção de dados pessoais se tornou um direito fundamental. O que deve ser destacado, porém, é que os órgãos de persecução penal devem atuar nos limites da autorização legal para intervenção nos direitos fundamentais.

[146]STF, ADO 84, Tribunal Pleno, Rel. Min. Cristiano Zanin, J. 16.04.2024, DJe 16.04.2024.
[147]STF, ADO 84, Tribunal Pleno, Rel. Min. Cristiano Zanin, J. 16.04.2024, DJe 16.04.2024.

Trazendo esse debate para o tema aqui desenvolvido, é preciso frisar que nos dias de hoje o acesso aos dados dos próprios bancos de dados feito pelas policiais judiciárias é fundamental para a prevenção e o combate ao crime organizado. Necessária fazer uma reflexão, poque cada vez mais os métodos para a prática de crimes se transformam, modernizando-se e encontrando novos formas para desenvolver novas infrações penais.

O entendimento também foi compartilhado por alguns parlamentares e especialistas que participaram, no dia 18 de novembro de 2021, de audiência pública[148] realizada com o intuito de debater o uso equivocado da Lei Geral de Proteção de Dados pela administração pública, para impedir o acesso a informações. Os especialistas ouvidos pela Comissão de Fiscalização Financeira e Controle da Câmara dos Deputados afirmaram que o acesso a informações de órgãos públicos e de agentes públicos não pode ser prejudicado por interpretações equivocadas da Lei Geral de Proteção de Dados. Também foi frisado que não há conflito entre a LGPD e a Lei de Acesso à informação.

À época, o Procurador da República encarregado pela proteção de dados pessoais no Ministério Público Federal, Leonardo Macedo[149], mencionou que:

> Recentemente foi inclusive editada uma nota técnica explicando que a Lei Geral de Proteção de Dados e o compartilhamento de dados previstos nesta legislação não afeta o poder de requisição de dados previsto na Lei Complementar 75/93, que confere ao Ministério Público a possibilidade de obter os dados de quaisquer instituições públicas e privadas", disse. "Evidentemente, tratando-se de dados sujeitos a sigilo, cabe a quem recebe esses dados adotar as medidas necessárias para a preservação desse sigilo.
> Fonte: Agência Câmara de Notícias[150].

Na mesma audiência pública, a Diretora da Autoridade Nacional de Proteção de Dados (ANPD), Miriam Wimmer[151], ressaltou que a transparência continua sendo a regra e o sigilo a exceção. Ainda de acordo com Miriam Wimmer, a Lei Geral de Proteção de Dados não criou novas hipóteses de sigilo, garantindo, tão somente, a proteção de dados e informações pessoais.

---

[148]Câmara dos Deputados. Deputados e sociedade civil denunciam uso equivocado da LGPD pela administração pública para impedir acesso a informações. Disponível em: https://www.camara.leg.br/noticias/828370-acesso-a-informacao-nao-pode-ser-prejudicado-por-conta-de-lei-de-protecao-de-dados-dizem-especialistas/. Acessado em: 21 de mai. 2024.
[149]*Ibid.*
[150]*Ibid.*
[151]*Ibid.*

Por fim, mencionou que não existe uma resposta fechada para todas as circunstâncias, mas que o agente público deve analisar nos casos concretos se existe o interesse público preponderante, afirmando que "é claro que a proteção de dados não deve ser levantada como óbice para o exercício de competências investigativas e fiscalizadoras decorrente da lei"[152].

Isso demonstra que, embora atuem profissionalmente em áreas distintas, os especialistas não divergem sobre como deve ser interpretada a proteção de dados diante de iminente violação a outros direitos fundamentais. Um dos grandes desafios para os órgãos de persecução penal é identificar as situações concretas onde a utilização dos dados pessoais deve prevalecer, diante do interesse público e de eventuais riscos a outros direitos fundamentais.

Seguindo a mesma lógica do que foi mencionado até agora, a terceira seção do Superior Tribunal de Justiça, a partir de precedentes do Supremo Tribunal Federal, considerou ilegal obtenção direta de dados fiscais por iniciativa do Ministério Público[153], sem autorização judicial. Nesse caso específico, o colegiado do STJ deu provimento a dois recursos em habeas corpus nos quais os acusados alegaram constrangimento ilegal em razão da obtenção direta de seus dados fiscais a partir de solicitação feita pela Ministério Público para a Receita Federal.

Para o Ministro Sebastião Reis Júnior, Relator de um dos recursos, a orientação do Supremo Tribunal Federal, no Tema 990[154], permite que a Receita Federal encaminhe ao Ministério Público dados fiscais quando houver suspeita de crime, mas não possibilita ao órgão de acusação requisitar esses mesmos dados sem autorização judicial. O STF referendou que é constitucional o compartilhamento de relatórios de inteligência financeira e de procedimentos fiscalizatórios da receita federal com órgãos de persecução penal para fins penais, sem prévia autorização da justiça.

Os acusados foram denunciados pelos crimes de estelionato majorado, falsidade ideológica e uso de documento falso. O Ministério Público solicitou diretamente ao superintendente da Receita Federal as declarações de Imposto de Renda dos investigados, de

---

[152]*Ibid.*

[153]Superior Tribunal de Justiça. A partir de precedente do Supremo Tribunal Federal, terceira seção considera ilegal obtenção direta de dados fiscais por iniciativa do MP. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/11022022-A-partir-de-precedente-do-STF--Terceira-Secao-considera-ilegal-obtencao-direta-de-dados-fiscais-por-iniciativa-do-.aspx. Acessado em 21 de mai. 2024.

[154]STF, TEMA 990, Tribunal Pleno, Rel. Min. Dias Toffoli, J. 04.12.2019, DJe 06.10.2020.

seus familiares e de empresas suspeitas, sem ordem judicial. Posteriormente, a documentação foi juntada ao processo com autorização do Juiz.

O Tribunal de origem negou a retirada dessas informações dos autos, pleiteada pelas defesas por meio de habeas corpus em que alegaram ter havido quebra de sigilo fiscal. De acordo com a corte regional, o aumento da corrupção e da criminalidade em geral recomenda que os órgãos de investigação sejam fortalecidos. Para o Relator, as poucas referências que o STF fez à solicitação direta de dados pelo Ministério Público, foram no sentido de sua ilegalidade. Nesse sentido, o Ministro Luís Roberto Barroso afirmou que "se o Ministério Público quiser ter acesso direto a informações bancárias, ele precisa de autorização judicial. Essa é a determinação constitucional"[155], concluiu.

O Relator também mencionou que nos dias de hoje as informações protegidas por qualquer tipo de sigilo se tornam públicas com muita frequência, sem que os responsáveis pelo vazamento sejam identificados e punidos[156]. Por esse motivo, para o Ministro, isso reforça a preocupação que se deve ter com a possibilidade de obtenção de informações sigilosas, de modo informal e sem controle ou supervisão. No momento em que determinou a exclusão, nos autos, de todas as informações obtidas pelo Ministério Público por intermédio da Receita Federal, o Ministro reiterou que o caso julgado se distingue do precedente do STF no Tema 990, porque nesse caso o Ministério Público não fez a requisição diretamente para a Receita Federal.

Por fim, o Ministro Sebastião Reis Júnior afirmou que:

> "Em um Estado de Direto, não é possível admitir que órgãos de investigação em procedimentos informais e não urgentes, solicitem informações detalhadas sobre indivíduos ou empresas, informações essas constitucionalmente protegidas, salvo se houver autorização judicial"[157].

[155]Superior Tribunal de Justiça. A partir de precedente do Supremo Tribunal Federal, terceira seção considera ilegal obtenção direta de dados fiscais por iniciativa do MP. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/11022022-A-partir-de-precedente-do-STF--Terceira-Secao-considera-ilegal-obtencao-direta-de-dados-fiscais-por-iniciativa-do-.aspx. Acessado em 21 de mai. 2024.
[156]*Ibid.*
[157]*Ibid.*

Cabe ressaltar que a 5ª Turma do Superior Tribunal de Justiça[158] entendeu que a autoridade policial pode acionar o Coaf antes da instauração de inquérito policial, sendo necessária apenas que isso seja feito por comunicação formal, em procedimento com garantia de sigilo e sujeito a controle.

O RE 1.055.941[159] tornou-se um *Leading Case,* porque aborda a temática do compartilhamento de dados pessoais na esfera criminal, tendo em vista a inexistência de legislação específica para regular o tema, porque, conforme mencionado acima, o Supremo Tribunal Federal fixou a tese de que "é constitucional o compartilhamento de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil, com órgãos de persecução penal, para fins criminais, sem prévia autorização judicial".

A mesma 5ª Turma do Superior Tribunal de Justiça entendeu, em junho de 2024[160], que o Ministério Público não pode requisitar informações ao Coaf sem prévia instauração de um inquérito formal. A decisão foi tomada por maioria, em análise de recurso que questionava a validade de relatórios de inteligência financeira obtidos antes da formalização de uma investigação.

Os temas debatidos acima em nossas Cortes Superiores nos remetem à autodeterminação informativa[161], que é o poder que todos nós temos de controlar nossos próprios dados, pressupondo a existência de uma finalidade específica para que órgãos públicos ou empresas privadas realizem o tratamento de dados pessoais. Para Ademar Borges, "Uma das exigências é que a autodeterminação informacional impõe à atuação do Estado é a vinculação finalística no tratamento de dados pessoais"[162]. Ainda de acordo com Ademar Borges, "a ideia de que o manejo de dados pelo poder público – em particular dados pessoais – está submetido ao princípio da vinculação finalística ou da vinculação a um fim"[163].

---

[158]BRASIL. Quinta Turma – STJ. Autoridade policial pode acionar Coaf antes de instaurar inquérito policial, diz STJ. Disponível em: https://www.youtube.com/watch?v=x1mIz2LbyLY. Acessado em 22 de mai. 2024.
[159]STF, RE 1055941, Tribunal Pleno, Rel. Min. Dias Toffoli, J. 04.12.2019, DJe 06.10.2020.
[160]Estadão. Decisão do STJ que veta dados do Coaf para Polícia sem inquérito põe fim a "devassa indiscriminada". Disponível em: https://www.estadao.com.br/politica/blog-do-fausto-macedo/decisao-do-stj-que-veta-dados-do-coaf-para-policia-sem-inquerito-poe-fim-a-devassa-indiscriminada/. Acesso em 25 de set. 2024.
[161]MENDES, Laura S. F. Autodeterminação informativa: a história de um conceito. Rev. de Ciências Jurídicas Pensar, v. 25, n. 4, 2020. Disponível em: <https://periodicos.unifor.br/rpen/article/view/10828/pdf>. Acesso em 28 de out. 2024.
[162]BORGES, Ademar. O relatório de inteligência financeira como meio de obtenção de prova no processo penal. *Revista Brasileira de Ciências Criminais* vol. 176. ano 29. p. 69-105. São Paulo, fevereiro/2021.
[163]*Ibid.*

Sobre a mesma temática, Alaor Leite e Adriano Teixeira escreveram o artigo intitulado *Gestão do Poder Informacional no Processo Penal no RHC 147.797-STJ*. "É Tarefa do legislador, mas também da jurisprudência e da doutrina, determinar com precisão como se dá o ingresso de informações obtidas por outros órgãos no seu de uma investigação criminal"[164], concluem. Uma solução equilibrada, que leve em conta a tensão instalada entre interesses persecutórios e direitos individuais, deverá partir de uma espécie de tipologia das modalidades de compartilhamento de dados[165].

Ainda de acordo com os autores, é inegável o quadro de divergência jurisprudencial entre o STF e o STJ, o que é potencializado pela lacuna legislativa. Tal desencontro não é meramente semântico e, por produzir efeitos práticos evidentes, demanda alguma elaboração doutrinária, até que o legislador atue ou que nova decisão aclaradora sobrevenha[166]. Enquanto isso, inúmeras investigações criminais no âmbito do intercâmbio da troca de informações prosseguem incertas quanto ao seu destino[167], o que não significar dizer que deve ocorrer anulação irrestrita de tudo o que foi realizado até aqui pelos órgãos de persecução penal. A dúvida existente tampouco deve significar uma autorização geral implícita, antecipada ou clarividente, para a livre circulação de dados; Constitui irrevogável avanço do publicismo liberal o de distinguir claramente entre norma de competência e norma de autorização[168].

No Dossiê – *Privacidade de Dados Pessoais na Segurança Pública e no Processo Penal*, Heloisa Estellita abordou o RE 1.055.94, sob o pretexto de explorar alguns limites à transmissão, distribuição, comunicação, transferência e difusão de dados pessoais pelo COAF. Nesse artigo, a Autora analisou a questão central do RE, que é aferir se a revelação de informações sigilosas (financeiras) pelo Conselho de Controle de Atividades Financeiras

[164]LEITE; Alaor; TEIXEIRA; Adriano. Consultor Jurídico. Gestão do Poder Informacional no Processo Penal no RHC 147.707-STJ (parte 1). Disponível em: https://www.conjur.com.br/2023-set-14/leite-teixeira-gestao-poder-informacional-processo-penal/. Acesso em 09 de set. 2024.
[165]*Ibid.*
[166]LEITE; Alaor; TEIXEIRA; Adriano. Consultor Jurídico. Gestão do Poder Informacional no Processo Penal no RHC 147.707-STJ (parte 1). Disponível em: https://www.conjur.com.br/2023-set-14/leite-teixeira-gestao-poder-informacional-processo-penal/. Acesso em 09 de set. 2024.
[167]*Ibid.*
[168]*Ibid.*

(COAF) às autoridades de persecução penal por meio de relatórios de inteligência financeira (RIFs) necessita ou não de autorização judicial prévia[169].

Estellita reforçou que cada forma ou fase do tratamento de dados – a obtenção, o armazenamento, a utilização, a transferência etc. – configura uma espécie de uma intervenção autônoma no direito à autodeterminação informacional, direito que garante ao titular o controle sobre cada tratamento que é feito com seus dados[170]. Heloisa Estelita menciona, ainda, que "tanto a coleta de um dado para fins de inteligência ou segurança pública (uma finalidade), como por exemplo a sua transmissão e utilização para fins de persecução penal (outra finalidade) têm de estar autorizadas em lei"[171].

Ainda de acordo com Heloisa Estelita, diante da questão da proteção de dados no Brasil, é preciso observar que toda legislação vigente no Brasil se compõe dos seguintes elementos: dever de abstenção frente aos direitos fundamentais e intervenções apenas quando autorizadas por lei que seja proporcional, respeitando o direito fundamental à proteção de dados pessoais, a autorização legal e a finalidade prevista para o tratamento. Por fim, a Autora mencionou que para não gerar prejuízos irreparáveis às atividades de inteligência, de segurança pública e de persecução penal, é possível aproveitar o que os alemães denominam de "bônus de transição"[172], que no Brasil é chamado de modulação dos efeitos, concedendo um prazo mais razoável para adaptação da legislação às exigências da proteção de dados.

Até outubro de 2024, o compartilhamento de Relatórios de Inteligências Financeiras nos Tribunais Superiores foi analisado nos seguintes julgamentos: 2019/STF/TEMA 990: É Constitucional o compartilhamento de RIFs sem autorização judicial. Requisitos: a) procedimentos formais de investigação; b) comunicações formais; c) garantia de sigilo; d) certificação de destinatário; e) controle posterior; 2021/STF/HC 201.965/RJ: É nulo o RIF produzido a pedido (RIF a pedido) das autoridades sem a prévia instauração de investigação. A realização de diligências pelo COAF junto a bancos configura *fishing expedition*;

---

[169]ESTELITA, Heloísa. Portal de Periódicos IDP. *O RE 1.055.941: um pretexto para explorar alguns limites à transmissão, distribuição, comunicação, transferência e difusão de dados pessoais pelo COAF*. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5991. Acesso em 10 de set. 2024.
[170]*Ibid.*
[171]ESTELITA, Heloísa. Portal de Periódicos IDP. *O RE 1.055.941: um pretexto para explorar alguns limites à transmissão, distribuição, comunicação, transferência e difusão de dados pessoais pelo COAF*. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5991. Acesso em 10 de set. 2024.
[172]*Ibid.*

2023/STJ/RHC 147.707: Nulidade do RIF de intercâmbio (a pedido das autoridades de persecução penal) sem autorização judicial. Legitimidade do RIF de ofício (encaminhado pelo COAF sem prévia solicitação); 2023/STF/RCL 61.944: É válida a confecção de RIFs a pedido (de intercâmbio) sem autorização judicial, em consonância com o Tema 990. *Decisão Monocrática; 2024/STF/RCL 61.944: Primeira Turma confirma a decisão monocrática. Estão permitidos RIFs a pedido sem autorização judicial; 2024/STF/RE 1.393.219: Segunda Turma, referindo o Tema 990 (mencionado acima), decidiu que o MP não pode requisitar dados fiscais diretamente à Receita Federal; 2024/STJ/RHC 188.838: É legítimo o compartilhamento de RIF de intercâmbio, sem autorização judicial, antes da instauração de inquérito policial. (21 de maio); 2024/STJ/RHC 187.335: MP não pode requerer RIF de intercâmbio sem autorização judicial, antes da instauração de inquérito. (18 de junho); 2024/STF/RCL 70.191: Oposição ao RHC 187.335. É legítimo o compartilhamento de RIF de intercâmbio sem autorização judicial, mesmo antes da instauração de inquérito policial. (26 de agosto); 2024/STJ/RHC 188.838 EDS: PF não pode requerer RIF de intercâmbio, sem autorização judicial, antes da instauração de inquérito. (26 de setembro).

Enquanto não houver uma legislação específica para o tratamento de dados na segurança pública e persecução penal, os Tribunais Superiores continuarão recebendo inúmeras demandas relacionadas à privacidade e a proteção de dados pessoais. Nas palavras de Alaor Leite e Adriano Teixeira, "gerir a distribuição do poder informacional do Estado, de modo a equilibrar interesses persecutórios e direitos individuais, é, de fato, dos maiores desafios que o processo penal moderno tem diante de si"[173].Sensível a essa demanda, a Autoridade Nacional de Proteção de Dados, que não pode ser omissa, emitiu a Nota Técnica número 175/2023/CGF/ANPD[174], que avaliou acordo firmado entre o Ministério da Justiça e Segurança Pública (MJSP) e a Confederação Brasileira de Futebol (CBF).

A Nota Técnica trata sobre o acordo de cooperação entre o MJSP e a CBF para compartilhamento de dados pessoais visando o aprimoramento do Projeto Estádio Seguro, que prevê ações de combate ao racismo e à violência nos estádios brasileiros, com a aplicação do

[173]LEITE; Alaor; TEIXEIRA; Adriano. Consultor Jurídico. Gestão do poder informacional no processo penal no RHC 147.707-STJ (parte 2). Disponível em: https://www.conjur.com.br/2023-set-15/leite-teixeira-gestao-poder-informacional-processo-penal-2/. Acesso em 25 de nov. 2024.
[174]AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Nota Técnica nº 175/2023/CGF/ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acessado em de junho. 2024.

uso de tecnologias que permitam identificar torcedores que tenham se envolvido em ilícitos e possam por ventura, causar problemas nos estádios[175].

Além de promover ações de combate ao racismo e à violência nos estádios brasileiros, o acordo de cooperação também prevê a aplicação de tecnologias para verificar se o comprador de ingressos possui mandados de prisão em aberto ou se há a utilização de documento falso. Embora a Nota Técnica tenha o objetivo de combater e prevenir a prática de crimes, o que envolve a segurança pública e a persecução penal, há a previsão de que os princípios previstos na Lei Geral de Proteção de Dados devem ser observados. Além disso, coube ao Poder Público o relatório de ciclo de monitoramento do tratamento dos dados pessoais[176].

Embora exista uma previsão no Artigo 1º, § 4º da Lei Geral de Proteção de Dados, que determina uma exceção para que os dados pessoais não sejam tratados para fins de segurança pública, o tratamento, caso ocorra, deve observar o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD. Outro aspecto que deve ser destacado é que a LGPD atribuí, de forma expressa, competência para que a ANPD emita opiniões ou recomendações referentes às exceções previstas no inciso III do Artigo 4º da Lei (o tratamento

[175]Para confecção dessa Nota Técnica, a ANPD utilizou como referência as seguintes legislações: Lei número 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados; Lei número 13.675, de 11 de junho de 2018 – Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública, nos termos do § 7º do art. 144 da Constituição Federal; cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS); institui o Sistema Único de Segurança Pública (Susp); altera a Lei Complementar 79, de 7 de janeiro de 1994, a Lei número 10.201, de 14 de fevereiro de 2001, e a Lei nº 11.530, de 24 de outubro de 2007; e revoga dispositivos da Lei n° 12.681, de 04 de julho de 2012; Lei número 8.159, de 08 de janeiro de 1991 – Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências; Lei número 14.597, de 14 de junho de 2023 – Institui a Lei Geral do Esporte; Decreto número 9.489, de 30 de agosto de 2018 – Regulamenta, no âmbito da União, a Lei número 13.675, de 11 de junho de 2018, para estabelecer normas, estrutura e procedimentos para a execução da Política Nacional de Segurança Pública e Defesa Social; Portaria Ministerial número 218, de 29 de setembro de 2021 – Dispõe sobre a Plataforma Integrada de Operações e Monitoramento de Segurança Pública – Córtex; Decreto número 11.348, de 1º de janeiro de 2023 – Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Justiça e Segurança Pública e remaneja cargos em comissão e funções de confiança; Decreto número 10.777, de 24 de agosto de 2021 – Política Nacional de Inteligência de Segurança Pública (PNISP);Decreto número 10.778, de 24 de agosto de 2021 – Estratégia Nacional de Inteligência de Segurança Pública (ENISP); Decreto número 10.046, de 09 de outubro de 2019 – Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

[176]AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Nota Técnica nº 175/2023/CGF/ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acessado em de junho. 2024.

de dados previsto na lei não pode ser utilizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão à infrações penais)[177].

Conforme consta na Nota, o acordo de cooperação no âmbito do Projeto Estádio Seguro tem como finalidade a recaptura de indivíduos com mandado de prisão ou medidas penais restritivas, o auxílio na recuperação de veículos roubados ou furtados e o combate à falsidade documental no ato da compra de ingressos, o que pode prevenir a prática do "cambismo".

Vários são os pontos relevantes da Nota Técnica, tendo em vista ser a primeira vez que a Autoridade Nacional de Proteção de Dados foi acionada para falar sobre o tratamento de dados pessoais na prevenção e repressão de práticas criminosas. Um dos pontos relevantes foi o Ministério da Justiça e Segurança Pública ter indicado a Coordenação-Geral de Inteligência do próprio Ministério como operador. A ANPD fez uma ressalva, informando que muito embora a prática não seja um erro, é preciso esclarecer que a indicação do operador, quando se constitui em órgão do próprio controlador, no caso o Ministério da Justiça, se torna, nas palavras da Nota Técnica, uma "denominação eficaz"[178].

A ressalva da Autoridade Nacional de Proteção de Dados é relevante, porque apesar de não ser comum a nomeação de um controlador que exerça funções no próprio órgão controlador, o profissional precisa conhecer o dia a dia da instituição, o que mitigará os riscos e os desafios que serão enfrentados no tratamento dos dados pessoais. preciso estabelecer a diferença entre os atores elencados pela Lei Geral de Proteção de Dados. São eles o titular de

[177]BRASIL. Lei número 13.709/2018. Lei Geral de Proteção de Dados. Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: (...) III – realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou (...) § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta lei. § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo. § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impactos à proteção de dados pessoais. § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que se trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. Art. 55-J. Compete à ANPD: (...) XX – deliberar, na esfera administrativa, em caráter terminativo, sobre interpretação desta Lei, as suas competências e os casos omissos. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 02 de nov. 2024.

[178]AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Nota Técnica nº 175/2023/CGF/ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acessado em de junho. 2024.

dados pessoais, o controlador, o operador de dados, o encarregado e a Autoridade Nacional de Proteção de Dados.

Dos cinco atores, os três que mais geram dúvidas são o controlador, o operador de dados e o encarregado. O controlador de dados, conforme consta na Lei Geral de Proteção de Dados, é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. O controlador será o responsável pela conferência dos elementos necessários para o esse tratamento de dados pessoais, tais como finalidade, base legal, natureza dos dados coletados e duração do tratamento. O controlador, portanto, possui um poder de decisão, o que faz com que faz com que esse encargo não possa ser exercido por profissional que não possua autonomia para julgar a melhor forma de tratamento dos dados pessoais[179].

O operador, por sua vez, é a pessoa natural ou jurídica de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Significa dizer que o operador é o responsável pelo tratamento de dados pessoais em nome do controlador, que determina todas as diretrizes. Nesse sentido, o operador não possui poder de decisão sobre os elementos essenciais do tratamento, porém pode ser responsabilizado por danos causados em razão do tratamento irregular de dados. A responsabilização ocorrerá em caso de descumprimento das obrigações legais ou se houver inobservância das instruções do controlador. Percebe-se, portanto, que o tratamento de dados pessoais não é, necessariamente, realizado exclusivamente pelo controlador, que apesar de também poder realizar o tratamento de dados pessoais, tem o poder de decisão para, depois de estabelecer diretrizes, transferir a missão ao operador[180].

O encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares de dados e a Autoridade Nacional de Proteção de Dados. Conforme será visto adiante, o encarregado também é conhecido como DPO (Data Protection officer), não se exigindo nenhuma qualificação profissional específica para o exercício dessa função. Recomenda-se, no entanto, que o profissional tenha conhecimento do

[179]Ministério da Ciência Tecnologia e Inovação. Controlador, Operador e Encarregado de Dados. Disponível em:https://www.gov.br/aeb/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd/controlador-operador-e-encarregado-de-dados. Acesso em 02 de nov. 2024.
[180]*Ibid.*

fluxo de dados dentro da organização, coordene a implantação e a manutenção do sistema de gestão de dados pessoais, assegure que o tratamento esteja em conformidade com a lei e principalmente tenha autonomia para realizar suas atribuições e que possua conhecimento adequado de proteção e tratamento de dados pessoais[181].

O objeto de tratamento pessoais abordado neste trabalho está vinculado às instituições policiais, mais especificamente à Polícia Civil do Distrito Federal, o que faz com que a indicação do responsável pelos sistemas que armazenam dados pessoais seja decidida com muita cautela. Foi mencionado acima que o profissional precisa conhecer o fluxo de dados pessoais que tramitam em sua instituição. Isso não quer dizer, porém, que profissionais de outras instituições públicas, como é o caso dos Membros dos Ministérios Públicos, não possam auxiliar nessa função.

O Ministério Público possui diversas atribuições previstas no Artigo 129 da Constituição da República Federativa do Brasil de 1988[182]. Dentre as funções institucionais do Ministério Público, merece destaque, por estar diretamente ligada ao tema deste trabalho, o controle externo da atividade policial. O controle externo da atividade policial foi tema de trabalho desenvolvido pelo Conselho Nacional do Ministério Público[183], que elaborou o relatório[184] denominado *O Ministério Público e o Controle Externo da Atividade Policial*.

O Plenário do Conselho Nacional do Ministério Público aprovou, em novembro de 2023, por unanimidade, nova regulamentação das atribuições no Ministério Público no controle

---

[181]*Ibid.*

[182]BRASIL. Art. 129. São funções institucionais do Ministério Público: I - promover, privativamente, a ação penal pública, na forma da lei; II - zelar pelo efetivo respeito dos Poderes Públicos e dos serviços de relevância pública aos direitos assegurados nesta Constituição, promovendo as medidas necessárias a sua garantia; III - promover o inquérito civil e a ação civil pública, para a proteção do patrimônio público e social, do meio ambiente e de outros interesses difusos e coletivos; IV - promover a ação de inconstitucionalidade ou representação para fins de intervenção da União e dos Estados, nos casos previstos nesta Constituição ; V - defender judicialmente os direitos e interesses das populações indígenas; VI - expedir notificações nos procedimentos administrativos de sua competência, requisitando informações e documentos para instruí-los, na forma da lei complementar respectiva; VII - exercer o controle externo da atividade policial, na forma da lei complementar mencionada no artigo anterior; VIII - requisitar diligências investigatórias e a instauração de inquérito policial, indicados os fundamentos jurídicos de suas manifestações processuais; IX - exercer outras funções que lhe forem conferidas, desde que compatíveis com sua finalidade, sendo-lhe vedada a representação judicial e a consultoria jurídica de entidades públicas. Art. 129 da Constituição Federal de 88. Disponível em: <https://www.jusbrasil.com.br/topicos/10677474/artigo-129-da-constituicao-federal-de-1988>. Acessado em: 11 de jun. 2024.

[183]Conselho Nacional do Ministério Público - Início. Disponível em: <https://www.cnmp.mp.br/portal/>. Acessado em 11 de jun. 2024.

[184]Conselho Nacional do Ministério Público. O Ministério Público e o Controle Externo da Atividade Policial - Conselho Nacional do Ministério Público. Disponível em: <https://www.cnmp.mp.br/portal/publicacoes/12399-o-ministerio-publico-e-o-controle-externo-da-atividade-policial>. Acessado em 11 de jun. 2024.

externo da atividade policial[185]. De acordo com o novo texto, o controle externo da atividade policial não se limita às atribuições no Ministério Público na área criminal[186]. A abrangência e a especificidades relacionadas ao exercício das atribuições devem ser consideradas pelo Ministério Público na elaboração de seus planos, programas e projetos de atuação, o que reforça a tese de que o Ministério Público pode e deve monitorar a utilização dos bancos de dados das Polícias Judiciárias brasileiras.

Interessante fazer essa observação, porque a Segurança Pública, por ser um direito indisponível, merece o amparo e a fiscalização do Ministério Público. O Supremo Tribunal Federal, inclusive, no julgamento do RE 559646 PR[187], entendeu que o direito a segurança é prerrogativa constitucional indisponível, garantido mediante a aplicação de políticas públicas, impondo ao Estado a obrigação de criar condições que possibilitem o efetivo acesso a tal serviço.

No que diz respeito ao tema, o Supremo Tribunal Federal, nos Autos da ADPF 635[188], com o intuito de reduzir a letalidade praticada por policiais militares no Estado do Rio de Janeiro, obrigou o uso de câmeras corporais nas fardas dos policiais e nas viaturas, além do aviso antecipado das operações para autoridades das áreas de saúde e educação, para proteger escolas de tiroteios e garantir atendimento médico à população. Nesse sentido, um grupo de trabalho do Conselho Nacional de Justiça (CNJ), formado para acompanhar as ações para reduzir a letalidade policial no Rio de Janeiro, apresentou um relatório ao Ministro Fachin. A conclusão foi de que a única forma de fiscalizar a atuação policial e preservar os direitos humanos é promover a transparência dos dados das investigações, ocorrências e operações policiais, sob a supervisão do Ministério Público, que tem o dever constitucional de executar o controle externo da atividade policial[189].

---

[185]Conselho Nacional do Ministério Público. CNMP aprova nova regulamentação das atribuições do Ministério Público no controle externo da atividade policial. Disponível em: https://www.cnmp.mp.br/portal/todas-as-noticias/17146-cnmp-aprova-nova-regulamentacao-das-atribuicoes-do-ministeriopubliconocontroleexternodaatividadepolicial#:~:text=O%20Plen%C3%A1rio%20do%20Conselho%20Nacional,18%C2%AA%20Sess%C3%A3o%20Ordin%C3%A1ria%20de%202023.. Acesso em 29 de set. 2024.

[186]*Ibid.*

[187]STF, RE 559646 PR, Segunda Turma, Rel. Min. Ellen Gracie, J. 07.06.2011, DJe 24.06.2011..

[188]STF, ADPF 635, Tribunal Pleno, Rel. Min Edson Fachin, J. 26.06.2020, DJe 31.08.2020.

[189]Supremo Tribunal Federal. Entenda: STF julga ação sobre letalidade das operações policiais no Rio de Janeiro. Disponível em: https://noticias.stf.jus.br/postsnoticias/entenda-stf-julga-acao-sobre-letalidade-das-operacoes-policiais-no-rio-de-janeiro/. Acesso em 25 de nov. 2024.

Ainda sobre a Nota Técnica da Autoridade Nacional de Proteção de Dados, restou consignado a existência de interesse público no tratamento de dados pessoais disponibilizados pela Confederação Brasileira de Futebol ao mencionar que o tratamento de dados pessoais deve estar condicionado ao Artigo 4º §§ 1º ao 4º da LGPD[190], além de ter que ser capaz de demonstrar o interesse público e a vinculação do tratamento com as atribuições legais do órgão ou entidade que atuará como controlador.

A Nota Técnica da Autoridade Nacional de Proteção de Dados inovou, de forma positiva, no ordenamento jurídico brasileiro, tendo em vista que, ainda que de forma incipiente, jogou luz em um tema não regulamentado em nosso país. A partir do momento em que o tratamento de dados pessoais é utilizado pelos órgãos de segurança pública no âmbito dos estádios brasileiros para investigar e reprimir a prática de infrações penais, faz-se uso da Lei Geral de Proteção de Dados, ainda que exista previsão expressa de que a sua utilização não pode ser aplicada para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

Outro aspecto relevante do Relatório de Impacto à Proteção de Dados (RIPD) que consta na Nota Técnica foi o fato do Ministério da Justiça manifestar interesse em utilizar os dados pessoais com a finalidade de atividade de inteligência[191]. Aqui é necessário fazer uma distinção entre a inteligência policial e a investigação policial. Enquanto na investigação policial existe um protocolo a ser seguido, com uma série de procedimentos administrativos que devem respeitar um rito previsto no Processo Penal, na inteligência policial há uma espécie de coleta de dados que podem ser transformar em informações para serem utilizadas no âmbito da

[190]Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei. § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo. § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais. § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público.

[191]Autoridade Nacional de Proteção de Dados. Nota Técnica nº 175/2023/CGF/ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acessado em de junho. 2024.

investigação policial. Embora na inteligência policial exista maior flexibilidade na coleta de dados, isso não quer dizer que essa prática possa ser feita de forma ilícita, desrespeitando direitos e garantias fundamentais.

A atividade de inteligência, portanto, é mais abrangente que a investigação policial, porque coleta dados de diversas fontes que podem ser utilizadas para a investigação ou prevenção de um delito[192]. As informações utilizadas nas investigações policiais devem ser formalizadas através dos relatórios de inteligência, que auxiliam as autoridades policiais em processos decisórios. Apenas a título de exemplo, a Agência Brasileira de Inteligência é um órgão da Presidência da República destinado à produção de conhecimentos para subsidiar as decisões do Presidente da República e de seus Ministros. Além disso, a ABIN também é utilizada para incentivar e apoiar a elaboração doutrinária para a atividade de inteligência em nosso país.

A diferenciação entre investigação policial e inteligência policial fica muito evidente na Doutrina de Atividade de Inteligência da Agência Brasileira de Inteligência[193], que descreve a atividade de inteligência como sendo aquela capaz de produzir conhecimentos e realizar ações que visem a redução de vulnerabilidades e à neutralização de ameaças contra a segurança das pessoas e das instituições brasileiras. Além disso, a atividade de inteligência também visa proteger informações sobre pessoas, áreas, instalações e meios sensíveis, prevenindo, detectando, identificando, obstruindo e neutralizando ações de inteligências adversas. Para quem atua na prática de uma investigação policial, fica evidente a importância do trabalho da inteligência policial, conforme preceitua a própria Doutrina de Atividade de Inteligência da Abin:

> Em um mundo marcado por rápidas e radicais transformações globais no clima, na demografia, na matriz energética e nas tecnologias da Era Digital, o convívio político entre as diferentes sociedades ainda é largamente definido pela existência de Estados soberanos, conforme reconhecem a Convenção de Montevidéu sobre os Direitos e Obrigações dos Estados (1933) e a Carta das Nações Unidas (1945). Existem quase duas centenas de estados no mundo, muito desiguais entre si. Também existe uma densa rede formada por milhares

[192]Ministério Público do Estado do Maranhão. Distorções no entendimento do conceito de inteligência é tema de palestra na PGJ. Disponível em: https://www.mpma.mp.br/distorcoes-no-entendimento-do-conceito-de-inteligencia-e-tema-de-palestra-na-pgj/. Acesso em 02 de novembro de 2024.
[193]Agência Brasileira de Inteligência. Doutrina Nacional de Inteligência. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023>. Acessado em: 13 de ago. 2024.

> de organizações internacionais, além de uma enorme diversidade de empresas, grupos, redes e bilhões de indivíduos perseguindo diferentes objetivos no mundo. Quando existem conflitos de interesse e valor, nem sempre os mesmos são resolvidos pelas instituições internacionais formais e informais. Portanto, a preservação da soberania popular e nacional, entendida aqui como a capacidade coletiva de os brasileiros tomarem decisões e agirem nos termos da sua Constituição, é um imperativo que justifica e explica a necessidade de serviços de inteligência. Explica também porque, assim como as forças armadas e a diplomacia, existem serviços de inteligência em tantos países com ordenamentos constitucionais muito diversos no mundo contemporâneo.
> Nos termos do artigo 1º da Constituição de 1988, a República Federativa do Brasil é formada pela união indissolúvel dos estados e municípios e do Distrito Federal. Esta união constitui-se como um Estado Democrático de Direito e tem como fundamentos a soberania, a cidadania, a dignidade da pessoa humana, os valores sociais do trabalho e da livre iniciativa, bem como o pluralismo político. No artigo 3º da Constituição são definidos como objetivos fundamentais desta República a construção de uma sociedade livre, justa e solidária, a garantia do desenvolvimento nacional, a erradicação da pobreza e da marginalização, a redução das desigualdades sociais e regionais, bem como a promoção do bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação. No artigo 4º, são definidos os princípios que regem as relações internacionais do Brasil, a saber, a independência nacional, a prevalência de Direitos Humanos, a autodeterminação dos povos, a não-intervenção, a igualdade entre os Estados, a defesa da paz, a solução pacífica dos conflitos, o repúdio ao terrorismo e ao racismo, a cooperação entre os povos para o progresso da humanidade, a concessão de asilo político e a integração dos povos da América Latina.

Além da coleta de informações, a Doutrina de Atividade de Inteligência preceitua que as atividades de inteligência também devem agir em circunstâncias determinadas pela Lei. Isso passa pela obtenção de dados indisponíveis, pela proteção de conhecimentos, de informações e de dados sensíveis. Pessoas, áreas, instalações e meios que guardam ou veiculam informações devem ser observados, sempre com o propósito de prevenir, detectar, identificar, avaliar, obstruir ou neutralizar ações adversas de inteligência[194].

Para cumprir os seus objetivos de forma satisfatória, a atividade de inteligência, no entanto, está organizada em dois ramos: a inteligência e a contrainteligência. A inteligência é o ramo da atividade voltado para a produção e a difusão de conhecimentos relativos a fatos, eventos, situações ou fenômenos que ocorram dentro e fora do território nacional, de imediata ou potencial influência sobre o processo decisório e a ação governamental que indiquem oportunidades e ameaças aos objetivos fundamentais dos Estados[195].

---

[194] *Ibid.*
[195] *Ibid.*

A contrainteligência, por sua vez, tem como objetivo a produção de conhecimentos e a realização de ações voltadas para a proteção de dados, conhecimentos, infraestruturas críticas, como comunicações, transportes e tecnologias da informação, bem como outros ativos sensíveis e sigilosos de interesse do Estado e da sociedade. O trabalho da contrainteligência está focado na defesa contra ameaças de espionagem, sabotagem, vazamento de informações e o terrorismo. A contrainteligência, portanto, protege os conhecimentos produzidos pela atividade de inteligência[196].

Além disso, a contrainteligência também preserva dados e conhecimentos produzidos por entes nacionais, públicos ou privados, visando a prevenção, identificação e neutralização de ações promovidas por grupos de pessoas ou organizações vinculados ou não a governos que ameacem o desenvolvimento nacional e a segurança do Estado e da sociedade[197]. No mesmo contexto, existe a inteligência adversa, que é a atividade realizada por agente estatal ou não, com o emprego de ações especializadas, para obter acesso indevido ou não autorizado a dados e conhecimentos, áreas ou instalações, com o intuito de promover o interesse do seu patrocinador.

A contrainteligência, portanto, é o ramo da atividade que produz conhecimentos e desenvolve ações especializadas destinadas a prevenir, detectar, identificar, avaliar, obstruir e neutralizar atividades de inteligência adversa, incluindo ações que constituam ameaça a interesses da sociedade e do Estado, ao processo decisório, à salvaguarda de conhecimentos, informações e dados sensíveis, dos meios que os retenham ou que transitem, de seus detentores e de suas áreas de atuações[198].

As ações adversas são definidas como ações intencionais de um ou mais atores, patrocinada ou não, que se opõe à consecução dos interesses nacionais por meio da busca ilegítima por acesso a conhecimentos, informações e dados sensíveis, ameaçando a segurança das pessoas e instituições da República Federativa do Brasil. No ramo da inteligência, conforme preceitua a Doutrina de Atividade de Inteligência[199], são objeto de acompanhamento e análise as ações adversas perpetradas por organizações e indivíduos que empreguem técnicas

[196]Contrainteligência. Disponível em: <https://www.gov.br/abin/pt-br/assuntos/inteligencia-e-contrainteligencia/CI>. Acessado em: 13 de ago. 2024.
[197]*Ibid.*
[198]*Ibid.*
[199]*Ibid.*

especializadas (inteligência adversa), tais como recrutamento, entrada, dissimulação, desinformação e propaganda, entre outras.

Percebe-se, portanto, que os termos "inteligência" e "investigação" não podem ser confundidos, tendo em vista que atividade de inteligência policial e atividade de investigação policial serem termos distintos. A investigação policial é a atividade exercida pelas polícias judiciárias, para obter provas que visem identificar determinado autor de um já praticado ou em andamento. A inteligência policial, por outro lado, é uma atividade acessória e de natureza consultiva, que visa produzir e armazenar conhecimento, com o intuito de prevenir delitos que ainda não ocorreram e de auxiliar na identificação de autores de crimes já praticados ou que estejam em andamento. Diferentemente da investigação, a inteligência não tem como objetivo a produção de prova, prevista em nosso Código de Processo Penal.

Ademar Borges, porém, faz um alerta sobre o tratamento de dados pessoais que envolvam a união de órgãos de persecução penal. Para o Autor, no âmbito criminal a proteção de dados pessoais resulta na proibição da fusão de órgãos da segurança pública, tendo em vista que essa prática teria como resultado a extinção de uma linha limítrofe entre as atividades de inteligência e repressão criminal, o que ocasionaria uma eventual fragilidade dos direitos fundamentais e ampliaria o acesso irrestrito à informação que os órgãos investigativos possuem. Alega, ainda, que "Com efeito, a documentação de atividade de inteligência financeira possibilita ao imputado conhecer como as suas informações pessoais sigilosas foram obtidas, tratadas e disseminadas pela unidade de inteligência financeira"[200].

Outro aspecto que deve ser destacado é que o controle externo na investigação policial é exercido pelo Ministério Público, conforme previsto no Artigo 129, Inciso VII da Constituição da República Federativa do Brasil[201]. Já o controle externo da atividade de inteligência é exercido pela Comissão de Controle das Atividades de Inteligência (CCAI), composto por 06 (seis) integrantes, sendo 03 (três) deputados federais e 03 (três) senadores, além do Presidente

[200]BORGES, Ademar. O relatório de inteligência financeira como meio de obtenção de prova no processo penal. *Revista Brasileira de Ciências Criminais* vol. 176. ano 29. p. 69-105. São Paulo, fevereiro/2021.
[201]BRASIL. Constituição Federal. 1988. "Art. 129 São funções institucionais do Ministério Público: […] VII - exercer o controle externo da atividade policial, na forma da lei complementar mencionada no artigo anterior[...]". Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 22 ago. 2024.

da Comissão de Relações Exteriores e Defesa Nacional da Câmara dos Deputados e do Senado Federal, conforme o disposto no Parágrafo 1º Art. 6º da Lei 9.883/18[202].

Nina Nery alega que para se falar na concretização de uma sistema que esteja em consonância com o mandado de separação informacional de poderes, é essencial compreender que muito embora as atividades de inteligência, segurança pública e processo penal pareçam atuar de forma complementar, as suas razões de ser são distintas e, justamente por isso, suas instituições possuem prerrogativas e acesso a informações diferentes, de modo que a vedação à existência de bancos de dados comuns sobressai como um requisito essencial para impedir a instalação de uma entidade com poderes quase ilimitados[203].

Conforme preceitua Ademar Borges, a pretensão de estabelecer limites claros e tendencialmente intransponíveis entre essas duas atividades estatais tem como pano de fundo as ideias de proteção do direito fundamental à proteção de dados, de um lado, e de submissão integral dessas sensíveis funções estatais – cujo desempenho resulta em múltiplas restrições de direitos fundamentais – ao princípio da legalidade, de outro. As trocas de dados pessoais entre órgãos de inteligência e de repressão criminal estão submetidas, portanto, a um regime de rígida excepcionalidade e de estrita legalidade. Como os órgãos de inteligência têm acesso privilegiado a um amplo conjunto de dados pessoais dos cidadãos, caso viessem a desempenhar um papel de auxílio aos órgãos de repressão criminal, poderiam facilmente violar os limites constitucionais impostos à atividade persecutória do Estado, decorrentes de proteção da vida privada e do devido processo legal, sem que isso pudesse se sujeitar ao controle do Poder Judiciário[204].

Verifica-se, portanto, que os dois conceitos jamais poderão ser confundidos, embora sejam semelhantes. É preciso deixar claro que na atividade de inteligência há investigação e, eventualmente, na atividade de investigação pode haver atividade de inteligência. Tanto a

[202]BRASIL. Lei número 9.883/1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Art. 6º O controle e fiscalização externos da atividade de inteligência serão exercidos pelo Poder Legislativo na forma a ser estabelecida em ato do Congresso Nacional. § 1º Integrarão o órgão de controle externo da atividade de inteligência os líderes da maioria e da minoria na Câmara dos Deputados e no Senado Federal, assim como os Presidentes das Comissões de Relações Exteriores e Defesa Nacional da Câmara dos Deputados e do Senado Federal. Disponível em: https://planalto.gov.br/CCIVIL_03/LEIS/L9883.htm. Acesso em 22 de ago. 2024.
[203]NERY, Nina. O compartilhamento de dados financeiros no sistema antilavagem de dinheiro brasileiro. São Paulo: Thompson Reuters Brasil, 2024. p.96.
[204]BORGES, Ademar. O relatório de inteligência financeira como meio de obtenção de prova no processo penal. Revista Brasileira de Ciências Criminais, São Paulo, v. 176, p. 69-105, 2021, p. 71.

inteligência quanto a investigação são extremamente importantes para os órgãos de persecução penal, que precisam atuar com eficácia para prevenir e reprimir práticas criminosas cada vez mais sofisticadas. O principal foco deste trabalho não é aprofundar um estudo sobre os conceitos de inteligência e investigação, todavia é importante deixar o registro porque o acesso aos bancos de dados das polícias judiciárias brasileiras se dá através dessas duas práticas.

Apenas para termos a dimensão da importância e da necessidade de investigações reconhecidamente mais efetivas, à altura do crime organizado, mais de 4.500 (quatro mil e quinhentas pessoas) são alvos de tentativa de golpes financeiros no Brasil a cada meia hora[205], fora os casos de subnotificação, onde aproximadamente 30% dessas pessoas sequer procuram a polícia para registro de ocorrência policial. Os criminosos, portanto, estão cada vez mais habilidosos no aprimoramento da prática de crimes. De acordo com Oscar Vilhena, debelar o crime organizado constitui hoje o principal desafio da democracia brasileira. Para o autor, muitos são os fatores que levaram a essa expansão do crime, que vão da ausência ou presença arbitrária do Estado à inexistência de oportunidades econômicas. "Há, porém, uma dimensão institucional, que decorre de escolhas erradas no campo da segurança pública e da política criminal", conclui o autor[206].

O assunto nos leva a outro questionamento, que é o exercício das atividades de investigação e inteligência, quando praticadas por órgãos de persecução penal que exercem a função ostensiva, como é o caso das Polícias Militares. Nesse caso, as Polícias Militares podem exercer atividades de investigação e de inteligência? Para responder a pergunta, é preciso fazer, novamente, uma breve abordagem do Artigo 144 da nossa Constituição Federal.

Conforme consta no Artigo 144 da CRFB de 1988[207], a segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos: polícia federal; polícia rodoviária federal, polícia ferroviária federal, polícias civis, polícias militares e corpos de bombeiros militares, polícias penais federal, estaduais e distrital.

---

[205]País tem mais de 4,5 mil tentativas de golpe financeiro por hora. Disponível em: https://www.cnnbrasil.com.br/nacional/datafolha-pais-tem-mais-de-45-mil-tentativas-de-golpe-financeiro-por-hora/. Acesso em 22 de ago. 2024.
[206]VILHENA, Oscar. Combate ao crime organizado é questão de Estado. Folha de São Paulo. Disponível em: https://www1.folha.uol.com.br/colunas/oscarvilhenavieira/2024/11/combate-ao-crime-organizado-e-questao-de-estado.shtml. Acesso em 25 de nov. 2024.
[207]*Ibid.*

Embora diversos órgãos façam parte da segurança pública, o ponto que deve ser debatido é atribuição das policiais civis e das policias militares, já que, conforme será visto adiante, as instituições policiais possuem funções especificamente delimitadas pelo próprio texto constitucional. Enquanto às Polícias Civis cabem as funções de polícia judiciária e a apuração de infrações penais, exceto às militares, às Polícias Militares cabem a função de policiamento ostensivo e a preservação da ordem pública.

No dia a dia da atividade policial, o que se vê é um verdadeiro desvirtuamento de atribuições, já que Policiais Militares exercem atividades investigativas e Policiais Civis exercem atividades de policiamento ostensivo[208]. O fato é que em muitas ocasiões a inteligência exercida pelas Polícias Militares é questionada por juízes, promotores, delegados de polícia, pela mídia e até mesmo por uma parcela da sociedade.

Analisando o que diz a Constituição Federal e o Código Tributário Nacional[209], percebe-se que as Polícias Militares possuem a função de policiamento preventivo, mas também possuem autorização do Poder Público para a garantia da tranquilidade pública, do respeito à propriedade e aos direitos individuais e coletivos. Para que esses direitos sejam garantidos, é necessário, que, eventualmente, as Polícias Militares façam uso da inteligência ou contrainteligência.

Recentemente, o Supremo Tribunal Federal demonstrou uma espécie flexibilização das atribuições descritas acima. No ano de 2022, o STF entendeu que a Polícia Militar de Minas Gerais poderia lavrar termo circunstanciado[210], sob a alegação de que a função não é exclusiva da Polícia Judiciária, porque não se trata de atividade investigativa, mas sim de constatação da ocorrência de crimes de menor potencial ofensivo.

---

[208]Polícia Civil do Distrito Federal. PCDF deflagra Operação Delta no Paranoá. Polícia Civil do Distrito Federal. Disponível em: https://www.pcdf.df.gov.br/noticias/9250/pcdf-deflagra-operacao-delta-no-paranoa. Acesso em 26 de ago. 2024.

[209]BRASIL. Código Tributário Nacional. Artigo 78: Considera-se poder de polícia a atividade da Administração Pública que, limitando ou disciplinando direito, interesse ou liberdade, regula a prática de ato ou a abstenção de fato, em razão de interesse público concernente à segurança, à higiene, à ordem, aos costumes, à disciplina da produção e do mercado, ao exercício de atividades econômicas dependentes de concessão ou autorização do Poder Público, à tranquilidade pública ou ao respeito à propriedade e aos direitos individuais ou coletivos. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l5172compilado.htm. Acesso em 26 de ago. 2024.

[210]STF, ADI 3807, Tribunal Pleno, Rel. Min. Carmén Lúcia, J. 29.06.2020, DJe 13.08.2020.

Na ocasião, o Plenário do Supremo Tribunal Federal considerou constitucional dispositivo de lei do Estado de Minas Gerais que confere à Polícia Militar a possibilidade de lavrar termo circunstanciado, instrumento previsto para casos de crimes de menor potencial ofensivo em situações de flagrante. A Associação dos Delegados de Polícia do Brasil (Adepol), que na ocasião havia sido autora da ação, sustentava que a Lei Estadual número 22.250/2016 tratou de matéria reservada à União e que a competência para a instauração do procedimento do termo circunstanciado seria exclusiva da Polícia Federal e das Polícias Civis dos Estados e do Distrito Federal.

O Relator, Ministro Edson Fachin, entendeu que a lei de Minas Gerais foi produzida a partir da competência concorrente dos Estados para legislar sobre a criação, o funcionamento e o processo do juizado especial de pequenas causas e procedimentos em matéria processual (Artigo 24, Incisos X e XI da Constituição da República Federativa do Brasil). Fachin destacou a diferença entre o termo circunstanciado, lavrado pela autoridade policial que tomar conhecimento da ocorrência, e o inquérito policial, que é da competência do delegado de polícia. "O inquérito é o instrumento para viabilizar a investigação criminal, que consiste na atividade de apuração das infrações penais. Já o termo circunstanciado não tem função investigativa, ele se limita a constatar a ocorrência"[211].

Ainda de acordo com o Ministro Edson Fachin, o Artigo 69 da Lei dos Juizados Especiais (Lei número 9.099/1995)[212], ao dispor que a autoridade policial que tomar conhecimento da ocorrência lavrará o termo circunstanciado e o encaminhará imediatamente ao juizado, não se refere exclusivamente à polícia judiciária, mas às demais autoridades legalmente reconhecidas. Ele ressaltou que não há, nem na Constituição Federal nem no ordenamento jurídico federal, previsão normativa que expressamente retire dos Estados a competência para disciplinar a atribuição de lavratura do termo circunstanciado.

O mesmo Plenário do Supremo Tribunal Federal[213], desta vez no ano de 2023, entendeu que a Polícia Rodoviária Federal pode lavar termo circunstanciado ocorrência, ao entender que

---

[211] *Ibid.*
[212] BRASIL. Lei número 9.099/1995. Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9099.htm. Acesso em 26 de ago. 2024.
[213] BRASIL. Supremo Tribunal Federal. PRF pode lavrar termo circunstanciado de ocorrência, decide STF. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=503028&ori=1. Acesso em 26 de ago. 2024.

por não ser procedimento investigativo, prerrogativa não é exclusiva das Polícias Judiciárias. O Supremo Tribunal Federal validou Decreto da Presidência da República que deu competência à Polícia Rodoviária Federal (PRF) para lavrar termo circunstanciado de ocorrência de crime federal de menor potencial ofensivo.

O Judiciário, portanto, está atento à evolução das práticas criminosas, o que faz com que seja necessária a união das forças de segurança no combate ao crime organizado. Ainda no ano de 2022, a Comissão de Segurança Pública da Câmara dos Deputados[214] aprovou Projeto de Lei que regulamenta as ações de inteligência pela Polícia Rodoviária Federal, pelas Polícias Militares e pelas Polícias Penais. O texto prevê que o resultado das ações será elemento de prova e poderá subsidiar medidas judiciais.

Para Caroline Vivas Gonçalves, a atual sociedade de risco, marcada pelo crescimento da criminalidade transacional, insegurança e terrorismo, revelou a insuficiência do modelo tradicional de policiamento reativo e obrigou o surgimento de um novo paradigma quanto à forma de atuação em relação aos crimes, ganhando como uma grande aliada no combate à criminalidade, a tecnologia e a doutrina de inteligência policial[215].

De acordo com os autores da Proposta, os Deputados Subtenente Gonzaga e Capitão Derrite[216], pelas regras atuais, as investigações são de competência das polícias judiciárias (Policia Federal e Polícias Civis), ficando as Polícias Militares com a responsabilidade do policiamento ostensivo e da preservação da ordem pública. Assim, o conhecimento produzido pelas polícias ostensiva, ainda que suficientes para a elucidação de crimes, com definição de autoria e materialidade, é descartado, porque não pode ser juntado aos processos[217].

O Superior Tribunal de Justiça se manifestou nesse sentido no julgamento do AgRg no HC 734423 GO. Foi definido que a informação policial originada de informações obtidas por inteligência, que no caso em questão envolveu a Polícia Militar, e mediante informações prévias

[214]BRASIL. Câmara dos Deputados. Comissão aprova proposta que regulamenta ações de inteligência das polícias ostensivas. Disponível em: https://www.camara.leg.br/noticias/918138-COMISSAO-APROVA-PROPOSTA-QUE-REGULAMENTA-ACOES-DE-INTELIGENCIA-DAS-POLICIAS-OSTENSIVAS. Acesso em 27 de ago. 2024.
[215]GONÇALVES, Caroline Vivas. O DIREITO À EXPLICAÇÃO NA DIRETIVA (EU) 2016/680 E SUAS PERSPECTIVAS PARA O CENÁRIO BRASILEIRO. 2021. 100 f. Dissertação (Mestrado). Faculdade de Direito da Universidade Nova de Lisboa.
[216]*Ibid.*
[217]*Ibid.*

que redundam em acesso à residência do acusado, configura exercício regular da atividade investigativa promovida pelas autoridades policiais[218].

Não é difícil perceber que os Tribunais Superiores caminham na direção do compartilhamento de dados e informações de inteligência policial, que deve ser exercido por todos os órgãos da Segurança Pública. Conforme já foi mencionado alhures, cada vez mais se percebe o crescente uso de diversos tipos de ferramentas para a prática dos mais variados delitos. Isso não significa dizer que as atividades preventivas são absolutamente incompatíveis com o Estado Democrático de Direito. Como já mencionado, cabe aos órgãos de inteligência exercerem suas funções em caráter prospectivo, mirando acontecimentos futuros, sem que para exercerem essas atividades, essas agências devem ter acesso privilegiado a um amplo conjunto de dados pessoais[219].

Feitas as observações necessárias sobre a importância da atividade de inteligência, é preciso retornar à Nota Técnica da Autoridade Nacional de Proteção de Dados, para verificar com mais precisão o Relatório de Impacto à Proteção de Dados (RIPD)[220]. A ANPD fez questão de frisar que o devido processo legal deve ser respeitado no Acordo de Cooperação entre o Ministério da Justiça e Segurança Pública (MJSP) e a Confederação Brasileira de Futebol (CBF).

Aqui é preciso ressaltar que o devido processo legal deve ser analisado sob duas vertentes. A primeira diz respeito ao rito mínimo necessário para a formalização do compartilhamento de dados pessoais. A segunda versa sobre os cuidados que o Ministério da Justiça deve ter para impedir o uso indevido e o desvio de finalidade, que pode resultar em abuso e prejuízo ao direito fundamental à proteção de dados.

A observação feita pela ANPD faz todo sentido, porque o Supremo Tribunal Federal, no julgamento da ADI 6387[221], analisou o compartilhamento de dados por empresas prestadoras de serviço telefônico fixo e móvel com o Instituto Brasileiro de Geografia e Estatística (IBGE)

---

[218]STJ, AgRg no HC 734423 GO, Quinta Turma, Rel. Min. João Otávio de Noronha, J. 24.05.2022, DJe 26.05.2022.
[219]NERY, Nina. O compartilhamento de dados financeiros no sistema antilavagem de dinheiro brasileiro. São Paulo: Thompson Reuters Brasil, 2024. p.97.
[220]*Ibid.*
[221]STF, ADI 6387 DF, Tribunal Pleno, Rel. Min. Rosa Weber, J. 07.05.2020, DJe 12.11.2020.

e destacou a importância do devido processo legal, ao concluir que este não havia sido atendido pela MP número 954/2020[222].

Quando se trata de compartilhamento de dados entre órgãos públicos ou a partir de órgãos públicos, a Autoridade Nacional de Proteção de Dados tem reiteradamente se manifestado no sentido de que quando se tratar de dados pessoais, o compartilhamento deve ser precedido de análise técnica e jurídica, além de emissão de decisão administrativa motivada pela autoridade competente, deve constar a motivação e as condições a serem observadas no caso, em conformidade com o que preceitua a Lei Geral de Proteção de Dados[223].

Depreende-se, portanto, que com base na Nota Técnica, a utilização dos dados pessoais pela Polícia Civil do Distrito Federal, com o fim de instruir determinada investigação, deve respeitar o devido processo legal, ter os devidos cuidados para impedir o uso indevido e o desvio de finalidade e deve ser precedido de análise técnica e jurídica, além da emissão de decisão administrativa motivada pela autoridade competente, onde deve constar a motivação e as condições a serem observadas.

No caso específico da frequência do tratamento e do tempo de retenção dos dados pessoais, o Ministério da Justiça informou no Relatório de Impacto à Proteção de Dados (RIPD)[224] que os dados serão recebidos e tratados a cada partida de futebol, quando a entidade desportiva com mando de campo aderir ao acordo de cooperação. Os dados tratados serão encaminhados à autoridade policial militar e à autoridade de polícia judiciária indicados na Portaria, que estabelecerão uma comissão específica para a operacionalização de solução tecnológica de interesse da segurança pública e em competições desportivas no respectivo Estado.

A Nota Técnica não menciona se os dados encaminhados para as autoridades militares e de polícia judiciária são os dados de todos os cidadãos que frequentarão o evento esportivo

---

[222]BRASIL. Congresso Nacional. Medida Provisória número 954/2020. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141619#:~:text=Estabelece%20que%20os%20dados%20compartilhados,no%20%C3%A2mbito%20de%20pesquisas%20domiciliares. Acesso em 27 de ago. 2024.

[223]Autoridade Nacional de Proteção de Dados. Guia Orientativo. Tratamento de Dados Pessoais pelo Poder Público. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 02 de nov. 2024.

[224]*Ibid.*

ou se são, tão somente, os dados das pessoas que tiverem algum tipo de problema envolvendo falha na validação biométrica, suspeitos de uso de documento falso ou qualquer outro tipo de ocorrência.

A Autoridade Nacional de Proteção de Dados entendeu que ainda que o propósito seja a preservação da ordem pública e da incolumidade das pessoas e do patrimônio com o objetivo de garantir o bem-estar e a segurança da sociedade diante de situações que possam ameaçá-la ou causar dano, não se pode conceber o acúmulo e a produção de conhecimento despropositado, sob a justificativa de proteger a sociedade de seus próprios cidadãos[225]. Ficou registrado que o Ministério da Justiça deveria ajustar o Relatório de Impacto à Proteção de Dados (RIPD), para deixar claro que somente serão repassados os dados de sujeitos de interesse, que são aqueles que acusem problema de falha na validação biométrica ou aqueles suspeitos de usar documentos falsos ou que estejam envolvidos em qualquer outro tipo de ocorrência.

Se aplicarmos o mesmo parâmetro utilizado acima pela Autoridade Nacional de Proteção de Dados ao armazenamento de dados pessoais feitos pela Polícia Civil do Distrito Federal, o trabalho de investigação seria prejudicado, porque segundo a ANPD o encaminhamento dos dados pessoais só poderia ser feito paras polícias nos casos especificados acima (falha em validação biométrica, suspeitos de uso de documento falso ou qualquer outro tipo de ocorrência). Seguindo essa linha de raciocínio, os dados armazenados em ocorrências policiais de natureza administrativa, como é o caso de extravio de documentos ou acidente de trânsito sem vítima, não poderiam ser utilizados. Isso significar dizer que só podem ser usados dados daqueles que praticam ou já praticaram delitos?

O mais apropriado nessa Nota Técnica da ANPD é que diante do crescente aumento do crime cada vez mais organizado, tanto as Polícias Militares quando as Polícias Civis tivessem acesso pleno aos dados dos torcedores que frequentam o Estado, o que não significa dizer que a motivação para o acesso aos dados deva ser deixada de lado. Além disso, é preciso reforçar que a má utilização dos dados, sem o devido processo legal ou a motivação, pode implicar em sanções administrativas e criminais, pela prática de desvio de conduta.

[225] *Ibid.*

Sobre os prazos de armazenamento dos dados, deve ser observada a tabela de temporalidade do Ministério da Justiça[226], onde consta que os dados oriundos de produção de conhecimento e de inteligência e contrainteligência, serão guardados de forma permanente. É importante frisar que no acordo específico do Ministério da Justiça com a Confederação Brasileira de Futebol, não deve ser aplicada a tabela de temporalidade, conforme observação feita no Relatório de Impacto à Proteção de Dados Pessoais da ANPD[227].

Ainda de acordo com o Ministério da Justiça, que segue a Doutrina Nacional de Inteligência[228], o armazenamento de dados tem como finalidade subsidiar a produção do conhecimento de inteligência no âmbito da Coordenação Geral de Inteligência (CGINT/DIOPI/SENASP). A mesma Doutrina Nacional de Inteligência também estabelece que os conhecimentos produzidos pelas Agências de Inteligências (AIs) pertencem ao Subsistema de Inteligência de Segurança Pública (SISP) e devem ser formalizados em Documentos de Inteligência e disponibilizados ao tomador de decisão a ser assessorado, sem deixar de observar os princípios do sigilo, da oportunidade e da necessidade.

A temporalidade utilizada pelo Ministério da Justiça e Segurança Pública tem como base a Lei número 8.159/1991[229], que dispõe sobre a política nacional e arquivos públicos e privados. Consta na referida legislação que é dever do Poder Público a gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação.

O Poder Público, portanto, armazena dados pessoais das pessoas há anos, o que não pode ser visto como irregularidade. Os tempos mudaram, a sociedade evoluiu, a tecnologia se tornou uma realidade presente e em contante mutação, o que fez com que novas legislações, como a Lei Geral de Proteção de Dados, surgissem. O fato é que nos dias de hoje, a proteção de dados pessoais se tornou um Direito Fundamental Previsto em nossa Constituição Federal,

---

[226]Ministério da Justiça e Segurança Pública. CÓDIGO DE CLASSIFICAÇÃO E TABELA DE TEMPORALIDADE E DESTINAÇÃO DE DOCUMENTOS DE ARQUIVO RELATIVOS ÀS ATIVIDADES-FIM DO MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. Disponível em: https://www.gov.br/arquivonacional/pt-br/arquivos%20pdf/codigos-de-classificacao/CCD_TTD_MJSP.pdf. Acesso em 28 de ago. 2024.

[227]*Ibid.*

[228]*Ibid.*

[229]BRASIL. Lei número 8.159/1991 – Política Nacional de Arquivos Públicos e Privados. Disponível em: https://www.planalto.gov.br/cciviL_03/////LEIS/L8159.htm. Acesso em 28 de ago. 2024.

o que faz com que o armazenamento de dados, que sempre existiu, seja devidamente regulamentado, principalmente na área penal.

A atuação da Autoridade Nacional de Proteção de Dados na Nota Técnica em questão pode ser o início da regulamentação da proteção de dados pessoais no âmbito do Direito Penal. O mais apropriado seria que ANPD fosse obrigada a atuar em situações como essa, situação em que o Ministério da Justiça pretendia utilizar dados pessoais de torcedores em estádios, sob a alegação de prevenir a prática de delitos ou de prender procurados pela justiça.

O mais provável é que enquanto não houver legislação que regulamente a proteção de dados pessoais para fins criminais, a ANPD deve atuar no mesmo sentido da Nota Técnica analisada. A ANPD demonstrou ser um órgão independente, de fato, quando entendeu ser razoável que a utilização dos dados pessoais coletados pela CBF nos estádios deve estar sujeita à atualidade do momento, ou seja, o Ministério da Justiça recebe as informações, analisa se o torcedor está com mandado de prisão em seu desfavor ou se está praticando algum delito e logo em seguida descarta os dados. Em outras palavras, o Ministério da Justiça não poderia criar um banco de dados com essas informações, para utilizá-las futuramente.

Segundo a Autoridade Nacional de Proteção de Dados[230], não haveria razões para que a manutenção das informações ficasse armazenada pelo Ministério da Justiça além do tempo necessário para garantir a segurança do evento esportivo. Reforçou, ainda, que o acúmulo indiscriminado de dados pessoais pode colocar em risco a privacidade do titular de dados e violar direitos fundamentais e os ditames da Lei Geral de Proteção de Dados, em razão do risco de se criar um estado de vigilância indiscriminada.

Para a ANPD[231], sobre o tempo de retenção pelo Ministério da Justiça, os dados pessoais serão excluídos após o encerramento do evento esportivo, não havendo compartilhamento em tempo real e com imagem dos dados e as informações relativas aos registros das passagens e movimentações de veículos registrados pelas câmeras do estacionamento do estádio após o encerramento do evento esportivo.

[230] *Ibid.*
[231] *Ibid.*

Em outro ponto, a Autoridade Nacional de Proteção de Dados[232] também menciona que não há o menor sentido em submeter os dados coletados de cidadãos em pleno exercício de seus direitos civis, que não deram causa para serem objeto de interesse das atividades de segurança pública ao tratamento que convencional, o que levaria à retenção por 50 anos ou mais, sob o risco de instaurar-se o vigilantismo exacerbado por parte do Estado.

A questão que gerou dúvidas no caso em tela é se o Ministério da Justiça deveria ter o direito de armazenar os dados pessoais, para poder utilizá-los sempre que necessário, desde que cumpridos os requisitos já mencionados acima, que são os princípios do sigilo, da oportunidade e da necessidade, com a devida implementação de política pública para monitorar a utilização desses dados.

No contexto do Plano de Ação da Nota Técnica[233], a ANPD sugeriu que no ato da venda dos ingressos pela CBF, não haveria a necessidade de coleta do telefone do comprador para repassar ao Ministério da Justiça, sob a alegação de que diversas outras informações já estavam sendo coletadas, tais como registro facial, catraca na entrada do estádio e assento vinculado ao bilhete. Para a Autoridade Nacional de Proteção de Dados, a coleta do número do telefone é desnecessária e excessiva, levando em consideração a utilidade do dado no contexto da atualidade, tendo em vista que os dados serão utilizados durante o tempo necessário para garantir a segurança do evento esportivo.

Outra questão que merece atenção na Nota Técnica é a do consentimento para o tratamento de dados pessoais no âmbito da parceria firmada entre o Ministério da Justiça e a CBF. Conforme consta na Lei Geral de Proteção de Dados[234], o tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento do consentimento pelo titular. O consentimento em questão deve ser escrito ou por outro meio que demonstre a manifestação de vontade do titular. Caberá ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto com o que preceitua a lei.

---

[232] *Ibid.*
[233] *Ibid.*
[234] BRASIL. Lei Geral de Proteção de Dados - LGPD. Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 02 set. 2024.

Outro ponto fundamental é a vedação do tratamento de dados pessoais mediante vício de consentimento, que deve se referir a finalidades determinadas. As autorizações genéricas para o tratamento de dados pessoas serão nulas e o consentimento pode ser revogado a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado, enquanto não houver requerimento de eliminação.

Aqui é preciso analisar vários aspectos que podem ser fundamentais para o resultado esperado com o acordo de cooperação. Conforme já mencionado em diversos pontos deste trabalho, há, nos dias de hoje, uma omissão legislativa para o tratamento de dados pessoais na espera penal, tanto na prevenção quanto na investigação de crimes. A ANPD, com base na Lei Geral de Proteção de Dados, entendeu que é difícil conceber que um consentimento se dê de forma livre, principalmente em função da assimetria entre a força do Estado e a dos cidadãos[235].

O Ministério da Justiça, por sua vez, no Relatório de Impacto à Proteção de Dados (RIPD), sustentou que o tratamento de dados pessoais ocorrerá com ou até mesmo sem o consentimento prévio do titular, considerando que a simples confirmação da existência de tratamento de dados pessoais poderá comprometer a segurança pública, a defesa nacional, a segurança do Estado ou atividades de investigação e repressão de infrações penais. O MJ alegou que é necessário aguardar legislação específica, antes que sejam estabelecidos procedimentos para informar ao titular quais dados estão sendo tratados[236].

A ANPD entendeu que negar ciência ao titular impede que ele possa agir em defesa da sua privacidade ou da inviolabilidade de sua intimidade, honra e imagem[237]. O fato é que a Autoridade Nacional de Proteção de Dados está exercendo o seu papel, que é o de ser a guardiã da proteção de dados no Brasil e a responsável por fiscalizar o cumprimento da Lei Geral de Proteção de Dados.

A atividade de investigação de um delito é um ato complexo, que envolve uma série de procedimentos que se não forem feitos de forma correta, corre-se o risco de preservar o dado pessoal do autor, mantendo a sua impunidade e gerando, por consequência, restrições aos

[235]Autoridade Nacional de Proteção de Dados. Nota Técnica nº 175/2023/CGF/ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acessado em de junho. 2024.
[236]*Ibid.*
[237]*Ibid.*

direitos fundamentais das vítimas. Deve ser vista com cautela a tese de que a negativa de ciência ao titular dos dados pessoais impediria que ele possa agir em defesa de sua privacidade ou da inviolabilidade de sua intimidade, honra e imagem. De fato, o Ministério da Justiça acumularia uma quantidade de dados relevante, que talvez sequer fosse utilizada. Isso não quer dizer, porém, que os dados possam ser utilizados para fins que não sejam os estabelecidos pelo acordo com a CBF. Além disso, o processo penal proporciona o momento adequado para que o titular dos dados pessoais possa se defender e questionar o modo como a prova foi auferida.

Sobre o compartilhamento de dados pessoais com integrantes do Sistema Único de Segurança Pública – SUSP, a ANPD também entendeu que será preciso comprovar a necessidade do tratamento dos dados pessoais, precedido pela demonstração de que há, de fato, um devido processo legal e respeito aos princípios e direitos dos titulares, conforme previsão da Lei Geral de Proteção de Dados[238]. A Autoridade Nacional de Proteção de Dados também recomendou que o compartilhamento seja precedido das análises técnicas e jurídicas, além de emissão de decisão administrativa motivada pela autoridade competente, da qual constem a justificativa e as condições a serem observadas no caso concreto, conforme dispõe a LGPD[239].

Apesar de não existir legislação que regulamente a proteção de dados no Brasil, a Autoridade Nacional de Proteção de Dados, em sua primeira Nota Técnica sobre o assunto, recomendou que alguns dispositivos da Lei Geral de Proteção de Dados sejam utilizados, até que exista lei específica para tratar sobre o tema[240]. Apesar da iniciativa da ANPD ser digna de mérito, já que é muito difícil abordar um tema tão complexo pela primeira vez, é preciso levar em consideração que o tratamento de dados pessoais para fins penais necessita de um olhar diferente dos demais dados pessoais para fins não penais.

No que diz respeito ao tratamento de dados pessoais pela entidade de prática desportiva, a Autoridade Nacional de Proteção de Dados entendeu, de forma acertada, que a CBF não poderia realizar o tratamento de dados pessoais quando estiver atuando como controladora, não

[238] *Ibid.*
[239] *Ibid.*
[240] Autoridade Nacional de Proteção de Dados. Nota Técnica nº 175/2023/CGF/ANPD. 5.1. Insta salientar que, embora haja exceção prevista na legislação para o tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, III, da Lei nº 13.709/2018 - LGPD), tal tratamento deve observar o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD, de acordo com o disposto no §1º do artigo 4º da mesma lei. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acessado em de junho. 2024..

havendo, inclusive, possibilidade de que os dados sejam compartilhados. Tanto a CBF quanto a empresa que faz a comercialização dos ingressos, atuam apenas como operadoras. A própria Lei Geral de Proteção de Dados ressalva que os dados são de uso exclusivo das pessoas jurídicas de direito público, só podendo ser tratados por pessoas jurídicas de direito privado quando atuarem sob a tutela de pessoa jurídica de direito público.

Percebe-se uma atuação técnica e isenta da Autoridade Nacional de Proteção de Dados, quando foi ressaltado na Nota Técnica que se busca com atuação fiscalizatória uma típica atividade repressiva, como a atividade de monitoramento, orientação e prevenção, com o intuito de guiar o agente de tratamento à plena conformidade às obrigações previstas na Lei Geral de Proteção de Dados, para que o Ministério da Justiça e a Confederação Brasileira de Futebol atuem respeitando o devido processo legal, os princípios gerais de proteção de dados e os direitos dos titulares[241].

A mesma ANPD também regulamentou, através da resolução número 19/2024, a transferência internacional de dados[242], estabelecendo os procedimentos e as regras aplicáveis às operações de transferência internacional de dados, à luz da LGPD. A transferência internacional de dados ocorre no momento em que os dados pessoais são transferidos por um agente exportador que esteja no Brasil, para um agente importador localizado em outro país.

Embora exista uma exceção prevista na LGPD para o tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão penais, o tratamento deve observar o devido processo legal, os princípios já mencionados acima e os direitos do titular, também previstos na LGPD. A própria Lei Geral de Proteção de Dados atribuí à Autoridade Nacional de Proteção de Dados a competência para emitir opiniões técnicas ou recomendações referentes às exceções previstas[243].

---

[241]Autoridade Nacional de Proteção de Dados. Nota Técnica nº 175/2023/CGF/ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acessado em de junho. 2024.

[242]Autoridade Nacional de Proteção de Dados. Disponível em: ANPD aprova regulamento sobre transferências internacionais de dados. https://www.gov.br/anpd/pt-br/assuntos/noticias/resolucao-normatiza-transferencia-internacional-de-dados. Acesso em 03 de set. 2024.

[243]BRASIL. Lei número 13.709/2018. Lei Geral de Proteção de Dados. Art. 4º, § 3º § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 02 de nov. 2024.

Ficou evidente que durante a investigação de um delito, seja ele qual for, os princípios previstos na Lei Geral de Proteção de Dados não podem ser deixados de lado. A ausência de uma legislação penal para proteção de dados pessoais não pode servir de obstáculo para o pleno exercício dos órgãos de persecução penal. Por esse motivo, é possível que cada ação dependerá de uma regulamentação específica, com atuação pautada dentro dos limites da legalidade, respeitado o devido sigilo e o controle na utilização dos dados pessoais, para que os órgãos de persecução penal tenham condições de investigar crimes, utilizando dados pessoais dos seus próprios bancos de dados, sem a prática de excessos.

4 DIRETIVA 680/2016 (UE) E O TRATAMENTO DE DADOS PESSOAIS PELAS AUTORIDADES COMPETENTES PARA EFEITOS DE PREVENÇÃO, INVESTIGAÇÃO, DETECÇÃOE REPRESSÃO DE INFRAÇÕES PENAIS

A Diretiva 680/2016 (UE)[244] do Parlamento Europeu é extremamente importante para compreendermos o estudo do Anteprojeto Penal de Proteção de Dados Pessoais que tramita no Parlamento brasileiro. A Diretiva estabelece o tratamento de dados pessoais pelas autoridades competentes, para fins de prevenção, detecção ou repressão de infrações penais ou execução de sanções penais. Além disso, a Diretiva 680/2016 também protege os dados pessoais de testemunhas, vítimas ou suspeitos que estejam vinculados à prática de algum delito.

A norma em questão foi promulgada no mesmo dia do GDPR, o que faz com que ela tenha uma certa similaridade com o regulamento europeu. Diferentemente do que ocorreu na Europa, aqui no Brasil a LGPD entrou em vigor em 2018, porém, conforme já mencionado alhures, excluiu, de forma explícita, a sua aplicação nos casos de persecução penal, ou seja, não foi promulgada, no mesmo dia, como ocorreu na Europa, uma Lei Geral Penal de Proteção de Dados.

Tanto a Diretiva quanto o RGPD obrigam às autoridades o registro de todos os atos de tratamento, normas de segurança, notificação a uma autoridade nacional e a comunicação ao titular em caso de violação de dados, previsão de um encarregado de dados e normas sobre a transferência internacional de dados. A legislação também estabelece que o tratamento de dados

[244]DIRETIVA (UE) 2016/ 680 DO PARLAMENTO EUROPEU. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=HU. Acessado em 08 de abr. 2024.

para a prevenção, investigação ou repressão de investigações penais é necessário para se obter uma melhor compreensão das atividades criminais[245].

Vários são os aspectos relevantes desta norma que podem ser utilizados em nossa futura Lei Gera Penal de Proteção de Dados. Apenas a título de exemplo, consta na Diretiva que os dados não sejam excessivos nem conservados durante mais tempo do que o necessário para os efeitos para os quais são tratados. Também consta que os dados pessoais só deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios.

Aqui é preciso fazer uma observação, porque os dados armazenados pelas policiais judiciárias brasileiras são permanentes, ou seja, estarão sempre à disposição dos seus integrantes para que, a qualquer tempo, os utilize em caso de suspeita da prática de crimes, ou até mesmo para prevenir a prática de eventual delito. Indo de encontro ao que prevê a Diretiva, os dados não são desconsiderados após a sua utilização.

Importante fazer essa observação, porque na Diretiva consta que o responsável pelo tratamento dos dados fixe prazo para o apagamento ou revisão periódica. Também impõe que os dados pessoais deverão ser tratados de forma que garanta um nível adequado de segurança e confidencialidade, para que seja evitado o acesso ou a utilização desses dados e do equipamento utilizado para o seu tratamento por parte de pessoas não autorizadas, e que tenha em conta as técnicas e tecnologias mais avançadas os custos da sua aplicação em função dos riscos e a natureza dos dados pessoais que serão protegidos.

4.1 Concepção do Tratamento de Dados Pessoais como Direito Fundamental

Conforme já foi mencionado em alguns pontos desse trabalho, o Congresso Nacional promulgou, no dia 10 de fevereiro de 2022, a Emenda Constitucional número 115 de 2022, oriunda da PEC número 17 de 2019[246]. A Emenda Constitucional em questão alterou a Constituição Federal, para incluir a proteção de dados pessoais entre os direitos e garantias

---

[245] *Ibid.*

[246] BRASIL. Câmara dos Deputados. PEC 17/2019. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757#:~:text=PEC%2017%2F2019%20Inteiro%20teor,Proposta%20de%20Emenda%20%C3%A0%20Constitui%C3%A7%C3%A3o&text=Altera%20a%20Constitui%C3%A7%C3%A3o%20Federal%20para,e%20tratamento%20de%20dados%20pessoais. Acesso em 03 de nov. 2024.

fundamentais, além de fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

A proteção de dados pessoais, agora reconhecida de forma expressa como direito fundamental, fortalece os mecanismos de proteção dos direitos da personalidade. Não é a previsão de um texto na Constituição que garante a efetividade de um direito, mas os mecanismos capazes de protege-lo. Nas palavras de Marcelo Novelino, "as garantias não são um fim em si mesmo, mas um meio a serviço de um direito substancial. São instrumentos criados para assegurar a proteção e efetividade dos direitos fundamentais"[247].

Conforme será possível aprofundar adiante, podemos falar aqui sobre a dimensão objetiva desse direito fundamental. A dimensão objetiva independe de um titular específico para que determinado direito fundamental seja reivindicado ou protegido. Significa dizer que sob o espectro da dimensão objetiva, os direitos fundamentais funcionam como princípios estruturantes que orientam a ordem jurídica e a atuação do Estado de forma geral[248]. Martins sustenta que[249]:

> A função ou dimensão jurídico-objetiva dos direitos fundamentais encerra outras funções, algumas também já tornadas "clássicas", como as garantias de organização. Como "dimensão objetiva", define-se a dimensão dos direitos fundamentais, cuja percepção independe de seus titulares, vale dizer, dos sujeitos de direitos. Os direitos fundamentais seriam, quando observados por essa dimensão objetiva, critérios de controle da ação estatal, que devem ser observados independentemente de possíveis intervenções e violações concretas. Não é, destarte, equivocado afirmar que tenha, em geral, um caráter preventivo. A escolha do termo "dimensão" por Horst Dreier foi, nesse sentido, bem consciente, pois a dimensão objetiva não afasta, muito menos reduz a importância da dimensão subjetiva. A terminologia da função, ao contrário, dá margem a uma possível hierarquização que não condiz com o conceito clássico (liberal) de direito fundamental.

A perspectiva da dimensão objetiva força o Estado a atuar de forma vigilante e ativa na proteção dos direitos fundamentais, gerando uma constitucionalização do Direito e uma eficácia dos direitos fundamentais entre os particulares[250]. No contexto da dimensão objetiva, surge o

---

[247]NOVELINO, Marcelo. Curso de Direito Constitucional. Salvador: JusPodivm. 2017, p. 284.
[248]BONAVIDES, Paulo. Curso de Direito Constitucional. 11ª ed. São Paulo: Malheiros, 2001.
[249]MARTINS, Leonardo. Cinquenta Anos de Jurisprudência do Tribunal Constitucional Alemão. Montevidéu: Konrad Adenauer-Stilfung, 2005. (Organização e introdução, coletânea original de J. Schawabe).
[250]NASCIMENTO, Filippe. A DIMENSÃO OBJETIVA DOS DIREITOS FUNDAMENTAIS: É POSSÍVEL RECONHECER OS DIREITOS FUNDAMENTAIS COMO UMA ORDEM OBJETIVA DE VALORES?

que a doutrina chama de “jurisprudência de valores”, que de acordo com o Tribunal Constitucional Alemão, considera os valores como uma ordem hierárquica utilizável como parâmetro para o controle de constitucionalidade[251]. Segundo a “jurisprudência de valores”, o valor é o elemento de maior relevância no Direito, pois o fato é o suporte dos valores e a norma é um juízo de valor explícito no princípio e implícito na regra.

A dimensão objetiva, portanto, faz com que os direitos fundamentais deixem de ser pensados sob a ótica dos indivíduos, para ocuparem espaços de conformação coletiva, protegendo valores e bens jurídicos que não aderem ao titular no sentido da subjetividade clássica[252]. A compreensão e o reconhecimento da dimensão objetiva representam um avanço na operatividade dos direitos fundamentais, na medida em que as existências não representem apenas a exigência de que o Estado não viole determinadas posições jurídicas, mas também que ele se obrigue a perseguir a realização de valores objetivos que estão dispostos e determinados, com grau de vinculatividade, no corpo constitucional[253]. Portanto, a dimensão objetiva do direito fundamental à proteção de dados é a ideia de que o dever de proteção é prevalente para a efetividade desse direito[254].

A inclusão do direito fundamental à proteção de dados em nossa constituição federal foi um passo importante para o ordenamento jurídico brasileiro. Apesar do direito fundamental à proteção de dados já ter reconhecimento da doutrina e da jurisprudência antes de ser reconhecido em nossa carta magna, o reconhecimento desse direito encerra eventuais discussões sobre o tema, garantido segurança jurídica e abrindo novos caminhos para debates sobre outras perspectivas que visem garantir esse direito, como é o caso do tema debatido neste trabalho.

4.2 Utilização de Dados Pessoais na persecução penal

Com o passar dos anos e o avanço das tecnologias, cada vez mais empresas privadas e órgãos públicos armazenam diversos tipos de dados dos indivíduos. É preciso diferenciar, no

Disponível em: https://bdjur.stj.jus.br/jspui/bitstream/2011/43548/dimensao_objetiva_dos_nascimento.pdf. Acesso em 03 de nov. 2024.

[251]MAGALHÃES FILHO, Glauco Barreira. Hermenêutica e Unidade Axiológica da Constituição. 2ª ed. Belo Horizonte: Mandamentos, 2002.

[252]ANDRADE José Carlos Vieira. Direitos Fundamentais na Constituição Portuguesa de 1976. 3ª ed. Coimbra: Almedina, 2006, p. 115.

[253]BELLO FILO, Ney de Barros. A dimensão subjetiva e a dimensão objetiva da norma de direito fundamental ao ambiente. Revista do Tribunal Regional Federal da 1ª Região, v. 19, nº 11/12, nov/dez. 2007.

[254] *Ibid.*

entanto, o armazenamento de dados no setor privado, do armazenamento de dados no setor público. As *big techs,* conhecidas como grandes empresas que dominam o mercado de tecnologia e informação captam os mais variados tipos de dados pessoais, seja de crianças, adolescentes e seus pais ou responsáveis. Além dos dados pessoais, essas empresas também monitoram dados comportamentais dos seus usuários.

Os órgãos públicos, no entanto, armazenam dados pessoais de usuários que exercem suas vidas sociais, como por exemplo solicitar a emissão de passaporte, fazer uma cédula de identidade, enviar uma declaração de imposto de renda, ajuizar uma ação judicial etc. Os órgãos públicos armazenam dados dos cidadãos que exercem as atividades do cotidiano, o que demonstra uma enorme desigualdade entre os dados pessoais armazenados pelo setor público e os dados pessoais armazenados pelo setor privado. Sobre a utilização dos dados pessoais, via de regra, o setor privado os utiliza com a intenção de aumentar os seus lucros. Os órgãos públicos, em especial as intuições policiais que exercem o papel de polícia judiciária, os utiliza na elucidação dos crimes.

Esse fato, por si só, já coloca algumas instituições policiais em um patamar inferior no ato da elucidação de crimes. O tema proteção de dados pessoais se tornou um assunto muito comentado e debatido nos últimos anos. De fato, a proteção de dados pessoais precisa ser analisada com muita cautela, principalmente com o avanço da tecnologia e com a transformação da sociedade. Por outro lado, é inegável que a forma como o tema tem sido tratado, pode receber um outro ponto de vista, que é a análise sob a ótica da prevenção de crimes e do bem estar da coletividade.

Apenas a título de exemplo, depois dos atentados de 11 de setembro de 2001, ocorreu uma enorme transformação nos Estados Unidos, no que diz respeito à segurança e a informações sobre pessoas. Na prática, o efeito do atentado influenciou no cuidado com a segurança e a vida privada do cidadão americano[255]. Logo depois do atentado, o Presidente Busch assinou o *Patriot Act*[256], que facilitou as operações de vigilância das autoridades,

[255]BBC Brasil. Atentados de 11 de setembro: a tragédia que mudou os rumos do século 21. Disponível em: https://www.bbc.com/portuguese/internacional-55351015. Acessado em: 01 de mai. 2024.
[256]Departament of Justice. The Usa Patriot Act: Preserving Life and Liberty. Disponível em: https://www.justice.gov/archive/ll/highlights.htm. Acessado em 01 de mai. 2024.

permitindo um monitoramento de comunicações via telefone e internet. A legislação também facilitou a troca de informações entre órgãos de segurança, como FBI e CIA.

A primeira prioridade com a legislação para o Departamento de Justiça Americano foi o de prevenir futuros ataques terroristas. Desde a sua aprovação, após os atentados de 11 de setembro, o *Patriot Act* desempenhou um papel fundamental em uma série de operações bem-sucedidas para proteger os americanos. Um dos pontos que deve ser observado, é que ao aprovar essa lei, o Congresso Americano apenas utilizou princípios jurídicos existentes, que no Brasil seriam os Fundamentos, Objetivos e Princípios da República Federativa do Brasil, acrescido dos Direitos Fundamentais e Sociais, e os adaptou para preservar as vidas e a liberdade do povo americano, ameaçados por uma rede terrorista global.

O *patriot Act* aumentou a atuação dos órgãos de persecução penal dos Estados Unidos para ampliar a vigilância na prevenção dos crimes de terrorismo e dos crimes que tenham relação com o terrorismo, tais como tráfico de drogas e fraudes de passaportes. Além disso, a legislação também permitiu que autoridades conduzam investigações sem avisar aos terroristas. A prática foi adotada para evitar que os investigados tentem fugir, destruir provas ou até mesmo intimidar testemunhas. Os Tribunais Americanos, portanto, em algumas circunstâncias, permitem que a aplicação da lei adie por um tempo limitado quando o investigado será informado sobre um eventual mandado de busca e apreensão que foi executado[257].

Os órgãos de persecução penal, portanto, devem ter uma certa dose de flexibilidade para atuarem na prevenção e no combate a crimes. A flexibilidade, porém, não pode ser utilizada como uma carta branca para que uma investigação policial seja efetuada sem o devido respeito aos princípios constitucionais. Quem possui acesso a certos tipos de dados pessoais, também precisa ser monitorado e punido com rigor caso haja desvio de conduta.

No final do mês de janeiro de 2024, a Polícia Federal abriu uma investigação para apurar esquema ilegal de vazamento de dados[258] na Agência Brasileira de Inteligência – ABIN, que é o principal órgão do Sistema Brasileiro de Inteligência (SISBIN) e tem como função conceder

[257]Departament of Justice. The Usa Patriot Act: Preserving Life and Liberty. Disponível em: https://www.justice.gov/archive/ll/highlights.htm. Acessado em 01 de mai. 2024.
[258]Agência Brasil. CGU investigará policiais por suposta participação na "Abin paralela". Disponível em: https://agenciabrasil.ebc.com.br/radioagencia-nacional/geral/audio/2024-04/cgu-investigara-policiais-por-suposta-participacao-na-abin-paralela. Acessado em 01 de mai. 2024.

informações estratégicas e confiáveis ao Palácio do Planalto. As informações são enviadas ao Poder Executivo através de relatórios, que tem a finalidade de evitar ameaças ao Estado Democrático de Direito e à soberania nacional. Investigação da Polícia Federal apontou indícios de que além da espionagem ilegal de adversários e desafetos políticos, os sistemas de inteligência do Estado podem ter sido utilizados para conseguir informações sobre investigações sigilosas da própria Polícia Federal.

Apesar das práticas ilegais, os órgãos de persecução penal precisam utilizar os seus bancos de dados para a investigação das mais variadas práticas criminosas, o que nos leva a crer que o ponto central da questão aqui levantada não é o livre acesso aos dados que gerará dano à privacidade, mas sim o vazamento dos dados, o qual geralmente ocorre de forma criminosa. O problema não será resolvido com a vedação ao acesso dos dados armazenados, mas com a correta e devida fiscalização.

As instituições Policiais precisam se adaptar ao avanço da tecnologia, para capacitarem servidores em todo o processo da cadeia de custódia da proteção de dados pessoais. O profissional em questão é conhecido como *Data Protection Officer* – DPO, responsável pelo tratamento e processamento de dados dentro da sua instituição[259]. O DPO é essencial para empresas ou órgãos públicos que tratam dados pessoais. A legislação brasileira sobre proteção de dados não faz uma definição sobre a formação necessária para se tornar um DPO, mas o regulamento europeu estabelece que o profissional deve ser alguém que conheça as profundamente a legislação sobre proteção de dados[260]. Outro ponto importante é que o encargo seja exercido por um profissional que trabalhe com governança, gestão e transparência de dados e que exerça exclusivamente essa função dentro da instituição.

[259]Autoridade Nacional de Proteção de Dados – ANPD. ANPD aprova normas sobre a atuação sobre o Encarregado pelo Tratamento de Dados Pessoais. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aprova-norma-sobre-a-atuacao-do-encarregado-pelo-tratamento-de-dados-pessoais. Acesso em 03 de nov. 2024.
[260]European Data Protection Supervisor. Data Protection. Artigo 37 e seguintes. Disponível em: https://gdpr-info.eu/art-37-gdpr/. Acesso em 03 de nov. 2024.

Estudo realizado pela NordVPN, empresa especialista em segurança, demonstrou que mais de 88 milhões de dados pessoais já foram comercializados pela internet[261]. De mais a mais, 720 mil informações sobre brasileiros já foram vazadas e comercializadas para todo o mundo. Segundo o mesmo estudo, conduzido até abril de 2022, existem mais de 30 mil sites especializados na venda de dados pessoais, todos na chamada *Dark Web*, onde é possível encontrar informações sobre cartões de crédito, dados de identidade pessoal, carteira de motorista, passaportes, números de telefones, contas on line da Uber e Netflix, além de logins de contas bancárias.

Ainda no ano de 2017, matéria divulgada no site do uol[262] tratou sobre determinado site que, após uma simples busca, divulgava informações de brasileiros, tais como endereço, telefones e e-mail. Na ocasião, a Agência Nacional de Telecomunicações – ANATEL, divulgou uma nota alegando que a divulgação de números de telefones deveria ser feita com total anuência do consumidor e que não havia legislação que autorizasse a divulgação dos e-mails. Além da Anatel, Advogados e Institutos de Defesa do Consumidor alegaram, à época, que a divulgação de dados pessoais deveria observar a Constituição Federal, a Lei Geral de Telecomunicações, o Código Civil e o Marco Civil da Internet, já que em 2017 ainda não tínhamos a atual Lei Geral de Proteção de Dados.

O que mais chama atenção é que eventualmente dados ilegais são extraídos de bancos de dados públicos[263], conforme ocorreu em janeiro de 2024, quando uma investigação apontou que criminosos subtraíam dados de sistemas federais e revendiam as informações na internet. Os dados em questão eram utilizados pelos integrantes de facções criminosas e por integrantes das forças de segurança. A plataforma para consulta dos dados era disponibilizada em

[261]Uol. Criminosos faturam r$ 88 milhões com venda de dados roubados de brasileiros na dark web. Disponível em: https://cultura.uol.com.br/noticias/49848_criminosos-faturam-r-88-milhoes-com-venda-de-dados-roubados-de-brasileiros-na-dark-web.html. Acessado em 26 de mai. 2024.

[262]Uol. Site de mostra dados revê política de privacidade, mas ainda exibe celular. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2017/06/13/site-que-mostra-dados-reve-politica-de-privacidade-mas-ainda-exibe-celular.htm. Acessado em 26 de mai. 2024.

[263]Correio Braziliense. Facções e agentes de segurança usaram dados roubados de brasileiros, diz PF. Disponível em: https://www.correiobraziliense.com.br/brasil/2024/01/6795795-faccoes-e-agentes-de-seguranca-usaram-dados-roubados-de-brasileiros-diz-pf.html. Acessado em 26 de mai. 2024.

plataformas nas redes sociais, onde eram cobradas mensalidades que variavam de acordo com a quantidade de consultas realizadas durante um determinado período. A plataforma contava com aproximadamente 10 mil assinantes, que faziam uma média de 10 milhões de consultas mensais.

Outro fato parecido ocorreu no Distrito Federal, quando a Polícia Civil do DF[264] deflagrou uma operação para prender hackers especializados em vazamentos de dados sigilosos de milhares de brasileiros. Os dados coletados de forma ilícita eram utilizados para fraudes eletrônicas, elaboração de dossiês contra autoridades públicas e violação da intimidade dos cidadãos. Através da plataforma utilizada pelos criminosos, foi possível aferir que cerca de 200 milhões de dados pessoais sigilosos de brasileiros estavam expostos, através de fotos, assinaturas digitais, veículos, registros de armas e outras informações. Isso demonstra que em muitos casos, os autores de crimes utilizam, com certa facilidade, informações que os órgãos de persecução penal precisam de autorização judicial para obtê-las.

Apesar de no ano de 2022 não ser falar muito em Lei Geral Penal de Proteção de Dados, Laura Schertel e Jacqueline Abreu[265] abordaram a questão da Proteção de Dados Pessoais na Segurança Pública e no Processo Penal. As Autoras coordenaram uma chamada de Artigos para a elaboração para Dossiê Temático sobre Privacidade e Proteção de Dados Pessoais na Segurança Pública e no Processo Penal.

As Autoras alegaram que o Dossiê buscava contribuir para o debate teórico acerca dos limites jurídicos e do modelo regulatório pertinente para práticas invasivas da privacidade e/ou baseadas no tratamento de dados pessoais empregadas no contexto de atividades estatais voltadas à segurança pública e às investigações criminais. Também alegaram que a academia brasileira possui uma longa e relevante tradição de produção de trabalhos relacionados à tutela

[264]Polícia Civil do Distrito Federal. PCDF prende hackers especializados em vazamento de dados sigilosos de milhares de brasileiros. Disponível em: https://www.pcdf.df.gov.br/noticias/11843/pcdf-prende-hackers-especializados-em-vazamento-de-dados-sigilosos-de-milhares-de-brasileiros. Acessado em 26 de mai. 2024.
[265]MENDES, Laura Schertel; ABREU, Jacqueline. Portal de Periódicos do IDP. Privacidade e Proteção de Dados na Segurança Pública e no Processo Penal. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6214/pdf. Acesso em 08 de set. 2024.

penal da privacidade e à ilicitude de provas invasivas da privacidade, mas que com o avanço da tecnologia, diante de novas modalidades de atividades criminosas, como os crimes cibernéticos, há uma carência de trabalhos científicos investigativos e analítico sobre essas questões[266].

Os tópicos de interesse do Dossiê Temático abrangeriam as seguintes temáticas: Abordagens históricas sobre a regulação de privacidade e da proteção de dados no contexto administrativo de segurança pública e no contexto penal e processual penal; Estratégias e modelos regulatórios; Como deve ser a legislação específica brasileira sobre proteção de dados na segurança pública e no processo penal; Quais tipos de medidas investigativas que constituem violações da privacidade e quais limites esse direito impõe a tais técnicas, em termos de requisitos formais e matérias para poderem ser executadas; O impacto do uso de big data, reconhecimento facial, e outras novas tecnologias baseadas no uso de dados pessoais no policiamento e no processo penal; As doutrinas aplicadas pela jurisprudência brasileira em matéria de privacidade e dados pessoais no campo do processo penal e da segurança pública e suas virtudes, deficiências e consequências reais; Práticas informais de uso de dados por autoridades policiais (como "livros suspeitos") e sua legalidade e consequências práticas e respostas jurídicas; O papel do uso de dados pessoais em novas formas de discricionaridade policial; Compartilhamento de dados entre autoridades com competências diferentes (segurança pública x investigação criminal); Como problemas na proteção da privacidade e de dados pessoais já existentes no contexto da segurança pública e do processo penal são amplificados ou atenuados por uso de novas tecnologias; Constitucionalidade e Regulação de bases de dados sobre material genético; Limites de parcerias público-privadas e endereçamento regulatório e Novas engrenagens que ameaçam ou protegem a presunção de inocência e o devido processo legal no contexto de interesse[267].

Os temas abordados no dossiê demonstram inúmeros pontos que precisam ser analisados com cautela no caso de eventual regulamentação da nova Lei Geral Penal de Proteção de Dados. Cabel salientar, no entanto, que a Chamada de Artigos em questão foi realizada em 2021, ou seja, 1 ano antes da Proteção de Dados Pessoais se tornar um Direito Fundamental. Analisando

[266]Revista de Direito Público. Dossiê: Inteligência Artificial, Ética e Epistemologia. Dossiê: Privacidade e Proteção de Dados Pessoais na Segurança Pública e no Processo Penal. Volume 18. Ano 2021.
[267]MENDES, Laura Schertel; ABREU, Jacqueline. Portal de Periódicos do IDP. Privacidade e Proteção de Dados na Segurança Pública e no Processo Penal. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6214/pdf. Acesso em 08 de set. 2024.

de forma técnica os tópicos elaborados pelas autoras, é provável que já era previsível que a Proteção de Dados seria inserido em nossa Constituição Federal como direito fundamental.

No âmbito das discussões sobre proteção de dados no contexto criminal, em geral, o paradigma que vem à tona é o contraste entre o sigilo e a publicidade de dados nas investigações policiais. É comum a abordagem de medidas de "quebra de sigilo" pelas autoridades policiais, onde se busca o acesso a dados que a princípio são protegidos por sigilo, como é o caso dos dados bancários, telemáticos, telefônicos e biométricos[268].

Frise-se, porém, que o "sigilo/publicidade" não é passível de abarcar e regular a infinidade de medidas e de operações de tratamentos de dados pessoais que se colocam hoje à disposição para investigações criminais e para políticas de segurança pública de forma geral. Isso porque, no contexto atual tende-se a expandir o ramo da inteligência policial, a criação e integração de bancos de dados, o uso de tecnologias de inteligência artificial alimentadas por grandes volumes de dados, isto é, buscando-se usufruir dos benefícios e do poder do *big data*[269].

Toda essa atividade policial da era *big data* envolve a coleta e uso de dados de forma contínua e cumulativa de um grande número de pessoas, independentemente de possuírem histórico de condenação ou não. São informações geralmente utilizadas para abrir linhas de investigação, fazer provas pré-constituídas, correlacionar informações, detectar crimes e outras ações que podem ocasionar os mais diversos tipos de abusos e ilegalidades no tratamento de dados. Tais operações de dados podem envolver usos indevidos, usos abusivos, usos secundários (diferentes e estranhos à finalidade original), vazamentos, discriminação e erros por conta de dados sem acurácia e desatualizados[270].

A par disso, é inevitável e imprescindível a aplicação do direito à proteção de dados pessoais também nas esferas investigativas e da segurança pública, como já foi feito com a elaboração de uma lei para o setor privado. A existência dessa lacuna potencializa a exposição dos titulares de dados pessoais a violações e restrições em liberdades civis fundamentais graves, podendo levar pessoas a serem indevidamente inquiridas ou até mesmo presas[271].

---

[268] *Ibid.*
[269] *Ibid.*
[270] *Ibid.*
[271] *Ibid.*

Laura Schertel e Jacqueline Abreu advertem, no entanto, que[272]:

> O recorte existente na LGPD e o espaço para a aprovação de uma LGPD penal não significam que a noção de proteção de dados como a conhecemos hoje não seria aplicável no processo penal e na segurança pública. Dois pontos demonstram o contrário: primeiro, o reconhecimento da proteção de dados pessoais como direito fundamental autônomo pelo STF e a sua aplicação em contextos envolvendo inteligência nacional e segurança pública; segundo, a observância dos princípios e direitos e da proporcionalidade e devido processo legal, conforme determinado pela própria LGPD – que, inclusive, já determina a elaboração de relatório de impacto à proteção de dados pessoais, assim como regula em parte a cooperação internacional nessa seara.
> Nesse sentido, a importância de se aprovar uma lei específica de proteção de dados para investigação criminal e segurança pública o Brasil consiste em: criar parâmetros procedimentais para que existam balizas legais concretas no tratamento de dados pelos órgãos de investigação; ampliar a transparência sobre como dados são tratados para permitir a responsabilização e desencorajar usos secundários inadvertidos; e minimizar riscos de tratamentos abusivos, ilegais e de incidentes de segurança, dentre outros. À luz da sensibilização da discussão sobre o impacto de novas tecnologias, intersecção entre privacidade, proteção de dados e segurança pública e de novas modalidades de atividades criminosas e meios de obtenção de provas no processo penal, a academia brasileira possui importante papel na promoção de debates e no desenvolvimento de doutrina passível de endereçar problemas complexos e multidisciplinares.

A coleta de dados sob a alegação de proteção à segurança pública não pode servir de base para a violação de direitos fundamentais. Para Nathalie Fragoso e Gabriel Brezinski Rodrigues, já é possível perceber que os métodos ocultos de investigação provocaram fissuras na estrutura acusatória do processo penal, sobretudo no esgarçamento das garantias individuais, na erosão de direitos fundamentais clássicos, como as violações de sigilos de dados e comunicações, e no total abandono da concepção do acusado enquanto sujeito processual titular de direitos[273].

4.3 Proteção de Dados Penais na Europa como modelo para a Proteção de Dados Pessoais no Brasil

Conforme já mencionado acima, é cediço que atualmente diversas instituições em todo mundo, sejam públicas ou privadas, utilizam dados pessoais para o pleno desenvolvimento de suas atividades cotidianas. A utilização desses dados pessoais no âmbito penal vem atraindo

[272] *Ibid.*
[273] FRAGOSO, Nathalie; RODRIGUES, Gabriel Brezinski. Protodefesa à Brasileira: Contraditório e Ampla Defesa em Investigações Sigilosas. Revista de Direito Público. Volume 18. Ano 2021.

cada vez mais olhares, principalmente pela questão do conflito de direitos fundamentais que envolve o tema.

Foi possível aferir acima que o GDPR teve uma significante influência na elaboração e implementação da Lei Geral de Proteção de Dados no Brasil. No que diz respeito ao tratamento de dados pessoais na persecução penal, não poderia ser diferente. A diretiva (UE) 2016/680, também serviu de base para a discussão e elaboração do Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal.

Embora o Anteprojeto ainda esteja parado na Câmara dos Deputados, é possível perceber, após a leitura de cada artigo, o quanto o modelo Europeu serviu de parâmetro para que o primeiro passo sobre a regulamentação da proteção de dados no direito penal brasileiro fosse dado. Assim também foi com o direito Português, que em 2018 aprovou as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, detecção, investigação ou repressão de infrações penais ou de execução de sanções penais, conforme pode ser visto na Lei portuguesa número 59/2019[274] de 08 de agosto.

De forma ampla, a legislação portuguesa abrangeu a sua aplicação ao tratamento de dados nas leis processuais penais, nos sistemas automatizados, bem como a arquivos onde não exista automatização, o que demonstra a preocupação da lei portuguesa com o âmbito de sua abrangência, regulamentando, dessa forma, todo e qualquer dado que possa ser utilizado no âmbito do direito penal e processual penal. Outro ponto importante da legislação foi o de não limitar o intercâmbio de dados pessoais entre autoridades competentes da União Europeia[275].

Os dados genéticos, biométricos e os dados relativos à saúde também foram mencionados como sendo utilizáveis para a apuração de delitos. Os dados genéticos são os dados pessoais relativos às características genéticas, hereditárias ou adquiridas de uma pessoa, que forneçam informações únicas sobre a sua fisiologia ou sobre a saúde, que resultem da

[274]PORTUGAL. Lei número 59/2019 de 08 de agosto. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/59-2019-123815983. Acessado em 03 de jun. 2024.
[275]PORTUGAL. Lei número 59/2019 de 08 de agosto. **Objeto:** A presente lei estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, transpondo para a ordem jurídica interna a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/59-2019-123815983. Acessado em 03 de jun. 2024.

análise de uma amostra biológica. Os dados biométricos são os dados pessoais resultantes de um tratamento técnico específico, relativos às características físicas, fisiológicas ou comportamentais de uma pessoa, que permitam ou confirme a sua identificação única, tais como imagens faciais ou dados datiloscópicos. Por fim, os dados relativos à saúde são aqueles dados relativos à saúde física ou mental do indivíduo, incluindo informações que revelem o seu estado de saúde.

Na legislação portuguesa, os órgãos de persecução penal podem efetuar o tratamento dos dados pessoais de todos os envolvidos na persecução penal, com a ressalva de que deve ocorrer uma distinção entre diferentes categorias de titulares de dados. As categorias foram divididas entre pessoas que estão na iminência de cometer uma infração penal, pessoas condenadas pela prática de uma infração penal, vítimas de infrações penais ou pessoas que possam se tornar vítimas e terceiros envolvidos em uma infração penal, tais como testemunhas ou pessoas que possam fornecer informações sobre a prática de infrações penais.

Cabe salientar que sobre a limitação do direito de acesso ao titular dos dados pessoais, a lei portuguesa trouxe a possibilidade do responsável pelo tratamento recusar ou restringir o direito de acesso do titular dos dados, quando a limitação constituir uma necessária e proporcional para evitar prejuízo nas investigações, inquéritos ou processos judiciais, evitar prejuízo para a prevenção, detecção investigação ou repressão de infrações penais ou para execução de sanções penais, para proteger a segurança jurídica, para proteger a segurança nacional e para proteger os direitos liberdades e garantias de terceiros. Da mesma forma, a solicitação de exclusão dos dados pessoais também pode ser recusada pela autoridade competente, pelos mesmos motivos expostos no parágrafo anterior.

Outro ponto da legislação que merece destaque é o fato da Comissão Nacional de Proteção de Dados de Portugal[276] ter ficado com a atribuição de fiscalizar o cumprimento e fazer aplicar tudo o que está previsto na lei. Além disso, a CNPD também ficou responsável por propor e emitir pareceres sobre medidas legislativas e administrativas relacionadas com a proteção dos direitos e liberdades das pessoas em matéria de proteção de dados pessoais. Diferentemente do que ocorreu no Brasil, o Anteprojeto Penal de Proteção de Dados previu que a função cabe ao Conselho Nacional de Justiça – CNJ. A alegação da escolha se deve ao fato

[276]Comissão Nacional de Proteção de Dados. Portugal. Disponível em: https://www.cnpd.pt/. Acessado em 03 de jun. 2024.

de o CNJ possuir uma certa autonomia e pluralidade, já que seus integrantes também fazem parte do STF, STJ, TST, PGR, Conselho Federal da OAB, da Câmara dos Deputados e do Senado Federal. Outra razão seria a financeira, uma vez que não seria necessário gerar gastos com a criação de um órgão específico para a fiscalização da lei.

Maria Thereza de Assis Moura abordou o tema, quando falou sobre as oportunidades e desafios do CNJ como órgão regulador de proteção de dados[277]. Para a Ministra do STJ, é certo falar que a evolução tecnológica permitiu o advento de novos mecanismos de interconexão e transmissão de informações em tempo real, o que resultou em uma nova face da criminalidade, que fulminou a eficiência dos mecanismos tradicionais de investigação, que precisam ser aprimorados.

Desatacou, ainda, que no campo da investigação e repressão às infrações penais, o implemento das novas tecnologias se faz necessário para agregar a necessária eficiência efetividade e celeridade capazes de obstar a deterioração da prova material dos crimes. Diante disso, o Conselho Nacional de Justiça, atento à crescente utilização da internet e de modelos computacionais estruturados para o acesso e processamento de dados pelos órgãos judiciários brasileiros, adotou medidas preparatórias e ações iniciais para a adequação às disposições contidas na Lei Geral de Proteção de Dados.

Para tanto, o Conselho Nacional de Justiça recomendou[278]: a elaboração de um plano de ação por cada órgão do Poder Judiciário Brasileiro; a disponibilização ao público de informações sobre a aplicação da LGPD e de formulário para o exercício dos direitos dos titulares de dados pessoais; a elaboração e publicação de política de privacidade e o registro de tratamento dos dados pessoais; e constituição de Grupo de Trabalho para estudo e identificação das medidas necessárias à implementação da LGPD no âmbito do respectivo tribunal, cujo relatório subsidiará a elaboração de uma política nacional pelo Conselho Nacional de justiça.

O Conselho Nacional de Justiça, portanto, diante das competências que lhe foram atribuídas pelo Artigo 103-B da Constituição Federal, assumiu papel de protagonismo na

[277]BRITO CRUZ, Francisco; SIMÃO, Bárbara(eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. V. São Paulo. InternetLab, 2022.
[278]Conselho Nacional de Justiça. Recomenda aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequações às disposições contidas na Lei Geral de Proteção de Dados – LGPD. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3432. Acesso em 04 de nov. 2024.

implementação da Lei Geral de Proteção de Dados, com foco nas atividades desenvolvidas pelo Poder Judiciário e por órgãos prestadores de serviços notariais e de registros que atuem por delegação do poder público ou oficializados.

Ocorre que a atribuição prevista ao Conselho Nacional de Justiça não está prevista na Constituição Federal, o que ocasionaria em uma desvirtuação do CNJ. O mais apropriado, portanto, conforme será visto adiante, é que o parlamento brasileiro altere o Anteprojeto, para atribuir a função para a Autoridade Nacional de Proteção de Dados – ANPD, da mesma forma como ocorre em Portugal.

Além da legislação específica para o tratamento e dados pessoais no âmbito do processo penal, em Portugal também há uma lei destinada especificamente para a proteção de dados no processo judicial. A Lei número 34 de 2009[279] de 14 de julho estabelece o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial. O que chama a atenção é que em Portugal, ao que tudo indica, a lei, além de tratar da proteção de dados em processos cíveis, também o faz nos casos dos inquéritos policiais.

Voltando ao tema central do tópico deste capítulo, que é a proteção de dados penais na Europa como modelo para a proteção de dados pessoais no Brasil, está em vigor, no direito Português, a Lei número 38/2015[280] de 11 de maio, que estabelece as condições e os procedimentos para assegurar o uso dos sistemas de informação dos órgãos de polícia criminal. Conforme será possível aferir adiante, a Polícia Civil do Distrito Federal já possui diversas normas sobre Segurança da Informação e Segurança Orgânica, o que inclui a proteção de o tratamento de dados pessoais para fins não penais. Em Portugal, há a previsão de que as autoridades judiciárias competentes podem, a todo momento, no âmbito da direção da investigação criminal, bem como nas fases de inquérito e de instrução, nos termos da lei processual penal portuguesa, acessar informações constantes no sistema integrado de informação criminal[281].

[279]PORTUGAL. Lei número 34/2009 de julho. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/34-2009-492407. Acessada em 03 de jun.2024.
[280]PORTUGAL. Lei número 38/2015 de 11 de maio. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/38-2015-67185039. Acessado em 03 de jun. 2024.
[281]PORTUGAL. Lei número 38/2015 de 11 de maio. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/38-2015-67185039. Acessado em 03 de jun. 2024.

Aduz, inclusive, que o Ministério Público Português pode, no âmbito da realização de ações de prevenção criminal, acessar, através de plataforma, informações constantes no sistema integrado de informação criminal[282]. Embora aqui no Brasil os atos efetuados durante a investigação de um delito sejam mencionados no relatório do inquérito policial, é como se o Judiciário e o Ministério Público acompanhassem, quase em tempo real, todas as diligências que estejam sendo efetuadas durante a investigação policial.

A prática desse costume pode ser bem vista, tendo em vista ser mais um mecanismo contra o abuso na utilização dos dados pessoais. Cabe salientar que em Portugal o acesso é limitado ao Procurador Geral da República aos membros do Ministério Público envolvidos em funções de coordenação da investigação criminal ou no âmbito da prevenção criminal e aos Juízes que exerçam competências no âmbito da instrução criminal, relativamente aos processos onde atuem como titulares e aos Membros do Ministério Público que estejam vinculados ao inquérito policial[283].

Percebe-se, portanto, que o modelo da Diretiva 680/2016 serviu como parâmetro de tratamento de dados pessoais na persecução penal não só para os países da Europa, como também para a elaboração do Anteprojeto Penal de Proteção de Dados. Significa dizer que o Brasil está traçando o caminho necessário para o compartilhamento de dados pessoais para outro país ou para alguma organização internacional. É preciso reforçar, no entanto, que a prática só é possível nas seguintes condições: transferência necessária para atividades de segurança pública ou persecução penal; tiver sido adotada decisão de adequação, garantia adequada ou aplicação de derrogação; transferência para agente responsável e competente para fins de segurança pública ou persecução penal; consentimento prévio à transferência por país, o consentimento é dispensando somente em caso de ameaça à segurança pública quando não puder ser obtido em tempo hábil e deve ser informado à autoridade responsável em um prazo de 48 (quarenta e oito) horas; avaliação do procedimento em caso de transferência ulterior e a transferência não pode comprometer o nível de proteção das pessoas[284].

---

[282] *Ibid.*
[283] *Ibid.*
[284] ALVES SILVA, Amanda Cristina; SANTOS, Jéssica Guedes. Portal de Periódicos do IDP. COMPARTILHAMENTO INTERNACIONAL DE DADOS PARA SEGURANÇA PÚBLICA: PARARELO LEGISLATIVO ENTRE BRASIL E PORTUGAL. Disponível em: file:///C:/Users/Usuario/Downloads/6230-Texto%20do%20Artigo-18861-20303-10-20220130.pdf. Acesso em 04 de nov. 2024.

Embora ainda não exista em solo brasileiro uma Lei Geral Penal de Proteção de Dados que estabeleça as diretrizes para a transferência internacional de Dados, o Brasil foi o primeiro país da América Latina a ser convidado para fazer parte da Agência Europeia Para Cooperação em Justiça Criminal – EUROJUST[285]. Caso a adesão ocorra de fato, após passar pela aprovação do Congresso Brasileiro, o Brasil, através do Ministério Público Federal, poderá abrir processos e acessar bancos de dados da União Europeia, facilitando o combate da prática de crimes transacionais, o que auxiliaria, por exemplo, no caso das duas brasileiras que foram injustamente presas na Alemanha pela prática do crime de tráfico de drogas, após terem suas malas trocadas por outras repletas de substâncias entorpecentes[286].

A legislação europeia, GDPR, portanto, além das leis portuguesas sobre proteção de dados, influenciaram de forma muito clara o Anteprojeto Penal de Proteção de Dados no Brasil. Dessa forma, caso o Anteprojeto seja, de fato, transformado em lei, teremos uma proteção de dado no âmbito penal, muito semelhante à proteção existente na Europa, com destaque para a proteção de dados em Portugal[287].

Sobre a questão de proteção de dados para fins penais, o Tribunal Constitucional de Portugal[288] teve a oportunidade de analisar alguns litígios que podem servir de parâmetro para a abordagem do tema no Brasil. Tendo em vista que o foco central do objeto deste estudo não é a análise de todo o arcabouço jurídico português, analisaremos, tão somente, os Acórdãos 403/2015; 464/2019 e 687/2021.

O primeiro Acórdão, sob o número 403/2015[289], se pautou na análise do Regime Jurídico do Sistema de Informações da República Portuguesa, que em seu artigo 2º estabeleceu que os oficiais do SIS e do SIED poderiam acessar informações bancárias, fiscais, dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, a data, a hora a

[285]EUROJUST. Disponível em: https://www.eurojust.europa.eu/. Acessado em 03 de jun. 2024.
[286]*Ibid.*
[287]GDPR.EU. What is the LGPD? Brazil's version of the GDPR. Brazil passed the General Data Protection Law in 2018, and it will come into effect February 2020. This article examines the GDPR vs. the LGPD, how it differs, and what business owners globally need to do to prepare. Disponível em: https://gdpr.eu/gdpr-vs-lgpd/. Acesso em 26 de nov. 2024.
[288]Tribunal Constitucional Portugal. Disponível em: https://www.tribunalconstitucional.pt/tc/home.html. Acesso em 24 de set. 2024.
[289]Tribunal Constitucional Portugal. Acordão número 403/2015. Disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20150403.html. Acesso em 24 de set. 2024.

duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização, sempre que sejam necessários, adequados ou proporcionais, numa sociedade democrática, para o cumprimento das atribuições legais dos serviços de informações, mediante autorização prévia e obrigatória da Comissão de Controle Prévio, seguido de pedido devidamente fundamentado.

A justificação para a invasão de privacidade do dispositivo questionado no Tribunal Constitucional Portugal é que no contexto recente da Estratégia Nacional de Combate ao Terrorismo e dos desafios colocados pelas novas ameaças à segurança nacional, surgiria como incontornável o acesso a meios operacionais consagrados pela primeira vez de modo transparente e expresso na lei positiva, indo ao encontro do padrão de garantias da Carta Europeia dos Direitos Fundamentais e da Convenção Europeia dos Direitos do Homem. Nesse contexto, e em linha com a maior parte dos Estados-Membros da União Europeia, prevê-se o acesso aos metadados, isto é, o acesso a dados conservados pelas operadoras de telecomunicações, o que se rodeia de especiais regras para salvaguardar integralmente os direitos dos cidadãos, em especial o direito à privacidade.

A única questão levada ao Tribunal Constitucional Portugal foi o fato do Governo Português, por intermédio do Decreto número 426/XII da Assembleia da República, poder ter acesso a dados pessoais dos cidadãos portugueses, conforme mencionado acima, o que gerou uma análise da constitucionalidade da referida norma legal.

No caso específico, para o Tribunal Constitucional Portugal o acesso aos dados das comunicações efetivamente realizadas ou tentadas põe em causa direitos fundamentais das pessoas, não sendo apenas uma invasão ou intromissão do conteúdo informacional veiculado pelos meios de transmissão (dados de conteúdo), mas também das circunstâncias em que a comunicação foi realizada (dados de tráfego). Mesmo que não haja acesso ao conteúdo, a interconexão entre dados de tráfego pode fornecer um perfil complexo e completo da pessoa a ser investigada, tais como com quem conversa e os lugares que mais frequenta, o que demostra claramente que a manipulação ilegal ou ilegítima do conteúdo e das circunstâncias da comunicação pode violar a privacidade dos interlocutores, atentando ou pondo em risco esferas nucleares das pessoas, das suas vidas ou dimensões, do seu modo de ser ou estar.

O Tribunal Constitucional Portugal também entendeu que ao definir o campo de incidência da lei restritiva do direito à inviolabilidade das comunicações pela "matéria de processo criminal", a Constituição Portuguesa ponderou e tomou posição (em parte) sobre o conflito entre os bens jurídicos protegidos por aquele direito fundamental e os valores comunitários, especialmente os da segurança, cuja realização se dirige ao processo penal. Não obstante as restrições legais ao direito à inviolabilidade das comunicações que o legislador está autorizado a estabelecer, devem obedecer à ponderação do princípio da proporcionalidade, com preferência abstrata pelo valor da segurança em prejuízo da privacidade das comunicações, o que só serve para o processo penal.

Importante a Decisão do Tribunal Constitucional Portugal, porque a ingerência das autoridades públicas nos direitos fundamentais para fins penais garante que valores de "justiça" e de "segurança" sejam devidamente resguardados, para que as pessoas possam exercer diversos outros direitos fundamentais. O Tribunal entendeu, porém, que as restrições à privacidade só podem ocorrer para crimes já praticados, em um contexto previamente delimitado, utilizando apenas informações que sejam necessárias para o fim específico da investigação, o que envolve pessoas consideradas suspeitas[290].

[290]Tribunal Constitucional Portugal. Acordão número 403/2015. De facto, iniciando-se o processo penal com a *notitia criminis*, a recolha de informações para esse fim tem que se dirigir a um crime já praticado. De modo que, a recolha de dados no âmbito de processo criminal é sempre feita num contexto *previamente delimitado* pelo objeto desse processo, apenas se recolhendo informações no contexto da investigação de um *específico facto* e em relação a *específicos sujeitos* tidos como suspeitos. Diferente é a configuração da atuação "preventiva" dos serviços de informações, à qual corresponderá um acesso aos dados que pode abranger um universo de pessoas muito mais vasto, precisamente por não estar ainda pré-ordenado à investigação de um facto concreto e delimitado. As funções de recolha e tratamento de informações a levar a cabo pelo SIRP, porque preventivas, não se orientam para uma atividade investigatória de crimes praticados ou em execução. Não são atos de polícia judiciária, destinada à investigação criminal. É evidente que uma atuação investigatória processualizada e publicizada, na forma de *inquérito preliminar* ou de *instrução*, não só salvaguarda a liberdade e segurança no decurso do processo, como dá garantia de que a prova para ele canalizada foi obtida com respeito pelos direitos fundamentais. A mesma conclusão não se pode extrair de uma *ação de prevenção* não processualizada ou mesmo não suficientemente formalizada, coberta pelo segredo de Estado, que decorre na total ausência de instrumentos defensivos que comportem um mínimo de dialética processual. Os procedimentos preventivos dessa natureza, desvinculados da dependência funcional a uma autoridade judiciária, não fazem parte da investigação criminal. A Lei Fundamental enquadra essas ações no direito constitucional da polícia – artigo 272.º –, não como atividade auxiliar da realização da justiça, mas apenas como "medidas de polícia" de caráter preventivo. A atividade relativa à produção de informações pelo SIRP destinadas a prevenir os crimes contra a segurança do Estado, soberania nacional e realização do Estado de Direito, pode ser abrangida por esse preceito (cfr. Jorge Miranda e Rui Medeiros, *ob. cit.*, págs. 663 e 664), mas, porque não se dirige à descoberta da autoria de um crime, não reveste a natureza de investigação criminal. As ações de prevenção do SIRP são, pois, *procedimentos administrativos* que, devendo respeitar os direitos, liberdades e garantias (artigo 5.º do Decreto n.º 426/XII), não obedecem aos princípios jurídico-constitucionais conformadores do processo penal, proclamados no artigo 32.º da CRP. Disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20150403.html. Acesso em 24 de set. 2024.

Para a atuação preventiva, no entanto, o acesso aos dados pessoais pode violar a privacidade de diversas pessoas, justamente por não existir investigação criminal de um fato concreto e delimitado. O tratamento de dados e o acesso a informações de forma preventiva, portanto, não são guiados pela atividade de investigação, o que não representa os atos de polícia judiciária[291].

No Acordão número 464/2019[292] o Tribunal Constitucional Portugal se deparou com a solicitação de apreciação dos Artigos 3º e 4º da Lei Orgânica número 04/2017, que aprovou e regulou o procedimento especial de acesso a dados de telecomunicações e internet pelos oficiais de informações do Serviço de Informações de Segurança (SIS) e do Serviço de Informações Estratégicas de Defesa (SIED).

As normas questionadas tinham o seguinte teor: Artigo 3º. Acesso a dados de base e de localização de equipamento. Os oficiais de informações do SIS e do SIED podem ter acesso a dados de base e de localização de equipamento para efeitos de produção de informações necessárias à salvaguarda da defesa nacional, da segurança interna e da prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada e no seu exclusivo âmbito. Artigo 4º. Acesso a dados de tráfego. Os oficiais de informações do SIS e do SIED apenas podem ter acesso a dados de tráfego para efeitos de produção de informações necessárias à prevenção de atos de espionagem e de terrorismo.

Para impugnar a constitucionalidade das normas, os requerentes invocaram violação ao número 4 do Artigo 34 da Constituição Portuguesa, no qual consta que é proibida toda ingerência de autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvo os casos previstos na lei em matéria de processo criminal.

---

[291]Tribunal Constitucional Portugal. Acordão número 403/2015. Diferente é a configuração da atuação "preventiva" dos serviços de informações, à qual corresponderá um acesso aos dados que pode abranger um universo de pessoas muito mais vasto, precisamente por não estar ainda pré-ordenado à investigação de um facto concreto e delimitado. As funções de recolha e tratamento de informações a levar a cabo pelo SIRP, porque preventivas, não se orientam para uma atividade investigatória de crimes praticados ou em execução. Não são atos de polícia judiciária, destinada à investigação criminal. Disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20150403.html. Acesso em 24 de set. 2024.

[292]Tribunal Constitucional Portugal. Acórdão número 464/2019. Disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20190464.html. Acesso em 24 de set. 2024.

Da mesma forma como ocorreu no Acordão anterior, o Tribunal Constitucional Portugal também entendeu que o tratamento de dados e a utilização de informações dos cidadãos portugueses para efeito de prevenção se dissocia de forma clara e precisa da atividade de investigação criminal. No julgado em tela não ficou comprovado se as informações que constam no dispositivo legal em análise seriam utilizadas para uma atividade de investigação de crimes já praticados ou em execução[293].

Os Juízes do Tribunal Constitucional Portugal invocaram a tese de que a jurisprudência europeia é no sentido de preservação da proteção ao direito à privacidade e à tutela dos dados pessoais. A prevenção de crimes deve ser vista como proteção de pessoas e bens, vigilância de indivíduos e locais suspeitos, mas não podem ser medidas de limitação de direitos, liberdades e garantias dos cidadãos[294].

Por fim, no Acordão número 687/2021[295], os julgadores se depararam com o questionamento do Decreto número 167/XIV, relativo ao combate e à fraude de meios de pagamento que não seja efetuado em espécie, alterando o Código Penal Português. Na ocasião, foi questionado se as polícias poderiam utilizar, sem prévia autorização judicial, mensagens de e-mails em computadores apreendidos no âmbito de uma investigação policial[296].

---

[293]Tribunal Constitucional Portugal. Acórdão número 464/2019. Em primeiro lugar, é de recordar, nesta sede, o que este Tribunal afirmou, no Acórdão n.º 403/2015, acerca da caracterização o SIRP: "os fins e interesses que a lei incumbe ao SIRP de prosseguir, os poderes funcionais que confere ao seu pessoal e os procedimentos de atuação e de controlo que estabelece, colocam o acesso aos dados de tráfego fora do âmbito da investigação criminal", pelo que "a caracterização dessa concreta atividade como recolha de "informações" para efeitos de "prevenção" dissocia -a, de forma clara e precisa, da atividade própria de investigação criminal" (cf. o respetivo ponto 19). Desta forma, e apesar das mudanças operadas no sistema de acesso aos dados de tráfego, em relação ao que se previa nas normas fiscalizadas no Acórdão n.º 403/2015, não pode deixar de se considerar que, também nas normas ora em causa, o acesso aos dados se destina, tão -só, e sem qualquer dúvida, à prossecução das atribuições do SIRP, nos termos legalmente definidos; ou seja, a recolha de dados de tráfego não se destina a investigação ou produção de prova no âmbito de um processo penal em curso. Destina -se, sim, como pode ler -se no artigo 1.º da Lei Orgânica n.º 4/2017, a permitir, sempre que necessário "a prossecução da atividade de produção de informações pelo Sistema de Informações da República Portuguesa (SIRP) relacionadas com a segurança interna, a defesa, a segurança do Estado e a prevenção da espionagem e do terrorismo". Disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20190464.html. Acesso em 24 de set. 2024.

[294]*Ibid.*

[295]Tribunal Constitucional Portugal. Acordão número 687/2021. Disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20210687.html. Acesso em 24 de set. 2024.

[296]Tribunal Constitucional Portugal. Acordão número 687/2021. Artigo 17. 1. Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontradas, armazenadas nesses sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrônico ou de natureza semelhante que sejam necessárias à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a sua apreensão; 2. O órgão de polícia criminal pode efetuar as apreensões referidas no número anterior, sem prévia autorização judicial da autoridade judiciária, no discurso de pesquisa informática legitimamente ordenada e executada nos termos do Artigo 15º, bem como quando haja urgência ou perigo na demora, devendo tal apreensão ser validada pela autoridade judiciária no prazo máximo de 72 horas; 3. À apreensão de mensagens de correio eletrônico e de natureza semelhante aplica-se o

Para os requerentes, as normas questionadas padeciam de vício de inconstitucionalidade material, por violação do direito à inviolabilidade do domicílio e das correspondências. Desta vez, o entendimento do Tribunal Constitucional Portugal foi no sentido de garantir que os dados pessoais pudessem ser acessados pelas autoridades competentes na luta contra a criminalidade, onde os interesses são vitais para a segurança nacional, da defesa, ou da segurança pública, quando existirem elementos de que a prática possa contribuir para a luta contra atividades que atentem contra o Estado de Direito. Além disso, com o intuito de garantir, na prática, o pleno respeito aos requisitos para o acesso, é essencial que as autoridades competentes estejam sujeitas a uma fiscalização prévia, efetuada por um órgão jurisdicional ou por uma autoridade administrativa independente e que a decisão do órgão jurisdicional ou da entidade seja tomada na sequência de um pedido fundamentado dessas autoridades, apresentado, nomeadamente, no âmbito de processos de prevenção, de detecção ou de perseguição penal.

Aqui no Brasil, o Superior Tribunal de Justiça, no AgRg do Habeas Corpus número 828054 – RN[297], se deparou com uma situação onde ocorreu a apreensão de um aparelho de telefone celular, que teve dados pessoais extraídos através de capturas de telas. O STJ entendeu que o instituto da cadeia de custódia visa garantir que o tratamento dos elementos probatórios, desde a sua arrecadação até a análise pela autoridade judicial, seja idôneo e livre de qualquer interferência que possa macular a confiabilidade da prova.

A par disso, diante da volatilidade dos dados telemáticos e da maior suscetibilidade a alterações, é imprescindível que se faça a adoção de mecanismos que assegurem a preservação integral dos vestígios probatórios, de forma que seja possível a constatação de eventuais alterações, intencionais ou não, dos elementos inicialmente coletados, demonstrando-se a higidez do caminho percorrido pelo material[298].

---

disposto nos números 5 a 8 do artigo anterior; 4. O Ministério Público apresenta ao juiz, sob penal de nulidade, as mensagens de correio eletrônico ou de natureza semelhante cuja apreensão tiver ordenado ou validado e que considerem serem de grande interesse para a descoberta da verdade ou para a prova, ponderando o juiz a sua junção aos autos tendo em conta os interesses do caso concreto. 5. Os suportes técnicos que contenham as mensagens apreendidas cuja junção não tenha sido determinada pelo juiz são guardados em envelope lacrado, à ordem do tribunal e destruídos após o trânsito em julgado da decisão que puser termo ao processo; 6. No que não se encontrar previsto nos números anteriores, é aplicável, com as necessárias adaptações, o regime da apreensão de correspondência previsto no Código de Processo Penal. Disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20210687.html. Acesso em 24 de set. 2024.

[297]STJ, AgRg no Habeas Corpus 828.054, Segunda Turma, Rel. Min. Joel Ilan Paciornik, J. 23.04.2024, DJe 29.04.2024.

[298]*Ibid.*

Para o Superior Tribunal de Justiça, a observação do *princípio da mesmidade* visa assegurar a confiabilidade da prova, a fim de que seja possível se verificar a correspondência entre aquilo que foi colhido e o que resultou de todo o processo de extração da prova de seu substrato digital[299]. Uma forma de se garantir a mesmidade dos elementos digitais é a utilização da técnica de algorítmico *hash*, o qual deve vir acompanhada da utilização de um software confiável, auditável e amplamente certificado, que possibilite o acesso, a interpretação e a extração dos dados do arquivo digital.

No Habeas Corpus em questão, a defesa reiterou as alegações de nulidade em razão de uma violação de domicílio e da quebra da cadeia de custódia. Também sustentou que as denúncias anônimas, desacompanhadas de elementos preliminares, não constituem motivação para busca domiciliar, o que ocorreu no caso em tela. No ato do cumprimento do Mandado de Busca, Policiais acessaram o telefone celular do alvo da busca e, mediante *print screen*, extraíram várias conversas realizadas pelo aplicativo *Whatsapp*.

O que foi debatido nesse julgado do STJ é se a prova digital, no caso concreto, pode ser considerada um elemento lícito, válido e apto a produzir efeitos no processo penal. Conforme preceituam os Artigos 158 e seguintes do Código de Processo Penal, o instituto da cadeia de custódia visa garantir que o tratamento de elementos probatórios, desde a sua arrecadação até a análise e deliberação pela autoridade judicial seja idôneo e livre de qualquer interferência que possa macular a confiabilidade da prova[300].

O Tribunal entendeu que as provas digitais, em razão de sua natureza, facilmente e, imperceptivelmente, alterável, demandam ainda maior atenção e cuidado em sua custódia e tratamento, sob pena de ter seu grau de confiabilidade diminuído drasticamente ou até mesmo anulado. Na decisão, o STJ mencionou que Gustavo Badaró leciona que[301]:

> "Evidente que independentemente de qual procedimento técnico empregado, além de adequado segundo as melhores práticas, ele também precisará ser documentado e registrado em todas as suas etapas. Tal exigência é uma

[299] *Ibid.*
[300] BRASIL. Código de Processo Penal. Art. 158-A. Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em 25 de set. 2024.
[301] *Ibid.*

> garantia de um correto emprego das *operating procedures*, especialmente por envolver um dado probatório volátil e facilmente sujeito à mutação. Além disso, exatamente pela diferença ontológica da prova digital com relação à prova tradicional, devido àquela não se valer de uma linguagem natural, mas digital, é que, como diz Pittiruti, uma cadeia de custódia detalhada se faz ainda mais necessária".

Ainda de acordo com o Superior Tribunal de Justiça, é indispensável que todas as fases do processo de obtenção das provas digitais sejam documentadas, cabendo à polícia, além da adequação de metodologias tecnológicas que garantam a integridade dos elementos extraídos, o devido registro das etapas da cadeia de custódia, de modo que sejam asseguradas a autenticidade e a integralidade dos dados.

No caso concreto, foi verificado que a equipe policial não levou aos autos registros válidos sobre a extração de dados. Outro aspecto que deve ser destacado é que o próprio STJ já entendeu que é incabível simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia. De mais a mais, é ónus do Estado comprovar a integridade e a confiabilidade das fontes de prova por ele apresentadas.

Por fim, foi inafastável a conclusão de que não houve a adoção de procedimentos que assegurassem a idoneidade e a integridade dos elementos obtidos pela extração de dados do celular do réu, ficando evidente o prejuízo causado pela quebra da cadeia de custódia, o que gerou a imprestabilidade da prova digital.

Percebe-se, portanto, que no contexto do processo penal, tanto em Portugal quanto no Brasil, a proteção de dados pessoais é uma questão de grande importância e está regulamentada por legislações específicas. Em Portugal, a proteção de dados pessoais no âmbito penal é regida pelo Regulamento Geral sobre a Proteção de Dados (RGPD) e pela Lei n.º 59/2019. Esta Lei assegura a execução do RGPD na ordem jurídica nacional e regula o tratamento de dados pessoais por autoridades competentes para fins de prevenção, detecção, investigação ou repressão de infrações penais. A lei estabelece regras específicas para garantir que os dados pessoais sejam tratados de maneira segura e que os direitos dos titulares dos dados sejam respeitados.

No Brasil, conforme foi mencionado alhures, a Lei Geral de Proteção de Dados (LGPD) também se aplica ao tratamento de dados pessoais no contexto penal. A LGPD estabelece

diretrizes para a proteção de dados pessoais e inclui disposições que afetam processos judiciais, incluindo os penais. Embora a LGPD não tenha um capítulo específico para o processo penal, suas normas gerais são aplicáveis, garantindo que os dados pessoais sejam tratados com respeito à privacidade e à segurança. Ambos os países têm como objetivo proteger os direitos fundamentais dos indivíduos, garantindo que o tratamento de dados pessoais no contexto penal seja realizado de forma justa e segura.

Antes de partimos para Capítulo seguinte, é necessário que se façam algumas observações, no sentido de reforçar o que se busca com o presente estudo. Embora os entendimentos do Tribunal Constitucional Portugal e do Superior Tribunal de Justiça mencionados acima sejam de extrema importância para a análise do direito à privacidade e da validade das provas digitais, o foco deste trabalho é a utilização dos bancos de dados da Polícia Civil do Distrito Federal e das Polícias Judiciárias Brasileiras, de modo que a cadeia de custódia seja respeitada, garantindo a todos os acusados o devido processo legal e os recursos a eles inerentes, como a ampla defesa, o contraditório e o direito à prova lícita[302].

5 ANTEPROJETO DE LEI DE PROTEÇÃO DE DADOS PARA A SEGURANÇA PÚBLICA E PERSECUÇÃO PENAL – "LGPD PENAL"

No mês de novembro de 2019, o Presidente da Câmara dos Deputados determinou a criação de uma comissão de Juristas, que recebeu a missão de elaborar um Anteprojeto de lei para os casos de tratamento de dados pessoais relacionados à segurança pública e persecução penal. A comissão foi composta por 15 membros[303] e contou com a participação de diversos outros especialistas no tema. Um seminário internacional chegou a ser organizado no ano de 2020, para discutir as principais questões que gravitam em torno das investigações criminais diante das garantias constitucionais.

---

[302]Superior Tribunal de Justiça. A cadeia de custódia no processo penal: do Pacote Anticrime à jurisprudência do STJ. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/23042023-A-cadeia-de-custodia-no-processo-penal-do-Pacote-Anticrime-a-jurisprudencia-do-STJ.aspx. Acesso em 05 de nov. 2024.

[303]Superior Tribunal de Justiça. Comissão entrega à Câmara anteprojeto sobre tratamento de dados pessoais na área criminal. Instituída em novembro do ano passado pelo presidente da Câmara dos Deputados, a comissão de juristas teve, além dos ministros Nefi Cordeiro (presidente) e Antonio Saldanha Palheiro (vice-presidente), os seguintes membros: Laura Schertel Mendes (relatora), Pedro Ivo Velloso (secretário), Danilo Doneda, Davi Tangerino, Eduardo Queiroz, Heloisa Estellita, Humberto Fabretti, Ingo Sarlet, Jacqueline Abreu, Jorge Octávio Lavocat Galvão, Juliana Abrusio, Tércio Sampaio Ferraz Júnior e Vladimir Aras. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx Acesso em 05 de nov. 2024.

Conforme será visto adiante, ocorreram diversas opiniões sobre o tema, para decidir sobre a construção de uma lei comum que não inviabilizasse o tratamento de dados nas atividades policiais, mas que garantisse direitos fundamentais, criando uma situação de confiança entre Estado e cidadão.

A par disso, um ano depois de sua formação, a Comissão apresentou à Presidência da Câmara um Anteprojeto de Lei sobre o tema. O Anteprojeto ofereceu balizas e parâmetros para operações de tratamentos de dados pessoais no âmbito de atividades de segurança pública e de persecução criminal, equilibrando tanto a proteção do titular contra o mau uso e abusos como acesso de autoridades a todo potencial de ferramentas e plataformas modernas para segurança pública e investigações.

Ainda de acordo com o que consta no Anteprojeto, existe atualmente uma enorme deficiência na proteção de dados dos cidadãos, uma vez que não há uma regulamentação geral sobre a licitude, a transparência ou a segurança do tratamento de dados em matéria penal, tampouco direitos estabelecidos ou requisitos para a utilização de novas tecnologias que possibilitam um grau de vigilância e monitoramento impensável há alguns anos. A ausência de regulamentação sobre o tema gera uma assimetria de poder muito grande entre o Estado e o cidadão. O titular de dados, ou investigado, é deixado sem garantias normativas mínimas e mecanismos institucionais aplicáveis para resguardar o seu direito fundamental à proteção de dados.

Cabe salientar que o objetivo deste trabalho não é analisar cada um dos Artigos do Anteprojeto Penal de Dados pessoais. Apesar disso, os principais dispositivos serão abordados, para que seja possível imaginarmos como será o futuro da investigação criminal no Brasil com eventual aprovação do Anteprojeto do jeito que ele se encontra atualmente.

Várias foram as Notas Técnicas emitidas pelos mais variados órgãos depois que a Comissão de Juristas finalizou e entregou o Anteprojeto Penal de Proteção de Dados para o Presidente da Câmara dos Deputados. Algumas Notas Técnicas tiveram o objetivo de esclarecer o Anteprojeto, outras de criticá-lo. A Ação número 04/2021 da Estratégia Nacional de Combate

à Corrupção e à Lavagem de Dinheiro – ENCCLA[304], resultou na confecção de Nota Técnica contendo a avaliação, propostas de alterações, contrastando o texto do Anteprojeto com Convenções, recomendações e melhores práticas internacionais, em relação ao Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal – LGPD Penal.

No Capítulo I do Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal foi definido o seu objeto e âmbito de aplicação. Nesse contexto, a proposta define o objeto do Anteprojeto em "tratamento de dados pessoais realizados por autoridades competentes para atividades de segurança pública e de persecução penal", fazendo uma vinculação à tutela dos "direitos fundamentais de liberdade e de privacidade e ao livre desenvolvimento da personalidade da pessoa natural", demonstrando, de forma explícita, o direito tutelado pela Lei, conforme preceitua o Artigo 1º da Lei Geral de Proteção de Dados (Lei número 13.709/20180).

Apesar da simetria do Anteprojeto Penal de Proteção de Dados com a já vigente Lei Geral de Proteção de Dados, no que diz respeito à proteção da privacidade, é preciso ressaltar a necessidade de equilíbrio entre o respeito ao Direito Fundamental à proteção de dados e ao Direito à Segurança Pública, conforme será aferido em diversos pontos deste trabalho. Percebe-se no Anteprojeto a necessidade de se resguardar o interesse público no compartilhamento de dados entre autoridades estatais legalmente incumbidas das atividades de segurança pública, investigação e repressão de infrações penais e pessoas jurídicas de direito privado legalmente obrigadas a realizar esse compartilhamento.

Foi, portanto, sugerido na Nota Técnica elaborada pela ENCCLA[305] que o Artigo 1º do apresente de forma clara e sistemática a relação do Anteprojeto com o microssistema jurídico de proteção de dados estabelecido pela Lei Geral de Proteção de Dados, levando em consideração os dois objetos de tutela, e não apenas a privacidade.

A mesma preocupação descrita acima, relacionada à existência de mecanismos que permitam harmonização entre os direitos de privacidade e de proteção de dados e os meios de

[304]Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro – ENCCLA. Ação 04/2021. Disponível em: https://enccla.camara.gov.br/acoes/acoes-de-2021. Acesso em 17 de set. 2024.
[305]*Ibid.*

garantia da segurança pública e da persecução penal também estão presentes em outros dispositivos do Anteprojeto[306]. No Artigo 2º do Anteprojeto, consta que a disciplina da proteção de dados pessoais em atividades de segurança pública e persecução penal tem como fundamentos a dignidade, os direitos humanos, o livre desenvolvimento da personalidade, e o exercício da cidadania pelas pessoas naturais; a autodeterminação informativa; o respeito à vida privada e à intimidade; a liberdade de manifestação do pensamento, de expressão, de informação, de comunicação e de opinião; a presunção de inocência; confidencialidade e integridade dos sistemas informáticos pessoais; e garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal.

O Direito de Autodeterminação Informativa, considerado um dos pilares do direito à proteção de dados pessoais, deve ser observado em conjunto com os demais fundamentos, principalmente quando se debate o direito à privacidade (individual) versus o direito à segurança pública (coletivo). Diante disso, a Nota Técnica da ENCCLA[307] sugeriu a inclusão de fundamentos adicionais além dos que já existem, visando fomentar eventual ponderação entre os direitos tutelados. Foram sugeridas, portanto, as seguintes alterações: dever estatal de eficiência, por meio da previsão de mecanismos que otimizem a prevenção, investigação e repressão de infrações penais, sem incorrer em preconceitos de qualquer natureza; a proteção de direitos individuais e difusos, por meio da aplicação de sanções civis ou penais proporcionais à gravidade das violações; a observância do princípio da proibição da proteção deficiente de bens jurídicos de extração constitucional; e respeito ao direito à segurança.

A Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro[308] também sugere que, a fim de evitar a contradição entre definições existentes em um e outro ato normativo, o Anteprojeto seja reavaliado no que diz respeito aos conceitos trazidos, para que ocorra um alinhamento com o que preceitua a Lei Geral de Proteção de Dados, o que pode ser feito através de remissões.

O Anteprojeto também estabelece uma nova definição para dados sigilosos[309], que são os dados pessoais protegidos por sigilo constitucional ou legal. Tendo em vista que o conceito

---

[306] *Ibid.*
[307] *Ibid.*
[308] *Ibid.*
[309] BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Do Tratamento de Dados Pessoais Sigilosos. Art. 14. O tratamento de dados pessoais sigilosos por

sobre dado sigiloso já foi devidamente regulado, o que abrange os dados revestidos pelo sigilo fiscal e bancário por exemplo, é desnecessário que o Anteprojeto faça essa definição.

Todos os princípios, de fato, são relevantes para qualquer investigação policial, com ou sem tratamento de dado pessoais[310]. Uma observação, no entanto, precisa ser feita. Quando se fala em transparência no tratamento de dados pessoais para fins penais, depreende-se que o autor do fato deve ter acesso aos procedimentos de coleta de provas efetuados pelas polícias. A transparência no processo penal é fundamental para garantir a justiça e a confiança pública no sistema judicial. Ela envolve a abertura e a clareza em todas as etapas do processo, desde a investigação até o julgamento e a execução da sentença.

A Nota Técnica da ENCCLA definiu que o Anteprojeto agrega aos princípios referenciados na Lei Geral de Proteção de Dados o princípio da licitude[311]. A inclusão do princípio, que faz uma simples observância à própria lei, pode gerar dúvidas no que diz respeito

---

autoridades competentes somente poderá ser realizado se estiver previsto em lei e para atividades de persecução penal. §1º O acesso a dados pessoais sigilosos por meio de ferramentas de investigação e medidas cautelares de obtenção de prova deve observar a legislação especial aplicável. 2º O acesso a dados pessoais sigilosos controlados por pessoas jurídicas de direito privado será específico a pessoas investigadas e dependerá de ordem judicial prévia baseada em indícios de envolvimento dos titulares de dados afetados em infração penal e na demonstração de necessidade dos dados à investigação, na forma da lei, sem prejuízo da comunicação de operações suspeitas, nos termos do art. 11 da Lei nº 9.613. em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov. 2024.

[310]BRASIL. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. O Artigo 6º, por sua vez, menciona que as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - licitude: embasamento do tratamento de dados pessoas em hipótese legal, nos termos do Capítulo II desta Lei; II - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular sem tratamento posterior de forma incompatível com essas finalidades; III - adequação: pertinência e relevância do tratamento com os objetivos pretendidos, de acordo com o contexto do tratamento; IV - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; V - proporcionalidade: compatibilidade do tratamento com os objetivos pretendidos, de acordo com o contexto do tratamento; VI - livre acesso: garantia, aos titulares, de exatidão, clareza, relevância, e atualização dos dados, de acordo com a necessidade, e para o cumprimento da finalidade de seu tratamento; VII - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade para o comprimento da finalidade de seu tratamento; VIII - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; IX - segurança da informação: utilização de medidas técnicas e administrativas aptas a proteger dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; X - prevenção: adoção de medias para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; XI - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ou abusivos; e XII - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

[311]*Ibid.*

à licitude propriamente dita ou tipicidade dos meios de tratamento dos dados pessoais. Por esse motivo foi sugerida a supressão do inciso, com a recomendação de adoção do Caput do referido Artigo a mesma fórmula remissiva sugerida ao Artigo 5º do Anteprojeto, com referência aos princípios já enumerados na Lei Geral de Proteção de Dados.

Diante da necessidade de garantir que o Anteprojeto assegure os meios necessários à ponderação entre os direitos à autodeterminação informativa, privacidade e segurança, a leitura dos princípios deve ser realizada sob a lente do interesse público[312]. A análise dos princípios do livre acesso e da transparência devem ser respeitados, mas mitigados nas situações que eventualmente possam prejudicar o andamento de investigações criminais ou persecuções penais. Sobre o ponto específico em questão, a Nota Técnica da ENCCLA entendeu que:

> Referidos meios dizem respeito à possibilidade expressa de mitigação da abrangência de tais princípios de tal modo que a finalidade pública dessas atividades não seja prejudicada pelo acesso prematuro do investigado ou terceiros aos tratamentos de dados realizados no curso da investigação.
> Tal circunstância é semelhante à aquela já enfrentada pela Administração na interpretação do Artigo 31 da Lei número 12.527 de 2011 (Lei de Acesso à Informação) em caso de solicitação de dados pessoais utilizados em investigação preliminar (antes, portanto, de instaurado qualquer procedimento contraditório). Em referidos casos a interpretação preponderante considera tais informações de natureza "preparatória" permitindo-se desse modo a avaliação do interesse público sobre o acesso à informação demandada. O teste de interesse público nesse contexto tem como um de seus parâmetros precisamente aquele que aqui se busca prestigiar: o potencial prejuízo à legítima finalidade do processo.
> No âmbito da UE, o Regulamento 2018/1725, relativo à proteção de dados de pessoas naturais pelos órgãos e entidades da União, admite de modo expresso referidos meios de mitigação, ao dispor, em seu Artigo 25 sobre a limitação de direitos sobre o tratamento de dados pessoais quando "tal limitação respeite a essência dos direitos e das liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para salvaguardar", em especial no que tange à "prevenção, a investigação, a detecção e a repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda da segurança pública e a prevenção de ameaças à segurança pública".
> Considerando que o disposto no Artigo 20 do Anteprojeto já veicula conjunto de exceções alinhadas ao exposto, avalia-se que a referência a mencionado dispositivo em parágrafo único do Artigo 6º ou mesmo no Caput traria maior

[312]Sobre o tema, Ademar Borges alega que [...Por conta dessas múltiplas facetas, distingue-se o interesse verdadeiramente público (o interesse público *primário*) do interesse do Estado e das demais pessoas de direito público (o interesse público *secundário*). Segundo Luís Roberto Barroso, "[o] interesse público primário é a razão de ser do Estado e sintetiza-se nos fins que cabe a ele promover: justiça, segurança e bem-estar social", e corresponde, portanto, aos "interesses de toda a sociedade". Já o interesse público secundário "*é o da pessoa jurídica de direito público que seja parte em determinada relação jurídica*", e que, em ampla medida, "pode ser identificado como o interesse do erário, que é o de maximizar a arrecadação e minimizar despesas". SARMENTO, D; BORGES, A; ADAMI, E. Parecer. FILTRAGEM CONSTITUCIONAL DOS PEDIDOS DE SUSPENSÃO DE SEGURANÇA. INTERESSE PÚBLICO PRIMÁRIO QUE TUTELA DIREITOS FUNDAMENTAIS, SOBRETUDO DOS MAIS VULNERÁVEIS. LEGITIMIDADE ATIVA DA DEFENSORIA PÚBLICA COMO *CUSTUS VULNERABILIS*. Brasil.

> clareza e segurança sobre a forma como tais princípios deverão ser observados[313].

No Artigo 7º do Anteprojeto consta que no tratamento de dados pessoais, o responsável pelo tratamento deve, na medida do possível, fazer uma distinção clara entre as diferentes categorias de titulares dos dados. Aqui, a Comissão que elaborou o Anteprojeto criou categorias de pessoas que eventualmente tenham seus dados pessoais tratados. A divisão foi feita da seguinte forma:

> I - pessoas em relação às quais existem indícios suficientes de que cometeram uma infração penal;
> II - pessoas em relação às quais existem indícios suficientes de que estão prestes a cometer uma infração penal;
> III - pessoas processadas pela prática de infração penal; IV - pessoas condenadas definitivamente pela prática de infração penal;
> V - vítimas de uma infração penal ou pessoas em relação às quais certos fatos indicam que podem ser vítimas de uma infração penal; e
> VI - outras pessoas, tais como testemunhas, pessoas que possam fornecer informações ou contatos associados das pessoas referidas nos incisos I a V.

Sobre o Artigo 8º, a redação que consta no Anteprojeto não foi muito clara quando menciona que no tratamento de dados o responsável deve distinguir, na medida do possível, os dados pessoais baseados em fatos dos dados pessoais baseados em avaliações pessoais. O dispositivo deve ser retirado do pelas seguintes razões: A expressão "na medida do possível" é sinônimo de "dentro de um determinado limite". Qual seria, portanto, o limite? Não é possível fazer um juízo de valor dos dados pessoais baseados em fatos e dos dados pessoais baseados em avaliações pessoais. A única obrigação de um operador de dados pessoais é o cumprimento do tratamento de dados que foi determinado pelo controlador de dados pessoais.

No Parágrafo Único do Artigo 8º, foi previsto que caso o responsável verifique que tratou dados pessoais inexatos ou que tratou dados pessoais de forma ilícita, o destinatário deve ser informado tão logo seja possível e os dados pessoais devem ser retificados ou apagados. Da forma como consta na redação, parece que não existirão mecanismos que façam o monitoramento do tratamento dos dados pessoais. Apesar da boa-fé do controlador, encarregado ou operador, é preciso que seja implementado um instrumento capaz de detectar a má utilização desses dados. A exclusão dos dados pessoais ou a comunicação do tratamento dos dados aos titulares pode colocar em risco toda uma investigação criminal[314].

---

[313]*Ibid.*

[314]BRASIL. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Art. 8º No tratamento de dados, o responsável deve distinguir, na medida do possível, os dados pessoais baseados em fatos

O Anteprojeto estabeleceu apenas três requisitos para o tratamento de dados pessoais nas atividades de segurança pública e de persecução penal. São eles: I – quando necessário para o cumprimento de atribuição legal de autoridade competente, na persecução do interesse público, na forma da lei ou regulamento, observados os princípios gerais de proteção, os direitos do titular e os requisitos do Capítulo VI desta Lei; II -para execução de políticas públicas previstas em lei, na forma do regulamento, observados os princípios gerais de proteção, os direitos do titular e os requisitos do Capítulo VI desta Lei; e III – para proteção da vida ou da incolumidade física do titular ou de terceiros, contra perigo concreto e iminente.

Os requisitos em questão estão alinhados com o tema aqui debatido, porque as investigações policiais são de interesse público. Eventual monitoramento da utilização dos bancos de dados das polícias judiciárias brasileiras, pode ser feito através da execução de políticas públicas e, na grande maioria dos casos, nos casos de investigações policiais que visem a proteção da vida ou da incolumidade física do titular ou de terceiros, contra perigo concreto e iminente.

É preciso observar, no entanto, que a ideia de "supremacia do interesse público" não deve ser utilizada para se sobrepor a outros direitos fundamentais. Nas palavras de Gustavo Binenbojm, a noção tradicional de "supremacia do interesse público" é incompatível com o constitucionalismo democrático". Para o autor, isso se deve porque existem posições jurídicas individuais irredutíveis, relacionadas ao conteúdo essencial dos direitos fundamentais e à dignidade da pessoa humana. Além disso, existe a primazia *prima facie* dos direitos fundamentais sobre metas coletivas, ainda que o sistema constitucional admita a ponderação desses valores. Por fim, a noção de interesse público é polivalente, de modo a abarcar tanto a preservação de direitos fundamentais quanto a persecução de objetivos coletivos – propósitos que sem encontram, com grande frequência, conjugados e imbricados[315].

Outro ponto importante do Anteprojeto diz respeito ao registro das atividades de tratamento. Consta no referido Anteprojeto que o controlador e o operador devem manter

dos dados pessoais baseados em avaliações pessoais. Parágrafo único. Caso o responsável verifique que tratou dados pessoais inexatos ou que tratou dados pessoais de forma ilícita, o destinatário deve ser informado tão logo seja possível e os dados pessoais devem ser retificados ou apagados.

[315]BINENBOJM, G. Ainda a supremacia do interesse público. Revista da EMERJ, v. 21, n. 3, p. 238, set./dez.2019.

registro das operações de tratamento de dados pessoais que realizarem. Além disso, o controlador deve manter registro de todas as categorias de atividades de tratamento sob sua responsabilidade, devendo conter o nome e o contato de operadores, co-controladores e encarregados; a descrição das categorias de titulares de dados e das categorias de dados pessoais; as finalidades das operações de tratamento; a indicação da base legal do tratamento; a origem da coleta ou recebimento dos dados e as categorias de destinatários com quais os dados pessoais foram compartilhados; a utilização de técnicas e políticas de agrupamento de titulares em perfis, se for o caso; as categorias de transferências de dados pessoais para um país terceiro ou para uma organização internacional se for o caso disso; os prazos de conservação das diferentes categorias de dados pessoais ou os procedimentos previstos para revisão periódica da necessidade de conservação; uma descrição geral das medidas técnicas e organizativas em matéria de segurança pública referidas no capítulo V; e os pedidos apresentados pelos titulares dos dados e a respectiva tramitação, bem como as decisões do responsável pelo tratamento com a correspondente fundamentação[316].

No que diz respeito aos dados sigilosos, o Poder Judiciário, o Ministério Público, as Polícias e todos os demais agentes de tratamento que tenham acesso aos dados, deverão adotar as medidas de segurança para garantia do sigilo decretado judicialmente em todas as fases e instâncias processuais, principalmente quando crianças ou adolescentes estiverem envolvidos na investigação ou quando se tratar de crimes contra a dignidade sexual[317].

---

[316]BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Art. 32. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem. Art. 33. O controlador deve manter registro de todas as categorias de atividades de tratamento sob a sua responsabilidade, o qual conterá: I – o nome e os contatos de operadores, co-controladores e encarregados; II – a descrição das categorias de titulares de dados e das categorias de dados pessoais; III – as finalidades das operações de tratamento; IV – a indicação da base legal do tratamento; V – a origem da coleta ou recebimento dos dados e as categorias de destinatários com quais os dados pessoais foram compartilhados; VI – a utilização de técnicas e políticas de agrupamento de titulares em perfis, se for o caso; VII – as categorias de transferências de dados pessoais para um país terceiro ou para uma organização internacional, se for caso disso; VIII – os prazos de conservação das diferentes categorias de dados pessoais ou os procedimentos previstos para revisão periódica da necessidade de conservação; IX – uma descrição geral das medidas técnicas e organizativas em matéria de segurança referidas no capítulo V; e X – os pedidos apresentados pelos titulares dos dados e a respectiva tramitação, bem como as decisões do responsável pelo tratamento com a correspondente fundamentação. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov. 2024.

[317]BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Art. 36. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-

O Capítulo II – Do Tratamento de Dados Pessoas foi direcionado para regular o tratamento de dados pessoais para as atividades de segurança pública e persecução penal. Talvez aqui estejamos diante de um dos maiores problemas do atual Anteprojeto, porque seus dispositivos, além de restringirem ao máximo as possibilidades de tratamento e acesso a dados por autoridades policiais e de segurança pública, também estabelece uma série de condições que em muitos casos poderá obstruir as atividades de persecução penal e segurança pública, o que pode gerar prejuízos tanto para a prevenção de crimes quanto para a identificação de autores de delitos.

Para a Nota Técnica da ENCCLA[318], significa que o Anteprojeto retarda a ação policial e vai de encontro à eficiência e à celeridade das atividades de polícia judiciária, na medida em que burocratiza a atividade polícia, criando figuras, procedimentos, controles e ritos que, no afã de proteger os direitos à intimidade e à privacidade, acabam por ter efeitos negativos e contrários a ações necessárias para prevenir e reprimir diversos crimes, principalmente aqueles que afetam outros direitos fundamentais igualmente basilares ao Estado de Direito.

Da mesma forma, também foi compreendido como uma barreira ao sucesso das investigações a obrigação de que a requisição de dados descreva concretamente a sua adequação, necessidade e proporcionalidade ao caso concreto (Artigo 11) assim como a necessidade de especificação de quando deverá ser feita a notificação do acesso pelo titular aos dados que foram tratados (Artigo 11, § 4º).

O entendimento vai de encontro ao que preceitua o ordenamento jurídico brasileiro, que não faz as mesmas exigências do Anteprojeto e que já possui algumas normas de compartilhamento, acesso e requisição de dados pessoais e informações, tais como a Lei de Interceptação Telefônica (Lei número 9.296/1996); Lei de Identificação Criminal (Lei número 12.037/2009), que cuida do registro de dados pessoais, inclusive perfis genéticos, para uso em investigações criminais; os Artigos 17-B e 17-E da Lei de Lavagem de Dinheiro (Lei número 9.613/1998); os Artigos 15 a 17 da Lei do Crime Organizado (Lei número 12.850/2013); e os

documentos/DADOSAnteprojetocomissaoprotecaodadosseguranca persecucaoFINAL.pdf. Acesso em 05 de nov. 2024.

[318] *Ibid.*

Artigos 13-A e 13-B do Código de Processo Penal, que disciplinam o acesso a dados cadastrais e metadados para uso em investigações criminais sobre tráfico de pessoas.

A Nota Técnica ressalta que o ideal seria que o tratamento e o compartilhamento de dados fossem mantidos dentro das hipóteses legais já existentes, conforme previsto nas legislações acima, ou sejam incólumes com o intuito de garantir ao Estado o cumprimento de seu dever de zelar pela ordem pública[319]. Outro aspecto que deve ser destacado é que a análise de impacto regulatório para dados pessoais sensíveis prevista no Artigo 13 não encontra semelhança ou guarida na própria LGPD brasileira ou na Diretiva 680/2016 (UE), que serviu de base para o Anteprojeto[320].

A avaliação do descarte prevista no Artigo 15 ou o término do tratamento de dados pessoais deve ser realizada de forma que seja aferida a possibilidade do seu aproveitamento além da finalidade específica, desde que seja restrita para fins de prevenção ou repressão de crimes, o que abrange a persecução penal ou a segurança pública[321]. A sugestão, inclusive, está prevista no regulamento que serviu de base para o nosso Anteprojeto (Diretiva 680/2016 (UE), conforme consta no Artigo 27[322].

O dispositivo europeu, portanto, procurou racionalizar a atividade estatal, evitando a coleta do mesmo dado pessoal para a utilização em outras esferas sancionatórias, conforme preceitua o dispositivo da Diretiva 680/2016 (UE). Outro aspecto que deve ser destacado é que

---

[319] *Ibid.*

[320] BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Art. 13. O tratamento de dados pessoais sensíveis somente poderá ser realizado por autoridades competentes se estiver previsto em lei, observadas as salvaguardas desta Lei. Parágrafo único. A autoridade competente responsável pelo tratamento de dados pessoais sensíveis elaborará relatório de impacto à proteção de dados pessoais e informará o Conselho Nacional de Justiça. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov. 2024.

[321] BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Art. 15. A autoridade competente deve manter procedimentos para evitar que, no curso de suas atividades, obtenha e trate dados pessoais irrelevantes ou excessivos à finalidade da operação de tratamento, devendo descartá-los imediatamente. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov. 2024.

[322] General Data Protection Regulation. Artigo 27. Para efeitos de prevenção, investigação ou repressão de infrações penais, é necessário que as autoridades competentes tratem os dados pessoais, recolhidos no contexto da prevenção, investigação, deteção ou repressão de infrações penais específicas para além desse contexto, a fim de obter uma melhor compreensão das atividades criminais e de estabelecer ligações entre as diferentes infrações penais detetadas. Disponível em: https://gdpr-info.eu/. Acesso em 27 de nov. 2024.

no tratamento de dados pessoais, além da produção de documentos, também é preciso observar o arquivamento de forma adequada, já regulamentado em nosso ordenamento jurídico brasileiro[323].

Não se pode, portanto, deixar de observar o Artigo 23, Inciso III da Constituição Federal de 1988, quando menciona que é competência comum da União, dos Estados, do Distrito Federal e dos Municípios proteger os documentos, as obras e outros bens de valor histórico, artístico e cultural, os monumentos, as paisagens naturais notáveis e os sítios arqueológicos. Além da previsão Constitucional, também existe a Lei número 8.159/1991[324], que dispõe sobre a política nacional de arquivos públicos e privados. Consta no Artigo 1º da referida legislação que é dever do Poder Público a gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação, o que reforça a importância e a necessidade de armazenamento dos dados pessoais utilizados para fins de persecução penal e segurança pública, uma vez que o seu descarte após o tratamento, conforme preceitua o Anteprojeto, pode prejudicar futuras investigações criminais e pode atrapalhar o serviço de inteligência policial, atividade que visa prevenir, identificar, neutralizar a obstruir ações criminosas.

O Artigo 10 do Anteprojeto faz uma previsão idêntica ao § 2º do Artigo 4º da Lei geral de Proteção de Dados, ao mencionar que é vedado o tratamento de dados pessoais para atividades de segurança pública e de persecução penal por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico ao Conselho Nacional de Justiça, sem prejuízo de outras exigências legais[325].

---

[323]BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Art. 5º Para os fins desta Lei, considera-se: XI - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, uso compartilhado, processamento, *arquivamento*, *armazenamento*, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov.

[324]BRASIL. Lei número 8.159/1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Disponível em: https://www2.camara.leg.br/legin/fed/lei/1991/lei-8159-8-janeiro-1991-322180-norma-pl.html. Acesso em 19 de set. 2024.

[325]BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Art. 10. É vedado o tratamento de dados pessoais para atividades de segurança pública e de persecução penal por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico ao Conselho Nacional de Justiça, sem prejuízo de outras exigências legais. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov.

O Artigo sofreu severas críticas da Nota Técnica da ENCCLA[326], porque uma das matérias-primas básicas de atividades relacionadas tanto à persecução penal quando à segurança pública é a busca, coleta e análise de dados que, em alguns casos, dependem da colaboração de pessoas jurídicas de direito privado.

Tendo em vista tantas restrições e obrigações, é temerária a vedação ao tratamento de dados pessoais por uma pessoa jurídica de direito privado, sem a tutela de pessoa jurídica de direito público, para fins de segurança pública ou de investigação e repressão a infrações penais, tendo em vista que há várias pessoas jurídicas de direito privado que podem subsidiar posterior repressão de infrações penais ou atividades de segurança pública, tendo em vista sua sujeição legal à coleta e compartilhamento de dados pessoais com autoridades de direito público, tanto de seus clientes como aqueles disponíveis publicamente, sempre com o fim de colaborar com a persecução criminal e a garantida da segurança pública.

Por fim, as entidades privadas detentoras de dados pessoais (cadastrais, bancários, telefônicos e telemáticos por exemplo), quando atende ordens judiciais já realizam tratamento de dados para que possam ser disponibilizados.

A vedação sugerida no Anteprojeto pode obstruir investigações internas e reportes realizados por pessoas jurídicas de direito privado para coleta e compartilhamento de dados de clientes ou pessoas envolvidas em atividades criminosas, o que também inclui as vítimas de eventuais crimes. As apurações e reportes são geralmente realizados por intermédio de atividades de gerenciamento de riscos de entidades privadas, previamente à instauração de inquéritos ou durante procedimentos de autoridades policiais e judiciárias competentes. Os atos de colaboração são fundamentais para o sucesso dos procedimentos, para o exercício regular de direitos por parte das vítimas e para instrução criminal adequada, permitindo a coleta de materiais que identifique autores de delitos.

A Nota Técnica da ENCCLA[327] reforça, ainda, que o dispositivo do Anteprojeto pode ter sua constitucionalidade questionada por ir de encontro aos princípios gerais da ordem econômica na Constituição Federal, como o da livre iniciativa e da livre concorrência, já que

[326] *Ibid.*
[327] *Ibid.*

no campo privado em onde são desenvolvidas as maiores gamas de inovações tecnológicas, como softwares de tratamento de dados que são cada vez mais utilizados nas atividades de persecução penal e segurança pública. Entendeu-se, portanto, que o melhor cenário seria a elaboração de critérios orientadores, ainda não definidos, a serem observados por pessoais jurídicas de direito privado, para que possam fazer o tratamento de dados em atividades de persecução penal.

O Capítulo III do Anteprojeto de Lei de Proteção de Dados para segurança Pública e Persecução Penal regula os princípios da autodeterminação informativa e da transparência, garantindo ao titular a prestação de informações e a concessão de acesso a dados pessoais por autoridades de segurança pública e persecução penal. Assegura, ainda, que toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade. O Anteprojeto, porém, faz uma ressalva ao afirmar que qualquer restrição a estes direitos deverá ser proporcional, limitada no tempo e necessária para finalidades de atividades de segurança pública e de persecução penal[328].

O Artigo 19 do Anteprojeto preceitua que o titular de dados pessoais de direito de obter do controlador, em relação aos dados do titular por ele tratados, mediante requisição, a conformação da existência de tratamento, o acesso aos dados, a correção de dados incompletos inexatos ou desatualizados, a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o Anteprojeto, bem como informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados[329].

---

[328]BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. CAPÍTULO III. DOS DIREITOS DO TITULAR. Art. 18. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei, sendo que qualquer restrição a estes direitos deverá ser proporcional, limitada no tempo e necessária para finalidades de atividades de segurança pública e de persecução penal. Art. 19. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; e V - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov.

[329]*Ibid.*

Os Artigos 27 e 28 procuram assegurar aos seus titulares de dados o exercício de apresentar denúncias anônimas por violação ao tratamento de dados e a possibilidade de defesa de seus direitos de maneira individual ou coletiva, o que demonstra harmonia com o que preceitua a nossa Constituição Federal. O Artigo 20, no entanto, afirma que a prestação de informações e a concessão e acesso a dados poder ser adiada, limitada, ou recusada para evitar prejuízo às investigações, inquéritos ou processos judiciais; evitar prejuízo à prevenção, detecção, investigação ou repressão de infrações penais ou para a execução de sanções penais; para proteger a segurança do Estado ou a Defesa Nacional; ou para proteger os direitos e garantias de terceiros[330].

A Nota Técnica da ENCCLA[331] fez mais uma observação relevante, quando ressaltou que no contexto do dispositivo em questão seria necessário que o Anteprojeto abrangesse outras hipóteses de adiamento, limitação ou recusa do acesso aos dados pessoais em tratamento, quando houver dúvidas sobre a identidade do solicitante e com a finalidade de proteger atividades de segurança pública.

O Artigo 24 do Anteprojeto prevê a necessidade de prévia autorização de órgão externo como condição necessária para a adoção de tratamento automatizado de dados pessoais[332]. A exigência é proporcional e cria uma espécie de mecanismo de controle para o tratamento de dados nas atividades de prevenção, detecção, investigação e repressão penal, passando a exigir que a atividade de investigação elabore relatório de impacto de proteção de dados pessoais à luz das circunstâncias concretas do tratamento em questão[333].

---

[330]BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Art. 27. O controlador deve assegurar o direito do titular de dados de realizar denúncias confidenciais a respeito de violações a esta Lei. Art. 28. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov.

[331]*Ibid.*

[332]BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Art. 24. As decisões tomadas com base no tratamento automatizado de dados que ensejem um elevado risco para os direitos fundamentais do titular ou que possam acarretar medidas coercitivas ou restritivas de direitos deverão ser precedidas de autorização do Conselho Nacional de Justiça e autorizadas por lei, que estabeleça as garantias adequadas para os direitos e liberdades do titular, observado o disposto nos artigos 25 e 44. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov.

[333]BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-

Apenas a título de exemplo, conforme já foi mencionado em outro ponto deste trabalho, diversos órgãos de persecução penal investem em softwares focados no tratamento automatizados de dados, o que abrande os dados bancários, telefônicos, fiscais e telemáticos[334]. Caso o dispositivo seja aprovado da forma como está, porém, pode ser criado um obstáculo para o auxílio tecnológico no tratamento de dados pessoais. Além disso, é possível que seja aumentado o abismo ainda entre os órgãos de persecução penal e o crime organizado, que cada vez mais utiliza recursos tecnológicos para a prática de crimes.

O Capítulo IV do Anteprojeto traz a obrigação da elaboração de impacto à proteção de dados pessoais para tratamento de dados pessoais sensíveis, sigilosos ou que apresentem elevado risco aos direitos, liberdades ou garantias dos titulares de dados pessoais. O controlador e o operador deverão manter registros de todas a operações de tratamento de dados pessoais que realizarem.

O controlador e o operador também deverão manter registro de todas as categorias de atividades de tratamento, devendo conter nos relatórios: os nomes e os contatos dos controladores, operadores e encarregados; a descrição das categorias de titulares de dados e das categorias de dados pessoais; as finalidades das operações de tratamento; a indicação de base legal do tratamento; a origem da coleta ou recebimento dos dados e as categorias de destinatários com os quais os dados foram compartilhados; a utilização de técnicas e políticas de agrupamento de titulares em perfis, se for o caso; as categorias de transparência de dados pessoais para um país terceiro ou para uma organização internacional, se for o caso; os prazos de conservação das diferentes categorias de dados pessoais ou procedimentos previstos para revisão periódica da necessidade de conservação; descrição geral das medidas técnicas e organizativas em matéria de segurança; e os pedidos apresentados pelos titulares dos dados e a respectiva tramitação, bem como as decisões do responsável pelo tratamento com a correspondente fundamentação[335].

---

legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov.

[334]Polícia Civil do Distrito Federal. Emenda parlamentar viabiliza aquisição de supercomputador para a PCDF. Disponível em: https://www.pcdf.df.gov.br/noticias/12781/emenda-parlamentar-viabiliza-aquisicao-de-supercomputador-para-a-pcdf. Acesso em 06 de nov. 2024.

[335]BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Registros das atividades de tratamento Art. 32. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem. Art. 33. O controlador deve manter registro de todas as categorias de atividades de tratamento sob a sua responsabilidade, o qual conterá: I – o nome e os contatos de

O Anteprojeto, portanto, estabeleceu as diretrizes necessárias para a implementação de uma espécie de rastreamento do tratamento de dados pessoais utilizados para fins de segurança pública e persecução penal. Na prática da atividade policial, as sugestões serão importantes para evitar que dados pessoais sejam utilizados para finalidades que não estejam previstas em lei. Um dos objetivos deste trabalho, inclusive, é justamente demonstrar, através da análise de protocolo na Polícia Civil do Distrito Federal, a necessidade da elaboração de uma lei que autorize a implementação de um modelo que permita a utilização dos dados que constam nos bancos de dados das polícias judiciárias brasileiras. O registro de todas as categorias de atividades de tratamento nas polícias, através dos relatórios, será utilizado, em um futuro próximo, para instruir processos judiciais.

O Capítulo V do Anteprojeto, por sua vez, aborda a segurança e o sigilo dos dados pessoais, tema de fundamental importância para a investigação criminal. A redação do Artigo 36 do Anteprojeto preceitua que os agentes de tratamento devem adotar medidas de segurança, técnicas administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito[336].

---

operadores, co-controladores e encarregados; II – a descrição das categorias de titulares de dados e das categorias de dados pessoais; III – as finalidades das operações de tratamento; IV – a indicação da base legal do tratamento; V – a origem da coleta ou recebimento dos dados e as categorias de destinatários com quais os dados pessoais foram compartilhados; VI – a utilização de técnicas e políticas de agrupamento de titulares em perfis, se for o caso; VII – as categorias de transferências de dados pessoais para um país terceiro ou para uma organização internacional, se for caso disso; VIII – os prazos de conservação das diferentes categorias de dados pessoais ou os procedimentos previstos para revisão periódica da necessidade de conservação; IX – uma descrição geral das medidas técnicas e organizativas em matéria de segurança referidas no capítulo V; e X – os pedidos apresentados pelos titulares dos dados e a respectiva tramitação, bem como as decisões do responsável pelo tratamento com a correspondente fundamentação. Art. 34. Controladores e operadores devem conservar em sistemas de tratamento automatizado registros cronológicos das seguintes operações de tratamento: de coleta, alteração, consulta, acesso, divulgação, transferências, interconexão, apagamento. § 1º Os registos cronológicos das operações de consulta e de divulgação devem permitir determinar o motivo, a data e a hora dessas operações, a identificação da pessoa que consultou ou divulgou dados pessoais e, sempre que possível, a identidade dos destinatários desses dados pessoais. § 2º Os registos cronológicos, cuja integridade e cuja reserva devem ser observadas pelos controladores e operadores, serão mantidos por no mínimo 5 anos e poderão ser utilizados para efeitos de verificação da licitude do tratamento, controle administrativo, exercício do poder disciplinar, garantia da integridade e segurança dos dados pessoais, análise pelo Conselho Nacional de Justiça e instrução de processos penais, inclusive a pedido da defesa. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov.

[336]BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Art. 36. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. § 1º O Conselho Nacional de Justiça poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da

Aqui, a Nota Técnica da ENCCLA entendeu como destaque a necessidade de compatibilizar o prazo para comunicar incidente de segurança, previsto no Artigo 38, a no mínimo o mesmo prazo previsto na Lei Geral de Proteção de Dados, de forma a não conferir tratamento maus restritivo à ocorrência de incidente de segurança em relação às autoridades competentes para as atividades de segurança e de persecução penal[337].

Outro ponto que merece destaque é que a redação do § 3º do Artigo 39 do Anteprojeto diz que nos autos de investigação e processo penal que tiverem por objeto crimes contra a dignidade sexual, os elementos identificadores dos ofendidos serão protegidos em todas as fases e instâncias processuais, independente da decretação de sigilo do processo. Com o intuito de afastar interpretações jurídicas equivocadas, é preciso que a redação seja corrigida para que o termo "ofendidos" seja substituído por "envolvidos" o que abrange o autor, a vítima e as testemunhas[338].

---

tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do artigo 6º desta Lei. § 2º Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término. § 3º As medidas de que trata o caput devem ser adotadas com as seguintes finalidades: I - controle de acesso ao equipamento: impedir o acesso de pessoas não autorizadas ao equipamento utilizado para o tratamento; II - controle de suporte de dados: impedir que os suportes de dados sejam lidos, copiados, alterados ou retirados sem autorização; III - controle da conservação: impedir a introdução não autorizada de dados pessoais, bem como qualquer inspeção, alteração ou apagamento não autorizados de dados pessoais conservados; IV - controle dos utilizadores: impedir que os sistemas de tratamento automatizado sejam utilizados por pessoas não autorizadas por meio de equipamento de comunicação de dados; V - controle do acesso aos dados: assegurar que as pessoas autorizadas a utilizar um sistema de tratamento automatizado só tenham acesso aos dados pessoais abrangidos pela sua autorização de acesso; VI - controle da comunicação: assegurar que possa ser verificado e determinado a organismos os dados pessoais que foram ou podem ser transmitidos ou facultados utilizando equipamento de comunicação de dados; VII - controle da inserção: assegurar que possa ser verificado e determinado a posteriori quais os dados pessoais introduzidos nos sistemas de tratamento automatizado, quando e por quem; VIII - controle do transporte: impedir que, durante as transferências de dados pessoais ou o transporte de suportes de dados, os dados pessoais possam ser lidos, copiados, alterados ou suprimidos sem autorização; IX - recuperação: assegurar que os sistemas utilizados possam ser restaurados em caso de interrupção; e X - assegurar que as funções do sistema funcionem, que os erros de funcionamento sejam assinalados (fiabilidade) e que os dados pessoais conservados não possam ser falseados por um mau funcionamento do sistema. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov.

[337] *Ibid.*

[338] BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Art. 39. O tratamento de registros criminais deverá atender aos princípios e fundamentos desta lei, em especial a presunção da inocência e a finalidade de integração social do condenado. § 1º O Poder Judiciário, o Ministério Público, as Polícias e todos os demais agentes de tratamento que tenham acesso a autos sigilosos deverão adotar as medidas de segurança para garantia do sigilo decretado judicialmente em todas as fases e instâncias processuais. § 2º Nos autos de investigação e nos processos relativos a atos infracionais, os elementos identificadores das crianças ou adolescentes envolvidos serão protegidos em todas as fases e instâncias processuais, independentemente da decretação de sigilo do processo. § 3º Nos autos de investigação e processo penal que tiverem por objeto crimes contra a dignidade sexual, os elementos identificadores dos ofendidos serão protegidos em todas as fases e instâncias processuais, independentemente da decretação de sigilo do processo.

O Capítulo VI do Anteprojeto aborda a questão do acesso à informação e transparência, ao afirmar que as autoridades competentes informarão as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a base legal, a finalidade, os objetivos específicos, os procedimentos e as práticas utilizadas para a execução dessas atividades.

Nos Artigos 40 e 41, o Anteprojeto pretendeu disciplinar o acesso à informação e transparência, matérias exaustivamente disciplinadas na Lei número 12.527/2011 (Lei de Acesso à Informação). A Nota Técnica da ENCCLA[339] fez uma crítica ao Capítulo, sob a alegação de que o Anteprojeto não deveria tratar sobre o acesso à informação e à transparência, sendo suficiente para a proteção de dados pessoais e para a promoção do direito à segurança pública e à persecução penal eficiente à legislação processual penal e à Lei de Acesso à Informação[340].

Da forma como foi previsto no Anteprojeto, o tema causaria embaraços prejudiciais para às atividades de segurança pública, investigação e persecução penal, pela própria natureza

Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov.

[339] *Ibid.*

[340][340] BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Art. 40. As autoridades competentes informarão as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a base legal, a finalidade, os objetivos específicos, os procedimentos e as práticas utilizadas para a execução dessas atividades. § 1º As informações a que se refere este artigo serão pormenorizadas em lei ou regulamento, conforme a base legal, observadas as normas do Capítulo II; § 2º O acesso facilitado às informações sobre o tratamento de dados se dará em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, de forma clara, adequada e ostensiva, devendo incluir informações previstas em regulamentação para o atendimento do princípio do livre acesso, sobre: I - finalidade específica do tratamento; II - forma, escopo e duração do tratamento; III - políticas de retenção, descarte e acesso; IV- identificação do controlador; V - informações de contato do controlador; VI - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VII - responsabilidades dos agentes que realizarão o tratamento; e VIII - direitos do titular, com menção explícita aos direitos contidos nesta Lei. § 3º O Conselho Nacional de Justiça poderá dispor sobre as formas de publicidade das operações de tratamento, especialmente tendo em vista a garantia da segurança pública e atividades de repressão, investigação e persecução de infrações penais e execução da pena. Art. 41. A autoridade máxima de cada autoridade competente publicará anualmente em seu sítio na internet relatórios estatísticos de requisição de dados pessoais sigilosos para atividades de persecução penal, contendo: I - o número de pedidos realizados; II - a natureza dos dados solicitados; III - as categorias de pessoas jurídicas de direito privado aos quais os dados foram requeridos; IV - quando o dado for protegido por reserva de jurisdição, o número de pedidos deferidos e o número de pedidos indeferidos judicialmente à luz dos pedidos totais realizados; e V - o número de titulares afetados por tais solicitações. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov.

dessas atividades, que exigem sigilo no tratamento dos dados no curso de investigações criminais.

O § 3º do Artigo 40 do Anteprojeto, por sua vez, preceitua que o Conselho Nacional de Justiça poderá dispor sobre as formas de publicidade das operações de tratamento, especialmente tendo em vista a garantia da segurança pública e atividades de repressão, investigação e persecução de infrações penais e execução da pena[341].

O Capítulo VII do Anteprojeto aborda as tecnologias de monitoramento e tratamento de dados de elevado risco, ao afirmar que a utilização de tecnologias de monitoramento ou o tratamento de dados pessoais que representem elevado risco para direitos, liberdades e garantias dos titulares dos dados por autoridades competentes dependerá de previsão legal específica que estabeleça garantias aos direitos dos titulares e seja precedida de relatório de impacto de vigilância.

Os dispositivos do Capítulo VII buscam disciplinar a utilização de tecnologias de monitoramento ou o tratamento de dados pessoais que representem grau elevado de risco para direitos, liberdades e garantias dos titulares de dados. O fato é que o Anteprojeto não definiu o que são as tecnologias de monitoramento e tratamento de dados pessoais que representem elevado risco, o que pode gerar insegurança jurídica. Outro ponto que pode obstruir o trabalho das instituições policiais foi a exigência da edição de lei específica para condicionar a utilização de novas tecnologias de monitoramento e tratamento de dados pessoais.

O Anteprojeto também apresentou possível inconstitucionalidade, porque tentou disciplinar o processo legislativo como condição necessária para a utilização de tecnologias de vigilância[342]. Conforme entendimento do Supremo Tribunal Federal, nenhuma lei pode disciplinar o processo legislativo no Brasil, pois os princípios que regem a formação de leis estão exclusivamente na Constituição Federal. O processo legislativo é regido por princípios constitucionais, que incluem o exercício do poder de iniciativa das leis. Uma lei, por exemplo, não pode impor ao chefe do Executivo o exercício compulsório do poder de iniciativa legislativa. O devido processo legislativo é um direito constitucional subjetivo dos parlamentares, que visa garantir a regularidade e legitimidade do processo de formação de atos

[341] *Ibid.*
[342] STF, MS 22690, Tribunal Pleno, Rel. Min. Celso de Mello, J, 17.04.1997, DJe 07/12/2006.

do Poder Legislativo. O que deve ser ressaltado é que essa exigência não foi prevista na Lei Geral de Proteção de Dados e na Diretiva 680/2016 (UE). Lei ordinária não é o instrumento normativo correto para disciplinar o processo legislativo, conforme preceitua o Artigo 59, § único da Constituição Federal[343].

O Artigo 43, por sua vez, vedou, no âmbito de atividades de segurança pública, a utilização de tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial[344].

Outro ponto que deve ser ressaltado é que a atividade de investigação policial é dinâmica e imediatista, não possibilitando, na maioria dos casos, que o policial tenha tempo necessário para confecção de relatório individual de impacto à proteção de dados pessoais como condição necessária para a garantia da utilização de novas tecnologias. O dispositivo pode ser retirado da proposta legislativa, porque o Artigo 29 do Anteprojeto, conforme já mencionado acima, exigiu a necessidade de elaboração de relatório de impacto à proteção de dados pessoais para o tratamento de dados pessoais sensíveis, sigilosos, ou em operações que apresentem elevado risco aos direitos, liberdades e garantias dos titulares de dados[345].

---

[343]BRASIL. Constituição Federal. Art. 59. O processo legislativo compreende a elaboração de:I - emendas à Constituição; II - leis complementares; III - leis ordinárias; IV - leis delegadas; V - medidas provisórias; VI - decretos legislativos; VII - resoluções. Parágrafo único. Lei complementar disporá sobre a elaboração, redação, alteração e consolidação das leis. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 27 de nov. 2024.

[344]BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Art. 43. No âmbito de atividades de segurança pública, é vedada a utilização de tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov.

[345]BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Art. 29. É obrigatória a elaboração de relatório de impacto à proteção de dados pessoais para tratamento de dados pessoais sensíveis, sigilosos, ou em operações que apresentem elevado risco aos direitos, liberdades e garantias dos titulares de dados. § 1º O Conselho Nacional de Justiça poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, referente a suas operações de tratamento de dados. § 2º A elaboração e apresentação de relatório de impacto à proteção de dados pessoais também poderá ser requisitada pelo Ministério Público e pela Defensoria Pública na defesa de direitos individuais ou coletivos, quando cabível no exercício de suas atribuições. § 3º Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov.

O Capítulo VIII faz uma abordagem sobre o compartilhamento de dados pessoais para fins de segurança pública e persecução penal. A redação do Artigo 45 preceitua que qualquer modalidade de uso compartilhado de dados pessoais entre autoridades competentes somente será possível com autorização legal, com autorização judicial ou no contexto de atuações conjuntas realizadas legalmente, observados os propósitos legítimos e específicos para o tratamento, os direitos do titular, bem como os fundamentos, princípios e obrigações previstos no Anteprojeto[346].

De acordo com Nota Técnica da ENCCLA, a maneira desproporcional como a proposta procura refrear o compartilhamento de dados entre as instituições e os órgãos encarregados constitucionalmente das atividades de persecução penal e segurança pública não é reproduzida na Lei Geral de Proteção de Dados e na Diretiva 680/2016 (UE), na Lei Geral de Proteção de Dados Portuguesa e na Lei Geral de Proteção de Dados Alemã[347]. Diferentemente do que consta

[346][346]BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Art. 45. Qualquer modalidade de uso compartilhado de dados pessoais entre autoridades competentes somente será possível com autorização legal, com autorização judicial ou no contexto de atuações conjuntas autorizadas legalmente, observados os propósitos legítimos e específicos para o tratamento, os direitos do titular, bem como os fundamentos, princípios e obrigações previstos nesta Lei. § 1º Ressalvadas as hipóteses legais, é vedado o compartilhamento direto e contínuo de bancos de dados que contenham dados pessoais estabelecidos no âmbito de atividades de segurança pública com órgãos responsáveis pela persecução penal, exceto: I - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei; II - para investigação ou processo criminal específico. § 2º Requisições de acesso a dados entre autoridades competentes para uso compartilhado ocorrerão de forma devidamente motivada quanto ao contexto específico do pedido, à base legal, finalidade, necessidade e proporcionalidade, devendo o registro de acesso e de uso por agentes de autoridades competentes ser mantido por período de no mínimo 5 anos. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov.

[347]Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro. Ação 04/2021. Nota Técnica contendo a avaliação, propostas de alterações, contrastando o texto do anteprojeto com Convenções, recomendações e melhores práticas internacionais, em relação ao Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal – LGPD-Penal. A maneira desproporcional como a proposta procura refrear o compartilhamento de dados entre as instituições e os órgãos encarregados constitucionalmente das atividades de persecução penal e de segurança pública não é reproduzida na própria LGPD, na Diretiva (UE) 2016/680 (artigo 45, 2), na LGPD Portuguesa (Lei n.º 59/2019, art. 43) e na Lei Federal de Proteção de Dados Alemã, de 30 de junho de 2017 (arts. 7º, 9º, 60). Aliás, ao contrário do que pretende o anteprojeto de LGPD Penal brasileira, a Diretiva (UE) 2016/680, em seu Considerando 7, destaca a necessidade de facilitar o intercâmbio de dados pessoais entre as autoridades competentes, a fim de assegurar a eficácia da cooperação judiciária em matéria penal e da cooperação policial. Os artigos 45 a 52 pretenderam disciplinar qualquer modalidade de compartilhamento de dados pessoais entre autoridades competentes e o fizeram de forma extremamente restritiva e desproporcional, deixando completamente desprotegidos o direito fundamental à segurança e a atuação eficiente das autoridades competentes para as atividades de segurança pública e persecução penal. A vingar o texto proposto no anteprojeto, restará inviabilizada, por completo, a cooperação entre agências de persecução penal e de segurança pública, tão necessária ao combate da criminalidade organizada, cibernética, violenta ou de colarinho branco, bem como fatalmente comprometidas as dimensões da prevenção e da detecção de infrações penais, ao revés, inclusive, do quanto edificado no sistema europeu - inspiração do anteprojeto - e uma necessidade da vida em sociedade. Com efeito, o tratamento de dados realizado no âmbito de atividades de segurança pública não pode, de forma alguma, obstar que os dados pessoais sejam utilizados a execução de outras missões de interesse público, para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais. Essa é a

na proposta legislativa do Anteprojeto, a Diretiva 680/2016 (UE), que em seu Artigo 7º destaca a necessidade de facilitar o intercâmbio de dados pessoais entre autoridades competentes, a fim de assegurar a eficácia da cooperação judiciária em matéria penal e cooperação policial[348].

Caso o Anteprojeto seja aprovado da forma como está, prejudicará a cooperação entre agências de persecução penal e de segurança pública, ignorando o direito fundamental à segurança pública e impossibilitando a prevenção e detecção de infrações penais, o que não ocorre com as legislações europeias sobre proteção de dados, conforme foi possível observar acima.

Focado com a realidade e a necessidade de assegurar o direito à segurança dos portugueses, a Lei Geral de Proteção de Dados portuguesa destaca de forma expressa que as

solução adotada pela Diretiva (UE) 2016/680, como se vê do artigo 4º, 2, a seguir transcrito: Artigo 4º Princípios relativos ao tratamento de dados pessoais [...] 2. É permitido o tratamento pelo mesmo ou por outro responsável pelo tratamento para as finalidades previstas no artigo 1º, nº 1, diferentes da finalidade para a qual os dados pessoais foram recolhidos, DESDE QUE: a) O responsável pelo tratamento esteja autorizado a tratar esses dados pessoais com essa finalidade, nos termos do direito da União ou dos Estados-Membros; e b) O tratamento seja necessário e proporcionado para essa outra finalidade, nos termos do direito da União ou dos Estados Membros. [...] (29) Os dados pessoais deverão ser recolhidos para finalidades determinadas, explícitas e legítimas abrangidas pelo âmbito de aplicação da presente diretiva e não deverão ser tratados para fins incompatíveis com os da prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais — nomeadamente a salvaguarda e a prevenção de ameaças à segurança pública. Se os dados pessoais forem tratados, pelo mesmo ou por outro responsável pelo tratamento, para uma finalidade abrangida pelo âmbito de aplicação da presente diretiva que não aquela para a qual foram recolhidos, esse tratamento deverá ser permitido, na condição de que esse tratamento seja autorizado em conformidade com as disposições legais aplicáveis e necessário e proporcionado para a prossecução dessa outra finalidade. (35) Para ser lícito, o tratamento de dados pessoais nos termos da presente diretiva deverá ser necessário para a execução de uma missão de interesse público por uma autoridade competente com base no direito da União ou dos Estados-Membros para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. Estas funções deverão abranger a proteção dos interesses vitais do titular dos dados. O exercício das funções de prevenção, investigação, deteção ou repressão de infrações penais conferidas institucionalmente por lei às autoridades competentes permite-lhes exigir que as pessoas singulares cumpram o que lhes é solicitado. [...]. Mais condizente com a realidade e com a necessidade de se assegurar o direito à segurança, previsto no art. 6º da Constituição Federal, a LGPD Penal Portuguesa, por exemplo, destaca de forma expressa que as suas disposições não implicam qualquer restrição ou limitação na partilha e intercâmbio de dados entre os órgãos de polícia criminal e destes com as autoridades judiciárias, no âmbito do dever de cooperação estabelecido na lei de organização da investigação criminal (cf. art. 69 da Lei nº 59/2019), dispositivo que merece ser internalizado no âmbito da presente proposta de diploma legislativo.

[348]Eur-Lex. Diretiva 680/2016. É crucial assegurar um nível elevado e coerente de proteção dos dados pessoais das pessoas singulares e facilitar o intercâmbio de dados pessoais entre as autoridades competentes dos Estados-Membros, a fim de assegurar a eficácia da cooperação judiciária em matéria penal e da cooperação policial. Para tal, o nível de proteção dos direitos e liberdades individuais no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais — incluindo a salvaguarda e a prevenção de ameaças à segurança pública — deverá ser equivalente em todos os Estados-Membros. A proteção eficaz dos dados pessoais na União exige não só que sejam reforçados os direitos dos titulares dos dados e as obrigações de quem trata dados pessoais, mas também que haja reforço dos poderes equivalentes para controlar e assegurar a conformidade com as regras de proteção dos dados pessoais nos Estados-Membros. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680. Acesso em 27 de nov. 2024.

suas disposições não implicam qualquer restrição ou limitação na partilha e intercâmbio de dados entre os órgãos de polícia criminal e deste com as autoridades judiciárias no âmbito do dever de cooperação estabelecido na Lei de Organização da Investigação Criminal[349].

Da forma como foi redigida a redação do Anteprojeto, ocorrerá a impossibilidade do uso de tecnologias em detrimento da eficiência das atividades de segurança pública e persecução penal, o que resultará no comprometimento da eficiência dos resultados das polícias e, consequentemente, dos processos judiciais.

A Nota Técnica da ENCCLA também fez uma observação muito relevante, ao afirmar que a aprovação de dispositivo desta natureza teria o potencial de afetar a República Federativa do Brasil, inclusive no cenário internacional, diante da oposição de obstáculos ao atendimento às recomendações do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/FATF), conforme as Recomendações abaixo:

> Recomendação 29. Unidades de Inteligência Financeira: Os países deveriam estabelecer uma unidade de inteligência (UIF) que sirva como um centro nacional de recebimento e análise de: (a) comunicações de operações suspeitas; e (b) outras informações relevantes sobre a lavagem de dinheiro, crimes antecedentes e financiamento do terrorismo, e de disseminação dos resultados de tal análise. A UIF deveria ser capaz de obter informações adicionais das entidades comunicantes e ter acesso rápido a informações financeiras, administrativas e de investigação que necessite para desempenhar suas funções adequadamente.
> Recomendação 31. Poderes das autoridades de investigação e de aplicação da lei: Durante o curso de investigações de lavagem de dinheiro, de crimes antecedentes e de financiamento do terrorismo, as autoridades competentes deveriam ter acesso a todos os documentos e informações necessários para as investigações, bem como para as ações penais e outras ações a ela relacionadas. Esses poderes deveriam incluir o poder de adotar medidas compulsórias para a requisição de registros mantidos por instituições financeiras, APNFD e outras pessoas físicas ou jurídicas, bem como para a busca de pessoas e propriedades, para a tomada de declarações de testemunhas, e para a busca de obtenção de provas. Os países deveriam assegurar que as autoridades competentes ao conduzirem investigação tenham acesso a uma grande variedade de técnicas investigativas adequadas às investigações de lavagem de dinheiro, crimes antecedentes e financiamento do terrorismo. Tais técnicas incluem: operações

[349]PORTUGAL. Diário da República. Lei nº 58/2019. Artigo 69.º Sistema integrado de informação criminal O disposto na presente lei não implica qualquer restrição ou limitação na partilha e intercâmbio de dados entre os órgãos de polícia criminal e destes com as autoridades judiciárias, no âmbito do dever de cooperação estabelecido na lei de organização da investigação criminal, designadamente do sistema integrado de informação criminal instituído nos termos da Lei n.º 73/2009, de 12 de agosto, alterada pela Lei n.º 38/2015, de 11 de maio. Disponível em:https://www.uc.pt/site/assets/files/475840/20190808_lei_59_2019_prevencao_dtecao_investigacao_ou_repressao_de_infracoes.pdf. Acesso em 27 de nov. 2024.

> encobertas, interceptação de comunicações, acesso a sistemas computacionais e entrega controlada. Além disso, os países deveriam possuir mecanismos efetivos para identificar rapidamente se pessoas físicas ou jurídicas são titulares ou controlam contas. Deveriam também possuir mecanismos para garantir que as autoridades competentes tenham algum procedimento para identificar ativos sem notificação prévia do proprietário. Durante as investigações de lavagem de dinheiro, crimes antecedentes e financiamento do terrorismo, as autoridades competentes deveriam poder solicitar quaisquer informações relevantes à UIF[350].

O objetivo do Artigo 48 do Anteprojeto é tornar exceção o compartilhamento de dados por pessoas jurídicas de direito privado com autoridades competentes para as atividades de segurança pública e persecução penal. De acordo com a Nota Técnica da ENCCLA[351], a proibição como regra geral, ou a imposição de um caráter excepcional ao compartilhamento de dados entre pessoas jurídicas de direito privado e as autoridades competentes viola diretamente o princípio da proporcionalidade, porque deixa desprotegido o direito fundamental à segurança e compromete a atuação eficiente dos órgãos e instituições responsáveis pelas atividades de segurança pública e persecução penal em uma ponderação completamente desequilibrada com o direito à intimidade relativa aos dados pessoais custodiados por pessoas jurídicas de direito privado[352].

É preciso levar em consideração, inclusive, que o compartilhamento de dados entre pessoas jurídicas de direito privado e as autoridades competentes não é vedado pela Lei Geral de Proteção de Dados, o que significar dizer que não há motivo para que o Anteprojeto estabeleça como regra geral a proibição para o compartilhamento, que é fundamental para toda

---

[350]Ministério da Fazenda. Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/FATF). Disponível em: https://www.gov.br/susep/pt-br/assuntos/cidadao/pldftp/o-grupo-de-acao-financeira-gafi-fatf. Acesso em 21 de set. 2024.

[351]*Ibid.*

[352]Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro – ENCCLA. Ação 04/2021. Os artigos 45 a 52 pretenderam disciplinar qualquer modalidade de compartilhamento de dados pessoais entre autoridades competentes e o fizeram de forma extremamente restritiva e desproporcional, deixando completamente desprotegidos o direito fundamental à segurança e a atuação eficiente das autoridades competentes para as atividades de segurança pública e persecução penal. A vingar o texto proposto no anteprojeto, restará inviabilizada, por completo, a cooperação entre agências de persecução penal e de segurança pública, tão necessária ao combate da criminalidade organizada, cibernética, violenta ou de colarinho branco, bem como fatalmente comprometidas as dimensões da prevenção e da detecção de infrações penais, ao revés, inclusive, do quanto edificado no sistema europeu - inspiração do anteprojeto - e uma necessidade da vida em sociedade. Com efeito, o tratamento de dados realizado no âmbito de atividades de segurança pública não pode, de forma alguma, obstar que os dados pessoais sejam utilizados a execução de outras missões de interesse público, para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais. Disponível em: https://enccla.camara.gov.br/acoes/acoes-de-2021. Acesso em 28 de nov. 2024.

e qualquer atividade de persecução penal. O compartilhamento dentro do parâmetro da legalidade, com respeito aos direitos fundamentais e aplicada a devida proporcionalidade, resulta na eficiência dos serviços prestados, conforme preceitua o Artigo 37, Caput da Constituição Federal.

O Capítulo IX do Anteprojeto aborda a transferência internacional de dados, a cooperação internacional e preceitua que as autoridades competentes só podem transferir dados pessoais para outro país ou para uma organização internacional, inclusive dados que se destinem a transferências ulteriores para outro país ou outra organização internacional, se: a transferência for necessária para atividades de segurança pública ou persecução penal; tiver sido aforada uma decisão de adequação nos termos do disposto no Artigo 54 ou tiverem sido apresentadas garantias adequadas; os dados pessoais forem transferidos para agente responsável no outro país ou na organização internacional competente para fins de atividades de segurança pública ou persecução penal; no caso de os dados pessoais terem disso transmitidos ou disponibilizados por país estrangeiro e se esse país tiver dado o seu consentimento prévio à transferência; no caso de uma transferência ulterior para outro país ou para uma organização internacional, a autoridade competente que realizou a transferência inicial ou outra autoridade competente do mesmo país autorizar a transferência ulterior, após análise de todos os fatores pertinentes, nomeadamente a gravidade da infração penal, a finalidade para que os dados pessoais foram inicialmente transferidos e o nível de proteção no país ou na organização internacional para os quais os dados pessoais forem ulteriormente transferidos; e a transferência não comprometer o nível de proteção das pessoas assegurado pelo Anteprojeto. Não ficou claro, no entanto, se as hipóteses de transferência internacional mencionadas acima são alternativas e não cumulativas.

Ainda sobre o compartilhamento internacional de dados pessoais para fins penais, Raíssa Roese da Rosa escreveu o artigo *O Anteprojeto da LGPD Penal e a Necessidade de Cooperação Internacional para o Compartilhamento Extraterritorial de Dados Pessoais para Penais*. Foi proposta uma análise da necessidade de cooperação jurídica para operacionalizar o compartilhamento internacional de dados pessoais visando à persecução penal e de que maneira o Anteprojeto da LGPD Penal contribui na elucidação dessa questão[353].

[353] DA ROSA, Raíssa Roese. O ANTEPROJETO DA LGPD PENAL E A NECESSIDADE DE COOPERAÇÃO INTERNACIONAL PARA O COMPARTILHAMENTO EXTRATERRITORIAL DE DADOS PESSOAIS PARA FINS PENAIS. Disponível em: file:///C:/Users/Usuario/Downloads/6797-Texto%20do%20Artigo-21403-23245-10-20230128%20(1).pdf. Acesso em 21 de set. 2024.

A autora frisou que no processo penal, tradicionalmente o cumprimento de diligências ou de decisões jurídicas no exterior, ainda que seja para os casos de competência da justiça brasileira, requer o uso da cooperação jurídica internacional. Também ressaltou que alguns países condicionam a colaboração jurídica internacional à dupla incriminação, ou seja, "a transferência de informações somente será levada a efeito quando a conduta tida por ilícita configurar crime tanto no país requerente quando no país requerido"[354].

Raíssa também esclareceu que diante da inexistência de uma legislação que regulamente o compartilhamento internacional de dados, é necessário observar o que estabelece a Constituição Federal, o Código de Processo Civil e o Código de Processo Penal sobre o tema. O Inciso IX do Artigo 4º da nossa Constituição Federal lista como princípio das relações internacionais "a cooperação entre os povos para o progresso da humanidade". O Artigo 27 do Código de Processo Civil preceitua que a cooperação jurídica internacional terá por objeto "a colheita de provas e a obtenção de informações" além de "qualquer outra medida judicial ou extrajudicial não proibida pela Lei brasileira"[355]. O Artigo 782 do Código de Processo Penal é bem claro ao afirmar que "o trânsito, por via diplomática, dos documentos apresentados constituirá prova bastante de sua autenticidade"[356].

O Capítulo X do Anteprojeto talvez tenha sido o que mais sofreu críticas, porque atribuiu ao Conselho Nacional de Justiça – CNJ a atribuição de ser a Unidade Especial de Proteção de Dados em matéria penal. Para a Nota Tecnica da ENCCLA[357], a ampliação das atribuições constitucionais do Conselho Nacional de Justiça por meio de lei ordinária não se coaduna com o nosso regime jurídico-constitucional. Na forma disposto no Artigo 92, Inciso I-A da Constituição Federal, o Conselho Nacional de Justiça é um órgão do Poder Judiciário, com atribuições expressamente determinadas no Artigo 103-B, § 4º da própria Constituição Federal.

Propor, portanto, que o Conselho Nacional de Justiça constitua uma Unidade Especial de Proteção de Dados Pessoais em matéria penal para assumir a função da Autoridade Nacional

---

[354] *Ibid.*
[355] BRASIL. Código de Processo Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em 21 de set. 2024.
[356] *Ibid.*
[357] *Ibid.*

de Proteção de Dados resulta em uma ampliação inadequada do Conselho Nacional de Justiça. De acordo com o Supremo Tribunal Federal no julgamento da ADI 3367, o Conselho Nacional de Justiça foi criado para ser mais que um órgão de controle, porque trata-se de um órgão interno ao Judiciário e que detém as atribuições de centralizar tarefas de formulação de diagnósticos, elaborar políticas judiciárias, tecer críticas constritivas e elaborar programas que, no limite de suas responsabilidades constitucionais, possibilitem respostas eficazes aos múltiplos problemas comuns à atividade de prestação jurisdicional[358].

O que deve ser destacado é que a Constituição Federal pode autorizar que sejam ampliadas as competências do Conselho Nacional de Justiça, desde que a alteração seja levada a efeito pelo Estatuto da Magistratura, que segundo Artigo 93 da Constituição Federal, depende de Lei Complementar. O Anteprojeto, portanto, não respeitou a adequação formal quanto à espécie normativa, tendo em vista que se trata de Lei Ordinária e não de Lei Complementar de iniciativa privativa do Supremo Tribunal Federal.

Diante da irregularidade formal, já que há uma Lei Ordinária ampliando competência que a Constituição somente admite que seja ampliada por Lei Complementar de natureza privativa, não sendo apropriado falar que o Conselho Nacional de Justiça pode assumir a função de Unidade Especial de Proteção de Dados em matéria penal.

Embora muito bem elaborada em vários aspectos, a Nota Técnica da ENCCLA sugeriu, conforme mencionado acima, a criação de uma estrutura similar à ANPD, como se fosse uma ANPD Penal, com a participação de representantes do Judiciário a serem indicados pelo Conselho Nacional de Justiça, do Ministério Público a serem indicados pelo Conselho Nacional do Ministério Público, além de representantes do Ministério da Justiça, das Secretarias de Segurança dos Estados, dentre outros.

No entanto, é provável que sugestão da ENCCLA não seja aceita em caso de eventual reformulação do atual Anteprojeto. Caso acontecesse da forma como foi descrito na Nota Técnica, teríamos integrantes de diversos órgãos que fazem parte da persecução penal fazendo parte de uma estrutura que seria utilizada para aferir a legalidade da utilização e do tratamento de dados pessoais realizados pelos seus próprios pares. O mais apropriado, portanto, seria que

[358]STF, ADI 3367 (Med. Liminar), Tribunal Pleno, Rel. Min. Cezar Peluso, J. 17.03.2006, DJe 22.09.2006.

a atual Autoridade Nacional de Proteção de Dados fosse reestruturada, para contemplar essa nova ANPD Penal. A ANPD, inclusive, foi transformada em autarquia, o que lhe concedeu autonomia administrativa e financeira, reforçando a tese de que o mesmo pode acontecer com a implementação de eventual ANPD Penal.

Danilo Doneda entende que a garantia de autoridades independentes encontra sua justificativa na necessidade de garantir respostas mais adequadas e céleres do que as que seriam oferecidas pela administração direta, que não necessariamente possui atribuições técnicas sobre questões envolvendo a proteção de dados pessoais[359]. O Autor também alegou que a centralização da matéria em uma autoridade evita o risco da fragmentação da interpretação da lei entre tribunais e mesmo outros órgãos administrativos com competências eventualmente concorrentes e garante a uniformidade dos direitos do cidadão e a segurança jurídica na aplicação da LGPD. Ainda de acordo com o Doneda[360], para que se garanta a independência da autoridade, "suas atividades fiscalizatórias, sancionatória e decisional não devem se subordinar hierarquicamente a outros órgãos".

O Capítulo XI, por fim, aborda as sanções que serão aplicadas, de forma isolada ou cumulativa, caso ocorram infrações ao que foi previsto no Anteprojeto. Foram estabelecidas as seguintes sanções: advertência com indicação de prazo para adoção de medidas corretivas; publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua regularização, quando cabível; eliminação dos dados pessoais a que se refere a infração, quando cabível; suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador, quando cabível; suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, quando cabível[361].

---

[359]DONEDA, D. A Autoridade Nacional de Proteção de Dados e o Conselho Nacional de Proteção de Dados. *In:* MENDES, L. S.; SARLET, I. W.; RODRIGUES JÚNIOR, O. L.; BIONI, B. (Coords.). Rio de Janeiro: Foresne, 2021. P. 459.

[360]*Ibid.*

[361]Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro – ENCCLA. Ação 04/2021. 12. Capítulo XI - Sanções Por fim, quanto às sanções, previstas nesse capítulo, desde logo é de deixar claro que elas não poderão ser aplicadas ao tratamento de dados feito pelo Judiciário no exercício de sua atividade típica, isto é, no exercício da jurisdição. Por mais que a indeclinabilidade da jurisdição torne pouco provável que o órgão administrativo efetivamente possa aplicar sanções visando a coarctar a independência judicial e, portanto, a imparcialidade dos magistrados, não convém deixar aberta a porta para que se iniciem discussões acerca dessa matéria, especialmente quando se nota a sensibilidade da atuação em matéria penal. Da mesma forma, tendo em conta que se cuida de

Os § 1º e 2º do Artigo 63 sugerem que o agente público que facilitar ou der causa à infração das normas da referida lei responderá administrativamente, conforme a lei disciplinar aplicável, incluindo, conforme o caso, a Lei Improbidade Administrativa. Caso o mesmo fato constituir simultaneamente crime e infração administrativa conta a mesma pessoa natural, o procedimento administrativo será suspenso quando iniciada medida de investigação de infração penal, retomando-se caso não sobrevenha sentença declarando a inexistência material do fato ou sua prática em legítima defesa, estado de necessidade, exercício regular de um direito ou cumprimento de um dever[362].

O Capítulo XII, por sua vez, aborda as disposições finais e transitórias do Anteprojeto, reforçando que as autoridades fiscais e aduaneiras, as unidades de inteligência financeira, as autoridades administrativas independentes, as autoridades de supervisão dos mercados financeiros e valores mobiliários, obrigadas legalmente à comunicação de suspeita de prática de infração penal as autoridades, deverão se submeter ao que foi disposto no Anteprojeto, restringindo-se a transmissão aos dados necessários para o atendimento da finalidade legal específica, sem prejuízo da prévia autorização judicial quanto prevista em lei.

Também foi sugerida a criação de um novo tipo penal, denominado Transmissão Ilegal de Dados Pessoais (Transmitir, distribuir, usar de forma compartilhada, transferir, comunicar, difundir dados pessoais ou interconectar bancos de dados pessoais sem autorização legal para obter vantagem indevida ou prejudicar o titular dos dados ou a terceiros a ele relacionados),

---

regulamentar a atuação de agentes públicos, relacionada à utilização de dados coletados e armazenados em repositórios públicos, tampouco é possível pensar na possibilidade de aplicação das sanções previstas nos incisos V (suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador, quando cabível) e VI (suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de6 (seis) meses, prorrogável por igual período, quando cabível.) do anteprojeto, em razão de sua incompatibilidade com a natureza do tratamento de dados por autoridades competentes para atividades de segurança pública e de persecução penal. Disponível em: https://enccla.camara.gov.br/acoes/acoes-de-2021. Acesso em 28 de nov. 2024.

[362]BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Art. 63. As infrações às normas previstas nesta Lei ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa. § 1º O agente público que facilitar ou der causa à infração das normas desta Lei responderá administrativamente, conforme a lei disciplinar aplicável, incluindo, conforme o caso, a Lei de Improbidade Administrativa. § 2º Se o mesmo fato constituir simultaneamente crime e infração administrativa contra a mesma pessoa natural, o procedimento administrativo será suspenso quando iniciada medida de investigação de infração penal, retomando-se caso não sobrevenha sentença declarando a inexistência material do fato ou sua prática em legítima defesa, estado de necessidade, exercício regular de um direito ou cumprimento de um dever. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov.

cuja pena de reclusão vaiará de 1 (um) a 4 (quatro) anos e multa, com aumento de pena de um a dois terços se os dados pessoais forem sensíveis ou sigilosos ou se o crime for praticado por funcionário público em razão do exercício de suas funções[363].

O peso das regras rigorosas previstas para o tratamento de dados pessoais aplicado aos casos de persecução penal e segurança pública não foi o mesmo utilizado para criação do delito em tela. A pena mínima prevista para os delitos praticados ficou desproporcional em relação a outros crimes previstos no Código Penal Brasileiro. O tipo penal em questão precisa ter um caráter pedagógico e desestimulante para a prática de crimes previstos no tratamento de dados pessoais para fins penais.

Penas desproporcionais podem gerar uma sensação de impunidade. Cesare Beccaria[364] mencionou que os meios de que se utiliza a legislação para impedir os crimes devem ser mais fortes à proporção que o crime é mais contrário ao bem público e pode tornar-se mais frequente. Deve, portanto, haver uma proporção entre os crimes e as penas. O princípio da proporcionalidade deve funcionar como limite ao legislador e ao magistrado que aplicará a pena. Deve existir, portanto, uma proporcionalidade entre o crime que será praticado e a pena que será imposta.

De acordo com Cléber Masson, o princípio da proporcionalidade apresenta as seguintes três dimensões: Adequação da pena: a pena do crime deve ser um meio adequado, dentre todos os outros meios menos gravosos, para a realização de um fim, que é a proteção de determinado bem jurídico; Necessidade da pena: a pena do crime deve ser um meio adequado e um meio

[363]BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Art. 66. O Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações: Capítulo V - Dos crimes contra a proteção de dados pessoais (NR) Transmissão ilegal de dados pessoais (NR) Art. 154-C. Transmitir, distribuir, usar de forma compartilhada, transferir, comunicar, difundir dados pessoais ou interconectar bancos de dados pessoais sem autorização legal para obter vantagem indevida ou prejudicar o titular dos dados ou a terceiro a ele relacionados: (NR) Pena - reclusão, de 1 (um) a 4 (quatro), anos e multa. (NR) Parágrafo único. Aumenta-se a pena de um a dois terços se: (NR) I - os dados pessoais forem sensíveis ou sigilosos; (NR) II - o crime for praticado por funcionário público em razão do exercício de suas funções. (NR). Art. 67. A adequação do tratamento de dados às normas previstas nesta lei deverá ser implementada pelos agentes de tratamento até a sua entrada em vigor, sob pena de ilicitude do tratamento. Parágrafo único. O Conselho Nacional de Justiça deverá supervisionar o cumprimento do disposto neste artigo, emitindo orientações e estabelecendo normas sobre a adequação progressiva de bancos de dados constituídos até a entrada em vigor desta lei, considerando a complexidade das operações de tratamento, a natureza dos dados e a amplitude do compartilhamento de bancos de dados. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov.

[364]BECCARIA, Cesare. Dos Delitos e das Penas. São Paulo: Editora Martin Claret, 2000.

necessário para realizar um fim de proteção de determinado bem jurídico. Alguns meios podem ser adequados, mas não seriam necessários; Proporcionalidade em sentido estrito: a pena do crime cominada e/ou aplicada, considerada meio adequado e necessário, deve ser proporcional à natureza e extensão da lesão abstrata e/ou concreta do bem jurídico[365].

Ademar Borges foi preciso ao afirmar que, em geral, quando uma lei penal é submetida ao princípio da proporcionalidade, costuma-se reconhecer uma colisão entre o direito pela pena cominada ao delito e o bem jurídico tutelado pela lei penal. A restrição dos direitos fundamentais considerada por esse raciocínio se limita ao direito principal restringido pela norma de sanção: nas leis penais que estabelecem pena de reclusão como sanção para a prática da conduta proibida, identifica-se como restringido o direito à liberdade de locomoção na intensidade prevista pelo preceito secundário da lei. Essa formulação é, porém, incompleta e impede que se reconheça a ampla gama de direitos fundamentais restringidos pela lei penal. Tal equívoco impacta negativamente a aplicação do juízo da proporcionalidade em sentido estrito, pois enfraquece um dos lados da equação formulada no momento do sopesamento, desconsiderando o direito fundamental restringido pela norma de conduta e outros direitos fundamentais restringidos de forma secundária pela norma de sanção[366].

Estudo elaborado pela Fundação Getúlio Vargas e pelo Ministério da Justiça mostrou que projeto sobre penas mais duras geram distorções, onde crimes leves são punidos de forma muito severa, enquanto as condutas graves implicam em sanções mais brandas. O estudo, denominado *Análise das justificativas para a produção de normas penais* pesquisou 100 projetos de lei entre 1988 e 2006 e identificou que a maioria tipifica novos crimes e endurece as sanções. No total, foram 837 propostas de alterações legais, sendo que apenas quatro foram no sentido de diminuir penas e descriminalizar condutas[367].

Para Luiz Antônio Bressame, que coordenou o estudo, a percepção de impunidade por parte da sociedade muitas vezes leva os deputados a proporem um endurecimento das penas, o

[365]MASSON, Cleber. Direito Parte Geral - vol. 1. - 18.ª ed. rev., atual. e ampl. - Rio de Janeiro: Método, 2024.
[366]SOUSA FILHO, Ademar Borges de. O controle de constitucionalidade de leis penais no Brasil: graus de deferência ao legislador, parâmetros materiais e técnicas de decisão. 2019. 700 f. Tese (Doutorado em Direito) - Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2019.
[367]Agência Câmara dos Deputados. Estudo mostra que projetos sobre penas mais duras geram distorções. Disponível em: https://www.camara.leg.br/noticias/224214-estudo-mostra-que-projetos-sobre-penas-mais-duras-geram-distorcoes/. Acessado em 22 de set. 2024.

que pode gerar distorções[368]. O Relator da Comissão, Deputado Alessandro Molon, avaliou que o documento demonstrava que o Parlamento realmente estava tratando a questão penal de forma equivocada. Entre os exemplos citados de crimes cujas penas são desproporcionais, está o de falsificação de remédios, ou cosméticos, que pode levar de 10 a 15 anos de prisão, enquanto o homicídio tem pena de 6 a 20 anos de cadeia[369]. Por esse motivo, entendo que o tipo penal sugerido deve ser proporcional a todas as exigências do Anteprojeto.

Percebeu-se, portanto, que o Anteprojeto foi muito rígido com os órgãos de persecução penal, dando maior evidência à proteção dos dados pessoais que às investigações realizadas por esses órgãos. Os direitos fundamentais, inclusive o da proteção de dados pessoais, não são absolutos e não devem impedir ou obstruir o uso lícito desses danos nas atividades de prevenção, detecção, investigação e repressão de infrações penais, o que favorece o crime organizado, que já faz uso desses dados pessoais.

O Anteprojeto, portanto, apresenta um desequilíbrio entre a busca do equilíbrio e proporcionalidade entre a proteção a direitos individuais e o dever social de persecução penal e de segurança pública, o que deve ser avaliado quando o tema for novamente debatido no Congresso Nacional. Nas palavras da Nota Técnica da ENCCLA, "o texto do Anteprojeto necessita de profundas reformulações, de modo a compatibilizar o direito fundamental à segurança pública e o dever de eficiência do sistema penal com os direitos individuais afetos à personalidade, proteção de dados e autodeterminação informativa"[370].

---

[368]*Ibid.*

[369]BRASIL. Código Penal Brasileiro. Homicídio simples. Art. 121. Matar alguém: Pena - reclusão, de seis a vinte anos. Falsificação, corrupção, adulteração ou alteração de produto destinado a fins terapêuticos ou medicinais. Art. 273 - Falsificar, corromper, adulterar ou alterar produto destinado a fins terapêuticos ou medicinais: Pena - reclusão, de 10 (dez) a 15 (quinze) anos, e multa. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 06 de nov. 2024.

[370]Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro – ENCCLA. Ação 04/2021. 14. Conclusão. É cediço que cada vez mais a internet e aplicações tecnológicas passam constantemente por avanços, e isso implica em pontos positivos e negativos para a sociedade. Entre os pontos negativos encontra-se uma gama de dados pessoais, públicos, sigilosos e sensíveis, que devem ser tratados de maneira segura por entidades e órgãos públicos e privados, a fim de evitar a violação de direitos individuais da sociedade. Contudo, não se pode perder de vista que, para que órgãos e entidades de segurança pública e persecução penal possam cumprir suas funções institucionais, o tratamento e compartilhamento de dados pessoais para essa finalidade não pode seguir a mesma lógica da Lei Geral de Proteção de Dados ou adotar regramento mais gravoso, sob pena de inviabilizara eficiência de suas atividades. Sem prejuízo, pode adotar seus conceitos e princípios para fins de coesão sistêmica, contanto que esses não afrontem ou violem a eficiente persecução penal e a garantia da segurança pública, fundamentais para a ordem pública brasileira. Os direitos fundamentais não são absolutos e não podem impedir o uso inteligente de dados nas atividades de prevenção, detecção, investigação e repressão de infrações penais, funcionando escudo para a atuação de organizações criminosas. A partir disso, o anteprojeto apresenta, na verdade, um grande descompasso na busca de equilíbrio e proporcionalidade entre a proteção a direitos individuais e o dever social de persecução penal e de segurança pública, criando embaraços aos mecanismos e instrumentos básicos de

5.1 Fundamentação legal e Críticas ao Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Persecução Penal

Todo Anteprojeto que tenha como objetivo determinada mudança no ordenamento jurídico brasileiro, seja qual for o tema, receberá críticas e elogios. Com o referido Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Persecução Penal não foi diferente. Embora as críticas sejam de extrema relevância para o aperfeiçoamento do texto, é necessário começar a abordagem elogiando a Comissão de Juristas instituída por Ato do Presidente da Câmara dos Deputados.

A Comissão foi composta por profissionais capacitados e reconhecidos nas suas respectivas áreas de atuação. Através de muito empenho, os profissionais tentaram demonstrar a necessidade, a estrutura e os principais conceitos da proposta legislativa, com o intuito de regular o tratamento de dados no âmbito da segurança pública, das atividades de persecução penal e na repressão das infrações penais. Percebe-se que o Anteprojeto foi muito bem elaborado, já que seus autores buscaram harmonizar a segurança jurídica nas investigações realizadas pelos órgãos da persecução penal, com os Direitos Fundamentais previstos em nossa Constituição Federal.

O Anteprojeto deixa clara a preocupação dos dados previstos na Lei Geral de Proteção de Dados, demonstrando que os profissionais da segurança pública, os membros do Ministério Público e do Poder Judiciário devem se submeter a essa nova norma. Para fazer valer a aplicação da Lei, foi criado um novo tipo penal que criminaliza quem não dá a devida proteção aos dados pessoais.

O novo tipo penal seria inserido no Código Penal Brasileiro da seguinte forma:

---

investigação, repressão, prevenção e segurança pública. Portanto, essa Ação da ENCCLA entende que o texto do anteprojeto necessita de profundas reformulações, de modo a compatibilizar o direto fundamental à segurança pública e o dever de eficiência do sistema penal com os direitos individuais afetos à personalidade, proteção de dados e autodeterminação informativa. Disponível em: https://enccla.camara.gov.br/acoes/acoes-de-2021. Acesso em 28 de nov. 2024.

> Artigo 154-C – Transmitir, distribuir, usar de forma compartilhada, transferir, comunicar, difundir dados pessoais ou interconectar banco de dados pessoais sem autorização legal para obter vantagem indevida ou prejudicar o titular dos dados ou a terceiro a ele relacionados: Pena – reclusão de 1 (um) a 4 (quatro), anos e multa. Parágrafo único. Aumenta-se a pena de um a dois terços se: I – Os dados pessoais forem sensíveis ou sigilosos; II – O crime for praticado por funcionário público em razão do exercício de suas funções.

Da forma como foi originalmente apresentado, o Anteprojeto acabará, de certo modo, dificultando o trabalho de investigação criminal e persecução penal, já que cria um tipo penal com causa de aumento de pena caso a violação de dados pessoais ocorra no exercício das funções. Aqui merece destaque a ação pública no delito em questão (ação penal pública incondicionada), dando a entender que a violação de um direito fundamental não pode estar na esfera de disponibilidade da vítima. Outro questionamento que precisará ser esclarecido será se o Estado e a vítima serão sujeitos passivos desse crime.

Embora o Anteprojeto esteja bem estruturado, ainda há vários pontos que precisam ser discutidos. Toda investigação criminal exige muita destreza daqueles que estão envolvidos na cadeia de investigação, sob pena da ocorrência de erros que podem ser muito graves para aquele que está sendo investigado. Profissionais da segurança pública, do Ministério Público e do judiciário podem elaborar um estudo que esteja alinhado com o referido Anteprojeto, amparado em princípios constitucionais balizadores da atuação do legislador penal, sem deixar que isso prejudique o esclarecimento de eventual crime, seja ele grave ou não.

Nota Técnica do Ministério Público do Estado de Santa Catarina[371] apontou inconsistências constitucionais no Anteprojeto Penal de Proteção de Dados, constatando-se a necessidade de reformulação da proposta atual. Após análise do texto, o MPSC entendeu que alguns dispositivos do Anteprojeto podem inviabilizar as investigações policias e o cumprimento das funções do Ministério Público bem como de outras instituições que combatem o crime. Além disso, também foram encontradas inconsistências constitucionais que podem ameaçar o direito fundamental à segurança pública.

[371]Ministério Público do Estado de Santa Catarina. Nota Técnica do Ministério Público do Estado de Santa Catarina aponta inconsistências constitucionais no Anteprojeto da LGPD penal e considera ser necessário reformular a proposta em tramitação no Congresso Nacional. Disponível em: https://www.facebook.com/photo/?fbid=3185976848346205&set=a.1425084504435457. Acesso em 16 de set. 2024.

A Nota Técnica 0005/2020/CCR do MPSC[372] apontou vários dispositivos que podem inviabilizar as investigações, porque "o comando legislativo que decorre do anteprojeto em estudo está em absoluto descompasso com a imprescindível integração entre os órgãos de segurança pública e persecução penal e o Ministério Público na defesa do direito fundamental à segurança pública e à persecução penal"[373].

O Anteprojeto restringe o acesso do Ministério Público a dados que hoje são obtidos por meio de requisição direta, tais como informações fiscais e registros telefônicos, conforme decisões do Superior Tribunal de Justiça e do Supremo Tribunal Federal que serão analisadas adiante. Além de não contemplar a segurança pública como direito fundamental, o Anteprojeto ignora as legislações internacionais que regulam a proteção de dados pessoais, prejudicando o equilíbrio entre os direitos individuais à privacidade e o acesso a dados com o objetivo de garantir a aplicação da lei e o combate ao crime organizado.

Ainda de acordo com o que consta na Nota Técnica do MPSC[374], o Anteprojeto incorre em fragilidade constitucional ao restringir o compartilhamento de dados entre o Ministério Público e os órgãos de segurança pública, o que sequer ocorre na Lei Geral de Proteção de Dados, na Diretiva 680/2016 (UE), na LGPD Portuguesa e na Lei Federal Alemã de proteção de dados. Inclusive, diferentemente do que prevê o Anteprojeto Penal de Proteção de Dados, a Diretiva 680/2016 (UE) destaca a necessidade de facilitar o intercâmbio de dados entre as autoridades competentes, a fim de "assegurar a eficácia da cooperação judiciária em matéria penal e da cooperação judicial"[375].

Caso não seja alterado, o Anteprojeto Penal de Proteção de Dados Pessoais prejudicará a prevenção e a investigação de crimes, porque todas as pessoas terão o direito de obter informações sobre como os seus dados pessoais estão sendo usados em qualquer esfera do poder público, mesmo no caso em que seja objeto de uma investigação policial, o que não faz sentido. "O Anteprojeto promove o prejuízo de inquéritos e investigações criminais, de medidas de

[372]*Ibid.*
[373]*Ibid.*
[374]Ministério Público do Estado de Santa Catarina. Nota Técnica do Ministério Público do Estado de Santa Catarina aponta inconsistências constitucionais no Anteprojeto da LGPD penal e considera ser necessário reformular a proposta em tramitação no Congresso Nacional. Disponível em: https://www.facebook.com/photo/?fbid=3185976848346205&set=a.1425084504435457. Acesso em 16 de set. 2024.
[375]*Ibid.*

prevenção e repressão a infrações penais, atingindo de frente políticas de segurança pública, atividades de inteligência e a direitos e liberdade de terceiros atingidos por atividades criminosas", conclui a Nota Técnica[376].

A última atualização demonstrou que o Anteprojeto está parado na Câmara dos Deputados, à espera de um parlamentar que o apresente, para se tornar um Projeto de Lei, que seguirá os trâmites normais, sendo submetido à avaliação de diversas comissões, pela própria Câmara dos Deputados, pelo Senado Federal e pela sanção Presidencial. Até que isso ocorra, é possível que surjam diversas alterações no Anteprojeto, cujo objetivo será preservar o direito fundamental da proteção de dados.

Noutro giro, alguns órgãos de persecução penal demonstraram insatisfação com este Anteprojeto. Durante evento promovido pela Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA), representantes do Ministério Público Federal fizeram fortes críticas ao anteprojeto da Lei Geral de Proteção de Dados Penal, diante dos impactos na persecução penal e na investigação criminal[377].

A principal crítica diz respeito à existência de regras que priorizam a prioridade dos dados pessoais em detrimento da persecução penal. Percebe-se, portanto, que essa temática deve ser debatida com mais amplitude, impondo limites na utilização dos dados, sem prejudicar a atuação dos órgãos da segurança pública.

O Ministério Público Federal questionou o Artigo 6º do Anteprojeto, que permite a um investigado ter livre acesso ao uso que está sendo feito de seus dados pessoais no curso de uma investigação. O Artigo 10, que proíbe empresas privadas de tratarem dados pessoais com o objetivo de apurar irregularidades que possam ter consequências na esfera criminal, também mereceu severas críticas[378].

---

[376] *Ibid.*

[377] Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro – ENCCLA. XVIII Reunião Plenária da Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro. Disponível em: https://enccla.camara.gov.br/acoes/acoes-de-2021. Acesso em 06 de nov. 2024.

[378] Ministério Público Federal. MPF critica desequilíbrio entre privacidade e efetividade da segurança pública e da investigação na LGPD Penal. Para representantes do órgão, medidas excessivamente restritivas para o tratamento de dados pessoais podem dificultar a prevenção e a apuração de atividades ilícitas. Obstáculo às investigações - O procurador da República Vítor Cunha lembrou que hoje, com o desafio do avanço das tecnologias digitais, os dados pessoais são a principal matéria-prima para solucionar crimes e punir os envolvidos. Para ele, é necessário criar normas que regulamentem o uso dessas informações pelos órgãos de segurança e de persecução, no entanto, sem criar obstáculos à atuação dessas instituições, que são essenciais para a garantia do interesse público.

Outro questionamento paira sobre os Artigos 19 e 20 do Anteprojeto, tendo em vista que os órgãos de investigação são obrigados a informar ao investigado se o seu dado está sendo tratado em determinado caso, além de exigir uma resposta por escrito sobre os motivos de uma eventual recusa de acesso à informação.

O Anteprojeto da Lei Geral de Proteção de Dados Penal pode ser um pouco mais lapidado, o que provavelmente acontecerá depois que alguns pontos específicos forem debatidos. Conforme mencionado acima, é possível que a implementação de práticas governança corporativa ou regras de *compliance* possam amenizar alguns aspectos vinculados à má utilização dos dados pessoais utilizados no âmbito de atividades de segurança pública e persecução penal. O fato é que a aplicação da ponderação de bens e do princípio da proporcionalidade será o ponto de partida para eventual apresentação de um novo Anteprojeto ou da alteração do já existente.

Durante webinário promovido pela Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro – ENCCLA[379], foram debatidos os impactos do Anteprojeto da LGPD Penal na investigação criminal e na persecução penal. O evento foi promovido pelo Ministério da Justiça, em parceria com o Ministério Público Federal e a Associação dos Juízes Federais. A maior preocupação daqueles que atuam em uma das esferas da persecução penal é como proteger os dados dos cidadãos, sem deixar de proceder, com eficiência, uma investigação criminal.

O artigo 46 da LGPD Penal, por exemplo, prevê que os órgãos de segurança e persecução penal só podem usar os dados pessoais coletados por outras instituições públicas se ficar comprovado o uso compatível com a finalidade original da coleta das informações. Essa regra, segundo Cunha, vai impedir que o Ministério Público ou a polícia utilizem dados coletados pelo Ibama, Incra ou Secretarias de Meio Ambiente, por exemplo, em apurações de crimes ambientais. "A vedação ao compartilhamento, ou o estabelecimento de critérios muito rigorosos, não observa o equilíbrio que se procura. Outro ponto criticado pelos membros do MPF são os artigos 19 e 20 do anteprojeto, que obriga aos órgãos investigadores informarem ao investigado se o seu dado está sendo tratado em determinado caso, além de exigir uma resposta por escrito sobre os motivos de uma eventual recusa de acesso à informação. Pelo texto atual, os órgãos precisarão ainda informar a data em que o uso dos dados será encerrado, o que implica em dizer quando uma investigação criminal será concluída. “São regras desproporcionais que podem acabar gerando um apagão na persecução penal, com impacto em diversas outras áreas relacionadas, incluindo compromissos internacionais firmados pelo Brasil”, conclui Cunha. Disponível em: https://www.mpf.mp.br/pgr/noticias-pgr/mpf-critica-desequilibrio-entre-privacidade-e-efetividade-da-seguranca-publica-e-da-investigacao-na-lgpd-penal. Acesso em 27 de nov. 2024.

[379]Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro – ENCCLA. Ações de 2021 — Estratégia Nacional de Combate à Corrupção e Lavagem de Dinheiro. Disponível em: <http://enccla.camara.leg.br/acoes/acoes-de-2021>. Acesso em: 13 abr. 2023.

Esse debate, denominado de Ação 04/2021 da ENCCLA, resultou na Nota Técnica já mencionada acima, onde foram feitas avaliações e propostas de alterações, contrastando o texto do Anteprojeto com Convenções, recomendações e melhores práticas internacionais que podem contribuir para o aperfeiçoamento do Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Persecução Penal – LGPD Penal.

Para que as alterações sugeridas possam ser incluídas no Anteprojeto, é necessário que ocorram diálogos entre todos os envolvidos que participam da investigação criminal ao processo judicial. Não é possível avançar o estudo de um tema tão importante para a segurança pública, se todas partes interessadas não forem ouvidas.

Percebe-se no Anteprojeto uma preocupação evidente com a proteção de dados, o que não ocorreu com os atos que englobam a cadeia de custódia. Aqui cabe uma pequena observação, já que o Anteprojeto menciona que a proteção de dados será utilizada para fins de "segurança pública" e "persecução penal". A não distinção não parece ser a mais apropriada, já que os conceitos de segurança pública e persecução penal se misturam. Bruno Bioni[380] ressalta que:

> Se agente trabalha com a ideia de segurança pública, é muito mais relacionada ao momento pré-crime. É vinculada à ideia de prevenção. Persecução Criminal é a ideia de repressão. Na segurança pública eu ainda não tenho um objeto ou um alvo bem definindo, enquanto na persecução criminal eu já tenho. Na segurança pública, talvez eu tenho uma justa causa menos evidente para a interferência do Estado nesse direito fundamental. Na persecução criminal, talvez essa justa causa seja mais evidente. A segurança pública está mais próxima do campo de proteção de dados pessoais. Uma massa de dados pode gerar inteligência para a prevenção de crimes, enquanto no campo da persecução penal agente trabalha muito com o direito à privacidade, quebra de sigilos e assim por diante.

Outro aspecto mencionado na Nota Técnica da Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro – ENCCLA, foi a Comissão de Juristas ter mencionado que o texto do Anteprojeto teve como referência a Diretiva 2016/80[381], do Parlamento Europeu

[380]Seminário Internacional da Comissão de Juristas - Discussão sobre Proteção de Dados Pessoais - YouTube. Disponível em: <https://www.youtube.com/watch?v=NMkSuHEryXE>. Acesso em: 13 abr. 2023.
[381]DIRETIVA (UE) 2016/ 680 DO PARLAMENTO EUROPEU E DO CONSELHO - de 27 de abril de 2016 - relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas a utoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-

e do Conselho, que regula o tratamento de dados pessoais para fins de segurança pública e persecução penal no âmbito da União Europeia. Apesar disso, o Anteprojeto está em absoluto descompasso com a imprescindível integração entre os órgãos que fazem parte dos atos de segurança pública e persecução penal.

Após breve leitura da Diretiva (UE) 2016/680 do Parlamento Europeu, foi possível aferir que um dos seus objetivos é a proteção dos direitos fundamentais das pessoas dos singulares, assegurando o intercâmbio desses dados pelas autoridades na União Europeia, demonstrando que esse objetivo almejado pela Diretiva Europeia atinge o tratamento de dados pessoais realizado pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública.

No Anteprojeto da Lei Geral Penal de Proteção de Dados, porém, foi utilizada, tão somente, a ideia de investigação e repressão de infrações penais. A prevenção e a detecção de tais crimes foram deixadas de lado. Clarissa Nogueira Josino[382] também aponta que o Anteprojeto vai de encontro ao que preceitua a Lei número 12.850/2013[383] (Lei das Organizações Criminosas) e a Lei número 9.613/1998[384] (Lavagem de Dinheiro), que estabelecem acesso aos dados pela autoridade policial e o Ministério Público, independentemente de autorização judicial. A Autora reforça que o Anteprojeto apresenta uma distinção até então não conhecida no ordenamento jurídico brasileiro, mais especificamente no Processo Penal Brasileiro, que é a diferença entre a persecução penal e segurança pública.

Sobre essa temática, Nina Nery ressalta que enquanto as atividades de segurança pública, desenvolvidas pelas polícias militares e rodoviárias, atuam para evitar perigos

Quadro 2008/ 977/ JAI do Conselho. [s.d.]. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=HU>. Acesso em: 13 abr. 2023.

[382]Universidade Federal Do Ceará Faculdade De Direito. CURSO DE GRADUAÇÃO EM DIREITO. CLARISSA NOGUEIRA JOSINO. DADOS PESSOAIS. SEGURANÇA PÚBLICA E INVESTIGAÇÃO CRIMINAL: UM PANORAMA DA PROTEÇÃO DE DADOS E SEUS DESAFIOS REGULATÓRIOS NO BRASIL. Fortaleza,2021.[s.d.].Disponível em: < https://repositorio.ufc.br/bitstream/riufc/58510/1/2021_tcc_cnjosino.pdf>. Acesso em: 17 abr. 2023.

[383]BRASIL. Lei número 12.850/2013 (Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm>. Acesso em: 17 abr. 2023.

[384]BRASIL. Lei número 9.613/1998 (Dispõe sobre os crimes de “lavagem” ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá o. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9613.htm>. Acesso em: 17 abr. 2023.

concretos em situações que possuem o potencial de violar direitos, mas que não estão voltadas a um sujeito individualizado, a persecução penal é desenvolvida pelo Ministério Público e pelas polícias judiciárias e temo como objeto atividades suspeitas, amparadas em fatos determinados. Significa dizer, portanto, que ao contrário dos órgãos de inteligência, os órgãos de persecução penal atuam com os olhos voltados para situações do passado e buscam conferir uma resposta penal a aqueles que já causaram danos ou já colocaram em perigo algum bem juridicamente tutelado[385].

O Supremo Tribunal Federal[386] e o Superior Tribunal de Justiça[387] já se manifestaram sobre a distinção entre as atividades de inteligência e as atividades de persecução penal. Tanto o STF quanto o STJ firmaram entendimento no sentido de que a diferença está assentada na finalidade e na amplitude das atribuições de cada órgão. As Cortes reconheceram que os agentes de inteligência possuem funções preventivas e genéricas, voltadas ao futuro, enquanto os agentes de persecução penal desenvolvem atividades repressivas e investigativas, buscando elementos probatórios relacionados a fatos criminosos determinados ocorridos no passado.

Nina Nery reforça não haver dúvidas de que as atividades de inteligência e de persecução atingem diferentes níveis de direitos fundamentais e estão subjetiva, objetiva e temporalmente voltadas para finalidades distintas, merecendo disciplinas que levem em conta

[385]NERY, Nina. O compartilhamento de dados financeiros no sistema antilavagem de dinheiro brasileiro. São Paulo: Thompson Reuters Brasil, 2024. p.92.
[385]*Ibid.*
[386]STF, HC 147837, Segunda Turma, Rel. Min. Gilmar Mendes, J. 26/02/2019, DJe 26/06/2019.
[387]Em seu voto, o Ministro Rogerio Schietti distingui as atividades de inteligência das ações de infiltração em investigação criminal, assentando que "Os dois primeiros critérios para distinguir a infiltração em ação de inteligência da efetuada em investigação criminal são a finalidade e a amplitude da investigação. A ação de inteligência, geralmente tem a função preventiva e foco voltado às complexidades das conjunturas sociais, enquanto a investigação criminal é reativa – dela podendo decorrer a prisão de investigados – e concentrada na apuração exclusivamente dos fatos a eles imputados. [...]. Outra diferença reside na fiscalização judicial, objeto da Lei n. 12.850/2013, que, todavia, não tece maiores considerações sobre quais atividades seriam típicas dessa ação de investigação. Limita-se a Lei a prever a representação pelo delegado de polícia ou o requerimento pelo Ministério Público, com a demonstração da necessidade da medida, bem como o alcance das tarefas dos agentes; a necessidade de demonstração e que a prova não pode ser produzida por outros meios; o prazo de até 6 meses, sem prejuízo de eventuais renovações; a produção de relatório circunstanciado, que será oportunamente juntado à denúncia, quando será disponibilizado à defesa; dispõe não ser punível "no âmbito da infiltração, a prática de crime pelo agente infiltrado no curso da investigação, quando inexigível conduta diversa", nos limites do princípio da proporcionalidade. Assim, a Lei n. 12.850/2013, ao exigir que o pedido ministerial ou da autoridade policial descreva o alcance das tarefas dos agentes, confere à autoridade judiciária – ao deferir a atividade de investigação – o dever de decidir novamente sobre os limites da atuação do agente, à luz das peculiaridades do caso concreto e da ponderação de valores entre a atividade invasiva e os direitos fundamentais em conflito. Portanto, o que a lei veda é a infiltração de agentes de inteligência no âmbito de investigação criminal, bem como o compartilhamento em investigação criminal de informações provenientes de infiltração em ação de inteligência, visto que somente a infiltração prevista na Lei n. 12.850/2013 passa pelo crivo purificador do controle judicial" (STJ, RHC 57023, Sexta Turma, Rel. Min. Sebastião Reis Júnior, J, 08.08.2017, DJe 16.08.2017.

cada uma das suas especificidades[388]. Para a autora, a observância do princípio da vinculação finalística está diretamente relacionada à preservação do mandato de separação informacional dos poderes, uma vez que, por exercerem atividades voltadas para finalidades distintas e atingirem diferentes níveis de direitos fundamentais, alguns critérios e requisitos devem ser fixados para assegurar que a atuação dos órgãos de inteligência e dos órgãos de persecução penal esteja de acordo com o processo penal garantista[389].

Foi notória a preocupação com a proteção de dados, mas foi deixada de lado a importância da utilização dos dados para a prevenção e a repressão de crimes e contravenções. Daí a necessidade de ser feita uma ponderação entre eventual violação ao direito fundamental da proteção de dados e a investigação de determinado tipo de delito. A nota técnica confeccionada por intermédio do ofício número 539/2020 da Secretaria de Perícia, Pesquisa e Análise o Ministério Público Federal, alerta o referido descompasso entre a Diretiva (EU) 2016/680 e o Anteprojeto da "LGPD Penal"[390].

---

[388]"Por outro lado, a história também já comprovou que o exercício indiscriminado do poder punitivo, sem a fixação dos limites e requisitos claros que confiram legitimidade para a atuação das instituições estatais, contraria tudo aquilo que foi conquistado com a consolidação de um processo penal garantista, único modelo compatível com a fundação e com a conservação do Estado Democrático de Direito. O processo penal moderno, muito mais do que um instrumento de repressão à prática criminosa, se estruturou como um mecanismo de preservação de direitos fundamentais, que são, justamente, aqueles que conferem existência ao próprio Estado Democrático de Direito, contrapondo-se ao Estado autoritário que atua sem limites contra tudo e contra todos, quase sempre sob o discurso de que o uso de poder é condição para a conquista de uma sociedade livre de riscos. O uso indiscriminado do poder punitivo coloca a sociedade no limite da ruptura das garantias que fundamentaram o Estado Democrático de Direito e, não por outro motivo, o processo penal moderno é marcado pela constante busca de uma convivência harmônica entre o garantismo penal e a eficiência, em um arranjo que não se contenta com a mera invocação de uma quase intangível sociedade livre de riscos". NERY, Nina. O compartilhamento de dados financeiros no sistema antilavagem de dinheiro brasileiro. São Paulo: Thompson Reuters Brasil, 2024. p.95.

[389]NERY, Nina. O compartilhamento de dados financeiros no sistema antilavagem de dinheiro brasileiro. São Paulo: Thompson Reuters Brasil, 2024. p.94.

[390]Ministério Público Federal. PROCURADORIA GERAL DA REPÚBLICA SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE. [s.d.]. Ministério Público Federal. PROCURADORIA GERAL DA REPÚBLICA SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE. [s.d.]. A incorporação do conceito de dado sigiloso no artigo 5º associada ao regramento do artigo 14 do anteprojeto, amplia as hipóteses de reserva de jurisdição, afastando o acesso a dados sigilosos atualmente obtidos por meio de requisição do Ministério Público e das Polícias (dados cadastrais telefônicos, por exemplo), situação entendida pelo STF e STJ como transferência de sigilo, e não como quebra. Pode inviabilizar, também, a atuação do COAF no recebimento e comunicação de informações de inteligência financeira. O anteprojeto, neste ponto, excede o seu escopo e adentra em questões próprias ao Código de Processo Penal, o que, caso não corrigido, causará embaraços de todo o tipo à persecução penal. Registre-se que a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (art. 45), a LGPD Penal Portuguesa (art. 68), a LGPD Penal Italiana (art. 37, 6), a LGPD Alemã (art. 9º) excluem da supervisão da autoridade de controle as operações de tratamento de dados efetuados no exercício da função jurisdicional. O normativo brasileiro deve trilhar o mesmo caminho da LGPD Penal Portuguesa (art. 68) e da LGPD Penal Italiana (art. 14) que dispõem, expressamente, que o tratamento de dados pessoais constante de processo penal, de decisão judicial ou do registo criminal é regulado nos termos da lei processual penal. Disponível em: https://www.mpf.mp.br/pgr/documentos/Sppea_PGR00456556.20205.pdf. Acesso em: 21 abr. 2023. Disponível em: https://www.mpf.mp.br/pgr/documentos/Sppea_PGR00456556.20205.pdf. Acesso em: 21 abr. 2023.

Todos os artigos do Anteprojeto da "LGPD Penal" foram detalhadamente analisados e comparados com a Diretiva Europeia, o que resultou em um estudo técnico e direcionado à otimização de mecanismos que possam auxiliar na repressão e na prevenção à corrupção, à lavagem de capitais, ao financiamento do terrorismo e a outros crimes mais graves. Apenas a título de exemplo, de acordo com a referida Nota Técnica do Ministério Público Federal, os Artigos 29 e 35 da Diretiva Europeia são peremptórios quando mencionam que[391]:

> (29) Os dados pessoais deverão ser recolhidos para finalidades determinadas, explícitas e legítimas abrangidas pelo âmbito de aplicação da presente diretiva e não deverão ser tratados para fins incompatíveis com os da prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais – nomeadamente a salvaguarda e a prevenção de ameaças à segurança pública. Se os dados pessoais forem tratados, pelo mesmo ou por outro responsável pelo tratamento, para uma finalidade abrangida pelo âmbito de aplicação da presente diretiva que não aquela para qual foram recolhidos, esse tratamento deverá ser permitido, na condição de que esse tratamento seja autorizado em conformidade com as disposições legais aplicáveis e necessário e proporcionado para a prossecução dessa outra finalidade.
> (35) Para ser lícito, o tratamento de dados pessoais, nos termos da presente diretiva deverá ser necessário para a execução de uma missão de interesse público por uma autoridade competente com base no direito da União ou dos Estados-Membros para efeitos de prevenção, investigação, detecção ou repressão de infrações penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. Estas funções deverão abranger a proteção dos interesses vitais do titular dos dados. O exercício das funções de prevenção, investigação, detecção ou repressão de infrações penais conferidas institucionalmente por lei às autoridades competentes permite-lhes exigir que as pessoas singulares cumpram o que lhes é solicitado. Neste caso, o consentimento do titular dos dados, na aceção do Regulamento (EU) 2016 (679), não deverá constituir fundamento jurídico do tratamento de dados pessoais pelas autoridades competentes. [...][392].

A Diretiva (EU) 2016/680 demonstrou a importância do tratamento de dados, sem deixar de lado a questão da prevenção, investigação, detecção e repressão de infrações penais e ameaças à segurança pública. Outro aspecto que precisa ser aferido no Anteprojeto é uma abordagem sobre os bancos de dados das polícias judiciárias. Conforme já mencionado alhures, as polícias brasileiras, sejam elas judiciárias ou não, possuem uma enorme quantidade de

[392]Eur.Lex. Diretiva 680/2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680. Acesso em: 28 de nov. 2024.

informações de todos aqueles que precisam utilizar os serviços do Estado, o que precisa ser regulado para que não seja feito o mau uso dos dados[393].

Sobre o tratamento de dados pessoais sigilosos, o Anteprojeto estabelece no Artigo 14 que o tratamento de dados pessoais sigilosos por autoridades competentes somente poderá ser realizado se estiver previsto em lei e para atividades de persecução penal e que o acesso a dados pessoais sigilosos por meio de ferramentas de investigação e medidas cautelares de obtenção de prova deve observar a legislação especial aplicável. O Ministério Público Federal sugeriu o tratamento de dados pessoais constante no processo penal, de decisão judicial ou do registro criminal seja regulado nos termos da lei processual penal[394].

Para o MPF, a incorporação do conceito de dado sigiloso no Artigo 5º associada ao que consta no Artigo 14 do Anteprojeto, amplia as hipóteses de reserva de jurisdição, afastando o acesso a dados sigilosos atualmente obtidos por meio de requisição do Ministério Público e das Polícias (dados cadastrais telefônicos, por exemplo), situação entendida pelo STF e STJ como transferência de sigilo e não como quebra[395]. A redação proposta no Anteprojeto também poderia inviabilizar a atuação do COAF no recebimento de informações de inteligência financeira.

Ainda de acordo com o MPF, o Anteprojeto excede o seu escopo e adentra em questões próprias ao Código de Processo Penal, o que pode gerar problemas para a persecução penal. A Diretiva 680/2016 (EU), a LGPD Portuguesa, a LGPD Penal Italiana e a LGPD Alemã excluem da supervisão da autoridade de controle as operações de tratamento de dados efetuadas no exercício da função jurisdicional[396]. "O normativo brasileiro deve trilhar o mesmo caminho da

---

[393]*Ibid.*

[394]BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Do Tratamento de Dados Pessoais Sigilosos Art. 14. O tratamento de dados pessoais sigilosos por autoridades competentes somente poderá ser realizado se estiver previsto em lei e para atividades de persecução penal. §1º O acesso a dados pessoais sigilosos por meio de ferramentas de investigação e medidas cautelares de obtenção de prova deve observar a legislação especial aplicável. 2º O acesso a dados pessoais sigilosos controlados por pessoas jurídicas de direito privado será específico a pessoas investigadas e dependerá de ordem judicial prévia baseada em indícios de envolvimento dos titulares de dados afetados em infração penal e na demonstração de necessidade dos dados à investigação, na forma da lei, sem prejuízo da comunicação de operações suspeitas, nos termos do art. 11 da Lei nº 9.613.Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov.

[395]As decisões do STF e STJ que abordam a referida temática serão analisadas adiante, em tópico específico.

[396]*Ibid.*

LGPD Penal Portuguesa (Art. 68) e da LGPD Penal Italiana (Art. 14), as quais dispõem expressamente que o tratamento de dados pessoais constante de processo penal, de decisão judicial ou do registro criminal é regulado nos termos da lei processual penal", frisou o Ministério Público Federal.

No que diz respeito ao compartilhamento de dados, o Anteprojeto fez a previsão de que qualquer modalidade de uso compartilhado de dados pessoais entre autoridades competentes somente será possível com autorização legal, com autorização judicial ou no contexto de atuações conjuntas autorizadas legalmente, observados os propósitos legítimos e específicos para o tratamento, os princípios e obrigações previstos no Anteprojeto[397].

O MPF sugeriu uma alteração, sob a alegação de que o dispositivo do Anteprojeto não implica em qualquer restrição ou limitação ao compartilhamento de dados entre os órgãos federais, distritais estatuais e municipais incumbidos legalmente de atividades de segurança pública e de persecução penal. Também sustentou que o compartilhamento de dados pessoais entre autoridades competentes ou entre uma autoridade competente e um órgão ou entidade da administração pública não competente para os fins do Anteprojeto é permitido para o cumprimento das tarefas que são da responsabilidade da autoridade competente transmissora ou da autoridade competente a quem os dados são transmitidos[398].

---

[397]Ministério Público Federal. PROCURADORIA GERAL DA REPÚBLICA SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE. [s.d.]. Ministério Público Federal. PROCURADORIA GERAL DA REPÚBLICA SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE. [s.d.]. Artigo 45. Qualquer modalidade de uso compartilhado de dados pessoais entre autoridades competentes somente será possível com autorização legal, com autorização judicial ou no contexto de atuações conjuntas autorizadas legalmente, observados os propósitos legítimos e específicos para o tratamento, os direitos do titular, bem como os fundamentos, princípios e obrigações previstos nesta Lei. § 1º Ressalvadas as hipóteses legais, é vedado o compartilhamento direto e contínuo de bancos de dados que contenham dados pessoais estabelecidos no âmbito de atividades de segurança pública com órgãos responsáveis pela persecução penal, exceto: I – nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei; II – para investigação ou processo criminal específico; § 2º Requisições de acesso a dados entre autoridades competentes para uso compartilhado ocorrerão de forma devidamente motivada quanto ao contexto específico do pedido, à base legal, finalidade, necessidade e proporcionalidade, devendo o registro de acesso e de uso por agentes de autoridade competentes ser mantidos por período de no mínimo 05 anos. Disponível em: https://www.mpf.mp.br/pgr/documentos/Sppea_PGR00456556.20205.pdf. Acesso em: 21 abr. 2023.

[398]Ministério Público Federal. PROCURADORIA GERAL DA REPÚBLICA SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE. [s.d.]. Ministério Público Federal. PROCURADORIA GERAL DA REPÚBLICA SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE. [s.d.]. Artigo 45. O dispositivo na presente lei não implica em qualquer restrição ou limitação ao compartilhamento de dados entre os órgãos federais, distritais, estaduais e municipais incumbidos legalmente de atividades de segurança pública e de persecução penal, no âmbito do descer de cooperação estabelecido no art. 3º da Lei nº 12.850, de 02 de agosto de 2013. §1º. O compartilhamento de dados pessoais entre autoridades competentes ou entre uma autoridade competente e um órgão ou entidade da administração pública não competente para os fins desta lei é permitido para cumprimento das tarefas que são da responsabilidade da autoridade competente transmissora ou da autoridade competente a quem os dados são transmitidos. §2º. O registro de acesso e de uso por agentes de autoridades competentes ser mantido por período

No caso do dispositivo em questão, o Ministério Público Federal entendeu que houve uma regulamentação desproporcionalmente restritiva que não encontra semelhança na Diretiva 680/2016 (UE) e que serviu como fonte de inspiração para o nosso Anteprojeto. Caso o dispositivo não seja alterado, a cooperação entre agências de persecução penal e de segurança pública será inviabilizada, o que pode influenciar na prevenção e na detecção de infrações penais. Ainda de acordo com o MPF, o tratamento de dados realizado no âmbito de atividades de segurança pública não obsta que os dados pessoais sejam utilizados a execução de outras missões de interesse público, para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais.[399]

É preciso ressaltar o hábito brasileiro de comparar o nosso ordenamento jurídico com a legislação de outros países. A prova de que isso pode não ser bom é que existem diversas Leis com pouco ou quase nenhuma aplicabilidade em solo brasileiro[400]. Os legisladores precisam entender que o Brasil possui algumas peculiaridades que outros países não possuem. Caso isso não mude, corre-se o risco de não encontrarmos soluções para a proteção de dados na seara penal, o que pode ser frustrante para todos. Cópias estrangeiras inadequadas não funcionam. É preciso pensar em uma Lei Geral de Proteção de Dados para o Brasil, sem deixar de lado o equilíbrio entre a garantia constitucional da proteção de dados pessoais e a investigação penal.

O Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Persecução Penal precisa de mais diálogo entre todos os órgãos que fazem parte da persecução penal, com uma nova Comissão contendo membros da Academia, do Judiciário, dos Ministérios Públicos Estaduais e Federal, das Polícias Civis dos Estados, da Polícia Federal, da Polícia Rodoviária Federal e das Polícias Militares. Além disso, é necessária a preocupação com a proteção de dados pessoais, sem que isso prejudique ou engesse os métodos de investigação criminal.

---

de no mínimo 5 anos. Disponível em: https://www.mpf.mp.br/pgr/documentos/Sppea_PGR00456556.20205.pdf. Acesso em: 21 abr. 2023.

[399]Ministério Público Federal. PROCURADORIA GERAL DA REPÚBLICA SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE. [s.d.]. Ministério Público Federal. PROCURADORIA GERAL DA REPÚBLICA SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE. [s.d.]. Disponível em: https://www.mpf.mp.br/pgr/documentos/Sppea_PGR00456556.20205.pdf. Acesso em: 21 abr. 2023.

[400]Assembleia Legislativa do Espírito Santo. PL revoga mais 1.108 leis sem eficácia. Disponível em: https://www.al.es.gov.br/Noticia/2019/11/38404/pl-revoga-mais-1108-leis-sem-eficacia.html. Acesso em 06 de nov. 2024.

A proteção de dados pessoais não pode ter um peso maior que o direito à segurança pública, porque esta engloba outros direitos fundamentais que também precisam ser preservados, tais como a vida, liberdade, intimidade, propriedade e tranquilidade. O equilíbrio previsto na Diretiva 680/2026, que serviu de parâmetro para a Comissão de Juristas, não foi encontrado no Anteprojeto Penal de Proteção de Dados.

Cabe salientar que no dia 07 de junho de 2022, foi apresentada a proposta de projeto de lei número 1515/2022[401], que aborda a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD), para fins de segurança do Estado, de Defesa Nacional, de Segurança Pública e de Investigação e Repressão de Infrações Penais. O objetivo da proposta foi justamente regular o Artigo da Lei Geral de Proteção de Dados que prevê regra específica para o tratamento de dados pessoais aos casos mencionados acima.

O referido projeto está baseado em três pilares: proteção dos direitos fundamentais de segurança, liberdade e de privacidade; eficiência da atuação dos órgãos responsáveis; e intercâmbio de dados pessoais entre autoridades competentes. Diferentemente do que menciona o Anteprojeto já descrito alhures, essa nossa proposta legislativa sugere que caberá à Autoridade Nacional de Proteção de Dados (ANPD), atual responsável pela aplicação da Lei Geral de Proteção de Dados, supervisionar a proteção dos dados pessoais para fins de segurança do Estado, de Defesa Nacional, de Segurança Pública e de Investigação e Repressão de Infrações Penais.

O projeto também proíbe o tratamento de dados relativos à segurança pública e defesa nacional por empresas privadas, exceto em processos geridos por pessoa jurídica de direito público[402]. Mesmo nesses casos, é proibido à iniciativa privada o controle total de informações em bancos de dados. O texto permite o compartilhamento de dados pessoais controlados pelos

[401]Câmara dos Deputados. Projeto altera Lei de Proteção de Dados para resguardar segurança pública e defesa nacional - Notícias - Portal da Câmara dos Deputados. Disponível em: <https://www.camara.leg.br/noticias/893704-projeto-altera-lei-de-protecao-de-dados-para-resguardar-seguranca-publica-e-defesa-nacional/>. Acesso em: 13 abr. 2023.

[402]BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Art. 10. É vedado o tratamento de dados pessoais para atividades de segurança pública e de persecução penal por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico ao Conselho Nacional de Justiça, sem prejuízo de outras exigências legais. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 05 de nov.

órgãos de segurança pública em casos excepcionais, quando houver interesse público e desde que sejam observadas normas de proteção de dados previstas no próprio projeto.

Sobre o acesso à informação, o titular poderá ter acesso aos seus dados pessoais por meio de requerimento às autoridades competentes, que terão um prazo de 20 dias para fornecer a resposta. Essa informação poderá ser negada, com a justificativa de prejuízo às ações de inteligência e de defesa nacional, bem como para proteger os direitos e garantias de terceiros. Dessa recusa, cabe questionamento à ANPD ou ação judicial. A proposta também garante ao titular o direito de saber dobre a existência de informações a seu respeito em análise pelo órgão de inteligência, além do acesso a essa informação para possível correção.

O que deve ser destacado é que o acesso pode ser realizado através de outra forma de proteção, com a utilização do *Habeas Data*, previsto no Artigo 5º, inciso LXXII da CRFB/1988. O dispositivo preceitua que *conceder-se-á "habeas data" para assegurar o conhecimento de informações relativa à pessoa do impetrante, constantes de registros ou banco de dados de entidades governamentais ou de caráter público; para retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.* Maria Sylvia Di Pietro menciona que o "habeas data é um remédio constitucional que tem por objeto proteger a esfera interna dos indivíduos contra*:*

> Uso abusivos de registro de dados pessoais coletados por meios fraudulentos, desleais ou ilícitos;
> Introdução nesses registros de dados sensíveis (assim chamados os de origem racial, opinião política, filosófica ou religiosa, filiação partidária e sindical, orientação sexual etc.);
> Conservação de dados falsos ou com fins diversos autorizados em lei[403]".

Importante frisar que o sujeito passivo do *habeas data* são os entes governamentais ou de caráter público. O remédio constitucional é geralmente utilizado quando o titular do direito prefira não utilizar processo sigiloso, na via judicial ou administrativa. A Lei número 9.507/1997 disciplina todo o procedimento para impetração do *habeas data*. De acordo com José dos Santos Carvalho Filho, *"*o direito à informação o habeas data se subdivide em dois aspectos: o conhecimento da informação e a retificação da informação[404]*"*. Depreende-se,

[403]DI PIETRO, Maria Sylvia Zanella. Direito Administrativo. 33ª ed., Rio de Janeiro: Forense, 2020.
[404]CARVALHO FILHO, José dos Santos. Manual de direito administrativo / José dos Santos Carvalho Filho. – 34. Ed. – São Paulo: Atlas, 2020.

portanto, que o direito fundamental de proteção de dados tem garantida a proteção do instrumento fundamental denominado *habeas data*.

No que diz respeito à transferência internacional, o projeto permite a transferência de dados pessoais para organização internacional ou agente no exterior que atuem na área de segurança pública, defesa nacional e persecução penal. Quando as informações estiverem em bancos de dados internacionais, é necessário que o país estrangeiro tenha concordado, exceto se a transferência for necessária para prevenir ameaça imediata e grave à segurança pública do Brasil ou de país estrangeiro e o consentimento prévio não puder ser obtido em tempo hábil. Percebe-se, portanto, que a apesar de ter importado diversos pontos da Diretiva 680/2026 (UE), o Anteprojeto deixou de observar os dispositivos do regulamento europeu que focam na prevenção de delitos.

A Coalizão Direitos na Rede (CDR)[405], composta por várias entidades que reúnem diversas organizações acadêmicas e da sociedade civil em defesa dos direitos digitais tendo como temas principais de atuação a defesa do acesso, liberdade de expressão, proteção de dados pessoais e privacidade na internet, solicitou ao Presidente da Câmara dos Deputados a interrupção da tramitação do Projeto de Lei número 1515/2022, sob a alegação de que a referida proposta legislativa seria um desmonte às garantias constitucionais elaborada pela Comissão de Juristas que construíram o Anteprojeto da LGPD Penal.

As principais críticas ao referido projeto de lei foram: promove o desmonte das garantias democraticamente construídas no âmbito do Anteprojeto de LGPD Penal elaborado por comissão de juristas; amplia demasiadamente o âmbito de aplicação do texto a matérias que possuem fundamentos e principiologia próprias; elimina conceitos importantes e fragiliza a proteção dada aos dados cadastrais; promove o desmonte do arcabouço principiológico de controle sobre as autoridades; enfraquece o repertório de controle sobre decisões automatizadas; e autoriza de forma demasiadamente genérica o compartilhamento de dados entre entidades da administração pública e o acesso a bancos de dados mantidos por atores privados.

[405]Direitos na Rede. CDR solicita ao presidente da Câmara dos Deputados a interrupção da tramitação do "PL da LGPD Penal" - Coalizão Direitos na Rede. Disponível em: <https://direitosnarede.org.br/2022/08/01/cdr-solicita-ao-presidente-da-camara-dos-deputados-a-interrupcao-da-tramitacao-do-pl-da-lgpd-penal/>. Acesso em: 13 abr. 2023.

O Laboratório de Pesquisa em Políticas Públicas e Internet – LAPIN[406], emitiu uma nota técnica elencando os seguintes tópicos como principais pontos de preocupação: debilitação do sistema de conceitos, princípios e fundamentos da proteção de dados, com a supressão de noções importantes, como "autodeterminação informativa", "proporcionalidade", "dados sigilosos" e "responsabilização e prestação de contas"; ampliação indevida e excessiva do escopo regulado, incluindo atividades de defesa nacional, segurança de Estado e de inteligência, as quais são parametrizadas de forma insuficiente, podendo favorecer abusos; supressão de todo o arcabouço de transparência e do controle sobre o tratamento dos dados pessoais na esfera penal, bem como daquele referente às tecnologias de monitoramento; ampliação excessiva das bases legais para o tratamento de dados para os fins tutelados, bem como das hipóteses de compartilhamento entre autoridades e do acesso a dados mantidos por agentes privados, com a adição de incentivos para a precarização das infraestruturas tecnológicas e enfraquecimento de direitos e proteções referentes a decisões automatizadas, como exigência de autorização prévia e de relatórios de impacto adequadamente procedimentalizados, em favor de disposições genéricas e de aplicabilidade limitada.

Conforme já mencionado anteriormente, embora todas as críticas sejam válidas para o aperfeiçoamento de eventual proposta legislativa, parece que o Projeto de Lei número 1515/2022 não seguirá adiante por vários motivos. O primeiro deles é que o autor do Projeto de Lei não foi reeleito. Além disso, atualmente o PL está aguardando a Criação de Comissão Temporária pela Mesa, conforme previsto no Artigo 34, Inciso II do Regimento Interno da Câmara dos Deputados[407].

5.2 Atuação dos Órgãos de Persecução Penal com a Implementação de uma Lei Geral Penal de Proteção de Dados

Diante de tudo o que foi mencionado até aqui, é inegável que a intimidade e os dados pessoais de qualquer cidadão merecem ser preservados, independentemente de ser ou não autor de algum crime. A própria Constituição Federal é clara ao falar que são invioláveis a intimidade,

[406]LAPIN.ORG. Nota técnica: Análise comparativa entre o anteprojeto de LGPD Penal e o PL 1515/2022 - LAPIN. Disponível em: <https://lapin.org.br/2022/11/23/nota-tecnica-analise-comparativa-entre-o-anteprojeto-de-lgpd-penal-e-o-pl-1515-2022/>. Acesso em: 13 abr. 2023.
[407]BRASIL. Regimentos do Congresso, Senado e Câmara - Congresso Nacional. Disponível em: <https://www.congressonacional.leg.br/legislacao-e-publicacoes/regimento-do-congresso-nacional>. Acesso em: 14 abr. 2023.

a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

Percebe-se, portanto, que é necessário haver um equilíbrio entre o direito à privacidade e a garantia da persecução penal. De acordo com Luciano Rocha de Oliveira, "o questionamento que se faz é se a proteção de dados na seara penal é constitucionalmente adequada à proteção integral dos Direitos Fundamentais, especialmente da segurança pública e da privacidade à luz do paradigma do Estado Democrático de Direito[408]". Aduz ainda, o referido autor, que:

> É importante salientar que os órgãos de investigação e repressão estatais necessitam de dados pessoais para alcançar os objetivos de segurança e políticas públicas, sem os quais acabariam por ferir direitos fundamentais constitucionais tais como a vida, a propriedade, o lazer etc. Por outro lado, paradoxalmente, essa atuação estatal, caso seja feita de forma descontrolada e ilimitada, inevitavelmente irá ferir outros direitos individuais, em especial a privacidade[409].

Diante da relevância do tema, no início do mês de outubro de 2024 o Tribunal Constitucional Alemão entendeu que a Lei Criminal Federal de armazenamento de dados violava o direito à Autodeterminação Informativa. A Lei alemã autorizava o Departamento Federal de Polícia Criminal a armazenar dados nos bancos de dados da referida instituição policial. Os reclamantes, que incluíram Advogados, um ativista político e membros de uma torcida organizada de futebol, contestaram os poderes do Departamento Federal de Polícia Criminal, que conduzia vigilância secreta de pessoas, mesmo não suspeitas de atividades terroristas, mas que estavam vinculadas a pessoas suspeitas de atividades terroristas[410].

---

[408]OLIVEIRA, Luciano Rocha de. Proteção de Dados Pessoais no Processo Penal e na Segurança Pública: problemas e atuais perspectivas. São Paulo: Editora Dialética, 2020, p 23.

[409]*Ibid.*

[410]Bundesverfarssungsgericht. Certain powers of the Federal Criminal Police Office for data collection (§ 45(1) first sentence no. 4 of the Federal Criminal Police Office Act) and data retention (§ 18(1) no. 2 of the Federal Criminal Police Office Act) are unconstitutional in part. Julgamento do Primeiro Senado de 1 de Outubro de 2024 - 1 BvR 1160/19 - Lei II da Polícia Criminal Federal. Um requisito mínimo para a vigilância secreta de pessoas de contato usando meios intrusivos com o objetivo de coletar dados é que a vigilância comparável da pessoa responsável, no sentido da lei policial, pelo perigo em questão seria permitida. Para garantir que os dados pessoais coletados anteriormente sejam usados de acordo com a finalidade para a qual foram originalmente coletados, tais dados devem, em princípio, ser excluídos assim que o caso específico para o qual foram coletados tiver sido concluído e a finalidade específica subjacente à coleta de dados tiver sido alcançada. É possível abster-se de excluir os dados após a conclusão do caso específico para o qual foram coletados se os dados – por si só ou em combinação com outras informações disponíveis para a autoridade – tiverem, nesse meio tempo, fornecido uma base específica para investigações posteriores, ou seja, se os pré-requisitos para uma mudança na finalidade tiverem sido atendidos. Para que o Departamento Federal de Polícia Criminal retenha, de forma preventiva e em uma plataforma de dados da polícia federal, dados pessoais básicos de pessoas acusadas de um crime que sejam adequados para fins de identificação e se relacionem a determinada conduta com implicações no direito penal, limites apropriados para a retenção de dados e um período de retenção apropriado devem ser determinados. A retenção preventiva de dados deve ser baseada em um limite que garanta, de acordo com o princípio da proporcionalidade, que a retenção

Os reclamantes alegaram que Lei alemã carecia de um limite apropriado para a retenção de dados, bem como sobre regras suficientes sobre o período de retenção, o que gerou uma desproporcionalidade. O Departamento Federal de Polícia Criminal, por sua vez, alegou que por ser uma agência central de informações e comunicações policiais, além de apoiar outras forças de segurança na prevenção e no combate de crimes, poderia fazer o armazenamento e uso de tais dados, sob o amparo da Lei ora questionada no Tribunal Constitucional Federal.

Para o Tribunal Constitucional Federal da Alemanha, as interferências ao Direito Fundamental da Autodeterminação Informativa devem possuir uma base legítima, que possua um propósito que vise o bem comum, sendo devidamente necessário e proporcional no sentido estrito, para que seja possível atingir o proposito almejado. Assim, ao especificar os requisitos para a justificação de uma interferência, devem ser feitas distinções entre as diferentes interferências aos direitos fundamentais atingidos.

No caso analisado, a coleta de dados pessoais feita pelo Departamento Federal de Polícia Criminal foi dividida duas etapas. A primeira etapa consistia na retenção de dados propriamente dita, enquanto a segunda etapa dizia respeito à posterior utilização dos dados pessoais. A utilização dos dados coletados anteriormente para propósitos diferentes daqueles para os quais foram originalmente coletados, dá origem a uma nova interferência nos direitos fundamentais, devendo ser justificada sob o amparo da Constituição Alemã.

O Tribunal Constitucional Alemão ratificou o entendimento de que mesmo em relação a uma pessoa responsável por determinado perigo, o uso de poderes de vigilância secreta

preventiva de dados pessoais esteja vinculada à obtenção do propósito da retenção; ela também deve abordar adequadamente os riscos específicos da retenção preventiva de dados. Para dados retidos para fins de prevenção e acusação de infrações penais, esse pré-requisito só é atendido se as pessoas afetadas tiverem probabilidade suficiente de estarem conectadas a crimes potenciais de uma maneira relevante sob a lei criminal e se forem precisamente os dados retidos que podem fazer uma contribuição razoável para a prevenção e acusação de tais crimes. Esse prognóstico deve ser baseado em indicações factuais suficientes. Um período de retenção apropriado deve ser estabelecido na lei. O período apropriado é determinado principalmente pela gravidade da interferência, a força do prognóstico ao longo do tempo e outros aspectos decorrentes do princípio da proporcionalidade. Em princípio, um prognóstico se torna menos persuasivo ao longo do tempo, a menos que surjam novas circunstâncias relevantes.Disponívelem:https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2024/bvg24-083.html.Acesso em: 03 de out. 2024.

intrusiva, como os do Departamento Federal de Polícia Criminal, requer, pelo menos, um perigo identificável para um interesse legal de peso suficiente. A lei questionada não satisfez os requisitos, porque não descreveu o elo entre a pessoa afetada e o perigo associado à pessoa investigada, afastando a base legal para a vigilância de pessoas que não sejam responsáveis pela prática de crimes.

A decisão do Tribunal também foi no sentido de que todos os dados processados posteriormente de acordo com a finalidade para a qual foram originalmente coletados, deverão ser excluídos assim que o caso for concluído, ou seja, quando a finalidade de coleta do dado tiver sido alcançada. Para o caso em tela, a retenção dos dados resultou em maior gravidade, porque foram coletados diante de medidas de vigilância particularmente invasivas.

Ficou claro na decisão do Tribunal Constitucional Alemão que a retenção preventiva de dados constitui mudança de propósito, o que viola preceitos constitucionais. Para justificar o armazenamento dos dados, é preciso especificar os propósitos e limites apropriados para a retenção, bem como o período apropriado para que os dados continuem nos bancos de dados. Ao determinar o limite para a retenção dos dados, o legislador deve levar em consideração a fonte, o tipo e o escopo dos dados.

Para que a retenção preventiva de dados pessoais seja constitucionalmente justificada, a lei deve estabelecer um período de retenção apropriado, determinado pela gravidade da interferência, pela força do prognóstico e com observância ao princípio da proporcionalidade. Por fim, a decisão do Tribunal Constitucional Alemão foi no sentido de que os dados pessoais devem ser excluídos se o processamento for ilegal, se a exclusão for necessária para cumprir uma obrigação legal ou se o conhecimento dos dados não for mais necessário para executar as tarefas em questão.

A decisão em tela talvez seja a que tenha chegado mais perto do objetivo deste trabalho, que é a análise da utilização dos bancos de dados das Polícias Judiciárias brasileiras. A diferença, porém, é que o Departamento Federal de Polícia Criminal utilizada de métodos e estratégias para alimentar o seu banco de dados, ao passo que o objeto do presente estudo é a análise dos dados fornecidos pelos próprios titulares, de forma espontânea, quando procuram as polícias para confeccionarem registros de ocorrências policiais ou mesmo quando são autores vítimas ou testemunhas de crimes.

5.3 Necessidade de Regulamentação da Proteção de Dados na Esfera Penal

Apesar das inúmeras críticas ao Anteprojeto Penal de Proteção de Dados Pessoais, é preciso dizer que o Direito Processual Penal precisará dessa regulamentação. Conforme já foi mencionado em diversos pontos deste trabalho, não existe atualmente no Brasil uma legislação para proteção de dados pessoais no âmbito da justiça criminal e da segurança pública. O ideal seria que essa legislação fosse promulgada no mesmo momento em que que foi promulgada a atual Lei Geral de Proteção de Dados, da mesma forma como ocorreu na Europa.

Embora tenhamos esse vácuo legislativo, a Lei Geral de Proteção de Dados não pode ser descartada pelos profissionais que atuam na área da segurança pública. Os princípios gerais de proteção de dados e os direitos dos titulares dos dados devem ser utilizados na seara penal durante as investigações policiais e no processo penal como um todo, em plena consonância com o que preceitua a Constituição Federal[411].

A futura norma que abordará os dados pessoais no âmbito criminal, deverá esculpir em seu texto a obrigatoriedade de observação das medidas a serem utilizadas no tratamento de dados pessoais para a persecução pena, prevendo medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção de dados e os direitos do titular.

Antes da entrada em vigor da Lei Geral de Proteção de Dados Pessoais, já havia uma tendência legislativa para a preservação dos dados pessoais. Apenas a título de exemplo, no Artigo 9º da Lei número 9.296/1996, consta que a gravação não interessada à prova será inutilizada por decisão judicial, durante o inquérito, a instrução processual ou após esta, em virtude de requerimento do Ministério Público ou da parte interessada. A referida legislação ainda reforçou em seu parágrafo único que o incidente de inutilização deve ser assistido pelo Ministério Público, sendo facultada a presença do acusado ou de seu representante legal.

Eventual novo Anteprojeto não pode dificultar a atuação do Estado Brasileiro no combate ao crime, sobretudo a atuação das polícias judiciárias brasileiras, que diuturnamente

[411]Jota. Aplicabilidade da LGPD às atividades de segurança pública e persecução penal. Desde a tramitação do projeto que se converteu na Lei 13.709/2018– conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD) – pende o debate sobre sua aplicabilidade ou não a certas atividades estatais relacionadas à segurança pública, à persecução criminal e à defesa nacional.Disponível em: https://www.jota.info/artigos/aplicabilidade-da-lgpd-as-atividades-de-seguranca-publica-e-persecucao-penal. Acesso em 06 de nov. 2024.

precisam dos dados pessoais de forma imediata para que alguns tipos de delito não se consumem ou que não causem prejuízos maiores para a sociedade. Embora eventualmente possa acontecer a coleta excessiva ou o tratamento desnecessário de dados por parte daquele que vai investigar, essa não é a regra. Uma polícia democrática deve pautar a sua atuação respeitando a legislação, com o intuito de evitar que dados pessoais sejam tratados de forma incorreta, principalmente no que diz respeito à privacidade dos dados que são tratados.

Embora exista uma lacuna legislativa no que diz respeito à proteção de dados pessoais na persecução penal, não se pode desconsiderar o novo direito fundamental à proteção de dados pessoais, que servirá de leme para implementação da futura Lei Geral Penal de Proteção de Dados Pessoais.

Com o intuito de esclarecer algumas dúvidas sobre as estratégias utilizadas pela Comissão de Juristas na elaboração do Anteprojeto Penal de Proteção de Dados para a Persecução Penal e Segurança Pública, foi realizada uma entrevista semiestruturada com a Professora Heloisa Estellita, que fez parte da referida Comissão.

A entrevista semiestruturada consiste em um modelo flexível, onde há um roteiro prévio, para que o diálogo se torne natural e dinâmico. Foi indagado para a entrevistada se a ANPD participou de todas as etapas da elaboração da proposta de regulamentação da proteção de dados na persecução penal. Necessária fazer essa pergunta, porque a Autoridade Nacional de Proteção de Dados passou a funcionar efetivamente no dia 06 de novembro de 2020 e o Ato do Presidente da Câmara que instituiu a Comissão de Juristas que elaborou o Anteprojeto de Lei de Proteção de Dados foi efetivado em 2019.

Heloísa Estellita alegou que a ANPD não participou em nenhuma etapa da elaboração da proposta, porque na época a Autoridade estava sendo implementada em uma estrutura jurídica de total dependência da Presidência da República e, claramente, pelos *standards* da época, não tinha competência para regular a proteção de dados em matéria penal.

A segunda pergunta focou nas contribuições da sociedade civil durante a elaboração do Anteprojeto. Foi indagado para a entrevistada se durante a elaboração do Anteprojeto, integrantes das polícias judiciárias brasileiras foram ouvidos nas audiências públicas.

A entrevistada informou que não foram realizadas audiências públicas, porque a comissão de juristas estava encarregada de elaborar apenas e tão somente o Anteprojeto, contando com a certeza de que no decorrer do processo legislativo, todos os interessados teriam a oportunidade de fazer suas considerações e prestar suas contribuições. Além disso, o Brasil enfrentava uma pandemia, o que fez com que todos os integrantes da comissão tivessem que se adaptar ao mundo digital, não parecendo viável a realização de audiências públicas naquele contexto.

A terceira pergunta foi direcionada ao direito fundamental da proteção de dados, previsto em nossa Constituição Federal após a elaboração do Anteprojeto. Foi indagado à entrevistada se durante a elaboração do Anteprojeto, foi levada em consideração a percepção de que a proteção de dados pessoas seria elevada ao patamar de Direito Fundamental.

Heloísa Estellita alegou que essa questão foi sim levada em consideração, porque já havia proposta de Emenda |Constitucional, mas não havia perspectiva concreta de sua aprovação. Além disso, o Supremo Tribunal Federal já estava começando a se manifestar no sentido de que a proteção de dados pessoais derivava da combinação de uma série de direitos fundamentais.

A quarta indagação focou na similaridade entre a Lei Geral de Proteção de Dados Brasileira e o Regulamento Europeu *General Data Protection Regulation*. Foi perguntado para a entrevistada por qual motivo, no Brasil, a regulação para o tratamento de dados pessoais voltado para a segurança pública e a persecução penal não entrou em vigor no mesmo dia da LGPD, da mesma forma como ocorreu na Europa, quando o GDPR e a Diretiva 680/2016 foram publicadas no mesmo dia.

Heloisa Estellita alegou que a resposta a essa pergunta demandaria um exame mais detalhado do regime europeu. Frisou que naquele ambiente há dois instrumentos diversos tratando da proteção de dados. Falando de "grosso modo e de forma muito simplificada", o tratamento de dados previsto em nossa LGPD pode ter impacto penal por agentes privados e está disciplinado no regulamento. O tratamento de dados para fins penais por autoridades ligadas à investigação, à persecução e à execução penal estão regulados em uma diretiva. A necessidade de dois diplomas legais diversos no ambiente europeu tem diversas razões, mas a principal delas, no que nos interessa, é que a União Europeia não tem competência para tratar

de matéria penal em sentido amplo via regulamentos. Ela tem que tratar essa matéria por diretivas que devem ser transpostas para o sistema interno dos países. Compreender essa diferença é fundamental para entender a estrutura da regulamentação europeia. Sem prejuízo, algumas regras do tratamento geral da proteção de dados têm de ser adaptadas à esfera penal, ou seja, é conveniente que a matéria seja dividida em dois diplomas legais ou, se em um diploma só, que seja feito um capítulo dedicado à matéria penal. Um exemplo esclarece isso: o direito dos titulares de eliminação de seus dados não pode ser exercido na área penal como pode ser exercido na área extra penal. As informações que tenho sobre a LGPD e a exclusão da matéria penal refletem o temor dos que a propuseram de que, se a matéria penal fosse incorporada ao projeto de lei, haveria grande chance de projeto não aprovado. Por isso houve a exclusão, mas com a regra, que mais parece uma advertência, no sentido de que a futura legislação deveria atender aos princípios e garantias gerais da própria LGPD.

Com o intuito de tentar compreender um pouco as críticas ao Anteprojeto, a maioria delas sob a alegação de que havia um descompasso entre o tratamento de dados para fins penais e a garantia do direito fundamental à segurança pública, foi indagado para a entrevistada se a Comissão que elaborou o Anteprojeto teve a oportunidade de se reunir novamente, para análise das críticas que foram feitas, em sua grande maioria por órgãos que fazem parte da persecução penal.

Heloísa Estellita alegou que infelizmente as Comissões de Juristas têm um prazo incompreensivelmente curto para o desenvolvimento de seus trabalhos. Embora tenha ocorrido uma prorrogação em virtude da pandemia, não houve tempo regulamentar para colher as críticas, refletir sobre elas e fazer as devidas adaptações. A esperança dos membros da Comissão era que, convertido o Anteprojeto em projeto de lei, houvesse amplo espaço para essa discussão. Mas como todos sabem, o Anteprojeto nunca foi convertido em projeto de lei.

O Anteprojeto foi entregue ao Presidente da Câmara dos Deputados em novembro 2020. Durante os últimos 04 anos, a percepção sobre a proteção de dados mudou consideravelmente, principalmente no que diz respeito ao avanço das tecnologias que violam os dados pessoais. Por isso foi indagado à entrevistada se é possível que o Anteprojeto apresentado pela Comissão passe por alguma atualização.

A entrevistada alegou que certamente o Anteprojeto precisa ser atualizado, não só em virtude do avanço das tecnologias, mas em razão do que foi considerado na resposta anterior, já que é necessária uma discussão ampla do texto com todas as pessoas afetadas, o que engloba não só as autoridades públicas incumbidas da segurança pública da persecução penal, mas também das organizações dos titulares de dados que terão suas vidas afetadas por essa forma de tratamento de dados pessoais.

A sétima indagação teve o objetivo de aferir de que forma um tópico específico do Anteprojeto pode interferir no trabalho dos órgãos de persecução penal. Foi mencionado para a entrevistada que o Anteprojeto confere ao titular de dados pessoais o direito de obter informações acerca da existência de tratamento de suas informações pessoais pelo controlador. Foi perguntado para Heloisa Estellita se de alguma forma isso prejudicará a prevenção e a repressão de crimes.

Heloisa Estellita mencionou que sim, porque conforme mencionado na quarta questão, essa é uma das diferenças entre o tratamento de dados na matéria penal e extra penal. Completou dizendo que o Anteprojeto contemplava disciplina especial para o direito do titular de saber da existência do tratamento de seus dados.

A oitava pergunta indagou para a entrevistada se depois que a proteção de dados pessoais passou a ser reconhecida como Direito Fundamental, previsto em nossa Constituição Federal, a Autoridade Nacional de Proteção de Dados deveria exercer um papel mais relevante no tratamento de dados pessoais para fins penais.

Para Heloísa Estellita, a ANPD tem uma competência residual em matéria penal na medida em que ela pode exigir a preparação de relatórios de impacto no caso de emprego de tecnologias potencialmente interventoras do direito à proteção de dados em matéria penal. Continuou afirmando que essa competência só foi exercida no caso da nota técnica 174/2023. Mas esse é o único papel, embora bastante relevante, que a ANP tem em matéria penal em virtude do disposto na LGPD.

Sobre as atribuições da Autoridade Nacional de Proteção de Dados, foi indagado para a entrevistada se a ANPD não seria a mais indicada para supervisionar a proteção de dados pessoais nas circunstâncias previstas no Anteprojeto, e não o CNJ.

Heloísa Estellita entente que com certeza a ANPD é o órgão mais indicado pra supervisionar a proteção de dados em matéria penal. Mas na época em que o Anteprojeto foi elaborado, ela não tinha estrutura autônoma como tem hoje. Era um órgão diretamente subordinado à presidência da República. Um órgão com essa característica não seria aceito no âmbito da comissão europeia para fins de cooperação internacional em matéria de dados para segurança pública e persecução penal, justamente pela falta de autonomia. Foi por isso que a comissão indicou, provisoriamente, o CNJ como autoridade de supervisão, ciente de que essa solução tinha diversos problemas. No quadro atual certamente a ANPD é um órgão que tem as garantias para exercer adequadamente a supervisão, apenas nos parece que o seu quadro deveria ser incrementado com profissionais especialistas em proteção de dados em matéria penal, que a autoridade hoje não tem em virtude de não ter competência ampla nessa matéria.

Por fim, foi mencionado para a entrevistada que a segurança pública também é prevista em nossa Constituição Federal como direito fundamental. A indagação feita foi no sentido de aferir se o Direito Fundamental á proteção de dados pode ser mitigado para fins de investigação criminal.

Heloísa Estellita respondeu que há poucos direitos fundamentais intocáveis. A maioria dos direitos fundamentais pode ser objeto de intervenção que não toque em seu núcleo essencial e desde que a intervenção seja veiculada por lei (em sentido formal) proporcional. “Sendo assim, respeitados esses pressupostos constitucionais da intervenção em direitos fundamentais, não vejo motivo para que a segurança pública seja utilizada no juízo de proporcionalidade como fundamento para intervenções”.

Conforme foi possível aferir nos parágrafos acima, o respeito aos direitos fundamentais deve ser a regra, apesar de sabermos que não existem direitos absolutos. A alegação de que a segurança pública deve prevalecer sobre direitos fundamentais, restringindo-os, não pode prevalecer. A intervenção em Direitos Fundamentais, repita-se, só deve ser exercida em caráter excepcional e devidamente autorizada por lei, sendo que a norma autorizativa deve prever a autorização de acesso em ambas as pontas da intervenção, assegurando que as agências estatais só possam ter acesso à informações pessoais nos estritos limites de suas atribuições, a serem

fixadas de acordo com a finalidade de cada instituição[412]. Os bancos de dados existentes nas polícias judiciárias brasileiras parecem não atender esses requisitos.

6 PROTEÇÃO DE DADOS COMO DIREITO E GARANTIA FUNDAMENTAL

A compreensão do significado de um direito fundamental dependerá do entendimento de uma sociedade em determinado momento e pode variar ao longo da história. Significa dizer que o conceito de direito fundamental não é fechado, já que pode variar no tempo e no espaço. Os direitos fundamentais são: inalienáveis - porque não possuem conteúdo econômico patrimonial, não podem ser comercializados ou permutados; imprescritíveis - ou seja, serão sempre exigíveis. Ainda que não utilizados, jamais deixarão de pertencer a quem os possui; irrenunciáveis - ainda que não exercidos pelo titular, não pode dispor desse direito; relativos - não são direitos absolutos. Se ocorrer a colisão entre dois ou mais direitos fundamentais, isso será analisado por um juízo de ponderação ou pela aplicação do juízo da proporcionalidade; personalidade - onde os direitos fundamentais não se transmitem; concorrência e cumulatividade - os direitos fundamentais são direitos que podem ser exercidos ao mesmo tempo; universalidade – independente das nações terem assinado a declaração, devem ser reconhecidos em todo o planeta, independentemente da cultura, política ou sociedade[413].

O entendimento sobre a universalidade dos direitos fundamentais não é absoluto, já que, conforme mencionado acima, devem ser reconhecidos na medida da cultura de cada sociedade. Outro aspecto que deve ser destacado é que é proibido o retrocesso dos direitos fundamentais. Isso quer dizer que não se pode retroceder no que diz respeito aos avanços históricos já conquistados. De acordo com Canotilho[414], o núcleo essencial dos direitos sociais já realizado e efetivado através de medidas legislativas deve ser considerado constitucionalmente garantido, sendo inconstitucionais quaisquer medidas que, sem a criação de outros esquemas alternativos e compensatórios, se traduzam na prática em uma anulação ou revogação pura e simples.

---

[412] A autora também alega que além de conferir fundamento para a intervenção, a reserva de lei também acaba por minimizar a discricionariedade do intérprete, pois permite que o Poder Judiciário avalie se o caso concreto se enquadra à norma e fixe as condições a serem observadas durante a atuação dos órgãos de persecução penal. NERY, Nina. O compartilhamento de dados financeiros no sistema antilavagem de dinheiro brasileiro. São Paulo: Thompson Reuters Brasil, 2024.pg 118.

[413]DA SILVA, José Afonso. Comentário Contextual à Constituição. São Paulo. Editora Malheiros. 2007.

[414]CANOTILHO, J.J. Gomes; MOREIRA, Vital. Fundamentos da Constituição. Coimbra: Coimbra Editora, 1991.

A Teoria do Status, de Georg Jellinek[415], é uma base utilizada e difundida pela doutrina ao falar da classificação dos direitos fundamentais. Segundo a teoria, o status é a relação com o Estado que qualifica o indivíduo, ou seja, demonstra aquilo que ele é. Não se confunde com os direitos propriamente ditos, já que esses são detidos pelos indivíduos - uma pessoa é cidadã (status, "ser") detentora de x direitos ("ter"). Na doutrina estabelecida por Jellinek, os status são divididos da seguinte forma: Status Passivo (*status subjections*): referem-se às obrigações do indivíduo perante o Estado; Status Negativo (*status libertatis*): são as faculdades/liberdades do indivíduo em face do Estado (sentido estrito), assim como seus direitos de defesa (sentido amplo); Status Positivo (status civitatis): são as prestações positivas exigidas pelo indivíduo e que devem ser tomadas pelo Estado; Status Ativo (status da cidadania ativa): é a participação do indivíduo na atividade política.

A teoria dos quatro status, desenvolvida pelo Autor defende que os indivíduos podem se colocar sob quatro posições (status) perante o Estado: *status subjectionis* (ou passivo), status *negativus* (ou negativo), status civitatis (ou positivo) e *status activus* (ou ativo).

Depreende-se, portanto, que os direitos fundamentais são um conjunto de direitos e garantias que visam proteger a dignidade humana e assegurar a liberdade, igualdade e fraternidade de todos os indivíduos. Eles são classificados em quatro dimensões, que correspondem a diferentes gerações de direitos: Primeira dimensão: refere-se aos direitos de liberdade, como a liberdade de expressão, de pensamento, de religião, de associação, de reunião, de propriedade, de locomoção, entre outros. Esses direitos surgiram no contexto do constitucionalismo liberal do século XVIII e XIX, quando o Estado de Direito foi estabelecido como uma forma de limitar o poder do Estado e proteger os indivíduos contra a tirania e a arbitrariedade; Segunda dimensão: refere-se aos direitos sociais, econômicos e culturais, como o direito à educação, à saúde, ao trabalho, à moradia, à segurança social, à cultura, entre outros. Esses direitos surgiram no contexto do constitucionalismo social do século XX, quando o Estado de Bem-Estar Social foi estabelecido como uma forma de promover a justiça social e a igualdade material; Terceira dimensão: refere-se aos direitos coletivos, difusos e de solidariedade, como o direito ao meio ambiente saudável, ao desenvolvimento sustentável, à paz, à autodeterminação dos povos, entre outros. Esses direitos surgiram no contexto do constitucionalismo democrático e participativo do final do século XX e início do século XXI,

[415]Revista de Teorias e Filosofias do Estado. A justificativa do Estado na doutrina de Georg Jellinek. Disponível em: https://www.indexlaw.org/index.php/revistateoriasfilosofias/article/view/1141. Acessado em 27/05/2024.

quando a cidadania ativa e a participação popular foram reconhecidas como formas de fortalecer a democracia e a governança global; Quarta dimensão: refere-se aos direitos transindividuais, como o direito à informação, à privacidade, à segurança, à identidade, à diversidade, entre outros. Esses direitos surgiram no contexto do constitucionalismo cosmopolita e digital do século XXI, quando a globalização e a tecnologia transformaram as relações sociais e políticas em escala global e virtual; Quinta dimensão: Segundo Paulo Bonavides[416], o direito à paz, enquanto axioma da democracia participativa e supremo direito da humanidade, como um direito fundamental de quinta dimensão;

Cada dimensão dos direitos fundamentais tem suas próprias características, desafios e perspectivas. No entanto, todas elas têm em comum a ideia de que os Direitos Fundamentais são universais, inalienáveis, interdependentes e indivisíveis, e quem devem ser respeitados e protegidos pelo Estado e pela sociedade em geral.

A par disso, o Congresso Nacional promulgou, no dia 10 de fevereiro de 2022, a Emenda Constitucional número 115 de 2022[417], que modificou a Constituição Federal, para incluir a proteção de dados pessoais, elevando-o ao mesmo patamar dos direitos e garantias fundamentais. A alteração também fixou a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

A proteção de dados tornou-se uma garantia fundamental, prevista no Artigo 5º da Constituição Federal da República Federativa do Brasil de 1988. Embora o Direito Fundamental seja de extrema importância, noutro giro existe a polêmica de sua aplicação nas investigações criminais e na persecução penal, o que reforça a necessidade de uma análise preditiva da Lei Geral Penal de Proteção de Dados nos bancos de dados das polícias judiciárias brasileiras, como forma de aferir a ponderação de bens jurídicos e o princípio da proporcionalidade diante de eventual violação ao direito fundamental da proteção de dados pessoais nas investigações criminais.

---

[416]Quinta geração dos direitos fundamentais. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/534. Acessado em 27 de mai. 2024.

[417]BRASIL. Emenda Constitucional número 115 de 2022 - Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: < https://legis.senado.leg.br/norma/35485358. >. Acesso em 04 jan. 2024.

Apesar da existência de inúmeras diferenças entre as instituições policiais brasileiras, a maioria delas utiliza o mesmo método de "alimentação" dos seus bancos de dados. Os mecanismos de controle da atividade policial, seja das ouvidorias, do Ministério Público ou de outras instituições, são muito atuantes quando ocorre a má utilização dos dados. O debate será um divisor de águas para que a sociedade brasileira, através dos parlamentares, defina a atribuição e os limites dos órgãos de persecução penal.

É necessário abordar a discussão sobre a necessidade das polícias durante a investigação de um delito versus a preservação do direito fundamental de proteção de dados, sem retirar a autonomia e a força dos órgãos de investigação, o que fará com que seja possível a redução da impunidade e uma resposta rápida aos crimes que, em alguns casos, são de extrema gravidade e merecem uma resposta eficaz e imediata.

Uma sugestão para o acesso aos dados de forma íntegra, seria a criação, no âmbito das Polícias Judiciárias Brasileiras, de mecanismos que visem a utilização dos dados armazenados nos bancos de dados, sem violar o direito fundamental em questão. Outra forma de utilização é a criação de sistemas de prevenção, visando identificar, avaliar e mitigar o risco de ocorrência de desvios éticos no tratamento de dados; de detecção, visando contemplar mecanismos capazes de, tempestivamente, identificar e interromper eventual desvio ético que porventura não tenha sido evitado pelas ações de prevenção, possibilitando a responsabilização dos envolvidos; e de correção, cujo objetivo principal será estabelecer a responsabilização e a penalidade aplicável a cada caso de desvio ético comprovado, bem como possibilitar o aperfeiçoamento das fragilidades que originaram o respectivo desvio e a recuperação de eventuais prejuízos.

Identificar formas para a criação de políticas e procedimentos, ou seja, planos e ações de controle, com o intuito de elaborar uma norma visando esclarecer em que casos os órgãos de persecução penal podem fazer uso da ponderação de bens e do princípio da proporcionalidade diante de eventual violação ao direito fundamental da proteção de dados.

Daí surge a necessidade de restrição do direito fundamental da proteção de dados na investigação de alguns tipos de delitos, de forma que possa ser aplicada a devida adequação. O princípio da proporcionalidade ou da razoabilidade em essência, consubstancia uma pauta de

natureza axiológica que emana diretamente das ideias de justiça, equidade, bom senso, prudência, moderação, justa medida, proibição de excesso, direito justo e valores afins"[418].

Aplicando a mesma linha de raciocínio ao caso concreto, imagine que diante da investigação de um crime hediondo, determinados dados pessoais do autor do delito sejam utilizados sem o seu consentimento, violando eventual legislação de Proteção de Dados para a Segurança Pública e Persecução Penal, indo de encontro ao direito fundamental da proteção de dados previsto no Artigo 5º da Constituição Federal.

Embora todo e qualquer tipo de delito seja relevante para a atuação da atividade policial, imagine que o foco agora sejam os crimes de menor potencial ofensivo. Seria prudente a restrição do direito fundamental da proteção de dados para apuração de uma contravenção penal de perturbação da tranquilidade? Ou até mesmo para a elucidação da autoria de um crime contra a honra?

Diante da utilização dos princípios da proporcionalidade ou da razoabilidade, e levando em consideração a ponderação de bens, essa restrição não seria possível. E se estivermos diante crime de menor potencial ofensivo, como o de ameaça, previsto no Artigo 147 do Código Penal Brasileiro, por exemplo? Ainda assim a restrição a um direito fundamental seria excesso para apuração do referido delito? Depende. Se for uma ameaça comum, a violação precisa ser ponderada. Mas se essa ameaça resultar em uma invasão ao Congresso Nacional, ao Supremo Tribunal Federal e ao Palácio do Planalto, como ocorreu no último dia 08 de janeiro de 2023, ou até mesmo uma ameaça de morte ao Presidente da República ou a um Ministro do STF. É provável que o posicionamento adotado seja diferente.

Para que todo e qualquer direito fundamental seja preservado, é preciso que a análise passe pela técnica da ponderação de bens e pela aplicação da razoabilidade e da proporcionalidade. Apesar da intenção do legislador ter sido válida, vários outros critérios precisam ser levados em consideração no momento em que for votado o Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Persecução Penal, como por exemplo a análise de todas as notas técnicas analisadas anteriormente.

[418]NOVELINO, Marcelo. Curso de Direito Constitucional, 12ª ed. rev, ampl. e atual. Salvador: Ed. JusPodivm, 2017. p. 301.

Antes da proteção de dados se transformar em direito fundamental previsto na Constituição Federal, o Governo Federal editou a Media Provisória número 954/2020[419], que versou sobre o compartilhamento de dados por empresas de telecomunicações durante a pandemia. Conforme consta na Constituição Federal, as Medidas Provisórias são atos normativos, com força de lei, de competência exclusiva do Presidente da República, e podem ser adotadas em casos relevantes e urgentes.

O Plenário do Supremo Tribunal Federal suspendeu a eficácia dessa Medida Provisória, que previa o compartilhamento de dados de usuários de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE), para a produção de estatística oficial durante a pandemia do coronavírus. Firmou-se o entendimento de que o compartilhamento previsto na Medida Provisória violava o direito constitucional à intimidade, à vida privada e ao sigilo de dados[420].

Um dos argumentos utilizados pelos autores das ações que foram propostas junto ao Supremo Tribunal Federal foi o fato de que ao obrigar as empresas de telefonia fixa e móvel a disponibilizarem ao IBGE a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas, a Medida Provisória estaria violando dispositivos da Constituição Federal que asseguram a dignidade da pessoa humana, a inviolabilidade da intimidade, da vida provada, da honra e da imagem das pessoas, além do sigilo dos dados. Na ocasião, a Relatora da Ação, Ministra Rosa Weber, alegou que "não se pode legitimar, no combate à pandemia, o atropelo de garantias fundamentais consagradas na Constituição"[421].

O fato é que com o avanço da tecnologia, a proteção de dados passou a ser vista como uma das grandes preocupações do presente e do futuro. Embora a proteção de dados já estivesse implícita na Constituição Federal, a positivação dessa garantia de forma explícita, demonstra a preocupação do Estado com as necessidades que surgem em detrimento do avanço da tecnologia, o que gerará inúmeros debates por parte dos operadores do direito e de diversas outras profissões.

---

[419]BRASIL. Medida Provisória 954/2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm>. Acesso em: 21 abr. 2023.
[420]STF, ADI 6387, Tribunal Pleno, Rel. Min. Rosa Weber, J. 07.05.2020, DJe 12.11.2020.
[421]*Ibid.*

A inclusão do direito fundamental à proteção de dados em nossa Constituição Federal, fez com que qualquer cidadão tivesse a garantia de mais um instrumento de proteção ao direito da personalidade, visando resguardar a honra e a imagem. Antes disso, a proteção de dados era, tão somente, compreendida sob a perspectiva do direito à privacidade. Importante ressaltar que os direitos fundamentais devem estar amparados pelo princípio da dignidade da pessoa humana, garantido o mínimo necessário para a existência dos indivíduos[422].

Os direitos fundamentais são uma espécie de direito subjetivo, cujas diferenças residem na sua fundamentabilidade. A fundamentabilidade dos direitos fundamentais consiste em um conjunto de propriedades formais e materiais. Para que um direito seja considerado fundamental, um direito subjetivo precisa manifestar pelo menos uma propriedade formal. A fundamentabilidade formal é a previsão explícita dos direitos fundamentais na Constituição, ao passo que a fundamentabilidade material é a essência do que é um direito fundamental. Um direito subjetivo, portanto, precisa manifestar pelo menos uma propriedade material e uma propriedade formal para ser considerado fundamental, prevalecendo as propriedades materiais sobre as formais[423].

6.1 Constituição Federal de 1988, a Inviolabilidade de Dados e o Direito à Privacidade

Os litígios envolvendo o direito à preservação da honra e da intimidade e o direito da livre manifestação do pensamento e acesso à informação ganharam mais força na medida em que as tecnologias de difusão da informação foram aumentando, o que acontece até o presente momento. O direito ao esquecimento e à desindexação é um tema que entrou em evidência depois dos Recursos Especiais do caso Aída Curi (RE 1.335.153 - RJ) e Candelária (RE 1.334.097 - RJ). Os recursos serão mais amplamente abordados quando tratarmos sobre o entendimento dos Tribunais Superiores. Os referidos recursos foram muito bem fundamentados e são verdadeiros manuais sobre o direito ao esquecimento.

O Direito ao Esquecimento, ou direito de não ser lembrado, não é recente. O mecanismo de esquecimento ou direito de esquecimento começou a ser objeto de ações judiciais com o

[422]SARLET, Wolfgang Ingo. Dignidade da pessoa humana e direitos fundamentais na Constituição da República de 1988. Porto Alegre: Livraria do Advogado, 2002.
[423]PULIDO, Carlos Bernal. A fundamentalidade dos direitos fundamentais. Tradução: Ana Paula Soares Carvalho. In: ASENSI, Felipe Dutra; DE PAULA, Daniel Giotti (coord.). Tratado de direito constitucional: Constituição, política e sociedade. Rio de Janeiro: Campus JurídicoElsevier, 2013. p. 387-401.

início do funcionamento da google no Brasil, no ano de 2005. Nos Estados Unidos, o google começou a funcionar em 1998. Desde então, se analisarmos o histórico de demandas no judiciário que envolvem o tema, aferiremos que milhares de pessoas já ajuizaram ações com pedidos de esquecimento e desindexação em desfavor de provedores de busca da internet, sempre com o objetivo de proteção dos dados pessoais e da privacidade.

O direito ao esquecimento, também conhecido como direito de apagamento, é um conceito importante no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. Este direito permite que indivíduos solicitem a exclusão de seus dados pessoais armazenados por organizações ou provedores de serviços.

O GDPR, especificamente no artigo 17, define as condições em que o direito ao apagamento se aplica e estabelece um prazo de um mês para que as organizações respondam a essas solicitações. No entanto, este direito não é absoluto e pode haver circunstâncias em que a exclusão dos dados não seja possível, como quando os dados são necessários para o exercício da liberdade de expressão ou para o cumprimento de uma obrigação legal[424].

[424]Eur-Lex. GDPR. Artigo 17º do RGPDDireito ao apagamento ('direito de ser esquecido') 1. O titular dos dados tem o direito de obter do responsável pelo tratamento o apagamento dos dados pessoais que lhe digam respeito, sem demora injustificada, e o responsável pelo tratamento tem a obrigação de apagar os dados pessoais sem demora injustificada, sempre que se aplique um dos seguintes motivos: (a). os dados pessoais não são mais necessários para a finalidade que motivou a sua recolha ou tratamento; (b). o titular dos dados retira o consentimento em que se baseia o tratamento, nos termos do artigo 6.º , n.º 1, alínea a), ou do artigo 9.º , n.º 2, alínea a), e quando não exista outro fundamento jurídico para o tratamento; (d). o titular dos dados se opõe ao tratamento nos termos do artigo 21.º (1) e não existem motivos legítimos imperiosos para o tratamento, ou o titular dos dados se opõe ao tratamento nos termos do artigo 21.º (2); (e) os dados pessoais foram processados ilegalmente; (f). os dados pessoais têm de ser apagados para cumprimento de uma obrigação legal prevista no direito da União ou dos Estados-Membros à qual o responsável pelo tratamento esteja sujeito; 2. os dados pessoais foram recolhidos em relação à oferta de serviços da sociedade da informação referidos no artigo 8.º 2. Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado, nos termos do parágrafo 1, a apagar os dados pessoais, o responsável pelo tratamento, tendo em conta a tecnologia disponível e o custo de implementação, tomará medidas razoáveis, incluindo medidas técnicas, para informar os responsáveis pelo tratamento que estão a processar os dados pessoais de que o titular dos dados solicitou a eliminação por esses responsáveis de quaisquer ligações, cópias ou replicações desses dados pessoais. 3. Os parágrafos 1 e 2 não se aplicam na medida em que o tratamento seja necessário: (a). para exercer o direito à liberdade de expressão e informação; (b)para cumprimento de uma obrigação legal que exija o tratamento nos termos do direito da União ou do Estado-Membro ao qual o responsável pelo tratamento esteja sujeito ou para a execução de uma tarefa de interesse público ou no exercício da autoridade pública de que está investido o responsável pelo tratamento; (c) por razões de interesse público no domínio da saúde pública, em conformidade com as alíneas h) e i) do artigo 9.º (2), bem como com o artigo 9.º (3); (d) para fins de arquivamento de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.º (1), na medida em que o direito referido no n.º 1 seja suscetível de tornar impossível ou prejudicar gravemente a concretização dos objetivos desse tratamento; ou (e) para o estabelecimento, exercício ou defesa de reivindicações legais.

No Brasil, a Lei Geral de Proteção de Dados (LGPD) também aborda o direito ao esquecimento, embora com algumas diferenças em relação ao GDPR. A LGPD permite que os titulares de dados solicitem a exclusão de seus dados pessoais em determinadas situações, como quando os dados não são mais necessários para os fins para os quais foram coletados ou quando o titular retira o consentimento[425].

Necessária fazer essa abordagem porque conforme será visto adiante, a Polícia Civil do Distrito Federal não definiu a temporalidade dos dados armazenados. O problema do armazenamento de dados nos bancos de dados da PCDF é justamente a sua utilização para fins penais. Diante da recusa de exclusão do apagamento desses dados, o titular pode ser utilizar de um incidente judicial, que inclusive pode ser provocado pelas partes, para solicitar, por analogia, com base no art. 9º da Lei de Interceptação Telefônica, o descarte dos dados que foram arrecadados no âmbito de uma investigação[426].

A falta de razoabilidade e proporcionalidade ao se permitir um armazenamento eterno de dados para fins penais aparenta ter aspectos de incongruência até mesmo com as leis mais recentes que criaram bancos de dados de identificação digital de perfis genéticos, conforme foi visto alhures. Nesses casos, o legislador criou hipóteses e limites de tempo, já que em caso de absolvição, por exemplo, o investigado pode ter seus dados excluídos do banco de dados de perfis genéticos. Mesmo nos casos em que o legislador fez uma opção em casos de crimes mais graves, foram criados limites. Não é coerente com o sistema, portanto, imaginar que para qualquer outro crime o Estado pode fazer mais do que o a lei permite para determinados crimes específicos.

O direito ao esquecimento, porém, que hoje é amplamente divulgado em diversas Decisões Judicias, começou a ganhar força com a criação do *General Data Protection Regulation* – GDPR, que, conforme já mencionado anteriormente, serviu como fonte de

[425]BRASIL. Lei Geral de Proteção de Dados. Lei nº 13.709/2018. Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

[426]BRASIL. Lei das interceptações telefônicas. Lei nº 9.296/1996. Art. 9° A gravação que não interessar à prova será inutilizada por decisão judicial, durante o inquérito, a instrução processual ou após esta, em virtude de requerimento do Ministério Público ou da parte interessada. Parágrafo único. O incidente de inutilização será assistido pelo Ministério Público, sendo facultada a presença do acusado ou de seu representante legal. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em 28 de nov. 2024.

inspiração para a elaboração da nossa Lei Geral de Proteção de Dados. O Direito ao Esquecimento ganhou mais notoriedade no próprio Tribunal de Justiça da União Europeia, após o case Mario Costeja Gonçalez, cidadão espanhol, x Google[427].

O senhor Gonzales ajuizou uma ação em desfavor da google espanhola, sob a alegação de que qualquer internauta que digitasse seu nome nesse site de busca, teria acesso a uma lista de resultado que mostrava links para duas páginas de um determinado jornal, onde constava o anúncio de um leilão imobiliário que havia sido organizado depois de um processo de penhora para a quitação de dívidas previdenciárias devidas pelo Senhor Gonzáles, que solicitou que a google removesse ou ocultasse as páginas que lhe faziam menção, para que as informações não mais aparecessem.

De imediato, a google recusou o pedido do senhor Gonzales. O caso foi parar na Agência Espanhola de Proteção de Dados e posteriormente foi destinado ao Tribunal de Justiça da União Europeia. Em aproximadamente duas semanas, o referido Tribunal emitiu duas decisões distintas sobre o mesmo tema[428]. No dia 24 de setembro de 2019, o Tribunal de Justiça da União Europeia decidiu um caso em que a Google só deveria atender a solicitação de remoção de dados que estivesse em buscadores hospedados em países que integravam o bloco da União Europeia.

O mesmo Tribunal, porém, alguns dias depois, tomou uma decisão em sentido contrário, entendendo que o Facebook, Twiter e Instagram estariam obrigados a removerem informações de usuários não apenas nos países que compõe o Bloco da União Europeia, mas em todo o mundo. Na decisão em tela, o Tribunal justificou a diferença alegando que a Google seria apenas um intermediário e não um hospedeiro de conteúdo, o que justificaria essa diferença nas decisões. Fica evidente que o tema ainda não está pacificado e que muito ainda será discutido.

Muito se fala do direito ao esquecimento. É importante frisar que esse direito está intimamente relacionado à desindexação do conteúdo exposto. Essa desindexação não seria um

[427]Supremo Tribunal Federal. Boletim de Jurisprudência Internacional. Direito ao Esquecimento. 2018. Disponível em: https://www.stf.jus.br/arquivo/cms/jurisprudenciaBoletim/anexo/BJI5_DIREITOAOESQUECIMENTO.pdf. Acesso em 28 de nov. 2024.

[428]O Globo. Europa limita lei de 'direito a ser esquecido' na internet. Disponível em: https://oglobo.globo.com/mundo/europa-limita-lei-de-direito-ser-esquecido-na-internet-23970764. Acesso em: 24 jul. 2020.

apagamento de dados. Seria, tão somente, uma espécie de dificultar o acesso a determinados tipos de informações.

Apenas para ilustramos, imaginemos que precisemos ir até uma biblioteca para realizar uma pesquisa sobre determinado assunto. Que nessa biblioteca não haja funcionários, não haja prateleiras e não haja identificação dos livros. Os livros estão todos jogados ao chão. Nós sabemos que a informação que queremos está ali, no meio daqueles livros. Ocorre que teremos uma certa dificuldade para localizar as informações. É exatamente isso que ocorre na desindexação.

Muito importante mencionar que para alguns estudiosos do tema, o direito ao esquecimento que não se trata de direito ao esquecimento propriamente dito. Alegam que o melhor seria chamá-lo de mecanismo de esquecimento, uma vez que não há nada que o tipifique como direito.

Quando debatemos o direito ao esquecimento e o direito à desindexação, geralmente estamos diante de um embate jurídico que versa sobre o direito à intimidade e privacidade x direito à informação, direito à liberdade de imprensa e não censura. Podemos dizer, inclusive, que temos três espécies de Direito ao Esquecimento.

A primeira espécie, está vinculada, geralmente, à utilização, por parte da imprensa, de fatos que estão amplamente divulgados na internet, e são utilizados sem o devido consentimento do envolvido ou da família do envolvido caso ele tenha falecido. A segunda fala sobre o envolvido que solicita a remoção ou a desindexação de acesso à alguma informação que esteja armazenada em um determinado site de busca. A terceira fala sobre aquele que foi denunciando, condenado, cumpriu a sua pena, porém terá a sua vida exposta perpetuamente na internet e que também deseja fazer a remoção de qualquer conteúdo que faça menção ao seu nome.

Em todas essas todas essas situações, teremos direitos do mesmo status constitucional, que devem ser analisados através de uma ponderação de bens. Observa-se, porém, que há uma tendência de que a doutrina e a jurisprudência deem preferência ao direito de liberdade de expressão.

O fato é que todas as pessoas, seja um político, seja famoso ou seja um anônimo, todas tem direito à privacidade. Muitos alegam que se analisa o grau de maturidade de um povo pela imprensa que ele possui. O que parece é que a maioria dos países latino americanos ainda ostentam cicatrizes causadas pela ditadura. A pergunta que fica é: por conta desse trauma, a impressa pode agir com irresponsabilidade, lesando o direito à intimidade e à privacidade? Entendo que cada caso será analisado de forma isolada.

Sobre o tema, temos, conforme mencionado anteriormente, como referência os Recursos Especiais 1.335.153 – RJ[429] (Caso Ainda Curi) e o RE 1.334.09 – RJ[430] (Caso Candelária). No primeiro RE, a família de Aida Curi, que foi brutalmente morta em Copacabana, em 1958, depois de ter sido jogada de um prédio, ajuizou uma ação em desfavor da rede globo, por conta da exibição da simulação da morte de Aida Curi no programa linha direta, sem o consentimento da família da vítima.

A família de Aida Curi não teve o direito ao esquecimento reconhecido em primeira e segunda instâncias. O caso foi parar no Superior Tribunal de Justiça, que negou provimento ao recurso especial, decidindo sim pelo direito ao esquecimento, sem, contudo, ter garantido aos familiares um pretendido direito à indenização. Apenas a título de curiosidade, se pesquisarmos o nome Ainda Curi no google, aparecem 468 mil resultados para a pesquisa. No caso Mario Costeja Gonçalez versus google são localizados 146 mil resultados

O mais curioso é que em todos esses casos, a busca pelo esquecimento tornou os envolvidos ainda mais lembrados. Atualmente o caso Ainda Curi está no Supremo Tribunal Federal e já foi reconhecido como sendo de repercussão geral. O STF está dano muita importância ao tema, e chegou a fazer uma audiência pública, com participação de todos os interessados na causa, com o intuito auxiliar os seus próprios ministros a tomarem uma decisão.

Em parecer juntado aos autos, a Procuradoria Geral da República propôs a tese de que o direito ao esquecimento seja um desdobramento do direito à privacidade, e que deve ser ponderado no caso concreto, com a proteção do direito à informação e à liberdade de expressão.

[429]STJ, RE 1.335.153 RJ, Quarta Turma, Rel. Luis Felipe Salomão, J. 28.05.2013, DJe 10.09.2013.
[430]STJ, RE 1.334.097 RJ, Quarta Turma, Rel. Luis Felipe Salomão, J. 09.11.2021, DJe 01.02.2022.

No final das contas, essa tese proposta pela PGR continuou com a manutenção da incógnita sobre o que o STF de fato decidirá.

O fato é que se fossemos analisar o relatório do Ministro Luís Felipe Salomão e o que foi decidido na ação judicial do cantor Roberto Carlos, saberíamos que o STF referendaria o que foi decido pelo Ministro Luís Felipe Salomão, sendo favorável à liberdade de imprensa. Apesar da decisão do STF[431] se tratar de conteúdo televisivo, certamente afetou o curso do debate sobre direito ao esquecimento e desindexação de resultados em provedores de busca.

[431]Supremo Tribunal Federal. STF conclui que direito ao esquecimento é incompatível com a Constituição Federal. Por decisão majoritária, nesta quinta-feira (11), o Supremo Tribunal Federal (STF) concluiu que é incompatível com a Constituição Federal a ideia de um direito ao esquecimento que possibilite impedir, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos em meios de comunicação. Segundo a Corte, eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, com base em parâmetros constitucionais e na legislação penal e civil. O Tribunal, por maioria dos votos, negou provimento ao Recurso Extraordinário (RE) 1010606, com repercussão geral reconhecida, em que familiares da vítima de um crime de grande repercussão nos anos 1950 no Rio de Janeiro buscavam reparação pela reconstituição do caso, em 2004, no programa "Linha Direta", da TV Globo, sem a sua autorização. Após quatro sessões de debates, o julgamento foi concluído hoje, com a apresentação de mais cinco votos (ministra Cármen Lúcia e ministros Ricardo Lewandowski, Gilmar Mendes, Marco Aurélio e Luiz Fux).Solidariedade entre gerações. Ao votar pelo desprovimento do recurso, a ministra Cármen Lúcia afirmou que não há como extrair do sistema jurídico brasileiro, de forma genérica e plena, o esquecimento como direito fundamental limitador da liberdade de expressão "e, portanto, "como forma de coatar outros direitos à memória coletiva". Cármen Lúcia fez referência ao direito à verdade histórica no âmbito do princípio da solidariedade entre gerações e considerou que não é possível, do ponto de vista jurídico, que uma geração negue à próxima o direito de saber a sua história. "Quem vai saber da escravidão, da violência contra mulher, contra índios, contra gays, senão pelo relato e pela exibição de exemplos específicos para comprovar a existência da agressão, da tortura e do feminicídio?", refletiu. Ponderação de valores. No voto em que acompanhou o relator, ministro Dias Toffoli, pelo desprovimento do RE, o ministro Ricardo Lewandowski afirmou que a liberdade de expressão é um direito de capital importância, ligado ao exercício das franquias democráticas. No seu entendimento, enquanto categoria, o direito ao esquecimento só pode ser apurado caso a caso, em uma ponderação de valores, de maneira a sopesar qual dos dois direitos fundamentais (a liberdade de expressão ou os direitos de personalidade) deve ter prevalência. "A humanidade, ainda que queira suprimir o passado, ainda é obrigada a revivê-lo", concluiu. Exposição vexatória. Por outro lado, o ministro Gilmar Mendes votou pelo parcial provimento do RE, acompanhando a divergência apresentada pelo ministro Nunes Marques. Com fundamento nos direitos à intimidade e à vida privada, Mendes entendeu que a exposição humilhante ou vexatória de dados, da imagem e do nome de pessoas (autor e vítima) é indenizável, ainda que haja interesse público, histórico e social, devendo o tribunal de origem apreciar o pedido de indenização. O ministro concluiu que, na hipótese de conflito entre normas constitucionais de igual hierarquia, como no caso, é necessário examinar de forma pontual qual deles deve prevalecer para fins de direito de resposta e indenização, sem prejuízo de outros instrumentos a serem aprovados pelo Legislativo. Ares democráticos. O ministro Marco Aurélio também seguiu o relator. A seu ver, o artigo 220 da Constituição Federal, que assegura a livre manifestação do pensamento, da criação, da expressão e da informação, está inserido em um capítulo que sinaliza a proteção de direitos. "Não cabe passar a borracha e partir para um verdadeiro obscurantismo e um retrocesso em termos de ares democráticos", avaliou. Segundo o ministro, os veículos de comunicação têm o dever de retratar o ocorrido. Por essa razão, ele entendeu que decisões do juízo de origem e do órgão revisor não merecem censura, uma vez que a emissora não cometeu ato ilícito. Fato notório e de domínio público. Para o presidente do STF, ministro Luiz Fux, é inegável que o direito ao esquecimento é uma decorrência lógica do princípio da dignidade da pessoa humana, e, quando há confronto entre valores constitucionais, é preciso eleger a prevalência de um deles. Para o ministro, o direito ao esquecimento pode ser aplicado. Mas, no caso dos autos, ele observou que os fatos são notórios e assumiram domínio público, tendo sido retratados não apenas no programa televisivo, mas em livros, revistas e jornais. Por esse motivo, ele acompanhou o relator pelo desprovimento do recurso. Não participou do julgamento o ministro Luís Roberto Barroso, que declarou sua suspeição, por já ter atuado, quando era advogado, em outro processo da ré em situação parecida com a deste julgamento. Tese. A tese de repercussão geral firmada no julgamento foi a seguinte: "É incompatível com a Constituição Federal a ideia de um direito ao esquecimento,

No caso do cantor Roberto Carlos o Supremo Tribunal Federal liberou biografias sem autorização prévia, sob a alegação de que a biografia de uma pessoa não se escreve a vida de uma pessoa, mas o relato de um povo e os caminhos de uma sociedade, defendendo, desta forma, a liberdade de expressão e o direito à informação.

Sobre o Recurso Especial 1334.097 – RJ, um dos indiciados na chacina da candelária foi submetido a júri e absolvido por negativa de autoria pela unanimidade dos membros do conselho de sentença. Novamente a rede globo tentou entrar em contato com o ofendido para tentar agendar uma entrevista, o que negado.

Para a surpresa do envolvido, o programa linha direta foi ao ar, mencionado que o autor havia sido apontado como um dos autores na chacina, mas que havia sido absolvido no júri. Diante disso ele decidiu ajuizar uma ação de indenização por danos morais, além de ter pleiteado o direito ao esquecimento. Em primeira instância o pedido indenizatório foi julgado improcedente. Em segunda instância, em grau de apelação, a sentença foi reformada e a rede globo foi condenada.

O caso também foi parar no Superior Tribunal de Justiça, onde, mais uma vez, o Ministro Luís Felipe Salomão foi o relator. Foi negado o provimento ao recurso especial. Em seu relatório, o Ministro Luís Felipe Salomão reconheceu o direito ao esquecimento com a manutenção da responsabilidade pelo ressarcimento.

Importante frisar que tanto no caso Aida Curi, quanto no caso da Candelária, o Superior Tribunal de Justiça se fundamentou no enunciado 531 da VI Jornada de Direito Civil. Esses julgados nos trazem dois elementos muito importantes. O primeiro diz respeito ao fato de que novas tecnologias vêm trazendo especial preocupação no tocante ao aspecto da dignidade. O

assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social – analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais, especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral, e as expressas e específicas previsões legais nos âmbitos penal e civel".
Disponívelem:https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=460414&ori=1&post_type=eventos&s=gestao. Acesso em 03 de out. 2024.

segundo elemento desse enunciado faz uma ressalva à importância da dimensão pública e ao direito à informação.

Também é importante comentar que recentemente um famoso apresentador de televisão teve sua vida pessoal exposta em sites da internet, após envolver-se em um suposto caso extraconjugal. O fato aconteceu no Estado de São Paulo. Em primeira instância, esse apresentador conseguiu uma decisão favorável e teve o reconhecido o seu direito de retirar dos sites de busca da internet todos os conteúdos sobre esse suposto caso extra conjugal

O Tribunal de Justiça, porém, reverteu a decisão de segunda instância, alegando que salvo em situações excepcionalíssimas, não cabe impor ao provedor de pesquisas a obrigação de desindexação de sítios existente na rede mundial de computadores. Os Desembargadores entenderam que no caso em questão, entre o direito à intimidade e a liberdade de expressão e opinião de imprensa, prevalecem essas últimas, sob pena de censura.

Alguns doutrinadores alegam que o esquecimento fere o direito à informação e a liberdade de imprensa, mas a quem interessa saber que um apresentador de televisão teve um caso extraconjugal? Será que no futuro nós mediremos a maturidade do nosso povo e a liberdade de imprensa do nosso país com base nesse tipo de informação? Cabe uma reflexão. O melhor equacionamento será sempre observar as particularidades do caso concreto. Antigamente, cada estado decidia de uma forma diferente. Seja em primeira ou segunda instância.

Com a decisão do STF, proferida no dia 11 de fevereiro de 2021[432], foi pacificado o entendimento de que o direito ao esquecimento é incompatível com a Constituição Federal, mitigando, dessa forma, o direto à privacidade. O Supremo Tribunal Federal (STF), concluiu que é incompatível com a Constituição Federal a ideia de um direito ao esquecimento que possibilite impedir, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos em meios de comunicação.

Ainda de acordo com a Corte, eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, com base em parâmetros

[432] *Ibid.*

constitucionais e na legislação penal e civil. O Tribunal negou, por maioria dos votos, provimento ao Recurso Extraordinário (RE) 1010606, com repercussão geral reconhecida. Quando votou pelo desprovimento do recurso, a Ministra Cármen Lúcia afirmou que não há como extrair do sistema jurídico brasileiro, de forma genérica e pela, o esquecimento como direito fundamental limitador da liberdade de expressão e, portanto, como forma de coatar outros direitos à memória coletiva.

Carmén Lúcia fez referência ao direito à verdade histórica no âmbito do princípio da solidariedade entre gerações e considerou que não é possível, do ponto de vista jurídico, que uma geração negue à próxima o direito de saber a sua história. No voto em que acompanhou o relator, Ministro Dias Toffoli, pelo desprovimento do RE, o Ministro Ricardo Lewandowski afirmou que a liberdade de expressão é um direito de capital importância, ligado ao exercício das franquias democráticas. No seu entendimento, enquanto categoria, o direito ao esquecimento só pode ser apurado caso a caso, em uma ponderação de valores, de maneira sopesar qual dos dois direitos fundamentais (a liberdade de expressão ou os direitos de personalidade) deve ter prevalência.

O Ministro Gilmar Mendes votou pelo parcial provimento do RE, acompanhando a divergência apresentada pelo Ministro Nunes Marques. Com fundamento nos direitos à intimidade e à vida privada, Mendes entendeu que a exposição humilhante ou vexatória de dados, da imagem e do nome de pessoas, seja autor ou vítima, é indenizável, ainda que haja interesse público, histórico e social, devendo o tribunal de origem apreciar o pedido de indenização. Reforçou, ainda, que na hipótese de conflito entre normas constitucionais de igual hierarquia, como no caso em tela, é necessário examinar de forma pontual qual deves deve prevalecer para fins de direito de resposta e indenização, sem prejuízo de outros instrumentos a serem aprovados pelo Legislativo.

Da mesma forma, o Ministro Marco Aurelio também seguiu o relator, soba a alegação de que o Artigo 220 da Constituição Federal, que assegura a livre manifestação do pensamento, da criação, da expressão e da informação, está inserido em um capítulo que sinaliza a proteção de direitos. Segundo o Ministro Luiz Fux, é inegável que o direito ao esquecimento é uma decorrência lógica do princípio da dignidade da pessoa humana, e quando há confronto entre valores constitucionais, é preciso eleger a prevalência de um deles. Para o ministro, o direito ao esquecimento pode ser aplicado, mas no caso em questão foi observado que os fatos eram

notórios e assumiram domínio público, já que foram retratados não apenas no programa televisivo, mas em livros, revistas e jornais.

A tese de repercussão geral formada no julgamento foi a seguinte:

> É incompatível com a Constituição Federal a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social – analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais, especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral, e as expressas e específicas previsões legais nos âmbitos penal e cível.

6.2 Normas que já Regulamentavam a Privacidade Proteção de Dados Pessoais no Ordenamento Jurídico Brasileiro

A era digital nos trouxe a necessidade de tutelarmos a nossa privacidade, com o intuito de proteger dados pessoais. Foi justamente por conta desse avanço da tecnologia, que a União Europeia editou a Diretiva 95/46/CE[433] do Parlamento Europeu. Essa diretiva estabeleceu que o tratamento e dados pessoais deve respeitar as liberdades e os direitos fundamentais previstos no artigo 1º. No ano de 2002, foi a vez do Parlamento Europeu editar a Diretiva 2022/58/CE[434], que fala sobre o tratamento de dados pessoais e a proteção da privacidade das comunicações eletrônicas.

A proteção de dados no Brasil vem sendo compreendida como uma extensão dos direitos da personalidade. Por esse motivo, os dados referentes ao nome, à intimidade, à vida privada, à honra e à imagem das pessoas já estavam previstos na Constituição Federal e no ordenamento jurídico infraconstitucional, antes da proteção de dados se transformar em direito fundamental. A Lei Geral de Proteção de Dados, portanto, apenas reforçou que já estava previso de forma implícita.

O Artigo 5º da Constituição Federal afirma que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente

---

[433]Diretiva 95/46/CE. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em 26 abri. 2024.
[434]*Ibid.*

de sua violação. Da mesma forma, o Artigo 11 Código Civil Brasileiro menciona que os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

Também no Brasil, houve, no ano de 2014, a edição do Marco Civil da Internet – Lei número 12.965/2014[435], que instituiu vários princípios, disciplinando o uso da internet e protegendo a privacidade e os dados pessoais. Isso acabou refletindo nas Decisões proferidas Tribunais Superiores, STJ e STF, nos julgamentos de casos que envolveram o direito ao esquecimento. Essas decisões judiciais precisaram buscar o equilíbrio entre o direito de informação e o direito à privacidade e à dignidade da pessoa humana, sob o prisma do Processo Penal. O tema ganhou maior repercussão após a entrada do sancionamento da Lei número 13.709/2018 (Lei Geral de Proteção de Dados). De um lado, temos o interesse da ampla divulgação de informações, amparada sob o fundamento do afastamento de qualquer prática que possa configurar algum tipo de censura, e de outro lado temos aqueles que não querem ver sua intimidade exposta, por algum fato de foro íntimo que não caracterize informação de interesse público.

De qualquer forma, é importante que reconheçamos os principais dispositivos que já abordavam, ainda que de forma incipiente, a proteção ou a utilização de dados pessoais no ordenamento jurídico brasileiro.

O art. 1º da Constituição Federal, por exemplo, fez a previsão de que a República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em estado de direito e tem como fundamentos a dignidade da pessoa humana[436]. Da mesma forma, os incisos X, XII, XXXIII, XXXIV "b", LXXII e LXXVII, todos do artigo 5º da Constituição Federal, fizeram menção ao direito à privacidade[437].

---

[435]BRASIL. Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 26 abr.2024.

[436]Brasil. Constituição Federal. Artigo 1º: A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em estado de direito e tem como fundamentos (...) III – a dignidade da pessoa humana (...) Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 28 de nov. 2024.

[437]Brasil. Constituição Federal. Artigo 5º: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; XIV – é assegurado a todos o cesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional; XXXIII - todos têm direito a receber dos órgãos públicos

O Código Penal resguardou a privacidade, quando tipificou como crime a divulgação de segredo e a violação do segredo profissional, fazendo a ressalva de que não é permitido divulgar, sem justa causa, conteúdo de documento particular ou correspondência confidencial ou informações sigilosas ou reservadas, contidas ou não nos sistemas de informações ou "bancos de dados da Administração Pública. Também foi tipificada a conduta de invasão de dispositivo informático e a inserção de dados falsos em sistemas de informações."[438].

O Código de Processo Penal, por sua vez, preceitua que para determinados tipos de crimes, o membro do Ministério Público ou o Delegado e Polícia poderão requisitar, de quaisquer órgãos do poder público ou de empresas da iniciativa privada, dados e informações cadastrais da vítima ou de suspeitos. Nos casos de crimes mais graves, também foi mencionado que se necessário à prevenção e a repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o Delegado de Polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviços de telecomunicações e/ou telemáticas, que disponibilizem imediatamente os meios técnicos adequados, como sinais, informações e outros que permitam a localização da vítima ou dos suspeitos do delito em curso[439].

---

informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado; XXXIV - são a todos assegurados, independentemente do pagamento de taxas: a) o direito de petição aos Poderes Públicos em defesa de direitos ou contra ilegalidade ou abuso de poder; b) a obtenção de certidões em repartições públicas, para defesa de direitos e esclarecimento de situações de interesse pessoal; LXXII - conceder-se-á *"habeas-data":* a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; LXXVII - são gratuitas as ações de *"habeas-corpus"* e *"habeas-data"*, e, na forma da lei, os atos necessários ao exercício da cidadania. LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 28 de nov. 2024.

[438]BRASIL. Código Penal Brasileiro. Decreto-Lei nº 2.848, de 07 de dezembro de 1940. **Divulgação de Segredo.** Artigo 153: Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem: § 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: (Incluído pela Lei nº 9.983, de 2000); **Violação do segredo profissional**. Artigo 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: **Invasão de dispositivo informático** (Incluído pela Lei nº 12.737, de 2012) . Artigo 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021). **Inserção de dados falsos em sistema de informações** (Incluído pela Lei nº 9.983, de 2000). Artigo 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: (Incluído pela Lei nº 9.983, de 2000)). Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 28 de nov. 2024.

[439]BRASIL. Código de Processo Penal. Artigo 13-A. Nos crimes previstos nos arts. 148, 149 e 149-A, no § 3º do art. 158 e no art. 159 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal), e no art. 239 da Lei

A Lei número 7.116/83, que assegura a validade nacional às carteiras de identidade já fazia menção a diversos dados pessoais e à base de dados da receita federal[440]. A Lei número 7.232 também fez uma previsão, considerando atividades de informática aquelas ligadas ao tratamento racional e automático da informação, especificamente a estruturação e exploração de base de dados[441]. Da mesma forma, o Código de Defesa do Consumidor frisou que o consumidor pode ter acesso às informações existente em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como as suas respectivas fontes. Aqui merece destaque outra previsão do CDC, pune criminalmente quem impedir ou dificultar acesso de consumidor às informações sobre ele em cadastros, bancos de dados, fichas e registros ou até mesmo deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata[442].

nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), o membro do Ministério Público ou o delegado de polícia poderá requisitar, de quaisquer órgãos do poder público ou de empresas da iniciativa privada, dados e informações cadastrais da vítima ou de suspeitos; Artigo 13-B. Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 28 de nov. 2024.

[440]BRASIL. Lei nº 7.716 de 29 de agosto de 1983. Assegura validade nacional às carteiras de identidade, regula sua expedição e dá outras providências. Artigo 3º - A Carteira de Identidade conterá os seguintes elementos: a) Armas da República e inscrição "República Federativa do Brasil"; b) nome da Unidade da Federação; c) identificação do órgão expedidor; d) registro geral no órgão emitente, local e data da expedição; e) nome, filiação, local e data de nascimento do identificado, bem como, de forma resumida, a comarca, cartório, livro, folha e número do registro de nascimento; f) fotografia, no formato 3 x 4 cm, assinatura e impressão digital do polegar direito do identificado; g) assinatura do dirigente do órgão expedidor; h) número de inscrição no Cadastro de Pessoas Físicas (CPF). § 1º A inclusão do número de inscrição no CPF na Carteira de Identidade, conforme disposto na alínea "h" do **caput** deste artigo, ocorrerá sempre que o órgão de identificação tiver acesso a documento comprobatório ou à base de dados administrada pela Secretaria Especial da Receita Federal do Brasil § 1º O órgão emissor deverá, na emissão de novos documentos, utilizar o número de inscrição no CPF como número de registro geral da Carteira de Identidade. § 2º A incorporação do número de inscrição no CPF à Carteira de Identidade será precedida de consulta e de validação com a base de dados administrada pela Secretaria Especial da Receita Federal do Brasil. § 2º Os órgãos emissores de registro geral deverão realizar pesquisa na base do CPF, a fim de verificar a integridade das informações, bem como disponibilizar dados cadastrais e biométricos do registro geral à Secretaria Especial da Receita Federal do Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/1980-1988/l7116.htm. Acesso em 28 de nov. 2024.

[441]BRASIL. Lei nº 7.232 de 29 de outubro de 1984. Dispõe sobre Política Nacional de Informática, e dá outras providências. Artigo 3º. Para os efeitos desta Lei, consideram-se atividades de informática aquelas ligadas ao tratamento racional e automático da informação e, especificamente as de: IV - estruturação e exploração de bases dedados;Disponívelem:https://www.planalto.gov.br/ccivil_03/Leis/L7232.htm#:~:text=LEI%20N%C2%BA%207.232%2C%20DE%2029%20DE%20OUTUBRO%20DE%201984.&text=Disp%C3%B5e%20sobre%20a%20Pol%C3%ADtica%20Nacional,Art.. Acesso em 28 de nov. 2024.

[442]BRASIL. Lei nº 8.078 de 11 de setembro de 1990. Código de Defesa do Consumidor. Artigo 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. Das infrações Penais: Artigo 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros. Artigo 73. Deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em 28 de nov. 2024.

A Lei número 9.472/1997, que dispõe sobre a organização dos serviços de telecomunicações prevê que o usuário de serviços de telecomunicações tem direito à inviolabilidade e ao segredo de sua comunicação, salvo nas hipóteses e condições constitucional e legalmente previstas. Além disso, também prevê que o usuário tem direito ao respeito de sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora de serviço[443]. A Lei do *Habeas Data* considerou de caráter público todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações[444].

A Lei número 9.504/97, que estabelece normas para as eleições, pontuou que mediante requerimento à Justiça Eleitoral, os partidos poderão ter acesso ao sistema interno de controle, verificação e fiscalização da coleta de dados. Das entidades que divulgaram pesquisas de opinião relativas às eleições, incluídos os referentes à identificação dos entrevistadores e, por meio de escolha livre e aleatória de planilhas individuais, mapas ou equivalentes, confrontar e conferir os dados publicados, preservada a identidade dos respondentes[445].

A Lei número 12.414/2021, que disciplina a formação e consulta a banco de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas para a formação de histórico de crédito dispõe que os bancos de dados instituídos ou mantidos por pessoas jurídicas de direito público interno serão regidos por legislação específica. Para os efeitos da lei é considerado banco de dados o conjunto de dados relativo à pessoa natural ou jurídica armazenados com a finalidade de subsidiar a concessão de crédito, a realização de venda a prazo ou de outras transações comerciais e empresariais que impliquem em risco financeiro[446].

---

[443]BRASIL. Lei nº 9.742, de 16 de julho de 1997. Dispõe sobre a utilização dos serviços de telecomunicações. Disponívelem:https://www.planalto.gov.br/ccivil_03/leis/l9472.htm#:~:text=LEI%20N%C2%BA%209.472%2C%20DE%2016%20DE%20JULHO%20DE%201997.&text=Disp%C3%B5e%20sobre%20a%20organiza%C3%A7%C3%A3o%20dos,Constitucional%20n%C2%BA%208%2C%20de%201995. Acesso em 29 de nov. 2024.

[444]BRASIL. Lei nº 9.507 de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data.

[445]BRASIL. Lei nº 9.504 de 30 de setembro de 1997. Estabelece normas para as eleições. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em 29 de nov. 2024.

[446]BRASIL. Lei nº 12.414, de 09 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponívelem:https://www.planalto.gov.br/ccivil_03/_ato20112014/2011/lei/l12414.htm#:~:text=LEI%20N%C2%BA%2012.414%2C%20DE%209%20DE%20JUNHO%20DE%202011.&text=Convers%C3%A3o%20da%20Medida%20Provis%C3%B3ria%20n%C2%BA%20518%2C%20de%202010.&text=Disciplina%20a%20forma%C3%A7%C3%A3o%20e%20consulta,forma%C3%A7%C3%A3o%20de%20hist%C3%B3rico%20de%20cr%C3%A9dito.. Acesso em 29 de nov. 2024.

.

A Lei nº 12.527/2011, que regula o acesso a informações previsto no Inciso XXXIII do Artigo 5º, no Inciso II do § 3º do Artigo 37 e no § 2º do Artigo 216 da Constituição Federal, dispõe que os procedimentos previstos se destinam a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração. O que mais chamou atenção nessa Lei foi o fato de ter sido publicada em 2011, ano em que era impensável a ideia de termos no Brasil uma Lei Geral de Proteção de Dados. Apesar disso, a referida legislação fez uma inovação no ordenamento jurídico, dispondo sobre informação, dados processados, informação sigilosa e informação pessoal[447].

A Lei número 12.654/2012, que prevê a coleta de perfil genético como forma de identificação, menciona que os dados relacionados à coleta do perfil genético deverão ser armazenados em bancos de dados de perfis genéticos gerenciados por uma unidade oficial de perícia criminal. A lei também preceitua que os dados constantes nos bancos de dados de perfis genéticos terão caráter sigiloso, respondendo civil, penal e administrativamente aquele que permitir ou promover a sua utilização para fins diversos do previsto em lei ou decisão judicial. O que mais chamou atenção na referida legislação, foi o fato da previsão de exclusão dos perfis genéticos dos bancos de dados, no término do prazo estabelecido em Lei para a prescrição do delito[448].

---

[447]BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Artigo 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes: I - observância da publicidade como preceito geral e do sigilo como exceção; II - divulgação de informações de interesse público, independentemente de solicitações; III - utilização de meios de comunicação viabilizados pela tecnologia da informação; IV - fomento ao desenvolvimento da cultura de transparência na administração pública; V - desenvolvimento do controle social da administração pública. Art. 4º Para os efeitos desta Lei, considera-se: I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato; II - documento: unidade de registro de informações, qualquer que seja o suporte ou formato; III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado; IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável; V - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação; VI - disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados; VII - autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema; VIII - integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino; IX - primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 29 de nov. 2024.

[448]BRASIL. Lei nº 12.654. de 28 de maio de 2012. Altera as Leis nºs 12.037, de 1º de outubro de 2009, e 7.210, de 11 de julho de 1984 - Lei de Execução Penal, para prever a coleta de perfil genético como forma de identificação criminal, e dá outras providências. Artigo 1º O art. 5º da Lei nº 12.037, de 1º de outubro de 2009, passa a vigorar acrescido do seguinte parágrafo único: "Artigo 5º.Parágrafo único. Na hipótese do inciso IV do art. 3º , a

Conforme foi possível aferir, antes da entrada em vigor da Lei Geral de Proteção de Dados, várias leis fizeram previsão do direito à privacidade, da proteção e do compartilhamento de dados pessoais. Apesar disso, nenhuma das normas protegeu, de fato, os dados pessoais dos cidadãos brasileiros, o que só ocorreu com a Emenda que elevou o tratamento de dados pessoais ao status de Direito Fundamental e com a LGPD.

André Rocha Ferreira defende que há um enorme déficit de proteção dos cidadãos, visto que não há regulação geral sobre a licitude, a transparência ou a segurança do tratamento de dados em matéria penal, tampouco direitos estabelecidos ou requisitos para a utilização de novas tecnologias que possibilitam um grau de vigilância e monitoramento impensável há alguns anos. Apesar do crescimento vertiginoso de novas técnicas de vigilância e de investigação, a ausência de regulamentação sobre o tema gera uma assimetria de poder muito grande entre o Estado e o cidadão. O titular dos dados é deixado sem garantias normativa mínimas e mecanismos institucionais inaplicáveis para resguardar seus direitos de personalidade, suas liberdades individuais e até a observância do devido processo legal[449].

Isso demonstra que a Lei Geral de Proteção de Dados aponta diretrizes para futuras legislações a atos administrativos que abordem o tratamento de dados pessoais para fins

identificação criminal poderá incluir a coleta de material biológico para a obtenção do perfil genético." (NR). Artigo 2º A Lei nº 12.037, de 1º de outubro de 2009, passa a vigorar acrescida dos seguintes artigos: "Artigo 5º-A. Os dados relacionados à coleta do perfil genético deverão ser armazenados em banco de dados de perfis genéticos, gerenciado por unidade oficial de perícia criminal. § 1º As informações genéticas contidas nos bancos de dados de perfis genéticos não poderão revelar traços somáticos ou comportamentais das pessoas, exceto determinação genética de gênero, consoante as normas constitucionais e internacionais sobre direitos humanos, genoma humano e dados genéticos. § 2º Os dados constantes dos bancos de dados de perfis genéticos terão caráter sigiloso, respondendo civil, penal e administrativamente aquele que permitir ou promover sua utilização para fins diversos dos previstos nesta Lei ou em decisão judicial. § 3º As informações obtidas a partir da coincidência de perfis genéticos deverão ser consignadas em laudo pericial firmado por perito oficial devidamente habilitado." "Artigo 7º-A. A exclusão dos perfis genéticos dos bancos de dados ocorrerá no término do prazo estabelecido em lei para a prescrição do delito." "Artigo 7º-B. A identificação do perfil genético será armazenada em banco de dados sigiloso, conforme regulamento a ser expedido pelo Poder Executivo." Art. 3º A Lei nº 7.210, de 11 de julho de 1984 - Lei de Execução Penal, passa a vigorar acrescida do seguinte art. 9º-A: "Artigo 9º-A. Os condenados por crime praticado, dolosamente, com violência de natureza grave contra pessoa, ou por qualquer dos crimes previstos no art. 1º da Lei nº 8.072, de 25 de julho de 1990, serão submetidos, obrigatoriamente, à identificação do perfil genético, mediante extração de DNA - ácido desoxirribonucleico, por técnica adequada e indolor. § 1º A identificação do perfil genético será armazenada em banco de dados sigiloso, conforme regulamento a ser expedido pelo Poder Executivo. § 2º A autoridade policial, federal ou estadual, poderá requerer ao juiz competente, no caso de inquérito instaurado, o acesso ao banco de dados de identificação de perfil genético." Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12654.htm. Acesso em 29 de nov. 2024.

[449]FERREIRA, André da Rocha. Tratamento de Dados Pessoais em investigações criminais: O Direito Fundamental à Autodeterminação Informativa como Limite Constitucional. Revista Brasileira de Ciências Criminais. Vol.185. ano 29. p. 115-159. São Paulo: Ed. RT, novembro de 2021.

penais[450]. As notas técnicas da Autoridade Nacional de Proteção de Dados e da Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro também devem ser observadas. A aplicação da Lei Geral de Proteção de Dados para o tratamento de dados penais deve ser levada em consideração pela abordagem da autodeterminação informativa no tratamento de dados pessoais, o que pode ser comprovado com a aferição da igualdade dos princípios previstos na LGPD e no Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Persecução Penal[451].

Depreende-se, contudo, que da mesma forma que os princípios da Lei Geral de Proteção de Dados são aplicados ao tratamento de dados autorizados pela própria LGPD, os princípios

---

[450] *Ibid.*

[451] Lei Geral de Proteção de Dados: Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. Anteprojeto de Proteção de Dados para Segurança Pública e Persecução Penal: Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I – licitude: embasamento do tratamento de dados pessoais em hipótese legal, nos termos do Capítulo II desta Lei; II - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; III - adequação: pertinência e relevância do tratamento com os objetivos pretendidos, de acordo com o contexto do tratamento; IV - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; V – proporcionalidade: compatibilidade do tratamento com os objetivos pretendidos, de acordo com o contexto do tratamento; VI - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; VII - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VIII - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; IX - segurança da informação: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; X - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; XI - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; XII - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

constitucionais da dignidade da pessoa humana, da proporcionalidade, da autodeterminação informativa e dos direitos da intimidade e da vida privada devem ser aplicados no tratamento de na custódia dos dados penais. Desta forma, as legislações anteriores e posteriores à Lei Geral de Proteção de Dados que vinculem a captação, o tratamento e o compartilhamento de dados pelo Estado ao gestor de dados, sem levar em consideração os princípios da proporcionalidade e da autodeterminação informativa, devem ser interpretados na conformidade constitucional, sob pena de servirem como dados de Troia para a democracia[452]. Conforme foi possível aferir acima, o ordenamento jurídico brasileiro não dispõe de instrumentos para garantir o tratamento de dados penais para fins penais, deixando os bancos de dados das polícias judiciárias brasileiras em uma evidente situação de lacuna normativa.

6.3 Reflexos da Proteção de Dados no Contexto dos Direitos Fundamentais

A Constituição da República Federativa do Brasil assegura o direito fundamental à proteção de dados pessoais, conforme consta no artigo 5º, inciso XII. Esse dispositivo legal assegura a inviolabilidade do sigilo de dados e de comunicações telefônicas, bem como o sigilo de correspondências e comunicações telegráficas. A própria Constituição Federal, porém, permite que esse direito fundamental possa ser flexibilizado, diante da finalidade de investigação ou instrução criminal ou instrução processual penal.

> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Antes da Emenda Constitucional que inseriu a proteção de dados pessoais como direito fundamental, alguns doutrinadores entendiam que os dados mencionados no inciso XII do Artigo 5º da nossa Constituição Federal não eram os dados pessoais previstos na Lei Geral de Proteção de Dados e no Anteprojeto Penal de Proteção de Dados. Conforme será possível aferir adiante, a discussão tornou-se irrelevante após o julgamento da ADI 6387, porque a proteção de dados pessoais estava prevista no inciso X do mesmo Artigo, que protege o direito à intimidade e à privacidade.

---

[452]TOSCHI, Aline Seabra; LOPES Herbert Emílio Araújo. Dados de Troia. In: Associação Nacional dos Procuradores da República; Ministério Público Federal; ARAS, Vladimir Barros; MENDONÇA, Andrey Borges de; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA, Marcos Antônio da Silva (Orgs). Proteção de dados pessoais e investigação criminal. Brasília: ANPR, 2020.

Embora a proteção de dados pessoais só tenha sido efetivamente reconhecida como direito fundamental após a Emenda Constitucional número 115 de 2002[453], a garantia sempre esteve prevista, de forma implícita, em nossa Constituição Federal. Isso pode ser comprovado através das mais diversas questões sobre direito da personalidade, analisadas pelo Supremo Tribunal Federal (STF) nos últimos anos. Apesar do STF já ter julgado diversas demandas envolvendo colisão de direitos fundamentais, cada caso é um caso, o que faz com que o tema em questão necessite de um estudo contínuo, sempre à espera de um novo fato que necessite de uma decisão fundamentada na razoabilidade.

Na prática, podemos citar como exemplos as medidas cautelares concedidas nas ADIs 6387, 6388, 6389, 6390, 6390 e 6393, onde o Supremo Tribunal Federal manifestou-se, pela primeira vez, sobre a definição do direito à privacidade e à proteção de dados diante do avanço da tecnologia. O caso em questão foi relatado pela ministra Rosa Weber, que utilizou a Constituição Federal para dirimir a questão, sem deixar de violar os referidos direitos fundamentais.

No dia 17 de abril de 2020 entrou em vigor a Medida Provisória número 954[454], que, durante a pandemia decorrente do coronavírus, determinou, em caráter de urgência, que empresas de telecomunicação, prestadoras de serviço de telefonia, deveriam compartilhar com a Fundação Instituto Brasileiro de Geografia e Estatística – IBGE, através de meios eletrônicos, a relação dos nomes, números de telefones, e endereço dos consumidores, pessoas físicas ou jurídicas, com o objetivo de produzir um relatório de estatística não presencial, o que seria feito por intermédio de entrevistas.

Tendo em vista a iminência do risco de compartilhamento compulsório de dados pessoais de milhões de usuários de serviço de telefonia no Brasil, no dia 20 de abril de 2024, o Conselho Federal da Ordem dos Advogados do Brasil – OAB, propôs Ações Direta de Inconstitucionalidade (ADI 6387)[455], o que também foi feito pelo Partido da Social Democracia

[453]BRASIL. Emenda Constitucional número 115 de 2022 - Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: < https://legis.senado.leg.br/norma/35485358. >. Acesso em 04 jan. 2024.
[454]BRASIL. Medida Provisória 954/2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 21 de abr. 2024.
[455]STF, ADI 6.387, Tribunal Pleno, Rel. Min. Rosa Weber, J. 07.05.2020, DJe 12.11.2020.

Brasileira – PSDB, (ADI 6388), pelo Partido Socialista Brasileiro – PSB (ADI 6389), pelo partido socialismo e liberdade – PSOL (ADI 6390) e pelo Partido Comunista do Brasil – PCdoB (ADI 6393). Todas as ações de inconstitucionalidade em questão, foram apensadas à ADI 6387, que foi a primeira a ser protocolada no STF.

Foi argumentado na petição inicial, pelo Conselho Federal da Ordem dos Advogados do Brasil, que, na era da informática, alguns dados pessoais, como nome, número de telefone e endereço de todos os usuários de telefonia do Brasil, não poderiam ser considerados irrelevantes, porque eventual vazamento de tais dados, colocaria em risco a liberdade democrática por meio da manifestação de vontade do eleitorado.

Além dos motivos já mencionados acima, o compartilhamento de dados pessoais sem o consentimento do seu titular no caso em tela, não apresentou necessidade da pesquisa para o compartilhamento de dados pessoais e não apresentou o mecanismo de segurança para minimizar o risco de acesso ou o uso indevido de dados. Outro aspecto que deve ser destacado é que o Conselho Federal da Ordem dos Advogados do Brasil também sustentou que a referida Medida Provisória padecia de inconstitucionalidade formal, por ausência de preenchimento dos pressupostos constitucionais de urgência e relevância; e inconstitucionalidade material, por violação direta aos artigos 1º inciso III e 5º incisos X e XII da Constituição Federal, que asseguram, respectivamente, a dignidade da pessoa humana, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas; o sigilo dos dados e o direito à autodeterminação informativa, sob a alegação de violação ao princípio da proporcionalidade.

Ficou claro que a referida Medida Provisória violaria do sigilo dos dados de uma grande parte da população brasileira, restringindo a privacidade e a intimidade de todos. Outro ponto levantado pelo Conselho Federal da OAB foi o fato de no IBGE só trabalharem servidores comissionados, por um determinado período, o que tornaria ainda mais frágil a segurança dos dados pessoais, dando a entender que a depender do momento político vivido no Brasil, esses dados poderiam ser utilizados, inclusive, para tentar alterar o rumo das eleições. Conforme consta na petição inicial dessa ADI, “esses cargos de nomeação política trazem em si um compromisso político entre o nomeado e o nomeante”[456].

[456] *Ibid.*

Os postulantes das Ações Diretas de Inconstitucionalidade esperavam que o Supremo Tribunal Federal tivesse o mesmo entendimento da decisão proferida nos autos do RE 1055941, onde discutiu-se o compartilhamento de dados pelo COAF/UIF diretamente ao Ministério Público. Na ocasião, foi fixado, em repercussão geral, o seguinte entendimento:

> É constitucional o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil, que define o lançamento do tributo, com os órgãos de persecução penal, para fins criminais, sem a obrigatoriedade de prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional.
> O compartilhamento pela UIF e pela Receita Federal do Brasil, referente ao item anterior, deve ser feito unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios"[457].

O entendimento anterior do STF, acerca do compartilhamento de dados sigilosos pelo COAF, para fins criminais, diante da presença de indícios de ilícitos e com as cercaduras formais e controle judicial aptos a garantir a prevalência do sigilo perante terceiros, serviu de precedente que pode foi aplicado para o reconhecimento da inconstitucionalidade do compartilhamento previsto na Medida Provisória que estava sendo analisada, principalmente pelo fato da ausência de todos os pressupostos reconhecidos como necessários pelo STF para ensejar a relativização do direito fundamental a proteção de dados pessoais.

Importante fazer as observações, porque embora a Emenda número 115 de 2022, que incluiu LXXIX no Artigo 5º da Constituição Federal, reconhecendo o Direito Fundamental à proteção de dados pessoais, só tenha sido publicada e entrado em vigor em fevereiro de 2022, foi o julgamento da ADI 6387 que firmou o entendimento jurisprudencial necessário para declarar que o compartilhamento compulsório de dados pessoais determinado pela Medida Provisória número 954 violava o Direito Fundamental à proteção de dados pessoais e à autodeterminação informativa, reconhecidos a partir de uma interpretação dos Incisos XI e X do Artigo 5º da Constituição Federal e do Artigo 2º inciso II da Lei Geral de Proteção de Dados.

A relatora da ADI 6387, Ministra Rosa Weber, deferiu, no dia 24 de abril de 2020, a medida cautelar para suspender a Medida Provisória número 954/2020[458], determinando que o IBGE não poderia solicitar às operadoras de telefonia a disponibilização de dados pessoais dos

[457] *Ibid.*
[458] STF, ADI 6.387, Tribunal Pleno, Rel. Min. Rosa Weber, J. 07.05.2020, DJe 12.11.2020.

consumidores ou que suspendesse a solicitação caso ela já tivesse sido efetuada. A Ministra Rosa Weber iniciou a justificativa do seu voto sustentando que o tratamento de dados pessoais em meio digital, por agentes públicos ou privados, seria um dos maiores desafios contemporâneos do direito fundamental à privacidade, assegurado no artigo 5º inciso X da nossa Constituição Federal.

Mencionou, ainda, que o Artigo 2º da Medida Provisória número 954 impôs às empresas prestadoras do Serviço Telefônico Fixo Comutado – STFC e do Serviço Móvel Pessoal – SMP, o compartilhamento, com o IBGE, de informações relacionadas à identificação – efetiva ou potencial – de pessoa natural, o que configuram dados pessoais. Eventual manipulação dessas informações poderia lesionar cláusulas constitucionais assecuratórias da liberdade individual (Artigo 5º, Caput, da CRFB), da privacidade e do livre desenvolvimento da personalidade (Artigo 5º, Incisos X e XII da CRFB). Além disso, como decorrência dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa[459], foram positivados no Artigo 2º, incisos I e II da Lei número 13.709/2018 (Lei Geral de Proteção de Dados).

Na mesma decisão, a Ministra Rosa Weber também fez menção ao artigo *The Right do Privacy*, já abordado neste estudo, escrito por Samuel Warren e Louis Brandeis, onde reforçou que as mudanças políticas, sociais e econômicas, demandam incessantemente o reconhecimento de novos direitos, razão pela qual, de tempos em tempos, é necessário redefinir a exata natureza e extensão da proteção à privacidade do indivíduo.

A MP número 954 não apresentou mecanismos técnicos ou administrativos aptos a protegerem os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão ou no tratamento. A adequada tutela do direito à intimidade, privacidade e proteção de dados pessoais é estruturada pela característica da inviolabilidade. Com o objetivo de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel, com o caráter precário próprio aos juízos perfunctórios e sem prejuízo de exame mais aprofundado quando do julgamento do mérito, foi deferida a medida cautelar requerida, *ad referendum* do Plenário desta Suprema Corte, para suspender a eficácia da Medida Provisória número 954/2020.

[459]BRASIL. Artigo 2º da Lei Geral de Proteção de dados. (...) Art. 2º: A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à privacidade; II – a autodeterminação informativa. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 de abr. 2024.

O que deve ser destacado é que a Procuradoria Geral da República se manifestou, entendendo que a decisão liminar não deveria ser referendada pelo Plenário do Supremo Tribunal Federal, sob a alegação de que a Medida Provisória seria necessária, adequada e proporcional para a realização da pesquisa do IBGE durante a crise epidêmica que assolava o Brasil[460]. A alegação foi a de que os dados cadastrais dos consumidores de serviço de telefonia não seriam resguardados pelo sigilo das comunicações do artigo 5º, inciso XII da Constituição Federal.

Em opinião contrária ao argumento utilizado pela Procuradoria Geral da República, a Associação *Data Privacy* Brasil[461], admitida como *animus curiae* na ação, sustentou que o feito não tratava de sigilo de dados, mas sim do direito à proteção de dados pessoais como expressão do projeto constitucional de livre desenvolvimento da personalidade humana em constante ameaça pelas modernas técnicas de tratamento de dados.

Cabe destacar que para Bruno Bioni, desde o Marco Civil da Internet (Lei número 12.965/2014), o ordenamento jurídico pátrio adotou a autodeterminação como parâmetro normativo para proteção de dados pessoais e garantia da privacidade, pois permitiu ao usuário o controle de seus dados pessoais por meio do consentimento, informação e exclusão[462].

A decisão da Ministra Rosa Weber foi referendada pela maioria do Plenário do Supremo Tribunal Federal, no dia 07 de maio de 2020, ocasião em que foi deferida medida cautelar deferida para suspender a eficácia da Medida Provisória número 954 de 2020, que ratificou o entendimento de que a Medida Provisória violava o direito constitucional à intimidade, à vida privada e ao sigilo de dados.

O Ministro Alexandre de Moraes acompanhou integralmente o voto da relatora e ressaltou que os direitos fundamentais só podem ser relativizados se houver observância ao

[460]Procuradoria Geral da República. Manifestação da PGR (27551/2020). In: Ação Direta de Inconstitucionalidade n. 6387. Disponível em http://redir.stf.jus.br/. Acesso em 30 de abr. 2024.
[461]BIONI, Bruno; RIRELLI, Mariana; ZANATTA, Rafael. 110 -Petição de apresentação de manifestação (28539/2020). In: Ação Direta de Inconstitucionalidade n. 6387. Disponível em http://redir.stf.jus.br/. Acesso em 30 de abr. 2024.
[462]BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro. Forense: 2019.p. 132.

princípio da proporcionalidade. Para Luis Roberto Barroso, a ponderação sobre o compartilhamento de dados pessoais de todos os usuários de telefonia do Brasil para a realização de uma pesquisa deveria ter sido precedida de debate público acerca da necessidade, da relevância e da urgência.

O Ministro Gilmar Mendes esclareceu que o Decreto número 10.212/2020[463] incorporou ao ordenamento jurídico pátrio o regulamento da Organização Mundial da Saúde (OMS), que afastou a possibilidade de processamento de dados desnecessários e incompatíveis com o propósito de avaliação e manejo dos riscos à saúde. Os ministros Celso de Mello, Edson Fachin, Luiz Fux, Ricardo Lewandowski, Carmén Lúcia e Dias Toffoli também seguiram o voto da relatora. O ministro Marco Aurélio entendeu ser necessária análise prévia da Medida Provisória pelo Congresso Nacional. O Plenário do Supremo Tribunal Federal, portanto, suspendeu a eficácia da Medida Provisória número 954 de 2020, abrindo precedente jurisprudencial sobre o direito fundamental à proteção de dados pessoais.

Para Ingo Sarlet[464], os direitos fundamentais em geral, assim como o direito à proteção de dados pessoais, apresentam uma dupla dimensão subjetiva e objetiva, cumprindo uma multiplicidade de funções na ordem jurídico-constitucional. Para o Autor, na condição de direito subjetivo, e considerando como um direito em sentido amplo, o direito a proteção de dados pessoais se decodifica em um conjunto heterogêneo de posições subjetivas de natureza defensiva (negativa), mas também assume a condição de direito a prestações, cujo objeto consiste em uma atuação do Estado mediante a disponibilização de prestações de natureza fática ou normativa.

7 DESCRIÇÃO DO PROTOCOLO E ESTRATÉGIAS PARA O TRATAMENTO DE DADOS ARMAZENADOS NA POLÍCIA CIVIL DO DISTRITO FEDERAL

Diante de tudo o que foi mencionado até agora, percebe-se que as Polícias Judiciárias Brasileiras precisam se adaptar à proteção de dados pessoais, transmitindo aos seus servidores o tamanho da responsabilidade que qualquer um deve ter ao utilizar os bancos de dados para a investigação criminal. Isso deve ser feito de forma clara e didática, com ensinamento de

[463]BRASIL. Decreto número 10.212/2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10212.htm. Acesso em 30 de abr. 2024.
[464]SARLET, Ingo Wolfgang. O direito fundamental à proteção de dados pessoais como direito subjetivo. Disponível em: https://www.conjur.com.br/2021-ago-15/direitos-fundamentais-direito-protecao-dados-pessoais-direito-subjetivo/. Acesso em 25 de set. 2024.

conceitos, fundamentos e princípios de eventual Lei Geral Penal de Proteção de dados. Desta forma, todos os profissionais que trabalham na persecução penal, exercendo funções relacionadas à polícia judiciária, terão um norte para realizar o tratamento de dados de forma ética, seguindo parâmetros legais.

Só será possível alcançar o objetivo com a devida escolha dos agentes envolvidos no tratamento de dados, com o esclarecimento dos direitos dos titulares dos dados e com a fomentação da disseminação da cultura de proteção de dados na instituição policial. De acordo com Daniel Donda, o melhor método para ficar em conformidade com a Lei Geral de Proteção de dados é: criar um comitê (governança) para análise e tomadas de decisão; designar um DPO (oficial de proteção de dados); mapear e entender o ciclo de vida dos dados; adotar regulamentações e padrões de segurança da informação; auditar e monitorar o ambiente; criar um relatório de impacto à proteção de dados pessoais; criar um plano de ação para situações de emergência[465].

A estruturação do sistema de análise de proteção de dados está diretamente ligada às funções atribuídas ao DPO (*Data Protection Officer*), também conhecido como Encarregado pelo Tratamento de Dados Pessoais**.** Esse profissional, já nomeado pela Polícia Civil do Distrito Federal, é o principal responsável por manter a conformidade das organizações com a LGPD, sendo considerado o verdadeiro guardião do Sistema de Governança em Privacidade.

De acordo com a Lei Geral de Proteção de Dados, o DPO deve ser uma pessoa natural ou jurídica, que será indicada pelo controlador, para atuar como uma ponte entre o agente de tratamento, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Toda empresa, seja pública ou privada, e toda instituição policial de atividade investigativa que realize o tratamento de dados pessoais deve nomear um DPO.

O DPO recebe reclamações dos titulares de dados pessoais, presta todos os devidos esclarecimentos, toma as providências cabíveis e também recebe as demandas da Autoridade Nacional de Proteção de Dados, solucionando-as de forma imediata. Outro papel do DPO é a

[465]DONDA, Daniel. Guia Prático de Implementação da LGPD. São Paulo: Ed. Labrador, 2022. p 26.

conscientização dos servidores sobre a importância do respeito aos protocolos legais no ato do tratamento de dados[466].

O DPO deve implementar regras de boas práticas para o bom funcionamento dos Sistemas de Tratamento de Dados Pessoais, garantindo que os princípios previstos na Lei Geral de Proteção de Dados sejam respeitados. Isso deve ser feito através do mapeamento do ciclo de vida dos dados pessoais. As práticas passam pela avaliação das atividades que geram riscos para a instituição e aos titulares de dados pessoais. A avaliação deve ser feita através da definição dos protocolos de segurança que devem ser adotados para a proteção dos dados.

Feitas as referidas implementações, é necessário que ocorra um constante monitoramento da conformidade da organização com a Lei Geral de Proteção de Dados, através da elaboração de relatórios das operações de tratamento de dados pessoais e do relatório de impacto da proteção desses dados. Todas as práticas só podem ser enraizadas na cultura da instituição depois da realização de constantes treinamentos e capacitações a todos os servidores.

Levando em consideração que os conceitos previstos no Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Persecução Penal foram extraídos da Lei Geral de Proteção de Dados, é possível conceituar, de acordo com o Artigo 5º da LGPD[467], que:

---

[466]Ministério da Defesa. Encarregado pelo Tratamento de Dado Pessoais – DPO. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/hfa/acesso-a-informacao/encarregado-pelo-tratamento-de-dados-pessoaisdpo#:~:text=O%20encarregado%20pelo%20tratamento%20de,Prote%C3%A7%C3%A3o%20de%20Dados%20(ANPD).. Acesso em 07 de nov. 2024.

[467]BRASIL. Artigo 5º da Lei Geral de Proteção de Dados - LGPD. Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); IX - agentes de tratamento: o controlador e o operador; X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo; XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados; XIV - eliminação: exclusão de dado ou de

> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
> IX - agentes de tratamento: o controlador e o operador.

Embora exista uma lacuna diante da ausência de uma Lei Geral Penal de Proteção de Dados, as Instituições Policiais devem se planejar para seguir os princípios e fundamentos da LGPD, conforme foi mencionado por Heloísa Estellita[468]. O caminho de adequação à LGPD seve seguir os seguintes passos: Conhecimento das leis: É importante que as empresas entendam os requisitos do GDPR e da LGPD e como eles se aplicam aos seus negócios; Mapeamento dos dados: As empresas devem mapear todos os dados pessoais que coletam,

---

conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado; XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro; XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados; XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 12 jan. 2024.

[468]Tendo em vista a similaridade entre a nossa LGPD e o regulamento Europeu (GDPR), por que aqui no Brasil a regulação para o tratamento de Dados Pessoais voltada para a segurança pública e a persecução penal não entrou em vigor no mesmo dia da LGPD, da mesma forma como ocorreu na Europa? A resposta a essa pergunta demandaria um exame mais detalhado do regime europeu. Naquele ambiente, também há dois instrumentos diversos tratando da proteção de dados. Grosso modo e de forma muito simplificada, o tratamento de dados que também podem ter impacto penal por agentes privados está regulado no regulamento. O tratamento de dados para fins penais por autoridades ligadas à investigação, à persecução e à execução penal estão regulados em uma diretiva. A necessidade de dois diplomas legais diversos no ambiente europeu tem diversas razões, mas a principal delas, no que nos interessa, é que a União Europeia não tem competência para tratar de matéria penal em sentido amplo via regulamentos. Ela tem que tratar essa matéria por diretivas que devem ser transpostas para o sistema interno dos países. Compreender essa diferença é fundamental para entender a estrutura da regulamentação europeia. Sem prejuízo, algumas regras do tratamento geral da proteção de dados têm de ser adaptadas à esfera penal, ou seja, é conveniente que a matéria seja dividida em dois diplomas legais ou, se em um diploma só, que seja feito um capítulo dedicado à matéria penal. Um exemplo esclarece isso: o direito dos titulares de eliminação de seus dados não pode ser exercido na área penal como pode ser exercido na área extra penal. As informações que tenho sobre a LGPD e a exclusão da matéria penal refletem o temor dos que a propuseram de que, se a matéria penal fosse incorporada ao projeto de lei, haveria grande chance de projeto não aprovado. Por isso houve a exclusão, mas com a regra, que mais parece uma advertência, *no sentido de que a futura legislação deveria atender aos princípios e garantias gerais da própria LGPD.*

processam e armazenam, incluindo onde os dados estão localizados e como são usados; Obtenção de consentimento: As empresas devem obter consentimento explícito dos indivíduos para coletar seus dados pessoais e informá-los sobre como seus dados serão usados; Proteção dos dados: As empresas devem implementar medidas de segurança adequadas para proteger os dados pessoais que coletam, processam e armazenam; Nomeação de um encarregado de proteção de dados: As empresas devem nomear um encarregado de proteção de dados (DPO) para garantir que estejam em conformidade com o GDPR e a LGPD; Treinamento dos funcionários: As empresas devem treinar seus funcionários sobre as leis de privacidade de dados e como elas se aplicam aos seus negócios; Criação de um plano de resposta a incidentes: As empresas devem criar um plano de resposta a incidentes para lidar com violações de dados e notificar os indivíduos afetados, se necessário; Realização de auditorias regulares: As empresas devem realizar auditorias regulares para garantir que estejam em conformidade com o GDPR e a LGPD[469].

No boletim interno número 127, do dia 06 de julho de 2023, o Diretor Geral da PCDF instituiu, por intermédio da Portaria número 224, de 30 de junho de 2023, a Política de Privacidade no âmbito da Polícia Civil do Distrito Federal. A Política de Privacidade definiu os conceitos de agente de tratamento, autoridade nacional, banco de dados, consentimento, controlador, dado anonimizado, dado pessoal sensível, operador, titular, transferência internacional de dados e uso compartilhado de dados.

A portaria nº 224, de 30 de junho de 2023 instituiu a Política de privacidade no âmbito da Polícia Civil do Distrito Federal e trouxe as principais definições sobre os agentes envolvidos no tratamento de dados pessoais, conforme preceitua a Lei Geral de Proteção de Dados. Além da definição de agentes de tratamento, também foram abordados os conceitos de controlador, operador, anonimização, autoridade nacional, banco de dados, consentimento, dado anonimizado, dado pessoal, dado pessoal sensível, operador, órgão de pesquisa, titular, tratamento e uso compartilhado de dados[470].

---

[469]Controladoria Geral do Estado do Paraná. Manual de implementação da LGPD. Disponível em: https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/202106/manual_implementacao_lgpd.pdf. Acesso em 29 de nov. 2024.

[470]DISTRITO FEDERAL. PORTARIA Nº 224, DE 30 DE JUNHO DE 2023. Institui a Política de Privacidade no âmbito da Polícia Civil do Distrito Federal. O DELEGADO-GERAL DA POLÍCIA CIVIL DO DISTRITO FEDERAL, no uso de suas atribuições legais, conferidas pelo artigo 4°, inciso I, do Decreto Federal nº 10.573, de 14 de dezembro de 2020, e artigo 5º, inciso I, do Decreto Distrital nº 42.940, de 24 de janeiro de 2022, e considerando a Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e a Lei Federal nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), resolve: Art. 1º Instituir, na forma do ANEXO

desta Portaria, a Política de Privacidade no âmbito da Polícia Civil do Distrito Federal. Parágrafo único. Publique-se no DODF. Art. 2º Esta Portaria entra em vigor na data de sua publicação. ROBSON CÂNDIDO DA SILVA ANEXO Política de Privacidade Definições Agentes de tratamento: controlador e operador. Anonimização: Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Autoridade Nacional: Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. Banco de Dados: Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico. Consentimento: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Dado Anonimizado: Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Dado Pessoal: Informação relacionada a pessoa natural identificada ou identificável. Dado Pessoal Sensível: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Encarregado: Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Órgão de Pesquisa: Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico. Titular: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Transferência Internacional de Dados: Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro. Tratamento: Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Uso Compartilhado de Dados: Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados. Base legal para tratamento de dados pessoais. Os tratamentos de dados realizados pela PCDF utilizam como base os Arts. 7°, incisos II, III, IV, V e IX, e 11, inciso II, alíneas “a”, “b” e “c”, da LGPD e se limitam ao cumprimento de obrigações legais e regulatórias, execução de políticas públicas, execução de contratos e realização de estudos de pesquisa. 3. Encarregado Para os serviços da PCDF, o profissional responsável por atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados será designado por ato do Delegado-Geral da Polícia Civil. 4. Direitos do titular dos dados pessoais Respeitadas, ainda, as demais normas relativas à proteção da privacidade, o cidadão, na qualidade de titular de dados pessoais, mediante solicitação prévia, tem direito a obter da PCDF: confirmação da existência de dados pessoais de sua titularidade por ela tratados; acesso aos dados pessoais sob tratamento; correção de dados pessoais incompletos, inexatos ou desatualizados; e anonimização ou cessação do tratamento de dados desnecessários, excessivos ou desconformes. A proteção de dados pessoais tratados pela PCDF alcança todos aqueles que com ela se relacionem, independente do meio em que se encontram, se físico ou eletrônico, e da forma de sua obtenção, se em coleta presencial ou remota. Os direitos aqui assegurados são os relativos ao tratamento dos dados pessoais que não sejam realizados com base nos Arts. 7°, incisos II, III, IV, V e IX, e 11, inciso II, alíneas “a”, “b” e “c”, da LGPD, ou seja, para as atividades fim da PCDF a LGPD não se aplica, não havendo acionamento de direitos dos titulares de dados pessoais e/ou aplicação da LGPD neste contexto. 5. Quais dados são tratados? Quais dados pessoais são tratados pelos serviços digitais fornecidos pela PCDF? Na utilização pelo usuário dos serviços digitais fornecidos pela PCDF, são coletadas informações para garantir as funcionalidades das aplicações, tais como: Nome completo, Data de nascimento, Sexo, Número de inscrição no CPF, Endereço de e-mail, Número de telefone, Localização do usuário, Foto do usuário. Alguns recursos ou informações podem ser solicitados pelas aplicações e notificados por meio do sistema operacional do seu dispositivo móvel, quando necessários para utilização dos serviços pela primeira vez ou mesmo na instalação, por exemplo: Acesso à rede (internet móvel ou WiFi); Acesso à identificação do dispositivo; Acesso à câmera e fotos, mídia e arquivos de áudio e vídeo de seu aparelho. 6.Meios de coleta e finalidades para o tratamento A Polícia Civil do Distrito Federal – PCDF, por meio do fornecimento dos seus serviços digitais, solicita à concordância dos usuários e coleta os seguintes dados pessoais para atingimento das finalidades: Nome Completo; Data de Nascimento; CPF; E-mail. Para que fim utilizamos seus dados? A Polícia Civil do Distrito Federal – PCDF, por meio das suas aplicações digitais, coleta os seus dados pessoais para fornecimento de serviços solicitados por você. Qual o tratamento realizado com os dados pessoais? O tratamento dos dados nos ajuda a

Isso demonstra um alinhamento com o que está descrito na Lei Geral de Proteção de Dados, embora essa lei não seja aplicada aos casos que envolvam a segurança pública. A base legal da PCDF para o tratamento de dados pessoais teve como eixo os Artigos 7º, incisos II, III, IV, V e IX e 11, inciso II, alíneas "a", "b" e "c" da Lei Geral de Proteção de Dados e se limitam ao cumprimento de obrigações legais e regulatórias, execução de políticas públicas, execução de contratos e realização de estudos de pesquisas.

O que mais chama atenção na referida Portaria, é que a norma possui estreita relação com o objeto deste estudo. Os direitos dos titulares dos dados pessoais não foram deixados de lado, demonstrando que respeitadas todas as normas relativas à proteção da privacidade, o cidadão, na qualidade de titular de dados pessoais, mediante solicitação prévia, tem direito a obter da Polícia Civil do Distrito Federal a confirmação da existência de dados pessoais de sua titularidade por ela tratados, o acesso aos dados pessoais sob tratamento, a correção de dados pessoais incompletos, inexatos, ou desatualizados, bem como a anonimização ou cessação do tratamento de dados do tratamento de dados desnecessários, excessivos ou desconformes, desde que esses dados não estejam vinculados ao banco de dados utilizado para fins penais. Necessária fazer essa observação, porque os dados mencionados na Portaria são vinculados aos dados armazenados pela PCDF em suas funções administrativas, ou seja, não penais.

---

melhorar a segurança e confiabilidade dos nossos serviços. Como por exemplo: Melhorar a sua experiência; Garantir a continuidade e segurança dos nossos serviços; Prevenir, detectar, impedir e resolver fraudes. 7. Compartilhamento de dados O uso, acesso e compartilhamento da base de dados formada nos termos da presente Política de Privacidade poderão ser realizados dentro dos limites e propósitos das atividades legais da PCDF. As bases poderão ser fornecidas e disponibilizadas para acesso e/ou consulta de órgãos ou instituições da Administração Pública. Os dados coletados nas aplicações digitais podem ser utilizados para análises estatísticas e estudos, bem como para avaliar o desempenho dos serviços fornecidos. Com isso, buscamos manter e aprimorar as aplicações, com ênfase na melhoria contínua dos serviços fornecidos e prospecção de disponibilização de novos serviços que podem ser úteis para a população. 8. Transferência internacional de dados A Polícia Civil do Distrito Federal – PCDF, para cumprir obrigações regulatórias, exercer seus direitos e garantir a eficiência e qualidade de seus serviços, realiza transferência internacional de dados pessoais para entidades públicas e parceiros externos. Tal tratamento se dá verificando a segurança da informação do órgão de destino e o devido tratamento dos dados pessoais, além disso, observa-se o cumprimento das legislações vigentes. 9. Tratamento posterior para outras finalidades A Polícia Civil do Distrito Federal – PCDF poderá utilizar a coleta de dados pessoais (identificar os dados pessoais que serão tratados) a qualquer tempo para a melhoria contínua dos seus serviços e aprimoramento das experiências dos usuários. Todo e qualquer tratamento de dados pessoais posterior ao alcance de sua finalidade será comunicado ao titular de dados. A transparência será proporcionada nos termos da Lei de Acesso à Informação – Lei nº 12.527/2012, e pelos direitos concedidos na Lei Geral de Proteção de Dados Pessoais – Lei 13.709/2018. 10.Modificações e atualizações na Política de Privacidade Versão: 01 Última atualização: 20JUN2023.

Ainda de acordo com a Portaria, a proteção de dados pessoais tratados pela Polícia Civil do Distrito Federal alcança todos aqueles que com ela se relacionem, independente do meio em que se encontram, se físico ou eletrônico, e da forma de sua obtenção, se em coleta presencial ou remota. A portaria, porém, reforça que para a atividade fim da PCDF a Lei Geral de Proteção de Dados não será aplicada, ou seja, não haverá acionamento de direitos dos titulares de dados pessoais ou a aplicação da LGPD nesse contexto.

O titular de dados não pode, por exemplo, entrar em contato com a Polícia Civil do Distrito Federal para solicitar a exclusão de dados que supostamente estejam em um registro de ocorrência policial, seja ele criminal ou administrativo, como é o caso das ocorrências de extravio e de acidente de trânsito sem vítima. Quais seriam, portanto, os dados tratados pela Polícia Civil do Distrito Federal?

Na Portaria constam que os dados pessoais tratados pela PCDF são aqueles abrangidos pelos serviços digitais disponibilizados pela própria instituição. Nesse caso, são coletados os seguintes dados: nome completo, data de nascimento, sexo, CPF, e-mail, número de telefone, localização do usuário, foto do usuário, acesso à rede (internet móvel ou WiFi), acesso à identificação do dispositivo, acesso à câmera e foto, mídia e arquivos de áudio e vídeo do aparelho de telefone celular[471].

Na Polícia Civil do Distrito Federal, a coleta dos dados é necessária para o fornecimento de serviços utilizados pelo próprio usuário. Sobre o tratamento de dados, a PCDF alega que a prática ajuda a melhorar a segurança e a confiabilidade dos serviços, com o objetivo de prevenir, detectar, impedir e resolver fraudes. No que diz respeito ao compartilhamento de dados, consta na Portaria que a prática pode ser realizada dentro dos limites e propósitos das atividades legais da PCDF.

As bases poderão ser fornecidas e disponibilizadas para acesso e ou consulta de órgãos ou instituições da Administração Pública. Os dados coletados nas aplicações digitais podem ser utilizados para análises estatísticas e estudos, bem como para avaliar o desempenho dos serviços fornecidos. O entendimento é o mesmo na transferência internacional de dados. A prática deverá ser feita através da verificação de segurança da informação do órgão de destino e o

[471] *Ibid.*

devido tratamento dos dados pessoais, sem deixar de observar o cumprimento das legislações vigentes.

Por fim, a Polícia Civil do Distrito Federal, através da Portaria, realiza o tratamento de dados para outras finalidades, o que será feito a qualquer momento, para a melhoria contínua dos seus serviços e aprimoramento das experiências dos usuários. Todo e qualquer tratamento dos dados posterior ao alcance de sua finalidade será comunicado ao titular de dados. A transparência no âmbito da Polícia Civil do Distrito Federal será proporcionada nos termos da Lei de Acesso à informação, Lei número 12.527/2012, e pelos direitos concedidos na Lei Geral de Proteção de Dados, Lei número 13.709/2023.

Sobre as estratégias para o tratamento e a utilização dos dados armazenados pelas Polícias Judiciárias Brasileiras, cabem algumas observações. A primeira delas é que embora a Polícia Civil do Distrito Federal seja uma referência para as demais Polícias Judiciárias Brasileiras, o que foi mencionado acima ocorre no Distrito Federal. O ideal é que o tema seja debatido em todas as outras instituições policiais, mas o presente estudo não tem o objetivo de fazer a análise de âmbito nacional.

A segunda observação diz respeito a uma curiosidade que ocorreu na União Europeia e em países que já debatem a proteção de dados há alguns anos. Enquanto ao redor do mundo primeiro ocorreu a preocupação com a proteção de dados, para depois implementarem as Leis de Acesso à Informação, o Brasil fez o oposto. Aqui, primeiro houve a liberação do acesso aos dados pessoais e demais informações, para depois restringirem o acesso às informações, o que se deu através da através da Lei Geral de Proteção de Dados. Ou seja, países que se tornaram referência na proteção de dados protegeram os dados pessoais dos cidadãos, para depois liberarem o acesso através de lei específica. No Brasil, primeiro liberaram o acesso à informação, para depois protegerem os dados. É óbvio, por uma série de fatores, que a primeira opção foi a mais acertada.

Percebe-se que que na Portaria da Polícia Civil do Distrito Federal não constam quais são as consequências para o servidor que utilizar os dados armazenados durante uma investigação. A omissão é justificável porque a questão do tratamento de dados na persecução penal ainda não foi regulamentada por legislação específica. Mesmo com a aprovação de

eventual legislação, os Ministérios Públicos deverão fazer a fiscalização, tendo em vista que já atuam no controle externo da atividade policial.

O controle externo da atividade policial pelo Ministério Público tem como principal objetivo a manutenção da regularidade dos serviços das polícias, adequando procedimentos que são utilizados pelas polícias. A fiscalização é de extrema importância, porque pode auxiliar na manutenção do respeito aos direitos fundamentais, na preservação dos direitos humanos, no cumprimento das leis e dos tratados e convenções internacionais, garantindo, dessa forma, a manutenção da ordem pública.

Segundo o Conselho Nacional do Ministério Público, as funções de controle externo da atividade policial serão exercidas por intermédio das seguintes modalidades: em sede de controle difuso, por todos os membros do Ministério Público com atribuição nas áreas criminal ou cível, quando do exame de procedimentos investigatórios de qualquer natureza, bem como processos judiciais que lhe forem atribuídos; e em sede de controle concentrado, por órgãos especializados, que deverão dispor de condições materiais, técnicas e operacionais necessários e compatíveis para o exercício dessas atribuições[472].

Qualquer estratégia para o tratamento e a utilização dos dados armazenados pelas Polícias Judiciárias brasileiras, deve passar pelo Ministério Público, através do controle externo da atividade policial, que deverá acompanhar toda a cadeia do tratamento de dados. Conforme já mencionado, a ausência de uma legislação de proteção de dados para a segurança pública e persecução penal não inviabiliza a implementação de estratégias para o tratamento de dados pelas policiais judiciárias.

Embora seja comum a utilização dos dados para a investigação de diversos tipos de crimes, algumas instituições policiais já fazem o monitoramento da utilização dos dados pessoais, como é o caso da Polícia Civil do Distrito Federal. Isso pode ser feito através do desenvolvimento de softwares que acompanhem a utilização de determinado tipo de dado, com

[472]Conselho Nacional do Ministério Público. Disponível em: <https://www.cnmp.mp.br/portal/todas-as-noticias/17146-cnmp-aprova-nova-regulamentacao-das-atribuicoes-do-ministerio-publico-no-controle-externo-daatividadepolicial#:~:text=O%20Plen%C3%A1rio%20do%20Conselho%20Nacional,18%C2%AA%20Sess%C3%A3o%20Ordin%C3%A1ria%20de%202023. >.Acesso em 06 jan. 2024.

o devido respaldo que justifique o acesso ao referido dado. A identificação do servidor que acessou esse tipo de informação também deve ser registrada.

Outra estratégia que pode ser adotada é a autorregulação. De acordo com Thiago Sombra, a autorregulação é um modelo no qual as empresas ou um conjunto de empresas elaboram regras próprias para disciplinar suas atividades por meio de códigos de conduta, selos políticas, padrões tecnológicos e arranjos contratuais, dotados de flexibilidade e capazes de facilmente se adaptarem à evolução tecnológica. É comum que esses instrumentos sejam utilizados como forma de se antecipar à regulação ou até mesmo evitá-la[473].

Para Sombra, o êxito dos instrumentos de autorregulação é imprevisível e bastante variável, a depender do setor, país e condições de implementação. Frisa que, via de regra, dependem de um conjunto de fatores políticos, organizacionais, culturais, tecnológicos e econômicos, cujo principal objetivo deva ser a implantação de um arcabouço regulatório com capacidade de impor sanções e assegurar o efetivo equilíbrio entre tutela de dados pessoais e fomento à inovação[474].

Apenas a título de exemplo, o Banco Nacional de Desenvolvimento Econômico e Social – BNDES, disponibilizou em seu site uma área específica, onde foi ofertada uma área exclusiva para esclarecimentos sobre a Lei Geral de Proteção de Dados[475]. Além disso, o BNDES se preocupou em informar ao cidadão o conceito de proteção de dados e o motivo pelo qualba LGPD é importante, o que demonstra um elevado grau de comprometimento com a privacidade daqueles que tenham qualquer tipo de relação com o banco.

O modelo do BNDES pode servir de parâmetro porque além de transparente, estabelece a diferença entre dados pessoais e dados pessoais sensíveis, demonstrando quais dados são coletados e com que utilidade são coletados. Durante tudo o que foi mencionado até agora, é possível depreender que diante da inexistência da Lei Geral Penal de Proteção de Dados, as

[473]SOMBRA, Thiago Luís Santos. Fundamentos da Regulação da Privacidade e Proteção de Dados Pessoais: Pluralismo Jurídico Transparência e Perspectiva. São Paulo: Thomson Reuters, 2019. p. 94.
[474]*Ibid.*
[475]BNDES. Lei Geral de Proteção de Dados – LGPD. Disponível em: https://www.bndes.gov.br/wps/portal/site/home/transparencia/lgpd. Acessado em 29 de mai. 2024.

empresas privadas não podem negar algumas informações para as polícias, mas estas, por sua vez, não podem desrespeitar os princípios norteadores da LGPD.

Nesse sentido, o BNDES trata, coleta, processa, armazena e usa dados pessoais de diversas classes de titulares que constituem seu público de relacionamento interno ou externo. Como exemplo, o próprio banco cita algumas das seguintes finalidades para o tratamento dos dados pessoais:

> Administradores, representantes legais e demais colaboradores de clientes, agentes financeiros, outros parceiros de negócios e fornecedores: para o cumprimento de obrigações impostas pela legislação de prevenção à lavagem de dinheiro e financiamento ao terrorismo; atendimento da legislação civil na formalização de contratos; atendimento de outras legislações a que o BNDES está sujeito como empresa pública federal e como instituição financeira; proteção de crédito etc.;
> Potenciais clientes ou pessoas que visitam nossos portais na Internet: para garantir o acesso; prevenir fraudes; ofertar os produtos mais adequados ao perfil do usuário; atender a legislação aplicável a instituições financeiras públicas; analisar o desempenho e a utilização dos sites; viabilizar o recebimento de comunicações digitais; garantir a inscrição em eventos organizados pelo BNDES; aprimorar os serviços prestados; dentre outros;
> Empregados e membros da Alta Administração: para o cumprimento de obrigações trabalhistas; controle de suas atividades laborais; verificação do atendimento a requisitos previstos na legislação para sua nomeação; atendimento de obrigações legais de natureza administrativa etc;
> Colaboradores terceirizados e estagiários: para o cumprimento de obrigações legais; o controle de segurança; o controle de suas atividades laborais etc;
> Outros terceiros com quem o BNDES tenha litígios judiciais ou administrativos, para o exercício de sua defesa;
> Pessoas que comparecem a eventos realizados pelo BNDES ou em suas dependências.

Percebe-se o compromisso da instituição com a proteção de dados pessoais, que além das práticas mencionadas acima, também permite ao titular de dados pessoais verificar a confirmação da existência de um ou mais dados pessoais sendo tratados; o acesso aos dados pessoais conservados que lhe digam respeito; correção dos dados pessoais incompletos, inexatos ou desatualizados; eliminação de dados pessoais desnecessários, excessivos ou caso o seu tratamento seja ilícito; portabilidade de dados a outro fornecedor de serviço ou produto; eliminação de dados (exceto quando o tratamento é legal, mesmo que sem o consentimento do titular); informação sobre compartilhamento dos seus dados com entes públicos e privados, caso isso exista; informação sobre o não consentimento, ou seja, sobre a opção de não autorizar

o tratamento e as consequências da negativa; revogação do consentimento, nos termos da lei; reclamação contra o controlador dos dados junto à autoridade nacional e oposição, caso discorde de um tratamento feito sem o seu consentimento e o considere irregular[476].

Um dos aspectos mais interessantes do modelo de aplicação da proteção de dados no BNDES foi a apresentação, na própria página do site mencionado acima, de um relatório de *Feedback* feito especificamente pelo o banco, para o Tribunal de Contas da União – TCU[477], ocasião em que foi realizada uma auditoria para elaborar diagnósticos acerca dos controles implementados por organizações públicas federais para adequação à Lei Geral de Proteção de Dados.

O método utilizado para avaliar as organizações foi o de autoavaliação de controles (*Control Self-Assessment – CSA*), onde disponibilizaram um questionário eletrônico para que os gestores preenchessem as respostas que melhor retratem a situação das respectivas organizações em relação aos controles relacionados à LGPD. Isso permitiu que as instituições verificassem quais controles associados à LGPD foram implementados, ou caso não tenha ocorrido, as questões devem ser utilizadas como referência de futuras iniciativas de adequação.

No questionário constaram 60 questões organizadas em duas perspectivas e nove dimensões. Com o intuito de consolidar os dados obtidos para possibilitar a comparação das organizações auditadas para aferir o nível de adequação à Lei Geral de Proteção de Dados, um subconjunto de 42 questões foi escolhido para compor um indicador elaborado com o intuito de resumir as respostas fornecidas por cada organização. De acordo com o que consta no próprio relatório, o cálculo do indicador considerou as possíveis respostas de cada questão selecionada, atribuindo uma nota numérica a cada uma delas.

Desta forma, respostas “sim”, “parcialmente” e “não”, correspondem, respectivamente, às notas 1, 0,5 e 0. O valor do indicador é atingido pela soma das notas obtidas em cada uma das questões divididas por 42. Desta forma, para cada organização o valor indicador pode variar de 0 (nota 0 em todas as questões), para 1 (nota 1 em todas as questões). A partir dos valores do indicador, foram definidos quatro níveis de adequação à Lei Geral de Proteção de Dados.

---

[476] *Ibid.*

[477] BNDES. Relatório BNDES – Tribunal de Contas da União. Disponível em: https://www.bndes.gov.br/wps/wcm/connect/site/3c4a346e-2406-423a-baf9-b19cc8b39683/Relat%C3%B3rio+de+Feedback+BNDES.pdf?MOD=AJPERES&CVID=og-e9dt. Acessado em 29 de mai. 2024.

São eles: inexpressivo (indicador menor ou igual a 0,15), inicial (indicador maior que 0,15 e menor ou igual a 0,5), intermediário (indicador maior do que 0,5 e menor ou igual a 0,8) e aprimorado (indicador maior que 0,8). Conforme o valor indicado obtido, portanto, as organizações foram classificadas em um dos níveis de maturidade. O BNDES auferiu a nota 0,54, atingindo o nível "intermediário".

Conforme consta no relatório do TCU, o indicador pode ser desmembrado e também apresentado levando em consideração os valores referentes a cada uma das seguintes dimensões do questionário: preparação, contexto organizacional, liderança, capacitação, conformidade no tratamento, direitos do titular, compartilhamento de dados pessoais, violação de dados pessoais e medidas de proteção[478].

Sobre a "preparação", consta no relatório que antes de iniciar o processo de adequação à Lei Geral de Proteção de Dados, a organização deve adotar as medidas para construir um ambiente propício ao sucesso da iniciativa. As questões da dimensão abordam aspectos relacionados à identificação e ao planejamento das medidas necessárias à adequação. Nessa dimensão, foram feiras as seguintes indagações: A organização conduziu iniciativa para

[478]BNDES. Relatório BNDES – Tribunal de Contas da União. Avaliação da adequação à LGPD O método utilizado para avaliar as organizações foi o de autoavaliação de controles (do inglês Control Self-Assessment – CSA), por meio do qual foi disponibilizado um questionário eletrônico para que os gestores preenchessem as respostas que melhor refletiam a situação das respectivas organizações com relação aos controles relacionados à LGPD. Além de permitir que as organizações verificassem quais controles associados à LGPD foram implementados, as questões também devem ser utilizadas como referência para a condução de futuras iniciativas de adequação. O questionário contemplou 60 questões organizadas em duas perspectivas e nove dimensões (Figura 1). As questões tiveram como referência a própria LGPD e a norma técnica ABNT NBR ISO/IEC 27701:2019 (extensão das normas de segurança da informação ABNT NBR ISO/IEC 27.001 e ABNT NBR ISO/IEC 27.002 para gestão da privacidade da informação). no que tange ao nível de adequação à LGPD, um subconjunto de 42 questões foi escolhido para compor um indicador elaborado com o intuito de resumir as respostas fornecidas por cada organização. O cálculo do indicador considerou as possíveis respostas de cada questão selecionada, atribuindo uma nota numérica a cada uma delas. Assim, as respostas dos tipos "Sim", "Parcialmente" e "Não" correspondem, respectivamente, às notas 1, 0,5 e 0; sendo que o valor do indicador é obtido pela soma das notas obtidas em cada uma das questões dividida por 42. Assim, para cada organização, o valor do indicador pode variar de 0 (nota 0 em todas as questões) a 1 (nota 1 em todas as questões)1 . A partir dos valores do indicador, foram definidos quatro níveis de adequação à LGPD: "Inexpressivo" (indicador menor ou igual a 0,15), "Inicial" (indicador maior do que 0,15 e menor ou igual a 0,5), "Intermediário" (indicador maior do que 0,5 e menor ou igual a 0,8) e "Aprimorado" (indicador maior do que 0,8). Assim, conforme o valor do indicador obtido, as organizações foram classificadas em um desses níveis de maturidade. A organização BNDES obteve o valor 0,54 para o indicador de adequação, o que corresponde ao nível "Intermediário". O indicador pode ser desmembrado e também apresentado levando em consideração os valores referentes a cada uma das dimensões do questionário: "Preparação", "Contexto Organizacional", "Liderança", "Capacitação", "Conformidade do Tratamento", "Direitos do Titular", "Compartilhamento de Dados Pessoais", "Violação de Dados Pessoais" e "Medidas de Proteção". Na Tabela 1 é apresentado um resumo da avaliação da organização contendo os valores de cada dimensão do questionário e do indicador de adequação à LGPD, possibilitando comparar os valores da própria organização e os valores médios do conjunto das 382 organizações avaliadas. Disponível em:https://www.bndes.gov.br/wps/wcm/connect/site/3c4a346e2406423abaf9b19cc8b39683/Relat%C3%B3rio+de+Feedback+BNDES.pdf?MOD=AJPERES&CVID=og-e9dt.Acessado em 29 de mai. 2024.

identificar e planejar as medidas necessárias à adequação à LGPD? A organização elaborou plano de ação, plano de projeto ou documento similar para direcionar a iniciativa de adequação à LGPD?

Na dimensão do "contexto organizacional", foi mencionado que para alcançar os resultados pretendidos pela iniciativa de adequação à Lei Geral de Proteção de Dados, a organização deve avaliar questões internas e externas que são relevantes para atingir os objetivos. As questões da dimensão em questão abordam aspectos relacionados à identificação de normativos relacionados à proteção de dados pessoais que devem ser respeitados pela organização, à identificação das partes interessadas e à análise dos dados pessoais tratados pela organização e dos processos organizacionais que tratam os dados.

A organização que pretende implementar adequação à LGPD deve responder as seguintes indagações: A organização conduziu iniciativa para identificar outros normativos (leis, regulamentos e instruções normativas), além da LGPD, que abrangem comandos relacionados à proteção de dados pessoais e que também devem ser respeitados? A organização identificou categorias de titulares de dados pessoais com os quais se relaciona? A organização conduziu iniciativa para identificar os operadores que realizam tratamento de dados pessoais em seu nome? A organização avaliou se há tratamento de dados pessoais que envolva controlador conjunto? A organização identificou os processos de negócio que realizam tratamento de dados pessoais? A organização identificou quem são os responsáveis pelos processos de negócio que realizam tratamento de dados pessoais e que já foram identificados? A organização identificou quais são os dados pessoais tratados por ela? A organização identificou os locais onde os dados pessoais identificados são armazenados? A organização avaliou os riscos dos processos de tratamento de dados pessoais que foram identificados?

Na dimensão da "liderança", o relatório apontou que a alta direção deve demonstrar liderança e comprometimento com iniciativa de adequação à Lei Geral de Proteção de Dados. Frisou que a existência e a elaboração de políticas relacionadas à proteção de dados pessoais e a nomeação de um encarregado que tenha autonomia para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) são fundamentais para o processo de adequação[479].

[479]BNDES. Relatório BNDES – Tribunal de Contas da União. A alta direção deve demonstrar liderança e comprometimento com a iniciativa de adequação à LGPD. A existência e a elaboração de políticas relacionadas à

As indagações desta dimensão, que integram o índice de adequação à Lei Geral de Proteção de Dados, foram as seguintes: A organização possui Política de Segurança da Informação ou instrumento similar? A organização possui Política de Classificação da Informação ou instrumento similar? A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para a classificação de dados pessoais? A Política de Classificação da Informação (ou instrumento similar) abrange diretrizes para identificar dados pessoais sensíveis e relacionados a crianças e a adolescentes? A Política de Classificação da Informação (ou instrumento similar) abrande diretrizes para identificar dados pessoais de crianças e de adolescentes? A organização possui política de Proteção de Dados Pessoais (ou instrumento similar)? A organização nomeou o encarregado pelo tratamento de dados pessoais? A nomeação do encarregado foi publicada em veículo de comunicação oficial? A identidade e as informações de contato do encarregado foram divulgadas na internet?

A dimensão da "capacitação" preceitua que a organização deve conduzir iniciativas para conscientizar os colaboradores em proteção de dados pessoais. A conscientização, ainda de cordo com o relatório do TCU, é importante para que os colaboradores conheçam as políticas organizacionais relacionada à proteção de dados pessoais e para que reconheçam como suas ações são importantes para a preservação da privacidade dos titulares[480].

As ações de capacitação devem levar em consideração diferentes níveis de envolvimento dos colaboradores do tema, de modo que os responsáveis por funções essenciais relacionadas à proteção de dados pessoais recebam treinamento diferenciado, além do nível básico fornecido aos demais. Da mesma forma como ocorre nas dimensões anteriores, na

proteção de dados pessoais e a nomeação de um encarregado que tenha autonomia para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) são fundamentais para o processo de adequação. As questões desta seção são relacionadas à nomeação do encarregado e à existência de políticas que buscam assegurar a segurança das informações e a proteção dos dados pessoais. Disponível em: https://www.bndes.gov.br/wps/wcm/connect/site/3c4a346e-2406-423a-baf9-b19cc8b39683/Relat%C3%B3rio+de+Feedback+BNDES.pdf?MOD=AJPERES&CVID=og-e9dt. Acessado em 29 de mai. 2024.

[480]BNDES. Relatório BNDES – Tribunal de Contas da União. A organização deve conduzir iniciativas para conscientizar e capacitar os colaboradores em proteção de dados pessoais. A conscientização é importante para que os colaboradores conheçam as políticas organizacionais relacionadas à proteção de dados pessoais e para que reconheçam como suas ações são importantes para a preservação da privacidade dos titulares. As ações de capacitação devem considerar diferentes níveis de envolvimento dos colaboradores no tema, de forma que aqueles que ocupam funções com responsabilidades essenciais relacionadas à proteção de dados pessoais recebam treinamento diferenciado, além do nível básico fornecido aos demais. Nesta seção são abordadas questões para avaliar o planejamento e a realização de ações de conscientização e de capacitação. Disponível em: https://www.bndes.gov.br/wps/wcm/connect/site/3c4a346e-2406-423a-baf9-b19cc8b39683/Relat%C3%B3rio+de+Feedback+BNDES.pdf?MOD=AJPERES&CVID=og-e9dt. Acessado em 29 de mai. 2024.

capacitação também foram previstas as seguintes indagações: A organização possui Plano de Capacitação (ou instrumento similar) que abrange treinamento conscientização dos seus colaboradores em proteção de dados pessoais? O Plano de Capacitação (ou instrumento similar) considera que pessoas que exerçam funções com responsabilidades essenciais relacionadas à proteção de dados pessoais devem receber treinamento diferenciado? Colaboradores da organização que estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema?

Sobre a dimensão "conformidade do tratamento", a organização deve ser capaz de provar que o tratamento de dados pessoais realizados é lícito. Para que isso seja possível, será necessário demonstrar que os princípios estabelecidos pela Lei Geral de Proteção de Dados são seguidos e que os tratamentos são fundamentados em, ao menos, uma das bases legais descritas na legislação. O foco das indagações feitas aqui é se os tratamentos estão em conformidade com alguns dos princípios e se estão fundamentados e alguma base legal. Também será avaliado se a organização possui registro para documentar detalhes das atividades de tratamento. As indagações foram as seguintes: A organização identificou e documentou as finalidades das atividades de tratamento de dados pessoais? A organização avaliou se coleta apenas os dados estritamente necessários para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas? A organização avaliou se os dados pessoais são retidos (armazenados) durante o tempo estritamente necessário para cumprir com as finalidades de tratamento de dados pessoais que foram identificadas? A organização identificou e documentou as bases legais que fundamentam as atividades de tratamento de dados pessoais? Há um registro (inventário) instituído para consolidar informações relacionadas às características das atividades de tratamento de dados pessoais?[481]

Na abordagem da dimensão "direitos do titular", foi mencionado que a organização deve assegurar que os titulares tenham acesso a informações relacionadas ao tratamento de seus dados pessoais e deve estar preparada para atender todos os direitos dos titulares que são

[481]BNDES. Relatório BNDES – Tribunal de Contas da União. são lícitos. Para isso é fundamental demonstrar que os princípios estabelecidos pela LGPD são seguidos e que os tratamentos são fundamentados em, ao menos, uma das bases legais descritas na legislação. Nesta seção são abordadas questões para avaliar se os tratamentos estão em conformidade com alguns dos princípios e se estão fundamentados em alguma base legal. Também será avaliado se a organização possui um registro para documentar detalhes das atividades de tratamento. Disponível em:https://www.bndes.gov.br/wps/wcm/connect/site/3c4a346e-2406-423a-baf9-b19cc8b39683/Relat%C3%B3rio+de+Feedback+BNDES.pdf?MOD=AJPERES&CVID=og-e9dt. Acessado em 29 de mai. 2024.

elencados na Lei Geral de Proteção de Dados. Aqui, as indagações foram direcionadas para a elaboração de política de privacidade para o atendimento dos direitos dos titulares[482].

As perguntas foram divididas da seguinte forma: A organização possui Política de Privacidade (ou instrumento similar)? A Política de Privacidade (ou instrumento similar) está publicada na internet? Foram implementados mecanismos para atender os direitos dos titulares elencados no art. 18 da LGPD e aplicáveis à organização?

Na dimensão do "compartilhamento de dados pessoais", constou no relatório que a organização deve documentar detalhes relacionados ao compartilhamento de dados pessoais com terceiros, sob a alegação de que a realização de compartilhamento demanda a adoção de controles adequados para mitigar os riscos que possam comprometer a proteção de dados pessoais. A Lei Geral de Proteção de Dados defende que as precauções a serem adotadas entre as partes envolvidas no compartilhamento sejam formalizadas em contrato e que os cuidados especiais devem ser adotados no caso de transferência internacional dos dados.

O foco aqui foi a identificação dos dados pessoais que são compartilhados ao registro de eventos correlatos aos compartilhamentos e à transferência internacional de dados pessoais. Foi feita a seguinte pergunta: A organização identificou os dados pessoais que são compartilhados com terceiros?

Sobre a dimensão da "violação de dados pessoais", a organização deve gerenciar incidentes de segurança da informação que envolvem a violação de dados pessoais. As indagações aqui estão vinculadas à identificação, ao registro e ao tratamento de incidentes de violação de dados pessoais. Além disso, também será avaliado se a organização dispõe de

[482]BNDES. Relatório BNDES – Tribunal de Contas da União. A organização deve assegurar que os titulares tenham acesso a informações relacionadas ao tratamento de seus dados pessoais. Para isso, a organização deve publicar, de maneira clara e concisa, informações relativas ao tratamento de dados pessoais. A organização também deve estar preparada para atender todos os direitos dos titulares que são elencados na LGPD. Nesta seção são abordadas questões relacionadas à elaboração da política de privacidade e ao atendimento dos direitos dos titulares. Disponível em: https://www.bndes.gov.br/wps/wcm/connect/site/3c4a346e-2406-423a-baf9-b19cc8b39683/Relat%C3%B3rio+de+Feedback+BNDES.pdf?MOD=AJPERES&CVID=og-e9dt. Acessado em 29 de mai. 2024.

mecanismo para notificar a Autoridade Nacional de Proteção de Dados e os titulares nos casos de incidentes que possam acarretar risco ou dano relevantes aos titulares[483].

As perguntas sobre essa violação de dados pessoais foram organizadas da seguinte forma: A organização possui Plano de Resposta a Incidentes (ou documento similar) que abrange o tratamento de incidentes que envolvem a violação de dados pessoais? A organização possui sistema para o registro de incidentes de segurança da informação que envolvem violação de dados pessoais? A organização possui sistema para registro das ações adotadas para solucionar incidentes se segurança da informação que envolvem violação de dados pessoais? A organização monitora proativamente a ocorrência de eventos que podem ser associados à violação de dados pessoais? A organização estabeleceu procedimentos para comunicar à Autoridade Nacional de Proteção de Dados e ao Titular a ocorrência de incidente se segurança que possa acarretar risco ou dano relevante aos titulares?

Por fim, na dimensão das "medidas de proteção", a organização deve adotar medidas de segurança técnicas e administrativas para que os dados pessoais sejam protegidos. Isso deve ser feito através da mitigação de riscos que possam resultar em violação da privacidade. Nessa dimensão, as indagações foram estruturadas no sentido de aferir se a organização implementou controles para a restrição e o rastreamento do acesso a dados pessoais e se ocorreu a avaliação de impacto sobre a proteção de dados pessoais[484].

As indagações sobre as medidas de proteção podem ser feitas da seguinte forma: A organização é capaz de comprovar que adotou medidas de segurança técnicas e administrativas

[483]BNDES. Relatório BNDES – Tribunal de Contas da União. A organização deve gerenciar incidentes de segurança da informação que envolvem a violação de dados pessoais. Nesta seção são abordadas questões relacionadas à identificação, ao registro e ao tratamento de incidentes de violação de dados pessoais. Também será avaliado se a organização dispõe de mecanismo para notificar a Autoridade Nacional de Proteção de Dados e os titulares nos casos de incidentes que possam acarretar risco ou dano relevante aos titulares. Disponível em: https://www.bndes.gov.br/wps/wcm/connect/site/3c4a346e-2406-423a-baf9-b19cc8b39683/Relat%C3%B3rio+de+Feedback+BNDES.pdf?MOD=AJPERES&CVID=og-e9dt. Acessado em 29 de mai. 2024.

[484]BNDES. Relatório BNDES – Tribunal de Contas da União. A organização deve adotar medidas de segurança, técnicas e administrativas, para proteger os dados pessoais. Para isso, convém que sejam implementados controles capazes de mitigar riscos que possam resultar em violação da privacidade. Nesta seção serão abordadas questões relacionadas à implementação de controles para restringir e rastrear o acesso a dados pessoais e à avaliação de impacto sobre a proteção de dados pessoais. Disponível em: https://www.bndes.gov.br/wps/wcm/connect/site/3c4a346e-2406-423a-baf9-b19cc8b39683/Relat%C3%B3rio+de+Feedback+BNDES.pdf?MOD=AJPERES&CVID=og-e9dt. Acessado em 29 de mai. 2024.

aptas a proteger os dados pessoais? A organização implementou processo para registro, cancelamento e provisionamento de usuários em sistemas que realizam o tratamento de dados pessoais? A organização registra eventos das atividades de tratamento de dados pessoais? A organização utiliza criptografia para proteger dados pessoais? A organização adotou medidas para assegurar que processos e sistemas sejam projetados, desde a concepção, em conformidade com a Lei Geral de Proteção de Dados (*Privacy by Design e Privacy by Default*)?

Da mesma forma como ocorreu com o BNDES, a Petrobrás também foi avaliada através do Relatório de Feedback do Tribunal de Contas da União. A Petrobrás, inclusive, dedica uma área do seu site para tratar sobre privacidade e proteção de dados pessoais[485]. Por uma questão lógica, embora o BNDES e a Petrobrás não tratem dados pessoais para fins penais, o modelo de estrutura do tratamento de dados pessoais apresentado pelas duas empresas pode servir de referência para futura eventual estruturação da proteção de dados no direito penal.

7.1 Armazenamento de Dados nas Polícias Judiciárias Brasileiras

Antes da abordagem desse armazenamento de dados pelas Polícias Judiciárias Brasileiras, é importante ressaltar que todo aquele que, no desempenho de suas funções, trabalha com dados pessoais, é obrigado pautar sua atuação com bases nos pilares da confidencialidade e da integridade. Embora a utilização dos dados pessoais armazenados pelas Polícias Judiciárias brasileiras dispense autorização judicial, o tema precisa ser analisado sob o prisma do direito fundamental da proteção de dados, previsto em nossa Constituição Federal.

Conforme já mencionado anteriormente, ao longo dos anos, com o veloz avanço dos meios tecnológicos, as Polícias Judiciárias foram obrigadas a reestruturarem a forma como os dados pessoais são armazenados e utilizados. Isso foi necessário porque o crime está cada vez mais organizado, utilizando os meios digitais e a alta tecnologia como instrumentos facilitadores para a prática de novos tipos de delitos.

A investigação dos mais variados tipos de crimes faz com que seja praticamente obrigatória uma adequada capacitação profissional de todos os profissionais que fazem parte da persecução penal, o que não é o suficiente para uma investigação bem sucedida. É preciso

[485]Petrobrás. Privacidade e Proteção de Dados pessoais. Disponível em: https://petrobras.com.br/privacidade-protecao-de-dados. Acessado em 02 de jun. 2024.

modernizar as leis, para permitir, sem deixar de observar as garantias previstas na Constituição Federal, maior controle das Polícias na fiscalização de utilização de métodos tecnológicos.

Isso não quer dizer que a polícia necessite de autorização judicial para ter acesso a determinados tipos de informações, mas caso isso seja necessário, que a autorização seja ágil e eficiente, a ponto de não se perder o imediatismo que determinados tipos de investigação requerem. Sabemos que a exigência imediata de autorização judicial para acesso ao manuseio de determinados tipos de dados é praticamente impossível. Apenas a título de exemplo, embora a temática não esteja diretamente ligada ao tema abordado neste trabalho, vejamos o Tema 977 do Supremo Tribunal Federal[486].

O Tema se refere à verificação da licitude da prova produzida durante o inquérito policial, relativa ao acesso, sem autorização judicial, a registros e informações contidos em aparelho de telefone celular, relacionados à conduta delitiva e hábeis a identificar o agente do crime. O Tema em questão foi incluído no Plenário Virtual no dia de outubro de 2020. O Ministro Dias Toffoli foi favorável ao provimento do recurso extraordinário do Ministério Público, nos moldes do precedente do HC 91.867/PA[487].

O Ministro Gilmar Mendes, no entanto, divergiu e reviu o seu posicionamento, afirmando que a mudança das circunstâncias fáticas faz com que os dados armazenados em aparelhos celulares alcancem a proteção constitucional do sigilo, tendo em vista que, nos dias atuais, "cada vez mais a nossa vida quase inteira está registrada em nossos aparelhos celulares". Da mesma forma, quando precisamos fazer o registro de ocorrência policial, quando precisamos solicitar a emissão de uma carteira de identidade ou quando precisamos de um passaporte, dados pessoais de extrema importância são armazenados. A partir do armazenamento dos dados, é possível saber o seu endereço, os números dos seus documentos, quantos carros há em seu nome, além de outros tipos de informações. É possível que o acesso aos dados pessoais que constam nos bancos de dados das polícias judiciárias brasileiras, seja mais invasivo que o acesso aos dados debatidos no Tema 977.

[486]STF, ARE 1042075, Tema 977, Tribunal Pleno, Rel. Min. Dias Toffoli, J. 24.11.2017, DJe 12.12.2017.
[487]STF HC 91867 PA, Segunda Turma, Min. Gilmar Mendes, J. 24.04.2012, DJe 20.09.2012.

O fato é que o Ministro Gilmar Mendes alegou que a mudança do seu posicionamento se deu após a promulgação do Marco Civil da Internet[488]. Consta no Artigo 7º, Inciso III do referido regulamento que o acesso à internet é essencial ao exercício da cidadania, sendo assegurado ao usuário o direito à inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial. Ainda de acordo com o Ministro Gilmar Mendes, nos dias de hoje os telefones celulares concentram grande poder de armazenamento em relação à vida pessoa dos acusados, atingindo naturalmente sua intimidade, de deve gozar de garantia constitucional.

Na ocasião, o Ministro citou o julgamento ocorrido na Alemanha em 2018. Lei estadual do Estado de Nordrhein-Westfalen foi declarada inconstitucional porque permitia à polícia a realização de busca ou de investigações secretas e remotas em computadores de pessoas suspeitas. O Tribunal Constitucional da Alemanha decidiu que dados pessoais não poderiam ser acessados de forma indiscriminada, sem haver um procedimento com instrumentos de controle contra os acessos indevidos. Ainda em seu voto, foi citado o *case Riley v Califónia*, onde a Suprema Corte Americana decidiu que uma busca de conteúdos digitais em celular apreendido durante prisão seria inconstitucional por falta de autorização judicial e por violação da 4ª Emenda.

A 4ª Emenda dispõe que:

> O direito das pessoas de estarem seguros em suas pessoas, casas, papéis e pertences, contra buscas e apreensões injustificadas, não será violado, e nenhum mandado será emitido, mas mediante causa provável, apoiada por juramento ou afirmação, e particularmente descrevendo o local a ser revistado e as pessoas ou coisas a serem apreendidas[489].

O que deve ser destacado é que no julgamento ora analisado foi abordada a tese de que os dados digitais armazenados em telefone celular não podem, por si só, serem usados como arma para prejudicar um policial que realizou uma prisão ou para efetuar a fuga do preso. Os agentes da lei continuaram livres para examinar os aspectos físicos de um telefone e para garantir que eventualmente o aparelho não seja utilizado como uma arma – por exemplo, como já ocorreu com criminosos que esconderam lâminas de barbear entre o aparelho de telefone e a

[488]BRASIL. Marco Civil da Internet. Lei número 12.965/2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acessado em 05 de mai. 2024.
[489]Whitehouse.gov. The Constitution. Disponível em: https://www.whitehouse.gov/about-the-white-house/our-government/the-constitution/. Acessado em 05 de mai. 2024.

capa de silicone que o protege. Uma vez que um policial tenha protegido um telefone e eliminado quaisquer ameaças físicas potenciais, os dados no telefone não poderão colocar ninguém em perigo.

Gilmar Mendes também mencionou sobre o risco de autorizar o acesso parcial a informações, o que seria um incentivo à prática do *fishing expedition*[490], também conhecida como pescaria predatória, que é uma prática proibida pelo ordenamento jurídico brasileiro, onde não se admite investigações especulativas indiscriminadas, sem objetivo certos ou não declarados, que lança suas redes na esperança de "pescar" qualquer prova para subsidiar uma futura acusação. Admite-se, porém, o fenômeno do encontro fortuito, ou serendipidade, entendido como a descoberta inesperada, no decorrer de uma investigação legalmente autorizada, de provas sobre crime que a princípio não estava sendo investigado.

Seguindo a corrente capitaneada pela Suprema Corte dos Estados Unidos, o Ministro Gilmar Mendes negou provimento ao recurso, alegando que o acesso a registros telefônicos, agenda de contatos e demais dados contidos em aparelhos celulares apreendidos no local do crime atribuído ao acusado depende de prévia decisão judicial que justifique, com base em elementos concretos, a necessidade e adequação da medida e delimite a sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade e ao sigilo das comunicações e dados dos indivíduos[491].

Cabe ressaltar que durante o julgamento do caso, o relator, Ministro Dias Toffoli, retificou o seu posicionamento e aderiu ao mesmo entendimento do Ministro Gilmar Mendes. Na ocasião, foi fixada uma nova tese de repercussão geral, onde o acesso a informações de telefones apreendidos no local de crime, depende de prévia autorização judicial tendo em vista os direitos fundamentais à privacidade, intimidade, ao sigilo das comunicações e à proteção de dados.

O fato é que toda investigação policial, de certo modo, restringe algum tipo de direito fundamental. Isso pode acontecer desde que haja previsão legal, com indicação concreta e fundamentada de indícios de autoria e materialidade em face de pessoa determinada ou possível de determinação. Seja qual for o delito que precisa ser investigado, é necessário que existam

[490]STJ, HC 663055 MT, Sexta Turma, Rel. Min. Rogério Schietti Cruz, J. 22.03.2022, DJe 31.03.2022.
[491]*Ibid.*

critérios legais objetivos. O que temos hoje é um imenso vácuo legislativo, já que o Marco Civil da Internet faz menção ao sigilo dos dados, mas até o presente momento nada foi regulamentado. Nina Nery afirma que o uso indiscriminado do poder punitivo coloca a sociedade no limite da ruptura das garantias que fundamentam o Estado Democrático de Direito, onde se busca uma convivência harmônica entre o garantismo penal e a eficiência[492].

A cada ano as instituições policiais aumentam seus bancos de dados, seja através de informações colhidas no ato de um simples registro de ocorrência policial, onde o titular dos dados pode ter sido vítima de um crime, seja através de suspeito que esteja sendo investigado. Apesar da enorme quantidade de informações, o mapeamento de dados, por si só, não afeta a vida das pessoas, tão pouco viola a dignidade da pessoa humana, mas pode restringir o direito fundamental à proteção de dados pessoais. A Administração Pública é, em última análise, uma máquina informacional que precisa ser controlada pelo Direito[493]. A organização do Estado moderno exige que o poder público realize volumosas operações de tratamento de dados pessoais para tomar decisões e realizar suas finalidades públicas. Há, portanto, uma íntima relação entre a gestão informacional dos órgãos e entes públicos e a realização eficiente de atividades de interesse público[494].

Diante da ausência de legislação específica, a partir do momento em que os dados são utilizados é que o Estado deverá interceder, possivelmente na forma de incidente judicial, para aferir de que forma a utilização pode afetar o mínimo possível a autonomia das pessoas, observando quais direitos fundamentais serão atingidos com o tratamento dos dados pessoais. Outro aspecto que deve ser destacado é que, no âmbito da atividade policial, dificilmente os dados são acessados com o consentimento do titular, o que significa dizer que eventualmente o Estado fará o acesso sem que o titular sequer desconfie. Cabe salientar que a aferição da ponderação de bens mencionada neste trabalho não cabe às polícias, mas ao legislador e ao judiciário.

---

[492]NERY, Nina. O compartilhamento de dados financeiros no sistema antilavagem de dinheiro brasileiro. São Paulo: Thompson Reuters Brasil, 2024. P.95.

[493]BREGA, José Fernando Ferreira. O Governo eletrônico e direito administrativo. Tese de Doutorado apresentada à Universidade de São Paulo, São Paulo. 2012. p.61.

[494]GASIOLA, Gustavo Gil; MACHADO, Diego; MENDES, Laura Schertel. A Administração Pública entre transparência e proteção de dados. Revista de Direito do Consumidor. Vol. 135. Ano 30. P. 179-201. São Paulo: Ed. RT, maio/jun. 2021. Disponível em: http://revistadostribunais.com.br/maf/app/document?stid=st-rql&marg=DTR-2021-9042. Acesso em 29 de nov. 2024.

Há quem diga que a prática pode violar direitos fundamentais, além de gerar enormes danos aos titulares de dados pessoais. Quando o Estado, através das instituições policiais, inicia uma investigação para identificar a autoria de algum crime, seja ele qual for, é porque outro direito fundamental também foi violado (fala-se em direito fundamental da vítima). Além disso, também é preciso frisar que em muitos casos, os dados pessoais utilizados pelas polícias são os mesmos dados que facilmente podem ser vistos no google, por exemplo.

É preciso ressaltar, mais uma vez, que qualquer intervenção do Estado em direitos fundamentais necessita de uma justificação especial, tornando ilícita qualquer violação que não seja justificada. A liberdade individual constitui um limite à atividade do Estado, que não pode invadir a esfera da autodeterminação do indivíduo fora das hipóteses taxativas e dos requisitos expressamente previstos em lei[495].

Ainda sobre a temática, Maíra Fernandes escreveu artigo intitulado *Lei de Proteção de Dados para a Segurança Pública e Persecução Penal*, demonstrando a urgência de aprovação de uma Lei Geral de Proteção de Dados no âmbito penal. Para Maíra Fernandes, "a proteção de dados individuais carece de previsão legal quando às investigações criminais e ações penais, seara em que, sabiamente, os direitos e garantias fundamentais do indivíduo acusado ou investigado não mais relativizados"[496].

Para Jamilla Monteiro Sarkis, "a necessidade de coleta de dados da pessoa imputada, para fins de persecução penal, é premente"[497]. A Autora reforça que as fases de investigação, processamento e julgamento de fatos penais dependem, necessariamente, da identificação e individualização daqueles que, ao menos em tese, podem ser criminalmente responsáveis pela prática de um crime. "É natural, portanto, que os bancos de dados de informação do Estado sejam utilizados para identificação criminal, desde que regulamentados com base nos direitos constitucionalmente consagrados"[498], conclui.

---

[495]GRINOVER, Ada Pelegrini. Liberdades públicas e processo penal: as interceptações telefônicas. 2ª ed. São Paulo: Revista dos Tribunais, 1982.

[496][496]FERNANDES, Maíra. Lei de Proteção de Dados para Segurança Pública e Persecução Penal. Disponível em: https://www.conjur.com.br/2022-out-28/escritos-mulher-lei-protecao-dados-seguranca-publica-persecucao-penal/. Acesso em 09 de set. 2024.

[497]SARKIS, Jamilla Monteiro. Dados Pessoais no Processo Penal: tutela da Personalidade e da Inocência diante da Tecnologia. Revista Brasileira de Ciências Criminais. Vol. 190. Ano 30. p. 117-156. São Paulo: Ed. RT, maio/jun. 2022.

[498]*Ibid.*

Percebe-se uma preocupação da autora com a questão de falha em reconhecimentos faciais, reconhecimentos fotográficos equivocados, má utilização de dados e de invasão de privacidade pelos órgãos de persecução e repressão penal quando fazem mau uso da individualização e identificação de pessoas através da geolocalização, bem como devassas em sigilos telefônicos, telemáticos, de dados, bancários e compartilhamento de dados, tudo em detrimento de um relativo sucesso das investigações.

De fato, as questões ora levantadas são muito sensíveis e podem colocar em risco toda a instrução criminal. O Poder de Polícia possui algumas barreiras que se forem ultrapassadas, saem da seara da legalidade e entram na seara da arbitrariedade, do abuso de poder e do abuso de autoridade, o que leva o agente público a sofrer sanções de natureza administrativa, cível e criminal.

O Poder de Polícia, no entanto, é necessário para satisfação do interesse da coletividade. Segundo Jean Rivero, para que a Administração Pública assegure o bem estar geral, não pode se colocar em pé de igualdade com os particulares. Por esse motivo, a Administração Pública possui o instrumento jurídico denominado Poder de Polícia, que autoriza a execução de atos coercitivos que, quando se colidem, fazem o interesse geral prevalecer sobre o interesse individual[499].

Transportando o mesmo raciocínio para o tema deste trabalho, podemos depreender que no âmbito de uma investigação policial, eventualmente o direito fundamental da proteção de dados do autor de um delito deve ser mitigado em detrimento dos direitos dundamentais da vítima. Percebe-se uma enorme preocupação com a proteção de dados pessoais, mas é preciso reforçar que existem outros direitos fundamentais que também precisam ser protegidos.

A impressão que se tem é a de que a missão da proteção de dados pessoais se tornará cada vez mais difícil, já que com o avanço da tecnologia, nossos dados pessoais estão registrados e armazenados em todos os lugares. Apenas a título de exemplo, para aguardarmos na fila de espera de um restaurante, nos pedem nossos nomes e os números dos nossos números de telefones celulares, para que possamos receber uma mensagem quando a mesa estiver

[499]RIVERO, Jean. Direito Administrativo. tradução de Rogério Ehrhardt Soares, Livraria Almedina, Coimbra, Portugal, 1981, p. 15.

disponível. Qualquer compra efetuada na internet só pode ser concluída com a inserção dos nossos dados pessoais. Até mesmo nas compras presenciais nos pedem nossos dados sob a alegação de que clientes cadastrados possuem descontos.

O que deve ser observado não é a utilização dos bancos de dados pelas polícias para a prevenção ou apuração de crimes, mas o mau uso ou o abuso de poder na utilização dos dados pessoais. Todo agente público, seja ele político ou administrativo, exerce uma espécie de autoridade pública, que não é um privilégio, mas uma prerrogativa decorrente da investidura do cargo público que ocupa.

Os dados armazenados nos bancos de dados das Polícias Judiciárias Brasileiras no ato de um registro de ocorrência policial ou da confecção de uma carteira de identidade, por exemplo, são os mesmos dados utilizados pelos cidadãos para fazerem compras pela internet. Quando acessamos quaisquer sites, empresas privadas dispõe das mesmas informações que as polícias possuem nos bancos de dados. A diferença é que as instituições policiais utilizam os dados para identificar autores de crimes, ao passo que as empresas privadas os utilizam para mapear o perfil de consumo do cliente.

Além disso, é muito comum que a identificação de autores de crimes também aconteça através das chamadas fontes abertas, que são as informações ou dados disponíveis na internet ou em redes sociais para qualquer pessoa, ou seja, livre de sigilos. Orlandino Gleizer, no entanto, ressaltar que a obtenção, o armazenamento, a transferência e a utilização de dados por para do Estado devem ser compreendidas como intervenções autônomas, porque interferem quantitativa e qualitativamente de formas distintas nos direitos fundamentais dos seus titulares[500].

O agente público, portanto, deve cumprir seu ofício regido pelos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência, conforme preceitua o Artigo 37 Caput da Constituição Federal. Hely Lopes Meirelles escreveu que o uso de poder é uma

[500]GLEIZER, Orlandino. A proteção de dados por duas portas nas intervenções informacionais. A declaração de inconstitucionalidade pelo Tribunal Federal Constitucional alemão de regras garantidoras de acesso estatal a dados constitutivos de serviços de telecomunicação (Bestandsdatenauskunft II). Revista de Estudos Criminais, São Paulo, v. 19, n. 79, 2020, p. 211-230.

prerrogativa da autoridade, mas o poder há de ser usado normalmente sem abuso[501]. Usar normalmente o poder é emprega-lo segundo as normas legais, a moral da instituição, a finalidade do ato e as exigências do interesse público. Abusar do poder é empregá-lo fora da lei, sem utilidade pública. O poder é confiado ao administrador público para ser usado em benefício da coletividade, nos justos limites que o bem estar social exigir. A utilização desproporcional do poder, o emprego arbitrário da força, da violência contra o administrado constituem forma abusivas do uso do poder estatal, não toleradas pelo direito e geradoras de nulidades de atos.

O uso do poder é lícito e o abuso é sempre ilícito, por esse motivo todo ato abusivo é nulo por excesso ou desvio de poder. Ainda de acordo com Hely Lopes Meirelles, o abuso de poder ora se apresenta ostensivo como a truculência, às vezes dissimulado como o estelionato, e não raro encoberto pela aparência ilusória de atos legais. Em qualquer desses aspectos, flagrante ou disfarçado, o abuso de poder é sempre uma ilegalidade que invalida o ato administrativo[502].

Para Hely Lopes Meirelles, o abuso de poder ocorre tanto por ação quanto por omissão, que através das formas comissivas e omissivas são capazes de afrontar as leis e causar lesão ao direito individual do administrado, que resulta na forma omissiva de abuso de poder, seja o ato doloso ou culposo[503].

O Poder de Polícia, portanto, não é ilimitado. Quem trabalha com investigação policial, não recebe uma carta branca do Estado para fazer o que quiser com dados pessoais, sejam dados de autores, vítimas ou testemunhas. Conforme preceitua José Cretella Júnior, da mesma forma que os direitos individuais são relativos, assim também ocorre com o Poder de Polícia, que longe de ser onipotente, incontrolável, é circunscrito, jamais podendo colocar em perigo a liberdade e a propriedade[504]. Ainda de acordo com José Cretella Júnior, "a missão primordial do Estado é a busca pelo bem comum e a segurança das pessoas e dos bens é elemento básico

[501]LOPES MEIRELLES, Hely. Direito Administrativo Brasileiro. Ed. atualizada por ANDRADE AZEVEDO, Eurico de et alii, 1995, Malheiros Editora, São Paulo, p. 94.
[502]*Ibid, p. 95.*
[503]*Ibid. p. 95.*
[504]CRETELA JÚNIOR, José. Polícia e Poder de Polícia. Revista de Direito Administrativo. Fundação Getúlio Vargas, Rio de Janeiro, nº 162, p. 31-32.

das condições universais, fator absolutamente indispensável para o natural desenvolvimento da personalidade humana[505].

Com as devidas adaptações, trazendo o raciocínio para os dias de hoje, vivemos em uma sociedade digital, na qual a segurança das pessoas continua sendo condição universal para o desenvolvimento da personalidade humana, o que faz com que o Direito Fundamental à proteção de dados seja mitigado, mas não desrespeitado. É preciso frisar que o abuso no exercício do Poder de Polícia está sujeito aos controles administrativo e judicial. Apesar disso, segundo Luís Roberto Barroso, os princípios da dignidade humana e da razão pública identificarão o interesse público preponderante[506].

Quando escreveu sobre a violação sistemática dos direitos humanos como limite à consolidação do Estado de Direito no Brasil, Oscar Vilhena Vieira ponderou no sentido de que para a fruição dos direitos dos indivíduos, é necessário que o Estado seja estruturado de uma forma específica voltada para limitar o seu poder. Para o Autor, a regra fundamental do modelo de Estado é a separação de poderes, sendo garantido aos indivíduos a possibilidade de recorrerem ao Poder Judiciário todas as vezes que se virem ameaçados em seus direitos[507].

É necessário reforçar o que já foi dito alhures neste trabalho, ou seja, que o Poder Executivo não possui carta branca para implementar políticas de segurança pública que ofenda a Constituição[508]. Apenas a título de exemplo, imaginemos que determinado Policial possa

---

[505]CRETELLA JÚNIOR, José. Lições de Direito Administrativo. Forense Editora, Rio de Janeiro. cit. p. 227.

[506]"O interesse público primário, consubstanciado em valores fundamentais como a justiça e segurança, há de desfrutar de supremacia de um sistema constitucional e democrático. Deverá ele pautar todas as relações jurídicas e sociais – dos particulares entre si, deles com as pessoas de direito público e destas entre si. O interesse público primário desfruta de supremacia porque não é passível de ponderação; ele é o parâmetro de ponderação; ele é o parâmetro de ponderação. Em suma: o interesse público primário consiste na melhor realização possível, à vista da situação concreta a ser planejada, da vontade constitucional, dos valores fundamentais que ao intérprete cabe preservar ou promover. O problema ganha complexidade quando há confronto entre o interesse público primário consubstanciado em uma meta coletiva e o interesse público primário que se realiza mediante a garantia de um direito fundamental. [...] Na solução desse tipo de colisão, o intérprete deverá observar, sobretudo, dois parâmetros: a dignidade humana e a razão pública. [...]. Assim, se determinada política representa a concretização de importante meta coletiva (como a garantia da segurança pública ou da saúde pública, por exemplo), mas implica a violação da dignidade humana de uma só pessoa, tal política deve ser preterida, como há muito reconhecem os publicistas comprometidos com o Estado de Direito. Cf. sobre o tema, SARMENTO, D. Dignidade da Pessoa Humana: conteúdo, trajetórias e metodologia. 3. Ed. Belo Horizonte: Fórum, 2021; BARROSO, L.R. A dignidade da pessoa humana no direito constitucional contemporâneo. Belo Horizonte: Fórum, 2013.

[507]VILHENA VIEIRA, Oscar et aljj. Direito, Cidadania e Justiça. coordenação de DI GIORGI, Beatriz, CAMPILONGO, Celso Fernandes e PIOVESAN, Flávia, I!ed., 1995, Editora Revista dos Tribunais, São Paulo, p. 191.

[508]SARMENTO, D; BORGES, A; ADAMI, E. Parecer. FILTRAGEM CONSTITUCIONAL DOS PEDIDOS DE SUSPENSÃO DE SEGURANÇA. INTERESSE PÚBLICO PRIMÁRIO QUE TUTELA DIREITOS

buscar nos bancos de dados de sua instituição informações sobre suspeito de suposto crime de roubo. O mesmo Policial, no entanto, não pode se valer do seu cargo para atender pedido de amigo que lhe solicita consulta do nome de determinada pessoa que pretende contratar, sob a alegação de não querer funcionário com "antecedentes criminais".

Embora exista o meio correto para isso, que é a solicitação de certidão de antecedentes criminais, no dia a dia é comum que Policiais recebam esse tipo de pedido, o que configura um fato grave. Os bancos de dados das Polícias só devem ser utilizados para identificar autores de crimes ou para prevenir delitos que estejam na iminência de acontecer.

Toda prática ilegal que viole as boas regras que gravitam ao redor da utilização dos dados pessoais, deve ser punida com rigor. Apenas a título de exemplo, o Ministério Público Federal (MPF) e o Instituto de Defesa dos Consumidores (IDEC), ajuizaram Ação Civil Pública[509] para que o WhatsApp fosse condenado a pagar indenização de R$ 1.733 bilhão por danos morais coletivos, entre outras obrigações.

O Ministério Público Federal e o Instituto de Defesa dos Consumidores alegaram que sem apresentar informações adequadas sobre as mudanças de sua política de privacidade em 2021, a empresa violou direitos dos usuários no Brasil ao forçar adesão às novas regras, o que viabilizou a coleta e o compartilhamento abusivo de dados pessoas com outras plataformas do Grupo Meta, entra elas o Facebook e o Instagram. Na ocasião, a Autoridade Nacional de Proteção de Dados também foi alvo dessa Ação Civil Pública.

O valor da indenização exigida teve como base os mesmos parâmetros utilizados na Europa, quando o WhatsApp cometeu irregularidades semelhantes. Durante os anos de 2021 a 2023, a União Europeia impôs ao WhatsApp multas de 230,5 milhões de euros, por omissões e ilegalidades na política de privacidade do aplicativo que ampliaram o compartilhamento de informações pessoais dos usuários na Europa. As sanções foram mantidas judicialmente, mesmo após a impetração de recursos.

FUNDAMENTAIS, SOBRETUDO DOS MAIS VULNERÁVEIS. LEGITIMIDADE ATIVA DA DEFENSORIA PÚBLICA COMO *CUSTUS VULNERABILIS*. Brasil.

[509]Ministério Público Federal. MPF e Idec querem que Whatsapp pague R$ 1,7 bilhão por violações de direitos em política de privacidade. Disponível em: https://www.mpf.mp.br/sp/sala-de-imprensa/noticias-sp/mpf-e-idec-querem-que-whatsapp-pague-r-1-7-bilhao-por-violacoes-de-direitos-em-politica-de-privacidade. Acesso em 09 de set. 2024.

Além da indenização, o Ministério Público Federal e o Instituto de Defesa dos Consumidores pediram que o WhatsApp fosse obrigado a interromper imediatamente o compartilhamento de dados pessoais para finalidades próprias das demais empresas do Grupo Meta, com a veiculação personalizada de anúncios de terceiros. A ação também requereu que o aplicativo disponibilizasse funcionalidades simples que permitam aos usuários o exercício de seu direito de recusar as mudanças trazidas pela política de privacidade da plataforma a partir de 2021, caso não estejam de acordo com seus termos, ou mesmo de voltar atrás e cancelar a adesão que eventualmente já tenham feito a essas regras, sem que sejam proibidos de continuar utilizando o aplicativo.

De acordo com a Ação Civil Pública, as práticas do WhatsApp violaram diversos dispositivos da Lei Geral de Proteção de Dados, principalmente o que confere aos cidadãos de estarem amplamente informados e livres de coação ao manifestarem o consentimento para que seus dados pessoais sejam utilizados no mercado. Com a atualização da política de privacidade, o WhatsApp deixou de explicar aos usuários sobre as alterações que seriam feitas e os forçaram a manifestar concordância com as mudanças.

Ainda de acordo com o Ministério Público Federal e o Instituto de Defesa dos Consumidores, com a prática o WhatsApp passou a ter acesso a diversos dados dos usuários, tais como nomes completos, fotos dos perfis, lista de contatos, grupos e comunidades que fazem parte, localização, tempo de uso da plataforma e até mesmo o nível de bateria dos aparelhos. Todas as informações estavam sendo compartilhadas com empresas do Grupo Meta, para fazer um mapeamento de hábitos, preferências e características dos usuários. A Autoridade Nacional de Proteção de Dados – ANPD, também figurou como ré na referida Ação Civil Pública, por omissão e falta de cooperação diante das práticas abusivas exercidas pelo WhatsApp.

Outra Ação Civil Pública que também foi objeto de análise da Justiça Federal foi a proposta pelo Ministério Público Federal em desfavor da União, no ano de 2022[510].A Ação Civil Pública teve como objeto a obtenção de prestação jurisdicional para anular parte do Projeto Excel, cujo protocolo foi aprovado pela Portaria número 26, do dia 09 de julho de 2020,

[510]Data Privacy Br. Ação Civil Pública/Inquérito Civil nº 1.16.000.002757/2022-36. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2022/12/pr-df-00128369.2022-2.pdf. Acesso em 12 de set. 2024.

no ponto em que estabeleceu o compartilhamento dos dados extraídos por força de decisão judicial com a SOPI/MJSP como contrapartida à disponibilização de ferramentas de extração e análise de dados de dispositivos móveis.

Os outros objetivos da Ação Civil Pública foram: solicitar a anulação das cláusulas constantes nos termos de adesão firmados com os Estados, que impõem aos aderentes o compartilhamento de dados extraídos por força de decisão judicial com a SEOPI/MJSP, como contrapartida à utilização de ferramenta de extração e análise de dados de dispositivos móveis; e obrigar a União a destruir a integralidade dos dados eventualmente já compartilhados com a Secretaria de Operações Integradas (SEOPI), em razão do Projeto Excel.

Antes de falarmos mais sobre essa Ação Civil Pública, é de extrema importância falar sobre o Projeto Excel, do Ministério da Justiça e Segurança Pública[511]. O projeto, criado em 2020, foi um investimento em tecnologia feito pelo MJSP, para auxiliar as forças de segurança estaduais no combate ao crime organizado. Sob coordenação da Secretaria de Operações Integradas (SEOPI), o projeto Excel auxilia as Polícias Civis com o fornecimento de softwares forenses e hardwares para dar mais celeridade na extração e análise de celulares apreendidos de indivíduos envolvidos com o crime organizado.

O trabalho é feito mediante ordem judicial prévia de quebra de sigilo telemático no âmbito dos inquéritos policiais. Até o mês de fevereiro de 2022, mais de 2.350 ordens judiciais autorizaram o uso dos equipamentos pelas forças policiais de 26 unidades da federação que aderiram formalmente ao Projeto Excel. Os principais crimes investigados pelo Projeto são o tráfico de drogas, homicídios, roubo (cargas, banco e carro forte), lavagem de dinheiro, tráfico de armas e investigações relacionadas à pedofilia.

Além do investimento na aquisição de ferramentas, o Ministério da Justiça também capacitou servidores na atividade de extração e análise de dados. A Secretaria de Operações Integradas do Ministério da Justiça tem como objetivo estimular e induzir a investigação de infrações penais de maneira integrada com as forças federais e estaduais. A SEOPI também

[511]Ministério da Justiça e Segurança Pública. Projeto Excel. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/acao-do-ministerio-da-justica-e-seguranca-publica-ja-causou-prejuizo-de-r-1-bi-ao-crime-organizado. Acessado em 12 de set. 2024.

promove a integração das atividades de inteligência de segurança pública com órgãos que compõe o Subsistema de Inteligência e Segurança Pública.

Cabe ressaltar que a Secretaria de Operações Integradas (SEOPI), foi a mesma que foi proibida pelo Plenário do Supremo Federal de produzir ou compartilhar informações sobre a vida pessoal, as escolhas pessoais e as práticas cívicas de cidadãos e de servidores públicos federais, estaduais ou municipais identificados como integrantes do movimento político antifascistas[512].

Para integrantes do Intercept Brasil, a troca de informações foi mal intencionada e o acesso aos dados pode extrapolar os limites da investigação policial, porque não havia transparência na forma como o Ministério da Justiça acessava os dados, além do projeto misturar as funções de investigação e inteligência[513].

O Data Privacy Brasil, organização que tem como objetivo a fomentação e a cultura de proteção de dados e direitos digitais no brasil e no mundo, se mobilizou com as organizações Conectas, Transparência Internacional e Fórum Brasileiro de Segurança Pública e apresentou um ofício à 7ª Câmara de Coordenação e Revisão do Ministério Público Federal, solicitando a instauração de um inquérito para a obtenção de mais detalhes sobre o Projeto Excel, visando responsabilizar os órgãos públicos que eventualmente estivesse praticando abuso de autoridade. As organizações também realizaram reunião técnica com os Membros do Ministério Público Federal, para discutir detalhes do Projeto Excel, os aspectos de legalidade e licitude, diante de possíveis riscos ao devido processo legal e ao direito fundamental da proteção de dados pessoais, ambos previstos em nossa Constituição Federal.[514]

Na ocasião, as entidades levaram em consideração o entendimento do Supremo Tribunal Federal na Decisão da ADI 6529, que impossibilitou o uso de dados de inteligência sem motivação adequada e que desrespeite a reserva de jurisdição. No caso específico, a Rede Sustentabilidade e o Partido Socialista Brasileiro (PSB), ajuizaram no Supremo Tribunal

[512]STF, ADPF 722, Tribunal Pleno, Rel. Carmén Lúcia, J. 16.05.2022, DJe 22.06.2022.
[513]Intercept Brasil. Após reportagem do Intercept, MPF ajuíza ação civil pública contra Projeto Excel. Projeto do Ministério da Justiça que equipa polícias estaduais em troca de dados é considerado ilegal. Disponível em: https://www.intercept.com.br/2022/12/14/mpf-ajuiza-acao-contra-projeto-excel/. Acesso em 12 de set. 2024.
[514]Data Privacy Brasil. Projeto Excel: articulação da sociedade civil resulta em Ação Civil Pública do Ministério Público. Disponível em: https://www.dataprivacybr.org/documentos/projeto-excel-articulacao-da-sociedade-civil-resulta-em-acao-civil-publica-do-ministerio-publico/. Acesso em 12 de set. 2024.

Federal uma Ação Direta de Inconstitucionalidade, contra norma que condiciona a ato do Presidente da República o fornecimento de dados e conhecimentos específicos relacionados com a defesa das instituições e dos interesses nacionais à Agência Brasileira de Inteligência (Abin)[515].

Para os Autores da Ação Direta de Inconstitucionalidade, a Abin tem o poder de requisitar dados de investigações sigilosas, sigilo fiscal, relatórios do Conselho de Controle de Atividades Financeiras (Coaf) e dados de sigilo telefônico, dentre tantas outras informações sensíveis e sigilosas. O Objeto de questionamento da ADI foi o parágrafo 4º da Lei 9.883/1999[516], que, segundo argumentam, possibilita o desvirtuamento de finalidade da Agência, uma vez que o poder requisitório de informações e dados de todos os integrantes do Sistema Brasileiro de Inteligência (Sisbin) depende de regulamentação pelo Presidente da República.

Depois de fazerem um histórico desde o ano 2000 sobre os decretos regulamentadores da Lei 9.883/1999, os partidos perceberam que a requisição de informações se tornou ainda mais sensível com a edição do Decreto número 10.445/2020[517], o qual aprovou a estrutura regimental da Abin e deixou de restringir as hipóteses de requisição das informações no âmbito do Sisbin pela Agência.Com a mudança, portanto, basta uma requisição para que o Diretor Geral da Abin tenha acesso a informações sigilosas. Os Partidos alegaram que o Decreto número 10.445/2020 era mais um dos abusos do Governo Federal cuja intenção não seria aperfeiçoar o serviço de inteligência, mas dar mais dados a sua linha investigativa paralela, contra possíveis adversários políticos-ideológicos.

Os partidos buscaram reduzir o potencial alcance do dispositivo questionado[518], com a fixação, pelo STF, do entendimento de que o compartilhamento de dados no âmbito do Sisbin deve cumprir e preservar os direitos e garantias fundamentais dos cidadãos, “com especial

---

[515]STF, ADI 6529 DF, Tribunal Pleno, Rel. Min. Cármen Lúcia, J. 08.10.2021, DJe 18.10.2021.
STF Supremo Tribunal Federal. STF confirma limitações ao compartilhamento de dados do Sisbin. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=474835&ori=1. Acessado em 12 de set. 2024.

[516]BRASIL. Presidência da República. Lei número 9.883/1999. Disponível em: https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=9883&ano=1999&ato=83bQzaE9keNpWT7c9. Acessado em: 12 de set. 2024.

[517]BRASIL. Câmara dos Deputados. Decreto número 10.445/2020. Disponível em: https://www2.camara.leg.br/legin/fed/decret/2020/decreto-10445-30-julho-2020-790490-publicacaooriginal-161220-pe.html. Acessado em 12 de set. 2024.

[518]*Ibid.*

atenção aos deveres de motivação das solicitações, razoabilidade e proporcionalidade das demandas e proteção aos sigilos gravados por reserva de jurisdição.

Por unanimidade, o Supremo Tribunal Federal estabeleceu que os órgãos componentes do Sistema Brasileiro de Inteligência (Sisbin) somente podem fornecer dados e conhecimentos específicos à Agência Brasileira de Inteligência (Abin) quando comprovado o interesse público da medida, afastando qualquer possibilidade de atendimento a interesses pessoais ou privados[519].

A Relatora da Ação, Ministra Carmén Lúcia, reforçou que o fornecimento de dados à Abin visa integrá-los e tornar eficiente a defesa das instituições e dos interesses nacionais. Também reforçou que "somente dados e conhecimentos específicos relacionados a essas finalidades são legalmente admitidos e compatibilizam-se com a Constituição da República. Qualquer outra interpretação é inválida".

Segundo a Ministra, o compartilhamento de informações que visem ao interesse privado do órgão ou de agente público caracteriza desvio de finalidade e abuso de direito. "É proibido que se torne subterfúgio para o atendimento ou benefício de interesses particulares ou pessoais, especialmente daqueles que tem acesso aos dados, desvirtuando-se competências constitucionalmente definidas. Ainda de acordo com Carmén Lúcia, a sociedade não pode ser refém do voluntarismo de governantes ou de agentes públicos. O abuso da máquina estatal para atendimento de objetivos pessoais "é atitude ditatorial, em contraste com o Estado Democrático de Direito".

O Supremo Tribunal Federal entendeu, portanto, que as decisões sobre o fornecimento de dados deverão ser devidas e formalmente motivadas para eventual controle de legalidade pelo Poder Judiciário. Mesmo que haja interesse público, informações referentes às comunicações telefônicas ou de dados não podem ser compartilhadas, em razão de limitação aos direitos fundamentais. O STF também entendeu que nas hipóteses cabíveis de fornecimento de informações e dados à Abin, é imprescindível a instauração formal de procedimento e a existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização em caso de eventual omissão, desvio ou abuso.

---

[519] *Ibid.*

O entendimento do Supremo Tribunal Federal segue o mesmo raciocínio defendido neste trabalho. Diante da omissão legislativa no que diz respeito ao tratamento de dados para fins penais, mais especificamente o acesso aos bancos de dados das policiais judiciárias brasileiras, nada impede que não só as instituições policiais, mas todos os órgãos de persecução penal implementem políticas públicas direcionadas ao monitoramento da utilização dos dados, respeitado o interesse público, a implantação de sistemas que permitam identificar quem acessou os dados pessoais e a confecção de relatório de uso dos dados. As práticas permitirão que os órgãos de persecução penal, a qualquer momento, prestem contas ao Judiciário em caso de suspeita de abuso de poder.

Feitas essas observações, é necessário retornar para a Ação Civil Pública que questionou a União sobre possíveis irregularidades no Projeto Excel, regulamentado pela Portaria 26 de 2020, editada pela Secretaria de Operações Integradas no Ministério da Justiça e Segurança Pública (SEOPI/MJSP).

Conforme já foi mencionado acima, o Projeto Excel teve como objetivo a disponibilização, para as Secretarias de Segurança dos Estados, de ferramenta de extração e análise dos dispositivos móveis apreendidos por força de decisão judicial. A condição exigida dos Estados para a utilização desses softwares foi a autorização judicial para o compartilhamento dos dados extraídos com a Diretoria de Inteligência do Ministério da Justiça, com o objetivo de criar uma base de dados que possibilitasse a produção de conhecimento para fins de inteligência de segurança pública.

Conforme mencionado na própria Ação Civil Pública, a SEOPI/MJSP descreve, na informação número 20/2020/CGI/DNIT/SEOPI (PR-DF-00079824/2022), os seguintes objetivos do Projeto Excel:

> O Projeto Excel consiste na disponibilização, por empréstimo, às Secretarias de Segurança Pública dos Estados da Federação, de ferramenta de extração e análise de dados de dispositivos móveis apreendidos no bojo das suas investigações criminais, mediante prévia e imprescindível, em caso, autorização de uso pela DNIT/SEOP/MJSP precedida necessariamente de ordem judicial com determinação expressa par ao acesso ao material por parte do profissional por ela habilitado, a ser realizada por meio de solução tecnológica forense operada por profissional de polícia judiciária devidamente capacitado no uso da ferramenta, em acordo com o regramento do termo de adesão firmado pelos órgãos aderentes via Secretaria de Segurança Pública.

> Como contrapartida, estipulou-se que, na representação a ser encaminhada à Justiça com o pleito pela quebra do sigilo telemático do dispositivo apreendido, deveria o presidente da investigação solicitar também autorização para o compartilhamento dos dados extraídos com a Diretoria de Inteligência da SEOPI/MJSP, na qualidade de Agência Central do SISP – conforme Decreto número 3.695/2000 c/c Decreto número 9.662, de 1º de janeiro de 2019, visando a "criação de uma base de dados constituída por dados extraídos por ferramenta própria e compartilhados com a Diretoria de Inteligência, possibilitando a produção de conhecimento qualificado, oportuno e eficiente e que resulte em efetivas ações policiais em face das organizações criminosas"[520].

O Ministério Público Federal alegou que não existe em nosso ordenamento jurídico brasileiro norma que autorize o compartilhamento de dados sujeitos a reserva de jurisdição, obtidos em investigação criminal para fins de inteligência. Seguindo essa linha de raciocínio, o MPF fez menção à decisão do Supremo Tribunal Federal, proferida no julgamento da ADI 6529/DF, que possui eficácia contra todos e efeito vinculante, relativamente aos demais órgãos do Poder Judiciário e à administração pública direta e indireta, nas esferas federal, estadual e municipal, conforme preceitua o Artigo 102, § 2° da Constituição Federal.

O Ministério Público, portanto, expediu uma recomendação ao Ministro da Justiça e Segurança Pública, para que fossem adotadas as medidas necessárias aptas a anularem os dispositivos da referida portaria e das cláusulas dos termos de adesão firmado com os Estados, bem como procedesse a destruição de todos os dados sujeitos à reserva de jurisdição eventualmente já compartilhados com a SEOPI/MJSP em detrimento do Projeto Excel. Na ocasião, a SEOPI/MJSP enviou um Ofício ao Ministério Público Federal, informando que não acolheria a recomendação expedida e solicitou que fosse feito uma reavaliação do entendimento exposto na recomendação em questão, o que motivou o MPF a ajuizar a Ação Civil Pública diante da ausência de interesse de ajuste das condutas em âmbito extrajudicial.

Na fundamentação da Ação Civil Pública, o MPF alegou inconstitucionalidade do compartilhamento de dados sujeitos à reserva de jurisdição para fins de inteligência no âmbito do Projeto Excel, por violação dos Artigos 5º, Incisos X, XII e LXXIX; 37, Caput e 102, § 2º, todos da Constituição Federal, sob o fundamento de que a nossa Carta Magna conferia proteção especial à intimidade, à vida privada, à inviolabilidade e o sigilo de correspondências e

[520]Ministério da Justiça e Segurança Pública. Projeto Excel. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/acao-do-ministerio-da-justica-e-seguranca-publica-ja-causou-prejuizo-de-r-1-bi-ao-crime-organizado. Acessado em 12 de set. 2024.

comunicações telegráficas de dados e telefônicas, além do direito à proteção de dados pessoais, até mesmo nos meios digitais.

Sob essa perspectiva, o Ministério Público Federal entendeu que não existe norma legal no ordenamento jurídico brasileiro que autorize o compartilhamento de dados sujeitos à reserva de jurisdição, obtidos em investigação criminal para fins de inteligência. Entendeu, ainda, que enquanto a SEOPI/MJSP continuasse recebendo o compartilhamento e custodiando dados pessoais sigilosos, obtidos por força de decisão judicial, em razão do denominado Projeto Excel, haveria violação sistemática e permanente aos direitos e garantias fundamentais dos cidadãos, que teriam seus dados – sujeitos à reserva de jurisdição – transmitidos para agências de inteligência sem a existência de previsão legal para tal prática.

Seguindo entendimento diametralmente oposto, o Ministério da Justiça, acompanhado da Polícia Federal e da Anatel, defenderam a implementação de um software intrusivo nacional, para inibir e desestimular a aquisição de programas estrangeiros e provados de espionagem[521]. Durante audiência pública realizada no Supremo Tribunal Federal, o Ministro do STF, Cristiano Zanin, manifestou preocupação com o tema, diante de "suposta violação sistemática de preceitos fundamentais no uso de tais equipamentos para monitorar advogados, jornalistas, políticos e defensores de direitos humanos".

Para Victor Teixeira[522], consultor jurídico do Ministério da Justiça, não se pode permitir que empresas privadas acessem informações a partir de exploração de vulnerabilidades da rede pública de telecomunicações, como é o caso do sistema Pégasus, que é um software espião (*spyware*), que tem o objetivo de invadir celulares das vítimas sem que elas saibam, copiando o máximo de dados disponíveis nesses aparelhos.

Mensagens de texto, histórico de navegação da internet, localização são apenas alguns dos dados que podem ser coletados pelo sistema Pégasus. A ferramenta também é capaz de ativar microfones, câmeras e gravar chamadas. O Pégaus foi criado por uma empresa israelense

[521]Folha de São Paulo. Governo e PF defendem proibição de uso de softwares espiões. Disponível em: https://www1.folha.uol.com.br/poder/2024/06/governo-e-pf-defendem-no-stf-proibicao-de-uso-de-softwares-espioes-por-orgaos-de-inteligencia.shtml. Acesso em 13 de set. 2024.
[522]Consultor Jurídico. Ministério, PF e Anatel defendem software intrusivo nacional para inibir sistemas estrangeiros. Disponível em: https://www.conjur.com.br/2024-jun-11/ministerio-defende-software-intrusivo-nacional-para-inibir-sistemas-estrangeiros/. Acesso em 13 de set. 2024.

de cibersegurança, que é responsável pela comercialização e licenciamento do software para empresas e governos no mundo inteiro.

A empresa responsável pelo Pégasus, NOS Group, alega em seu site que o programa só é comercializado para agências governamentais que passam por uma avaliação do Governo de Israel[523]. Frisa que a empresa sempre destacou em seus comunicados oficiais que o Pégasus tem por objetivo ajudar governos, agências de inteligência e forças de segurança no combate ao terrorismo e outros crimes graves. O problema é que o software é usado por governos ao redor do mundo de forma sigilosa, o que pode resultar em uma espécie de vigilância autoritária. A NSO Group não divulga os nomes das instituições que fazem uso do Pégasus.

Estudo realizado em 2022 pelo Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.REC), considerando lapso temporal de 2015 a 2021, identificou 209 contratos para contratação de software de hacking treinamento de funcionários, termos aditivos e atualização de softwares[524]. O estudo também revelou que a existência de contratos do gênero em todos os Estados brasileiros, realizados por diversos órgãos.

Apenas no ano de 2020, houve um gasto de 55 milhões de reais com a compra desses softwares, sendo que em 2019 o gasto havia sido de 7 milhões de reais. Segundo Raquel Saraiva, presidente e fundadora do Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.REC), até órgãos que não possuem competência para investigar, como é o caso das Secretarias de Fazenda, efetuaram compras dessas ferramentas intrusivas. Para Raquel, atualmente as ferramentas de extração de dados em massa dominam as secretarias estaduais, órgãos estaduais e estão presentes em todos os Estados federativos, inclusive órgãos que, a princípio, não teriam competência investigativa. Entre as ferramentas, destacamos o avanço da empresa israelense Cellebrite, que desenvolve um software responsável por extração de dados em massa[525].

---

[523]NSO Group. NSO Group develops best-in-class technology to help government agencies detect and prevent terrorism and crime. Our products help licensed government intelligence and law-enforcement agencies lawfully address the most dangerous issues in today's world. NSO's technology has helped prevent terrorism, break up criminal operations, find missing persons, and assist search and rescue teams. Disponível em: https://www.nsogroup.com/. Acesso em 13 de set. 2024.

[524]*Ibid.*

[525]UOL. PF usa "maleta espiã" para invadir celulares em casos que vão de Lava Jato a pedofilia. Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2017/08/17/pf-usa-maleta-espia-para-invadir-celulares-em-casos-que-vao-de-lava-jato-a-pedofilia.htm. Acesso em 13 de set. 2024.

No ato da Audiência Pública, um dos representantes da Polícia Federal confirmou que em pelo menos um Estado da Federação utiliza ou utilizou a ferramenta FirstMile, que explora vulnerabilidades no sistema de telecomunicações, para providenciar dados geográficos[526]. Com esse software é possível saber a posição de uma pessoa a partir da comunicação do aparelho de telefone celular com antenas de telecomunicação. O FirstMile ficou conhecido no caso denominado "abin pararela", onde jornalistas, autoridades e Ministros do STF foram monitorados.

Ainda de acordo com levantamento do Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.REC)[527], os Ministérios Públicos de 18 Estados contrataram ou renovaram a contratação de softwares, na sua maioria para extração de dados. Contrataram ou renovaram serviços desse tipo os MPs do Rio Grande do Sul, Santa Catarina, Mato Grosso, Mato Grosso do Sul, Goiás, Distrito Federal, Rio de Janeiro, São Paulo, Minas Gerais, Rio Grande do Norte, Piauí, Pernambuco, Paraíba, Bahia, Alagoas, Roraima, Amapá e Acre.

A Ordem dos Advogados do Brasil apontou a necessidade de regulação do tema e a ilegalidade dos programas espiões enquanto não houver legislação específica para regulamentar o tema. Laura Schertel Mendes afirmou que se por um lado há um aumento na eficiência das investigações com a utilização desses softwares, de outro esses sistemas possuem um potencial invasivo muito grande[528]. "Estamos a falar de softwares espiões que se infiltram clandestinamente nos sistemas de informações, como computadores e celulares, permitindo acesso a todas as informações armazenadas no aparelho, bem com ações produzidas em tempo real, como mensagens e e-mails digitados, mas não enviados", pontuou Laura.

Embora tenha ocorrido a preocupação com os softwares israelenses, a invasão de privacidade e a violação ao direito fundamental da proteção de dados continuou mesmo após à realização da Audiência Pública no Supremo Tribunal Federal. Em setembro de 2024 foi divulgada uma matéria jornalística onde foi noticiado que um dos mais importantes Sistemas

[526]CNN. FirstMile: como funciona o software espião que teria sido usado pela Abin de Ramagem Disponível em: https://www.cnnbrasil.com.br/politica/firstmile-como-funciona-o-software-espiao-que-teria-sido-usado-pela-abin-de-ramagem/. Acesso em 13 de set. 2024.
[527]*Ibid.*
[528]*Ibid.*

de Dados da Segurança Pública havia sido utilizado de forma ilegal para acessar dados do Ministro do STF Alexandre de Moraes e de Delegados da Polícia Federal[529].

Foram identificados acessos de 25 agentes públicos ao Infoseg, rede nacional que integra informações dos órgãos de Segurança Pública, Justiça e de Fiscalização em todo o País, provendo dados de pessoas com inquéritos, processos, mandados de prisão, além de dados de veículos, condutores e armas[530]. A Rede INFOSEG disponibiliza informações dos seguintes órgãos: Polícias Civis; Polícias Militares; Departamento Nacional de Trânsito; Exército Brasileiro; Superior Tribunal de Justiça e Justiça Federal. Departamento de Polícia Rodoviária Federal; Departamento de Polícia Federal; Secretaria da Receita Federal; SENASP (Projeto Fronteiras); Tribunais de Justiça Estaduais; Superior Tribunal de Justiça e Justiça Federal.

O Córtex, plataforma de monitoramento utilizada pelo Ministério da Justiça, também foi alvo de denúncias por possível abuso no acesso a dados pessoais[531]. O Córtex é uma ferramenta de inteligência mantida pelo Ministério da Justiça e Segurança Pública, que permite fazer o monitoramento em tempo real de pessoas e veículos nas ruas de diversos municípios e rodovias em todo o país, sem que seja necessária uma motivação prévia para a realização da consulta, o que dispensa autorização judicial e instauração prévia de inquérito policial.

Dados obtidos através da Lei de Acesso à Informação demonstraram que 55 mil usuários civis e militares possuem acesso ao sistema em mais de 180 órgãos públicos no país, através do acompanhamento, em tempo real, de mais de trinta e cinco mil câmeras espalhadas em pontos estratégicos de todo o Brasil[532]. O Ministério da Justiça reconheceu que os usuários não estão obrigados a explicar o motivo da escolha dos seus alvos, sob a alegação de que as consultas são efetuadas para fins de segurança pública[533].

---

[529]UOL. Disponível em: https://noticias.uol.com.br/colunas/leticia-casado/2024/09/11/exposed-moraes-x.htm. Acesso em 13 de set. 2024.
[530]Conselho Nacional de Justiça. Infoseg. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2011/02/infoseg.pdf. Acesso em 13 de set. 2024.
[531]Uol. Programa do Ministério da Justiça admite monitorar 'alvo' sem justificativa. Disponível em: https://noticias.uol.com.br/ultimas-noticias/agencia-publica/2024/10/09/programa-do-mj-permite-monitorar-alvos-sem-justificativa.htm. Acesso em 14 de out. 2024.
[532]Agência Pública. Com milhares de usuários civis e militares, sistema Córtex do Ministério da Justiça explodiu desde o governo Bolsonaro. Disponível em: https://apublica.org/2024/10/vigilancia-55-mil-agentes-podem-monitorar-alvos-sem-justificativa/. Acesso em 14 de out. 2024.
[533]*Ibid.*

Embora o Ministério da Justiça tenha se recusado a informar quantas pessoas haviam sido monitoradas pelo Córtex, através da Lei de Acesso à Informação foi possível aferir que entre janeiro de 2019 e janeiro de 2022 mais de 360 mil alvos haviam sido identificados através da plataforma. O maior problema dos sistemas que acessam dados pessoais dos cidadãos é justamente a falta de um mecanismo que faça o controle do acesso a essas informações. Embora a Portaria que regulamenta o uso do Córtex exija que os órgãos com acesso realizem auditorias e enviem relatórios mensais sobre o uso, apenas 62 relatórios de auditorias foram registrados nos quatro anos de uso do sistema.

Ainda em setembro de 2024, o Supremo Tribunal Federal validou norma que autorizou o Ministério Público e a Polícia a requisitar dados cadastrais de investigados em empresas de telefonia, sem que haja a necessidade de autorização judicial[534]. Nesse caso, as informações foram restritas aos dados de qualificação pessoal, filiação e endereço das pessoas investigadas. A decisão foi tomada no julgamento da Ação Direta de Inconstitucionalidade (ADI) 4906. A ação foi movida pela Associação Brasileira de Concessionárias de Serviço Telefônico Fixo Comutado (Abrafix), contra o Artigo 17-B da Lei de Lavagem de Dinheiro (Lei 9.613/1998), inserida pela Lei 12.683/2012. O dispositivo em questão estabelece que autoridades policiais e o Ministério Público podem ter acesso a dados cadastrais de investigados, como filiação, endereço e qualificação pessoal mantidos por empresas de telefonia, sem a necessidade de ordem judicial.

O Relator da ADI, Ministro Nunes Marques, entendeu que o referido dispositivo questionado é constitucional, porque os dados previstos na lei são de caráter objetivo, fornecidos pelo próprio usuário ao assinar um serviço com a empresa telefônica, o que os afastaria eventual proteção de sigilo. Afirmou que "os dados cadastrais não estão protegidos pelo sigilo. Logo, seu compartilhamento com órgãos de persecução penal para efeito de investigação criminal independe de autorização da justiça"[535].

O entendimento ora analisado pode auxiliar a compreender o que se debate neste trabalho, que é o acesso aos bancos de dados das Polícias Judiciárias, mais especificamente da Polícia Civil do Distrito Federal, para investigação e eventual prevenção de crimes. O banco de dados, conforme já mencionado em outras partes do presente estudo, não é alimentado de

[534]STF, ADI 4906, Tribunal Pleno, Rel. Min. Nunes Marques, J. 12.09.2024, DJe 24.10.2024.
[535]*Ibid.*

maneira obscura, já que os dados são fornecidos pelo próprio usuário que procura um posto de identificação para confeccionar uma cédula de identidade ou uma delegacia de polícia para confecção de registro de ocorrência policial.

O problema, portando, não é o acesso aos dados pessoais para fins penais, mas a forma como os dados são utilizados e a existência ou não de um mecanismo que controle o acesso aos dados. Apenas a título de exemplo, a Polícia Federal e o Ministério da Justiça e Segurança Pública implementaram um Programa denominado Brasil Mais[536]. O Programa está sendo utilizado para o monitoramento de crimes ambientais, através do acesso gratuito a imagens de satélites de alta resolução.

O objetivo do projeto foi auxiliar órgãos públicos na resposta a desastres naturais, fornecendo informações precisas e atualizadas sobre áreas afetadas por queimadas. A ferramenta desenvolvida produz imagens diárias e alerta de cicatriz de queimadas e focos de incêndios, o que pode contribuir para o planejamento no combate aos desastres ambientais. Dois pontos, no entanto, merecem destaque nesse Programa e podem ser utilizados na implementação de eventual política pública para a utilização e o monitoramento da utilização de dados pessoais nas Polícias Judiciárias Brasileiras.

O primeiro ponto diz respeito à capacitação dos usuários. No site do Programa Brasil Mais, há um link onde o usuário que se cadastra para ter acesso às imagens de satélite possui cursos na modalidade EAD, o que permite aperfeiçoamento nas investigações e operações. Na plataforma os cursos são organizados por tema, onde são disponibilizados vídeos, apresentações, aulas gravadas, documentos técnicos e cases de diferentes aplicações. O segundo ponto relevante é a utilização de uma ferramenta indicadora de uso e de resultados, que faz uma apuração mensal dos indicadores de uso e resultados do Programa Brasil Mais, o que também pode ser utilizado como modelo para a utilização dos bancos de dados das Polícias Judiciárias brasileiras para fins penais.

[536]Ministério da Justiça e Segurança Pública. Programa Brasil Mais, do MJSP, permite acesso a imagens de satélite para auxiliar no combate às queimadas no Pantanal. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/programa-brasil-mais-do-mjsp-permite-acesso-a-imagens-de-satelite-para-auxiliar-no-combate-as-queimadas-no-pantanal. Acesso em 16 de set. 2024.

Na obra *O Inviolável e o Intocável no Direito Processual Penal: Reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal*, de autoria do alemão Jürgen Wolter[537] e traduzida por Luís Greco, Alaor Leite e Eduardo Viana, foi mencionado que existe uma separação entre a atividade de inteligência, a atividade de polícia preventiva e a atividade repressiva (justiça penal em sentido amplo).

Para o autor alemão, os dados obtidos para fins de inteligência, de prevenção de perigos ou de persecução penal, respectivamente, não podem ter a finalidade alterada, ou seja, os dados de inteligência não podem ser usados pela polícia preventiva, os da polícia preventiva não podem ser usados repressivamente e vice-versa, sem que haja expressa previsão legal[538].

O autor também mencionou que a vinculação à finalidade implica em um dever de renunciar aos dados desnecessários, o que se entende pelo *princípio alemão da evitação de dados ou da economia de dados* (*Datenvermeidung, Datensparsamkeit*). O Estado não pode armazenar dados como se fosse um estoque (*Speicherung auf Vorrat*), sem uma clara determinação da finalidade desse armazenamento, só para tê-los à disposição para qualquer necessidade[539].

Quando a finalidade da utilização dos dados se esgotar, ou porque foi alcançada ou porque não poderá mais ser alcançada, surge um imperativo de apagamento (*Löschung*) dos dados, que poderá ser limitado para que seja permitido um controle judicial. Por fim, conclui dizendo que a vinculação à finalidade, conjugada à separação entre inteligência, polícia e justiça significa também que:

> É inadmissível uma base de dados comum a todos os órgãos estatais. Toda tentativa de enxergar a administração pública como uma unidade informacional é incompatível com uma proteção eficiente de dados. Se saber é poder, o Estado não pode saber tudo, porque um Estado que tem conhecimentos ilimitados tem também um poder ilimitado. O direito de proteção de dados, que começa como direito subjetivo, mostra-se, ao mesmo em boa parte, como garantia institucional, relativa à própria estrutura da sociedade e do Estado. Nesse nível macro, o direito se transforma em uma

[537]WOLTER, Jürgen. O Inviolável e o Intocável no Direito Processual Penal: Reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. Organizada e traduzida por Luís Greco. Tradução: Alaor Leite e Eduardo Viana. 1ª edição. São Paulo: Marcial Pons, 2018.
[538]*Ibid.*
[539]*Ibid.*

> exigência de *separação informacional de poderes*, um dos temas centrais da obra de Wolter. No Brasil, na contra mão desses princípios, vejo com preocupação enquanto escrevo as presentes linhas que o Senado acaba de aprovar um Sistema Único de Segurança Pública (PLC 19/2018), que eleva a integração de informações de inteligência e de segurança obtidas por autoridades dos mais diversos níveis (polícias, bombeiros, órgãos penitenciários, agentes de trânsito etc., federais, estaduais e municipais) a uma de suas bandeiras centrais. O fato de que esses esforços não tenham provocado um escândalo público é a prova da urgência de uma reflexão mais aprofundada sobre os princípios que acabo de expor[540].

Sobre esse ponto de vista, é preciso que sejam feitas algumas observações. A tradução da obra alemã, que foi escrita nos anos 90, demonstra a preocupação dos europeus com a questão da proteção de dados pessoais e com o poder do Estado no armazenamento dos dados. Embora uma grande parte dos países da Europa seja considera berço do reconhecimento à proteção de dados pessoais, é preciso reconhecer o abismo que existe entre esses países e o Brasil. Conforme o Índice Global da Paz, a Alemanha foi considerada um dos países mais seguros do mundo[541]. Apesar disso, estudos comprovam que mesmo sendo um dos países mais seguros, a criminalidade na Alemanha aumenta a cada ano[542].

7.2 Utilização dos Dados Armazenados como Forma Prevenção e Combate ao Crime

Em alguns Estados Brasileiros, as Polícias Judiciárias vão muito além do registro de ocorrência policial para a apuração de crimes. Geralmente, essas instituições emitem cédulas de identidade e registram fatos não criminosos, como o acidente de trânsito sem vítima e o extravio. Todas as informações, alimentam os bancos de dados das polícias, o que auxilia na prevenção e no combate à prática de diversos delitos.

No início dos anos 2000, algumas Polícias Judiciárias Brasileiras começaram a informatizar os seus bancos de dados. No ano de 1999, conforme será possível aferir adiante, a Polícia Civil do Distrito Federal, por exemplo, passou a utilizar um sistema denominado *Millenium*, para que os servidores deixassem de utilizar o papel e passassem a utilizar o

---

[540] *Ibid.*

[541] Perfil da Alemanha. Segurança na Alemanha. Disponível em: https://www.tatsachen-ueber-deutschland.de/pt-br/vida-na-alemanha/seguranca-na-alemanha#:~:text=A%20Alemanha%20tem%20taxas%20comparativamente,est%C3%A3o%20conectadas%20em%20redes%20internacionais. Acesso em 23 de set. 2024.

[542] Isto é. Alemanha tem maior número de crimes violentos em 15 anos. Disponível em: https://istoedinheiro.com.br/alemanha-tem-maior-numero-de-crimes-violentos-em-15-anos/. Acessado em 23 de set. 2024.

computador. Com base nisso, qualquer consulta feita nos dias de hoje consegue localizar com rapidez e precisão todos os fatos registrados de 1999 até a presente data.

A utilização dos dados, porém, precisa estar amparada pelo Direito Constitucional, conforme já mencionado anteriormente. Isso deve ser feito à luz do entendimento do Supremo Tribunal Federal, que nos últimos anos tem acompanhado o avanço tecnológico e dado uma resposta satisfatória a todas as demandas que surgem com as novas tecnologias. O tema abordado no presente estudo é novo e merece uma reflexão.

Atualmente não há decisões sobre o uso das informações que constam nos bancos de dados das Polícias Judiciárias brasileiras. Conforme foi visto anteriormente, embora seja comum e necessária a autorização judicial para acessos a alguns tipos de informações, não me parece que esse seja o melhor entendimento para acesso aos bancos de dados das polícias, porque a apuração da grande maioria dos crimes necessita de uma atuação imediata e eficaz.

Com o intuito de aferir o nível de proteção de dados pessoais na Polícia Civil do Distrito Federal, foram feitas algumas perguntas para a Divisão de Controle Interno e a Divisão de Tecnologia. As indagações foram feitas com base na Lei de Acesso à Informação, através do site Participa DF[543], da seguinte forma:

1) A Polícia Civil do Distrito Federal adota ações para garantir que o tratamento de dados esteja de acordo com a Lei Geral de Proteção de Dados?
2) Caso afirmativo, qual a finalidade da Polícia Civil do Distrito Federal, ao tratar os Dados Pessoais?
3) Por quanto tempo a Polícia Civil do Distrito Federal armazena os Dados Pessoais?
4) A partir de que ano os Dados Pessoais foram inseridos nos sistemas informatizados da Polícia Civil do Distrito Federal?
5) Em que ano a Polícia Civil do Distrito Federal passou a ter acesso ao Prontuário de Identificação Civil informatizado?
6) A partir de que ano as cédulas de identidade passaram a ser emitidas pela Polícia Civil do Distrito Federal?
7) Os servidores administrativos da Polícia Civil do Distrito Federal possuem acesso ao Prontuário de Identificação Civil e ao Sistema onde são registradas as Ocorrências Policiais?
8) Existe algum setor que faça o monitoramento diário, semanal, quinzenal ou mensal dos acessos feitos aos sistemas que armazenam Dados Pessoais?
9) Os Dados Pessoais armazenados pela Polícia Civil do Distrito Federal são compartilhados com outros órgãos públicos?
10) A Polícia Civil do Distrito Federal implementa medidas de segurança da informação para a proteção de Dados Pessoais?

[543]Governo do Distrito Federal. Participa DF. Disponível em: https://www.participa.df.gov.br/. Acessado em 27 de mai. 2024.

11) A Polícia Civil do Distrito Federal já sofreu algum incidente de vazamento de Dados Pessoais? Se sim, como a Polícia Civil do Distrito Federal atuou diante desse incidente? A Polícia Civil do Distrito Federal possui algum protocolo para atuar em caso de eventuais incidentes de vazamento de Dados Pessoais?
12) Atualmente, o titular de Dados Pessoais pode consultar suas informações nos bancos de dados da Polícia Civil do Distrito Federal?
13) Esse titular mencionado acima pode solicitar a exclusão de algum Dado Pessoal?
14) Existe na Polícia Civil do Distrito Federal algum DPO (Encarregado)?
15) Como o titular de Dados Pessoais pode entrar em contato com o DPO?
16) Existe alguma finalidade específica, para a utilização dos Dados Pessoais que são captados pela Polícia Civil do Distrito Federal?
17) A Polícia Civil do Distrito Federal participou do grupo de trabalho que elaborou o Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal?
18) A Divisão de Controle de Denúncias Anônimas adota ações para garantir que o tratamento de dados esteja de acordo com a Lei Geral de Proteção de Dados?
19) Conforme divulgado pela própria Polícia Civil do Distrito Federal, o anonimato é garantido para o cidadão que faz uma Denúncia Anônima. Caso o Denunciante queira se identificar, como é feito o tratamento desses Dados?
20) Caso o Denunciante se sinta ameaçado diante do vazamento de seus Dados Pessoais após a confecção da Denúncia Anônima, existe algum canal específico para comunicação desse fato?
21) É possível que o Denunciante entre em contato com a Divisão de Controle de Denúncias Anônimas para solicitar a exclusão dos seus dados pessoais? (Exemplo: número te telefone registrado no ato da comunicação da denúncia anônima ou gravação do áudio com a ligação que originou a denúncia);
22) A Polícia Civil do Distrito Federal possui algum convênio/acordo, para que outros órgãos acessem seus sistemas?
23) Caso positivo, quais são os órgãos que firmaram esse acordo com a PCDF?
24) Quais sistemas da PCDF esses órgãos podem acessar?
25) Esses acordos também permitem que a PCDF tenha acesso aos sistemas dos órgãos mencionados acima?
26) Gostaria de solicitar uma cópia da resolução número 39 de 02 de julho de 2024, publicada no dia 18 de julho de 2024, no Boletim Interno da PCDF. A referida resolução aprova a norma de classificação da informação no âmbito da Polícia Civil do Distrito Federal. Desde já, agradeço;
27) Visando instruir minha tese de Doutorado em Direito Constitucional, gostaria, por gentileza, de ter acesso ao Glossário de Segurança da Informação instituído no âmbito da PCDF.
28) Quando um celular é apreendido como evidência, é necessário realizar uma perícia para extrair informações relevantes, como mensagens de texto, registros de chamadas, fotos e vídeos. Os dados extraídos desses telefones celulares são descartados após o laudo pericial ser incluído no inquérito policial? Ou esses dados continuam armazenados em algum sistema específico do Instituto de Criminalística da PCDF, para eventual futura utilização? Caso fiquem armazenados, existe algum prazo para isso?
29) Bom dia.
30) Visando instruir minha tese de Doutorado, gostaria de solicitar a NORMA DE SEGURANÇA DA INFORMAÇÃO DE GESTÃO DE COMPUTAÇÃO EM NUVEM POLÍCIA CIVIL DO DISTRITO FEDERAL, publicada no boletim interno do dia 19 DE JULHO DE 2024. Obrigado.

Conforme será visto a seguir, o primeiro sistema de coleta de dados da Polícia Civil do Distrito Federal se chamava SIOCOP e foi instituído em 1991. Dessa data para os dias de hoje, o avanço da tecnologia aperfeiçoou a forma de captação de armazenamento dos dados. Sobre a utilização desses dados, o Departamento de Tecnologia da PCDF (DITEC) informou que os

sistemas possuem um controle de acesso e permissionamento, possibilitando que cada usuário acesse as informações que são necessárias para a execução de suas atividades laborais dentro de sua função.

Atualmente, existem na Polícia Civil do DF os servidores de carreira e os servidores administrativos, que também possuem acesso ao sistemas. Sobre os servidores públicos administrativos, a DITEC esclareceu que muitas funções dos servidores públicos administrativos exigem responsabilidades e obrigações impostas por lei. Para processar pedidos e requerimentos de documentos, por exemplo, os servidores administrativos precisam verificar a identidade, renda e outras informações pertinentes. Além disso, o acesso a dados pessoais permite que os servidores verifiquem a autenticidade das informações fornecidas e, assim, evitem fraudes que podem resultar em perdas financeiras para o Estado.

Sobre a indagação a respeito do monitoramento do acesso a esses dados, a DITEC esclareceu que não teria como prestar o esclarecimento, porque na Divisão de Tecnologia o monitoramento vai além dos dados pessoais propriamente ditos, tendo em vista que o nível de monitoramento está relacionado à segurança dos dados de forma mais generalista. Mesmo sem a existência de uma lei que regule a proteção de dados na esfera penal, a DITEC entende que a Lei Geral de Proteção de Dados estabelece regras sobre o tratamento de dados pessoais, incluindo o seu armazenamento, processamento e transferência por entidades públicas e privadas. O encargo de monitorar os acessos a sistemas que armazenam dados pessoais, bem como garantir a segurança dos dados, frequentemente recai sobre o “encarregado” ou “DPO”. Entretanto, a Divisão de Tecnologia ressaltou que a Lei Geral de Proteção de Dados não especifica a frequência (diária, semanal ou quinzenal) com que os acessos aos sistemas devem ser monitorados.

A determinação da frequência de monitoramento pode depender da natureza do sistema, da sensibilidade dos dados armazenados e das práticas internas da organização, bem como das diretrizes e regulamentações subsequentes da ANPD. Por fim, a DITEC esclareceu que a LGPD enfatiza a necessidade de adotar medidas de segurança, práticas e processos organizacionais que garantam a proteção de dados. Isso pode incluir o monitoramento regular dos acessos, a realização de auditorias e a verificação de possíveis vulnerabilidades nos sistemas.

Por fim, foi indagado à referida Divisão se a Polícia Civil do Distrito Federal já havia sofrido algum incidente de vazamento de dados pessoais e como a instituição age diante de eventual incidente de vazamento de dados pessoais, bem como se existe algum protocolo que deve ser seguido. Como reposta, mencionaram que em caso de eventual incidente, a Divisão de Tecnologia informa ao Gestor de Segurança da Informação e ao Encarregado Setorial, ambos nomeados pela instituição, cabendo aos dois a comunicação ao Encarregado Central e aos titulares dos dados pessoais, para que a organização (controlador) tome as medidas necessárias para conter o incidente, investigar a causa e evitar recorrências, mitigando os impactos para os titulares afetados.

A Divisão de Controle da PCDF também respondeu aos questionamentos mencionados acima, informando que a Polícia Civil do Distrito Federal adota ações para garantir que os dados tratados estejam de acordo com a Lei Geral de Proteção de Dados e que já havia contratado uma empresa especializada para esse fim. Dentre as ações já realizadas, estão o mapeamento de entrada e tratamento de dados pessoas, o mapeamento dos riscos do tratamento, o relatório de impacto da proteção de dados pessoais, a criação da política de proteção de dados pessoais, política de cookies, termo de sigilo, gerenciamento dos pedidos dos titulares e dos órgãos, gerenciamento de violações e notificações, nomeação do DPO e evento de conscientização sobre proteção de dados pessoais.

Sobre a finalidade do tratamento de dados pela Polícia Civil do Distrito Federal, foi respondido que essa instituição realiza o tratamento de dados pessoais única e exclusivamente para o atendimento de sua finalidade pública, na persecução do interesse público, e com o objetivo de executar as suas competências legais e cumprir com as atribuições legais que lhe foram conferidas. No que diz respeito ao tempo do armazenamento de dados pela PCDF, foi respondido que a Polícia Civil do Distrito Federal não definiu prazo para o armazenamento dos dados pessoais.

Sobre a questão do titular de dados pessoais poder consultar suas informações nos bancos de dados da Polícia Civil do Distrito Federal, foi respondido que o requerente titular de dados pessoais ou seu representante legal podem consultar suas informações nos bancos de dados da PCDF da seguinte forma: realizar uma solicitação pela Ouvidoria do GDF, que deve ser direcionada ao tratamento de dados pessoais/ Lei Geral de Proteção de Dados Pessoais (LGPD) ou presencialmente na Ouvidoria especializada da PCDF. Na solicitação deverão

conter as informações necessárias para embasar o atendimento da manifestação solicitada pelo titular.

Sobre a possibilidade de o titular solicitar a exclusão dos seus dados pessoais dos sistemas da PCDF, foi esclarecido que de acordo com as normas internas da Polícia Civil do Distrito Federal, o titular de dados pessoais pode solicitar, a qualquer tempo, a eliminação de dados, conforme previsto no Artigo 5º, XIV da Lei Geral de Proteção de Dados. O encarregado receberá a solicitação, verificará se os pressupostos iniciais (confirmação da existência de tratamento, legitimidade e competência) foram atendidos e se há alguma obrigação legal, legítimo gerenciamento dos pedidos dos titulares e dos órgãos interesse do controlador ou outro motivo regulatório que impeça a eliminação dos dados pessoais do titular.

Por fim, foi frisado que caso seja possível realizar a eliminação de dados, o Encarregado demandará às áreas detentoras das informações, para realizarem a efetiva eliminação dos dados pessoais do titular. Caso não seja possível tratar a solicitação ou eliminar os dados solicitados, o Encarregado enviará ao titular resposta à solicitação contendo justificativa para não atender a demanda. Percebe-se, portanto, que a Polícia Civil do Distrito Federal já está alinhada com a Lei Geral de Proteção de Dados, demonstrando a importância da análise do tratamento de dados pessoais no direito penal. Percebe-se o comprometimento da instituição com a recepção da LGPD e dos seus princípios, o que será de fundamental importância para eventual implementação do tema em questão, que é a proteção de dados na persecução penal.

As respostas fornecidas no anexo deste trabalho demonstram um elevado nível de comprometimento da Polícia Civil do Distrito Federal no sentido de cumprir o que foi estabelecido na Lei Geral de Proteção de Dados, ainda que não exista uma legislação específica para o tratamento de dados pessoais na espera penal e processual penal.

Outra iniciativa vinculada ao campo da Segurança da Informação na Polícia Civil do Distrito Federal foi a aprovação do Regimento Interno do Comitê Gestor de Segurança da Informação e Comunicação no âmbito da PCDF. Esse Regimento, publicado através da Portaria número 60, de 03 de julho de 2020, implementou o referido comitê, de natureza consultiva e deliberativa, cuja finalidade é deliberar sobre políticas, estratégias, diretrizes e processos relacionados à segurança da informação e gestão de riscos de tecnologia da informação e

comunicação, promovendo a proteção do ativo institucional segundo boas práticas de segurança da informação.

Esse foi um passo muito importante, porque a Polícia Civil do Distrito Federal passou a dar mais atenção às Normas de Segurança da Informação, que, conforme será visto adiante, passaram a ser aplicadas a todos os servidores, colaboradores e prestadores de serviço que atuem nas unidades da estrutura organizacional da PCDF, bem como a qualquer outra pessoa que execute atividades no ciclo de vida da informação no ambiente da PCDF[544].

Todas as Resoluções mencionadas acima demonstram compromisso e comprometimento da Polícia Civil do Distrito Federal com a proteção de dados pessoais e com e com o Marco Civil da Internet. Das Normas implementadas pela PCDF, talvez a mais relevante para o trabalho em questão seja a Portaria número 224, de 30 de junho de 2023, que instituí a *Política de Privacidade no Âmbito da Polícia Civil do Distrito Federal*.

Na Portaria, a PCDF aborda a questão da Política de Privacidade, definindo os conceitos de agentes de tratamento, anonimização, autoridade nacional, banco de dados, consentimento,

[544]A Polícia Civil do Distrito Federal aprovou as seguintes Normas no âmbito da Segurança da Informação: RESOLUÇÃO Nº 03/2022 - Aprova a Norma de Segurança da Informação de Gestão de Segurança da Informação no âmbito da Polícia Civil do Distrito Federal; RESOLUÇÃO Nº 04/2022 - Aprova a Norma de Segurança da Informação de Segurança Física e do Ambiente no âmbito da Polícia Civil do Distrito Federal; RESOLUÇÃO Nº 05/2022 - Aprova a Norma de Segurança da Informação de Gestão de Incidentes em Segurança da Informação no âmbito da Polícia Civil do Distrito Federal; RESOLUÇÃO Nº 06/2022 - Aprova a Norma de Segurança da Informação e Gestão de Ativos no âmbito da Polícia Civil do Distrito Federal; RESOLUÇÃO Nº 07/2022 - Aprova a Norma de Segurança da Informação de Armazenamento e Descarte de Ativos no âmbito da Polícia Civil do Distrito Federal; RESOLUÇÃO Nº 08/2022 - Aprova a Norma de Segurança da Informação de Gestão no Uso dos Recursos Computacionais no âmbito da Polícia Civil do Distrito Federal; RESOLUÇÃO Nº 09/2022 - Aprova a Norma de Segurança da Informação de Controle de Acesso Lógico no âmbito da Polícia Civil do Distrito Federal; RESOLUÇÃO Nº 10/2022 - Aprova a Norma de Segurança da Informação de Gestão de Riscos de Segurança da Informação no âmbito da Polícia Civil do Distrito Federal; RESOLUÇÃO N° 11/2022 - Aprova a Norma de Segurança da Informação de Gestão de Continuidade de negócios no âmbito da Polícia Civil do Distrito Federal; RESOLUÇÃO Nº 12/2022 - Aprova a Norma de Segurança da Informação de Auditoria de Conformidade no âmbito da Polícia Civil do Distrito Federal; RESOLUÇÃO Nº 13/2022 - Aprova a Norma de Segurança da Informação de Desenvolvimento Seguro de Sistemas no âmbito da Polícia Civil do Distrito Federal; RESOLUÇÃO Nº 14/2022 - Aprova a Norma de Segurança da Informação de Controle de Documentos de Segurança da Informação no âmbito da Polícia Civil do Distrito Federal; RESOLUÇÃO N° 15/2022 - Aprova a Norma de Segurança da Informação de Mesa Limpa e Tela Limpa no âmbito da Polícia Civil do Distrito Federal; RESOLUÇÃO Nº 16/2022 - Aprova a Norma de Segurança da Informação de Backup e Retenção de Registros no âmbito da Polícia Civil do Distrito Federal; RESOLUÇÃO Nº 17/2022 - Aprova a Norma de Segurança da Informação de Uso de Controles Criptográficos e de Chaves Criptográficas no âmbito da Polícia Civil do Distrito Federal; RESOLUÇÃO Nº 18/2022 - Aprova a Norma de Segurança da Informação de Gestão de Computação em Nuvem no âmbito da Polícia Civil do Distrito Federal.

controlador, dado anonimizado, dado pessoal, dado pessoal sensível, encarregado, operador, órgãos de pesquisa, titular, transferência internacional de dados, tratamento e uso compartilhado de dados.

O que mais chamou atenção foi fato de constar na referida Portaria que os tratamentos de dados realizados pela Polícia Civil do Distrito Federal utilizam como base os Artigos 7º, incisos II, III, IV, V e IX, e 11, Inciso II, Alíneas "a", "b", e "c" da Lei Geral de Proteção de Dados. Consta nos referidos dispositivos que:

> Artigo 7º. O tratamento de dados pessoais somente será realizado nas seguintes hipóteses:
> II – Para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III – Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV – Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V – Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular de dados;
> IX – Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
> Artigo 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> II – Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) Cumprimento de obrigação legal ou regulatória pelo controlador;
> b) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) Realização de estudos por órgão de pesquisa, garantia, sempre que possível, a anonimização dos dados pessoais sensíveis.

Significa dizer que o cidadão, na qualidade de titular dos dados pessoais, mediante solicitação prévia, terá direito de obter da Polícia Civil do Distrito Federal informações sobre os seus dados, desde que não estejam vinculados à atividade fim. Os titulares de dados terão direito às informações sobre a existência de dados pessoais sob sua titularidade tratados pela PCDF, acesso aos dados pessoais sob tratamento, correção de dados pessoais incompletos, inexatos ou desatualizados e anonimização ou cessação do tratamento de dados desnecessários, excessivos ou desconforme, desde que as informações não estejam relacionadas a investigações criminais.

Fora do contexto de dados pessoais no âmbito da atividade fim, os dados pessoais tratados pela Polícia Civil do Distrito Federal são: nome completo, data de nascimento, sexo, número de inscrição no CPF, endereço de e-mail, número de telefone, localização do usuário e foto do usuário. Alguns recursos ou informações podem ser solicitados pelas aplicações e notificados por meio do sistema operacional do dispositivo móvel do titular dos dados pessoais, quando necessários para utilização dos serviços pela primeira vez ou mesmo na instalação, como por exemplo acesso à rede de internet móvel ou WiFi, acesso à identificação de dispositivo ou acesso à câmeras e fotos, mídia e arquivos de áudios e vídeo de seu aparelho.

A prática de armazenamento de dados pessoais é comum e se tornou uma realidade presente em diversos setores. Quando entramos pela primeira vez em um prédio, seja público ou privado, é comum que nos solicitem o documento de identidade. Para compramos uma passagem de avião, o mesmo acontece. Bancos, operadoras de telefone, prestadoras de serviços públicos, nossos dados estão em todos os lugares. O fato de a prática de coleta de dados estar em todos os lugares, demonstra que não há problema que a mesma coleta de dados seja feita pelas Polícias Judiciárias brasileiras.

Retornando às indagações feitas à PCDF, através da Lei de Acesso à Informação, na pergunta número 26 foi solicitada, através da Lei de Acesso à Informação, uma cópia da resolução número 39 de 02 de julho de 2024, publicada no dia 18 de julho de 2024, do Boletim Interno da PCDF, que aprovou a norma de classificação da informação no âmbito da Polícia Civil do Distrito Federal.

A Norma de Classificação da Informação se aplica a toda documentação, produzida ou recebida, em tramitação na Polícia Civil do Distrito Federal, bem como a todos os servidores, prestadores de serviços, parceiros estratégicos e fornecedores que utilizam os recursos computacionais e as instalações da PCDF, em caráter permanente ou temporário, visando a segurança e privacidade da informação e da comunicação.

A Resolução foi pautada na Instrução Normativa GSIPR número 01, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal. A norma ABNT NBR ISO/IEC 27001/2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização, a norma

ABNT NBR ISSO/IEC 27002/2013, documento que tem por finalidade orientar organizações na implementação de controles de segurança da informação, e a norma NBR ISSO/IEC 27701/2019, extensão da ABNT NBR ISSO/IEC 27001/2013, que em conjunto com a ABNT NBR ISSO/IEC 27002/2013, estabelecem requisitos e diretrizes para a gestão da privacidade da informação.

Além das normas mencionadas acima, a Resolução levou em consideração o que dispõe as seguintes legislações: Norma Complementar número 10/IN01/DSIC/GSIPR, que estabelece diretrizes pra o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública direta e indireta, Norma Complementar número 11/IN01/DSIC/GSIPR, que estabelece diretrizes para a avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal direta e indireta, Norma Complementar número 19/IN01/DSIC/GSIPR, que estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal, direta e indireta, Norma Complementar número 20/IN01/DSIC/GSIPR, que estabelece as diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento de Informação nos órgãos e entidades da Administração Pública Federal direta e indireta, Lei Federal número 12.527/2011, que regula o acesso à informações, Lei Federal número 13.709/20128 (Lei Geral de Proteção de Dados Pessoais) e Lei Distrital número 4.990/2012, que regula o acesso a informações no âmbito do Distrito Federal.

Sobre a diretriz geral da Norma de Classificação da Informação, a Polícia Civil do Distrito Federal adotou como preceito geral a publicidade e como exceção o sigilo. A informação no âmbito da PCDF pode ser definida como ultrassecreta, secreta ou reservada. O prazo de restrição de acesso à essas informações começarão a valer a partir da data de sua produção e terão um prazo de 25 anos para informações ultrassecretas, 15 anos para informações secretas e 05 anos para informações reservadas.

Caso as informações possam colocar em risco a segurança do Presidente e do Vice-Presidente da República, do Governador e do Vice-Governador do Distrito Federal, do Delegado-Geral e do Delegado-Geral Adjunto da PCDF e dos respectivos cônjuges ou descendentes, são classificadas como reservadas e ficam sob sigilo até o término do mandato em exercício ou do último mandato, em caso de reeleição. A classificação da informação para

esses graus de sigilos observará o interesse público, onde deverá ser levada em consideração a gravidade do risco ou dano à segurança da sociedade e do Estado e o prazo máximo de restrição ou evento que defina o seu termo final.

Como penalidade, o servidor que desrespeitar ou violar os termos da Resolução, poderá ser suspenso de forma temporária ou permanente, o que influenciará nas autorizações de acesso aos recursos disponíveis. Além disso, existe a possibilidade de aplicação de penas e sanções administrativas determinadas pela PCDF, sem prejuízo da aplicação de medidas penais e/ou cíveis previstas em Lei.

Vários pontos da Resolução são relevantes para demonstrar que a Polícia Civil do Distrito Federal já pode se planejar para implementar políticas públicas de monitoramento da utilização dos seus bancos de dados para fins penais. No Plano Diretor de Segurança da Informação 2022-2023, o Comitê de Segurança da Informação e Comunicação – CGSIC, estabeleceu como plano de metas e ações de segurança da informação assegurar às pessoas que a polícia de segurança da informação da PCDF seja efetiva no tratamento e salvaguarda de seus dados.

Na apresentação do Plano Diretor de Segurança da Informação da PCDF, foi mencionado que com a recorrente demanda por adaptações de acessos e perfis aos ativos institucionais para usuários de órgãos externos atuantes junto a atividade policial, diversos questionamentos foram levantados quando a segurança da informação aplicada na Polícia Civil do Distrito Federal.

As metodologias utilizadas no desenvolvimento do Plano Diretor de Segurança da Informação – PDSI foram baseadas no modelo do Plano Diretor de Tecnologia da Informação, que é um instrumento de diagnóstico de planejamento e gestão dos recursos e processos de tecnologia da informação, cujo principal objetivo é o atendimento às necessidades finalísticas e de informação de um órgão ou entidade para um determinado período.

As necessidades de segurança da informação foram definidas com base no diagnóstico da situação atual de segurança da informação da Polícia Civil do Distrito Federal. Por esse motivo, para a realização do diagnóstico da situação atual de Segurança da Informação na

PCDF foi utilizada a matriz SWOT[545]. Foram identificados os pontos fortes, pontos fracos, as oportunidades e ameaças com a implantação e a implementação do Plano Diretor de Segurança da Informação.

Chegou-se à conclusão de que o cenário encontrado pelos gestores foi o de uma organização que enfrenta o desafio para a formação e formalização de equipe técnica de Segurança da Informação em nível estratégico da estrutura organizacional, devido ao número insuficiente de servidores com conhecimentos técnicos na matéria.

O Plano Diretor de Segurança da Informação (PDSI), portanto, é o documento que direciona a atuação da segurança da informação em âmbito institucional, sendo resultante da estruturação de um processo de planejamento estratégico para a PCDF, alinhado com as metas estabelecidas. O principal intuito do PDSI, portanto, é direcionar os esforços institucionais na manutenção, inovação e melhoria dentro da visão de gestão de riscos, visando a diminuição dos impactos recorrentes de falhas de segurança da informação.

Foi frisado nesse Plano Diretor de Segurança da Informação que a Lei de Acesso à Informação – LAI e a Lei Geral de Proteção de Dados – LGPD trazem diretrizes que, ao mesmo tempo em que a LAI permite o acesso aos dados, a LGPD define que os dados pessoais sensíveis sejam tratados e protegidos contra vazamentos que venham a comprometer seus titulares. A Política de Segurança da Informação da Polícia Civil do Distrito Federal é o instrumento que

[545]SEBRAE. Conheça a Análise SWOT. Se você está pensando em fazer um planejamento estratégico na sua empresa, este artigo vai ajudar nos primeiros passos. Já ouviu falar em Análise SWOT (ou FOFA, na tradução do inglês)? A ferramenta Análise SWOT é uma matriz que identifica as forças (*strengths*), fraquezas (*weaknesses*), oportunidades (*opportunities*) e ameaças (*threats*) de um negócio. Trata-se de uma ferramenta de gestão empresarial que ajuda o empreendedor a entender o seu negócio a partir de uma análise dos ambientes externo e interno, independentemente do porte da empresa. A avaliação dos quatro fatores que compõem a sigla SWOT tem grande importância para o sucesso e crescimento do empreendimento, uma vez que permite traçar um diagnóstico para a definição das metas, estratégias e ações para o negócio. Em outras palavras, a partir da análise, é possível tomar decisões mais acertadas, reduzindo riscos desnecessários. Para fazer a análise SWOT, devem-se seguir os seguintes passos: 1) análise do ambiente interno: identifique forças (diferencial da empresa diante da concorrência, habilidades e competências dos colaboradores, recursos, entre outros) e fraquezas (setores com baixo desempenho, falhas em produtos, serviços e/ou processos, falta de recursos, entre outros); 2) análise do ambiente externo: reconheça as oportunidades (desde aspectos político-econômicos até eventos, novas tecnologias) e as ameaças (concorrentes, novos hábitos de consumo, preços de matéria-prima, para citar algumas). Depois de reunir todas as informações, faça uma análise de todos os dados e pense em estratégias que possam minimizar as ameaças e ajudem a superar as fraquezas, bem como em formas de aproveitar as oportunidades e potencializar as forças. Defina metas e elabore o plano de ação, que deve ser retomado periodicamente, ou seja, não basta ter um plano, é preciso fazer o controle das metas para que os resultados sejam alcançados. Disponível em:https://sebrae.com.br/sites/PortalSebrae/conhecaaanaliseswot,202f64e8feb67810VgnVCM1000001b00320aRCRD. Acesso em 06 de set. 2024.

possibilitará assegurar às pessoas a existência de diretrizes para minimizar os riscos de exposição ou vazamento de dados sob a custódia da PCDF.

A meta da PCDF é o tratamento e a proteção de dados pessoais com todas as diretrizes da Lei Geral de Proteção de Dados. Reforçando que o tratamento não é referente ao tratamento de dados pessoais para a atividade fim da PCDF, que é a investigação de crimes ou, em outras palavras, quando exerce a função de Polícia Judiciária. Na meta mencionada acima está incluída a ação de implementar requisitos para o tratamento dos dados pessoais e sensíveis, bem como a utilização de normas de classificação da informação e a utilização das diretrizes estabelecidas pela LGPD.

Outro ponto relevante no Plano Diretor de Segurança da Informação foi a utilização de um inventário de necessidades, visto como principal insumo para a elaboração de um Plano de Implantação. A par disso, foi realizado um levantamento das ações que devem ser implementadas em um curto, médio e longo prazo e que necessitarão de mecanismos de controles da Segurança da Informação no âmbito da Polícia Civil do Distrito Federal.

Ficou estabelecido que as ações de alto impacto devem ser implementadas em até 06 meses, as ações de médio impacto devem ser implementadas em até 12 meses e as ações de baixo impacto devem ser implementadas acima de 12 meses. No que tange ao tratamento e à salvaguarda no âmbito da PCDF, ficou estabelecido que quatro necessidades seriam de alto impacto e uma necessidade seria de baixo impacto.

As necessidades de alto impacto foram definidas das seguintes formas: modelagem do processo de Gestão de Incidentes; definição e institucionalização dos Integrantes da Equipe de Prevenção, Tratamento e Respostas a Incidentes Mista; publicação de divulgação da ETIR (Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos); criação de painéis para gestão dos indicadores de incidentes. O mapeamento e a modelagem do processo de cadeia de custódia de informação foram definidos como uma necessidade de baixo impacto.

Seguindo uma ordem cronológica sobre a normatização de Segurança da Informação da na Polícia Civil do Distrito Federal, o que inclui o tratamento de dados pessoais, é preciso mencionar a Resolução número 01, de 10 de agosto de 2022. Essa Resolução aprovou a política de Segurança da Informação no âmbito da Polícia Civil do Distrito Federal.

Visando a necessidade de garantir um ambiente tecnológico seguro, de forma a ofertar todas as informações necessárias aos processos estabelecidos na Polícia Civil do Distrito Federal, assegurando confidencialidade, disponibilidade e integridade a informação, o Comitê Gestor de Segurança da Informação e Comunicação da PCDF resolveu aprovar a referida resolução.

A Política de Segurança da Informação da Polícia Civil do Distrito Federal tem como objetivo estabelecer, dentro da estrutura organizacional da PCDF, princípios, diretrizes que visam manter a conformidade com disposições legais vigentes para assegurar a confidencialidade, a disponibilidade e a integridade das informações, conforme já mencionado acima.

A Resolução também estabeleceu que as diretrizes da Segurança da Informação estabelecidas pela Política de Segurança da Informação devem manter alinhamento com o Plano Estratégico Institucional da PCDF. Todos os servidores, colaboradores e prestadores de serviço deverão ser sensibilizados sobre essa Política de Segurança da Informação, bem como sobre suas normas e seus procedimentos complementares, por meio de um plano contínuo de capacitação que possibilite o seu cumprimento dentro e fora da PCDF, com observância dos princípios da legalidade, impessoalidade, eficiência, moralidade, publicidade, motivação, razoabilidade, proporcionalidade e interesse público.

Outro aspecto que deve ser destacado é que a implementação do modelo de Gestão de Segurança da Informação na Polícia Civil do Distrito Federal deve ser realizada por uma equipe técnica composta por servidores capacitados para manter a conformidade com todos os normativos legais, para o acompanhamento e divulgação dos resultados e indicadores do Plano Diretor de Segurança da Informação.

A realização de convênios, visitas técnicas, acordos de cooperação técnicas e outros instrumentos também foi aventada na Resolução, com o intuito de elevar o nível de maturidade do modelo de Gestão e Informação da Polícia Civil do Distrito Federal. Nesses casos, todos os processos de trabalhos e atividades essenciais que incluam processamento de informação devem ser mapeados e modelados para fins de identificação, análise e avaliação e tratamento dos riscos.

Sobre a gestão de incidentes em Segurança da Informação, foi mencionado na Resolução número 01 de 2022 que os incidentes de infraestrutura computacional devem ser solucionados pela Divisão de Tecnologia (DITEC). O Gestor de Segurança da Informação deve definir o modelo de Equipes de Tratamento de Incidentes de Redes – ETIR, que melhor se adeque às necessidades das unidades da PCDF, bem como modelar o processo de gestão de incidentes, mantendo a conformidade com a legislação correspondente.

A referida Resolução trouxe informações significativas e que podem ser utilizadas para o monitoramento do acesso e da utilização de dados pessoais para fins penais. Sobre o uso da internet e dos recursos de tecnologia da informação, consta na Resolução que o acesso à internet no âmbito da PCDF deve ser realizado com a finalidade exclusiva de executar as atividades de interesse público e aquelas desempenhadas pelo órgão, observando sempre a moralidade administrativa.

A Divisão de Tecnologia da PCDF (DITEC), ficou com a missão de monitorar os acessos à internet, os recursos e sistemas de informação dentro das dependências da Polícia Civil do Distrito Federal, bem como bloquear sites que tenham conteúdo suspeito ou perigoso para a execução dos objetivos, missão e visão da Instituição.

Por esse motivo, foram vedados: a instalação de *softwares* não homologados ou licenciados pela unidade de tecnologia da informação; o acesso ou tentativa de ou a tentativa de acesso a recurso tecnológico do qual não seja detentor de autorização, em especial àqueles que contenham conteúdo considerado ofensivo, ilegal ou impróprio; a utilização de recursos tecnológicos da PCDF para fins estranhos às atividades de polícia judiciária; a prática de quaisquer atos tendentes a tornar indisponível qualquer recurso tecnológico sem autorização; o uso de provedores de acesso externo ou de qualquer outra forma de conexão não autorizada no ambiente de rede da PCDF.

No que diz respeito à gestão dos riscos de Segurança da Informação, as unidades responsáveis por atividades que executem processamento da informação devem realizar a gestão dos riscos em conformidade com a metodologia de riscos de segurança da informação e com os objetivos estratégicos da Polícia Civil do Distrito Federal.

Visando o sigilo dos dados tratados pela PCDF para fins não penais, a Seção XIII da Resolução fez menção ao Termo de Compromisso de Responsabilidade, onde consta que todos os servidores, colaboradores e prestadores de serviço deverão assinar os termos de compromisso e responsabilidade aplicáveis às suas atribuições, visando a manutenção do sigilo das informações.

Ainda no ano de 2022, o Delegado Geral da Polícia Civil do Distrito Federal, no uso de suas atribuições legais, instituiu, através da Portaria número 197, de 15 de setembro, o Glossário de Segurança da Informação no âmbito da Polícia Civil do Distrito Federal, cujo único objetivo foi a divulgação de todos os termos técnicos que são utilizados no tratamento de dados pessoais realizados no âmbito da PCDF. Cabe ressaltar que esse glossário, conforme mencionado acima, foi direcionado para a Segurança da Informação, o que inclui o tratamento de dados pessoais para fins não penais.

Após a instituição da Portaria número 197, de 15 de setembro de 2022, que publicou o Glossário de Segurança da Informação no âmbito da Polícia Civil do Distrito Federal, o Delegado Geral da PCDF publicou a Portaria número 220, de 18 de maio de 2023, que aprovou o Documento de Constituição da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR, da Polícia Civil do Distrito Federal.

A missão dessa equipe é facilitar e coordenar as atividades de tratamento e respostas a incidentes em redes computacionais da Polícia Civil do Distrito Federal, apoiando e coordenando as atividades de recuperação de sistemas, através da análise de ataques e intrusões, de forma a cooperar com equipes de outros órgãos, participando de fóruns e redes internacionais.

A Portaria chama muita atenção, poque é possível que com a implementação de uma Legislação Penal de Proteção de Dados Pessoais, a Polícia Civil do Distrito Federal utilize o mesmo modelo para mobilizar uma equipe que tenha a única e exclusiva função de fazer o monitoramento dos dados utilizados em investigações criminais. O monitoramento geraria uma espécie de relatório que seria armazenado e ficaria disponível nos sistemas da PCDF, detalhando todos os atos que desencadearam a utilização de dados pessoais no decorrer de uma investigação policial. Além disso, seria interessante a criação de um sistema inteligência

artificial que efetuasse algumas perguntas ao servidor responsável pelo acesso aos dados. As respostas do servidor gerariam um relatório, que seria monitorado por equipe específica.

Na mesma Portaria 220/2013 também consta que a estrutura organizacional da ETIR/PCDF será composta por um Agente Responsável da Divisão de Tecnologia (DITEC), que coordenará os demais membros da equipe e se reportará à Direção da Divisão e ao Gestor de Segurança da Informação. O mesmo Agente Responsável também coordenará as atividades de respostas a incidentes, a elaboração de informes sobre segurança e assuntos correlatos, bem como a comunicação com os demais grupos de resposta a incidentes existentes. Embora essa Portaria esteja focada na disseminação de uma cultura de segurança da informação, no gerenciamento de eventos e na gestão de incidentes, ela pode servir de modelo para eventual monitoramento de dados para fins penais, que é a atividade fim da Polícia Civil do Distrito Federal.

Outro ponto relevante da Portaria foi a iniciativa de apoio à construção de políticas e normas de segurança da informação, cujo objetivo é a preservação dos ativos de informação e da imagem institucional da Polícia Civil do Distrito Federal. Trata-se de apoio na construção das políticas e normas de segurança da informação e comunicações, que têm por objetivo a instituição de diretrizes estratégicas que visam garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações, bem como atitudes adequadas para manuseio do tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos, armazenados sob guarda ou transmitidos por qualquer meio ou recurso contra ameaças e vulnerabilidades. Isso resulta na descrição das funções e dos procedimentos, que é a realização do levantamento das informações necessárias para prestar apoio na elaboração de políticas e normas voltadas à adequação da Polícia Civil do Distrito Federal às melhores práticas de segurança da informação.

Durante o ano de 2024, o Comitê Gestor de Segurança da Informação e Comunicação da Polícia Civil do Distrito Federal aprovou a Resolução número 41 de 02 de julho, que aprovou a Norma de Gestão de Computação em Nuvem no âmbito da PCDF. Essa Resolução possui ligação com o tema deste trabalho, porque em muitos casos essas nuvens são utilizadas para o armazenamento dos bancos de dados.

No caso em tela, a Resolução número 41/2024 definiu as diretrizes necessárias para a utilização de soluções de infraestrutura e armazenamento em nuvem, tendo em vista a proteção do acesso às informações custodiadas pela Polícia Civil do Distrito Federal. A aplicação dessa norma é feita em conjunto com o Glossário de Segurança da Informação já mencionado anteriormente.

A Resolução define como *computação em nuvem* o modelo que habilita o acesso via rede a um grupo escalável e elástico de recursos (físicos ou virtuais) compartilháveis, a partir de provisionamento via autoatendimento e administração sob demanda. Esse modelo de implantação de nuvem pode ser organizado com base no controle e no compartilhamento de recursos físicos ou virtuais. Essas nuvens podem ser classificadas como:

> I - **Nuvem comunitária:** infraestrutura de nuvem dedicada ao uso compartilhado, composta por órgãos que compartilham requisitos, bem como a mesma natureza de trabalho e obrigações;
> **II - Nuvem Híbrida:** infraestrutura de nuvem composta por dias o mais infraestruturas distintas (privadas, comunitárias ou públicas), as quais permanecem com suas próprias características, mas encontram-se agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações;
> **III - Nuvem privada ou interna:** infraestrutura de nuvem dedicada ao uso exclusivo do órgão, o qual controla e mantém os recursos da nuvem; e
> **IV - Nuvem pública ou externa:** infraestrutura de nuvem dedicada ao uso aberto, potencialmente disponível a qualquer cliente, com recursos controlados e mantidos pelo provedor do serviço de nuvem.

Por fim, em julho de 2024 a Polícia Civil do Distrito Federal estabeleceu a Política de Segurança Orgânica, onde foi definido que a Segurança das Comunicações, da Informática e da Telemática é o conjunto de normas, medidas e procedimentos voltados para os meios de comunicações, no sentido de salvaguardar dados e conhecimentos, de modo a impedir ou dificultar a interceptação, análise da transmissão e do tráfego de dados e sinais, visando preservar os sistemas da tecnologia de informação, de modo a garantir a continuidade do seu funcionamento, a integridade dos conhecimentos e o controle do acesso.

Com a implementação dessas Normas, a Polícia Civil do Distrito Federal partiu para o plano de conscientização dos seus servidores, colocando em prática a Campanha de Conscientização em Segurança da Informação – CCSI. A Campanha e a Cartilha de Conscientização em Segurança da Informação foram divulgadas na Intranet (página da PCDF exclusiva para servidores).

No decorrer da Campanha de Conscientização, a PCDF reforçou a necessidade de confidencialidade exigida em alguns casos que exigem cuidado especial durante o exercício de atividades profissionais no ambiente institucional, além de frisar que todos os servidores devem prestar atenção ao grau de classificação atribuído a cada informação, observando a ocorrência de vazamentos, acessos indevidos ou exclusões acidentais.

É preciso reforçar que o foco desse trabalho é análise dos protocolos utilizados pela Polícia Civil do Distrito Federal nos casos de tratamento de dados pessoais, vislumbrando a futura implementação de políticas públicas que criem mecanismos de controle no acesso aos dados pessoais de autores ou vítimas de delitos, ainda que não exista uma legislação específica para o tratamento de dados no campo penal. Conforme já mencionado em diversos momentos desse trabalho, as instituições policiais em todo o Brasil, o que inclui a Polícia Civil do Distrito Federal, armazenam diariamente dados dos cidadãos que buscam fazer identidades, ocorrências policiais criminais ou simples registros de extravio ou acidente de trânsito sem vítima.

Cabe salientar que o objetivo dessas instituições policiais não é a captação de dados para futura comercialização, como ocorre em alguns casos[546]. Vejo essa alimentação dos bancos de dados como algo inerente à atividade policial, porque diariamente diversas pessoas procuram as delegacias para comunicarem que foram vítimas de crimes. Os dados, quando utilizados de forma correta, servem para prevenir a prática de delitos e para identificar autores de crimes.

Apesar disso, é preciso reforçar que toda intervenção em direitos fundamentais precede de uma justificação especial, de forma que qualquer violação não justificada será ilícita. A liberdade individual compreende um limite à atividade estatal, que não pode adentar na esfera de autodeterminação do indivíduo fora das hipóteses e dos requisitos expressamente previstos em lei[547].

---

[546]Exame negócios. Ele vai fazer R$ 100 milhões com 'império de dados' vindos do wi-fi que você acessa de graça por aí. Disponível em: https://exame.com/negocios/ele-criou-um-imperio-de-dados-de-r-100-milhoes-com-o-sinal-wi-fi-que-voce-acessa-de-graca-por-ai/. Acesso em 04 de set. 2024.

[547]GRINOVER, Ada Pelegrini. Liberdades públicas e processo penal: as interceptações telefônicas. 2ª ed. São Paulo: Revista dos Tribunais, 1982. p. 15.

Da mesma forma como ocorreu na Polícia Civil do Distrito Federal, o Governo do Distrito Federal, por intermédio da Secretaria de Estado de Economia do Distrito Federal, publicou e enviou, em outubro de 2022, a todos os Órgãos e Entidades do Distrito Federal a Circular número 13/2022, que abordou aspectos relevantes sobre a Lei Geral de Proteção de Dados.

A referida Circular recomendou que todos os Órgãos e Entidades do Distrito Federal, ao iniciarem um processo no SEI-GDF[548], escolhessem o tipo de processo, com o intuito de identificar o objetivo de análise para definir o seu nível de acesso. O nível de acesso em um processo em trâmite no SEI-GDF permite a publicidade da informação ou a restrição para visualização aos usuários autorizados a conhecer informações que constam nos documentos.

A Circular frisa que a restrição de acesso ocorrerá para documentos que contiverem informações pessoais relacionadas à intimidade, vida privada, honra e imagem da pessoa natural ou alguma outra restrição baseada em legislação específica. Outras informações que também precisarão ser protegidas pela restrição de acesso estão relacionadas ao sigilo comercial, bancário, fiscal e contábil, bem como os direitos autoriais, as auditorias, PADs[549] e aqueles protegidos por segredo de justiça.

Outras recomendações foram feitas pela Secretaria de Economia, no sentido de reforçar que todos os usuários do SEI-GDF têm responsabilidade sobre as informações que cadastra no sistema, bem como sobre os documentos que produz e o nível de acesso atribuído aos documentos. Com fundamento na Lei de Acesso à Informação e na Lei Geral de Proteção de Dados, a Circular reforçou a importância de todos os servidores estarem atentos à proteção de dados pessoais de qualquer pessoa, interna ou externa ao GDF.

Também foi recomendado que ao incluir um documento em processo, o usuário deverá ficar atento às informações pessoais que o documento venha a ter, o que torna obrigatório o

[548]Instituto de Pesquisa Econômica Avançada. Sistema Eletrônico de Informações – SEI. O que é o SEI? O Sistema Eletrônico de Informações (SEI) é um sistema de gestão de processos e documentos eletrônicos, que oferece suporte à produção, edição, assinatura e trâmite de tais processos e documentos. Trata-se de uma plataforma que engloba um conjunto de módulos e funcionalidades capazes de promover a eficiência administrativa e práticas inovadoras de trabalho, em interface amigável. Disponível em: https://www.ipea.gov.br/portal/sistema-eletronico-de-informacoes. Acesso em 09 de set. 2024.

[549]Controladoria Geral do Distrito Federal. Processo Administrativo Disciplinar – PAD. Disponível em: https://www.cg.df.gov.br/processo-administrativo-disciplinar-pad-voce-sabe-o-que-e/. Acesso em 09 de set. 2024.

cadastro do documento como o nível de acesso restrito ou sigiloso, com respaldo na hipótese legal de informação pessoal. Caso seja identificado que um documento contenha informação pessoal e que esteja com nível de acesso público, o servidor será obrigado a alterar o nível de acesso para restrito ou sigiloso, bem como alterar o nível de acesso restrito/sigiloso para público caso um processo/documento esteja com restrição equivocada.

As informações que deverão estar com nível de acesso restrito ou sigiloso são informações relacionadas à pessoa natural, relativas à intimidade, vida privada, honra e imagem. Essas informações podem constar, por exemplo, em data de nascimento, endereço, telefone residencial, telefone particular, quaisquer dados médios, números de documentos pessoais, como RG, CPF e título de eleitor, orientação sexual, dados financeiros pessoais, números de contas e números de cartões.

Por fim, foi solicitada aos servidores do GDF uma atenção especial quando os dados do processo SEI-GDF se referir a crianças e adolescentes, uma vez que além da Lei Geral de Proteção de Dados, o Estatuto da Criança e do Adolescente também deverá ser respeitado. Sobre esse tema, inclusive, a Autoridade Nacional de Proteção de Dados divulgou, em maio de 2023, enunciado sobre tratamento de dados pessoais para crianças e adolescentes[550].

O objetivo da ANPD com o Enunciado foi uniformizar a interpretação da Lei Geral de Proteção de Dados quanto às hipóteses legais que autorizam o tratamento de dados de crianças e adolescentes. Conforme consta no Enunciando, o tratamento de dados pessoais de crianças e adolescentes pode ser realizado com base nas hipóteses legais previstas na LGPD, como nos casos de consentimento fornecido pelo titular, de cumprimento de obrigação legal, de proteção à vida ou de atendimento a interesse legítimo do controlador.

A proteção de dados pessoais, portanto, é um caminho que não possui mais volta. A cultura de proteção de dados pessoais vem ganhando relevância em grande maioria dos órgãos públicos, seja no executivo, legislativo ou judiciário. O Ministério Público Federal instituiu, no

[550]Autoridade Nacional de Proteção de Dados. ANPD divulga enunciado sobre o tratamento de dados pessoais de crianças e adolescentes. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes. Acesso em 09 de set. 2024.

início de janeiro de 2021, a Comissão de Conformidade à Lei Geral de Proteção de Dados Pessoais no Ministério Público Federal[551].

A Comissão foi presidida e coordenada pelo Oficial de Proteção de Dados (DPO), designado pelo Procurador Geral da República. Os principais objetivos do Ministério Público Federal com essa Comissão foi: elaborar plano de ação cronograma para conformidade do MPF à LGPD; distribuir e realizar as atividades de conformidade do MPF à LGPD; promover e acompanhar iniciativas institucionais relacionadas ao tema, atuando sempre que necessário para manter o alinhamento; propor políticas, diretrizes e padrões técnicos relacionados ao tema; trocar experiências e boas práticas com órgãos públicos entidades privadas e universidades, em especial com o Conselho Nacional do Ministério Público, Ministério da Economia e Escola Nacional de Administração Pública; e promover debates, conversas, palestras e encontros acerca da proteção de dados pessoais como forma de intercâmbio de conhecimento e experiências sobre o tema.

O tema de proteção de dados no Direito Penal e no Processo Penal, mais especificamente nas investigações criminais, deve ser tratado dentro do contexto de políticas públicas. O objetivo da implementação dessas políticas públicas é fazer com que a utilização dos dados existentes nos bancos de dados das polícias judiciárias brasileiras esteja em consonância com o que preceitua a Constituição Federal, de forma que o direito fundamental da proteção de dados sofra o mínimo de restrição possível.

Somente quem trabalha com a atividade Policial, sabe o quanto é importante ter acesso a informações que possam prevenir a prática de crimes que estejam na iminência de acontecer. A utilização dos bancos de dados pode até servir como auxílio para identificar autores de crimes, mas para o policial que está na linha de frente observando diariamente as mazelas da sociedade, é mais gratificante quanto se consegue prevenir um delito, seja ele qual for. Beatriz Vargas de Rezende, quando escreveu o trabalho *A Ilusão do Poibicionismo: Estudo sobre a Criminalização Secundária do Tráfico de Drogas no Distrito Federal*, referendou a importância do Policial no ordenamento jurídico brasileiro, quando disse que " o Juiz é detentor

[551]Ministério Público Federal. PORTARIA PGR/MPF Nº 24, DE 27 DE JANEIRO DE 2021. Disponível em: https://biblioteca.mpf.mp.br/repositorio/items/99012da8-45fa-4814-ba46-940cc1dbfca3. Acesso em 09 de set. 2024.

do maior capital simbólico do sistema penal, embora seu poder de seleção criminal seja muito inferior ao do policial”[552].

Isso não quer dizer, porém, que o direito das vítimas ou o direito à segurança pública não sejam respeitados. Daí a importância das políticas de segurança pública, que servirão para criar condições adequadas ao tratamento de dados pessoais para fins penais, monitorando a utilização desses dados, de forma a amenizar a colisão de direitos fundamentais que eventualmente exista entre o direito à proteção de dados e o direito à segurança pública.

O primeiro passo para a análise da necessidade de aplicação de uma política pública é definir o que, de fato, se entende por política pública. Segundo o Manual de Políticas Públicas do Ministério Público do Estado do Ceará[553], entende-se por política pública “a totalidade de ações, metas e planos que os governos (nacionais, estaduais ou municipais) traçam para alcançar o bem-estar da sociedade e o interesse público”[554].

A implantação e a implementação de uma política pública necessitam de uma análise bem criteriosa. Além da aferição da necessidade da política pública, é importante que o Estado faça uma análise da importância do tema, da quantidade de pessoas que a política atingirá e dos custos necessários para o seu efetivo funcionamento.

Apesar da Polícia Civil do Distrito Federal já ter colocado em prática diversas normas de segurança da informação, o que é válido, é preciso implementar políticas públicas que criem mecanismos capazes de fazer o monitoramento da utilização dos bancos de dados da instituição, quando utilizados no âmbito de uma investigação. Outro aspecto que também deve ser observado é que não basta simplesmente instituir uma política de monitoramento da utilização desses dados. É preciso que a política acompanhe a evolução da sociedade, visando sempre o seu aperfeiçoamento e buscando soluções inovadoras que tenham o objetivo de justificar que a

[552]REZENDE, Beatriz Vargas Ramos Gonçalves de; A Ilusão do Poibicionismo: Estudo sobre a Criminalização Secundária do Tráfico de Drogas no Distrito Federal. 2011. 148 f. Tese (Doutorado em Direito). Universidade de Brasília – UNB.

[553]CALDAS, Ricardo Warendorff (coord.). Políticas públicas: conceitos e práticas. Belo Horizonte: Sebrae/MG, 2008. (Série Políticas Públicas, v. 7). Disponível em: http://www.mp.ce.gov.br/nespeciais/promulher/manuais/MANUAL DE POLITICAS PÚBLICAS.pdf. Acesso em: 04 set. 2024.

[554]O tema foi abordado em artigo de mesma autoria, publicado em 2022: MARWELL, Daniel Bastos. Sistemas de Compliance na Atividade Policial: A integridade nas Polícias Judiciárias Brasileiras. Rio de Janeiro: Lumen Juris, 364 p.

utilização de eventuais dados tenha sido necessária para a identificação de autores de crimes, visando sempre o bem estar e a segurança da coletividade.

Políticas públicas são extremamente importantes porque demonstram que o Estado está aberto à modernização, fazendo reformas pontuais que contribuirão de forma significativa para o bem-estar da sociedade e dos cidadãos. O Estado Brasileiro precisa ter a consciência de que uma política pública adequada pode trazer benefícios imensuráveis, sendo imprescindível para uma boa prestação de serviços públicos.

Para Daniel Piñeiro Rodriguez, a efetivação de políticas públicas de proteção de dados pessoais em atenção às garantias fundamentais estabelecidas em um Estado Democrático de Direito, salienta ainda mais a estreita relação entre liberdade, privacidade e dignidade. "Sem dispor de uma robusta tutela das informações que digam respeito à pessoa, estará o Poder Público permitindo não só a intrusão de terceiros na esfera privada, mas também se omitindo na garantia de outros direitos fundamentais"[555], conclui.

Para que uma política pública possa ser aplicada com eficiência também se faz necessária uma análise prévia da política que se quer implantar, tendo em vista que essa análise pode resultar em mais efetividade e eficácia. O comitê interno de governança da Casa Civil da Presidência da República lançou um guia prático de análise *ex ante* para a aplicação de políticas públicas[556].

No referido guia consta que a análise *ex ante* de uma política pública deve seguir as seguintes etapas: i) diagnóstico do problema; ii) caracterização da política pública: objetivos, ações, público-alvo e resultados esperados; iii) desenho da política; iv) estratégia de construção de confiabilidade e credibilidade; v) estratégia de implementação; vi) estratégias de monitoramento, de avaliação e de controle; vii) análise de custo-benefício; e viii) impacto orçamentário e financeiro.

---

[555]RODRIGUEZ, Daniel Piñeiro. O Direito Fundamental à Proteção de Dados: Vigilância, Privacidade e Regulação. Rio de Janeiro. Lumen Juris. 2021. 232 p.

[556]BRASIL. Presidência da República. Casa Civil. Avaliação de Políticas Públicas. 12 de dezembro de 2008. Disponível em: http://www.casacivil.gov.br/orgaos-vinculados/comite-interministerial-de-governanca. Acesso em: 04 set. 2024.

Seguindo as etapas, é possível compreender que o diagnóstico do problema no estudo deste trabalho é a utilização dos bancos de dados da Polícia Civil do Distrito Federal, sem o devido monitoramento. O principal objetivo da aplicação de uma política pública será a implementação de controle sobre a utilização dos bancos de dados da PCDF. Espera-se que a implementação da política pública seja incorporada ao dia a dia dos integrantes da Polícia Civil do Distrito Federal, fazendo com que a utilização dos dados pessoais siga os princípios estabelecidos na Lei Geral de Proteção de Dados.

Da racionalização de uma política pública à implementação e ao seu monitoramento há um longo caminho a ser percorrido. Além da análise do problema, será necessário analisar os impactos do projeto de política pública, os seus objetivos, o seu custo-benefício, além do seu devido monitoramento.

A Lei Geral de Proteção de Dados e o Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Persecução Penal traçam todas as diretrizes para a implementação da política pública. Trazendo a ideia para a área das políticas públicas, o diagnóstico do problema seria um dos pilares. É necessário que, ao se cogitar a racionalização de uma política pública, exista o diagnóstico do que se quer combater.

No caso do objeto em estudo, a criação de um mecanismo que faça o monitoramento do servidor que utilize qualquer tipo de dados dos bancos de dados da Polícia Civil do Distrito Federal é o objeto da política pública aventada. A identificação do problema é necessária porque permite que durante a execução da política pública, o suposto problema seja devidamente acompanhado. Não basta somente a identificação do problema para que uma política pública atinja os objetivos almejados, também se faz necessária a busca por soluções para que o problema diagnosticado seja extinto ou minimizado.

O diagnóstico do problema também pode vir acompanhado de pesquisas quantitativas ou qualitativas, que podem servir para demonstrar a necessidade de execução de uma política pública. O caso da falta de um mecanismo que faça o monitoramento da utilização de dados pessoais para fins penais ainda não foi muito debatido pela sociedade.

Nesse aspecto, o diagnóstico do problema seria feito com base em informações baseadas no período em que o problema ocorre, quem são os principais prejudicados com a ausência de

uma política pública, se o problema ocorre em diversas regiões, se há algum indicador ou estudo que possa ajudar o Estado a compreender a importância da sua atuação. Aqui deve ser destacado que uma política pública já existente pode ajudar na criação de uma nova política pública.

A abordagem que será feita agora é, na verdade, um complemento do que já foi mencionado. Depois de abordar a aplicação de políticas públicas para o monitoramento da utilização dos bancos de dados da Polícia Civil do Distrito Federal, de mencionar a análise preliminar da necessidade de aplicação de uma política pública e de aferir a necessidade do diagnóstico de um problema que justifique a aplicação desta, passar-se-á a abordar a caracterização de uma política pública.

Antes de começar a definir os critérios para essa caracterização, é importante frisar que a tarefa não é simples. Os requisitos, porém, foram muito bem definidos e traçados pelos guias de avaliação de políticas públicas emitidos pela Casa Civil da Presidência da República, através da Subchefia de Análise e Acompanhamento de Políticas Governamentais, pelo Ministério da Fazenda, pelo Ministério do Planejamento, Desenvolvimento e Gestão e pelo Ministério da Transparência e Controladoria-Geral da União.

Os referidos guias, denominados "Avaliações de Políticas Públicas – Guia Prático de Análise *Ex Ante*"[557] e "Avaliação de Políticas Públicas – Guia Prático de Análise *Ex Post*",[558] foram precisos na explicação dos mecanismos e das diretrizes necessárias para a implementação de uma política pública, tornando-se verdadeiros manuais sobre o tema.

Além disso, os guias serviram de base para tentar explicar, neste trabalho, por que a implantação desse mecanismo de controle na Polícia Civil do Distrito Federal é um tema que atinge o bem-estar social, merecendo ser tratado na forma de política pública, passando pelo diagnóstico do problema, pelo desenho da política pública e sua caracterização, pelo impacto orçamentário e financeiro, pela estratégia de implementação, pela estratégia de construção de

[557]BRASIL. Casa Civil da Presidência da República. Avaliação de Políticas Públicas: Guia Prático de Análise *Ex Ante*. v. 1. Brasília: Ipea, 2018. Disponível em: https://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=32688. Acesso em: 04 set. 2024.

[558]BRASIL. Casa Civil da Presidência da República. Avaliação de Políticas Públicas: Guia prático de análise *ex post*. v. 2. Brasília: Casa Civil da Presidência da República, 2018. Disponível em: https://ipea.gov.br/portal/index.php?option=com_content&id=34504. Acesso em: 04 set. 2024.

confiança e suporte, pela estratégia de monitoramento, avaliação e controle, pela avaliação dos resultados e pela mensuração do retorno econômico e social.

Depois de aferir o diagnóstico e a identificação do problema, é necessário debater a forma correta de criação de uma política pública que seja capaz de atingir a causa que gerou o problema, visando diminuí-lo ou erradicá-lo. Isso se faz necessário porque, a depender do tipo de caracterização da política pública mais adequada, será feita uma análise do valor a ser gasto com a implementação da referida política pública, o tempo de funcionamento e o resultado que se pretende obter.

A já descrita caracterização de uma política pública também permite que o desenho do seu projeto seja feito exatamente da mesma forma quando ocorreu a racionalização dessa política pública, sem intercorrências por gastos extras e gerando a eficiência esperada. Isso fica mais claro quando se fala das etapas a serem percorridas com o diagnóstico do problema, o objetivo, o público-alvo, os meios e instrumentos, os atores e arranjo institucional e a definição de metas.

Por fim, a caracterização permite que os resultados sejam mais claros, possibilitando que no futuro seja possível aferir que a política pública de fato alcançou os resultados esperados. Outro aspecto que deve ser destacado é que a caracterização da política pública, depois de cumprida todas as etapas, também passa a possibilidade de o objetivo ser atingido, daí a sua importância.

Seguindo a mesma linha de raciocínio do que foi mencionado anteriormente, ainda utilizando como referencial os guias de Avaliação de Políticas Públicas, é fundamental a análise estratégica da implementação de uma política pública. Essa fase talvez seja a mais importante de toda a cadeia de processo, porque aferirá se todos os atores e recursos estão devidamente estruturados para a execução das metas e das ações planejadas.

A etapa em questão tem como principal objetivo o mapeamento de eventuais erros ou falhas que possam ter ocorrido durante o processo de implantação, otimizando, dessa forma, a política pública a ser implementada. Para isso, os atores envolvidos em sua construção adotarão os seguintes passos:

> Definição do modelo de gestão e de governança, explicitando os mecanismos de liderança, estratégia e controle que serão postos em prática para avaliar, direcionar e monitorar a política;
> Análise das atribuições e dos incentivos dos atores envolvidos na execução da política, verificando se o arranjo institucional proposto é adequado;
> Análise da base legal da política e da espécie de instrumento que será utilizado para constituir as obrigações e avenças necessárias à sua consecução e dos seus programas e ações;
> Definição do plano de comunicação a ser executado durante todas as etapas da política; e
> Análise de riscos eventuais ao longo da execução da política pública, com sua identificação, elaboração de estratégias de mitigação, administração e controle, compatível com a matriz Swot (do inglês, *strengths, weaknesses, opportunities and threats*)[559].

Do mesmo modo como ocorre nos sistemas de *compliance*, aqui também haverá um planejamento dedicados aos riscos, com o principal objetivo de mitigá-los caso eles venham a acontecer. Cabe ressaltar que a implementação estratégia da política pública ainda está no campo da análise *ex ante*, ou seja, antes da implementação.

Estudos têm demonstrado que a implementação estratégica tem como principal objetivo criar alternativas que sejam utilizadas em caso de alguma falha ocorrida durante a execução da política pública[560]. Isso não quer dizer que eventualmente situações inesperadas não possam acontecer, o que se busca aqui é a reparação imediata de falhas que normalmente ocorrem quando a política pública está em pleno funcionamento.

Tudo o que foi falado sobre política pública até aqui diz respeito a metodologias e técnicas utilizadas antes da sua entrada em vigor, ou seja, foi feita uma análise *ex ante*. A partir de agora será possível aferir o que é necessário fazer depois que uma política pública começa a funcionar, ou seja, será feita uma abordagem *ex post*, o que possibilitará analisar que a efetividade de uma política pública deve passar por constantes monitoramentos e avaliações, sempre visando o seu aperfeiçoamento.

Quanto maior for a efetividade de uma política pública, maior será o retorno recebido pela sociedade. O monitoramento, a avaliação e o controle de uma política pública também são necessários para que seja aferido se os resultados obtidos ao longo de sua implementação são

---

[559] *Ibid.*

[560] Enap. Teorias e Análises sobre Implementação de Políticas Públicas no Brasil. Disponível em: https://repositorio.enap.gov.br/bitstream/1/4162/1/Livro_Teorias%20e%20An%C3%A1lises%20sobre%20Implementa%C3%A7%C3%A3o%20de%20Pol%C3%ADticas%20P%C3%BAblicas%20no%20Brasil.pdf. Acesso em 08 de nov. 2024.

aqueles racionalizados no início de todo o projeto. Por isso a importância de fazer o acompanhamento em uma política pública já implementada, principalmente pelo fato de aferir se o dinheiro público está sendo bem utilizado, em uma causa que esteja surtindo o efeito esperado.

Conforme consta no Manual de "Avaliação de Políticas Públicas - Guia Prático de Análise *ex post*",[561] uma política pública já implantada deve passar pela avaliação do desenho, pela avaliação de implementação, pela avaliação de governança da política pública, pela avaliação dos resultados, pela avaliação do impacto, pela avaliação econômica e pela análise de eficiência.

A avaliação dos resultados de uma política pública já implantada também deve passar por um mapeamento dos resultados apresentados. É possível que, com a análise dos desfechos, a política pública seja ainda mais aperfeiçoada, superando os resultados esperados na fase que antecedeu a sua materialização. Por esse motivo, a partir deste momento os impactos da política pública serão devidamente monitorados e avaliados, buscando aferir o resultado, o orçamento e sua eficiência.

Embora na grande maioria das vezes os dados pessoais debatidos até aqui sejam utilizados de forma consciente, não se pode permitir a prática de abusos ou até erros graves na utilização dos dados. Daí a necessidade de implementação de políticas públicas, conforme justificado acima. Sobre os erros, inclusive, Laura Schertel, ao debater sobre a Autoridade de Proteção de Dados na Segurança Pública[562], alertou que alguns dados não são protegidos por sigilo, seja na Constituição Federal, seja no Código Penal, seja no Código de Processo Penal ou em Leis Extravagantes. Como exemplo, mencionou as diversas notícias jornalísticas onde pessoas sem antecedentes criminais foram presas com base em fotos que elas sequer souberam como foram parar nos bancos de dados das delegacias.

Apesar da Polícia Civil do Distrito Federal estar preparada para o tratamento de dados pessoais utilizados para fins penais, é necessária a participação do Ministério Público, órgão de

---

[561] *Ibid.*

[562] Internet Lab. Direitos Fundamentais e Processo Penal na era digital. Disponível em: https://internetlab.org.br/wp-content/uploads/2023/01/Direitos-Fudamentais-e-Processo-Penal-na-era-digital-2021.pdf. Acesso em 16 de set. 2024.

controle externo da atividade policial. Para Carlos Vinícius Alves Ribeiro[563] o Ministério Público possui inúmeras atribuições extrajudiciais, além das já elencadas nos artigos 127, 128 e 129 da nossa Carta Magna. Segundo o Autor "desde que deixou de exercer apenas a titularidade da ação penal, ainda antes da Constituição da República de 1988, o Ministério Público foi se agigantando". Isso pode ser comprovado com as inúmeras atribuições do Ministério Público, que estão espalhadas em diversos textos normativos. A Lei Orgânica Nacional do Ministério Público[564], que dispõem sobre normas gerais para a organização dos Ministérios Públicos, assevera que o Ministério Público é instituição permanente, essencial à função jurisdicional do Estado, incumbindo-lhe a defesa da ordem jurídica do regime democrático e dos interesses individuais e sociais indisponíveis.

Outro ponto que precisa ser destacado é que o armazenamento dos dados também pode ser utilizado para auxiliar pesquisas que tenham como objetivo o aperfeiçoamento do tratamento de dados pessoais. Sem dados, não é possível planejar o futuro. No trabalho intitulado *O Estudo de Impacto Legislativo como Estratégia de Enfrentamento a Discursos Punitivos na Execução Penal*, Carolina Costa Ferreira retratou a sua decepção com os dados produzidos sobre o sistema penitenciário até a data em que fez a pesquisa, ao afirmar que "é inegável que as instituições públicas brasileiras precisam melhorar as etapas de compilação, produção e publicação de informações e dados que sejam importantes à formulação de políticas públicas"[565].

Interessante fazer essa observação, porque a Segurança Pública, por ser um direito indisponível, merece o amparo e a fiscalização do Ministério Público. O Supremo Tribunal Federal, inclusive, no julgamento do RE 559646 PR[566], entendeu que o direito à segurança é prerrogativa constitucional indisponível, garantido mediante a aplicação de políticas públicas, impondo ao Estado a obrigação de criar condições que possibilitem o efetivo acesso a tal serviço.

---

[563]RIBEIRO, C. V. A. Ministério Público - Funções Extrajudiciais. 1ª Edição ed. Belo Horizonte: Fórum, 2015.
[564]BRASIL. Lei 8.625/93 - Lei Orgânica Nacional do Ministério Público. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8625.htm>. Acesso em: 26 mar. 2021.
[565]FERREIRA, Carolina Costa. O Estudo de Impacto Legislativo como Estratégia de Enfrentamento a Discursos Punitivos na Execução Penal. 2016. 182 f. Tese (Doutorado em Direito). Universidade de Brasília – UNB.
[566]STF, RE 559646 PR, Segunda Turma, Rel. Ellen Gracie, J. 07.06.2011, DJe 24.06.2011.

Após análise da legislação que trata das atribuições do Ministério Público, será possível aferir, como diz Carlos Vinícius[567], que não há um rol fechado. Depreende-se, portanto, que o Ministério Público pode exercer atividades nunca imagináveis na defesa dos interesses da sociedade. Embora uma grande parte dessas atribuições seja exercida de forma judicial, nada impede que também sejam exercidas atividades extrajudiciais, como por exemplo, por que não, o acompanhamento da implementação de políticas públicas que tenham como objetivo o monitoramento da utilização dos bancos de dados da Polícia Civil do Distrito Federal.

Apesar de ainda não termos uma legislação que regulamente a utilização desses bancos de dados para fins penais, nada impede que o Ministério Público já comece a fazer esse monitoramento, com o intuito de fazer com que o exercício do direito fundamental à segurança pública não prejudique o exercício do direito fundamental à proteção de dados. Renato Leite Monteiro frisou que mesmo antes da vigência da Lei Geral de Proteção de Dados, o Ministério Público do Distrito Federal e Territórios (MPDFT), por intermédio de sua Comissão Especial de Proteção de Dados pessoais, instaurou uma série de inquéritos contra empresas que haviam supostamente violado a LGPD[568].

Na ocasião, o MPDFT exigiu que uma empresa elaborasse relatório de impacto à proteção de dados pessoais. Outros Ministérios Públicos também fizeram o mesmo, quando diversas ações coletivas foram ajuizadas entre os anos de 2016 e 2018, antes mesmo da entrada em vigor da atual Lei Geral de Proteção de Dados. É possível, portanto, que após a proteção de dados pessoais ter sido elevada ao patamar de direito fundamental, os Ministérios Públicos passem a fiscalizar com mais rigor a utilização de dados pessoais para fins penais, ainda que não exista lei que regulamente a matéria.

7.3 Ponderação de bens jurídicos e o princípio da proporcionalidade diante de eventual violação ao direito fundamental da proteção de dados pessoais

Este tópico tem como foco principal a observância dos conflitos de direitos fundamentais, mais especificamente o direito à vida, liberdade e segurança pública versus o direito fundamental à proteção de dados pessoais. Aqui será possível aferir se o direito

---

[567] *Ibid.*

[568] MONTEIRO, Renato Leite. Desafios para a efetivação do direito à explicação na Lei Geral de Proteção de Dados no Brasil. 2021. 386f. Tese (Doutorado). Faculdade de Direito. Programa de Pós-Graduação. Área de concentração: Filosofia e Teoria Geral do Direito. Universidade de São Paulo. São Paulo.

fundamental da proteção de dados pode ser mitigado em detrimento de eventual persecução penal, independentemente do delito que esteja sendo investigado. A colisão de direitos fundamentais é um tema de extrema importância para o direito. É muito comum não só no Supremo Tribunal Federal, como em outras Supremas Cortes mundo afora, o julgamento de temas que envolvam esse aparente conflito de normas. Conforme já mencionado anteriormente nos julgados do STF sobre o caso Ainda Curi[569], cada caso deve ser analisado de forma individualizada, tendo em vista que os tempos mudam e a forma de pensar da sociedade também se transforma.

A colisão de direitos fundamentais é um tema instigante e muito interessante, porque conforme será aferido adiante, a aparente colisão exige ponderação e uma análise criteriosa para que se chegue ao equilíbrio ideal. É nesse contexto que a doutrina e a jurisprudência se baseiam para utilizar técnicas e fundamentos que busquem suprimir o conflito, cujo principal objetivo é a justa resolução para o caso concreto. A colisão de Direitos Fundamentais tem sido pauta frequente no Supremo Tribunal Federal e em diversos Tribunais do Mundo.

De acordo com Gilmar Mendes, fala-se em colisão de direitos fundamentais quando se identifica o conflito decorrente do exercício de direitos individuais por diferentes titulares. "A colisão pode decorrer, igualmente, de conflito entre direitos individuais do titular e bens jurídicos da comunidade"[570], conclui.

Na maioria dos casos, a colisão ocorre quando o exercício de um direito exercido por qualquer um de nós entra em conflito com o exercício de um direito exercido por outra pessoa ou pelo próprio Estado. Quando estamos diante de uma situação dessa, o mais comum na jurisprudência é a utilização do recurso da dignidade da pessoa humana, que é considerado um dos pilares fundamentais do direito, por ser inerente a todo ser humano. O princípio da dignidade da pessoa humana é visto como um princípio norteador para subsidiar decisões judicias mais justas e equitativas.

---

[569]STF, RE 1010606, Tribunal Pleno, Rel. Min. Dias Toffoli, J. 18.02.2021, DJe 20.05.2021.

[570]MENDES, Gilmar. Ela pede vista: Estudos em Homenagem à Ministra Rosa Weber. O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E A ABERTURA DA ORDEM CONSTITUCIONAL À TRANSFORMAÇÃO TECNOLÓGICA: ANÁLISE DO JULGAMENTO DA ADI 6.378. Londrina – PR: Thoth, 2023. p. 329.

No Brasil, o princípio da dignidade da pessoa humana foi inserido no artigo 1º da Constituição Federal[571], se tornando um fundamento para a República Federativa do Brasil e servindo de parâmetro para aplicação em todo o ordenamento jurídico e de fundamento para a garantia dos direitos fundamentais, como o direito à vida, liberdade, igualdade, saúde, segurança, educação e trabalho. Para José Afonso da Silva[572], a dignidade da pessoa humana não é apenas uma criação constitucional, por ser um desses conceito *a priori*, um dado preexistente a toda experiência especulativa, tal como a própria pessoa humana.

Segundo Laura Schertel, o reconhecimento do caráter objetivo dos direitos fundamentais enseja um dever de proteção direcionado tanto ao Estado-Legislador quanto ao Estado-Juiz. Para a Autora, o primeiro destinatário do dever de proteção derivado do direito à proteção de dados pessoais é o legislador, que tem a obrigação constitucional de estabelecer a arquitetura institucional adequada para a proteção da personalidade do cidadão contra os riscos decorrentes do processamento de dados pessoais pelo setor público e privado[573].

Ainda de acordo com Laura Schertel, o segundo destinatário do dever de proteção é o Poder Judiciário, que na ausência ou na insuficiência da ação do legislador deve assegurar a proteção devida a partir das normas já existentes. Também é possível compreender o executivo como um destinatário do dever de proteção, já que dispõe de estruturas administrativas e de controle, aptas a fazer valer a proteção constitucional[574].

Por fim, conclui Laura Schertel que o direito fundamental à proteção de dados não é um direito absoluto, podendo ser limitado em razão da aplicação de outro direito fundamental ou preceito constitucional, aplicado ao caso concreto. Para Alan Westin, o desejo do indivíduo por privacidade nunca é absoluto, porque a participação em sociedade é igualmente importante[575]. Diante disso, cada indivíduo está continuamente envolvido em um processo pessoal de

---

[571]BRASIL. Dignidade da Pessoa Humana. Constituição da República Federativa do Brasil de 1988. Artigo 1º: A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: (...) III – a dignidade da pessoa humana (...). Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 28 de abr. 2024.

[572]DA SILVA, José Afonso. Comentário Contextual à Constituição. 4ª ed. São Paulo. Ed. Malheiros, 2007. p.38.

[573]MENDES, Laura Schertel Ferreira. HABEAS DATA E AUTODETERMINAÇÃO INFORMATIVA: OS DOIS LADOS DA MESMA MOEDA. Direitos Fundamentais e Justiça. Belo Horizonte. Ano 12. Número 39. P, 185-216, jul/deze.2018.

[574]*Ibid.*

[575]WESTIN, Alan. Privacy and freedoms. New York: Atheneum, 1970.

equilíbrio e o desejo de exposição e comunicação com os outros, à luz de condições do ambiente e de normas sociais na sociedade em que vive.

Serge Gutwirth e Paul de Hert entendem que a função central da privacidade não implica em falar que a privacidade e a liberdade que ela protege são absolutas e invioláveis. “Mesmo diante da privacidade em um Estado Constitucional Democrático, trata-se de um Direito Fundamental relativamente fraco. Na verdade, nenhum aspecto da privacidade sobrepõe-se a outros direitos e interesses”[576], concluem os Autores.

Para Jorge Reis Novais, a colisão de direitos fundamentais só pode ser resolvida com o recurso da ponderação, devendo ser utilizada a solução normativa que garanta a realização otimizada de cada um dos princípios envolvidos. De acordo com o Autor, uma colisão entre direitos fundamentais ou entre direitos fundamentais e outros princípios deve sempre se resolver em função do peso relativo que cada um deles representa no caso concreto[577].

Ingo Sarlet afirma que:

> O princípio da proporcionalidade costuma ser desdobrado em três elementos (subcritérios ou subprincípios constitutivos, como prefere Gomes Canotilho): a) a adequação ou conformidade, no sentido de um controle da viabilidade (isto é, da idoneidade técnica) de que seja em princípio possível alcançar o fim almejado por aquele determinado meio, muito embora para alguns, para que seja atendido o critério, bastaria que o poder público (mediante ação restritiva), cumpra com o seu dever de fomentar o fim almejado; b) da necessidade, ou em outras palavras, a opção pelo meio restritivo menos gravoso para o direito objeto da restrição, exame que envolve duas etapas de investigação: o exame da igualdade de adequação dos meios (a fim de verificar se os meios alternativos promovem igualmente o fim) e, em segundo lugar, o exame do meio menos restritivo (com vista a verificar se os meios alternativos restringem em menor medida os direitos fundamentais afetados); c) da proporcionalidade em sentido estrito (que exige a manutenção de um equilíbrio (proporção e, portanto, de uma análise comparativa entre os meios utilizados e os fins colimados, no sentido do que para muitos tem sido também chamado de razoabilidade ou justa medida, já que mesmo uma medida adequada e necessária poderá ser desproporcional[578].

[576]GUTWIRTH, Serge; HERT, Paul de. Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power. RDP, Brasília, v. 18, n. 100, p. 500-549, out./dez. 2021.
[577]NOVAIS, Jorge Reis. Limites dos Direitos Fundamentais: Fundamento, Justificação e Controlo. Portugal. Almedina. p. 5-/51. 2021.
[578]SARLET, Ingo Wolfgang. A Eficácia dos Direitos Fundamentais. Porto Alegre: Livraria do Advogado. 2° ed., 2011, p. 397.

Robert Alexy desenvolveu uma teoria que tenta explicar como agir em situações onde ocorram as colisões de Direitos Fundamentais[579]. Alexy considera, na denominada Teoria dos Princípios, os Direitos Fundamentais como princípios, e não regras. Para o autor, princípios são normas que ordenam que algo seja realizado na maior medida possível, dentro das possibilidades jurídicas e fáticas. Eles não descrevem como as coisas são, mas como deveriam ser pensadas parar evitar contradições. Ainda de acordo com Alexy, os princípios absolutos não são compatíveis com um ordenamento jurídico que inclua direitos fundamentais[580].

Quando dois princípios entram em conflito, Alexy propõe a ponderação como método para resolver essa colisão. Isso é feito através de uma avaliação, que aferirá qual princípio, quando aplicado, causará menor agressividade e intensidade ao outro. A teoria de Alexy, portanto, visa encontrar estruturas dogmáticas, revelar princípios e valores implícitos aos direitos fundamentais, buscando a solução de conflitos e a ponderação de princípios. Robert Alexy sintetiza a necessidade como a exigência de que "dentre dois meios aproximadamente adequados, seja escolhido aquele que intervenha menos de modo intenso".

Isso deve ser feito através da ponderação de princípios que, nas palavras de Alexy, "quanto maior for o grau de não-satisfação ou de afetação de um princípio, tanto maior terá que ser a importância da satisfação do outro[581]". A ponderação de Alexy é dividida em três etapas. Na primeira etapa será avaliado o gravame do princípio ou do direito que está sofrendo a intervenção. Na segunda etapa será avaliada a importância da satisfação do princípio indiferente. Por fim, será verificada se essa importância justificará a intensidade do gravame causado no princípio que está sofrendo a intervenção. Como exemplos de ponderação de princípios, podemos citar o direito à privacidade versus à liberdade de expressão, conforme foi mencionado no case Ainda Curi, a liberdade religiosa versus a igualdade, ou ainda direitos autorais versus acesso à informação.

Cabe salientar que para a nossa Constituição Federal, a Segurança Pública é um direito fundamental porque sem ela não é possível exercer o exercício pleno da cidadania e não é possível ter liberdade. Além disso, vários outros princípios são afetados pela ausência da

---

[579]*Ibid.*
[580]*Ibid.*
[581]ALEXY, Robert. *Teoria dos direitos fundamentais*. Tradução Virgílio Afonso da Silva. 2ª ed. São Paulo: Malheiros, 2012. p. 248.

segurança pública. De acordo com Flávia Ferrer, o Direito à Segurança é uma espécie de direito social, que traz para o Estado o dever de implementar políticas públicas de segurança que garantam aos cidadãos o direito de ir e vir e transitar com tranquilidade nos locais públicos, e também assegurem a defesa de sua integridade física e de seu patrimônio[582]. A autora continua dizendo que o Direito à Segurança é parte fundamental do direito à qualidade de vida e do próprio direito fundamental à vida, na medida em que a insegurança traz aumento de violência e perturbação à ordem pública e social.

Embora não esteja inserido no Artigo 5º da Constituição Federal, o Direito à Segurança pública também é um direito fundamental, por expressa previsão no Artigo 6º da nossa Carta Magna (*Art. 6º São direitos sociais a educação, a saúde, a alimentação, o trabalho, a moradia,* o *transporte, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição*). É sabido, porém, que o alto custo de implementação dos direitos sociais faz com que os Estados não consigam implementar aquilo que está previsto na Constituição Federal. Nas palavras de Marcelo Novelino, "na perspectiva do demandante do direito social, devem ser analisadas a proporcionalidade da prestação de serviço e a razoabilidade de sua exigência"[583].

É possível afirmar que o direito à Segurança Pública faz parte de um *mínimo existencial*[584]. A expressão surgiu na Alemanha, em uma decisão do Tribunal Federal Administrativo de 1953, sendo posteriormente incorporada na jurisprudência daquele país. Como desdobramento dos princípios da dignidade da pessoa humana, da liberdade material e do Estado social, o termo pode ser compreendido como um conjunto de bens e utilidades básicas imprescindíveis para uma vida humana e digna. Nas palavras de Ingo Sarlet, os direitos sociais "podem ser considerados uma densificação do princípio da justiça social"[585].

---

[582]FERRER, Flávia. O Direito à Segurança Pública. Revista do Ministério Público do Estado do Rio de Janeiro - MPRJ. 2017. Disponível em: https://www.mprj.mp.br/documents/20184/2740997/Flavia_Ferrer.pdf. Acessado em 05 de mai. 2024.

[583]NOVELINO, Marcelo. Curso de Direito Constitucional. Salvador: JusPodivm. 2017, p. 482.

[584]SANTOS, Roberto Mizuki Dias dos. A SEGURANÇA PÚBLICA INTEGRADA AO MÍNIMO EXISTENCIAL NO DIREITO BRASILEIRO ENQUANTO MEDIDA NECESSÁRIA PARA SUA EFETIVAÇÃO PELO PODER JUDICIÁRIO. 2011. 149 f. Dissertação (Mestrado). Universidade Federal da Bahia – UFBA.

[585]SARLET, Ingo Wolfgang. A Eficácia dos Direitos Fundamentais. Porto Alegre: Livraria do Advogado. 2° ed., 2001, p. 52.

No parecer denominado *Proteção de Dados no Campo Penal e de Segurança Pública: Nota Técnica sobre o Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Investigação Criminal*, a organização Data Privacy Brasil, Eduardo Viana, Lucas Montenegro e Orlandino Gleizer mencionam os aspectos centrais de um direito de segurança pública, abordando o bem protegido, o perigo e os destinatários. Para os Autores, é preciso fazer uma distinção entre crimes de perigo concreto e crimes de perigo abstrato, para a utilização de critérios de adequação da medida e do nível de intervenção tolerável em direitos fundamentais. "Em geral, perigos concretos e danos mais intensos autorizam intervenções mais invasivas do que perigos abstratos e danos de menor intensidade"[586], concluem.

Para José Afonso da Silva, Segurança Pública é uma "situação de preservação ou restauração da convivência social, que permite que todos gozem de seus direitos e exerçam suas atividades sem perturbação de outrem, salvo nos limites do gozo e reivindicação de seus próprios direitos e defesa de seus legítimos interesses"[587]. A obrigação do Estado, prevista no artigo 144 da Constituição Federal, faz com que caibam às polícias as funções de prevenir, reprimir e apurar a prática de delitos que violem a segurança pública dos cidadãos[588].

De acordo com Ademar Borges, a concepção constitucionalmente adequada de segurança pública não a concebe como combate, mas como prestação de serviço público[589]. Nas palavras de Luís Roberto Barroso, a expressão "identifica o conjunto de instituições, políticas públicas e ações materiais voltadas à proteção da vida, da integridade física, do patrimônio e de outros direitos fundamentais das pessoas contra condutas ilegais ou criminosas"[590]. Guilherme de Souza Nucci ressalta que segurança pública diz respeito ao bem-

---

[586]Data Privacy Brasil. Proteção de Dados no Campo Penal e de Segurança Pública: Nota Técnica sobre o Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Investigação Criminal. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2020/12/NOTA-T%C3%89CNICA-PROTE%C3%87%C3%83O-DE-DADOS-NO-CAMPO-PENAL-E-DE-SEGURAN%C3%87A-P%C3%9ABLICA-VF-31.11.2020.pdf. Acesso em: 23 de set. 2024.

[587]S1LVA, José Afonso da. Curso de Direito Constitucional Positivo. São Paulo: RT, 6' ed., 1990, p. 650.

[588]BRASIL. Artigo 144 da Constituição Federal. *Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos: I - polícia federal; II - polícia rodoviária federal; III - polícia ferroviária federal; IV - polícias civis; V - polícias militares e corpos de bombeiros militares. VI - polícias penais federal, estaduais e distrital.* Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acessado em 05 de mai. 2024.

[589]SARMENTO, D; BORGES, A; ADAMI, E. Parecer. FILTRAGEM CONSTITUCIONAL DOS PEDIDOS DE SUSPENSÃO DE SEGURANÇA. INTERESSE PÚBLICO PRIMÁRIO QUE TUTELA DIREITOS FUNDAMENTAIS, SOBRETUDO DOS MAIS VULNERÁVEIS. LEGITIMIDADE ATIVA DA DEFENSORIA PÚBLICA COMO *CUSTUS VULNERABILIS.* Brasil.

[590]STF, ADPF 635-MC-ED, Tribunal Pleno, Rel. Min. Edson Fachin, J. 03.02.2022, DJe 03.06.2022.

estar social, associado à paz e à ordem da comunidade em várias acepções e vários aspectos, sendo certo que essa modalidade de segurança não tem por base, tão somente, o combate ao crime[591].

Ao tratar sobre essa temática, Cláudio Pereira da Souza Neto descreve, com precisão, os atributos da nova referência de segurança pública adotada pela Constituição de 1988:

> O cidadão é o destinatário desse serviço. Não há mais "inimigo" a combater, mas cidadão para servir. A polícia democrática, prestadora que é de um serviço público, em regra, uma polícia civil, embora possa atuar uniformizada, sobretudo no policiamento ostensivo. A polícia democrática não discrimina, não faz distinções arbitrária: trata os barracos nas favelas como "domicílios invioláveis", respeita os direitos individuais, independentemente de classe, etnia e orientação sexual; não só se atém aos limites inerentes ao Estado democrático de direito, como entendo que o seu papel é promove-lo. A concepção democrática estimula a participação popular na gestão de segurança pública; valoriza os arranjos participativos e incrementa a transparência das instituições policiais. Para ela, a função da atividade policial é gerar "coesão social", não pronunciar antagonismos; é propiciar um contexto adequado à cooperação entre cidadãos livres e iguais. O combate militar é substituído pela prevenção, pela integração com políticas sociais, por medidas administrativas de redução dos riscos e pela ênfase na investigação criminal. A decisão de usar a força passa a considerar não apenas os objetivos específicos a serem alcançados pelas ações policiais, mas também, e fundamentalmente, a segurança e o bem-estar da população envolvida[592].

No Brasil, diferentemente da Alemanha, é possível aferir que os Tribunais não utilizam os mesmos parâmetros para a definição dos fundamentos do *mínimo existencial*. É comum o Estado invocar o princípio da *reserva do possível* para negar prestações demandadas como sendo de conteúdo do mínimo existencial. Os Tribunais entendem que nos casos em que o pedido se fundamenta no direito ao *mínimo existencial*, não se admite a incidência do princípio da *reserva do possível*[593].

---

[591]NUCCI, G. de S. Direitos humanos versus segurança pública. Rio de Janeiro: Forense, 2016. p. 49.

[592]SOUZA NETO, C. P. de. A segurança pública na Constituição Federal de 1988: conceituação constitucionalmente adequada

[593]De acordo com a ADPF 45 MC/DF de 29 de abril de 2004, de relatoria do Min. Celso de Mello e que se tornou entendimento pacífico na Corte "a limitação de recursos existe e é uma contingência que não se pode negar [...]. Por outro lado, não se pode esquecer que a finalidade do Estado ao obter recursos, para em seguida, gastá-los sob a forma de obras, prestação de serviços, ou qualquer outra política pública, é exatamente realizar os objetivos fundamentais da Constituição. A meta das Constituições modernas, e da Carta de 1988 em particular, pode ser resumida [...] na promoção do bem-estar do homem, cujo ponto de partida está em assegurar as condições de sua própria dignidade, que inclui, além da proteção dos direitos individuais, condições materiais mínimas de existência. Ao apurar os elementos fundamentais dessa dignidade (mínimo existencial), estar-se-ão estabelecendo exatamente os alvos prioritários dos gastos públicos. Apenas depois de atingi-los é que se poderá discutir, relativamente aos recursos remanescentes, em quais outros projetos dever-se-á investir. O mínimo existencial, como se vê, associado ao estabelecimento de prioridades orçamentárias, é capaz de conviver produtivamente com a reserva do possível". Disponível em: http://www.stf.jus.br/arquivo/informativo/documento/informativo345.htm. Acessado em 05 de mai. 2024.

Nesse caso, portanto, caso ocorra uma omissão ou inércia do Poder Público, o Judiciário pode, de forma excepcional, determinar, de fora coercitiva, a implementação da política pública que implemente o direito fundamental almejado. Nos dias de hoje, essa prática é conhecida como ativismo judicial que, de certo modo, pode ser visto de forma positiva, quando satisfaz um direito fundamental não concretizado. A prática, porém, pode ser compreendida como violação aos princípios da separação dos poderes e do Estado de direito.

Importante fazer essas observações, porque a proteção de dados pessoais no contexto da persecução penal fará com que os operadores do direito reflitam sobre a necessidade da busca pela efetividade e concretização do direto constitucional à Segurança Pública, refletindo na valoração das provas no processo penal brasileiro, o que pode surtir efeitos em toda a cadeia de custódia penal. Uma prova colhida em um banco de dados de uma polícia judiciária brasileira, fere o princípio fundamental da proteção de dados pessoais? Como eventual Lei Geral Penal de Proteção de Dados pode prever essa hipótese?

Percebe-se que o debate não gira em torno somente do aparente conflito de normas entre vários direitos fundamentais, tais como privacidade, proteção de dados pessoais e segurança pública, afetando diretamente a produção de provas, o que pode influenciar no resultado do processo penal. De acordo com Gustavo Badaró, a atividade probatória de ser compreendida como (i) investigação; (ii) instrução; (iii) valoração; (iv) decisão e (v) justificação[594].

O postulado constitucional da proporcionalidade deve permear todo o procedimento investigativo, de forma que a validade das provas colhidas durante a investigação policial seja inquestionável no que diz respeito à idoneidade no momento em que foram coletadas. Aqui cabe estabelecer uma diferença entre meios de prova e meios de obtenção de provas. Enquanto o primeiro se caracteriza como instrumento de introdução dos dados probatórios no processo, os meios de obtenção de provas são fontes ou elementos de provas que em um momento posterior poderão ser levadas ao processo.

Os meios de obtenção de provas são aqueles específicos para certos tipos de procedimentos que comumente são extraprocessuais. Podemos citar como exemplos as buscas

[594]BADARÓ, Gustavo Henrique. Epistemologia judiciária e prova penal. São Paulo: Thompson Reuters. Brasil, 2019. p. 127.

e apreensões, as interceptações telefônicas, as quebras de sigilo, a confissão e as provas periciais. Gustavo Badaró preceitua que os meios de provas são aptos a servir, diretamente, ao convencimento do juiz sobre a veracidade ou não de uma afirmação fática[595]. Como exemplo, o referido autor menciona o depoimento de uma testemunha ou o teor de uma escritura pública. Os meios de obtenção de prova são os instrumentos para a colheita de elementos ou fontes de provas, aptos a convencer o julgador. Enquanto o meio de prova se presta ao convencimento direto do julgador, os meios de obtenção de provas somente indiretamente, e dependendo do resultado de sua realização, poderão servir à história dos fatos.

É inegável que a utilização de dados pessoais na persecução penal é de extrema importância para o ordenamento jurídico brasileiro. A ausência de regulamentação do uso de dados pessoais para fins penais pode fazer com que as provas colhidas nas investigações criminais sejam questionadas, porque está em jogo um aparente conflito de direitos fundamentais. Para Guilherme Peña de Moraes[596], a colisão de direitos fundamentais *lato sensu* é fracionada em dois tipos. A primeira é a colisão de direitos fundamentais *stricto sensu* e a segunda colisão de direitos fundamentais e outros valores constitucionais. No caso da colisão de direitos fundamentais *stricto sensu*, o exercício de um direito fundamental por parte de um titular colide com o exercício de direito fundamental, idêntico ou diverso, por parte do outro titular. Por outro lado, na colisão de direitos fundamentais e outros valores constitucionais é exteriorizada na hipótese em que o exercício de um direito fundamental colide com a necessidade de preservação de bens jurídicos protegidos constitucionalmente.

Isso demonstra que nenhum direito fundamental pode ser absoluto, o que reforça o pensamento de que esse conflito de direitos fundamentais é tão somente aparente, porque na prática sempre haverá uma solução para cada caso concreto. No caso do objeto do presente estudo, o conflito de direitos fundamentais é, de fato, aparente, porque não é cabível que alguém cometa um ilícito penal, seja ele qual for, e depois tente alegar que a investigação para apuração do delito praticado deve ser questionada, em detrimento de eventual violação aos direitos fundamentais da privacidade e da proteção de dados pessoais. Isso não seria razoável. Diante

[595]BADARÓ, Gustavo Henrique. Epistemologia judiciária e prova penal. São Paulo: Thompson Reuters. Brasil, 2019. p. 127.
[596]MORAES, Guilherme Braga Peña de. Direitos Fundamentais: Conflitos e Soluções. Niterói – RJ, Labor Juris, 2000, p. 91.

disso, é possível afirmar que prevalece a tese da relatividade dos direitos fundamentais, respeitados os princípios da razoabilidade e da proporcionalidade.

Nesse sentido, o postulado da proporcionalidade encontra algumas divergências, porque para alguns autores ele não deve ser confundido com razoabilidade. Inclusive, é preciso ressaltar que no que diz respeito à expressão "princípio da razoabilidade", não há um consenso, já que a proporcionalidade ora é tratada como princípio, regra ou postulado. Segundo Marcelo Novelino, a proporcionalidade deve ser tratada como um postulado, por ser considerada uma "metanorma que prescreve o modo de raciocínio e de argumentação relacionado às normas restritivas de direitos fundamentais"[597].

O estudo do postulado da proporcionalidade é composto pela adequação, necessidade e proporcionalidade em sentido estrito (também denominada de ponderação). A adequação deve ser compreendida como a análise do meio empregado e do objetivo a ser alcançado. Tanto a análise do meio empregado quanto o objetivo a ser alcançado devem ser legítimos, ou seja, quando estivermos diante de uma medida restritiva de direitos fundamentais, para que ocorra uma efetividade do uso da proporcionalidade, é preciso que a medida restritiva seja legítima. Caso uma determinada medida atrapalhe a realização do suposto princípio, mostrando-se ineficiente para a fomentação de outro princípio determinado, não restará dúvidas de que a intervenção é inapropriada.

A intervenção só será legítima se a forma utilizada for precisa e juridicamente permitida. No caso em tela, podemos citar como exemplo a utilização de dados pessoais dos bancos de dados das policiais judiciárias brasileiras, o que geralmente ocorre sem autorização judicial. Nesse caso, o objetivo é legítimo, porque se pretende investigar a prática de um fato criminoso. Diante da urgência de uma resposta efetiva que o momento requer, o acesso aos dados pessoais é feito sem que o titular de dados tome ciência, já que se isso acontecer, o investigado pode tentar destruir provas e atrapalhar a investigação. Aqui também estamos diante de um objetivo legítimo. Os dados pessoais utilizados na investigação não podem, porém, ser repassados para terceiros ou utilizados para fins que não estejam relacionados à investigação policial em curso, o que tornaria o método ilegítimo.

[597]NOVELINO, Marcelo. Curso de Direito Constitucional. Salvador: JusPodivm. 2017, p. 302.

Sobre a necessidade, segundo componente do postulado da proporcionalidade, é preciso ressaltar que existe uma obrigação para que, de todas as formas que podem ser utilizadas para se alcançar o objetivo pretendido, seja aplicada, na medida do possível, aquela que seja menos invasiva. Ainda nas palavras de Marcelo Novelino, "uma medida deve ser considerada desproporcional quando for constatada, de forma inequívoca, a existência de outra menos onerosa e com semelhante eficácia"[598]. Em outras palavras, é preciso verificar se a existência de medias alternativas similares serão eficazes para fomentar o fim pretendido. Posteriormente, será preciso analisar se as medidas serão menos danosas que a medida efetivamente adotada.

Já na proporcionalidade em sentido estrito (ou ponderação), há a exigência de uma medida proporcional, onde os benefícios obtidos por meio da intervenção justifiquem o ônus imposto ao indivíduo que teve o seu direito fundamental mitigado, de modo que não ocorra um desequilíbrio excessivo entre os meios e os fins. Para Robert Alexy, a proporcionalidade em sentido estrito corresponde à lei material do sopesamento, segundo a qual "quanto maior for o grau de não satisfação ou de afetação de um princípio, tanto maior terá que ser a importância da satisfação do outro"[599].

Nesse caso, não é necessário que a medida restritiva de determinado princípio fomente outro princípio em grau máximo, mas que busque um ponto de equilíbrio entre eles. A otimização em relação aos princípios que estão em colisão recebe o nome de sopesamento. Ainda de acordo com Alexy, para que isso ocorra é preciso seguir as seguintes etapas: análise da intensidade na intervenção no princípio afetado; verificação do grau de importância da satisfação do princípio promovido; e avaliação da satisfação do princípio fomentado em face da intervenção no princípio restringido[600].

A escala de satisfação do princípio que deve prevalecer e de intervenção do princípio contraposto pode ser construída em três níveis. São eles o leve, o moderado e o sério. Quando dois princípios tiverem peso abstrato igual e o grau de afetação ou não satisfação de um princípio for maior que o grau de satisfação de outro, a medida não passará pelo teste da proporcionalidade em sentido estrito. Em sentido contrário, quando dois princípios tiverem

[598]NOVELINO, Marcelo. Curso de Direito Constitucional. Salvador: JusPodivm. 2017, p. 303.
[599]ALEXY, Robert. *Teoria dos direitos fundamentais.* Tradução Virgílio Afonso da Silva. 2ª ed. São Paulo: Malheiros, 2012. p. 247.
[600]*Ibid.*

peso abstrato igual e da intervenção em um princípio for menor que o grau de satisfação do outro, a medida passará pelo teste da proporcionalidade em sentido estrito.

Outro ponto importante e que merece ser ressaltado é a distinção entre a proporcionalidade e a razoabilidade, que são tratados de forma uniforme pelo Supremo Tribunal Federal e por uma grande parte da doutrina no Brasil. Apesar disso, o postulado da proporcionalidade é diferente da razoabilidade por motivos de origem e de forma de aplicação. Enquanto na proporcionalidade existe uma relação de causalidade entre o meio e o fim, o que exige dos poderes públicos a escolha mais adequada para atingir um fim, na razoabilidade as condições pessoais e individuais dos sujeitos envolvidos são levadas em consideração.

A concorrência e a colisão de direitos fundamentais também devem ser diferenciadas, já que a primeira ocorre quando um comportamento do mesmo titular se enquadra no âmbito de proteção de mais de um direito fundamental. Segundo Marcelo Novelino, "no cruzamento de direitos fundamentais, determinado comportamento é incluído no âmbito de proteção de mais de um direito, liberdade ou garantia. Na acumulação, determinado bem jurídico leva à aglomeração de dois ou mais direitos na mesma pessoa"[601]. Já a colisão de direitos fundamentais ocorre quando dois ou mais direitos abstratamente válidos entram em conflito diante de um caso concreto.

Ademar Borges menciona que "embora não haja consenso na doutrina especializada sobre a forma de inclusão dos princípios formais no sopesamento e no princípio da proporcionalidade, é bastante difundida a ideia de que se deve atribuir ao princípio forma um peso extra no processo ponderativo"[602]. A proposta, inclusive, foi apresentada por Alexy[603] e difundida no Brasil por Paulo Gonet Branco[604]. Para essa concepção, a solução do conflito entre uma regra e um princípio exige que se coloque ao lado do princípio que fundamenta a regra o princípio formal como um peso extra resultante do postulado que exige que as regras devem ser respeitadas. Para Alexy, a inclusão de um princípio formal no sopesamento só tem sentido

[601]NOVELINO, Marcelo. Curso de Direito Constitucional. Salvador: JusPodivm. 2017, p. 308.
[602]FILHO, Ademar Borges de Sousa. O Controle de Constitucionalidade de Leis Penais no Brasil: Graus de Deferência ao Legislador, Parâmetros Materiais de Técnicas de Decisão. 2019. 702 f. Tese (Doutorado em Direito Constitucional). Universidade do Estado do Rio de Janeiro – UERJ.
[603]ALEXY, Robert. Teoria dos Direitos Fundamentais. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008, p. 105.
[604]BRANCO, Paulo Gustavo Gonet. Juízo de Ponderação na Jurisdição Constitucional: Pressupostos de Fato e Teóricos Reveladores do seu Papel e do seu Limite. 2008. 393 f. Tese (Doutorado em Direito). Universidade de Brasília – UNB.

se ele estiver conectado a um princípio material, pois a restrição de direitos fundamentais não pode se justificar unicamente com base em argumentos formais[605].

Daniel Sarmento faz a distinção entre princípios e regras jurídicas e estabelece critérios de resolução das tensões entre princípios constitucionais, utilizando, para isso, a ponderação de bens[606]. De acordo com o autor, os princípios constituem os mandamentos nucleares do sistema jurídico, irradiando seus efeitos sobre diferentes normas e servindo de balizamento para a interpretação e integração de todo o setor do ordenamento em que radicam. Continua dizendo que os princípios se revestem de um grau de generalidade e de abstração superior ao das regras, sendo, por consequência, menor o seu raio de aplicação.

Ainda de acordo com o Daniel Sarmento, dentro do sistema jurídico os princípios passam por um processo de concretização e densificação sucessiva, através de princípios mais específicos e subprincípios, até adquirirem a concretização o das regras[607]. Outra distinção relevante é que os princípios, por ausência do grau de concretização, não permitem a subsunção. O conflito entre regras é resolvido de modo completamente diverso do conflito entre princípios, já que no primeiro caso só pode ser solucionado através da introdução de uma cláusula de exceção (regra mais especial regulará o caso em detrimento da regra mais geral)[608], ou mediante o reconhecimento da invalidade de alguma das regras confrontadas.

Claudio Pereira de Souza Neto, quando escreveu sobre jurisdição constitucional e democracia, mencionou que diante da vagueza e abertura de boa parte das normas constitucionais, bem como da possibilidade de que elas entrem em colisões, quem as interpreta e aplica também participa do seu processo de criação. O Autor também fez uma crítica ao afirmar que "a jurisdição constitucional acaba por conferir aos juízes uma espécie de "poder constituinte permanente" pois lhes permite moldar a Constituição de acordo com as suas preferências políticas e valorativas, em detrimento daquelas adotadas pelo legislador eleito"[609].

---

[605]ALEXY, Robert. Teoria dos Direitos Fundamentais. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008, p. 431.
[606]*Ibid.*
[607]*Ibid.*
[608]*Ibid.*
[609]SOUZA NETO, Claudio Pereira de; SARMENTO, Daniel. NOTAS SOBRE JURISDIÇÃO CONSTITUCIONAL E DEMOCRACIA: A QUESTÃO DA"ÚLTIMA PALAVRA" E ALGUNS PARÂMETROS DE AUTOCONTENÇÃO JUDICIAL: A EXPANSÃO DA JURISDIÇÃO CONSTITUCIONAL E A CHAMADA "DIFICULDADE CONTRAMAJORITÁRIA". Disponível em: file:///C:/Users/Usuario/Downloads/acrb,+6+-+Jurisdi%C3%A7%C3%A3o+constitucional+e+democracia_Daniel+Sarmento.pdf. Acesso em 24 de sete. 2024.

No caso do conflito entre princípios, não se desenrola no campo da validade, mas sim na dimensão do peso, já que há uma hierarquia entre princípios, pois a prevalência de cada um deles na solução do problema jurídico dependerá das circunstâncias específicas do caso concreto. Necessária fazer essa observação, porque os princípios constitucionais não são apenas aqueles previstos na Constituição Federal, mas também os que estão implícitos e que também podem entrar em colisão com os princípios expressamente previstos.

Regras, portanto, são mais específicas e determinam o que pode e o que não pode ser feito, diante de um determinado contexto social. Já os princípios são diretrizes mais abstratas que servem para orientar a interpretação e a aplicação das normas. Isso significa dizer que os princípios não são tão específicos como as regras e possuem um grau de generalidade e abstração mais elevado. Os princípios são vistos como mandados de otimização, porque ordenam que algo seja, na medida do possível, realizado dentro das possibilidades jurídicas e reais existentes.

Essa diferenciação se faz necessária, para que seja possível compreender a ponderação de bens e o grau de intervenção nos direitos humanos, diante da mitigação ao direito fundamental da proteção de dados no contexto do direito penal, mais especificamente durante a investigação criminal propriamente dita. Conforme foi possível aferir anteriormente, a resolução de um conflito entre princípios constitucionais necessita de uma análise da situação concreta que emergiu o conflito.

Para Daniel Sarmento, "o equacionamento das tensões principiológicas só pode ser empreendido à luz das variáveis fáticas do caso, as quais indicarão ao intérprete o peso específico que deve ser atribuído a cada cânone constitucional em confronto. E a técnica de decisão que, sem perder de vista os aspectos normativos do problema, atribui especial relevância às suas dimensões fáticas, é o método de ponderação de bens"[610]. O método da ponderação de bens está intimamente ligado ao de hermenêutica constitucional da "concordância prática de Canotilho, que impõe a coordenação e combinação dos bens jurídicos em conflito ou em concorrência de forma a evitar o sacrifício (total) de uns em relação a outros[611].

[610]SARMENTO, Daniel. Teoria dos Direitos Fundamentais. 2ª ed. Rio de Janeiro: Renovar, 2001, p. 55.
[611]*Ibid.*

No momento em que for aplicada a ponderação de bens, o julgador deve, inicialmente, aferir se o caso concreto está, de fato, na esfera de proteção de mais de um princípio. Caso isso seja confirmado, o intérprete fará compressões recíprocas sobre os bens jurídicos protegidos pelos princípios em disputa, com a finalidade de alcançar a medida em que a restrição a cada bem seja a mínima indispensável, o que dependerá de cada caso concreto, onde deve imperar a lógica do razoável. No caso do estudo em questão, o razoável é que em caso de eventual análise da ponderação de bens entre a proteção à privacidade e aos dados pessoais do investigado e a proteção dos interesses da coletividade, abrangidos pela proteção da segurança e da ordem pública, esses devem prevalecer.

O Direito Alemão criou um método para aferir a constitucionalidade de uma intervenção em direitos fundamentais. A primeira etapa passa pela identificação do direito fundamental afetado. Posteriormente, é necessário aferir em que circunstâncias esse direito fundamental será atingido, para que a justificativa dessa intervenção encontre amparo na Constituição Federal. É preciso verificar se a intervenção utilizada pode alcançar o fim almejado, se não há método menos danoso para atingir o mesmo objetivo e, por fim, se o direito fundamental escolhido deve prevalecer sobre o direito fundamental postergado[612].

O próprio Supremo Tribunal Federal utiliza a técnica da ponderação como instrumento da resolução de conflitos de interesses, quando há colisão entre Direitos Fundamentais:

> Em síntese, a aplicação do princípio da proporcionalidade se dá quando verificada restrição a determinado direito fundamental ou um conflito entre distintos princípios constitucionais de modo a exigir que se estabeleça o peso relativo de cada um dos direitos por meio da aplicação das máximas que integram o mencionado princípio da proporcionalidade. (Intervenção Federal n. 2.257-6/SP, Rel. Ministro Gilmar Mendes, Pleno)[613].

Nesse sentido, o Superior Tribunal de Justiça entendeu que a colisão entre o direito coletivo à Segurança e o direito à apuração e à punição de quem tenha violado a Lei Penal bem como outros Direitos Fundamentais constitucionalmente assegurados deve partir da seguinte percepção:

---

[612]SARLET, Ingo Wolfgang. A Lei Fundamental da Alemanha nos seus 60 anos e o Direito Constitucional Brasileiro: Algumas Aproximações. Direitos Fundamentais e Justiça. Nº 7 – ABR.JUN. 2009.
[613]STF, Intervenção Federal 22576, Tribunal Pleno, Rel. Min. Gilmar Mendes, J. 12.08.2002, DJe 19.08.2002.

> A segurança é um bem protegido pela Constituição Federal de 1988 e constitui, também, um direito fundamental da pessoa. Situada no mesmo nível dos demais direitos fundamentais, se em conflito com outros direitos fundamentais, a segurança é um direito que pode ser levado à balança da ponderação. O seu "peso", avaliado no caso concreto, poderá, dependendo das circunstâncias, fazê-la preponderar sobre outros direitos ou bens constitucionalmente protegidos. (PRADO, Fabiana Lemes Zamalloa do. A ponderação de interesses em matéria de prova no processo penal. São Paulo: IBCCRIM, 2006, p. 196-197)[614].

Diante de tudo o que foi mencionado até agora, percebe-se que a colisão de princípios constitucionais ou direitos fundamentais não pode ser resolvida mediante emprego dos critérios tradicionais de solução de conflito de normas, como o hierárquico, o temporal e o da especialização. O intérprete deve utilizar a ponderação de normas, valores ou interesses, devendo fazer concessões recíprocas entre as pretensões em disputa, preservando o máximo do conteúdo de cada uma. Nos casos extremos, deverá escolher qual critério deve prevalecer e qual será sacrificado, devendo fundamentar racionalmente a adequação constitucional de sua decisão[615].

Nas palavras de Nina Nery, "caberá ao Poder Judiciário, norteado por parâmetros legais claros, autorizar e controlar a intervenção, fixando limites que, para além dos critérios em abstrato previstos em lei, estejam de acordo com o fato determinado ensejador da violação do direito fundamental"[616]. Caberá ao Poder Legislativo fixar os critérios para que a atuação dos órgãos de persecução penal não ultrapasse as barreiras e ao Judiciário a avaliação do caso concreto, parra aferir se estão dentro das balizas previstas em lei. Observadas essas medidas, a dignidade não será atingida, ainda que ocorra um clamor público por um "*direito fundamental à segurança pública*"[617].

---

[614]STJ, RMS 61.302-RJ, Terceira Seção, Rel. Min. Rogerio Schietti Cruz, J. 26.08.2020, DJe 04.09.2020.
[615]Barroso, L. R. (2004). Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa. *Revista De Direito Administrativo*, *235*, 1–36. https://doi.org/10.12660/rda.v235.2004.45123
[616]NERY, Nina. O compartilhamento de dados financeiros no sistema antilavagem de dinheiro brasileiro. São Paulo: Thompson Reuters Brasil, 2024. p. 106.
[617]*Ibid. p. 114.*

CONCLUSÃO

Os bancos de dados das Polícias Judiciárias Brasileiras enfrentam uma série de problemas complexos, que começaram a surgir com o advento da Lei Geral de Proteção de Dados e com a elevação da proteção de dados pessoais ao patamar de direito fundamental, previsto em nossa Constituição Federal. Nesse sentido, destaca-se a ausência de dispositivo legal que autorize o armazenamento de dados pessoais para fins penais, acrescido da falta de mecanismos para a utilização desses dados, bem como sobre a indefinição de prazo para que os dados permaneçam armazenados.

A ponderação entre o direito à proteção de dados e à persecução penal, bem como a utilização dos dados armazenados pelas Polícias Judiciárias Brasileiras, é um tema de grande relevância e complexidade no cenário atual. O avanço da tecnologia e a utilização cada vez mais intensa dos meios eletrônicos e digitais trouxeram à tona a discussão sobre proteção dos dados pessoais e a privacidade dos indivíduos, especialmente em relação às investigações criminais, demonstrando que o direito carece da adaptação dos seus institutos às novas condições atuais.

Embora a transformação tecnológica nos traga inúmeros benefícios, os riscos com a exposição dos nossos dados pessoais são inevitáveis. Um dos principais teóricos do Direito, Ronald Dworkin, aborda a questão da ponderação de direitos. Esse autor defende que a ponderação é uma técnica que deve ser utilizada quando há conflitos entre princípios, a fim de encontrar a solução mais justa e equilibrada para o caso concreto[618]. Dworkin entende que a ponderação não pode ser utilizada de forma arbitrária, mas deve ser fundamentada em princípios e valores jurídicos.

No contexto brasileiro, a Lei Geral de Proteção de Dados (LGPD) foi promulgada em 2018 e entrou em vigor em 2020. A LGPD, porém, não garantiu a proteção de dados pessoais no âmbito da persecução penal, deixando claro que o tratamento de dados pessoais não seria realizado para fins exclusivos de segurança pública, defesa nacional, segurança de Estado ou

[618]DWORKIN, Ronald. Uma questão de princípio. Trad. Luis Carlos Borges. 2a . ed. São Paulo: Martins Fontes, 2005.

atividades de investigação e repressão de infrações penais. Essa proteção foi descrita na exposição de motivos do Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal, através de ato do Presidente da Câmara dos Deputados, ocorrido no dia 26 de dezembro de 2019.

O Anteprojeto teve a intenção de regulamentar o Artigo 4º, caput, inciso III, alíneas "a" e "d" c/c §1º, da Lei n. 13.709/2018 (LGPD), de forma a garantir a proteção de dados pessoais no âmbito da persecução penal, estabelecendo regras claras e específicas para o tratamento de dados pessoas pelos órgãos responsáveis pela investigação criminal e pela aplicação da lei.

A norma intitulada Lei de Proteção de Dados para a Segurança Pública e Persecução Penal prevê que o tratamento de dados pessoais pelas autoridades competentes deve ser realizado de forma transparente, tendo como fundamentos a dignidade, os direitos humanos, o livre desenvolvimento da personalidade, o exercício da cidadania pelas pessoas naturais, a autodeterminação informativa, o respeito à vida privada e à intimidade, a liberdade de manifestação do pensamento, de expressão, e informação de comunicação, de opinião , a presunção de inocência, a confidencialidade, a integridade dos sistemas informáticos e pessoais, a garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal, respeitando, conforme já mencionado acima, os princípios da licitude, finalidade, adequação, necessidade, proporcionalidade, livre acesso, qualidade dos dados, transparência, segurança da informação, prevenção, não discriminação, responsabilização e prestação de contas.

No entanto, a aplicação da LGPD Penal na prática ainda é um desafio. O Anteprojeto encontra-se parado na Câmaras dos Deputados, aguardando a passagem por todos os trâmites legais para que, enfim, possa de fato virar lei. Além disso, há um intenso debate sobre a constitucionalidade de diversos artigos do referido Anteprojeto, tais como a transformação do Conselho Nacional de Justiça (CNJ), em órgão de controle de acesso aos dados pelos profissionais da segurança pública, bem como de outras medidas, que podem envolver a coleta e o tratamento de dados pessoais sensíveis na esfera criminal.

Cabe salientar que o Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Persecução Penal possui algumas diferenças em relação ao *General Data Protection Regulation*, legislação europeia de proteção de dados. Uma das principais diferenças é que o

referido Anteprojeto prevê a possibilidade de punição criminal para os responsáveis pelo tratamento ilícito de dados pessoais, ao passo que o GDPR se limita a punições administrativas e financeiras.

A ideia de que o direito à segurança pública e ao bem estar da coletividade deve prevalecer nas investigações policiais, precisa ser vista com muita cautela, já que em muitas ocasiões, com a justificativa de "garantia da ordem pública", direitos fundamentais da pessoa humana acabam sendo desrespeitados[619]. A segurança pública é um serviço público que deve ser universalizado de maneira igualitária, incidindo a dupla aplicação do *princípio republicano*, onde, do ponto de vista da população, exige-se a implementação da segurança pública de forma impessoal, objetiva e imparcial, impondo-se, sob o ponto de vista dos agentes públicos, o dever de *accountability* e a possibilidade de sua responsabilização[620]. A segurança pública, portanto, não pode ser promovida às custas de parcela dos direitos da população, já que é preciso adoção de medidas que conciliem o enfrentamento ao crime com a proteção de direitos[621].

A utilização dos bancos de dados pelas Polícias Judiciárias Brasileiras não demonstra contornos de inconstitucionalidade, porque o que se busca com a utilização das informações armazenadas é a proteção do direito fundamental da segurança pública e de outros direitos fundamentais, tais como vida, propriedade etc. No entanto, existe uma omissão que seve ser suprida pelo legislador, com menos espaço discricionário para a utilização dos dados pessoais armazenados e com a implementação de um protocolo que faça a fiscalização e o monitoramento do acesso aos dados acessados ou utilizados. A inexistência de previsão legal e a falta de autorização judicial prévia para a utilização dos bancos de dados em questão pode gerar o aumento na má utilização dos dados, conforme exemplos citados ao longo deste trabalho.

---

[619]SILVA, J. A. da. Curso de Direito Constitucional Positivo. São Paulo: Malheiros, 2022. P. 791.

[620]Sobre o princípio republicano na ordem constitucional brasileira, cf. SARMENTO, D. O princípio republicano nos 30 anos da Constituição de 88: por uma República inclusiva, Revista da Emerj, v. 20, n. 3, p. 296-318, set./dez. 2018. Sobre a incidência do princípio republicano na implementação igualitária de segurança pública, cf. SOUZA NETO, C. P. de. A segurança pública na Constituição Federal de 1988: conceituação constitucionalmente adequada, competências federativas e órgãos de execução das políticas. In: SOUZA NETO, C. P. de. Constitucionalismo democrático e governo das razões. Rio de Janeiro: Lumen Juris, 2011. P. 280-283.

[621]SARMENTO, D; BORGES, A; ADAMI, E. Parecer. FILTRAGEM CONSTITUCIONAL DOS PEDIDOS DE SUSPENSÃO DE SEGURANÇA. INTERESSE PÚBLICO PRIMÁRIO QUE TUTELA DIREITOS FUNDAMENTAIS, SOBRETUDO DOS MAIS VULNERÁVEIS. LEGITIMIDADE ATIVA DA DEFENSORIA PÚBLICA COMO *CUSTUS VULNERABILIS*. Brasil.

A principal discussão aqui aventada é se há, de fato, a necessidade da restrição, ou até mesmo do abandono, de direitos constitucionais conquistados com muita luta e legitimidade, como intimidade e privacidade, por exemplo, para termos uma melhor proteção do Estado e da segurança pública dos indivíduos.

Espera-se, portanto, que o Poder Legislativo supra essa lacuna e edite dispositivo legal específico para o tratamento de dados na persecução penal. Uma vez implementada a legislação, no entanto, as polícias não podem ter liberdade para fazerem o que quiserem. Seguindo preceitos constitucionais, é preciso que as novas diretrizes legais estabeleçam uma série de requisitos legais para que os dados pessoais sejam utilizados com o mínimo de restrição aos direitos fundamentais.

Nesse sentido, respondendo as indagações aventadas na introdução deste trabalho, é preciso ressaltar que as Polícias Judiciárias Brasileiras podem utilizar os seus bancos de dados, desde que exista autorização legal específica.

A ponderação entre o direito à proteção de dados e a persecução penal, que deve ser feita pelo legislador e pelo judiciário, precisa ser realizada com base em princípios e valores jurídicos, como defende Ronald Dworkin[622]. O Anteprojeto da LGPD Penal representa um avanço significativo na proteção dos dados pessoais no âmbito da investigação criminal, mas ainda é preciso que as autoridades e instituições se adaptem e apliquem adequadamente suas disposições. Isso não significa dizer que o Anteprojeto esteja pronto e acabado para ser implementado.

Tudo que foi mencionado até aqui, nos faz acreditar que o respeito aos Direitos Fundamentais seve ser a regra e a restrição a exceção. A alegação de que não existem direitos absolutos não pode servir como pano de fundo para obstar direitos constitucionais conquistados a duras penas. Por isso, é urgente a necessidade de regulamentação específica quanto à utilização dos bancos de dados das Polícias Judiciárias brasileiras, estabelecendo os agentes autorizados a compartilhar e requisitar dados, os tipos de dados que serão necessários para cada investigação policial e o devido monitoramento ao acesso desses bancos de dados. Nas palavras de Orlandino Gleizer, a Lei deve fixar “obstáculos interventivos”, exigindo a presença de

[622] *Ibid.*

perigos concretos para as atividades de segurança ou suspeitas iniciais para as atividades de persecução penal[623].

Apesar da Lei Geral de Proteção de Dados excluir a sua aplicação nas hipóteses em que a coleta, o tratamento e a disseminação de dados ocorram para fins de segurança pública, é preciso observar que a investigação criminal e a repressão de infrações penais deve respeitar os princípios previstos na LGPD. A elevação da proteção de dados ao patamar de Direito Fundamental tornou inafastável a ponderação desse direito em quaisquer circunstâncias, incluindo, portanto, os casos em que a manipulação de informações pessoais se dá no âmbito da atuação de órgãos da persecução penal[624].

Um Estado que verdadeiramente se preocupa com o livre desenvolvimento da personalidade dos seus cidadãos, deve assegurar condições para que o indivíduo não seja alvo de irrestritas faculdades de obtenção, armazenamento, utilização e transferência de sus dados pessoais[625]. O estudo em questão é mais diretivo que definitivo, porque ainda há muitas questões legislativas e judiciais a serem esclarecidas. O tratamento de dados pessoais para fins penais necessita de um controle legal e constitucional, diante das restrições que pode gerar aos direitos fundamentais. Até que a Lei Geral Penal de Proteção de Dados seja, de fato, promulgada, é possível que ocorram outras alterações, com debates mais aprofundados sobre a compatibilidade do Anteprojeto e com a implementação de normas de autorizadoras de acesso a bancos de dados, a fim de garantir a proteção dos dados pessoais, a privacidade dos indivíduos e a segurança pública, o que deve ser feito de forma equilibrada e justa.

---

[623]GLEIZER, Orlandino. A proteção de dados por duas portas nas intervenções informacionais. A declaração de inconstitucionalidade pelo Tribunal Federal Constitucional alemão de regras garantidoras de acesso estatal a dados constitutivos de serviços de telecomunicação (Bestandsdatenauskunft II). Revista de Estudos Criminais, São Paulo, v. 19, n. 79, 2020, p. 217.

[624]NERY, Nina. O compartilhamento de dados financeiros no sistema antilavagem de dinheiro brasileiro. São Paulo: Thompson Reuters Brasil, 2024. p. 81.

[625]DONEDA, Danilo. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. Pensar, Fortaleza, v. 23, n.4, 2018, p. 4.

REFERÊNCIAS

Agência Brasil. CGU investigará policiais por suposta participação na "Abin paralela". Disponível em: https://agenciabrasil.ebc.com.br/radioagencia-nacional/geral/audio/2024-04/cgu-investigara-policiais-por-suposta-participacao-na-abin-paralela. Acessado em 01 de mai. 2024.

Agência Brasileira de Inteligência. Contrainteligência. Disponível em: <https://www.gov.br/abin/pt-br/assuntos/inteligencia-e-contrainteligencia/CI>. Acessado em: 13 de ago. 2024.

Agência Brasileira de Inteligência. Doutrina Nacional de Inteligência. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023>. Acessado em: 13 de ago. 2024.

Agência Brasil. Legislação de proteção de dados já é realidade em outros países. Disponível em: https://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises. Acesso em 28 de 0ut. 2024.

Agência Câmara dos Deputados. Estudo mostra que projetos sobre penas mais duras geram distorções. Disponível em: https://www.camara.leg.br/noticias/224214-estudo-mostra-que-projetos-sobre-penas-mais-duras-geram-distorcoes/. Acessado em 22 de set. 2024.

Agência Pública. Com milhares de usuários civis e militares, sistema Córtex do Ministério da Justiça explodiu desde o governo Bolsonaro. Disponível em: https://apublica.org/2024/10/vigilancia-55-mil-agentes-podem-monitorar-alvos-sem-justificativa/. Acesso em 14 de out. 2024.

ALEXY, Robert. *Teoria dos direitos fundamentais.* Tradução Virgílio Afonso da Silva. 2ª ed. São Paulo: Malheiros, 2012.

ALVES SILVA, Amanda Cristina; SANTOS, Jéssica Guedes. Portal de Periódicos do IDP. COMPARTILHAMENTO INTERNACIONAL DE DADOS PARA SEGURANÇA PÚBLICA: PARARELO LEGISLATIVO ENTRE BRASIL E PORTUGAL. Disponível em: file:///C:/Users/Usuario/Downloads/6230-Texto%20do%20Artigo-18861-20303-10-20220130.pdf. Acesso em 04 de nov. 2024.

ANDRADE José Carlos Vieira. Direitos Fundamentais na Constituição Portuguesa de 1976. 3ª ed. Coimbra: Almedina, 2006, p. 115.

ARAS, Vladimir. Aplicabilidade da LGPD às atividades de segurança Pública e Persecução Penal. Jota. Disponível em: https://www.jota.info/artigos/aplicabilidade-da-lgpd-as-atividades-de-seguranca-publica-e-persecucao-penal. Acesso em 25 de nov. 2024.

Assembleia Legislativa do Espírito Santo. PL revoga mais 1.108 leis sem eficácia. Disponível em: https://www.al.es.gov.br/Noticia/2019/11/38404/pl-revoga-mais-1108-leis-sem-eficacia.html. Acesso em 06 de nov. 2024.

Autoridade Nacional de Proteção de Dados – ANPD. ANPD aprova normas sobre a atuação sobre o Encarregado pelo Tratamento de Dados Pessoais. Disponível em:

https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aprova-norma-sobre-a-atuacao-do-encarregado-pelo-tratamento-de-dados-pessoais. Acesso em 03 de nov. 2024.

Autoridade Nacional de Proteção de Dados - ANPD. ANPD aprova regulamento sobre transferências internacionais de dados. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/resolucao-normatiza-transferencia-internacional-de-dados. Acesso em 03 de set. 2024.

Autoridade Nacional de Proteção de Dados - ANPD. ANPD divulga enunciado sobre o tratamento de dados pessoais de crianças e adolescentes. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes. Acesso em 09 de set. 2024.

Autoridade Nacional de Proteção de Dados – ANPD. Guia orientativo. Tratamento de Dados Pessoais pelo Poder Público. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 29 de out. 2024.

Autoridade Nacional de Proteção de Dados. Guia Orientativo – Tratamento de Dados Pessoais pelo Poder Público. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em 11 dez. 2023.

Autoridade Nacional de Proteção de Dados - ANPD. Nota Técnica nº 175/2023/CGF/ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acessado em de junho. 2024.

Autoridade Nacional de Proteção de Dados – ANPD. Papel da ANPD, direitos dos titulares e função da ouvidoria. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/acoes-e-programas/programas-projetos-acoes-obras-e-atividades/semana-da-protecao-de-dados-2022/semana-da-protecao-de-dados-pessoais-2022-papel-da-anpd-direitos-dos-titulares-e-funcao-da-ouvidoria. Acesso em 29 de out. 2024.

Autoridade Nacional de Proteção de Dados – ANPD. Sanções Administrativas: o que muda após 1º de agosto de 2021? Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/sancoes-administrativas-o-que-muda-apos-1o-de-agosto-de-2021. Acesso em 29 de out. 2024.

BADARÓ, Gustavo Henrique. Epistemologia judiciária e prova penal. São Paulo: Thompson Reuters. Brasil, 2019. p. 127.

BADARÓ, Gustavo. Processo Penal. Rio de Janeiro: Campus, Elsevier, 2012, p. 270.

BAIÃO, Kelly C. Sampaio; GONÇALVES, Kalline Carvalho. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. Civilistica.com. Rio de Janeiro. Ano 03, nº 02, (jul. – dez.2014). [Com.25 abril 2018]. Disponível em: http://civilista.com/agarantia-da-privacidade-na-sociedade-tecnologica-um-imperativo-a-concretizacao-do-principio-da-dignidade-da-pessoa-humana/>. Acessado em 25 de abril de 2024.

BBC News Brasil. Atentados de 11 de setembro: a tragédia que mudou os rumos do século 21. Disponível em: https://www.bbc.com/portuguese/internacional-55351015. Acessado em: 01 de mai. 2024.

BARROSO, L.R. A dignidade da pessoa humana no direito constitucional contemporâneo. Belo Horizonte: Fórum, 2013.

BARROSO, L. R. (2004). Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa. *Revista De Direito Administrativo*, *235*, 1–36. https://doi.org/10.12660/rda.v235.2004.4512.

BECCARIA, Cesare. Dos Delitos e das Penas. São Paulo: Editora Martin Claret, 2000.

BELLO FILO, Ney de Barros. A dimensão subjetiva e a dimensão objetiva da norma de direito fundamental ao ambiente. Revista do Tribunal Regional Federal da 1ª Região, v. 19, nº 11/12, nov/dez. 2007.

BINENBOJM, G. Ainda a supremacia do interesse público. Revista da EMERJ, v. 21, n. 3, p. 238, set./dez.2019.

BIONI, Bruno; RIRELLI, Mariana; ZANATTA, Rafael. 110 -Petição de apresentação de manifestação (28539/2020). In: Ação Direta de Inconstitucionalidade n. 6387. Disponível em http://redir.stf.jus.br/. Acesso em 30 de abr. 2024.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro. Forense: 2019.p. 132.

BNDES. Lei Geral de Proteção de Dados – LGPD. Disponível em: https://www.bndes.gov.br/wps/portal/site/home/transparencia/lgpd. Acessado em 29 de mai. 2024.

BNDES. Relatório BNDES – Tribunal de Contas da União. Disponível em: https://www.bndes.gov.br/wps/wcm/connect/site/3c4a346e-2406-423a-baf9-b19cc8b39683/Relat%C3%B3rio+de+Feedback+BNDES.pdf?MOD=AJPERES&CVID=og-e9dt. Acessado em 29 de mai. 2024.

BONAVIDES, Paulo. Curso de Direito Constitucional. 11ª ed. São Paulo: Malheiros, 2001.

BORGES, Ademar. O relatório de inteligência financeira como meio de obtenção de prova no processo penal. *Revista Brasileira de Ciências Criminais* vol. 176. ano 29. p. 69-105. São Paulo, fevereiro/2021.

BRANCO, Paulo Gustavo Gonet. Juízo de Ponderação na Jurisdição Constitucional: Pressupostos de Fato e Teóricos Reveladores do seu Papel e do seu Limite. 2008. 393 f. Tese (Doutorado em Direito). Universidade de Brasília – UNB.

BRASIL. Ação Direta de Inconstitucionalidade número 5.642. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5117846. Acessado em 15 de mai. 2024.

BRASIL. Ação direta de Inconstitucionalidade número 6.387. Supremo Tribunal Federal. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 29 de abr. 2024.

BRASIL. ADO número 84. Supremo Tribunal Federal. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6816879. Acessado em 21 de mai. 2024.

BRASIL. ADPF 722 – Supremo Tribunal Federal. ARGUIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL. ALEGAÇÃO DE INVESTIGAÇÃO SIGILOSA NO MINISTÉRIO DA JUSTIÇA CONTRA OPOSITORES DO GOVERNO. LIBERDADES E DEMOCRACIA. RISCO DE INOBSERVÂNCIA DOS PRECEITOS FUNDAMENTAIS DA CONSTITUIÇÃO POR ÓRGÃO ESTATAL. ADOÇÃO DO RITO DO ART. 10 DA LEI N. 9.868/1999. REQUISIÇÃO DE INFORMAÇÕES URGENTES. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5967354. Acessado em 20 de mai. 2024.

BRASIL. Artigo 2º da Lei Geral de Proteção de dados. (...) Art. 2º: A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à privacidade; II – a autodeterminação informativa. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 de abr. 2024.

BRASIL. Artigo 4º da Lei Geral de Proteção de Dados. Disponível em < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 12 jan. 2024.

BRASIL. Artigo 5º da Lei Geral de Proteção de Dados – LGPD. Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 12 jan. 2024.

BRASIL. Artigo 5º Inciso X da Constituição Brasileira de 1988: Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no país a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) “Inciso X: São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”(...). Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acessado em 25 abr. 2024.

BRASIL. Artigo 21 do Código Civil Brasileiro: A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 26 de abr. 2024.

BRASIL. Art. 129 da Constituição Federal de 88. Disponível em: <https://www.jusbrasil.com.br/topicos/10677474/artigo-129-da-constituicao-federal-de-1988>. Acessado em: 11 de jun. 2024.

BRASIL. Artigo 144 da Constituição Federal. *Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos: I - polícia federal; II - polícia rodoviária federal; III - polícia ferroviária federal; IV - polícias civis; V - polícias militares e corpos de bombeiros militares. VI - polícias penais federal, estaduais e distrital*. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acessado em 05 de mai. 2024.

BRASIL. Casa Civil da Presidência da República. Avaliação de Políticas Públicas: Guia Prático de Análise *Ex Ante*. v. 1. Brasília: Ipea, 2018. Disponível em: https://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=32688. Acesso em: 04 set. 2024.

BRASIL. Casa Civil da Presidência da República. Avaliação de Políticas Públicas: Guia prático de análise *ex post*. v. 2. Brasília: Casa Civil da Presidência da República, 2018. Disponível em: https://ipea.gov.br/portal/index.php?option=com_content&id=34504. Acesso em: 04 set. 2024.

BRASIL. Código Penal Brasileiro. Homicídio simples. Art. 121. Matar alguém: Pena - reclusão, de seis a vinte anos. Falsificação, corrupção, adulteração ou alteração de produto destinado a fins terapêuticos ou medicinais. Art. 273 - Falsificar, corromper, adulterar ou alterar produto destinado a fins terapêuticos ou medicinais: Pena - reclusão, de 10 (dez) a 15 (quinze) anos, e multa. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 06 de nov. 2024.

BRASIL. Constituição Federal. Capítulo III. Da Segurança Pública. Artigo 144: A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos: I - polícia federal; II - polícia rodoviária federal; III - polícia ferroviária federal; IV - polícias civis; V - polícias militares e corpos de bombeiros militafederal, estaduais e distrital. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acessado em 07 de jun. 2024.

BRASIL. Constituição Federal. 1988 Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 19 jan. 2024.

BRASIL. Constituição Federal de 1988. LXXIX – é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 19 jan. 2024.

BRASIL. Decreto nº 7.950, de 12 de março de 2013. Institui o Banco Nacional de Perfis Genéticos e a Rede Integrada de Bancos de Perfis Genéticos. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7950.htm#:~:text=%C2%A7%201%C2%BA%20O%20Banco%20Nacional,destinadas%20%C3%A0%20apura%C3%A7%C3%A3o%20de%20crimes. Acesso em 25 de nov. 2024.

BRASIL. Decreto nº 10.212/2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10212.htm. Acesso em 30 de abr. 2024.

BRASIL. Lei nº 8.069/1990. Estatuto da Criança e do Adolescente. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em 31 de out. 2024.

BRASIL. Lei nº 8.078 de 11 de setembro de 1990. Código de Defesa do Consumidor. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em 28 de nov. 2024.

BRASIL. Câmara dos Deputados. PEC 17/2019. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757#:~:text=PEC%2017%2F2019%20Inteiro%20teor,Proposta%20de%20Emenda%20%C3%A0%20Constitui%C3%A7%C3%A3o&text=Altera%20a%20Constitui%C3%A7%C3%A3o%20Federal%20para,e%20tratamento%20de%20dados%20pessoais. Acesso em 03 de nov. 2024.

BRASIL. Câmara dos Deputados. Decreto número 10.445/2020. Disponível em: https://www2.camara.leg.br/legin/fed/decret/2020/decreto-10445-30-julho-2020-790490-publicacaooriginal-161220-pe.html. Acessado em 12 de set. 2024.

BRASIL. Câmara dos Deputados. Projeto de Lei número 4.365/1977. Disponível em:https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=220936&ficha Amigavel=nao. Acesso em 23 de set. 2024.

BRASIL. Código de Processo Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em 21 de set. 2024.

BRASIL. Código de Processo Penal. Art. 158-A. Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em 25 de set. 2024.

BRASIL. Código Tributário Nacional. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l5172compilado.htm. Acesso em 26 de ago. 2024.

BRASIL. Congresso Nacional. Medida Provisória número 954/2020. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141619#:~:text=Estabelece%20que%20os%20dados%20compartilhados,no%20%C3%A2mbito%20de%20pesquisas%20domiciliares. Acesso em 27 de ago. 2024.

BRASIL. Decisão ADI 6387. Supremo Tribunal Federal. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf. Acesso em: 30 de abr. 2024.

BRASIL. Decreto número 8.771/2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acessado em: 15 de mai. 2024.

BRASIL. Dignidade da Pessoa Humana. Constituição da República Federativa do Brasil de 1988. Artigo 1º: A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: (...) III – a dignidade da pessoa humana (...). Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 28 de abr. 2024.

BRASIL. DIREITO CONSTITUCIONAL. SEGURANÇA PÚBLICA AGRAVO REGIMENTAL EM RECURSO EXTRAORDINÁRIO. IMPLEMENTAÇÃO DE POLÍTICAS PÚBLICAS. AÇÃO CIVIL PÚBLICA. PROSSEGUIMENTO DE JULGAMENTO. AUSÊNCIA DE INGERÊNCIA NO PODER DISCRICIONÁRIO DO PODER EXECUTIVO. ARTIGOS 2º, 6ºE 144DA CONSTITUIÇÃO FEDERAL. Supremo Tribunal Federal STF - AG.REG. NO RECURSO EXTRAORDINÁRIO : RE 559646 PR. Disponível em: <https://stf.jusbrasil.com.br/jurisprudencia/20051286/agreg-no-recurso-extraordinario-re-559646-pr>. Acessado em 11 de jun. 2024. p. 62.

BRASIL. Emenda Constitucional número 115 de 2022 - Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: < https://legis.senado.leg.br/norma/35485358. >. Acesso em 04 jan. 2024.

BRASIL. Lei de Execução Penal. Art. 9º-A. O condenado por crime doloso praticado com violência grave contra a pessoa, bem como por crime contra a vida, contra a liberdade sexual ou por crime sexual contra vulnerável, será submetido, obrigatoriamente, à identificação do perfil genético, mediante extração de DNA (ácido desoxirribonucleico), por técnica adequada e indolor, por ocasião do ingresso no estabelecimento prisional. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7210.htm. Acesso em 25 de set. 2024.

BRASIL. Lei das interceptações telefônicas. Lei nº 9.296/1996. Art. 9° A gravação que não interessar à prova será inutilizada por decisão judicial, durante o inquérito, a instrução processual ou após esta, em virtude de requerimento do Ministério Público ou da parte interessada. Parágrafo único. O incidente de inutilização será assistido pelo Ministério Público, sendo facultada a presença do acusado ou de seu representante legal. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em 28 de nov. 2024.

BRASIL. Lei de Introdução às Normas do Direito Brasileiro – LINDB. Disponível em <https://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm>. Acesso em 12 dez. 2023.

BRASIL. Lei Geral de Proteção de Dados - LGPD. Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 13 nov. 2023.

BRASIL. Lei nº 7.232 de 29 de outubro de 1984. Dispõe sobre Política Nacional de Informática, e dá outras providências.Disponívelem:https://www.planalto.gov.br/ccivil_03/Leis/L7232.htm#:~:text=L

EI%20N%C2%BA%207.232%2C%20DE%2029%20DE%20OUTUBRO%20DE%201984.&text=Disp%C3%B5e%20sobre%20a%20Pol%C3%ADtica%20Nacional,Art.. Acesso em 28 de nov. 2024.

BRASIL. Lei nº 7.716 de 29 de agosto de 1983. Assegura validade nacional às carteiras de identidade, regula sua expedição e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/1980-1988/l7116.htm. Acesso em 28 de nov. 2024.

BRASIL. Lei número 8.159/1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Disponível em: https://www2.camara.leg.br/legin/fed/lei/1991/lei-8159-8-janeiro-1991-322180-norma-pl.html. Acesso em 19 de set. 2024.

BRASIL. Lei número 8.625/93 - Lei Orgânica Nacional do Ministério Público. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8625.htm>. Acessado em 11 de jun. 2021.

BRASIL. Lei número 9.099/1995. Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9099.htm. Acesso em 26 de ago. 2024.

BRASIL. Lei nº 9.504 de 30 de setembro de 1997. Estabelece normas para as eleições. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em 29 de nov. 2024.

BRASIL. Lei nº 9.507 de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data.

BRASIL. Lei número 9.613/1998 (Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá o. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9613.htm>. Acesso em: 17 abr. 2023.

BRASIL. Lei nº 9.742, de 16 de julho de 1997. Dispõe sobre a utilização dos serviços de telecomunicações.Disponívelem:https://www.planalto.gov.br/ccivil_03/leis/l9472.htm#:~:text=LEI%20N%C2%BA%209.472%2C%20DE%2016%20DE%20JULHO%20DE%201997.&text=Disp%C3%B5e%20sobre%20a%20organiza%C3%A7%C3%A3o%20dos,Constitucional%20n%C2%BA%208%2C%20de%201995. Acesso em 29 de nov. 2024.

BRASIL. Lei número 9.883/1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Art. 6º O controle e fiscalização externos da atividade de inteligência serão exercidos pelo Poder Legislativo na forma a ser estabelecida em ato do Congresso Nacional. § 1º Integrarão o órgão de controle externo da atividade de inteligência os líderes da maioria e da minoria na Câmara dos Deputados e no Senado Federal, assim como os Presidentes das Comissões de Relações Exteriores e Defesa Nacional da Câmara dos Deputados e do Senado Federal. Disponível em: https://planalto.gov.br/CCIVIL_03/LEIS/L9883.htm. Acesso em 22 de ago. 2024.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição

Federal. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 29 de nov. 2024.

BRASIL. Lei número 12.654/2012. Altera as Leis nºs 12.037, de 1º de outubro de 2009, e 7.210, de 11 de julho de 1984 - Lei de Execução Penal, para prever a coleta de perfil genético como forma de identificação criminal, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12654.htm. Acesso em 31 de out. 2024.

BRASIL. Lei número 12.683/2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12683.htm. Acesso em 15 mai. 2024.

BRASIL. Lei nº 12.414, de 09 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponívelem:https://www.planalto.gov.br/ccivil_03/_ato20112014/2011/lei/l12414.htm#:~:text=LEI%20N%C2%BA%2012.414%2C%20DE%209%20DE%20JUNHO%20DE%202011.&text=Convers%C3%A3o%20da%20Medida%20Provis%C3%B3ria%20n%C2%BA%20518%2C%20de%202010.&text=Disciplina%20a%20forma%C3%A7%C3%A3o%20e%20consulta,forma%C3%A7%C3%A3o%20de%20hist%C3%B3rico%20de%20cr%C3%A9dito.. Acesso em 29 de nov. 2024.

BRASIL. Lei nº 12.654. de 28 de maio de 2012. Altera as Leis nºs 12.037, de 1º de outubro de 2009, e 7.210, de 11 de julho de 1984 - Lei de Execução Penal, para prever a coleta de perfil genético como forma de identificação criminal, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12654.htm. Acesso em 29 de nov. 2024.

BRASIL. Lei número 12.850/2013 (Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm>. Acessado em: 18 de Mai. 2024.

BRASIL. Lei número 13.344/2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13344.htm. Acessado em 15 de mai. 2024.

BRASIL. Lei número 13.964/2019. Pacote Anticrime. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acessado em 18 de mai. 2024.

BRASIL. Marco Civil da Internet. CAPÍTULO II DOS DIREITOS E GARANTIAS DOS USUÁRIOS. Artigo 7º. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 29 de out. 2024.

BRASIL. Marco Civil da Internet. Lei número 12.965/2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acessado em 05 de mai. 2024.

BRASIL. Medida Provisória 954/2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm>. Acesso em: 21 abr. 2023.

BRASIL. Presidência da República. Casa Civil. Avaliação de Políticas Públicas. 12 de dezembro de 2008. Disponível em: http://www.casacivil.gov.br/orgaos-vinculados/comite-interministerial-de-governanca. Acesso em: 04 set. 2024.

BRASIL. Presidência da República. Lei número 9.883/1999. Disponível em: https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=9883&ano=1999&ato=83bQzaE9keNpWT7c9. Acessado em: 12 de set. 2024.

BRASIL. Projeto de Lei número 1.239/2024. Disponível em: https://www.camara.leg.br/noticias/1054261-PROJETO-OBRIGA-OPERADORAS-A-FORNECEREM-A-POLICIA-DADOS-SOBRE-CELULARES-IRREGULARES-HABILITADOS. Acessado em: 18 de mai. 2024.

BRASIL. STJ. RECURSO EM MANDADO DE SEGURANÇA Nº 61.302 - RJ (2019/0199132-0). Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201901991320&dt_publicacao=04/09/2020. Acesso em 30 de set. 2024.

BRASIL. Superior Tribunal de Justiça. AgRg no HABEAS CORPUS número 828054). Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202301896150&dt_publicacao=29/04/2024. Acesso em 25 de set. 2024.

BRASIL. Supremo Tribunal Federal. AÇÃO DIRETA DE INCONSTITUCIONALIDADE (Med. Liminar) – 3367. Disponível em: https://portal.stf.jus.br/peticaoInicial/verPeticaoInicial.asp?base=ADI&numProcesso=3367. Acesso em 21 de set. 2024.

BRASIL. Supremo Tribunal Federal. HC 91.867/PA. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=2792328. Acessado em 06 de mai. 2024.

BRASIL. Supremo Tribunal Federal – STF. RE 593727 (Reserva de Jurisdição). Disponível em: https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&queryString=PRINC%C3%8DPIO%20CONSTITUCIONAL%20DA%20RESERVA%20DE%20JURISDI%C3%87%C3%83O&sort=_score&sortBy=desc. Acesso em 31 de out. 2024.

BRASIL. Supremo Tribunal Federal. RE 1.055.941. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5213056&numeroProcesso=1055941&classeProcesso=RE&numeroTema=990. Acesso em 10 de set. 2024.

BRASIL. Supremo Tribunal Federal. Súmula Vinculante número 14. É direito do defensor, no interesse do representado, ter acesso amplo aos elementos de prova que, já documentados em procedimento investigatório realizado por órgão com competência de polícia judiciária, digam respeito ao exercício do direito de defesa. O direito do investigado de ter acesso aos autos não compreende diligências em andamento. Disponível em: https://portal.stf.jus.br/jurisprudencia/sumariosumulas.asp?base=26&sumula=1230. Acesso em 05 de nov. 2024.

BRASIL. Supremo Tribunal Federal. Tema 977 – Aferição da licitude da prova produzida durante o inquérito policial relativa ao acesso, sem autorização judicial, a registros e informações contidos em aparelho de telefone celular, relacionados à conduta delitiva e hábeis a identificar o agente do crime. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5173898&numeroProcesso=1042075&classeProcesso=ARE&numeroTema=977#:~:text=Tema%20977%20%2D%20Aferi%C3%A7%C3%A3o%20da%20licitude,identificar%20o%20agente%20do%20crime. Acessado em 06 de mai. 2024.

BRASIL. Supremo Tribunal Federal. Tema 990. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5213056&numeroProcesso=1055941&classeProcesso=RE&numeroTema=990. Acessado em 21 de mai. 2024.

BREGA, José Fernando Ferreira. O Governo eletrônico e direito administrativo. Tese de Doutorado apresentada à Universidade de São Paulo, São Paulo. 2012. p.61.

BRITO CRUZ, Francisco; SIMÃO, Bárbara(eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. V. São Paulo. InternetLab, 2022.

Bundesverfarssungsgericht. Certain powers of the Federal Criminal Police Office for data collection (§ 45(1) first sentence no. 4 of the Federal Criminal Police Office Act) and data retention (§ 18(1) no. 2 of the Federal Criminal Police Office Act) are unconstitutional in part. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2024/bvg24-083.html. Acesso em: 03 de out. 2024.

CALDAS, Ricardo Warendorff (coord.). Políticas públicas: conceitos e práticas. Belo Horizonte: Sebrae/MG, 2008. (Série Políticas Públicas, v. 7). Disponível em: http://www.mp.ce.gov.br/nespeciais/promulher/manuais/MANUAL DE POLITICAS PÚBLICAS.pdf. Acesso em: 04 set. 2024.

Câmara dos Deputados. CCJ aprova criação de banco de dados nacional de criminosos. Disponível em: https://www.camara.leg.br/noticias/764790-ccj-aprova-criacao-de-banco-de-dados-nacional-de-criminosos/. Acesso em 25 de nov. 2024.

Câmara dos Deputados. Comissão aprova proposta que regulamenta ações de inteligência das polícias ostensivas. Disponível em: https://www.camara.leg.br/noticias/918138-COMISSAO-APROVA-PROPOSTA-QUE-REGULAMENTA-ACOES-DE-INTELIGENCIA-DAS-POLICIAS-OSTENSIVAS. Acesso em 27 de ago. 2024.

Câmara dos Deputados. Comissão promove debate sobre o uso de ferramentas de reconhecimento facial no combate ao crime. Fonte: Agência Câmara de Notícias. Disponível em: https://www.camara.leg.br/noticias/1058042-comissao-promove-debate-sobre-o-uso-de-ferramentas-de-reconhecimento-facial-no-combate-ao-crime/. Acesso em 22 de nov. 2024.

Câmara dos Deputados. Empresas de internet e de telecomunicações negam repasse de dados de usuários. Fonte: Agência Câmara de Notícias. Disponível em: https://www.camara.leg.br/noticias/412182-empresas-de-internet-e-de-telecomunicacoes-negam-repasse-de-dados-de-usuarios/. Acesso em 31 de out. 2024.

CANOTILHO, J.J. Gomes; MOREIRA, Vital. Fundamentos da Constituição. Coimbra: Coimbra Editora, 1991.

CANOTILHO, José Joaquim Gomes; MOREIRA, Vital. Constituição da República Portuguesa Anotada. Vol. I. Coimbra: Coimbra Editora, 2007, p.467-468.

CANOTILHO, José Joaquim; MOREIRA; Vital. Constituição da República Portuguesa anotada. 1. Ed. Brasileira. Revista dos Tribunais, 2007.

CASTELLS, Manuel. A sociedade em rede. Rio de Janeiro: Paz e Terra, 2021, p. 18.

CARVALHO FILHO, José dos Santos. Manual de direito administrativo / José dos Santos Carvalho Filho. – 34. Ed. – São Paulo: Atlas, 2020.

Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia / Viviane Nóbrega Maldonado, Renato Opice Blum, coordenadores. 3ª ed. São Paulo: Thompson Reuters Brasil, 2021.

Comissão Nacional de Proteção de Dados. Portugal. Disponível em: https://www.cnpd.pt/. Acessado em 03 de jun. 2024.

Comitê Europeu para Proteção de Dados. Disponível em: <https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-board-edpb_pt. >. Acesso em 01 jan. 2024.

CNN Brasil. Brasil volta ao grupo das 10 maiores economias do mundo após alta do PIB. Disponível em: https://www.cnnbrasil.com.br/economia/macroeconomia/brasil-volta-ao-grupo-das-10-maiores-economias-do-mundo-apos-alta-do-pib/. Acessado em 24 de mai. 2024.

Conselho Nacional de Justiça. Recomenda aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequações às disposições contidas na Lei Geral de Proteção de Dados – LGPD. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3432. Acesso em 04 de nov. 2024.

CNN Brasil. FirstMile: como funciona o software espião que teria sido usado pela Abin de Ramagem
Disponível em: https://www.cnnbrasil.com.br/politica/firstmile-como-funciona-o-software-espiao-que-teria-sido-usado-pela-abin-de-ramagem/. Acesso em 13 de set. 2024.

CNN Brasil. País tem mais de 4,5 mil tentativas de golpe financeiro por hora. Disponível em: https://www.cnnbrasil.com.br/nacional/datafolha-pais-tem-mais-de-45-mil-tentativas-de-golpe-financeiro-por-hora/. Acesso em 22 de ago. 2024.

Conjur. Uso do reconhecimento facial na segurança pública. Disponível em: https://www.conjur.com.br/2024-jan-06/uso-do-reconhecimento-facial-na-seguranca-publica/. Acesso em 25 de out. 2024.

Controladoria Geral do Distrito Federal. Processo Administrativo Disciplinar – PAD. Disponível em: https://www.cg.df.gov.br/processo-administrativo-disciplinar-pad-voce-sabe-o-que-e/. Acesso em 09 de set. 2024.

Controladoria Geral do Estado do Paraná. Manual de implementação da LGPD. Disponível em: https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/202106/manual implementacao_lgpd.pdf. Acesso em 29 de nov. 2024.

Congresso Nacional. Regimentos do Congresso, Senado e Câmara. Disponível em: <https://www.congressonacional.leg.br/legislacao-e-publicacoes/regimento-do-congresso-nacional>. Acesso em: 14 abr. 2023.

Conselho Nacional do Ministério Público. CNMP aprova nova regulamentação das atribuições do Ministério Público no controle externo da atividade policial. Disponível em: https://www.cnmp.mp.br/portal/todas-as-noticias/17146-cnmp-aprova-nova-regulamentacao-das-atribuicoes-do-ministeriopubliconocontroleexternodaatividadepolicial#:~:text=O%20Plen%C3%A1rio%20do%20Conselho%20Nacional,18%C2%AA%20Sess%C3%A3o%20Ordin%C3%A1ria%20de%202023... Acesso em 29 de set. 2024.

Conselho Nacional do Ministério Público. O Ministério Público e o Controle Externo da Atividade Policial. Disponível em: <https://www.cnmp.mp.br/portal/publicacoes/12399-o-ministerio-publico-e-o-controle-externo-da-atividade-policial>. Acessado em 11 de jun. 2024.

Consultor Jurídico. Ministério, PF e Anatel defendem software intrusivo nacional para inibir sistemas estrangeiros. Disponível em: https://www.conjur.com.br/2024-jun-11/ministerio-defende-software-intrusivo-nacional-para-inibir-sistemas-estrangeiros/. Acesso em 13 de set. 2024.

Cornell Law School. Griswold v Connecticut. Disponível em: https://www.law.cornell.edu/wex/griswold_v_connecticut_(1965). Acessado em 25 abr. 2024.

Conselho Nacional de Justiça. Infoseg. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2011/02/infoseg.pdf. Acesso em 13 de set. 2024.

Correio Braziliense. Facções e agentes de segurança usaram dados roubados de brasileiros, diz PF. Disponível em: https://www.correiobraziliense.com.br/brasil/2024/01/6795795-faccoes-e-agentes-de-seguranca-usaram-dados-roubados-de-brasileiros-diz-pf.html. Acessado em 26 de mai. 2024.

Correio Braziliense. PF cumpre mandado de busca contra delegado acusado de vazar informações. Disponível em: <https://www.correiobraziliense.com.br/brasil/2023/10/5133295-

pf-cumpre-mandado-de-busca-contra-delegado-acusado-de-vazar-informacoes.html>. Acesso em 12 dez. 2023.

CRETELLA JÚNIOR, José. Lições de Direito Administrativo. Forense Editora, Rio de Janeiro. cit. p. 227.

CRETELA JÚNIOR, José. Polícia e Poder de Polícia. Revista de Direito Administrativo", Fundação Getúlio Vargas, Rio de Janeiro, nº 162, p. 31-32.

DA ROSA, Raíssa Roese. O ANTEPROJETO DA LGPD PENAL E A NECESSIDADE DE COOPERAÇÃO INTERNACIONAL PARA O COMPARTILHAMENTO EXTRATERRITORIAL DE DADOS PESSOAIS PARA FINS PENAIS. Disponível em: file:///C:/Users/Usuario/Downloads/6797-Texto%20do%20Artigo-21403-23245-10-20230128%20(1).pdf. Acesso em 21 de set. 2024.

DA SILVA, José Afonso. Comentário Contextual à Constiruição. São Paulo. Editora Malheiros. 2007.

Data Privacy Br. Ação Civil Pública/Inquérito Civil nº 1.16.000.002757/2022-36. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2022/12/pr-df-00128369.2022-2.pdf. Acesso em 12 de set. 2024.

Data Privacy Brasil. Projeto Excel: articulação da sociedade civil resulta em Ação Civil Pública do Ministério Público. Disponível em: https://www.dataprivacybr.org/documentos/projeto-excel-articulacao-da-sociedade-civil-resulta-em-acao-civil-publica-do-ministerio-publico/. Acesso em 12 de set. 2024.

Data Privacy Brasil. Proteção de Dados no Campo Penal e de Segurança Pública: Nota Técnica sobre o Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Investigação Criminal. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2020/12/NOTA-T%C3%89CNICA-PROTE%C3%87%C3%83O-DE-DADOS-NO-CAMPO-PENAL-E-DE-SEGURAN%C3%87A-P%C3%9ABLICA-VF-31.11.2020.pdf. Acesso em: 23 de set. 2024.

Departament of Justice. The Usa Patriot Act: Preserving Life and Liberty. Disponível em: https://www.justice.gov/archive/ll/highlights.htm. Acessado em 01 de mai. 2024.
DI PIETRO, Maria Sylvia Zanella. Direito Administrativo. 33ª ed., Rio de Janeiro: Forense, 2020.

Direitos na Rede. CDR solicita ao presidente da Câmara dos Deputados a interrupção da tramitação do “PL da LGPD Penal” - Coalizão Direitos na Rede. Disponível em: <https://direitosnarede.org.br/2022/08/01/cdr-solicita-ao-presidente-da-camara-dos-deputados-a-interrupcao-da-tramitacao-do-pl-da-lgpd-penal/>. Acesso em: 13 abr. 2023.

Diretiva 95/46/CE. Disponível em < https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em 26 dez. 2023.

Diretiva 2002/58/CE. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32002L0058>. Acesso em 26 abr. 2024.

DIRETIVA (UE) 2016/ 680 DO PARLAMENTO EUROPEU E DO CONSELHO - de 27 de abril de 2016 - relativa à proteção das pessoas singulares no que diz respeito ao trata mento de dados pessoais pelas autoridades competentes para efeitos de prevenção, inve stigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/ 977/ JAI do Conselho. [s.d.]. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=HU>. Acesso em: 13 abr. 2023.

DISTRITO FEDERAL. PORTARIA Nº 224, DE 30 DE JUNHO DE 2023. Institui a Política de Privacidade no âmbito da Polícia Civil do Distrito Federal.

DONEDA, D. A Autoridade Nacional de Proteção de Dados e o Conselho Nacional de Proteção de Dados. *In:* MENDES, L. S.; SARLET, I. W.; RODRIGUES JÚNIOR, O. L.; BIONI, B. (Coords.). Rio de Janeiro: Foresne, 2021. P. 459.

DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. In: TEPEDINO, Gustavo (Org.). Temas de direito civil. Rio de Janeiro: Renovar, 2000, p. 37-54.

DONEDA, Danilo. Cesar Maganhoto. Da privacidade à proteção de dados pessoais: Elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Thompson Reuters Brasil, 2020, p, 440/454.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019.

DONDA, Daniel. Guia Prático de Implementação da LGPD. São Paulo: Ed. Labrador, 2022. p 26.

DWORKIN, Ronald. Uma questão de princípio. Trad. Luis Carlos Borges. 2a . ed. São Paulo: Martins Fontes, 2005.

Enap. Teorias e Análises sobre Implementação de Políticas Públicas no Brasil. Disponível em:https://repositorio.enap.gov.br/bitstream/1/4162/1/Livro_Teorias%20e%20An%C3%A1lises%20sobre%20Implementa%C3%A7%C3%A3o%20de%20Pol%C3%ADticas%20P%C3%BAblicas%20no%20Brasil.pdf. Acesso em 08 de nov. 2024.

Estadão. Decisão do STJ que veta dados do Coaf para Polícia sem inquérito põe fim a "devassa indiscriminada". Disponível em: https://www.estadao.com.br/politica/blog-do-fausto-macedo/decisao-do-stj-que-veta-dados-do-coaf-para-policia-sem-inquerito-poe-fim-a-devassa-indiscriminada/. Acesso em 25 de set. 2024.

ESTELITA, Heloísa. Portal de Periódicos IDP. *O RE 1.055.941: um pretexto para explorar alguns limites à transmissão, distribuição, comunicação, transferência e difusão de dados pessoais pelo COAF*. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5991. Acesso em 10 de set. 2024.

Estratégia Nacional de Combate à Corrupção e Lavagem de Dinheiro. Ações de 2021. Disponível em: <http://enccla.camara.leg.br/acoes/acoes-de-2021>. Acesso em: 13 abr. 2023.

Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro – ENCCLA. XVIII Reunião Plenária da Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro. Disponível em: https://enccla.camara.gov.br/acoes/acoes-de-2021. Acesso em 06 de nov. 2024.

EUR-Lex. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE). Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em 28 de out. 2024.

EUROJUST. Disponível em: https://www.eurojust.europa.eu/. Acessado em 03 de jun. 2024.

European Commission. Proteção de Dados na UE. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pt. Acesso em 27 de out. 2024.

European Data. Disponível em: <https://data.europa.eu/pt/publications/overview. >. Acesso em 02 jan. 2024.

European Data Protection Supervisor. Data Protection. Artigo 37 e seguintes. Disponível em: https://gdpr-info.eu/art-37-gdpr/. Acesso em 03 de nov. 2024.

European Union. Carta de Direitos Fundamentais da União Europeia. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12012P/TXT. >. Acesso em 02 jan. 2024.

European Union. Diretivas da União Europeia. Disponível em: https://eur-lex.europa.eu/PT/legal-content/summary/european-union-directives.html. Acessado em 06 de mai. 2024.

Exame negócios. Ele vai fazer R$ 100 milhões com 'império de dados' vindos do wi-fi que você acessa de graça por aí. Disponível em: https://exame.com/negocios/ele-criou-um-imperio-de-dados-de-r-100-milhoes-com-o-sinal-wi-fi-que-voce-acessa-de-graca-por-ai/. Acesso em 04 de set. 2024.

Federal Trade Commission. Childen's Online Privacy Protection Rule – COPPA. Disponível em: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa. Acesso em 23 de set. 2024.

FERNANDES, Maíra. Lei de Proteção de Dados para Segurança Pública e Persecução Penal. Disponível em: https://www.conjur.com.br/2022-out-28/escritos-mulher-lei-protecao-dados-seguranca-publica-persecucao-penal/. Acesso em 09 de set. 2024.

FERNANDES, Milton, Proteção Civil da Intimidade. São Paulo: Saraiva, 1977.

FERREIRA, Carolina Costa. O Estudo de Impacto Legislativo como Estratégia de Enfrentamento a Discursos Punitivos na Execução Penal. 2016. 182 f. Tese (Doutorado em Direito). Universidade de Brasília – UNB.

FERREIRA, André da Rocha. Tratamento de Dados Pessoais em investigações criminais: O Direito Fundamental à Autodeterminação Informativa como Limite Constitucional. Revista Brasileira de Ciências Criminais. Vol.185. ano 29. p. 115-159. São Paulo: Ed. RT, novembro de 2021.

FERRER, Flávia. O Direito à Segurança Pública. Revista do Ministério Público do Estado do Rio de Janeiro - MPRJ. 2017. Disponível em: https://www.mprj.mp.br/documents/20184/2740997/Flavia_Ferrer.pdf. Acessado em 05 de mai. 2024.

f. Tese (Doutorado em Direito Constitucional). Universidade do Estado do Rio de Janeiro – UERJ.

Folha de São Paulo. Governo e PF defendem proibição de uso de softwares espiões. Disponível em: https://www1.folha.uol.com.br/poder/2024/06/governo-e-pf-defendem-no-stf-proibicao-de-uso-de-softwares-espioes-por-orgaos-de-inteligencia.shtml. Acesso em 13 de set. 2024.

FRAGOSO, Nathalie; RODRIGUES, Gabriel Brezinski. Protodefesa à Brasileira: Contraditório e Ampla Defesa em Investigações Sigilosas. Revista de Direito Público. Volume 18. Ano 2021.

GASIOLA, Gustavo Gil; MACHADO, Diego; MENDES, Laura Schertel. A Administração Pública entre transparência e proteção de dados. Revista de Direito do Consumidor. Vol. 135. Ano 30. P. 179-201. São Paulo: Ed. RT, maio/jun. 2021. Disponível em: http://revistadostribunais.com.br/maf/app/document?stid=st-rql&marg=DTR-2021-9042. Acesso em 29 de nov. 2024.

GDPR.EU. What is the LGPD? Brazil's version of the GDPR. Brazil passed the General Data Protection Law in 2018, and it will come into effect February 2020. This article examines the GDPR vs. the LGPD, how it differs, and what business owners globally need to do to prepare. Disponível em: https://gdpr.eu/gdpr-vs-lgpd/. Acesso em 26 de nov. 2024.

GLEIZER, Orlandino. A proteção de dados por duas portas nas intervenções informacionais. A declaração de inconstitucionalidade pelo Tribunal Federal Constitucional alemão de regras garantidoras de acesso estatal a dados constitutivos de serviços de telecomunicação (Bestandsdatenauskunft II). Revista de Estudos Criminais, São Paulo, v. 19, n. 79, 2020, p. 217.

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. O direito de proteção de dados no processo penal e na segurança pública. Rio de Janeiro: Marcial Pons, 2021.

Globo.com . Justiça condena a 48 anos de prisão Guarda Municipal de Belém que matou casal de vizinhos por causa de som alto. Disponível em: https://g1.globo.com/pa/para/noticia/2023/12/11/justica-condena-a-48-anos-de-prisao-guarda-municipal-de-belem-que-matou-casal-de-vizinhos-por-causa-de-som-alto.ghtml. Acesso em 12 dez. 2023.

Globo.com. Operadoras de telefonia são acionadas pelo Ministério Público por compartilharem dados pessoais de clientes na Bahia. Disponível em < https://g1.globo.com/ba/bahia/noticia/2022/01/18/operadoras-de-telefonia-sao-acionadas-

pelo-ministerio-publico-por-compartilhar-dados-pessoais-de-clientes-na-bahia.ghtml>. Acesso em 23 jan. 2024.

Governo Federal. Banco Nacional de Perfis Genéticos (BNPG). Disponível em: https://www.gov.br/pt-br/noticias/justica-e-seguranca/2022/12/banco-nacional-de-perfis-geneticos-conta-com-mais-de-175-mil-perfis-cadastrados. Acesso em 25 de set. 2024.

General Data Protection Regulation – GDPR. Disponível em <https://gdpr-info.eu/>. Acesso em 13 nov. 2023.

Geolocation. O que é geolocalização? Disponível em: https://www.geolocation.com/pt/index. Acesso em 31 de out. 2024.

GOMES, Orlando. Introdução ao direito civil. Rio de Janeiro: Forense Editora, 2019, p. 106. *E-book*.

GONÇALVES, Caroline Vivas. O DIREITO À EXPLICAÇÃO NA DIRETIVA (EU) 2016/680 E SUAS PERSPECTIVAS PARA O CENÁRIO BRASILEIRO. 2021. 100 f. Dissertação (Mestrado). Faculdade de Direito da Universidade Nova de Lisboa.

Governo do Distrito Federal. Participa DF. Disponível em: https://www.participa.df.gov.br/. Acessado em 27 de mai. 2024.

GRINOVER, Ada Pelegrini. Liberdades públicas e processo penal: as interceptações telefônicas. 2ª ed. São Paulo: Revista dos Tribunais, 1982.

GUIDI, Guilherme Berti de Campos. Proteção de Dados Pessoais: A composição de Sistemas pelo Direito Internacional. 2021. 215f. Tese (Doutorado). Faculdade de Direito. Programa de Pós-Graduação. Área de concentração: Direito Internacional. Universidade de São Paulo. São Paulo.

GUTWIRTH, Serge; HERT, Paul de. Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power. RDP, Brasília, v. 18, n. 100, p. 500-549, out./dez. 2021.

IBM. Califórnia Consumer Privacy Act - (CCPA). Disponível em: https://www.ibm.com/br-pt/topics/ccpa-compliance. Acesso em 23 de set. 2024.

Instituto de Pesquisa Econômica Avançada. Impacto do Valor Econômico dos Dados Abertos. Disponível em: < https://data.europa.eu/pt/publicacoes/open-data-impact. >. Acesso em 02 jan. 2024.
Sistema Eletrônico de Informações – SEI. Disponível em: https://www.ipea.gov.br/portal/sistema-eletronico-de-informacoes. Acesso em 09 de set. 2024.

Intercept Brasil. Após reportagem do Intercept, MPF ajuíza ação civil pública contra Projeto Excel. Projeto do Ministério da Justiça que equipa polícias estaduais em troca de dados é considerado ilegal. Disponível em: https://www.intercept.com.br/2022/12/14/mpf-ajuiza-acao-contra-projeto-excel/. Acesso em 12 de set. 2024.

Internet Lab. Direitos Fundamentais e Processo Penal na era digital. Disponível em: https://internetlab.org.br/wp-content/uploads/2023/01/Direitos-Fudamentais-e-Processo-Penal-na-era-digital-2021.pdf. Acesso em 16 de set. 2024.

Isto é. Alemanha tem maior número de crimes violentos em 15 anos. Disponível em: https://istoedinheiro.com.br/alemanha-tem-maior-numero-de-crimes-violentos-em-15-anos/. Acessado em 23 de set. 2024.

Jota. Aplicabilidade da LGPD às atividades de segurança pública e persecução penal. Desde a tramitação do projeto que se converteu na Lei 13.709/2018– conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD) – pende o debate sobre sua aplicabilidade ou não a certas atividades estatais relacionadas à segurança pública, à persecução criminal e à defesa nacional.Disponível em: https://www.jota.info/artigos/aplicabilidade-da-lgpd-as-atividades-de-seguranca-publica-e-persecucao-penal. Acesso em 06 de nov. 2024.

JOTA. Proteção de dados em perspectiva: como comparar a LGPD com o GDPR? Disponível em: https://www.jota.info/artigos/protecao-de-dados-em-perspectiva-como-comparar-a-lgpd-com-o-gdpr. Acessado em 29 de out. 2024.

Justice Gov. Privacy Act of 1974. Disponível em < https://www.justice.gov/opcl/privacy-act-1974#:~:text=The%20Privacy%20Act%20of%201974%2C%20as%20amended%2C%205%20U.S.C.,of%20records%20by%20federal%20agencies.>. Acesso em 01 jan. 2024.

LAPIN.ORG. Nota técnica: Análise comparativa entre o anteprojeto de LGPD Penal e o PL 1515/2022 - LAPIN. Disponível em: <https://lapin.org.br/2022/11/23/nota-tecnica-analise-comparativa-entre-o-anteprojeto-de-lgpd-penal-e-o-pl-1515-2022/>. Acesso em: 13 abr. 2023.

LAURENTTIS, Lucas de. Enciclopédia Jurídica da PUC-SP. Proteção de Dados Pessoais. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/557/edicao-1/protecao-de-dados-pessoais. Acesso em 27 de out. 2024.

LEC. Os 10 pilares de um programa de compliance. Disponível em: <https://lec.com.br/os-10-pilares-de-um-programa-de-compliance/>. Acesso em: 24 abr. 2023.

LENZA, Pedro. Direito Constitucional Esquematizado. 24ª edição. São Paulo: Saraiva Jur, 2020, pág. 181.

LEITE; Alaor; TEIXEIRA; Adriano. Consultor Jurídico. Gestão do Poder Informacional no Processo Penal no RHC 147.707-STJ. Disponível em: https://www.conjur.com.br/2023-set-14/leite-teixeira-gestao-poder-informacional-processo-penal/. Acesso em 09 de set. 2024.

LOPES MEIRELLES, Hely. Direito Administrativo Brasileiro. 2011 ed. atualizada por ANDRADE AZEVEDO, Eurico de et alii, 1995, Malheiros Editora, São Paulo, p. 94.
MENDES, Gilmar. Ela pede vista: Estudos em Homenagem à Ministra Rosa Weber. O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E A ABERTURA DA ORDEM CONSTITUCIONAL À TRANSFORMAÇÃO TECNOLÓGICA: ANÁLISE DO JULGAMENTO DA ADI 6.378. Londrina – PR: Thoth, 2023. p. 329.

MAGALHÃES FILHO, Glauco Barreira. Hermenêutica e Unidade Axiológica da Constituição. 2ª ed. Belo Horizonte: Mandamentos, 2002.

MARQUES, Andrea Neves Gonzaga. Direito à Intimidade e Privacidade. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2010/direito-a-intimidade-e-privacidade-andrea-neves-gonzaga-marques. Acesso em 29 de abr. 2024.

MARTINS, Leonardo. Cinquenta Anos de Jurisprudência do Tribunal Constitucional Alemão. Montevidéu: Konrad Adenauer-Stilfung, 2005. (Organização e introdução, coletânea original de J. Schawabe).

MARWELL, Daniel Bastos. SISTEMAS DE COMPLIANCE NA ATIVIDADE POLICIAL: A integridade nas Polícias Judiciárias Brasileiras. Rio de Janeiro: Lumen Juris, 2022. 364 p.

MASSON, Cleber. Direito Parte Geral - vol. 1. - 18.ª ed. rev., atual. e ampl. - Rio de Janeiro: Método, 2024.

MENDES, Laura S. F. Autodeterminação informativa: a história de um conceito. Rev. de Ciências Jurídicas Pensar, v. 25, n. 4, 2020. Disponível em: <https://periodicos.unifor.br/rpen/article/view/10828/pdf>. Acesso em 22 abr 2021.

MENDES, Laura Schertel; ABREU, Jacqueline. Portal de Periódicos do IDP. Privacidade e Proteção de Dados na Segurança Pública e no Processo Penal. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6214/pdf. Acesso em 08 de set. 2024.

MENDES, Laura Schertel Ferreira; ABREU, Jacqueline. Portal de Periódicos do IDP. Privacidade e Proteção de Dados na Segurança Pública e no Processo Penal. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6214/pdf. Acesso em 08 de set. 2024.

MENDES, Laura Schertel Ferreira. HABEAS DATA E AUTODETERMINAÇÃO INFORMATIVA: OS DOIS LADOS DA MESMA MOEDA. Direitos Fundamentais e Justiça. Belo Horizonte. Ano 12. Número 39. P, 185-216, jul/deze.2018.

MENDES, Laura Schertel Ferreira. Privacidade, proteção de dados e defesa do consumidor. São Paulo: Saraiva, 2014, p.28.

Ministério da Ciência Tecnologia e Inovação. Controlador, Operador e Encarregado de Dados. Disponível em: https://www.gov.br/aeb/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd/controlador-operador-e-encarregado-de-dados. Acesso em 02 de nov. 2024.

Ministério da Ciência, Tecnologia e Inovações – MCTI. Qual a diferença entre dados pessoais e dados sensíveis? Disponível em: https://www.gov.br/lncc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/campanha-lgpd/qual-a-diferenca-entre-dados-pessoais-e-dados-sensiveis. Acesso em 29 de out. 2024.

Ministério da Defesa. Encarregado pelo Tratamento de Dado Pessoais – DPO. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/hfa/acesso-a-informacao/encarregado-pelo-tratamento-de-dados-

pessoaisdpo#:~:text=O%20encarregado%20pelo%20tratamento%20de,Prote%C3%A7%C3%A3o%20de%20Dados%20(ANPD).. Acesso em 07 de nov. 2024.

Ministério da Fazenda. Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/FATF). Disponível em: https://www.gov.br/susep/pt-br/assuntos/cidadao/pldftp/o-grupo-de-acao-financeira-gafi-fatf. Acesso em 21 de set. 2024.

Ministério da Justiça e Segurança Pública. CÓDIGO DE CLASSIFICAÇÃO E TABELA DE TEMPORALIDADE E DESTINAÇÃO DE DOCUMENTOS DE ARQUIVO RELATIVOS ÀS ATIVIDADES-FIM DO MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. Disponível em: https://www.gov.br/arquivonacional/pt-br/arquivos%20pdf/codigos-de-classificacao/CCD_TTD_MJSP.pdf. Acesso em 28 de ago. 2024.

Ministério da Justiça e Segurança Pública. Córtex. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/operacoes-integradas/destaques/plataforma-de-monitoramento-cortex. Acesso em 14 de out. 2024.

Ministério da Justiça e Segurança Pública. Projeto Excel. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/acao-do-ministerio-da-justica-e-seguranca-publica-ja-causou-prejuizo-de-r-1-bi-ao-crime-organizado. Acessado em 12 de set. 2024.

Ministério da Justiça e Segurança Pública. Programa Brasil Mais, do MJSP, permite acesso a imagens de satélite para auxiliar no combate às queimadas no Pantanal. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/programa-brasil-mais-do-mjsp-permite-acesso-a-imagens-de-satelite-para-auxiliar-no-combate-as-queimadas-no-pantanal. Acesso em 16 de set. 2024.

Ministério Público do Estado de Santa Catarina. Nota Técnica do Ministério Público do Estado de Santa Catarina aponta inconsistências constitucionais no Anteprojeto da LGPD penal e considera ser necessário reformular a proposta em tramitação no Congresso Nacional. Disponível em: https://www.facebook.com/photo/?fbid=3185976848346205&set=a.1425084504435457. Acesso em 16 de set. 2024.

Ministério Público do Estado da Bahia. MP aciona Vivo, Tim, Oi e Claro por compartilhamento indevido de dados pessoais. Disponível em: https://www.mpba.mp.br/noticia/60732. Acesso em 25 nov. 2024.

Ministério Público do Estado do Maranhão. Distorções no entendimento do conceito de inteligência é tema de palestra na PGJ. Disponível em: https://www.mpma.mp.br/distorcoes-no-entendimento-do-conceito-de-inteligencia-e-tema-de-palestra-na-pgj/. Acesso em 02 de novembro de 2024.

Ministério dos Direitos Humanos. Pacto Internacional sobre Direitos Civis e Políticos. Disponível em: https://www.gov.br/mdh/pt-br/navegue-por-temas/atuacao-internacional/relatorios-internacionais-1/pacto-internacional-sobre-direitos-civis-e-politicos#:~:text=Instrumento%20por%20meio%20do%20qual,alguma%20por%20motivo%20de%20ra%C3%A7a%2C. Acesso em: 29 abr de 2024.

Ministério Público Federal. Fundamentos e Princípios da LGPD. Disponível em: https://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd/fundamentos-e-principios. Acesso em 28 de out. 2024.

Ministério Público Federal. Lei Geral de Proteção de Dados Pessoais e o poder requisitório do Ministério Público. Disponível em <https://www.mpf.mp.br/pgr/arquivos/2023/2023-11-estudo%20tecnico%20dados%20pessoais.pdf>.Acesso em 12 jan. 2024.

Ministério Público Federal. MPF e Idec querem que Whatsapp pague R$ 1,7 bilhão por violações de direitos em política de privacidade. Disponível em: https://www.mpf.mp.br/sp/sala-de-imprensa/noticias-sp/mpf-e-idec-querem-que-whatsapp-pague-r-1-7-bilhao-por-violacoes-de-direitos-em-politica-de-privacidade. Acesso em 09 de set. 2024.

Ministério Público Federal. PORTARIA PGR/MPF Nº 24, DE 27 DE JANEIRO DE 2021. Disponível em: https://biblioteca.mpf.mp.br/repositorio/items/99012da8-45fa-4814-ba46-940cc1dbfca3. Acesso em 09 de set. 2024.

Ministério Público Federal. PROCURADORIA GERAL DA REPÚBLICA SECRETARIA DE PERÍCIA, PESQUISA E ANÁLISE. [s.d.]. Disponível em: <https://criminal.mppr.mp.br/arquivos/File/ENCCLA_-_PGR-00456556-2020_NT.pdf>. Acesso em: 21 abr. 2023.

MONTEIRO, Renato Leite. Desafios para a efetivação do direito à explicação na Lei Geral de Proteção de Dados no Brasil. 2021. 386f. Tese (Doutorado). Faculdade de Direito. Programa de Pós-Graduação. Área de concentração: Filosofia e Teoria Geral do Direito. Universidade de São Paulo. São Paulo.

MORAES, Guilherme Braga Peña de. Direitos Fundamentais: Conflitos e Soluções. Niterói – RJ, Labor Juris, 2000, p. 91.

NASCIMENTO, Filippe. A DIMENSÃO OBJETIVA DOS DIREITOS FUNDAMENTAIS: É POSSÍVEL RECONHECER OS DIREITOS FUNDAMENTAIS COMO UMA ORDEM OBJETIVA DE VALORES? Disponível em: https://bdjur.stj.jus.br/jspui/bitstream/2011/43548/dimensao_objetiva_dos_nascimento.pdf. Acesso em 03 de nov. 2024.

NERY, Nina. O compartilhamento de dados financeiros no sistema antilavagem de dinheiro brasileiro. São Paulo: Thompson Reuters Brasil, 2024.

NOVAIS, Jorge Reis. Limites dos Direitos Fundamentais: Fundamento, Justificação e Controlo. Portugal. Almedina. p. 5-/51. 2021.

NOVELINO, Marcelo. Curso de Direito Constitucional, 12ª ed. rev, ampl. e atual. Salvador: Ed. JusPodivm, 2017. p. 301.

NSO Group. NSO Group develops best-in-class technology to help government agencies detect and prevent terrorism and crime. Our products help licensed government intelligence and law-enforcement agencies lawfully address the most dangerous issues in today's world. NSO's technology has helped prevent terrorism, break up criminal operations, find missing persons,

and assist search and rescue teams. Disponível em: https://www.nsogroup.com/. Acesso em 13 de set. 2024.

NUCCI, G. de S. Direitos humanos versus segurança pública. Rio de Janeiro: Forense, 2016. p. 49.

O´Connell, Felix C. The Rigth To Privacy. Disponível em: https://www.cambridge.org/core/books/abs/right-to-privacy/felix-c-oconnell/86C0D205334505A29DD621208909355C. Acesso em 23 de set. 2024.

O Globo. Europa limita lei de 'direito a ser esquecido' na internet. Disponível em: https://oglobo.globo.com/mundo/europa-limita-lei-de-direito-ser-esquecido-na-internet-23970764. Acesso em: 24 jul. 2020.

OLIVEIRA, Luciano Rocha de. Proteção de Dados Pessoais no Processo Penal e na Segurança Pública: problemas e atuais perspectivas. São Paulo: Editora Dialética, 2020, p. 23.

Organização das Nações Unidas. Crescimento da internet desacelera e 2,7 bilhões ficam fora da rede. Disponível em: https://news.un.org/pt/story/2022/09/1801381. Acesso em 26 de abr. 2024.

Perfil da Alemanha. Segurança na Alemanha. Disponível em: https://www.tatsachen-ueber-deutschland.de/pt-br/vida-na-alemanha/seguranca-na-alemanha#:~:text=A%20Alemanha%20tem%20taxas%20comparativamente,est%C3%A3o%20conectadas%20em%20redes%20internacionais. Acesso em 23 de set. 2024.

Petrobrás – Privacidade e Proteção de Dados pessoais. Disponível em: https://petrobras.com.br/privacidade-protecao-de-dados. Acessado em 02 de jun. 2024.

Polícia Civil do Distrito Federal. Emenda parlamentar viabiliza aquisição de supercomputador para a PCDF. Disponível em: https://www.pcdf.df.gov.br/noticias/12781/emenda-parlamentar-viabiliza-aquisicao-de-supercomputador-para-a-pcdf. Acesso em 06 de nov. 2024.

Polícia Civil do Distrito Federal. PCDF deflagra Operação Delta no Paranoá. Disponível em: https://www.pcdf.df.gov.br/noticias/9250/pcdf-deflagra-operacao-delta-no-paranoa. Acesso em 26 de ago. 2024.

Polícia Civil do Distrito Federal. PCDF prende hackers especializados em vazamento de dados sigilosos de milhares de brasileiros. Disponível em: https://www.pcdf.df.gov.br/noticias/11843/pcdf-prende-hackers-especializados-em-vazamento-de-dados-sigilosos-de-milhares-de-brasileiros. Acessado em 26 de mai. 2024.

Portal da Câmara dos Deputados. Projeto altera Lei de Proteção de Dados para resguardar segurança pública e defesa nacional. Disponível em: <https://www.camara.leg.br/noticias/893704-projeto-altera-lei-de-protecao-de-dados-para-resguardar-seguranca-publica-e-defesa-nacional/>. Acesso em: 13 abr. 2023.

PORTUGAL. Lei número 34/2009 de julho. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/34-2009-492407. Acessada em 03 de jun.2024.

PORTUGAL. Lei número 38/2015 de 11 de maio. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/38-2015-67185039. Acessado em 03 de jun. 2024.

PORTUGAL. Lei número 59/2019 de 08 de agosto. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/59-2019-123815983. Acessado em 03 de jun. 2024.

Procuradoria Geral da República. Manifestação da PGR (27551/2020). In: Ação Direta de Inconstitucionalidade n. 6387. Disponível em http://redir.stf.jus.br/. Acesso em 30 de abr. 2024.

PULIDO, Carlos Bernal. A fundamentalidade dos direitos fundamentais. Tradução: Ana Paula Soares Carvalho. In: ASENSI, Felipe Dutra; DE PAULA, Daniel Giotti (coord.). Tratado de direito constitucional: Constituição, política e sociedade. Rio de Janeiro: Campus JurídicoElsevier, 2013. p. 387-401.

Quinta geração dos direitos fundamentais. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/534. Acessado em 27 de mai. 2024.

Quinta Turma – STJ. Autoridade policial pode acionar Coaf antes de instaurar inquérito policial, diz STJ. Disponível em: https://www.youtube.com/watch?v=x1mIz2LbyLY. Acessado em 22 de mai. 2024.

REZENDE, Beatriz Vargas Ramos Gonçalves de; A Ilusão do Poibicionismo: Estudo sobre a Criminalização Secundária do Tráfico de Drogas no Distrito Federal. 2011. 148 f. Tese (Doutorado em Direito). Universidade de Brasília – UNB.

Revista de Teorias e Filosofias do Estado. A justificativa do Estado na doutrina de Georg Jellinek. Disponível em: https://www.indexlaw.org/index.php/revistateoriasfilosofias/article/view/1141. Acessado em 27/05/2024.

RIBEIRO, C. V. A. Ministério Público - Funções Extrajudiciais. 1ª Edição ed. Belo Horizonte: Fórum, 2015.

RIVERO, Jean. Direito Administrativo. tradução de Rogério Ehrhardt Soares, Livraria Almedina, Coimbra, Portugal, 1981, p. 15.

RODRIGUEZ, Daniel Piñeiro. O Direito Fundamental à Proteção de Dados: Vigilância, Privacidade e Regulação. Rio de Janeiro. Lumen Juris. 2021. 232 p.

SALDANHA, Nuno. Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar? Lisboa: Fca, 2018, p. XV.

SANTOS, Roberto Mizuki Dias dos. A SEGURANÇA PÚBLICA INTEGRADA AO MÍNIMO EXISTENCIAL NO DIREITO BRASILEIRO ENQUANTO MEDIDA NECESSÁRIA PARA SUA EFETIVAÇÃO PELO PODER JUDICIÁRIO. 2011. 149 f. Dissertação (Mestrado). Universidade Federal da Bahia – UFBA.

SARKIS, Jamilla Monteiro. Dados Pessoais no Processo Penal: tutela da Personalidade e da Inocência diante da Tecnologia. Revistra Brasileira de Ciências Criminais. Vol. 190. Ano 30. p. 117-156. São Paulo: Ed. RT, maio/jun. 2022.

SARLET, Ingo Wolfgang. A Eficácia dos Direitos Fundamentais. Porto Alegre: Livraria do Advogado. 2° ed., 2001, p. 52.

SARLET, Ingo Wolfgang. A Lei Fundamental da Alemanha nos seus 60 anos e o Direito Constitucional Brasileiro: Algumas Aproximações. Direitos Fundamentais e Justiça. Nº 7 – ABR.JUN. 2009.

SARLET, Wolfgang Ingo. Dignidade da pessoa humana e direitos fundamentais na Constituição da República de 1988. Porto Alegre: Livraria do Advogado, 2002.

SARLET, Ingo Wolfgang. O direito fundamental à proteção de dados pessoais como direito subjetivo. Disponível em: https://www.conjur.com.br/2021-ago-15/direitos-fundamentais-direito-protecao-dados-pessoais-direito-subjetivo/. Acesso em 25 de set. 2024.

SARMENTO, D; BORGES, A; ADAMI, E. Parecer. FILTRAGEM CONSTITUCIONAL DOS PEDIDOS DE SUSPENSÃO DE SEGURANÇA. INTERESSE PÚBLICO PRIMÁRIO QUE TUTELA DIREITOS FUNDAMENTAIS, SOBRETUDO DOS MAIS VULNERÁVEIS. LEGITIMIDADE ATIVA DA DEFENSORIA PÚBLICA COMO *CUSTUS VULNERABILIS*. Brasil.

SARMENTO, D. Dignidade da Pessoa Humana: conteúdo, trajetórias e metodologia. 3. Ed. Belo Horizonte: Fórum, 2021; BARROSO, L.R. A dignidade da pessoa humana no direito constitucional contemporâneo. Belo Horizonte: Fórum, 2013.

SARMENTO, Daniel. Teoria dos Direitos Fundamentais. 2ª ed. Rio de Janeiro: Renovar, 2001, p. 50.

Seminário Internacional da Comissão de Juristas - Discussão sobre Proteção de Dados Pessoais - YouTube. Disponível em: <https://www.youtube.com/watch?v=NMkSuHEryXE>. Acesso em: 13 abr. 2023.

Senado Federal. Condenados por crimes dolosos podem ter coleta obrigatória de DNA. Fonte: Agência Senado. Disponível em: https://www12.senado.leg.br/noticias/materias/2023/05/02/condenados-por-crimes-dolosos-podem-ter-coleta-obrigatoria-de-dna. Acesso em 25 de set. 2024.

Senado Federal. Congresso aprova criação de cadastro de condenados por crimes sexuais. Disponível em: https://www12.senado.leg.br/tv/programas/noticias-1/2024/10/aprovada-criacao-do-cadastro-de-pedofilos-e-predadoressexuais#:~:text=Nesta%20quarta%2Dfeira%20(30),a%20preven%C3%A7%C3%A3o%20contra%20novos%20crimes. Acesso em 31 de out. 2024.

Senado Federal. Punições pelo uso indevido de dados pessoais. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/07/29/punicoes-pelo-uso-indevido-de-dados-pessoais-comecam-a-valer-no-domingo. Acesso em 29 de out. 2024.

Serpro. LGPD: a versão brasileira do regulamento europeu. Disponível em: https://www.serpro.gov.br/lgpd/noticias/lgpd-versao-brasileira-gdpr-dados-pessoais. Acesso em 27 de out. 2024.

Serpro. O que são dados anonimizados, segundo a LGPD? Disponível em: https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-anonimizados-lgpd#:~:text=E%20o%20que%20anonimiza%C3%A7%C3%A3o%20tem,desvincula%C3%A7%C3%A3o%20dele%20a%20essa%20pessoa. Acesso em 29 de out. 2024.

SILVA, José Afonso da. Comentário Contextual à Constituição. 4ª ed. São Paulo. Ed. Malheiros, 2007. p.38.

SILVA, J. A. da. Curso de Direito Constitucional Positivo. São Paulo: Malheiros, 2022. P. 791.

SILVA, José Afonso da. Curso de Direito Constitucional Positivo. São Paulo: RT, 6' ed., 1990, p. 650.

Sobre o princípio republicano na ordem constitucional brasileira, cf. SARMENTO, D. O princípio republicano nos 30 anos da Constituição de 88: por uma República inclusiva, Revista da Emerj, v. 20, n. 3, p. 296-318, set./dez. 2018. Sobre a incidência do princípio republicano na implementação igualitária de segurança pública, cf. SOUZA NETO, C. P. de. A segurança pública na Constituição Federal de 1988: conceituação constitucionalmente adequada, competências federativas e órgãos de execução das políticas. In: SOUZA NETO, C. P. de. Constitucionalismo democrático e governo das razões. Rio de Janeiro: Lumen Juris, 2011. P. 280-283.

SOMBRA, Thiago Luís Santos. Fundamentos da Regulação da Privacidade e Proteção de Dados Pessoais: Pluralismo Jurídico Transparência e Perspectiva. São Paulo: Thomson Reuters, 2019. p. 94.

SOUSA FILHO, Ademar Borges de. O controle de constitucionalidade de leis penais no Brasil: graus de deferência ao legislador, parâmetros materiais e técnicas de decisão. 2019. 700 f. Tese (Doutorado em Direito) - Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2019.

SOUZA NETO, Claudio Pereira de; SARMENTO, Daniel. NOTAS SOBRE JURISDIÇÃO CONSTITUCIONAL E DEMOCRACIA: A QUESTÃO DA"ÚLTIMA PALAVRA" E ALGUNS PARÂMETROS DE AUTOCONTENÇÃO JUDICIAL: A EXPANSÃO DA JURISDIÇÃO CONSTITUCIONAL E A CHAMADA “DIFICULDADE CONTRAMAJORITÁRIA”. Disponível em: file:///C:/Users/Usuario/Downloads/acrb,+6+-+Jurisdi%C3%A7%C3%A3o+constitucional+e+democracia_Daniel+Sarmento.pdf. Acesso em 24 de sete. 2024.

Superior Tribunal de Justiça. A cadeia de custódia no processo penal: do Pacote Anticrime à jurisprudência do STJ. Disponível em: https://www.stj.jus.br/sites/portal/Paginas/Comunicacao/Noticias/2023/23042023-A-cadeia-de-custodia-no-processo-penal-do-Pacote-Anticrime-a-jurisprudencia-do-STJ.aspx. Acesso em 05 de nov. 2024.

Superior Tribunal de Justiça. A partir de precedente do Supremo Tribunal Federal, terceira seção considera ilegal obtenção direta de dados fiscais por iniciativa do MP. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/11022022-A-partir-de-

precedente-do-STF--Terceira-Secao-considera-ilegal-obtencao-direta-de-dados-fiscais-por-iniciativa-do-.aspx. Acessado em 21 de mai. 2024.

Superior Tribunal de Justiça. Comissão entrega à Câmara anteprojeto sobre tratamento de dados pessoais na área criminal. Instituída em novembro do ano passado pelo presidente da Câmara dos Deputados, a comissão de juristas teve, além dos ministros Nefi Cordeiro (presidente) e Antonio Saldanha Palheiro (vice-presidente), os seguintes membros: Laura Schertel Mendes (relatora), Pedro Ivo Velloso (secretário), Danilo Doneda, Davi Tangerino, Eduardo Queiroz, Heloisa Estellita, Humberto Fabretti, Ingo Sarlet, Jacqueline Abreu, Jorge Octávio Lavocat Galvão, Juliana Abrusio, Tércio Sampaio Ferraz Júnior e Vladimir Aras. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx Acesso em 05 de nov. 2024.

Superior Tribunal de Justiça. *Fishing Expedition.* Disponível em: Fishing expedition e serendipidade na jurisprudência do STJ. Acesso em 06 de mai. 2024.

Superior Tribunal de Justiça. Informativo número 738 (30 de maio de 2022). Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/?aplicacao=informativo&acao=pesquisar&livre=@CNOT=%27019099%27. Acesso em 27 de ago. 2024.

Superior Tribunal de Justiça. Os precedentes do STJ nos primeiros quatro anos de vigência da Lei Geral de Proteção de Dados Pessoais. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/27102024-Os-precedentes-do-STJ-nos-primeiros-quatro-anos-de-vigencia-da-Lei-Geral-de-Protecao-de-Dados-Pessoais.aspx. Acesso em 31 de out. 2024.

Superior Tribunal de Justiça. Preso não pode se negar a fornecer material genético para banco de DNA. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/25092024-Preso-nao-pode-se-negar-a-fornecer-material-genetico-para-banco-de-DNA-.aspx. Acesso em 25 de set. 2024.

Supremo Tribunal Federal. Boletim de Jurisprudência Internacional. Direito ao Esquecimento. 2018. Disponível em: https://www.stf.jus.br/arquivo/cms/jurisprudenciaBoletim/anexo/BJI5_DIREITOAOESQUECIMENTO.pdf. Acesso em 28 de nov. 2024.

Supremo Tribunal Federal. Cadastro Estadual de Usuários e Dependentes de Drogas. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=772302784. Acesso em 25 de set. 2024.

Supremo Tribunal Federal. EXECUÇÃO PENAL – PERFIL GENÉTICO – EXAME – DNA – ENTREGA DE MATERIAL – OBRIGATORIEDADE – IMPOSIÇÃO NA ORIGEM – RECURSO EXTRAORDINÁRIO – REPERCUSSÃO GERAL CONFIGURADA. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/verPronunciamento.asp?pronunciamento=6410103. Acesso em 25 de set. 2024.

Supremo Tribunal Federal. Nenhuma lei pode disciplinar o processo legislativo no Brasil, pois os princípios que regem a formação de leis estão exclusivamente na Constituição Federal. Disponível em: https://portal.stf.jus.br/constituicao-supremo/artigo.asp?abrirBase=CF&abrirArtigo=61#:~:text=A%20disciplina%20jur%C3%ADdica%20do%20processo,7%2D12%2D2006.%5D. Acesso em 06 de nov. 2024.

Supremo Tribunal Federal. Norma que autoriza MP e polícia a requisitar de telefônicas dados cadastrais de investigados é válida, decide STF. Disponível em: https://noticias.stf.jus.br/postsnoticias/norma-que-autoriza-mp-e-policia-a-requisitar-de-telefonicas-dados-cadastrais-de-investigados-e-valida-decide-stf/#:~:text=O%20Supremo%20Tribunal%20Federal%20(STF,a%20necessidade%20de%20ordem%20judicial. Acesso em 13 de set. 2024.

Supremo Tribunal Federal. Procuradoria Geral da República. 102 -Manifestação da PGR (27551/2020). In: Ação Direta de Inconstitucionalidade n. 6387. Disponível em http://redir.stf.jus.br/. Acesso em 30 de abr. 2024.

Supremo Tribunal FederaL. STF conclui que direito ao esquecimento é incompatível com a Constituição Federal. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=460414&ori=1&post_type=eventos&s=gestao. Acesso em 08 de nov. 2024.

Supremo Tribunal Federal. STF dispensa autorização para a polícia acessar dados controlados por operadoras de telefonia. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=532701&ori=1. Acessado em 15 de mai. 2024.

Supremo Tribunal Federal. Entenda: STF julga ação sobre letalidade das operações policiais no Rio de Janeiro. Disponível em: https://noticias.stf.jus.br/postsnoticias/entenda-stf-julga-acao-sobre-letalidade-das-operacoes-policiais-no-rio-de-janeiro/. Acesso em 25 de nov. 2024.

Supremo Tribunal Federal. STF suspende compartilhamento de dados de usuários de telefônicas com IBGE. Para a maioria dos ministros, a previsão contida na Medida Provisória 954/2020 viola o direito constitucional ao sigilo de dados, entre outros. Disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902>. Acesso em 21 abr. 2023.

Supremo Tribunal Federal. PRF pode lavrar termo circunstanciado de ocorrência, decide STF. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=503028&ori=1. Acesso em 26 de ago. 2024.

Supremo Tribunal Federal. STF conclui que direito ao esquecimento é incompatível com a Constituição Federal. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=460414&ori=1&post_type=eventos&s=gestao. Acesso em 03 de out. 2024.

Supremo Tribunal Federal. STF confirma limitações ao compartilhamento de dados do Sisbin. Disponível em:

https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=474835&ori=1. Acessado em 12 de set. 2024.

Supremo Tribunal Federal. STF suspende compartilhamento de dados de usuários de telefônicas com IBGE. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902&ori=1. Acesso em Acesso em 27 de ago. 2024.

Supremo Tribunal Federal. Supremo mantém possibilidade de PM-MG lavrar termo circunstanciado. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=483411&ori=1. Acesso em 26 de ago. 2024.

Supremo Tribunal Federal. Supremo Tribunal Federal proíbe elaboração de dossiês sobre antifascistas pela Secretaria de Operações Integradas (Seopi), do Ministério da Justiça e Segurança Pública Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=450007&ori=1. Acesso em 12 de set. 2024.

SEBRAE. Conheça a Análise SWOT. Disponível em: https://sebrae.com.br/sites/PortalSebrae/conheca-a-analise-swot,202f64e8feb67810VgnVCM1000001b00320aRCRD. Acesso em 06 de set. 2024.

TOSCHI, Aline Seabra; LOPES Herbert Emílio Araújo. Dados de Troia. In: Associação Nacional dos Procuradores da República; Ministério Público Federal; ARAS, Vladimir Barros; MENDONÇA, Andrey Borges de; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA, Marcos Antônio da Silva (Orgs). Proteção de dados pessoais e investigação criminal. Brasília: ANPR, 2020.

Tribunal de Justiça do Distrito Federal e Territórios. Marco Civil da Internet. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet#:~:text=O%20Marco%20Civil%20da%20Internet,da%20internet%20no%20Brasil. Acesso em 29 de out. 2024.

Tribunal Constitucional Portugal. Acordão número 91/2023. Disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20230091.html. Acesso em 24 de set. 2024.

Trecsson Business Scholl. O que é big data? Conceitos, Definição, Exemplos. Disponível em: https://www.trecsson.com.br/blog/tecnologia-e-ciencia-de-dados/o-que-e-big-data. Acesso em 01 de out. 2024.

Tribunal Constitucional Portugal. Acordão número 403/2015. Disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20150403.html. Acesso em 24 de set. 2024.

Tribunal Constitucional Portugal. Acórdão número 464/2019. Disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20190464.html. Acesso em 24 de set. 2024.

Tribunal Constitucional Portugal. Acordão número 687/2021. Disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20210687.html. Acesso em 24 de set. 2024.

Tribunal Constitucional Portugal. Disponível em: https://www.tribunalconstitucional.pt/tc/home.html. Acesso em 24 de set. 2024.

Tribunal de Contas da União. TCU verifica risco alto à privacidade de dados pessoais coletados pelo governo. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/tcu-verifica-risco-alto-a-privacidade-de-dados-pessoais-coletados-pelo-governo.htm. Acesso em 29 de ago. 2024.

Tribunal Superior do Trabalho. Fábrica de alimentos é condenada por exigir certidão de antecedentes criminais para contratar auxiliar. Disponível em: https://tst.jus.br/-/f%C3%A1brica-de-alimentos-%C3%A9-condenada-por-exigir-certid%C3%A3o-de-antecedentes-criminais-para-contratar-auxiliar. Acesso em 01 de out. 2024.

UK ETA. A lei de proteção de dados do Reino Unido pode alterar a forma como a ETA armazena os dados. Disponível em: https://uk-eta.com.br/a-lei-de-protecao-de-dados-do-reino-unido-pode-alterar-a-forma-como-a-eta-armazena-os-dados/. Acesso em 28 de out. 2024.

União Europeia. Tipos de Legislação. Disponível em https://european-union.europa.eu/institutions-law-budget/law/types-legislation_pt. Acesso em 28 de out. 2024.

Universidade Federal Do Ceará. FACULDADE DE DIREITO. CURSO DE GRADUAÇÃO EM DIREITO. CLARISSA NOGUEIRA JOSINO. DADOS PESSOAIS, SEGURANÇA PÚBLICA E INVESTIGAÇÃO CRIMINAL: UM PANORAMA DA PROTEÇÃO DE DADOS E SEUS DESAFIOS REGULATÓRIOS NO BRASIL. Fortaleza, 2021. [s.d.]. Disponível em: < https://repositorio.ufc.br/bitstream/riufc/58510/1/2021_tcc_cnjosino.pdf>. Acesso em: 17 abr. 2023.

Uol. Criminosos faturam r$ 88 milhões com venda de dados roubados de brasileiros na dark web. Disponível em: https://cultura.uol.com.br/noticias/49848_criminosos-faturam-r-88-milhoes-com-venda-de-dados-roubados-de-brasileiros-na-dark-web.html. Acessado em 26 de mai. 2024.

Uol. PF usa "maleta espiã" para invadir celulares em casos que vão de Lava Jato a pedofilia. Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2017/08/17/pf-usa-maleta-espia-para-invadir-celulares-em-casos-que-vao-de-lava-jato-a-pedofilia.htm. Acesso em 13 de set. 2024.

Uol. Programa do Ministério da Justiça admite monitorar 'alvo' sem justificativa. Disponível em: https://noticias.uol.com.br/ultimas-noticias/agencia-publica/2024/10/09/programa-do-mj-permite-monitorar-alvos-sem-justificativa.htm. Acesso em 14 de out. 2024.

Uol. Site de mostra dados revê política de privacidade, mas ainda exibe celular. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2017/06/13/site-que-mostra-dados-reve-politica-de-privacidade-mas-ainda-exibe-celular.htm. Acessado em 26 de mai. 2024.

U.S. Departament of Health and Human Services. Health Insurance Portability and Accountability – HIPAA. Disponível em: https://www.hhs.gov/hipaa/index.html. Acesso em 23 de set. 2024.

VILHENA, Oscar. Combate ao crime organizado é questão de Estado. Folha de São Paulo. Disponível em: https://www1.folha.uol.com.br/colunas/oscarvilhenavieira/2024/11/combate-ao-crime-organizado-e-questao-de-estado.shtml. Acesso em 25 de nov. 2024.

VILHENA VIEIRA, Oscar et aljj. Direito, Cidadania e Justiça. coordenação de DI GIORGI, Beatriz, CAMPILONGO, Celso Fernandes e PIOVESAN, Flávia, I!ed., 1995, Editora Revista dos Tribunais, São Paulo, p. 191.

WESTIN, Alan. Privacy and freedoms. New York: Atheneum, 1970.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. Harvard Law Review, v. 4, n.5., Dec. 15, 1890.Disponívelem:http://links.jstor.org/sici?sici=0017811x%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C. Acesso em 25 abr. 2024.

WARREN, Samuel; BRANDEIS, Loius D. The Right to Privacy. In: Harvard Law Review, Vol.4, nº 05 (Dec. 15, 1890). p. 193-220.

Whitehouse.gov. The Constitution. Disponível em: https://www.whitehouse.gov/about-the-white-house/our-government/the-constitution/. Acessado em 05 de mai. 2024.

WOLTER, Jürgen. O Inviolável e o Intocável no Direito Processual Penal: Reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. Organizada e traduzida por Luís Greco. Tradução: Alaor Leite e Eduardo Viana. 1ª edição. São Paulo: Marcial Pons, 2018.

Your Europe. A proteção de dados ao abrigo do RGPD. Disponível em: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_pt.htm. Acesso em 27 de out. 2024.

ZANATTA, Rafael Augusto Ferreira. A proteção coletiva dos dados pessoais no Brasil: a defesa de direitos entre autoritarismo e democracia. 2022. 356f. Tese (Doutorado). Instituto de Energia e Ambiente. Programa de Pós-Graduação em Ciência Ambiental. Universidade de São Paulo. São Paulo.

ANEXOS

(Respostas Lei de Acesso à Informação)

Governo do Distrito Federal
Polícia Civil do Distrito Federal
Departamento de Polícia Técnica
Instituto de Identificação do Departamento de Polícia Técnica

Memorando Nº 529/2023 - PCDF/DGPC/DPT/II Brasília-DF, 05 de outubro de 2023.

Para: **Departamento de Polícia Técnica**

Assunto: **SOLICITAÇÃO - E-SIC**

Senhor Diretor,

Com as minhas cordiais saudações, em resposta ao Despacho 123899940 desse Departamento, associado ao teor da Manifestação E-Sic 123455069, apresento a seguir as respostas aos questionamentos relacionados ao Instituto de Identificação.

Item 5 - Em que ano a Polícia Civil do Distrito Federal passou a ter acesso ao Prontuário de Identificação Civil informatizado?

A partir da assinatura do Contrato nº 209/2008-PCDF, o Consórcio ABNEC providenciou a digitalização dos prontuários civis originalmente produzidos em papel que compunham o arquivo físico do Instituto de Identificação - II/PCDF, e também possibilitou a geração da versão digital desses documentos, a partir da transposição dos dados biográficos e biométricos dos cidadãos para um sistema informatizado (denominado Sistema de Prontuário Digital - SPD, hoje desativado).

Posteriormente, após a aquisição de um Sistema Automatizado de Identificação Multibiométrico (ABIS) junto à empresa Thales Dis Brasil Cartões e Soluções de Tecnologia LTDA, por meio do Contrato nº 80/2019-PCDF, o prontuário civil físico deixou de ser produzido, passando os dados biográficos e biométricos dos cidadãos identificados a integrarem exclusivamente um banco de dados virtual, acessado via sistemas que integram o portal CABIS Single Sign On - SSO.

Item 6 - A partir de que ano as cédulas de identidade passaram a ser emitidas pela Polícia Civil do Distrito Federal?

Em consulta aos arquivos e sistemas de identificação civil deste Instituto, verificou-se que a primeira via da Carteira de Identidade referente ao RG nº 1 foi entregue ao requerente no dia 13 de março de 1963.

Item 16 - Existe alguma finalidade específica, para a utilização dos Dados Pessoais que são captados pela Polícia Civil do Distrito Federal?

Os dados biográficos e biométricos cadastrados nos sistemas do II/PCDF são utilizados para identificação e/ou confirmação da identidade de indivíduos relacionados a investigações policiais, processos administrativos e/ou judiciais, inclusive no caso de cadáveres de identidade duvidosa ou ignorada.

Respeitosamente,

Documento assinado eletronicamente por **RUBEN SERGIO VELOSO GUMPRICH - Matr.0058930-6**, **Diretor(a) do Instituto de Identificação**, em 05/10/2023, às 13:39, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **123965229** código CRC= **A0C39917**.

"Brasília - Patrimônio Cultural da Humanidade"
SPO, Lote 23, Bloco A, Complexo PCDF - Bairro Brasília - CEP 70.610-907 - DF
Telefone(s): (61)32074300
Sítio - www.pcdf.df.gov.br

Governo do Distrito Federal
Polícia Civil do Distrito Federal
Departamento de Inteligência, Tecnologia e Gestão da Informação
Divisão de Tecnologia

Nota Informativa n.º 15/2023 - PCDF/DGPC/DGI/DITEC Brasília-DF, 06 de outubro de 2023.

Senhor diretor,

Em atendimento ao despacho 123691180 de vossa senhoria que determina que as indagações apresentadas pelos itens 04, 07, 08 e 11 em manifestação encaminhada à Ouvidoria/PCDF através do sistema E -Sic (123455069), sejam devidamente respondidas, informo:

Quanto ao item 4 que questiona ***"A partir de que ano os Dados Pessoais foram inseridos nos sistemas informatizados da Polícia Civil do Distrito Federal?"*** temos a informar que considerando que para os fins da Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº13.709 de 14 de agosto de 2018, em seu art. 5º, inciso I define dado pessoal como:

> *"I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;"*

a Polícia Civil do Distrito Federal teve seu primeiro sistema automatizado de coleta de dados instituído em julho de 1991, denominado SIOCOP.

No item 7 em que questiona se ***"Os servidores administrativos da Polícia Civil do Distrito Federal possuem acesso ao Prontuário de Identificação Civil e ao Sistema onde são registradas as Ocorrências Policiais?"***, informa-que os sistemas possuem um controle de acesso e permissionamento que possibilitam que cada usuário acesse as informações que são necessárias para a execução de suas atividades laborais dentro de sua função. Muitas funções dos servidores públicos administrativos exigem a verificação ou processamento de dados pessoais para que eles possam cumprir com as responsabilidades e obrigações impostas por lei. Por exemplo, para processar pedidos e requerimentos de documentos, os servidores podem precisar verificar a identidade, renda e outras informações pertinentes. Dentre outros o acesso a dados pessoais permite que os servidores verifiquem a autenticidade das informações fornecidas e, assim, evitem fraudes que podem resultar em perdas financeiras para o estado.

Em relação ao item 8 em que questiona se ***"Existe algum setor que faça o monitoramento diário, semanal, quinzenal ou mensal dos acessos feitos aos sistemas que armazenam Dados Pessoais?"*** esta divisão não tem como informar, visto que na divisão de tecnologia o monitoramento vai além dos dados pessoais propriamente dito, o nível de monitoramento está relacionado a segurança dos dados de forma mais generalista.

Pelo entendimento desta divisão, a Lei Geral de Proteção de Dados (LGPD) do Brasil, Lei nº 13.709/2018, estabelece regras sobre o tratamento de dados pessoais, incluindo seu armazenamento, processamento e transferência, por entidades públicas e privadas.

O encargo de monitorar os acessos a sistemas que armazenam dados pessoais, bem como garantir a segurança dos dados, frequentemente recai sobre o chamado "Encarregado" ou "DPO (Data Protection Officer)" no contexto da LGPD. Entretanto, é importante ressaltar que a LGPD não especifica a

frequência (diária, semanal, quinzenal ou mensal) com que os acessos aos sistemas devem ser monitorados. A determinação da frequência de monitoramento pode depender da natureza do sistema, da sensibilidade dos dados armazenados e das práticas internas da organização, bem como das diretrizes e regulamentações subsequentes da ANPD.

O que a LGPD enfatiza é a necessidade de adotar medidas de segurança, práticas e processos organizacionais que garantam a proteção dos dados pessoais. Isso pode incluir o monitoramento regular dos acessos, a realização de auditorias e a verificação de possíveis vulnerabilidades nos sistemas.

E por fim, em relação ao item 11, em que questiona se ***"A Polícia Civil do Distrito Federal já sofreu algum incidente de vazamento de Dados Pessoais? Se sim, como a Polícia Civil do Distrito Federal atuou diante desse incidente? A Polícia Civil do Distrito Federal possui algum protocolo para atuar em caso de eventuais incidentes de vazamento de Dados Pessoais?"*** informo que o procedimento adotado quando identificado um incidente esta divisão informa o Gestor de Segurança da Informação e o Encarregado Setorial nomeados pela instituição, cabendo aos mesmos, além de informar o Encarregado Central e os titulares de dados, gerir para que a organização (controlador) tome as medidas necessárias para conter o incidente, investigar a causa e evitar recorrências, bem como, quando apropriado, mitigar os impactos para os titulares afetados. Suscintamente, se ocorrer um incidente de segurança, como uma violação de dados, o gestor de TI deve informar imediatamente o Encarregado, que tomará as medidas necessárias em termos de conformidade e comunicação.

Documento assinado eletronicamente por **SIMONE PEREIRA DUARTE FERREIRA - Matr.0078526-1**, **Agente de Polícia Civil**, em 06/10/2023, às 15:30, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **124111690** código CRC= **AE05443F**.

Governo do Distrito Federal
Polícia Civil do Distrito Federal
Gabinete do Delegado Geral
Divisão de Controle

Nota Informativa n.º 1/2023 - PCDF/DGPC/GABDG/DICON Brasília-DF, 10 de outubro de 2023.

Senhor Ouvidor,

Conforme estabelecido no Despacho (123691180) de lavra do Sr. Diretor do Departamento de Gestão da Informação - DGI - seguem as respostas constantes do pedido de acesso à informação no tocante às demandas repassadas ao Encarregado de Tratamento de Dados da Polícia Civil do Distrito Federal.

1) A Polícia Civil do Distrito Federal adota ações para garantir que o tratamento de dados esteja de acordo com a Lei Geral de Proteção de Dados?

Sim. A Policia Civil do Distrito Federal adota ações para garantir que os dados tratados estejam de acordo com a LGP, tendo sido feito um trabalho de adequação da Instituição por meio de contratação de empresa especializada para os fins. Algumas das ações realizadas: mapeamento de entrada e tratamento de dados pessoais; mapeamento dos riscos do tratamento; relatório de impacto a proteção de dados pessoais – DPIA; criação de Política de proteção de Dados Pessoais, Política de Cookies, Termo de Sigilo; gerenciamento dos pedidos dos titulares e dos Órgãos; gerenciamento de violações e notificações; nomeação do DPO; e eventos de conscientização.

2) Caso afirmativo, qual a finalidade da Polícia Civil do Distrito Federal, ao tratar os Dados Pessoais?

A Policia Civil do Distrito Federal realiza o tratamento de dados pessoais única e exclusivamente para o atendimento de sua finalidade pública, na persecução do interesse público, e com o objetivo de executar as suas competências legais e cumprir com as atribuições legais que lhe foram conferidas.

3) Por quanto tempo a Polícia Civil do Distrito Federal armazena os Dados Pessoais?

Não foi definida pela PCDF temporalidade desses dados.

12) Atualmente, o titular de Dados Pessoais pode consultar suas informações nos bancos de dados da Polícia Civil do Distrito Federal?

O requerente titular de dados pessoais ou seu representante legal pode consultar suas informações nos bancos de dados da PCDF da seguinte forma: realizar uma solicitação pelo OUV-DF direcionada ao tratamento de dados pessoais/Lei Geral de Proteção de Dados Pessoais (LGPD) ou presencialmente na Ouvidoria especializada da PCDF. Na solicitação deverá conter as informações necessárias para embasar o atendimento da manifestação solicitada pelo titular.

13) Esse titular mencionado acima pode solicitar a exclusão de algum Dado Pessoal?

Sim. Segundo as normas internas da PCDF, o titular de dados pessoais pode solicitar a eliminação de dados (art. 5º, XIV, LGPD): o titular de dados pessoais poderá requerer, a qualquer tempo, eliminação dos seus dados pessoais dos bancos de dados da PCDF. O Encarregado receberá a solicitação, verificará se os pressupostos iniciais (confirmação da existência de tratamento, legitimidade e competência) foram atendidos e se há alguma obrigação legal, legítimo Gerenciamento dos Pedidos dos Titulares e dos Órgãos interesse do Controlador ou outro motivo regulatório que impeça a eliminação dos dados pessoais do titular. Sendo possível realizar a eliminação de dados, o Encarregado demandará as áreas detentoras das informações para realizarem a efetiva eliminação dos dados pessoais do titular. A partir da confirmação de eliminação, ou não, o Encarregado responderá à solicitação do titular. Caso não seja possível tratar a solicitação ou eliminar os dados solicitados, o Encarregado enviará ao titular resposta à solicitação contendo justificativa para não atender à solicitação.

14) Existe na Polícia Civil do Distrito Federal algum DPO (Encarregado)?

A Polícia Civil do Distrito Federal (PCDF) nomeou, por meio da Portaria Nº 170, de 31 de Dezembro de 2021, publicada no Diário Oficial do DF de 04 de Janeiro de 2022, Luiz Fernando Alves Neto, Delegado de Polícia, como Encarregado pelo Tratamento de Dados Pessoais (DPO) na PCDF e Viviane da Cunha Bonato, Delegada de Polícia, como suplente, para desempenharem as funções previstas na Lei Geral de Proteção de Dados (LGPD), Nº 13.709, de 14 de agosto de 2018.

O encarregado pelo tratamento de dados pessoais possui a função de atuar como canal de comunicação entre instituição, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

TRATAMENTO DE DADOS PESSOAIS - DPO	
Endereço	SPO, Conjunto A, Lote 23, Complexo da PCDF, Ed. Sede - CEP 70.610-907
Responsável pelo DPO	Luiz Fernando Alves Neto
Cargo	Delegado de Polícia
E-mail	luiz.neto@pcdf.df.gov.br
Telefone	(61) 3207-4789
Instrumento de Designação	Portaria nº 170, de 31 de dezembro de 2021
Atribuições	I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

15) Como o titular de Dados Pessoais pode entrar em contato com o DPO?

O titular de Dados Pessoais pode entrar em contato com o DPO da PCDF por meio do e-mail: luiz.neto@pcdf.df.gov.br, ou pelo telefone (61) 3207-4789.

As informações acima constam no site da PCDF no endereço: https://www.pcdf.df.gov.br/transparencia/servico-de-informacao-ao-cidadao-sic

Luiz Fernando Alves Neto

Encarregado de Tratamento de Dados - DPO

Documento assinado eletronicamente por **LUIZ FERNANDO ALVES NETO - Matr.0237741-1**, **Diretor(a) da Divisão de Controle**, em 10/10/2023, às 14:43, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **124352774** código CRC= **E280E045**.

"Brasília - Patrimônio Cultural da Humanidade"
SPO , lote 23, Conjunto A, 1º Subsolo Ed. Sede Direção Geral - Bairro Setor Policial - CEP 70610-907 - DF
Telefone(s): (61) 32074025
Sítio - www.pcdf.df.gov.br

Governo do Distrito Federal
Polícia Civil do Distrito Federal
Delegacia-Geral da Polícia Civil
Comitê Gestor de Segurança da Informação e Comunicação

Despacho – PCDF/DGPC/CGSIC Brasília, 04 de outubro de 2023.

À Ouvidoria,

Assunto: Solicitação de informações, por meio do Participa DF, acerca do tratamento de dados pessoais na PCDF.

Exmo. Sr. Ouvidor da PCDF,

Em atendimento aos Despachos PCDF/DGPC/CGP/OUV (123878861) e PCDF/DGPC/DGI/GAB (123691180), passo a responder os itens 09 e 10 da Manifestação - E-Sic LAI-15637/2023 (123455069), formulada por DANIEL BASTOS MARWELL, visando instruir sua Tese de Doutorado em Direito Constitucional.

9) Os Dados Pessoais armazenados pela Polícia Civil do Distrito Federal são compartilhados com outros órgãos públicos?

Sim, com amparo no art. 7º, inciso III, da LGPD ("Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;").

10) A Polícia Civil do Distrito Federal implementa medidas de segurança da informação para a proteção de Dados Pessoais?

Sim, sendo que, segundo o art. 61 da Política de Segurança da Informação da PCDF, publicada no DODF nº 170 de 09/09/2022, "Art. 61. A ETIR deve tratar todos os incidentes que envolvam quebra de segurança da informação e comunicar imediatamente ao Encarregado Setorial da PCDF os que envolverem dados pessoais.". A Portaria nº 220, de 18/05/2023, que aprova o Documento de Constituição da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR da PCDF, encontra-se disponível para consulta pública no sítio eletrônico oficial da PCDF.

Na oportunidade, sugiro que todas as respostas, depois de compiladas e antes do envio ao solicitante, sejam encaminhadas ao Encarregado de Dados Pessoais (DPO) da PCDF para conhecimento e eventuais ajustes.

Respeitosamente,

MARIANA BORGES DA COSTA AGUIAR

Delegada de Polícia

Gestora de Segurança da Informação da PCDF

Documento assinado eletronicamente por **MARIANA BORGES DA COSTA AGUIAR - Matr. 0240537-7**, **Gestor(a) de Segurança da Informação e Comunicação**, em 04/10/2023, às 18:01, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **123921408** código CRC= **2345895E**.

"Brasília - Patrimônio Cultural da Humanidade"
SPO, lote 23, Conjunto A, Bloco A - Bairro Setor Policial - CEP 70610-907 - DF
Telefone(s): (61) 32075294
Sítio - www.pcdf.df.gov.br

Governo do Distrito Federal
Polícia Civil do Distrito Federal
Departamento de Inteligência, Tecnologia e Gestão da Informação
Serviço de Análise e Difusão de Informações

Nota Informativa n.º 7/2024 - PCDF/DGPC/DGI/SADI Brasília-DF, 04 de junho de 2024.

Sob nossa gestão e execução do contrato contabilizamos atualmente 17 acordos de Cooperação Técnica, sendo eles:

1- SPC/ORG - Processo SEI - 00052-00023934/2023-81 , onde temos acesso ao sistema de consultas dos mesmos, SPC JUD, sem contrapartida.

2 - DFLEGAL - Processo SEI - 04017-00012185/2023-53, onde acessamos o sistema SISAF e SIDAF e fornecemos em contrapartida PCDFNET, MILLENIUM E PROCED.

3 - CAESB - Processo SEI - 00052-00024854/2022-62, onde temos acesso ao sistema de consultas de cliente dos mesmos e fornecemos o PCDFNET.

4- CGDF - Processo SEI - 00480-00002848/2021-32, onde acessamos bancos de dados dos mesmos e fornecemos o PCDFNET.

5 - SPRF - Processo SEI - 00052-00009940/2021-64, onde acessamos o sistema ALERTA BRASIL e fornecemos o PCDFNET.

6- SEFAZ - Processo SEI - 00040-00012126/2021-11, onde acessamos o sistema SITAF e fornecemos o PCDFNET.

7 - TJDFT - Processo SEI - 00052-00007301/2021-64, onde acessamos o sistema SEEU e SISTJ/QVT e fornecemos PCDFNET, SICOLA, DIGIC, MILLENIUM, PROCED .

8 - SEJUSP/MS - Processo SEI - 00052-00023069/2020-21, onde acessamos o sistema SIGO, sem contrapartida.

9- MJSP - Processo SEI - 00052-00022742/2020-13, onde acessamos o sistema CÓRTEX, alguns bancos de dados, sem contrapartida.

10 - CARTORIO MG - Processo SEI - 00052-00015661/2020-59, onde temos acesso ao sistema de consultas dos mesmos, sem contrapartida.

11 - JUCIS/DF - Processo SEI - 00052-00008521/2020-24, onde temos acesso ao sistema de consultas dos mesmos, sem contrapartida.

12 - TRE/DF - Processo SEI - 00052-00019229/2019-01, onde acessamos o INFODIP e fornecemos o PCDFNET.

13- CODAHAB - Processo SEI - 00392-00008762/2019-51, onde acessamos bancos de dados dos mesmos e fornecemos o PCDFNET.

14 - DPF - Processo SEI - 00050-00017068/2019-60, onde acessamos o CINTEPOL e fornecemos o PCDFNET.

15 - MPDFT - Processo SEI - 0052-000557/2017, onde acessamos o PIN e o DILIGENTE e fornecemos o PCDFNET, SICOLA, DIGIC, MILLENIUM, PROCED .

16- SEAPE - Processo SEI - 0052-001895/2017, onde acessamos o SIAPENWEB e fornecemos o PCDFNET, SICOLA, MILLENIUM, PROCED e SIIC.

17 - ANOREG - Processo SEI - 0052-002117/2015, onde acessamos o CENSEC, CRC e ONR e fornecemos o PCDFNET.

Acrescento que existem outros Acordos celebrados e sob execução do CI/DGI, LABLD, DPELETRONICA e DITEL, onde apesar de sermos responsáveis, em parte, pelas contrapartidas, não temos nenhuma gestão sobre os mesmos.

Por fim informo que a DIPLANE catalogou sob demanda todos os ACTS envolvendo a PCDF, podendo também, S.M.J, ser consultada a qualquer tempo.

Atenciosamente,

LUCIANO ROCHA

Chefe da SADI/DGI

Documento assinado eletronicamente por **LUCIANO AURELIO DE ALMEIDA ROCHA - Matr.0057603-4, Agente de Polícia Civil**, em 04/06/2024, às 11:36, conforme art. 6º do Decreto nº 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **142473943** código CRC= **C8DB6AC0**.

"Brasília - Patrimônio Cultural da Humanidade"
SPO, Lote 23, conjunto A, Edfício Sede da Direção Geral, 2º Andar, Complexo da PCDF - Bairro SPO - CEP 70610-907 - DF
Telefone(s): 3207-4030
Sítio - www.pcdf.df.gov.br

Governo do Distrito Federal
Polícia Civil do Distrito Federal
Instituto de Criminalística do Departamento de Polícia Técnica
Divisão de Perícias Internas do Instituto de Criminalística

Manifestação - PCDF/DGPC/DPT/IC/DPI

Ao Ilmo. Diretor do Instituto de Criminalística,

Dr. Fábio Vasconcelos Braga

Senhor Diretor, visando fornecer a melhor resposta à Manifestação - E-Sic LAI-14014/2024 (147352292), acredito ser relevante informar que:

Nas investigações ocorridas na PCDF, os dispositivos digitais que podem conter vestígios de crimes são enviados para este Instituto de Criminalística, para a realização do exame pericial de informática.

O exame pericial de informática tem por objetivo:

1. Realizar a materialização dos vestígios digitais, o que é na maior parte das vezes alcançado com o procedimento conhecido como **extração de dados;**

2. Responder questionamentos levantados em relação aos vestígios digitais, objetivando alcançar subsídios para a determinação da dinâmica criminosa, além de buscar indícios que podem ajudar na determinação da autoria, o que é alcançado com a **análise dos dados extraídos**;

3. Elaboração do **Relatório Digital**, parte integrante do Laudo de Perícia Criminal, que é atrelado a este por meio do cálculo do HASH criptográfico. O Relatório Digital contém os dados achados relevantes pelo perito criminal que realizou os exames, e é fornecido em conjunto com um programa forense próprio para visualização e busca, que informa, dentre outros, os códigos HASH e os metadados de cada arquivo, além de seu conteúdo;

4. Tanto o Laudo de Perícia Criminal quanto o Relatório Digital ficam armazenados nos equipamentos de storage da PCDF, e são disponibilizados aos solicitantes por meio do sistema DigIC, que pode ser acessado na intranet da PCDF;

Todas as etapas do exame pericial de informática são embasadas, e precedem obrigatoriamente, de autorização judicial. A autorização delimita o que poderá ou não ser objeto dos exames, e assim compor o Laudo de Perícia Criminal. Apesar da delimitação imposta pela autorização judicial, **a etapa de extração de dados não pode ser realizada com delimitação**, devido a características técnicas dos dispositivos digitais e aos necessários procedimentos da informática forense. Então o conteúdo é primeiro extraído em sua totalidade, preferencialmente por meio da cópia física, e posteriormente analisado e filtrado.

Dessa forma, o produto final do exame pericial de informática é o **Laudo de Pericia Criminal** e o **Relatório Digital**, que contém os dados de interesse pericial. Os demais dados, que não estavam cobertos pela decisão judicial ou não foram vistos como relacionados ao caso pelo perito criminal, são descartados.

O Instituto de Criminalística armazena os Laudos de Perícia Criminal indefinidamente, assim como os relatórios digitais.