

**INSTITUTO BRASILIENSE DE DIREITO PÚBLICO – IDP  
ESCOLA DE DIREITO DE BRASÍLIA – EDB  
CURSO DE GRADUAÇÃO EM DIREITO**

**JAIRO FRANCISCO PACHECO RAMOS**

**A JURISDIÇÃO NOS CRIMES CIBERNÉTICOS: OS LIMITES DA JURISDIÇÃO  
PENAL E O PAPEL DO ESTADO NO COMBATE À CRIMINALIDADE  
CIBERNÉTICA**

Brasília – DF  
2017

**JAIRO FRANCISCO PACHECO RAMOS**

**A JURISDIÇÃO NOS CRIMES CIBERNÉTICOS: OS LIMITES DA JURISDIÇÃO  
PENAL E O PAPEL DO ESTADO NO COMBATE À CRIMINALIDADE  
CIBERNÉTICA**

Trabalho de Monografia, apresentada ao  
Curso de Graduação em Direito do  
Instituto Brasiliense de Direito Público –  
IDP como requisito para obtenção do  
título de bacharel.

Orientador: Prof. Dr. Flávio Daher

Brasília - DF  
2017

**JAIRO FRANCISCO PACHECO RAMOS**

**A JURISDIÇÃO NOS CRIMES CIBERNÉTICOS: OS LIMITES DA JURISDIÇÃO  
PENAL E O PAPEL DO ESTADO NO COMBATE À CRIMINALIDADE  
CIBERNÉTICA**

Monografia, apresentada ao Curso de  
Direito do Instituto Brasiliense de Direito  
Público – IDP como requisito para  
obtenção do título de bacharel.

Local, \_\_\_\_ de \_\_\_\_\_ de \_\_\_\_\_.

---

Prof.  
Professor Orientador

---

Prof.  
Membro da Banca Examinadora

---

Prof.  
Membro da Banca Examinadora

## RESUMO

O presente trabalho tem como proposta compreender a relação entre a jurisdição e os crimes cibernéticos em vista de um ofendido brasileiro presente no território nacional, questionando a possibilidade de o Poder Judiciário brasileiro ser apto a exercer a sua jurisdição para todo e qualquer delito realizado por meios informáticos em que a vítima seja um nacional. Para tanto, deve-se compreender como a internet funciona, isto é, a sua arquitetura, de forma que se possa entender o fenômeno a que se está a estudar, assim como o conceito de jurisdição e o seu desenvolvimento ao decorrer do tempo. Além disso, analisa-se a importância da cooperação jurídica internacional diante das inovações tecnológicas.

Palavras-chave: Crimes cibernéticos, jurisdição, internet, cooperação jurídica internacional.

## **ABSTRACT**

The present work aims to understand the relation between jurisdiction and cybercrimes in view of a Brazilian offended that is inside the national territory, questioning the possibility of the Brazilian Judicial Power to exercise its jurisdiction for all and any crimes that uses computerized means on which the victim is a national. For this purpose, it is important to understand how the internet works, i.e., its architecture, in a way that it can be understood what is the phenomenon that we are currently studying, as well as the concept of jurisdiction and its development in the course of time. In addition, the importance of the international judicial cooperation is analyzed in the face of the technological innovations.

Keywords: Cybercrimes, jurisdiction, internet, international judicial cooperation.

## SUMÁRIO

<b>INTRODUÇÃO .....</b>	<b>9</b>
<b>1 A ARQUITETURA DA INTERNET .....</b>	<b>12</b>
1.1 O que é a internet .....	12
1.2 Protocolos: Conceito e a Arquitetura da Rede .....	17
1.2.1 A camada de aplicação .....	19
1.2.1.1 As arquiteturas de uma aplicação de rede: Redes cliente-servidor e Redes ponto a ponto .....	20
1.2.1.2 A Web .....	22
1.2.1.2.1 O funcionamento da Web: HTTP e HTML .....	24
1.2.1.3 A transferência de arquivos: o FTP .....	27
1.2.1.4 O serviço de diretório da internet: o DNS .....	28
1.2.1.5 As camadas de apresentação e sessão .....	31
1.2.2 A camada de transporte .....	31
1.2.3 A camada de rede .....	34
1.2.4 A camada de enlace .....	36
1.2.5 A camada física .....	37
1.3. Direito e internet .....	37
<b>2 A JURISDIÇÃO .....</b>	<b>39</b>
2.1 O conceito de jurisdição .....	39
2.2 Os escopos da jurisdição .....	41

2.2.1 Os escopos sociais .....	42
2.2.2 Os escopos políticos .....	43
2.2.3 Os escopos jurídicos .....	45
2.3 O conceito contemporâneo de jurisdição .....	46
2.4 Os limites da jurisdição penal .....	51
2.5 A aplicação da Lei penal no Direito Brasileiro .....	53
2.5.1 O princípio da territorialidade: A regra geral .....	53
2.5.2 Os demais princípios e as condições da extraterritorialidade .....	55
2.6 O local do crime .....	59
2.7 A jurisdição e a internet .....	60
<b>3 OS CRIMES CIBERNÉTICOS .....</b>	<b>69</b>
3.1 A segurança na rede: Os seus elementos .....	71
3.2 O conceito de crimes cibernéticos .....	73
3.3 O bem jurídico em questão .....	74
3.4 Crimes cibernéticos próprios tipificados no Brasil .....	75
3.4.1 Invasão de dispositivo informático .....	76
3.4.2 Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública .....	80
3.4.3 Falsidade de cartão .....	81
3.5 Os crimes cibernéticos impróprios no Brasil .....	81
3.6 Os crimes cibernéticos e a jurisdição brasileira .....	82
<b>4 COOPERAÇÃO JURÍDICA INTERNACIONAL .....</b>	<b>90</b>
4.1 O conceito de cooperação jurídica internacional .....	92

<b>4.2 Extradução .....</b>	<b>92</b>
<b>4.3 Cartas rogatórias .....</b>	<b>95</b>
<b>4.4 Homologação de sentença estrangeira .....</b>	<b>98</b>
<b>4.5 Transferência de presos .....</b>	<b>99</b>
<b>4.6 Auxílio direto .....</b>	<b>100</b>
<b>4.7 Como o auxílio direto permite o combate ao crime cibernético .....</b>	<b>104</b>
<b>4.8 Limites às informações espontâneas .....</b>	<b>107</b>
<b>4.9 A importância do Brasil no cenário internacional no combate ao crime cibernético .....</b>	<b>109</b>
<b>CONCLUSÃO .....</b>	<b>111</b>
<b>REFERÊNCIAS .....</b>	<b>117</b>

## INTRODUÇÃO

Hoje nos deparamos, cada vez mais, com uma sociedade informatizada, em que as pessoas se veem gradualmente mais inseridas no universo tecnológico, seja por meio de *tablets*, telefones celulares ou até mesmo suas *smart tvs*, ocorrendo este acesso, principalmente, por meio da internet.

As pessoas estão se voltando gradualmente para este ambiente virtual, estabelecendo relações por este meio, assim como apresentando em suas páginas pessoais as suas últimas atividades, como o fato de ter ido a um restaurante ou fez algo relacionado a um hobby seu.

Entretanto, grande parte destes produtos é recente e apesar de trazerem várias benesses para toda a sociedade, ainda assim ela proporciona possibilidades para que atividades criminosas ocorram.

Conforme o *Norton Cyber Security Insights Report 2016* (SYMANTEC, 2016), o total de consumidores que sofreu em razão de crimes cibernéticos no ano anterior era de 42,4 milhões de brasileiros. Este número é claramente elevado e aponta uma tendência e uma necessidade.

Primeiramente, a tendência que se demonstra clara é o aumento de pessoas que fazem uso da internet no seu dia a dia. Veja-se, caso os brasileiros não se utilizassem deste meio, o número de consumidores afetados por crimes cibernéticos seria bem menor.

Não se afirma tão somente com base neste número. Há que se notar que as pessoas desejam participar desse novo ambiente, tendo em vista a quantidade de indivíduos que acessam, por exemplo, o sítio *facebook*, em que, conforme a empresa, 102 milhões de brasileiros se conectam a plataforma todos os meses, sendo que 93 milhões são por meio de dispositivos móveis (FACEBOOK, 2016).

O mundo virtual está claramente em desenvolvimento e o brasileiro está participando deste movimento, principalmente em redes sociais, como se viu acima. Portanto, a tendência é justamente o aumento de pessoas utilizando a internet.

Por sua vez, a necessidade se revela pela necessidade de se proteger estas pessoas ou ao menos encontrar alguma forma para reduzir a criminalidade neste ambiente, ainda mais com o crescente número de usuários.

Veja-se que em 2015, conforme a Agência Brasil (BOCCHINI, 2016), o número de brasileiros que acessavam a internet era de 102 milhões, representando um crescimento de 5% da quantidade de usuários registrados no ano de 2014. Considerando esse número e comparando com aquele apresentado pela empresa *Symantec*, tem-se aproximadamente 41% dos brasileiros já sofreu em razão de algum crime cibernético, sendo esta uma taxa muito alta.

Não corresponderia à realidade, todavia, considerar a internet apenas no Brasil, tendo em vista que há, definitivamente, uma facilidade de acesso a qualquer sítio do mundo, desde que seja público. Nesta nota, percebe-se que os crimes realizados pelo ambiente virtual não precisam ser realizados aqui no Brasil, pois, ao acessar a internet, o usuário está sujeito a atividades que podem ocorrer em território diverso do país que está situado.

Diante disto, percebe-se que os crimes cibernéticos apresentam, possivelmente, em razão de sua própria natureza, dificuldades investigativas, assim como em relação à sua repressão, pois ainda que o ofendido seja uma pessoa situada no território de determinada autoridade policial, tem-se que o infrator pode estar em outro Estado, longe da competência daquele primeiro.

Portanto, o presente trabalho se propõe a compreender em que medida a legislação penal brasileira é capaz de realizar a defesa dos interesses de seus nacionais em face de crimes cibernéticos cometidos no exterior, questionado se as regras referentes à jurisdição são suficientes e, nesta impossibilidade, qual a alternativa para suprir esta necessidade de proteção do ofendido brasileiro.

Para tanto, analisando-se a questão, tendo em vista o desenvolvimento do instituto da cooperação jurídica internacional nos anos recentes, tem-se que esta poderá ser a resposta para que o Brasil possa reprimir, em conjunto com os demais Estados, as condutas criminosas realizadas através da internet.

Sendo assim, o primeiro capítulo se propõe a compreender o que é a internet e como ela funciona, baseando-se, principalmente, na sua arquitetura e tendo como foco a área usualmente utilizada pelos diversos usuários, que é a *Web*.

Em seguida, o segundo capítulo deseja entender o desenvolvimento da jurisdição, ressaltando-se uma possível concepção atual do termo, e como ocorre a aplicação da lei penal no espaço, tendo em vista que o entendimento da jurisdição penal se liga, necessariamente, a este último. Além disso, voltou-se à compreensão

de como a jurisdição se aplica à internet, tendo em vista a sua própria natureza, verificando algumas posições com relação à aplicação do direito neste ambiente.

O terceiro capítulo, por sua vez, aborda os crimes cibernéticos no Brasil e explora mais a fundo a questão da possibilidade ou não de este país aplicar a sua lei perante todo e qualquer crime realizado por meio informático que tenha um nacional como vítima.

Por fim, o quarto capítulo passa a analisar como se dá a cooperação jurídica internacional e assinala uma forma pela qual os Estados podem se auxiliar para reduzir a criminalidade cibernética.

## **1 A ARQUITETURA DA INTERNET**

Para que existam leis sobre determinado assunto, verifica-se a necessidade de se compreender o evento natural, se este existir, para que a regulação exista. Por exemplo, o crime de homicídio existe por decorrência do fato natural de um indivíduo matar alguém e esta conduta ser repugnada pela sociedade.

Portanto, para que as relações sejam normatizadas, nota-se a relevância de sua compreensão natural, como elas ocorrem no seio da sociedade para que se possa concretizar a relação jurídica.

Desta forma, compreender a realidade que a norma jurídica visa a tratar se torna de suma importância, inclusive para evitar a edição normas que não possuem qualquer relevância para a atividade em questão e não atingem o fim necessário.

Além disso, a internet se torna cada dia mais um importante objeto da sociedade, principalmente em vista da nomenclatura adotada de nosso estágio atual, que é a sociedade da informação. A todo o momento recebemos por nossos dispositivos eletrônicos diversas informações, de diversas fontes, e disponibilizamos outras por nós mesmos, por meio de envio de mensagens, e-mails e, inclusive, comentários em um sítio eletrônico.

Compreender o que é e como a internet funciona, neste sentido, é entender o que se pretende regular e qual a forma mais eficaz de tratar desta questão.

Entretanto, devido a grande complexidade do tema e o pequeno espaço disponível para tratar sobre ele, considera-se relevante abordar, como já dito, o conceito e o funcionamento da internet, mas, neste campo, focar principalmente na camada de aplicação, que será explicada em momento oportuno, eis que esta é a que possui maior repercussão em nossa sociedade, pois é onde o serviço *Web* é acessado.

### **1.1 O que é a internet**

Para iniciarmos o nosso estudo, podemos utilizar o conceito utilizado por Cristos Velasco San Martín, auto do livro *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet*, para, posteriormente, entrar em alguns detalhes técnicos.

Este autor conferiu a seguinte definição:

*En términos generales, podemos definirlo como un sistema global descentralizado de redes de cómputo interconectadas entre sí con base en los estándares o protocolos conocidos como Protocolo de Transmisión de Control (TCP) y el Protocolo Internet (IP) que se utilizan para transmitir e intercambiar paquetes de datos<sup>1</sup> (2012).*

Nota-se a relevância de alguns conceitos desde logo. Devemos compreender o que são protocolos, diante de estes serem fundamentais ao funcionamento da internet, assim como o que seriam os pacotes de dados e o que eles contêm.

Kurose e Ross (2013, p. 2), por sua vez, em obra direcionada ao entendimento da arquitetura da internet, reconhecem que é possível compreender o conceito de internet por duas perspectivas, sendo uma por meio dos “componentes de *software* e *hardware* básicos que a formam”, enquanto que o segundo se dá através da descrição da “internet em termos de uma infraestrutura de redes que fornece serviços para aplicações distribuídas”.

Seguindo esta linha, conforme os componentes da rede compreende-se que ela é formada por diversos chamados “hospedeiros ou sistemas finais” (KUROSE; ROSS, 2013, p. 3), sendo estes todos os dispositivos ligados à rede, podendo ser os usuais computadores de mesa, como os novos telefones celulares, *tablets*, *smart* TVs, entre outros.

A conexão destes diversos dispositivos se dá por “enlaces (*links*) de comunicação e comutadores (*switches*) de pacotes” (KUROSE; ROSS, 2013, p. 3), em que os primeiros se referem à transmissão de dados<sup>2</sup>, enquanto o segundo é aquele que redireciona os dados para o destinatário final<sup>3</sup>.

A comunicação entre os sistemas finais se dá por meio da transferência de pacotes de informação, ou somente pacotes, que são a forma pela qual os dados

---

<sup>1</sup> Em termos gerais, podemos definir a internet como um sistema global descentralizado de redes de computador interconectadas entre si com base nos padrões ou protocolos conhecidos como Protocolo de Controle de Transmissão (TCP) e o Protocolo da Internet (IP), estes que são utilizados para transmitir e trocar pacotes de dados (tradução livre).

<sup>2</sup> Devem-se entender os enlaces como a parte física que possibilita a conexão entre os diversos usuários, como os “cabos coaxiais, fios de cobre, fibras óticas e ondas de rádio” (KUROSE; ROSS, 2013, p. 3). A principal diferença entre estes meios é a taxa de transmissão, isto é, a velocidade em que eles são transmitidos por essas estruturas.

<sup>3</sup> Os comutadores se dividem em comutadores ou roteadores. Os comutadores são “utilizados em redes de acesso, enquanto os roteadores são utilizados principalmente no núcleo da rede” (KUROSE; ROSS, 2013, p. 3).

são enviados por meio da rede. São estes que são liberados pelos enlaces e redirecionados pelos comutadores.

Não seria possível desconsiderar a forma de acesso à internet por estes sistemas finais, que se realiza pelos Provedores de Serviços de Internet, ou ISPs (*Internet Service Providers*), considerando-se que estes fornecem alguns serviços:

(...) oferecem aos sistemas finais uma variedade de tipos de acesso à rede, incluindo acesso residencial de banda larga como modem a cabo ou DSL (linha digital de assinatura), acesso por LAN de alta velocidade, acesso sem fio e acesso por modem discado de 56 kbits/s. ISPs também fornecem acesso a provedores de conteúdo, conectando sites diretamente à internet (KUROSE; ROSS, 2013, p. 3).

No entanto, o controle de envio e recebimento de informações não se dá de qualquer forma, tendo em vista que depende da execução de protocolos. Conforme o conceito já apontado, os mais relevantes são o TCP e o IP, notando-se que este tem o objetivo de especificar “o formato dos pacotes que são enviados e recebidos entre roteadores e sistemas finais” (KUROSE; ROSS, 2013, p. 4). Os protocolos serão estudados mais à frente.

Como é possível notar, são diversos os componentes da rede, mas estes são apenas alguns, ainda que fundamentais para o seu funcionamento.

O segundo conceito parte da noção de que a internet se trata de uma infraestrutura de redes que fornece serviços para aplicações distribuídas, este que são de uso corrente da sociedade como “correio eletrônico, navegação na *Web*, redes sociais, mensagem instantânea, Voz sobre IP(VoIP), vídeo em tempo real, jogos distribuídos,” (KUROSE; ROSS, 2013, p. 4), entre outros.

Como já estabelecido, esta é a parte que todos os usuários da internet utilizam e possuem algum grau de conhecimento, diversamente do que ocorre com relação à transferência dos dados em si, ou o sua ocasional criptografia. Entretanto, esta é apenas uma parte da arquitetura da rede, como demonstraremos abaixo.

A partir dos conceitos entregues, poder-se-ia conceber que a internet é uma grande rede de computadores, mas não isso não é correto. Os sistemas finais se ligam, na realidade, a uma rede, usualmente local (*LAN*<sup>4</sup>), para que, quando tentem

---

<sup>4</sup> Ou *Local Area Network*, sendo mais conhecida como rede local, é o tipo mais comum de rede, abrangendo o espaço de uma sala, escritório ou mesmo um prédio inteiro. (TORRES, 2015).

se comunicar com computadores que estão conectados a outra rede, se utilizem dos chamados *switches*, ou roteadores, para efetuar a comunicação.

Douglas E. Comer (2007, p. 110) expressa bem esta perspectiva ao estabelecer que “*the internet is not a single computer network. Instead, it consists of thousands of computer networks interconnected by dedicated, special-purpose computers called routers*”<sup>5</sup>.

Esta atividade dos roteadores é principalmente relevante em vista da sua função de conectar diversas redes com diferentes tecnologias, possibilitando a comunicação entre os diversos computadores. Um exemplo disso é a possibilidade de conexão entre uma “*Local Area Network and a Wide Area Network*”<sup>6</sup> (COMER, 2007, p. 110).

Essa noção se torna importante, justamente, para compreender que a internet é, na realidade, uma rede de redes.

Aprofundando-se na questão dos Provedores de Serviços de Internet, têm-se que eles fornecem, para os diversos tipos de consumidores, meios para que eles se conectem ao que conhecemos como internet. Antigamente era comum o uso da internet discada e, hoje, a banda larga predomina, verificando-se a diferença entre elas pela velocidade em que o acesso ocorre.

Entretanto, esta relação entre o consumidor e o Provedor é “uma pequena peça do quebra-cabeça que é interligar os bilhões de sistemas finais que compõem a internet”, que se realiza “criando uma rede de redes” (KUROSE e ROSS, 2013, p. 24).

Para compreender melhor qual seria o papel dos provedores, é necessário que se tenha em mente a abrangência de seus serviços. Eles se dividem em provedores locais, regionais e os chamados “*major ISPs*”, “*large ISPs*” (COMER, 2007, p. 113) ou “ISPs de nível 1” (KUROSE e ROSS, 2013, p. 24).

Trata-se de uma relação hierárquica, então, entre os diversos provedores, em que os Provedores de nível 1(um) irão fornecer ligações globais entre os diversos provedores, inclusive entre os de mesmo nível, garantindo que as mais diversas redes de computadores estejam, de fato, interligadas.

---

<sup>5</sup> A internet não é apenas uma rede de computadores. Na realidade, ela é formada por várias redes de computadores interligadas por computadores dedicados que suprem um específico propósito, chamados de roteadores (tradução livre).

<sup>6</sup> Também chamada rede de longa distância, abrange uma área maior do que apenas uma cidade (TORRES, 2015).

Comer explica bem como a hierarquia entre os diversos provedores funciona, adotando-se o ponto de vista da forma como ocorre o deslocamento dos pacotes de dados. Ele diz:

*To understand the hierarchy, consider two subscribers that are geographically distant. Assume that each subscriber connects to a local ISP in his or her area, and consider what happens when they communicate. When a message is sent, a packet travels from the sender's computer across an access network to the subscriber's local ISP. The local ISP forwards the packet to a regional ISP, which, in turn, forwards the packet to a tier 1 provider. If the destination is only reachable through another tier 1 provider, the packet passes across a peering point, and across a second tier 1 backbone. Once a packet reaches a regional ISP near the destination, the regional ISP forwards the packet to the correct local ISP, which then delivers the packet to its destination over an access network. Of course, each ISP along the path contains multiple networks and routers, and a packet may traverse many networks as it travels through an ISP<sup>7</sup> (2007, p. 114).*

Entretanto, a internet de hoje é ainda mais complexa, em que existem ligações não só entre os de maior e menor hierarquia, mas também aqueles de mesmo nível, como os provedores regionais, os chamados pontos de troca da internet e as redes de provedores de conteúdo.

Existe o *PoP*, que é “simplesmente um grupo de um ou mais roteadores (no mesmo local) na rede do provedor, onde os ISPs clientes podem se conectar no ISP provedor”. (KUROSE; ROSS, 2013, p. 25). Além disso, é possível que o provedor opte pela utilização de um multi-home, que significa “conectar-se a dois ou mais ISPs provedores”.

Os pontos de troca da Internet, por sua vez, são quando um terceiro decide estabelecer um “ponto de encontro onde vários ISPs podem se emparelhar”

---

<sup>7</sup> Para entender a hierarquia, considere que dois assinantes (consumidores de provedores) estão geograficamente distantes. Assuma que cada um deles se conecta a um provedor local em sua área, e considere o que acontece quando eles se comunicam. Quando a mensagem é enviada, um pacote se desloca do computador de quem o está enviado através de uma rede de acesso até a rede local deste usuário. O provedor local irá remeter este pacote para um provedor regional, que, por sua vez, irá remeter este mesmo pacote para um provedor de nível 1. Se o destino só for alcançado por meio de um outro provedor de nível 1, o pacote irá atravessar o chamado “peering point” ( que é a nomenclatura utilizada para se referir à ligação entre estes tipos de provedores), além da própria espinha dorsal( esta que é considerada uma WAN de maior grau à qual diversas redes se ligam) do segundo provedor de nível 1. Assim que um pacote chega ao provedor regional próximo ao seu destino, este irá remeter aquele para o provedor local específico, que, então, entrega o pacote para o seu destino por meio de uma rede de acesso. É claro que cada provedor, ao longo do caminho, possui diversas redes e roteadores, e um pacote pode atravessar várias destas redes enquanto se desloca por um provedor (tradução livre).

(KUROSE e ROSS, 2013, p. 25), sendo esta a forma pela qual provedores de menor hierarquia fazem ligações entre si para reduzirem os custos referentes à conexões com provedores superiores.

Por fim, as redes de provedores de conteúdo são aquelas que possibilitam a transferência mais rápida de informações entre centros de dados de determinada empresa, sendo, portanto, privada. Desta forma, o provedor de conteúdo “não apenas reduz seus pagamentos aos ISPs da camada mais alta, mas também tem maior controle de como seus serviços por fim são entregues aos usuários finais” (KUROSE; ROSS, 2013, p. 26).

Portanto, ainda que a internet não seja uma grande e única rede, como se poderia imaginar, ela é formada por diversas outras redes que possuem a sua devida importância para que os dados se desloquem entre os usuários finais.

O serviço fornecido por estes provedores é vital para que os diversos tipos de sistemas consigam se comunicar. A tecnologia de um celular acessando a internet via o 3G não é a mesma que um computador utilizando-se de sua placa de rede Wi-Fi, mas os respectivos roteadores são capazes de fazer com que os pacotes por eles enviados cheguem a seus respectivos destinatários.

Compreendida esta primeira parte, devemos seguir para, então, entendermos o papel dos protocolos nesta relação.

## **1.2 Protocolos: Conceito e a Arquitetura da Rede**

Para Gabriel Torres (2015), “grosso modo, protocolo é a ‘linguagem’ usada para computadores ‘conversarem’ em uma rede”.

No mesmo sentido, Comer (2007, p. 127) ainda informa que “*the term derives from diplomatic vocabulary, in which a protocol specifies the rules under which a diplomatic exchange occurs*”<sup>8</sup>.

Portanto, compreende-se a comunicação entre os usuários finais se dá por meio destes chamados protocolos, que estabelecem uma forma para que eles consigam se entender.

---

<sup>8</sup> O termo deriva do vocabulário diplomático, em que o protocolo especifica as regras que regem a troca diplomática (tradução livre).

Além disso, a fim de facilitar o entendimento acerca do funcionamento destes, e da própria comunicação das redes, criaram-se as camadas de protocolos. Conforme Kurose e Ross:

O sistema de camadas de protocolos tem vantagens conceituais e estruturais [RFC 3439]. Como vimos, a divisão em camadas proporciona um modo estruturado de discutir componentes de sistemas. A modularidade facilita a atualização e componentes de sistema (2013, p. 37).

O conhecido TCP/IP não é, na realidade, um protocolo, mas sim um “conjunto de protocolos” ou “pilha de protocolos” (TORRES, 2015), sendo que, neste caso, ela se divide em cinco camadas: física, de enlace, de rede, de transporte e de aplicação.

Interessante notar que uma “camada de protocolo pode ser executada em software, em hardware, ou em uma combinação dos dois” (KUROSE; ROSS, 2013, p. 37), a depender de suas individualidades.

Além desse modelo, há ainda o chamado modelo OSI, instituído pela Organização Internacional para Padronização, “propôs que as redes de computadores fossem organizadas em, mais ou menos, sete camadas” (KUROSE; ROSS, 2013, p. 39), diferenciando-se apenas a presença das camadas de apresentação e sessão.

Ainda assim, torna-se relevante este estudo em face do afirmado por Torres:

Em teoria cada camada seria de responsabilidade de um protocolo específico – e por isso falamos em um conjunto ou “pilha” de protocolos. Na prática, a maioria das pilhas de protocolos existente – como o TCP/ IP, o IPX/ SPX e o NetBEUI – não segue esse modelo de referência ao pé da letra, usando protocolos que correspondem a mais de uma camada do modelo OSI. Todavia, o estudo deste modelo é extremamente didático, pois através dele há como entender como deveria ser um “protocolo ideal”, bem como facilita enormemente a comparação do funcionamento de protocolos criados por diferentes fabricantes (2015).

De acordo com Torres, é possível dividir as camadas do modelo OSI, e por consequência do TCP/IP, em três grupos, sendo eles a de aplicação, transporte e rede. O primeiro é composto pelas camadas de aplicação, apresentação e sessão, enquanto o último é composto pelas camadas de rede, link de dados (ou enlace) e

física. Logicamente, o grupo de transporte é composto pela camada de transporte. São as funções de cada grupo:

As camadas de rede se preocupam com a transmissão e recepção dos dados através da rede e, portanto, são camadas de baixo nível. A camada de transporte é responsável por pegar os dados recebidos pela rede e repassá-los para as camadas de aplicação de uma forma compreensível, isto é, ela pega os pacotes de dados e transforma-os em dados quase prontos para serem usados pela aplicação. As camadas de aplicação, que são camadas de alto nível, colocam o dado recebido em um padrão que seja compreensível pelo programa (aplicação) que fará uso desse dado (2015)

Esta divisão se torna interessante principalmente por estabelecerem padrões comuns das camadas pertencentes ao mesmo grupo e determinar a relação entre estes, facilitando a compreensão dos modelos.

Qualquer que seja o modelo adotado, a interação entre as diversas camadas se dá por meio de um fenômeno que se chama encapsulamento, em que, “na transmissão de um dado, cada camada pega as informações passadas pela camada superior, acrescenta informações pelas quais ela seja responsável e passa os dados para a camada imediatamente inferior” (TORRES, 2015).

De qualquer forma, tem-se que o pacote de informação será formado na camada de aplicação de um usuário final para, então, se deslocar por todas as outras camadas, sempre se adicionando algo, para chegar até outro usuário final, local em que a informação será recebida pela camada de aplicação.

Diante disto, requer-se um estudo mais aprofundado das camadas de protocolo, especialmente da de aplicação e de transporte, em razão de elas formarem a base do funcionamento de toda a internet.

### *1.2.1 A camada de aplicação*

Sinteticamente, pode-se afirmar que nesta é “onde residem aplicações de rede e seus protocolos”. Nesta camada é possível se encontrar, dentre outros, o “HTTP (que provê requisição e transferência de documentos pela *Web*), o SMTP (que provê transferência de mensagens de correio eletrônico) e o FTP (que provê a transferência de arquivos entre dois sistemas finais)” (KUROSE; ROSS, 2013, p. 37).

Como já vimos anteriormente, são diversos os aplicativos que a internet oferece, como é o caso do Skype, YouTube, Netflix e da Web.

Nesta camada, a aplicação “utiliza o protocolo para trocar pacotes de informação com a aplicação em outro sistema final”, sendo que estes pacotes também podem ser chamados de “mensagem” (KUROSE; ROSS, 2013, p. 38) quando nesta camada.

Nos dizeres de Torres (2015), “a camada de aplicação faz a interface entre a pilha de protocolos e o aplicativo que pediu ou receberá a informação através da rede”.

#### *1.2.1.1 As arquiteturas de uma aplicação de rede: Redes cliente-servidor e Redes ponto a ponto*

Dentre as diversas arquiteturas de aplicação, sendo esta uma escolha do programador que a está projetando, duas são as mais utilizadas, sendo elas as redes cliente-servidor ou ponto a ponto, ou P2P.

Quanto à primeira, a rede cliente-servidor, “há um hospedeiro sempre em funcionamento, denominado servidor, que atende a requisições de muitos outros hospedeiros denominados clientes” (KUROSE; ROSS, 2013, p. 62).

Usualmente, conforme Comer, a comunicação entre o servidor e o cliente funciona da seguinte forma:

*Usually, people who use Internet services run client software. For example, a typical application program that uses the Internet to access a service becomes a client. The client uses the Internet to communicate with a server. For some services, the client interacts with the server using one request. The client forms a request, sends it to the server, and awaits a reply. For other services, the client engages in a long-term interaction. The client establishes communication with the server, and then continuously displays the data received from the server, while it transmits keystrokes or mouse input to the server<sup>9</sup> (2007, p. 146).*

---

<sup>9</sup> Usualmente, as pessoas que usam os serviços da internet rodam um software de cliente. Por exemplo, um programa de aplicação típica que usa a Internet para acessar o serviço se torna um cliente. Este cliente usa a Internet para se comunicar com um servidor. Para alguns serviços, o cliente interage com o servidor utilizando um requerimento. O cliente cria o requerimento, envia para o servidor e espera a resposta. Para outros serviços, o cliente inicia uma comunicação de longo termo. O cliente estabelece a comunicação com o servidor, e, então, continuamente exibe os dados recebidos do servidor, enquanto que o cliente transmite as teclas digitadas e os cliques de mouse para o servidor (tradução livre).

Um exemplo clássico, inclusive utilizado por Kurose e Ross, é a aplicação *Web*, em que o servidor sempre está conectado à internet, fornecendo as informações requeridas pelos diversos clientes.

Entretanto, o servidor não se restringe apenas à *Web*, tendo outros típicos exemplos, dentre eles “impressão, arquivos, *web*, correio eletrônico (e-mail), serviços de diretório etc.” (TORRES, 2015), tudo a depender do serviço que o servidor pretende fornecer, sendo possível até que mais de um destes esteja disponível para o cliente em um mesmo servidor.

Para demonstrar os diversos serviços que um servidor pode fornecer, Comer (2007, p. 144) assinala que “*one can send a message to a friend, retrieve a file, browse through directories, search a database, print a document, transmit a fax, or listen to music*”<sup>10</sup>.

São três as características principais desta estrutura, sendo elas: o funcionamento contínuo do servidor, “os clientes não se comunicam diretamente uns com os outros” e o “servidor tem um endereço fixo, bem conhecido denominado endereço IP” (KUROSE; ROSS, 2013, p. 62).

Ora, de nada adiantaria que o serviço fosse ininterrupto se o cliente não soubesse como acessar o servidor, sendo assim ele é conhecido pelo seu endereço IP, ou, mais comumente, pelo seu chamado “nome de hospedeiro (*hostname*)”, sendo este o preferido entre as pessoas “por ser mais fácil de lembrar” (KUROSE; ROSS, 2013, p. 95 e 96). Alguns exemplos clássicos de *hostnames* são google.com, yahoo.com, facebook.com, entre outros.

Inclusive, para que seja possível utilizar o nome de hospedeiro, “é necessário um serviço de diretório que traduza nomes de hospedeiro para endereços IP”, sendo esta a função do “DNS (*domain name system* – sistema de nomes de domínio) da internet” (KUROSE e ROSS, 2013, p. 96). Ou seja, há diversos servidores de diretório que contêm os respectivos nomes dos domínios e redirecionam ao endereço IP visado.

De qualquer forma, a arquitetura cliente-servidor é uma das duas mais utilizadas para as aplicações, sendo que a outra é a arquitetura ponto a ponto.

---

<sup>10</sup> Alguém pode enviar uma mensagem para um amigo, recuperar um arquivo, procurar (algo) através de diretórios, procurar (algo) em uma database, imprimir um documento, transmitir um fax, ou escutar música (tradução livre).

Diferentemente do que ocorre na outra estrutura, na arquitetura ponto a ponto, “a aplicação utiliza a comunicação direta entre duplas de hospedeiros conectados alternadamente, denominados pares, (...) sem passar por nenhum servidor dedicado” (KUROSE; ROSS, 2013, p. 63).

Torres define bem a diferença entre as duas arquiteturas, como se demonstra abaixo:

A maior diferença entre uma rede ponto a ponto e uma cliente/servidor é a ausência de um serviço de diretório, isto é, uma administração centralizada, um local onde usuários podem se autenticar e que vai dizer o que aquele usuário pode ou não pode fazer naquela rede. Com isso redes ponto a ponto são menos seguras e viáveis apenas para redes pequenas (2015).

Kurose e Ross (2013, p. 64) ainda caracterizam esta arquitetura pela sua autoescalabilidade, isto é, no caso de uma “aplicação de compartilhamento de arquivos P2P, embora cada par gere uma carga de trabalho solicitando arquivos, também acrescenta capacidade de serviço ao sistema”.

Alguns exemplos de aplicações que se utilizam desse tipo de arquitetura são os aplicativos de *torrent*, telefonia por Internet, como o Skype, entre outros.

Devemos nos atentar, neste instante, no funcionamento de algumas das aplicações disponíveis na internet.

#### 1.2.1.2 A Web

Conforme Kurose e Ross (2013, p. 72), “a Web é a aplicação que chamou a atenção do público em geral”, transformando “drasticamente a maneira como pessoas interagem dentro e fora de seus ambientes de trabalho”.

A proporção desta aplicação se dá pela facilidade de acesso, assim como pela disponibilidade de recursos de acordo com a vontade do utilizador, o que Kurose e Ross (2013, p. 72) chamam de “por demanda”, pois os “usuários recebem o que querem, quando querem”.

O acesso se dá por meio dos navegadores de Internet, ou *browsers*, além de um computador e uma conexão à internet. Com as devidas ferramentas, quando o usuário “*makes a request for information, the application software uses the Internet*”

*to access the requested information, and then displays the results on the screen for the user to see*<sup>11</sup> (COMER, 2007, p. 8).

O fato de o usuário apenas conseguir visualizar o resultado de sua informação requerida é bastante relevante para o trabalho. Diante disso, é perceptível que o trabalho do navegador é simplesmente de receber a cópia do objeto requerido, para, então, apresentá-lo para o usuário, mas este objeto se mantém armazenado no servidor a todo tempo. O que o cliente recebe, então, é tão somente uma cópia daquilo que se encontra no hospedeiro.

Um bom exemplo para esclarecer essa questão é o caso de uma página na internet que pretende se passar por um sítio conhecido, como a amazon.com. O indivíduo que colocou à disposição da internet tal página tem como intuito a obtenção de uma vantagem ilícita, qual seja o recebimento dos dados de cartão de crédito de diversas pessoas. Quando uma vítima passa por todo o procedimento de compra nesse sítio falso, o infrator tem acesso a todas as informações disponibilizadas por aquele.

Devemos nos atentar a duas coisas. Primeiramente, deve-se considerar onde estava localizado este servidor e a partir de que momento o crime se consuma. Estas duas questões são importantes, principalmente, em vista de onde é considerado o local do crime, sendo o primeiro o local da ação e o segundo o local em que se consumou.

Considerando que o servidor estivesse nos Estados Unidos da América, teríamos que, no ato de disponibilizar o sítio na internet como meio fraudulento, o infrator está apresentando para toda e qualquer pessoa que entre no seu sítio falso a possibilidade de ter algum prejuízo.

O local em que se consuma o crime, neste caso, também será nos Estados Unidos da América, tendo em vista que é preciso que a informação efetivamente chegue até o infrator, não tendo qualquer valia se a vantagem pretendida se mantivesse no computador da vítima, já que ele não tem esse acesso.

Efetivamente, então, o crime se consumou em um território diverso, ainda que o crime tenha total dependência da credibilidade do sítio e a inocência, ingenuidade ou imprudência de quem o está acessando.

---

<sup>11</sup> Faz um requerimento por informação, o software de aplicação utiliza a internet para acessar a informação requerida, e então apresenta os resultados na tela do usuário para que ele veja (tradução livre).

A princípio, a possibilidade de ocorrência de uma situação como essa parece extremamente baixa, mas, ao compreender como a *World Wide Web* funciona, é possível perceber que qualquer pessoa está suscetível a um perigo como esse se não tiver o mínimo de cautela.

#### 1.2.1.2.1 O funcionamento da Web: HTTP e HTML

Como já abordado anteriormente, para que os diversos usuários finais consigam conversar entre si, é necessário que eles falem a mesma linguagem, o que se realiza pela adoção de um protocolo.

No caso da *Web*, o protocolo utilizado é o HTTP, ou *HyperText Transfer Protocol* (Protocolo de Transferência de Hipertexto), sendo que este “define a estrutura dessas mensagens e o modo como o cliente e o servidor as trocam” (KUROSE; ROSS, 2013, p. 72). Para compreender melhor, estes autores aprofundam na concepção do que seria *Web*:

Uma página *Web* (também denominada documento) é constituída de objetos. Um objeto é apenas um arquivo – tal como um arquivo HTML, uma imagem JPEG, um *applet* Java, ou um clipe de vídeo – que se pode acessar com um único URL. A maioria das páginas *Web* é constituída de um arquivo-base HTML e diversos objetos referenciados. Por exemplo, se uma página contiver um texto HTML e cinco imagens JPEG, então ela terá seis objetos: o arquivo-base HTML e mais cinco imagens. O arquivo-base HTML referencia os outros objetos na página com os URLs dos objetos. Cada URL tem dois componentes: o nome de hospedeiro (*hostname*) do servidor que abriga o objeto e o nome do caminho do objeto (KUROSE; ROSS, 2013, p. 72).

Portanto, é a tarefa do servidor manter estes objetos armazenados, na espera que o cliente os requeira, enquanto que o propósito do HTTP é “definir como os clientes requisitam páginas aos servidores e como eles as transferem aos clientes”.

Entretanto, ainda não abordamos uma característica própria do aplicativo *Web*, que é justamente a presença do Hipertexto. Conforme Comer (2007, p. 205), “*the concept of embedding selectable items in text is called Hypertext*”<sup>12</sup>. Para tornar mais claro, basta se atentar a uma página como a do sítio Wikipédia, em que ao

---

<sup>12</sup> O conceito de incorporar itens selecionáveis no texto é chamado de Hipertexto (tradução livre).

visualizar um documento qualquer, este faz diversas referências a tantos outros que, com base em um clique apenas, podem ser acessados.

Estamos diante de uma das grandes funcionalidades e facilidades da internet, sendo este o acesso a diversos outros documentos com base em apenas um clique, independente de onde ele esteja, pois “*a browser can jump from one computer to another without a user knowing or caring about which computers are being accessed*”<sup>13</sup> (COMER, 2004, p. 199).

É interessante notar a perspectiva de Comer sobre este assunto, em que ele diz:

*The power of hypertext arises from its combination of generality and instant reference – each document can contain text or embedded menu items that point to other documents. A user can choose to read an entire document or merely scan for highlighted phrases. At any time, the user can return to the previous document or select a highlighted phrase that leads to a new document*<sup>14</sup> (2007, p. 206).

É válida a lembrança que documento é toda e qualquer página da *Web*, e que não existem apenas textos neste aplicativo. Eles podem conter, então, “*sounds, graphical images, and video*”<sup>15</sup>(COMER, 2007, p. 208).

Todavia, o HTTP é o protocolo que estabelece a estrutura das mensagens trocadas entre servidor e cliente, ele não serve para determinar a linguagem utilizada para a criação das próprias páginas da *Web*. Para tanto, utiliza-se o HTML, o *Hypertext Markup Language*.

Será a partir do que está no corpo da página da *Web* que o usuário poderá acessar uma imagem, um vídeo, um som ou outra página. O uso do HTML para a *Web* é de suma importância, como esclarecido por Comer:

*HTML is significant for two reasons. First, the language is sufficiently general to allow it to be used with a variety of browsers and computers. In particular, the language does not specify all the display details, but allows a browser freedom to choose. Second, HTML is*

---

<sup>13</sup> Um navegador pode “pular”(passar) de um computador para outro sem que o usuário tenha conhecimento ou se importe com qual computador ele está acessando.

<sup>14</sup> O poder do hipertexto surge da combinação da generalidade e da referência instantânea – cada documento pode conter texto ou menu de itens incorporados que apontam para outros documentos. Um usuário pode escolher ler um documento inteiro ou simplesmente buscar as frases em destaque. A qualquer momento, o usuário pode retornar para o documento anterior ou selecionar uma frase em destaque que leva até um novo documento (tradução livre).

<sup>15</sup> (podem conter) sons, imagens gráficas e vídeo (tradução livre).

*significant because it allows people to create web pages without a background in computer programming. Much of the popularity of the World Wide Web can be credited to HTML and web authoring tools which have made it easy for individuals and businesses to create web pages*<sup>16</sup> (2007, p. 236).

Interessante notar, já que oportuno, que há uma possível classificação com relação às páginas da *Web*, dividindo-se em páginas dinâmicas ou estáticas.

As páginas da *Web* estáticas são aquelas que o conteúdo “*is fixed by its author, and remains unchanged until the author revises it*”<sup>17</sup> (COMER, 2007, p. 239 e 240). Caso dois usuários finais acessem o mesmo sítio, “*the text and the graphic images will be identical on both screens, and the links to other web pages will operate exactly the same*”<sup>18</sup>.

No entanto, nem sempre esse tipo de documento é de interesse do cliente. Por vezes ele deseja obter alguma informação em tempo real e seria extremamente oneroso que o autor da página tivesse que atualizar alguns valores toda vez que algum deles mudasse, como, por exemplo, a temperatura de alguma cidade.

Por estas e outras razões, de forma a otimizar o fluxo de informações na *Web*, “*server-side scripting technologies were invented to allow web pages to have dynamics content*”<sup>19</sup>, em que o servidor pode associar uma “*URL with a computer program instead of a static document on disk*”<sup>20</sup> (COMER, 2007, p. 249).

Portanto, o servidor poderá apresentar outras informações aos diversos clientes, principalmente aquelas que necessitam ser atualizadas a todo o momento, como o estoque de algum produto, por exemplo.

---

<sup>16</sup> HTML é significativo por duas razões. Primeiramente, a linguagem é suficientemente geral para possibilitar que seja utilizada em uma grande variedade de navegadores e computadores. Particularmente, a linguagem (HTML) não especifica todos os detalhes de apresentação (o display), mas possibilita que o navegador livremente os escolha. Segundo, HTML é significante porque ele possibilita que pessoas criem a página de *Web* sem ter qualquer conhecimento de programação de computadores. A popularidade da *World Wide Web* deve ser muito creditada em razão do HTML e ferramenta de autor da *Web* (é um software que possibilita que uma pessoa faça o design da página da *Web*), que tornaram muito fácil a criação de páginas da *Web* por indivíduos e empresas (tradução livre).

<sup>17</sup> (O conteúdo) é determinado pelo autor, e permanece intocado até que este o revise (tradução livre).

<sup>18</sup> O texto e as imagens gráficas serão idênticas em ambas as telas, e os links para outras páginas da *Web* irão operar exatamente da mesma forma (tradução livre).

<sup>19</sup> As tecnologias de script (são programas criados para automatizar uma certa execução de tarefas) por parte do servidor foram criadas para possibilitar que as páginas da *Web* tenham conteúdo dinâmico (tradução livre).

<sup>20</sup> URL com um programa de computador ao invés de um documento estático no disco (tradução livre).

As páginas dinâmicas permitem outra funcionalidade que as estáticas não realizam, qual seja a possibilidade de o cliente enviar informações para o servidor. Tal função, entretanto, não é realizada por estes *scripts*, tendo em vista que eles agem tão somente no servidor.

Para tanto, os sítios possuem uma tecnologia específica que permite aos usuários o preenchimento de certas informações, que é conhecida como “*forms*”, em que a página da *Web* “*contain blank areas in which the user must enter information*”<sup>21</sup>, e, após o preenchimento, “*the browser sends the information to the server when requesting another page*”<sup>22</sup>.

Ainda assim, a relação entre o servidor e o cliente continua a mesma, em que a informação se encontra armazenada no primeiro, sendo enviada uma cópia para o outro assim que ela for requisitada.

### 1.2.1.3 A transferência de arquivos: o FTP

Como se depreende do nome do protocolo, FTP ou *File Transfer Protocol*<sup>23</sup>, ele possui como propósito “transferir arquivos de ou para um hospedeiro remoto”, somente sendo acessível por uma “identificação e uma senha” (KUROSE e ROSS, 2013, p. 85).

Principal diferença entre o HTTP e o FTP é justamente é que, além da troca de informações referente à identificação do usuário, como ocorreria no primeiro, o FTP é utilizado “para enviar de fato um arquivo” (KUROSE e ROSS, 2013, p. 85).

Como a maior parte de nossa interação com a internet é através dos navegadores, com o FTP não poderia ser diferente, ainda que este fosse acessado por outra aplicação anteriormente.

Para tanto, “*a browser uses the URL associated with a link to decide whether to run FTP – if the URL begins with the prefix ftp://, a browser interprets the rest of the URL as a request for a file transfer*”<sup>24</sup> (COMER, 2007, p. 297).

---

<sup>21</sup> Contém áreas em branco em que o usuário poderá preencher com informações (tradução livre).

<sup>22</sup> O navegador envia a informação para o servidor quando ele requisitar outra página (tradução livre).

<sup>23</sup> Protocolo de Transferência de Arquivo.

<sup>24</sup> Um navegador usa o URL associado com um link para decidir se irá utilizar o FTP – se o URL começar com o prefixo ftp://, o navegador interpretará o resto do URL como um requerimento para transferir um arquivo (tradução livre).

É importante notar que a troca de arquivos pode ocorrer tanto do servidor para o cliente, como deste para aquele. Sendo assim, o cliente poderá realizar o *download* do arquivo, assim como poderá fazer o *upload* de seus arquivos para o servidor. Para que esta função exista, entretanto, é necessário que o “*remote computer must be configured to allow uploading, and a user must be authorized*”<sup>25</sup> (COMER, 2007, p. 298).

Verifica-se, então, a necessidade de autorização para algumas ações, inclusive para o acesso a alguns arquivos específicos.

Usualmente, para ter acesso a um servidor FTP, o usuário deve fornecer o *login* e a senha para acessar os arquivos. O interessante é que o servidor pode ser configurado de modo a fornecer somente certos arquivos para alguns indivíduos, assim como o cliente pode ter a permissão para enviar arquivos, mas não pode baixar nenhum deles.

Entretanto, em certos casos, o administrador poderá definir que certos arquivos são de acesso público, em que qualquer pessoa, mesmo que sem *login*, poderá acessá-los. Neste sentido, o “*FTP restricts the user’s access to files that have been declared public; even if other files exist, an anonymous user will not be able to access them*”<sup>26</sup> (COMER, 2007, p. 298).

#### 1.2.1.4 O serviço de diretório da Internet: o DNS

Conforme já tratado anteriormente, aqueles que utilizam a internet normalmente usam o *hostname* para acessar algum serviço. Entretanto, para ter esse acesso, é necessário que a aplicação DNS intervenha, de forma a “traduzir nomes de hospedeiros fornecidos por usuários para endereços IP” (KUROSE; ROSS, 2013, p. 96).

É necessário se notar que o DNS é “um banco de dados distribuído executado em uma hierarquia de servidores de DNS” e, além disso, “um protocolo de camada de aplicação que permite que hospedeiros consultem o banco de dados distribuído” (KUROSE; ROSS, 2013, p. 96).

---

<sup>25</sup> O computador remoto deve estar configurado para permitir o envio (de arquivos), e o usuário deve estar autorizado para tanto (tradução livre).

<sup>26</sup> O (servidor) FTP restringe o acesso do usuário aos arquivos que forem considerados públicos, ainda que outros arquivos existam, um usuário anônimo não poderá acessar estes (tradução livre)

Portanto, trata-se de ferramenta fundamental para a utilização da internet, eis que, no uso corrente da *Web*, para que os usuários acessem os mais diversos sítios disponíveis, eles não contam, normalmente, com o endereço IP, mas sim o nome do hospedeiro.

Não seria interessante, entretanto, que o banco de dados se concentrasse em apenas um local, pois, como afirmado por Kurose e Ross, caso ele quebrasse, a internet não iria mais funcionar, sem contar o tráfego deste servidor, a distância que ele pode se encontrar do requerente e, inclusive, a extensão dos dados deste, tendo em vista que ele teria que conter todos os *hostnames* da internet.

Sendo assim, “*a given server does not store the names of all possible computer in the Internet*”<sup>27</sup> (COMER, 2007, p. 154), deduzindo-se que o seu funcionamento se dá de forma distribuída e hierárquica.

Conforme Torres(2015), toda e qualquer rede deveria ter um servidor DNS, mas é possível se utilizar “o servidor DNS da sua operadora de acesso”, do provedor de internet, não sendo necessário que “o servidor DNS se encontre na sua rede”.

Kurose e Ross (2013, p. 99 e 100) atentam que, apesar de este servidor DNS não estar presente na estrutura hierárquica, que será apresentada logo a frente, ele é essencial para o seu funcionamento. Usualmente, “quando um hospedeiro faz uma consulta ao DNS, ela é enviada ao servidor DNS local, que age como *proxy* e a retransmite para a hierarquia do servidor DNS”.

Sendo assim, a sua importância deriva justamente de sua função de ligação entre o requerente, o usuário final, e o acesso à hierarquia.

De acordo com Kurose e Ross (2013, p. 98 e 99), existem três tipos de servidores DNS, sendo eles: Servidores DNS raiz, Servidores DNS de Domínio de Alto Nível (TLD) e os Servidores DNS autoritativos.

Os primeiros têm como função repassar aos usuários finais os endereços IP dos servidores de Domínio de Alto Nível, sendo, então, “um conglomerado de servidores replicados, para fins de segurança e confiabilidade” (KUROSE; ROSS, 2013, p. 98).

Os segundos, por sua vez, são os responsáveis “por domínios de alto nível como *com, org, net, edu* e *gov*, e por todos os domínios de alto nível de países, tais como *uk, fr, ca* e *jp*” (KUROSE; ROSS, 2013, p. 98 e 99). Sendo assim eles são

---

<sup>27</sup> Certo servidor não armazena os nomes e endereços de todos os computadores possíveis da Internet (tradução livre).

capazes de informar ao usuário, de pronto, os endereços IP referentes a estes domínios.

Por fim, os terceiros, são aqueles que abrigam os demais registros, sendo que os hospedeiros poderão, conforme Kurose e Ross(2013, p. 99), armazenar por si mesmos estes dados, por meio de um servidor DNS próprio, ou poderão pagar um provedor para que ele abrigue tais informações.

Portanto, tem-se a seguinte relação: Os usuários, para acessarem alguma página na *Web*, irão, primeiramente, fornecer o domínio que eles têm conhecimento ao *browser* e este irá mandar uma mensagem de consulta ao servidor DNS local, que, por consequência, irá contatar o servidor DNS raiz. Este irá reconhecer o domínio e irá transmitir o endereço IP do servidor TLD, que, por sua vez, irá transmitir o endereço IP do servidor DNS autoritativo, quando requisitado. Sendo assim, estabelece-se a relação entre o cliente e o servidor desejado, assim que este último servidor disponibilizar o endereço IP pretendido ao servidor local e este repassar ao cliente.

Interessante notar que o servidor local, além de possibilitar que o cliente faça essas requisições na internet, ele irá armazenar a informação obtida e, “caso alguma outra máquina pergunte sobre o mesmo endereço novamente, ele sabe qual é a resposta (qual é o endereço IP)” (TORRES, 2015). Todavia, esta não será armazenada eternamente, tendo em vista que pode ocorrer a mudança de domínio do hospedeiro.

Portanto, tornam-se relevantes a palavras de Comer, que diz:

*A computer on the Internet only needs to know the location of one domain name server. A program becomes a client of the domain name service when it sends a computer's name to the local domain name server. The local server answers the request by translating the name into an IP address. Although the server may contact remote servers to obtain the information, the client receives an answer from the local server*<sup>28</sup> (2007, p. 156)

Ainda que esta interação ocorra a todo momento, como grande parte da internet, o usuário não tem conhecimento da maior parte de seu funcionamento,

---

<sup>28</sup> Um computador na internet só precisa saber da localização de um servidor DNS. Um programa se torna um cliente do DNS quando ele manda um nome de computador para o servidor local. Este irá responder ao pedido traduzindo o nome para um endereço IP. Ainda que o servidor entre em contato com servidores remotos para obter tal informação, o cliente recebe apenas a resposta de seu servidor local (tradução livre).

bastando apenas o acesso ao conteúdo pretendido. De qualquer forma, como demonstrado, o DNS é um instrumento fundamental do cotidiano virtual, tendo em vista a facilidade que ele traz para o uso e acesso à internet.

#### *1.2.1.5 As camadas de apresentação e sessão*

Caso se adote o modelo OSI, estas duas camadas seriam consideradas autônomas. Entretanto, considerando-se a pilha de protocolos TCP/IP, elas podem ser encontradas ainda na camada de aplicação.

Para a camada de apresentação, tem-se como função “prover serviços que permitam que as aplicações de comunicação interpretem o significado dos dados trocados” (KUROSE; ROSS, 2013, p. 39) e, por esta razão, ela é inclusive chamada de “camada de tradução”, sendo possível se utilizar para a “compressão de dados e criptografia” (TORRES, 2015).

Como é possível se notar, a compressão de dados torna a comunicação entre os usuários mais rápida, tendo em vista que “haverá menos dados a serem transmitidos”, enquanto que a criptografia tem como intuito trazer segurança ao que está sendo transmitido, sendo que “só serão decodificados na camada seis do dispositivo receptor” (TORRES, 2015).

Por sua vez, a camada de sessão ocupa-se em prover “a delimitação e sincronização da troca de dados, incluindo os meios de construir um esquema de pontos de verificação e de recuperação” (KUROSE; ROSS, 2013, p. 39), que se realizará por meio de “uma sessão de comunicação” (TORRES, 2015).

Sendo assim, esta camada tem como intuito garantir que, se, por ventura, a conexão seja terminada por qualquer razão, quando ela se restabelecer a troca de dados irá retomar a partir daquele ponto em que ela foi perdida.

Interessante notar que, apesar de toda a relevância destas camadas para a internet, elas não são essenciais para o seu uso, tratando-se, desta forma, de uma opção daquele que está desenvolvendo a aplicação, pois, nos dizeres de Kurose e Ross (2013, p. 39), cabe a ele decidir se há pertinência no uso desses serviços e, caso sejam necessários, que eles construam essa funcionalidade na aplicação.

#### *1.2.2 A camada de transporte.*

De acordo com Kurose e Ross (2013, p. 38), a camada de transporte “carrega mensagens da camada de aplicação entre os lados do cliente e servidor de uma aplicação”, sendo possível a utilização de dois protocolos: o TCP ou o UDP.

Mais a frente, estes mesmos autores (2013, p. 135 e 136) aprofundam mais sobre a funcionalidade do protocolo na camada de transporte, esclarecendo:

Um protocolo da camada de transporte fornece comunicação lógica entre processos de aplicação que rodam em hospedeiros diferentes. Comunicação lógica nesse contexto significa que, do ponto de vista de uma aplicação, tudo se passa como se os hospedeiros que rodam os processos estivessem conectados diretamente; na verdade, eles poderão estar em lados opostos do planeta, conectados por diversos roteadores e uma ampla variedade de tipos de enlace. Processos de aplicação usam a comunicação lógica fornecida pela camada de transporte para enviar mensagens entre si, livres da preocupação dos detalhes da infraestrutura física utilizada para transportá-las.

Como já estabelecido anteriormente, a maior parte dos usuários da internet apenas notam as aplicações, isto é, aqueles elementos que lhe fornecem serviços por meio da internet. Sendo assim, o funcionamento em si deste ambiente não é de notório conhecimento.

Portanto, a rapidez com que os diversos usuários finais conseguem se comunicar, certamente, cria uma ilusão de que se trata de uma terra sem fronteiras, em que a informação pode chegar em qualquer local do globo em questão de segundos. Porém, isso não ocorre por acaso.

Para tanto, a camada de transporte se utiliza do protocolo TCP, que é o *Transmission Control Protocol*, ou o Protocolo de Controle de Transmissão, que, em razão de sua importância, está no nome da pilha de protocolos utilizada pela internet, o TCP/IP mencionado anteriormente. Os protocolos TCP e IP trabalham coordenadamente para manter as conexões seguras e completas, mas só veremos o segundo quando tratarmos da camada de rede.

Qualquer serviço que esteja sendo prestado, o usuário espera que ele ocorra de forma eficiente. No entanto, quando estamos tratando de um serviço que pode ser utilizado por qualquer pessoa, a qualquer tempo, é possível se questionar se aquele que o fornece, no caso de diversos acessos simultâneos, conseguirá suprir a demanda.

Com isso em mente, a internet se utiliza do protocolo TCP, que justamente busca “*lost datagrams and handles the problem*”<sup>29</sup> (COMER, 2007, p. 139). Com relação ao termo datagrama, Kurose e Ross (2013, p. 138), preferem utilizar o termo segmento, tendo em vista a possível confusão que se pode ter em razão da utilização do primeiro na camada de rede. Sendo assim, adotaremos o termo utilizado por estes dois autores, ainda que nas citações de Comer ele use o primeiro termo.

O TCP, então, “oferece vários serviços adicionais às aplicações”, como a “transferência confiável de dados”, em que o protocolo garante que os dados “sejam entregues do processo remetente ao processo destinatário corretamente e em ordem” (KUROSE; ROSS, 2013, p. 139).

Para expandir mais nesta função, a transferência confiável de dados garante que os dados enviados, nos dizeres de Kurose e Ross (2013, p. 177), não possuem lacunas, duplicações e estão devidamente sequenciados. Portanto, garante-se, em suma, que os dados recebidos por usuário sejam exatamente iguais àqueles que foram enviados por outro.

O TCP se utiliza de algumas ferramentas para fazer as necessárias verificações, como é o caso do uso de “*timers and acknowledgments*”<sup>30</sup>, em que “*whenever data arrives at its final destination, TCP software on the receiving machine sends na acknowledgment back to the source*”<sup>31</sup>, considerando-se que “*an acknowledgement is a short message that specifies which data arrived*”<sup>32</sup>(COMER, 2007, p. 140).

De acordo com Comer (2007, p. 140 e 141), o temporizador funciona como um alarme, em que a partir do momento em que os dados são enviados, o tempo começa a ser contado. No caso de a confirmação chegar antes do tempo estimado pelo temporizador, reconhece-se que os dados chegaram de forma correta. Entretanto, caso a confirmação não chegue, e o tempo estimado pelo temporizador seja ultrapassado, o TCP irá reenviar os dados, considerando que eles se perderam e, por algum motivo, não chegaram a seu destinatário.

---

<sup>29</sup> Datagramas perdidos e cuida do problema (tradução livre).

<sup>30</sup> Temporizadores e reconhedores, ou confirmadores (tradução livre).

<sup>31</sup> Sempre que os dados chegarem em seu destino final, o software TCP na maquina que os recebeu manda uma confirmação para a fonte destes (tradução livre).

<sup>32</sup> Uma confirmação é uma pequena mensagem que especifica quais dados chegaram (tradução livre).

O temporizador age de acordo com as nuances da própria internet e a distância entre os usuários comunicantes, sendo este um dos aspectos mais importantes para o sucesso do TCP/IP, tendo em vista que “*a communication protocol must change the timeout automatically to achieve efficient data transfer*”<sup>33</sup> (COMER, 2007, p. 141).

Outro serviço que o protocolo fornece, conforme Kurose e Ross (2013, p. 139), mas que não se destina em específico à aplicação, mas sim a toda internet, é o chamado “controle de congestionamento”, em que ele possibilita que “conexões TCP trafegando por um enlace de rede congestionado compartilhem em pé de igualdade a largura de banda daquele enlace”, o que é feito por meio da “regulagem da taxa”.

Isso significa que uma conexão TCP poderá ser regulada pela sua taxa de emissão, a partir do remetente, possibilitando que ela chegue ao seu destinatário, ainda que existam diversas outras conexões ocorrendo simultaneamente.

Por sua vez, o UDP se diferencia por não verificar “se o pacote de dados chegou ou não ao seu destino”, justificando-se porque “não é usado no transporte de dados importantes como, por exemplo, arquivos e e-mails” (TORRES, 2015).

Sendo assim, poderia se questionar qual a razão de se utilizar tal protocolo, tendo em vista que ele não possui a maior função proposta pelo TCP, que é justamente a transferência confiável de dados.

De acordo com Torres (2015), a vantagem de se utilizar o UDP é justamente a sua transmissão mais rápida de dados, em que os pacotes de dados transmitidos são menores e não existe o sistema de confirmação realizado pelo TCP.

Compreendido como é efetuado o transporte, há que se considerar, neste momento, como são direcionados os pacotes de dados, isto é, qual é o protocolo determinante para o envio dos dados ao destinatário correto.

### 1.2.3 A camada de rede

Por mais interessante que esta camada seja, a sua estrutura é por demasiada complexa e não é o intuito deste trabalho desmistificar a maior parte do que ocorre

---

<sup>33</sup> Um protocolo de comunicação deve mudar o tempo estimado automaticamente para alcançar uma transferência de dados eficiente (tradução livre).

nesta etapa, eis que a forma como é definido um endereço para certo indivíduo não contribui para a discussão.

Basicamente, nesta camada há o endereçamento dos pacotes de dados, fazendo com que eles cheguem aos seus destinatários, passando pelos diversos roteadores que estão no caminho.

Com relação ao *Internet Protocol*, ou Protocolo de Internet, Comer consegue resumir bem a ideia que deve ser transmitida no presente momento:

*The Internet Protocol, IP, specifies the basic rules that a computer must follow to communicate across the Internet. IP defines the format of Internet packets, which are called IP datagrams. IP also defines an address scheme that assigns each computer a unique number used in all communication. More important, IP software makes an interconnected set of networks and routers operate like a single, large network<sup>34</sup>.*

*Each computer on the Internet must have IP software that allows it to create and send IP datagrams. Each router also has IP software that knows how to forward datagrams to their destinations. When a datagram arrives at a router, the IP software chooses the path that will lead to the datagram's destination<sup>35</sup> (2007, p. 135)*

Nota-se que o IP mantém a mesma perspectiva de todos os outros protocolos, isto é, ele estabelece uma base comum para que os diversos usuários e roteadores interajam na internet, o que é feito por meio dos datagramas.

Como o autor especifica, o importante é que cada máquina, incluindo os roteadores, possua o seu próprio endereço, pois não teria interesse em mandar um arquivo para um indivíduo e este chegar para outro. Ou ainda, não seria eficiente simplesmente lançar o datagrama na internet, na expectativa que, eventualmente, o destinatário seja encontrado.

Torres (2015) esclarece, por sua vez, que os pacotes de dados “precisam usar dois tipos de endereço, um endereço lógico e um endereço físico”. No caso desta camada, utiliza-se o endereço lógico, que “independe da arquitetura de rede

---

<sup>34</sup> O Protocolo da Internet, IP, especifica as regras básicas que o computador deve seguir para se comunicar através da internet. IP define o formato dos pacotes de internet, que são chamados de datagramas. IP também define um esquema de endereços que assinala para cada computador um único número que será usado em todas as suas comunicações. Mais importante, o software do IP faz com que um grande número de redes e roteadores conectados operem como se fossem uma singular e grande rede (tradução livre).

<sup>35</sup> Cada computador na internet tem que ter um software de IP que o possibilite criar e enviar datagramas. Cada roteador também tem um software de IP que sabe remeter os datagramas para os seus destinos. Quando um datagrama chega em um roteador, o software de IP escolhe o caminho que levará até o destino do datagrama (tradução livre).

sendo usada”, permitindo o contato entre uma rede *Ethernet* e uma *Token Ring*, por exemplo. O endereço físico, em razão de sua relação com a camada seguinte, será exposto a seguir.

Com relação ao endereço lógico, Torres (2015) esclarece que o destino permanece inalterado, importando chegar no seu destino.

Portanto, a relevância desta camada é justamente o fato de estabelecer um endereço próprio para cada máquina que se conecta a rede e, por consequência, que os documentos trocados na internet tenham um destino certo.

#### 1.2.4 A camada de enlace

De acordo com Torres esta camada possui as seguintes funções:

A camada de link de dados (também chamada camada de enlace) pega os pacotes de dados recebidos da camada de rede e os transforma em quadros ou células que serão trafegados pela rede, adicionando informações como o endereço da placa de rede de origem, o endereço da placa de rede de destino, dados de controle, os dados em si e dados de correção de erro (checksum ou CRC) (2015).

Além disso, responsabiliza-se também, no dizer do mesmo autor (2015), por se certificar que o meio pelo qual “os quadros serão transmitidos está disponível e pode ser usado”.

Com relação aos protocolos, Torres esclarece:

As camadas dois e um do modelo OSI são controladas pelo protocolo de baixo nível, isto é, pela arquitetura da rede (*Ethernet*, *Token Ring*, *FDDI*, *X. 25*, *Frame Relay*, *ATM* etc.) e, portanto, controladas por hardware – em outras palavras, controladas pela placa de rede do computador ou do periférico de rede. As camadas anteriores são tradicionalmente controladas por software, isto é, pela pilha de protocolos sendo usada (2015).

Entretanto, esta diversidade não é o foco do presente trabalho, não sendo necessário repassar as diferenças entre os diversos tipos de protocolos e a sua atuação, bastando ter conhecimento da sua existência e função genérica.

Interessante notar que se fez menção ao *checksum*, que se ressaltou na camada de transporte. Torres (2015) aponta que, ainda que seja um recurso que

possa ser utilizado pela camada de enlace, ele não é comum, recaindo tal função à outra camada já abordada.

Retomando um ponto anterior, o endereço lógico é trabalhado pela camada de rede, enquanto que o endereço físico é gerado na camada de enlace.

Para Kurose e Ross(2013, p. 38), a camada anterior depende do serviço desta camada quando há a transferência de “um pacote de um nó (hospedeiro ou roteador) ao nó seguinte da rota”<sup>36</sup>, sendo o propósito da camada de enlace, justamente, a “entrega, ao longo da rota, ao nó seguinte, no qual o datagrama é passado da camada de enlace para a de rede”.

Neste sentido, nota-se que o endereço físico ele se concentra em formar o caminho entre as máquinas, isto é, o endereço lógico irá visar chegar a máquina X, enquanto que o endereço físico irá determinar o caminho, entre os diversos roteadores, até chegar nesta determinada máquina.

A camada de enlace, ou de link de dados, então, é responsável por receber os pacotes de dados e transformá-los em quadros, realizando o transporte destes entre os diversos componentes que estão no caminho entre o remetente e o destinatário final.

### *1.2.5 A camada física*

A última camada, por sua vez, na visão de Kurose e Ross (2013, p. 39), tem a função de “movimentar os bits individuais que estão dentro do quadro de um nó para o seguinte”, dependendo da própria camada de enlace e do “meio de transmissão do enlace (por exemplo, fios de cobre trançado ou fibra ótica monomodal)”.

Por esta razão, reputa-se que os quadros serão codificados, de forma a serem transmitidos “através de sinais elétricos, luminosos ou de radiofrequência, dependendo se a rede usa cabos metálicos, fibra ótica ou é do tipo sem fio, respectivamente” (TORRES, 2015).

## **1.3 Direito e Internet**

---

<sup>36</sup> Nó ou ponto: cada ponto de conexão da rede, ou seja, cada computador ou periférico de rede, como roteadores (TORRES, 2015).

Tendo em vista o surgimento e o desenvolvimento da internet, as relações entre diversos indivíduos ao redor do mundo foram criadas ou desenvolvidas, em razão da velocidade em que as comunicações ocorrem e pela facilidade de encontrar outros que possuem o mesmo interesse, objetivo, entre outros.

Sendo assim, a internet se transformou numa plataforma útil ao mais diversos segmentos, mas principalmente ao comércio, fazendo com que o interesse estatal crescesse com relação aos fatos que ocorrem no mundo virtual.

Para que o Estado possa ter conhecimento destes fatos, na visão de seu Poder Judiciário, requer-se que eles respeitem os requisitos mínimos que a jurisdição interna daquele exige. Por esta razão, no próximo capítulo passaremos a analisar o que é a jurisdição, seus conceitos clássicos e contemporâneo, a sua diferença na esfera penal e, posteriormente, qual seria o papel deste instituto neste ambiente virtual.

## **2 A JURISDIÇÃO**

Como já abordado acima, é preciso, previamente, compreender o conceito de jurisdição e a sua finalidade, para, então, abranger qual a função da eficácia espacial da lei penal e quais são os princípios regentes deste instituto.

Desta forma, a jurisdição se sobressai como um dos principais elementos da problemática já aduzida, tendo em vista a necessidade de se estabelecer o limite da própria atuação do ente estatal nesta atividade, além dos seus interesses.

### **2.1 O Conceito de jurisdição**

Nas palavras de Guilherme de Souza Nucci (2010, p. 243), jurisdição “é o poder atribuído, constitucionalmente, ao Estado para aplicar a lei ao caso concreto, compondo litígios e resolvendo conflitos”.

Por sua vez, para Nestor Távora (2011, p. 229), este poder-dever se deve ao afastamento do uso da autotutela, cabendo, então, “ao Poder Judiciário a missão constitucional de certificar o direito, dirimindo as demandas que lhe são apresentadas”. Este ainda admite que a jurisdição pode ser exercida por outros órgãos, como o Senado Federal, com relação aos crimes de responsabilidade.

Em comum, é possível se notar a presença de alguns elementos, como a caracterização da jurisdição como poder, atividade inerente ao Estado, sendo assegurada na Magna Carta, e a aplicação da lei ao caso concreto com a finalidade de dirimir as demandas. Entretanto, estes não são os únicos elementos que a doutrina aponta.

Antônio Carlos de Araújo Cintra, Ada Pellegrini Grinover e Cândido Rangel Dinamarco ,definem a jurisdição como:

uma das funções do Estado, mediante a qual este se substitui aos titulares dos interesses em conflito para, imparcialmente, buscar a pacificação do conflito que os envolve, com justiça. Essa pacificação é feita mediante a atuação da vontade do direito objetivo que rege o caso apresentado em concreto para ser solucionado; e o Estado desempenha essa função sempre mediante o processo, seja expressando imperativamente o preceito (através de uma sentença de mérito), seja realizando no mundo das coisas o que o preceito estabelece (através da execução forçada) (2013, p. 155)

Interessante notar que estes autores, ainda, aduzem que a jurisdição é mais do que simplesmente um poder, sendo também, ao mesmo tempo, função e atividade (CINTRA; GRINOVER; DINAMARCO, 2013, p. 155). Enquanto poder, entende-se a jurisdição como a “capacidade de decidir imperativamente e impor decisões”. Enquanto isso, “como função, expressa o encargo que têm os órgãos estatais de promover a pacificação de conflitos interindividuais, mediante a realização do direito justo e através do processo”. Por fim, a atividade se revela como “o complexo de atos do juiz no processo, exercendo o poder e cumprindo a função que a lei lhe comete”.

Conforme se nota, a doutrina brasileira ainda se pauta, em grande parte, nas concepções clássicas de Chiovenda e Carnelutti, tanto na atuação baseada na atuação concreta da lei, assim como a presença da lide, do conflito, nos diversos conceitos.

Conforme preleciona Alexandre Freitas Câmara (2004, p. 66), a doutrina de Chiovenda parte do pressuposto de que “a lei, norma abstrata e genérica, regula todas as situações que eventualmente ocorram em concreto, devendo o Estado, no exercício da jurisdição, limitar-se à atuação da vontade concreta do direito objetivo”.

A colocação de Luiz Guilherme Marinoni, Sérgio Cruz Arenhart e Daniel Mitidiero (2015, p. 42), em obra conjunta, é pertinente, ao se referir que, apesar dos avanços ocasionados por pela definição de Chiovenda, com o desenvolvimento da “natureza publicista do processo”, ela ainda “manteve-se fiel ao positivismo clássico”.

Com relação ao conceito criado por Carnelutti, atribuiu-se à jurisdição “a função de justa composição da lide, entendida como o conflito de interesses qualificado pela pretensão de um e resistência do outro interessado” (MARINONI; ARENHART; MITIDIERO, 2015, p. 42).

A diferença clara que podemos traçar entre estas duas definições é, principalmente, a perspectiva adotada pelos doutrinadores. Chiovenda, ao tratar da aplicação da vontade objetiva da lei, volta-se à atividade do juiz, como este ator deve se pautar no processo. Enquanto isso, Carnelutti não se dirige a forma como o magistrado deve atuar, mas sim a percepção das partes com relação ao processo, isto é, origina-se a lide do encontro da pretensão de um indivíduo perante a resistência de outro.

Insta-se notar que ambos se tratam de conceitos clássicos, pautados no ideal de supremacia da lei, sendo que a perspectiva atualmente tem como base a ideia de constitucionalização dos instrumentos, isto é, o uso do filtro constitucional para a atividade legislativa, assim como para a judiciária. Sendo assim, logo mais abordaremos o conceito “contemporâneo” de jurisdição, conforme Marinoni, Arenhart e Mitidiero (2015, p. 156), e a sua pertinência ao tema.

Portanto, em suma, a concepção de jurisdição usualmente adotada no Brasil “reflete e alberga as opiniões da doutrina italiana do início do século XX sobre a essência do ato jurisdicional”, sendo que a maior parte da doutrina brasileira a repete “com maior ou menor variação, suprimindo por vezes um ou outro elemento” (OLIVEIRA; MITIDIERO, 2010, p. 122).

## **2.2 Os escopos da jurisdição**

O exercício da jurisdição pelo Estado não se dá sem qualquer propósito, aliás, as atividades do ente estatal possuem finalidades específicas em vista do princípio regente da atuação desta entidade, que é a supremacia do interesse público.

De qualquer modo, a jurisdição pode ter as suas finalidades manifestadas nos aspectos jurídicos, sociais e políticos, sendo pertinente a colocação de Cintra, Grinover e Dinamarco ,que reputam:

Para caracterizar a jurisdição, muitos critérios foram propostos pela doutrina tradicional, apoiada sempre em premissas exclusivamente jurídicas e despreocupada das de caráter sociopolítico. Hoje a perspectiva é substancialmente outra , na medida em que a moderna processualística busca a legitimidade do seu sistema na utilidade que o processo e o exercício da jurisdição possam oferecer à nação e às suas instituições. Daí a segura diretriz no sentido de afirmar os escopos sociais e políticos da jurisdição e especialmente o escopo de pacificação com justiça, (...) (2013, p. 156).

Portanto, não basta ao Estado tão somente subtrair o particular da sua autotutela, mas assegurar meios capazes de tornar o processo útil, eficiente, célere, entre outros, deste sistema, tendo em vista que a “jurisdição tem inegáveis implicações com a vida social, tanto que é o reconhecimento de sua utilidade pelos membros da sociedade, que a legitima no contexto das instituições políticas da nação” (DINAMARCO, 2008, p. 181).

As palavras de Candido Rangel Dinamarco (2008, P.181) também são relevantes com relação ao viés político, tendo em vista que a jurisdição “reflete, na conjuntura em que se insere, a fórmula das relações entre o Estado e sua população, além de servir de instrumento para a imposição e diretrizes estatais”. Portanto, é a forma que o Estado impõe a autoridade do seu ordenamento jurídico perante todo e qualquer caso que chegue ao seu conhecimento.

Sendo assim, há que se considerar não só o aspecto jurídico, eis que estaríamos tratando apenas de uma faceta dos diversos propósitos que a jurisdição traz, ampliando-se o espectro para notar as diversas finalidades possíveis, eis que ela cumpre objetivos perante a sociedade e o próprio Estado.

### *2.2.1 Os escopos sociais*

Na obra de Cândido Rangel Dinamarco (2008, p. 191), a decisão entregue pelo Juiz deve não só resolver o conflito, mas sim “eliminar conflitos mediante critérios justos”, sendo este o “mais elevado escopo social das atividades jurídicas do Estado”.

Não se está na busca da aprovação do que foi decidido, pois, usualmente, o processo dita sobre questões antagônicas, em que as partes possuem pretensões contrárias. A pacificação há de ocorrer com a resolução da controvérsia com justiça, buscando-se a chamada “paz social” (DINAMARCO, 2008, p. 188).

Alexandre Freitas Câmara determina que a justiça é aquela pautada conforme o direito objetivo, pois

sendo certo que o conceito de justiça é por demais abstrato, cada pessoa pode ter um senso próprio de justiça, diferente das demais, ou do senso comum. Até mesmo o juiz pode ter um senso próprio de justiça. Não se pode achar, porém, que o atingimento desse escopo da jurisdição se dá com a prolação, pelo juiz, de um provimento jurisdicional que dê ao caso a ele submetido a solução que ele, juiz, considere a mais justa, ainda que tal solução contrarie o direito objetivo. A justiça das decisões está intimamente ligada à sua adequação ao direito objetivo. Juiz justo é aquele que aplica ao caso concreto a vontade do direito objetivo, de acordo com os fins sociais a que a lei se destina e o bem comum (2004, p. 81).

Entretanto, este não é o único escopo social da jurisdição, tendo em vista que ela também possui uma função educacional com relação à sociedade. Trata-se de

ditar como as pessoas devem proceder, desde a limitação da arbitrariedade dos indivíduos, até mesmo como eles devem se portar caso sejam lesionados em suas relações cotidianas. Seria o que Dinamarco (2008, p. 191) chama de “conscientizar os membros desta (sociedade) para direitos e obrigações”.

Ao se reforçar o exercício da jurisdição, a sociedade que se submete a ela tem maior consciência dos seus direitos e deveres e, por consequência, respeitam, em maior medida, a ordem vigente, pois os membros dela sabem que, nos casos de violação de direito alheio, este será pleiteado perante o Poder Judiciário e, então, terá o seu devido ressarcimento.

Relaciona-se, simultaneamente, com a confiança que a sociedade possui com relação ao titular do poder jurisdicional, eis que, diante de frustrações, a possibilidade de buscar alguma tutela perante o órgão judiciário é menor.

Nota-se, então, estes dois escopos sociais com relação à jurisdição, devendo-se entender que “o escopo último continua sendo a pacificação social, que, na medida em que obtidos bons níveis de confiança no seio da população, torna-se mais fácil de ser também levada a níveis satisfatórios” (DINAMARCO, 2008, p. 193).

### 2.2.2 Os escopos políticos

Quanto aos escopos políticos, a doutrina aponta três expressões, como bem resume Alexandre Freitas Câmara (2004, p. 82), sendo elas a “afirmação do poder estatal, culto às liberdades públicas e garantia de participação do jurisdicionado nos destinos da sociedade”.

Pensar na afirmação do poder estatal não se confunde com a aplicação da vontade concreta da lei. Dinamarco (2008, p. 199) bem explica que esta é uma percepção individualista, isto é, se “referir todo o direito ao indivíduo e pensar no homem como sujeito de direitos e não como integrante da sociedade política e merecedor de condições para a felicidade pessoal”.

Como instituição do Estado, como qualquer outra, a jurisdição possui um fim político, sendo esta uma das formas de expressão de suas vontades e objetivos políticos. A jurisdição não age tão somente com relação a um particular, mas ela é “exercida diuturnamente em número indefinido de caso, com afirmação da autoridade e exercício do poder” (DINAMARCO, 2008, p. 200).

A segunda expressão dos escopos políticos da jurisdição se refere ao culto à liberdade, sendo esta entendida em seu sentido lato, revelando-se como “garantia fundamental” (CAMARA, 2004, p. 83). A jurisdição com o seu fim político visa a resguardar a ordem jurídica e impô-la perante a sociedade, mas, simultaneamente, visa a proteger as liberdades dos seus jurisdicionados.

Entretanto, Dinamarco (2008, p. 201) salienta que não se trata de qualquer relação, referindo-se àquela em que figuram como atores o “Estado e o indivíduo”, sendo expressão do Estado democrático a “solene promessa de observá-las e limitar o exercício do poder de modo a não invadir a esfera de liberdade deixada aos indivíduos sem dano à vida do grupo e ao desenvolvimento dos objetivos comuns”.

Por outro lado, há que se considerar que os diversos escopos da jurisdição, em suas diversas facetas, formas e expressões, não trabalham de forma individualizada. Neste sentido, a atuação desta face do escopo político, de certa forma, poderia atuar conjuntamente com o da pacificação social, parte do escopo social, eis que a resolução dos conflitos com justiça possui como intento o resguardo do direito de certo indivíduo diante de uma ameaça ou efetiva lesão.

Sendo assim, o culto à liberdade não se estenderia tão somente à limitação do poder estatal, mas também à regular as relações entre os particulares, impondo-se a presente ordem jurídica com a devida proteção das garantias fundamentais, educando os jurisdicionados com relação à extensão de suas respectivas obrigações e deveres.

Por fim, trata-se de um efeito do princípio democrático, que é a garantia de participação do indivíduo no destino da sociedade, sendo esta “essencial para a caracterização de um Estado como democrático de Direito” (Câmara, 2004, p. 83).

Em uma análise mais detida, nota-se que esta faceta é um desenvolvimento das demais expressões apresentadas, eis que o respeito à democracia é um fim político em si, um dos pilares do Estado que construímos no território brasileiro e, portanto, seria uma forma de impor um dos objetivos políticos atribuídos pela Constituição, assim como corresponde ao respeito desta liberdade que o próprio Estado concedeu aos seus jurisdicionados, que poderão exercê-las de diversas formas, como a ação popular, etc.

Nas palavras de Dinamarco (2008, p. 202) a democracia corresponde a “todas as formas de influência sobre os centros do poder”, devendo elas representar “algum peso para a tomada de decisões”.

### 2.2.3 Os escopos jurídicos

A respeito dos escopos jurídicos, a primeira colocação realizada por Dinamarco (2008, p. 210) é sobre as colocações introspectivas, “que consistem na visão do sistema processual em si mesmo, visão interna e pan-processualista” não servem ao propósito de compreender os escopos jurídicos da jurisdição.

Estas colocações introspectivas, em suma, teriam a visão extremamente limitada e, por vezes, excluiriam outras partes do processo. Por exemplo, considerar que o escopo da jurisdição é a produção de decisões seria uma forma de desconsiderar, completamente, o processo executivo, pois este não produz decisões que ensejem o fim do processo, fazendo apenas “com vista às realizações práticas” (DINAMARCO, 2008, p. 211)

O problema com relação à coisa julgada gira em torno de este instituto ser exterior ao próprio processo, sendo, inclusive, anterior a este, pois são as “normas de direito positivo que instituem a autoridade da coisa julgada material” (DINAMARCO, 2008, p. 212).

Conforme este doutrinador, definir o escopo jurídico depende de qual corrente se filia, eis que a relação entre o direito material e o processual influencia na função que a jurisdição possui. As teorias são a unitária e a dualista.

A diferença entre as duas teorias se dá por meio da “visão do direito material como sistema suficiente em si mesmo para a criação de direitos e obrigações logo ao suceder de fatos relevantes” (DINAMARCO, 2008, p. 223). A teoria dualista aceita esta percepção, enquanto que a unitária defende que “ele não tem toda essa aptidão, participando então o processo do iter criativo”.

Afinal, Dinamarco apontou que o direito material tem subsistência plena sem o sistema processual, tendo em vista que o exercício dos direitos e obrigações na sociedade não dependem da intervenção de algum juiz para que eles sejam constituídos, ainda que existam casos que necessitem. Torna-se pertinente o argumento do doutrinador :

(...), há casos de insatisfação resultante da maneira como o sistema do direito positivo é construído, ditando a canalização de certas pretensões ao Poder Judiciário como único caminho para eventual satisfação e o veto a qualquer outro modo, mesmo consensual; e casos em que a insatisfação decorre da recusa da pessoa que poderia validamente atender à pretensão e eventualmente satisfazê-la, mas não o faz. Em ambos os casos, por um motivo ou por outro, a constituição de situações novas só mesmo jurisdicionalmente se pode obter – e isso é assim, sempre por motivos de ordem política. Por outro lado, quando se deixa de pensar no *jus punitiois* concreto do Estado, ou no direito de qualquer sujeito a alguma transformação jurídica, para pensar-se então na própria imposição da pena ou na transformação jurídica em si mesma, na realidade já se pressupõe o direito a esses resultados, como premissa indispensável a eles; e os resultados obtidos através do exercício da jurisdição constituem, assim, a *atuação prática* da vontade jurídica preexistente – o que confirma e não desmente, a teoria dualista do ordenamento jurídico (DINAMARCO, 2008, p. 245 e 246)

Portanto, como se nota ao final desta citação, Dinamarco (2008, p. 257) defende justamente a atuação da vontade concreta do direito como o escopo jurídico da jurisdição, devendo-se compreender o verdadeiro sentido da fórmula por meio da utilização da “observação do social agindo sobre o jurídico, gerando a inexorabilidade da agilização e universalização da Justiça”.

### **2.3 O conceito contemporâneo de jurisdição**

No Estado Constitucional em que vivemos, a atividade do magistrado ultrapassa, em muito, a mera subsunção do caso à lei, isto é, o dever do juiz é de trazer, àquela situação particular, uma norma que comporta as suas peculiaridades, conferindo sentido àquele texto, que em si, é imutável porquanto a atividade legislativa não o modifique.

Todavia, a atuação do magistrado não importa na exclusão da lei, pois esta ainda fornece a base de como o caso concreto deve ser analisado, devendo-se compreender que a legislação não é “um produto perfeito e acabado” (MARINONI; ARENHART; MITIDIERO, 2015, p.103). Isso porque a lei deve ser validada constitucionalmente, que se note o seu fiel respeito ao texto constitucional, para que ela possa ter incidência.

Conforme Marinoni, Arenhart e Mitidiero (2015), então, percebe-se que há uma inversão do que se preconizava anteriormente. Não mais se nota a lei para, então, constatar o direito a ser tutelado, mas sim o contrário, devendo-se reportar, primeiramente, ao direito fundamental resguardado na Magna Carta para, então, verificar se a lei é aplicável.

Esta ideia se torna muito mais clara pela possibilidade do controle de constitucionalidade difuso, eis que qualquer órgão do Poder Judiciário pode negar a aplicação de uma lei em vista da sua incongruência com a norma máxima, sendo possível que isso se refira a apenas uma interpretação, devendo-se adotar tão somente aquela que resguarde o intento constitucional.

Todavia, ainda que a Magna Carta possua esta relevância, não é possível que o magistrado apenas se utilize da Constituição para a criação desta norma jurídica a ser aplicada, pois ele deve se atentar às “necessidades do direito material” (MARINONI, ARENHART, MITIDIERO, 2015, p. 124). Surge, então, a função da própria jurisdição, pois esta instituição visa à tutelar as necessidades do direito material, desde que se analise de acordo com as normas e princípios ditados pelo texto constitucional.

Desta forma, a atuação judicial não se concebe apenas como uma função declarativa da Constituição, sendo que, na realidade, ela traz uma complexidade muito maior. Conforme Marinoni, Arenhart e Mitidiero:

Tanto é verdade que lhe incumbe atribuir sentido aos textos jurídicos e ao caso, definindo as suas necessidades concretas, para então buscar no sistema jurídico a regulação da situação que lhe foi apresentada, ainda que tudo isso obviamente deva ser feito sempre a partir da Constituição (2015, p. 157)

Neste sentido, estes doutrinadores, com relação à função que a jurisdição possui, repudiam a noção de que ela se presta à obtenção da pacificação social, sendo este apenas um efeito do real propósito do instituto. Na sua visão (2015, p. 124), o chamado escopo social, isto é, “a expectativa de soluções dos conflitos sociais por uma ordem institucionalizada constitui o próprio escopo do Direito, não sendo por essa razão um objetivo direto da jurisdição no Estado Constitucional”.

Para tanto, nota-se que a atividade jurisdicional se volta à aplicação do “direito”, sendo a “tarefa do juiz no Estado Constitucional” a realização de uma

“atividade de reconstrução da ordem jurídica” (OLIVEIRA; MITIDIERO, 2010, p. 126 e 127). Não cabe a este órgão inovar as relações jurídicas, pois esta é de competência do Poder Legislativo, devendo o Judiciário notar os “elementos já constantes dentro do sistema jurídico” para alcançar a solução.

O termo direito acima transcrito representa a superação da concepção de que a atividade do juiz se limita apenas à aplicação da legislação, porquanto é de sua tarefa, também, a preservação dos direitos fundamentais. Diante das diversas orientações que estes exercem sobre a atuação jurisdicional, principalmente em vista do controle de constitucionalidade, é necessário que exista a tutela de um direito fundamental perante outro, isto é, diante de um conflito, há que se efetivar um deles por meio da “aplicação de postulados normativos, como a ponderação, a concordância prática, a proporcionalidade e a razoabilidade” (MARINONI, ARENHART, MITIDIERO, 2015, p. 107).

Nesses casos, então, é o postulado que será aplicado diante do caso concreto e não a legislação, sendo eles que trazem a “concretude direta e imediata à própria Constituição, ou melhor, a uma efetividade dos direitos fundamentais que não toma em conta o plano da legislação” (MARINONI, ARENHART, MITIDIERO, 2015, p. 109).

Portanto, como já estabelecido, a atividade jurisdicional se tornou ainda mais complexa, abandonando-se os valores antes adotados. O ensinamento de Marinoni, Arenhart e Mitidiero se torna relevante novamente, em que dizem:

Afirmar que a jurisdição simplesmente declara a vontade concreta da lei ou(sic) particulariza uma norma geral para a composição uma norma geral para a composição de uma lide significa ignorar a necessidade de o Estado Constitucional dar tutela aos direitos e solapar a função da doutrina e da jurisdição como instâncias críticas de controle da adequada tutela dos direitos (2015, p. 110 e 111)

Dar a tutela neste caso não se refere tão somente ao reconhecimento, devendo-se considerar a efetiva e concreta proteção dos direitos fundamentais. Nada adiantaria a aplicação do direito se não houvesse a real proteção daquilo que se discute no processo.

A partir dessas noções, depreende-se que a jurisdição corresponde à reconstrução da ordem jurídica, não sendo nem descritiva e nem criativa, mas sim “interpretativa”, adicionando-se, conforme estes autores, a necessidade de um

“processo estruturalmente guiado pela argumentação jurídica” (MARINONI; ARENHART; MITIDIERO, 2015, p. 157).

A argumentação jurídica tratada por estes doutrinadores não se refere só àquelas produzidas pelas partes, mas também do próprio juiz. A norma reconstruída tem como finalidade compor não a parte dispositiva da sentença, mas sim a fundamentação, que ensinará a restrição da subjetividade do magistrado.

Por esta razão se diz que a interpretação ultrapassou a perspectiva cognitivista para a perspectiva adscritiva, “em que a tarefa interpretativa está em reconstruir argumentativamente os possíveis significados dos textos em seus respectivos contextos, outorgando-lhes um significativo normativo” (MARINONI; ARENHART; MITIDIERO, 2015, p. 137).

O receio que se pode ter é, justamente, o excesso de subjetivismo que a decisão pode ter. Entretanto, como já abordado acima, concebe-se que a legislação é falha, sendo possível questioná-la em face dos valores constitucionais e, em vista disso, nota-se que não se pode limitar o juiz à mera reprodução do que expressa a lei. Neste sentido, “reconhecer, valorar e decidir são tarefas inerentes à jurisdição no Estado Constitucional” (MARINONI; ARENHART; MITIDIERO, 2015, p. 137).

Além disso, não teria qualquer propósito a decisão que não tivesse a contribuição dos interessados, por clara exigência da racionalidade das decisões, em que ela “tem de ser fruto do contraditório, sob pena de não ser democraticamente aceitável” (MARINONI; ARENHART; MITIDIERO, 2015, p. 116).

Portanto, para que seja garantido o controle, Marinoni, Arenhart e Mitidiero esclarecem que:

[...] é preciso atribuir ao juiz o dever de demonstrar que a sua decisão é a melhor possível mediante uma argumentação fundada em critérios racionais. Em primeiro lugar, isso deve ser feito a partir da justificação da atividade interpretativa e da coerência e universabilidade de seu resultado. Em segundo lugar, isso deve ser promovido mediante o respeito à autoridade dos precedentes das Cortes Supremas, rigorosamente meio que assegura a universabilidade das decisões, preservando-se daí a liberdade e o respeito à igualdade mediante a outorga de segurança jurídica, sem o que não há Estado de Direito (2015, p. 158).

Diante destas percepções, notam-se algumas mudanças com relação aos conceitos anteriormente apontados.

Primeiramente, não é possível o reconhecimento da substitutividade, sendo esta aquela atividade de substituição realizada por terceiro em favor de partes conflitantes, como característica da jurisdição.

Para tanto, Oliveira e Mitidiero (2010, p. 122 e 123) apontam três motivos para esta impossibilidade, sendo eles o fato de a substitutividade não se conformar às questões processuais, eis que esta atuação é claramente um exercício da jurisdição, mas não é perceptível a efetiva substituição da atividade dos interessados; o novo sentido da atividade judicial não se conforma a este elemento, tendo em vista que não basta a mera aplicação da vontade da lei, tendo em vista a atividade de reconstrução por parte do julgador; e, por fim, este elemento não pode “explicar de maneira satisfatória a natureza da tutela jurisdicional, que jamais pode ser assimilada a um simples substitutivo do comportamento devido pelo demandado”.

Caso se volte à concepção de Carnelutti, em que há a justa composição da lide, além de este ser um elemento “pré-processual” (OLIVEIRA; MITIDIERO, 2010, p. 123), ele não cumpre a sua função de distinguir a jurisdição, eis que esta não é uma exclusividade desta, sendo possível a resolução de conflitos “de maneira autocompositiva ou buscando mecanismos extrajudiciais”.

Parte da doutrina, também, aponta a coisa julgada como elemento inerente da jurisdição. Entretanto, este conceito não se estende a toda e qualquer atividade praticada no âmbito jurisdicional, devendo-se notar as palavras de Oliveira e Mitidiero a este respeito:

Do ponto de vista dogmático, todavia, se aceitássemos a coisa julgada como característica da jurisdição teríamos de negar caráter jurisdicional à atividade judicial realizada na fase de cumprimento da sentença por execução forçada, no processo de execução e no processo cautelar, cujas decisões finais são incapazes, pela ínfima dose de declaratividade, de propiciar a formação da coisa julgada. Está assente na doutrina, contudo, que a tutela jurisdicional executiva e a tutela jurisdicional cautelar caracterizam-se como atividades jurisdicionais (2010, p. 124).

Portanto, seguindo a linha de tudo que foi exposto, a jurisdição pressupõe a tarefa de reconstruir a ordem jurídica, aplicando-se o direito conforme as necessidades do direito material, filtrando-se as diversas interpretações possíveis de

acordo com a Constituição, conforme o caso concreto. De nada adiantaria, entretanto, esta árdua tarefa, se ela não tivesse força, isto é, imperatividade.

Nesta nota, por decorrência deste elemento da jurisdição, compreende-se que a aplicação do direito por meio da jurisdição é revestida pela “irreversibilidade externa” (OLIVEIRA; MITIDIERO, 2010, p. 127), em que a decisão não poderá ser modificada por órgãos estranhos ao Poder Judiciário.

Por este motivo, afasta-se qualquer expressão que poderia ser tida como jurisdicional, como a arbitragem e do Senado Federal em crimes de responsabilidade, tendo em vista que se exige que a decisão, afinal, seja definitiva.

Para afastar ainda mais a arbitragem da jurisdição, Oliveira e Mitidiero dispuseram da seguinte forma:

A jurisdição é antes de tudo poder – é uma das manifestações do poder do povo (art. 1º, parágrafo único, CRFB), canalizado no Estado, cujo exercício se leva a cabo por meio da função judiciária. A jurisdicionalidade de um ato é aferida na medida em que é fruto de um órgão estatal, dotado de império, investido em garantias funcionais que lhe outorguem imparcialidade e independência, cuja função é aplicar o direito (e não apenas a lei) de forma específica, dotado o seu pronunciamento de irreversibilidade externa (2010, p. 125)

Sendo assim, a doutrina aponta que são características da jurisdição a “estatalidade do órgão e sua imparcialidade” (OLIVEIRA; MITIDIERO, 2010, p. 125), considerando-se a primeira em razão da consequência de sua qualidade como poder e o segundo de sua colocação como manifestação de poder do povo, isto é, exige-se que ele só poder ser exercido “por quem ostente independência e imparcialidade”, ambos garantidos na Constituição Federal.

Em suma, no Estado Constitucional, temos que a jurisdição apresenta como seus elementos a estatalidade do órgão e sua imparcialidade, sendo pressuposto de sua atuação a irreversibilidade externa. A atividade, por sua vez, depreende que o magistrado irá reconstruir a ordem jurídica, com base na necessidade do direito material, fundado na argumentação jurídica, visando a tutela, efetiva, dos direitos fundamentais.

## **2.4 Os limites da jurisdição penal**

Considera-se que o poder do Estado, na realidade, é “uno e indivisível, mas o exercício desse poder pode se dar por três diferentes manifestações, que costumam ser designadas de funções do Estado” (CÂMARA, 2004, p. 63).

Conforme Dinamarco (2008, p.141), entretanto, ao se conceber que o poder estatal é uno, compreende-se que também há unidade na jurisdição, sendo que a “distribuição da competência visa somente a dar a medida da jurisdição atribuída a cada juiz e(...) expressa somente uma distribuição de atividades”.

Portanto, de acordo com Câmara (2004, p. 73), a classificação e a divisão entre as espécies se dá “com fins didáticos, sendo extremamente importantes para que se possa travar contato com as diferentes manifestações da função jurisdicional do Estado”.

Com relação à “pretensão submetida ao Estado-juiz” (Câmara, 2004, p. 73), divide-se a jurisdição em penal e civil, sendo que esta possui um sentido amplo, abarcando diversas outras matérias, situando-se aqui as causas “extrapenais”. Portanto, verifica-se a pretensão a partir do “direito material em que se fundamenta” (CINTRA; GRINOVER; DINAMARCO, 2013, p. 168).

Sendo assim, a jurisdição penal será aquela em que o Estado deve se manifestar acerca de “pretensões de natureza penal” (CÂMARA, 2004, p. 73), notando-se que não é toda e qualquer pretensão punitiva, tendo em vista a possibilidade de se estar diante de um habeas corpus e uma revisão criminal. Qualquer outro tipo de pretensão se encaixará na espécie de jurisdição civil.

Há que se questionar, então, qual é o limite desta manifestação do poder estatal. Ora, não seria possível considerar que ele pode ser aplicado em qualquer local, devendo-se estabelecer o seu limite.

Na seara penal, os dizeres de Cintra, Grinover e Dinamarco se tornam relevantes em vista da perspectiva que eles trazem com relação ao vínculo do direito processual penal com a eficácia espacial da lei penal ao dizer que:

[...]o direito penal (direito material) se rege estritamente pelo princípio da territorialidade, não se impondo além dos limites do Estado, e como as sanções do direito penal não podem ser impostas senão através do processo, segue-se que o juiz de um Estado soluciona as pretensões punitivas exclusivamente de acordo com a norma penal pátria; ou, em outras palavras, a jurisdição penal tem limites que correspondem precisamente aos de aplicação da própria norma penal material (2013, p. 176)

Neste sentido, torna-se imperioso compreender o âmbito de aplicação espacial do direito material penal para, então, compreendermos os limites da jurisdição penal, pois, nesta mesma linha, conforme Francisco de Assis Toledo (1998, p. 48), diante dos princípios regentes da aplicação da lei penal, tem-se a “definição dos limites da jurisdição penal do Estado”, assim como se determina “as hipóteses de aplicação do direito estrangeiro”.

## **2.5 A aplicação da Lei penal no Direito Brasileiro**

Compreender os limites da eficácia espacial de uma lei penal, terminologia adotada por Luiz Flavio Gomes, Alice Bianchini e Flávio Daher (2016), significa, também, entender a relação entre os Estados soberanos em vista das suas respectivas legislações criminais.

Para estes autores, o instituto possui duas dimensões, sendo elas o “âmbito de abrangência no espaço interno: crimes de competência da Justiça brasileira”, assim como o:

âmbito de abrangência no espaço internacional: regulado pelo direito penal internacional (conjunto de regras que disciplina o *ius puniendi* de um determinado Estado em suas relações com outros Estados – CP, arts. 5º a 9º) (GOMES; BIANCHINI; DAHER, 2016, p. 162).

Portanto, assimilam-se quais são os crimes que a Justiça brasileira pode conhecer, e julgar por consequência, e estabelece a relação entre os Estados com relação ao seu poder punitivo.

Para tanto, o nosso Código Penal estabeleceu duas regras, sendo uma geral e a outra sendo a exceção.

### **2.5.1 O princípio da territorialidade: A regra geral**

O Código Penal, Decreto-Lei nº 2.848, de 7 de dezembro de 1940, estabelece, em seu artigo 5º<sup>37</sup>, o princípio da territorialidade, em que “aplica-se a lei penal brasileira aos fatos puníveis praticados no território nacional,

---

<sup>37</sup> Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.

independentemente da nacionalidade do agente, da vítima ou do bem jurídico lesado” (BITENCOURT, p.198).

Entretanto, não se trata de uma aplicação desmedida, isto é, sem limites. Por certas vezes, ainda que o delito ocorra no território nacional, o Brasil não será competente para realizar o seu julgamento, tendo em vista a presença de tratados e regras de direito internacional. Sendo assim, “nossa legislação adotou o princípio da territorialidade relativa” (GOMES; BIANCHINI; DAHER, 2016, p. 163).

Devemos compreender, então, o que é território nacional. Conforme Julio Fabbrini Mirabete(2006, p. 58), “em sentido estrito (material) território abrange o solo (e subsolo) sem solução de continuidade e com limites reconhecidos as águas interiores, o mar territorial, a plataforma continental e o espaço aéreo”.

Entretanto, o §1º do artigo 5º<sup>38</sup> do Código Penal brasileiro, ainda, explicita o chamado “território por extensão” (MIRABETE, 2006, p. 60), em que se consideram todos os navios e aeronaves brasileiras, desde que públicas ou a serviço do governo brasileiro, ou, ainda que privadas, se estão no espaço aéreo brasileiro em alto mar como extensão do território nacional.

Ou seja, nesses casos, a lei penal brasileira será aplicada em virtude deste princípio, eis que a lei aumentou o âmbito de aplicação da lei, alcançando estes navios e aeronaves.

Com relação às demais aeronaves e embarcações marítimas, o §2º<sup>39</sup> do mesmo artigo do Código Penal brasileiro esclareceu que, desde que elas se encontrem em voo ou pousadas em território nacional ou no porto ou mar territorial brasileiro, a lei brasileira será aplicada.

Como se percebe, consideram-se as embarcações e aeronaves estrangeiras “como extensão do território correspondente à sua bandeira” (GRECO, 2011, p. 125), adotando-se a mesma lógica do §1º deste mesmo artigo.

Entendendo-se até que ponto o princípio da territorialidade é aplicado, deve-se passar a análise das exceções.

---

<sup>38</sup> § 1º - Para os efeitos penais, consideram-se como extensão do território nacional as embarcações e aeronaves brasileiras, de natureza pública ou a serviço do governo brasileiro onde quer que se encontrem, bem como as aeronaves e as embarcações brasileiras, mercantes ou de propriedade privada, que se achem, respectivamente, no espaço aéreo correspondente ou em alto-mar.

<sup>39</sup> § 2º - É também aplicável a lei brasileira aos crimes praticados a bordo de aeronaves ou embarcações estrangeiras de propriedade privada, achando-se aquelas em pouso no território nacional ou em vôo no espaço aéreo correspondente, e estas em porto ou mar territorial do Brasil

## 2.5.2 Os demais princípios e as condições da extraterritorialidade

As exceções ao princípio da territorialidade estão dispostas no artigo 7º do Código Penal brasileiro, em que se definem as hipóteses de extraterritorialidade, em que os infratores se sujeitam à lei penal ainda que estejam noutro território.

Conforme Nucci, estes são os princípios regentes da extraterritorialidade da lei penal:

b.1)defesa ou proteção (leva-se em consideração a nacionalidade brasileira do bem jurídico lesado pelo delito); b.2) justiça universal ou cosmopolita (tem-se em vista punir crimes com alcance internacional); b.3) nacionalidade ou personalidade (leva-se em conta a nacionalidade brasileira do agente do delito); b.4) representação ou bandeira (tem-se em consideração a bandeira brasileira da embarcação ou da aeronave privada, situada em território estrangeiro) (2011, p. 128).

Para melhor compreensão, devemos notar o que prescreve o artigo 7º do Código Penal para, então, determinarmos qual o princípio a ser aplicado. É o seu teor:

Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro:  
I - os crimes:  
a) contra a vida ou a liberdade do Presidente da República;  
b) contra o patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa pública, sociedade de economia mista, autarquia ou fundação instituída pelo Poder Público;  
c) contra a administração pública, por quem está a seu serviço;  
(BRASIL, 1984).

Diante da leitura do diploma legal em destaque, verifica-se que consiste na adoção do princípio real, da defesa ou da proteção, que, nas palavras de Bitencourt (2010, p. 199), “permite a extensão da jurisdição penal do Estado titular do bem jurídico lesado, para além dos seus limites territoriais, fundamentando na nacionalidade do bem jurídico lesado”, notando-se que o artigo é claro que se trata de uma hipótese de extraterritorialidade incondicionada, isto é, será aplicada, sendo que o “agente será punido segundo a lei brasileira, ainda que absolvido ou condenado no estrangeiro” (GRECO, 2011, p. 128).

O artigo 7º do mesmo códex continua com a alínea “d”, estabelecendo a aplicação da lei brasileira no caso “de genocídio, quando o agente for brasileiro ou domiciliado no Brasil”. A hipótese retratada demonstra a aplicação do princípio da competência universal, justiça universal ou cosmopolita, sendo decorrente da “cooperação penal internacional, porque permite a punição, por todos os Estados, de todos os crimes que forem objeto de tratados e de convenções internacionais” (BITENCOURT, 2010, p. 199).

Mirabete (2006, p. 57), por sua vez, assinala que este é o “princípio ideal no combate à criminalidade, evitando-se a impunidade pela fuga do agente do país em que cometeu o delito”. Porém, em razão deste crime ter ocorrido em outro território, reconhece-se a dificuldade de se produzir as provas referentes ao delito.

Percebe-se, então, o interesse do Estado em tutelar a defesa de certos bens jurídicos, independente de onde a efetiva lesão tenha ocorrido, aplicando-se a lei brasileira de forma incondicionada, isto é, “o interesse punitivo da Justiça brasileira deve ser exercido de qualquer maneira” (NUCCI, 2011, p. 132), sendo “obrigatória a aplicação da lei brasileira ao crime cometido fora do território brasileiro” (MIRABETE, 2006, p. 63).

O §1º do artigo 7º<sup>40</sup> do Código Penal estabelece, ainda, a possibilidade de aplicação da lei penal brasileira ainda que o agente tenha sido absolvido ou condenado no estrangeiro, não surtindo efeito quanto à persecução do *ius puniendi* brasileiro. No entanto, nota-se que o artigo 8º<sup>41</sup> do mesmo código, no intuito de prevenir o *bis in idem*, isto é, o cumprimento da mesma pena mais de uma vez, estabelece que a pena cumprida no estrangeiro atenua a pena ditada pela justiça brasileira ou considera-se cumprida caso seja idêntica. De qualquer forma, em vista destas características, trata-se da extraterritorialidade incondicionada.

Um obstáculo à aplicação destas hipóteses é, conforme Gomes, Bianchini e Daher (2016, p. 169), a dicção do artigo 366 do Código de Processo Penal em que se estabelece a suspensão do processo na ausência de indicação de advogado pelo réu. Em razão das circunstâncias em que a extraterritorialidade incondicionada se encontra, julgamento de crimes ocorridos fora do território nacional a qualquer custo,

---

<sup>40</sup> § 1º - Nos casos do inciso I, o agente é punido segundo a lei brasileira, ainda que absolvido ou condenado no estrangeiro.

<sup>41</sup> Art. 8º - A pena cumprida no estrangeiro atenua a pena imposta no Brasil pelo mesmo crime, quando diversas, ou nela é computada, quando idênticas.

sendo ele “citado por edital” na impossibilidade de encontra-lo, ensejando “a suspensão do processo e da prescrição”.

O artigo 7º, no inciso II, estabelece outros crimes que o Brasil irá reprimir ainda que tenham ocorrido no estrangeiro. Segue o texto:

Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro:

II - os crimes:

a) que, por tratado ou convenção, o Brasil se obrigou a reprimir;

b) praticados por brasileiro;

c) praticados em aeronaves ou embarcações brasileiras, mercantes ou de propriedade privada, quando em território estrangeiro e aí não sejam julgados (BRASIL, 1984).

Veja que cada alínea corresponde a um princípio diferente, sendo que o primeiro demonstra claramente a adoção do princípio da universalidade, que já foi comentado acima. De qualquer modo, trata-se de hipótese em que ligada “à cooperação penal internacional que deve existir entre os povos para prevenir e reprimir aquelas infrações penais que interessam a toda a comunidade internacional” (BITENCOURT, 2010, p. 204).

O princípio abordado na alínea “b” é aquele referente à nacionalidade, também sendo chamado de princípio da personalidade, em que se considera a nacionalidade do agente delitivo. Neste caso, reputa-se que o “Estado tem o direito de exigir que seu cidadão no estrangeiro tenha determinado comportamento” (MIRABETE, 2006, p. 57).

Para compreendermos a relevância desta hipótese apontada pelo legislador, devemos nos voltar, rapidamente, às regras de extradição, eis que, o inciso LI do artigo 5º<sup>42</sup> da Constituição Federal estabelece a impossibilidade de se extraditar um brasileiro nato. Desta forma, o legislador contribuiu para que se evitasse “eventual impunidade” no caso de não conceder a extradição, sendo “absolutamente correto que se aplique a lei brasileira” (BITENCOURT, 2010, p. 204).

Por fim, a última alínea adota o princípio da representação ou da bandeira, em que na ocasião de “deficiência legislativa ou desinteresse de quem deveria

---

<sup>42</sup> Art. 5º 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:

LI - nenhum brasileiro será extraditado, salvo o naturalizado, em caso de crime comum, praticado antes da naturalização, ou de comprovado envolvimento em tráfico ilícito de entorpecentes e drogas afins, na forma da lei;

reprimir, aplica-se a lei do Estado em que está registrada a embarcação ou a aeronave cuja bandeira ostenta aos delitos praticados em seu interior” (BITENCOURT, 2010, p. 200), sendo, deste modo, subsidiário.

Assim como na hipótese anterior, busca-se reprimir a impunidade caso o fato punível não seja julgado pelo Estado que detém o território em que ocorreu o crime.

Diversamente do que ocorre nos casos do inciso I, conforme esse inciso, a lei penal brasileira só será aplicada se certas condições forem adimplidas, conforme se determina pelo §2º do mesmo artigo, em que se determina:

§ 2º - Nos casos do inciso II, a aplicação da lei brasileira depende do concurso das seguintes condições:

- a) entrar o agente no território nacional;
- b) ser o fato punível também no país em que foi praticado;
- c) estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição;
- d) não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena;
- e) não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável (BRASIL, 1984)

Diante da necessidade de adimplemento destas condições, consideradas “condições objetivas de punibilidade”, conforme Gomes, Bianchini e Daher (2016, p. 170), nomeia-se esta situação como extraterritorialidade condicionada, notando-se que, não se preenchendo qualquer uma destas condições, tem-se que “não se trata de fato punível no Brasil”.

Por fim, o §3º determina a chamada extraterritorialidade hipercondicionada, em que se apresentam novos requisitos para que se tenha incidência da lei penal brasileira em uma específica hipótese, como se percebe do seu teor:

§ 3º - A lei brasileira aplica-se também ao crime cometido por estrangeiro contra brasileiro fora do Brasil, se, reunidas as condições previstas no parágrafo anterior:

- a) não foi pedida ou foi negada a extradição;
- b) houve requisição do Ministro da Justiça (BRASIL, 1984)

Aqui se trata da aplicação do princípio da personalidade, só que na sua modalidade passiva, eis que, no inciso II deste mesmo artigo, houve referência a este princípio, só que na modalidade ativa. Portanto, visa-se a proteger os nacionais

de alguns crimes que ocorrem no estrangeiro, mas sendo imperioso que se verifiquem todas as condições dos §§ 2º e 3º para que haja a incidência da lei pátria.

## 2.6 O local do crime

De nada adiantaria o estudo dos princípios adotados na eficácia espacial da lei penal se não conseguirmos determinar o local em que o crime ocorreu, estabelecendo-se um nexos de relevância entre estes dois institutos, como já assinalado por Mirabete (2006, p. 61), em que “para a aplicação da regra da territorialidade é necessário, entretanto, que se esclareça qual é o lugar do crime”.

Três são as teorias que podem ser adotadas para definir o lugar do crime e Greco (2011, p. 123) as sintetizou bem quanto à sua conceituação, como se demonstra abaixo:

Na teoria da atividade, lugar do crime seria o da ação ou da omissão, ainda que outro fosse o da ocorrência do resultado. Já a teoria do resultado despreza o lugar da conduta e defende a tese de que lugar do crime será tão somente, aquele em que ocorrer o resultado. A teoria da ubiquidade ou mista adota as duas posições anteriores e aduz que lugar do crime será o da ação ou da omissão, bem como onde se produziu ou deveria produzir-se o resultado (2011, p. 123).

Da leitura destes três conceitos, nota-se que a teoria da ubiquidade é aquela que melhor satisfaz o interesse estatal, pois se abarcam as situações em que apenas o resultado se produz em território nacional ou apenas a ação é aqui realizada.

O nosso Código Penal estabelece o lugar do crime no artigo 6º<sup>43</sup>, em que se verifica a adoção da teoria da ubiquidade, bastando, então, “qualquer contato do delito com o território brasileiro (juridicamente considerado)” (GOMES, BIANCHINI e DAHER, 2016, p. 208).

Há que se assinalar a relevância desta teoria, então, para os crimes que envolvem dois ou mais países, os chamados crimes a distância ou de espaço máximo, pois o “tocar”, compreendendo-se como “ato de execução ou consumação

---

<sup>43</sup> Art. 6º - Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.

no Brasil” (GOMES, BIANCHINI e DAHER, 2016, p. 208), é suficiente para a aplicação da lei penal.

Quanto a este ponto específico, Mirabete (2006, p. 62) ressalta alguns pontos com relação ao dispositivo já citado. Primeiramente, ele aponta que o texto foi suficiente para alcançar as tentativas, assim como, apesar da supressão do termo parte do resultado, compreende-se, conforme os “interesses nacionais”, que “parte do resultado também é resultado”.

Entretanto, ele anota também que “não vige a regra da territorialidade na hipótese de conduta e resultado ocorridos no exterior quando se produzam no território apenas efeitos secundários do crime” (MIRABETE, 2006, p. 62).

Compreendidos o papel da jurisdição e qual o limite dela com relação à matéria penal no Brasil, devemos, agora, compreender como a jurisdição e a internet se relacionam, tendo em vista as diversas percepções sobre esse assunto no plano internacional.

## 2.7 A jurisdição e a internet

Diante das peculiaridades da internet, como a ilusão de se estar em todos os locais simultaneamente, não é de se estranhar que tenha nascido a compreensão de que na internet não vigem as mesmas leis do que no mundo físico.

Já em 1996, John Perry Barlow escreveu uma carta às diversas nações do mundo postulando a “*declaration of the independence of Cyberspace*”<sup>44</sup>, em que afirmou, no começo do documento:

*Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather*<sup>45</sup> (1996).

Há que se notar, entretanto, que este ocorreu no começo da internet, um momento diverso. Hoje estamos acostumados com as diversas transações que

---

<sup>44</sup> Declaração de independência do ciberespaço (tradução livre).

<sup>45</sup> Governos do mundo industrial, seus gigantes de carne e aço, eu venho do Ciberespaço, a nova casa da mente. Em nome do futuro, eu peço para que vocês do passado nos deixem em paz. Vocês não são bem-vindos entre nós. Vocês não tem soberania onde nós nos reunimos (tradução livre)

podemos realizar pelo meio virtual, ações que refletem no nosso cotidiano, mas naquele tempo “*it did genuinely feel separate from the real world*”<sup>46</sup>, porque os usuários “*used it to participate in communities of people who rarely met face-to-face but who got to know one another intimately*”<sup>47</sup> (GOLDSMITH, 2006).

Ainda conforme Goldsmith (2006), o ponto principal para Barlow era justamente que “*the cyberspace legal order would reflect ethical deliberation instead of the coercive power that characterized real-space governance*”<sup>48</sup>

Berman (2007) reflete que este é um pensamento inicial, podendo chamar aos que aderem a esta perspectiva como “*exceptionalists*”, isto é, excepcionistas, pois estes compreendem que “*the medium itself created radically new problems requiring new analytical work to be done*”<sup>49</sup>.

Portanto, de acordo com os autores que defendem esta noção, as leis dos mais diversos Estados não poderiam ser aplicadas no meio virtual, afinal, quando estamos na internet, não estamos em nenhum local específico.

Não se concebe, entretanto, que se trate de um local definitivamente sem lei, pois quem seriam os criadores das regras naquele espaço seriam os próprios usuários em suas comunidades específicas.

David G. Post (1995), por sua vez, adota o ponto de vista de que quem deveria determinar as regras a serem seguidas seriam as próprias comunidades, ou como ele diz “*individual network organizations*”<sup>50</sup>.

O que este pretende dizer é que, para que uma pessoa participe de uma comunidade, ela deve se pautar conforme as regras inerentes da internet, isto é, a forma como as mensagens devem ser enviadas, além das que esta organização estabeleceu para o seu conteúdo. Por exemplo, se uma comunidade tem como intuito discutir as últimas inovações no ramo automobilístico, não faria sentido, e nem aceito, a abertura de um tópico em que se discutam os atuais caminhos percorridos pela política.

Tendo em vista esta perspectiva, o controle que estas organizações individuais possuem sobre seus membros, em conjunto com a própria natureza da

---

<sup>46</sup> (mas naquele tempo) realmente aparentava ser um local separado do mundo real (tradução livre).

<sup>47</sup> (porque os usuários) a utilizavam para participar de comunidades em que as pessoas raramente se conheciam pessoalmente, mas que conheciam de forma íntima uns aos outros (tradução livre).

<sup>48</sup> A organização legal do ciberespaço refletiria uma deliberação ética ao invés de um poder coercitivo que caracteriza a governança do espaço real (tradução livre).

<sup>49</sup> O meio por si só criou novos problemas que requerem novo trabalho analítico (tradução livre).

<sup>50</sup> Organizações de redes individuais (tradução livre)

internet, um meio que não é físico, não possui posição geográfica específica, em que não existe um sujeito que seja capaz de estabelecer regras gerais de conduta, não se admite que a Lei, elemento normativo estabelecido por um Estado seja suficiente e capaz para regular o ciberespaço.

Tal premissa se parte, primeiramente, da dificuldade de controle das atividades realizadas em meio virtual. Como visto anteriormente, a possibilidade de exercer a jurisdição brasileira em face dos crimes cibernéticos depende da noção de aplicação da lei penal no espaço. Para tanto, aplica-se, em regra o princípio da territorialidade. Todavia, admitem-se hipóteses em que é possível que a lei penal seja aplicável em espaços que não correspondam ao território brasileiro, quais sejam os princípios da defesa real, da bandeira, entre outros.

No dizer de Post (1995), entretanto, estes mecanismos “*entail additional enforcement costs, both in terms of the direct cost of projecting sovereign power extra-territorially and the costs of coordinating and harmonizing the legal regimes of competing sovereigns*”<sup>51</sup>.

A aplicação destes mecanismos se dificulta pela própria natureza da internet, pois, em um momento um indivíduo pode estar acessando um documento localizado na China e, posteriormente, por meio de um clique, acessar outro documento que está armazenado na Alemanha. O ponto principal para o autor, quanto a esta questão, é que o usuário não se importa com a localização do que quer que ele deseje acessar, contanto que ele tenha o acesso pretendido. Portanto, seriam irrelevantes as fronteiras físicas.

A aplicação de leis no âmbito virtual resultaria em duas situações, conforme Post (1995). A primeira seria a possibilidade de estas mesmas comunidades passarem despercebidas, tendo em vista o alto custo de monitorar toda e qualquer atividade na Internet. A segunda seria justamente realocar para fora do controle daquela jurisdição, isto é, manter os recursos em uma jurisdição que os aceite.

Sendo assim, a ausência de controle dos Estados sobre estas comunidades seria suficiente para se afirmar que as regras devem ser ditadas pelas próprias

---

<sup>51</sup> Implicam custos adicionais de aplicação, tanto em termos de custo direto de projetar o seu poder de soberania para fora de seu território como os custos de coordenar e harmonizar os regimes legais de outras soberanias (tradução livre)

comunidades, na visão deste autor, criando-se um “*Market of rules*”<sup>52</sup>, em que os usuários devem buscar aquelas comunidades que mais lhe adequem.

Entretanto, a adoção desta perspectiva pode gerar diversos abusos por parte destas comunidades. É possível supor o caso de um membro deste grupo praticar algum ato contrário à vontade da maioria e, então, sofrer a repressão deste, tendo os seus dados pessoais revelados. Ou ainda, no caso de duas comunidades conflitantes, espalha-se na internet, em outros locais, um suposto crime que um indivíduo desses grupos teria cometido.

Há que se questionar a proteção que estas vítimas ou qualquer indivíduo na rede terão diante de situações como este caso se entenda que as comunidades que determinam as suas regras.

Por outro lado, conforme Berman (2007), os *unexceptionalists* estabelecem que o ciberespaço, ainda que seja uma novidade, não traz qualquer inovação quanto à forma como devemos aplicar o direito, isto é, as instituições permanecem e são eficazes quando tratamos de regulação no espaço virtual.

Como um dos maiores expoentes dos chamados *unexceptionalists*, Goldsmith (2006) esclarece que a internet, na realidade, possui as mesmas barreiras geográficas que o mundo real tem. Como o seu próprio livro se intitula, a percepção de que o meio virtual seria um mundo sem fronteiras é tão somente uma ilusão.

Primeiramente, antes de se explicar a necessidade de se ter a aplicação do direito no mundo virtual, tem-se o motivo pelo qual a internet é dependente das questões geográficas.

A principal razão de se existirem fronteiras no meio virtual é resultante da própria arquitetura da rede. Veja-se, conforme foi afirmado anteriormente, ainda que exista um mundo virtual denso e complexo, para que ele efetivamente exista se requer todo um aparato físico que possibilite a sua atividade. No mesmo sentido, Goldsmith esclarece:

*Bandwidth limitations illustrate an important but poorly understood fact: the efficacy of Internet communications depends on the real-space location of both data and the underlying Internet hardware through which the data travel (routers and exchange points, and the*

---

<sup>52</sup> Mercado de regras (tradução livre).

*fiber-optic cables, phone lines, cable lines, and microwave and satellites transmitters and receptors that interconnect them*)<sup>53</sup> (2006).

Portanto, ainda que se pretenda acessar um conteúdo no Japão, por exemplo, há que se reconhecer que a existência deste depende de um aparato físico e isso influencia diretamente no tempo que levará para ter o seu acesso.

Em um artigo tratando especificamente dos dados presentes em uma *cloud*, Woods (2016) estabelece que “*data has physical and intangible features, both of which provide helpful precedent for states seeking to assert jurisdiction over data*”<sup>54</sup>, sendo que estes dados estão presentes em servidores, que, por sua vez, estão dentro de um território sujeito a alguma jurisdição.

O estudo deste é bastante interessante, tendo em vista que ele concebe que o tratamento dos dados como um objeto intangível não seria algo revolucionário no Direito, em razão da existência da propriedade intelectual e os débitos. Materialmente estes não existem, mas a abstração deles é plenamente aceita na sociedade e, inclusive, a aplicação de normas referentes a estes institutos poderá ocorrer de forma extraterritorial a depender do caso.

Como Woods (2016) mesmo reconhece, a aplicação extraterritorial do direito leva aos conflitos de jurisdição, que também não é uma novidade e esta afirmação, por si só, não resolve o problema que estes conflitos geram, mas provém “*a number of helpful insights drawn from past precedents*”<sup>55</sup>.

Mas não se trata apenas do aspecto físico, na concepção de Goldsmith (2006). Na realidade, os próprios usuários “*demanded different Internet experiences that corresponded to geography*”<sup>56</sup>, que se representa pelo conteúdo acessado, pelas publicidades apresentadas e, inclusive, a linguagem apresentada na página da *Web*.

Os indivíduos que acessam a internet desejam, ainda mais considerando a característica comercial como cada vez mais integrante deste meio, uma experiência

---

<sup>53</sup> As limitações da largura de banda ilustram um importante, mas pouco compreendido fato: a eficácia das comunicações da internet dependem da localização no espaço real tanto dos dados como do hardware fundamental da internet pelo qual a informação é transmitida (roteadores e pontos de troca, e cabos de fibra óptica, linhas telefônicas, linhas de cabo, e micro-ondas e transmissores de satélites e receptores que os interconectam (tradução livre).

<sup>54</sup> Dados possuem características físicas e intangíveis, ambas que proporcionam um precedente útil para os Estados que buscam afirmar as suas jurisdições sobre estes dados.

<sup>55</sup> Um número de perspectivas úteis de precedentes passados (tradução livre).

<sup>56</sup> Demandavam diferentes experiências com a internet que correspondem à geografia (tradução livre).

personalizada de acordo com a sua localização. Não interessa a um brasileiro certo desconto que apenas alcança moradores da Argentina, mas sim que tenha disponibilidade no Brasil.

Desta forma, concebe-se que a localização dos diversos usuários se torna extremamente relevante, tornando a internet cada vez mais acessível para as diferentes populações, estabelecendo o conteúdo conforme a sua linguagem e cultura, assim como oferecendo serviços que lhe alcançam.

Diante do exposto, deve-se abordar a necessidade de se ter a aplicação do direito quanto aos fatos ocorridos no meio virtual. Um grande exemplo trazido por Goldsmith (2006) é com relação ao eBay, um sítio conhecido internacionalmente, que possibilita a venda e compra dos mais diversos objetos disponibilizados por seus usuários.

A princípio, o seu criador acreditava que a comunidade conseguiria se coordenar de forma a garantir que não haveriam abusos. Entretanto, com o passar do tempo, o número de pessoas acessando e realizando as diversas transações ultrapassaram as expectativas e, logo, começaram a surgir diversos casos de fraude.

Goldsmith (2006) aponta que a lei não se volta aos usuários honestos do eBay, ou qualquer que seja o serviço virtual, mas sim se dirige às pessoas “*whose primary interest is stealing money or goods*”<sup>57</sup>, sendo que “*without the threat of law enforcement behind eBay’s community system, it could be quickly overrun by criminal fraud*”<sup>58</sup>.

Porém, a questão criminal é somente uma expressão da aplicação do direito às transações realizadas por meio do eBay. Veja-se que, no dizer deste mesmo autor, toda vez que os usuários fazem uma transação, eles estão ligados por meio de um contrato, em que a obrigação decorrente deste é essencial para o sítio.

Diante da situação apontada, Goldsmith indica que os *exceptionalists* não notaram uma questão particular das comunidades em geral. A intervenção do Estado se torna determinante quando estamos a tratar das relações entre particulares, de forma a proteger os interesses destes, evitando que os indivíduos abusem da sua posição de poder, que não ocorram crimes, entre outros. Não se

---

<sup>57</sup> Que o interesse principal é furtar dinheiro ou bens (tradução livre).

<sup>58</sup> Sem a ameaça da aplicação da lei por trás do sistema de comunidade do eBay, este logo seria inundado por fraudes (tradução livre).

ignora o fato de uma regulação abusiva, em que se retira a liberdade dos usuários, mas há que se notar que os limites devem sempre ser discutidos e definidos, de forma a evitar abusos por parte do próprio governo. O autor compreende, afinal:

*Public goods and related virtues of government control of the Internet are necessary across multiple dimensions for the Internet to work, and as a practical matter only traditional territorial governments can provide such goods*<sup>59</sup> (2006).

Portanto, concebe-se, na percepção dos *unexceptionalists*, que as regras e princípios existentes são suficientes para lidar com os fatos ocorridos no meio virtual, sem a necessidade de se pensar que se trata de algo novo. Berman (2007), por sua vez, combate esta perspectiva, tendo em vista que “*what is well-settled for one generation (or in one century) is apt to be very different from what is well-settled for the next*”<sup>60</sup>.

Berman (2002) compreende que devemos ter uma nova percepção de jurisdição. Na realidade, esta seria um produto de influências sociais, culturais, entre outros, motivos pelos quais se deveria considerar a presença de atores não estatais.

Basicamente, este autor parte da premissa de que a jurisdição estatal, como compreendida atualmente, partindo de conceitos territoriais, não seria suficiente para enfrentar os problemas atuais referentes às diversas relações que os nacionais de diversos Estados realizam entre si.

Portanto, parte-se de uma noção pluralista de jurisdição, diversamente da universalista. A diferença entre eles é justamente que este último se volta para a prevalência de somente uma jurisdição, suprimindo os pequenos grupos jurisdicionais e as relações que os indivíduos possuem com o local em que vivem, por exemplo.

A perspectiva pluralista busca evitar estes defeitos da perspectiva universalista, identificando os indivíduos com os seus territórios, assim como com relação às suas comunidades, além de reconhecer que “*law does not reside solely in*

---

<sup>59</sup> Bens públicos e virtudes relacionadas ao controle governamental da internet são necessárias através de múltiplas dimensões da internet para funcionar, e, num ponto de vista prático, somente os tradicionais governos territoriais podem prover tais bens (tradução livre).

<sup>60</sup> O que é bem assentado para uma geração (ou em um século) está apto a ser bem diferente do que será bem assentado para a próxima (tradução livre).

*the coercive commands of a sovereign power [...] law is constructed through the contest of various norm-generating communities*<sup>61</sup> (BERMAN, 2002, p. 492 e 493).

Para Berman (2002), a jurisdição seria tanto exercida por atores estatais quanto comunidades, qualquer uma, sendo que a diferença seria que as últimas não seriam capazes de executar a decisão, devendo-se voltar aos primeiros.

Neste sentido, as comunidades virtuais seriam capazes de criar suas regras, considerando-se que este seria um avanço natural, tendo em vista que há várias instituições autônomas que definem regras para os seus membros, como “*tribal or ethnic enclaves, religious organizations, corporate bylaws, social custos, private regulatory bodie, and a wide variety of groups, associations, and non-state institutions*” (BERMAN, 2002, 504).

Entretanto, por mais que as palavras de Berman apresentem uma perspectiva interessante, há que se ter noção da realidade vivida pelo Estado em questão, assim como da matéria a que se pretende regular.

Primeiramente, soberania é um conceito essencial quando estamos a tratar de Direito Internacional Público e se concebe que, dentre os pressupostos da soberania interna, existem os direitos à organização política, de legislação, de jurisdição e de domínio, conforme Accioly (2011, p. 320).

Note-se a perda que o Estado sofre com relação às situações que antes regulava. Atualmente, ele pode regular a maior parte das situações que ocorrem em seu território, excetuando-se apenas aquelas em que ele cedeu a terceiros em razão de acordos e tratados internacionais, enquanto que poderá aplicar a sua legislação a situações que ocorrem fora deste território em casos excepcionais.

Diante desta visão pluralista-cosmopolita, tem-se que o Estado passa a regular um menor número de situações e vê seu judiciário julgando ações que afetam certas comunidades de seu território que não necessariamente ocorreram neste local. Certamente, esta é uma restrição que poucos Estados estão aptos a fazer.

Isso sem falar do próprio Direito Penal, que é aplicado exclusivamente pelo Estado, questionando-se como que estas questões seriam reguladas, eis que a base do pensamento pluralista-cosmopolita seria o grau de contato com a comunidade. Não se trata apenas disso, tendo em vista que o fundamento desta área do direito se

---

<sup>61</sup> O direito não reside apenas em comandos coercitivos de um poder soberano [...] o direito é construído através do conflito entre várias comunidades criadoras de normas.

dá, também, pela retirada da autotutela, assegurando aos seus jurisdicionados que haverá a posterior pacificação com justiça.

A situação em que um membro de uma comunidade comete um delito contra outro representa, de certa forma, um fato simples de se resolver. Entretanto, diante de um indivíduo, alheio a certa comunidade, que comete um crime contra algum membro desta, nota-se uma complicação. Questiona-se qual o local que seria julgado o infrator, considerando-se o local em que ele estava ao tempo do crime, o da infração, da vítima e, inclusive, o da comunidade.

O fato é que estas ideias, apesar de incitarem o debate, não são aplicáveis à realidade brasileira, ou de qualquer lugar atualmente, devendo-se voltar às possibilidades que estão à disposição.

Apesar de as regras territoriais não serem imunes de crítica, elas definem o básico para que os países possam trabalhar entre si para garantir que não ocorra a impunidade, como se verá mais a frente.

Portanto, apesar de as regras existentes atualmente não serem as ideais, temos que elas realizam o seu trabalho de forma suficiente e, sendo necessário, ainda que de forma lenta, elas podem ser modificadas para garantir o alcance de certas situações pela jurisdição de certo Estado.

### 3 OS CRIMES CIBERNÉTICOS NO BRASIL

Esclarecido o funcionamento da internet, assim como a nova concepção de jurisdição no Estado Constitucional, resta compreender as condutas relevantes para o Direito Penal neste contexto.

Como é de conhecimento comum, esta seara do Direito possui como princípio a intervenção mínima, que, conforme Gomes, Biachini e Daher (2016, p. 62), manifesta-se por meio do seu caráter fragmentário e subsidiário.

O caráter fragmentário significa que o Direito Penal deve apenas se ocupar com “ataques (ofensas) intoleráveis (geradores de lesões ou perigo de lesão) a bem jurídicos relevantes” (GOMES; BIACHINI; DAHER, 2016, p. 62). Requer-se, então, que o ato praticado pelo delinquente seja suficiente para gerar a efetiva lesão, ou a sua ameaça, a um bem jurídico tutelado pelo Estado.

Por sua vez, a subsidiariedade aponta, ainda no dizer dos mesmos autores (2016, p. 63), que o Direito Penal deve atuar tão somente como a última medida, *ultima ratio*, principalmente em razão de suas implicações, como a privação da liberdade.

É possível se questionar quais seriam os bens jurídicos a serem tutelados quando tratamos da internet. Veja-se que o artigo 3º da Lei nº 12.965/14, o marco civil da internet, estabelece alguns princípios que devem ser observados quando da disciplina da internet no território brasileiro, assim como no artigo 7º, referem-se aos direitos dos usuários quanto ao acesso e uso da internet.

Da leitura destes artigos, destacam-se a garantia da liberdade dos indivíduos, a inviolabilidade de sua intimidade, seja pessoal ou o sigilo decorrente de suas comunicações, o acesso à internet e a proteção dos dados em si, significando a preservação de sua integridade.

O Estado visa a preservar tais situações, tendo em vista a própria natureza da internet. Nota-se que a partir do momento em que o indivíduo tem acesso a rede, ele está suscetível às diversas benesses do ambiente, assim como os seus malefícios.

Como em qualquer local, existem pessoas que visam ao bem, assim como aquelas que se aproveitam de determinadas circunstâncias para prejudicar os outros em seu benefício. Tais atividades são correntes na internet, principalmente em vista do anonimato.

Estabelecendo-se como princípios a proteção da privacidade, assim como a preservação e garantia da neutralidade da rede, conforme os incisos II e IV do artigo 3º da Lei nº 12.965/14, tem-se que os indivíduos podem acessar a internet sem que os outros saibam quem ele é, garantindo-se a sua privacidade, da mesma forma que sob um duplo aspecto se preserva a neutralidade da rede, seja pela igualdade de tratamento das informações, “qualquer que seja a informação, o destinatário ou a fonte”, ou a vedação que esta lei traz com relação à impossibilidade de os “provedores de conexão à internet, onerosa ou gratuita, de bloquear monitorar, filtrar, analisar ou fiscalizar o conteúdo dos pacotes de dados” (CARVALHO, 2014, p. 115 e 117).

Como já esclarecido acima, o anonimato vem com as suas consequências. Em razão desta qualidade, a internet está recheada de ameaças aos seus usuários, como se esclarece pela lista apresentada por Emerson Wendt e Higor Vinicius Nogueira Jorge (2013, p. 18 a 52), constando como exemplos a engenharia social, alguns tipos de vírus, *worm*, cavalo de troia, *Keylogger*, *Phishing*, entre outros.

Tais ameaças funcionam, no entanto, por uma perspectiva já tratada anteriormente, em que a maior parte dos usuários da internet não compreende como esta funciona, limitando-se a entender como a aplicação que pretende utilizar realiza o serviço esperado, sendo possível que estes acabem se sujeitando a certas situações não pretendidas.

No entender de Spencer Toth Sydow, a sociedade da informação que vivemos hoje seria uma sociedade de risco, em que se têm uma linha muito tênue entre a segurança real e a mera sensação de segurança. Neste sentido, ele diz:

O escudo que a tela do computador representa não raro traz ao usuário a sensação de segurança, dando aparência de inatingibilidade. Não estar exposto em suas fragilidades faz com que prevaleça a ideia de segurança e com que o ser humano tenda a agir com menos limites e mais ousadia em tal situação (2015, p. 39 a 42).

Ainda conforme Sydow (2015, p. 43), diversamente do que ocorre fora do ambiente virtual, em que o indivíduo pode notar o local que o cerca e perceber os perigos inerentes a este, no meio virtual, o usuário comum não possui esta mesma percepção, tendo em vista a ausência de familiaridade com o meio. Sendo assim, o

“usuário-vítima não sabe onde está na rede, porque não está em lugar algum e, ao mesmo tempo, está em todos”.

Tal afirmação é interessante, tendo em vista que aponta uma diferença relevante entre o presente trabalho e o do autor supracitado. Há que se notar que a perspectiva trazida por este tem como base a ubiquidade como característica do direito informático, em que, neste ambiente virtual, em razão da “conectividade, pode-se estar em diversos lugares virtuais ao mesmo tempo, independentemente da velocidade de sua conexão, da capacidade individual ou de barreiras físicas e políticas” (SYDOW, 2015, p. 107).

Entretanto, de acordo com o que foi visto anteriormente, não seria possível defender esta noção. Veja-se que, sim, o usuário tem acesso a uma enorme gama de conteúdos espalhados pelos diversos locais do globo, mas ele se encontra tão somente em um local, qual seja, no mesmo lugar em que se encontra a sua máquina.

Caso um indivíduo pretenda acessar um conteúdo que se encontra hospedado em um servidor na Inglaterra, por exemplo, ele irá enviar um requerimento até aquele, pedindo para que lhe seja enviado o documento, e, usualmente, será atendido. Entretanto, em momento algum ele se deslocou na rede, havendo, tão somente, a troca de pacotes de dados, o que ocorre a todo o momento na internet.

Portanto, o que se tem é necessidade de se garantir aos usuários que eles tenham segurança real, que só pode ser alcançada quando forem preservados três elementos, todos constantes da Convenção de Budapeste sobre Crime, em seu preâmbulo, sendo eles “a confidencialidade, a integridade e a disponibilidade” (SYDOW, 2015, p. 71 e 72).

Ainda que o Brasil não participe desta convenção, estas características são importantes para a compreensão do que significa a segurança na rede.

### **3.1 A segurança na rede: Os seus elementos**

A confidencialidade é “a qualidade de um dado manter-se restrito a acessos alheios até que haja permissão para tanto, dada por alguém legitimado” (SYDOW, 2015, p. 72).

Portanto, trata-se do sigilo das informações encontradas nas diversas máquinas, as quais se pressupõem que o acesso é limitado, compreendendo-se que “o material informático como verdadeira propriedade de um indivíduo” (SYDOW, 2015, p. 71).

Apesar de o Brasil não ser signatário da Convenção de Budapeste, percebe-se facilmente que a legislação nacional adotou a confidencialidade dos dados, como é possível se perceber nos incisos II, III e IV do artigo 3º da Lei nº 12.965/14 como princípios e, também, como direitos assegurados aos usuários nos incisos I, II e III do artigo 7º da mesma lei.

Aos usuários da rede, então, garante-se que os dados por eles criados, armazenados e enviados são invioláveis, excepcionando-se tão somente na presença de ordem judicial.

A integridade, por sua vez, refere-se à “incolumidade de dados ou informações na origem, no trânsito ou no destino”, conforme o inciso VIII do artigo 4º da Lei nº 12.527/11, sendo que “é prerrogativa do usuário que seus dados existam na forma como foram criados, copiados ou armazenados” (SYDOW, 2015, p. 74).

Tanto há esta proteção pela legislação brasileira, que o artigo 154-A do Código Penal determina que a obtenção, adulteração ou destruição de dados sem autorização expressa ou tácita do titular é crime.

Por fim, temos a disponibilidade, que, conforme Sydow (2015, p. 75 e 76), é vital para a compreensão da segurança informática, tendo em vista que a ausência deste elemento tornaria obsoleta qualquer proteção aos anteriores, pois este compreende o acesso aos dados, isto é, “a possibilidade livre de o usuário utilizar-se de seus dados no momento em que desejar”.

Da mesma forma, o artigo 3º da Lei nº 12.965/14, resguarda tal proteção ao nível de princípio, tendo em vista a sua previsão no inciso V, dispondo pela “preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas” (BRASIL, 2014).

Estes elementos da segurança da rede podem ser inferidos no uso corrente da internet. O usuário deseja acessar certo conteúdo (disponibilidade) e o deseja por inteiro (integridade), sendo este acesso restrito àqueles que o indivíduo optar por compartilhar (confidencialidade).

### 3.2 O conceito de crimes cibernéticos

Os crimes cibernéticos ainda não encontraram uma classificação e um conceito comum entre os diversos doutrinadores e estudiosos que se debruçam sobre o tema, devendo-se notar a perspectiva de alguns deles.

De uma forma geral e genérica, Jesus (2016, p. 49) define o crime cibernético, ou informático, como “um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores”, sendo que a informática será “o bem ofendido ou o meio para a ofensa a bens já protegidos pelo Direito Penal”.

Wendt e Jorge (2013, p. 19) determinam que os crimes cibernéticos pertencem a uma categoria inserida dentro de “condutas indevidas praticadas por computador”, sendo que eles ainda se dividem em crimes cibernéticos abertos e exclusivamente cibernéticos, a depender da possibilidade de se cometer o crime somente com a “utilização de computadores ou de outros recursos tecnológicos que permitem o acesso à internet”. Ainda existem as condutas chamadas de “ações prejudiciais atípicas” que correspondem àquelas que causam “algum transtorno e/ou prejuízo para a vítima, mas não existe previsão penal”.

Para Sydow (2015, p. 88), por sua vez, os crimes cibernéticos, ou delitos informáticos, podem ser impróprios ou próprios, a depender do alvo da conduta, isto é, serão os primeiros caso o infrator apenas utilize o meio informático, ainda que outros meios fossem possíveis para a consecução do delito, enquanto que os próprios são os que “visam a atingir um sistema informático ou seus dados, precisamente violando sua confidencialidade, sua integridade ou sua disponibilidade”.

Apesar de aparentemente os conceitos serem diversos, há que se notar que a nomenclatura é o fator diferenciador entre eles. Veja-se que quando um crime só pode ser executado por meio virtual, tem-se que visa a atingir a rede ou algum dos elementos da segurança na rede. Enquanto isso, diante de um crime cibernético aberto ou de um crime informático impróprio, tem-se a utilização facultativa do aparato tecnológico.

Portanto, a diferença que há entre eles é tão somente metodológica, isto é, a perspectiva adotada para se compreender o crime. Questiona-se o uso exclusivo da tecnologia ou o bem que visa a atingir.

No entanto, há que se questionar em que se diferenciam os crimes cibernéticos dos demais delitos, principalmente qual o bem que eles efetivamente buscam proteger.

### **3.3 O bem jurídico em questão**

Como afirmado anteriormente, o direito penal tem como pressuposto a atuação somente em casos que ele seja imprescindível, isto é, quando a agressão é tamanha que justifique a repressão estatal. Para tanto, o Estado determina alguns bens como aqueles que justificam esta interferência, tendo em vista a sua relevância. Sobre este respeito Damásio de Jesus reputa:

De fato, é inegável que onde há relevância econômica deve haver relevância jurídica, e é esta a tutela que se apresenta, a proteção à incolumidade de informações, bancárias, financeiras, dentre outras informações geradas e tratadas por pessoas físicas e jurídicas. Sistemas informáticos processam ou tratam dados eletrônicos, geram significado e informações. Logo, são merecedores da tutela penal, pois informação é bem precioso (2016, p. 47 e 48).

Sendo assim, ainda conforme Jesus (2016, p. 48), tendo em vista a compreensão de que vivemos atualmente na sociedade da informação, houve a necessidade de se tutelar certos bens jurídicos, sendo eles “a informática, ou a privacidade e a integridade dos dados informáticos”.

Como se percebe, os elementos anteriormente apontados como pertencentes à segurança na rede também estão presentes quando falamos do bem jurídico que o Estado visa a tutelar. Com a intervenção estatal, visa-se a proteger a privacidade e a integridade dos dados, sendo que não teria qualquer sentido defender esta última se não houver disponibilidade.

Sydow (2015, p. 78) aponta que os bens jurídicos não podem ser percebidos tão somente na perspectiva individual, devendo-se notar a internet e as tecnologias como uma expressão dos bens jurídicos da generalidade, isto é, “servem a cada

cidadão em particular, mas são gerais por representarem avanço de toda uma coletividade”.

Este autor, então, passa a analisar o mundo virtual a partir da ótica de um meio ambiente artificial, aquele construído artificialmente pelo homem, concebendo-se usualmente o meio ambiente do trabalho. O intento dele era justamente compreender a segurança na rede, em todas as suas características, como um direito difuso, mostrando-se “merecedora de proteção penal, uma vez que, dependendo do grau, sua afetação leva prejuízo a toda a coletividade”, tendo em vista que “as conexões tecnológicas e a virtualidade configuram um verdadeiro meio ambiente” (SYDOW, p. 79).

Todavia, não é toda a conduta que se dirige à rede em si, devendo-se conceber, então, que nem toda lesão ocorrida no meio virtual é uma lesão ao bem jurídico difuso. Neste sentido, Sydow (2015, p. 86) afirma que “não se pode confundir o ataque a um bem jurídico difuso com um ataque maciço (e múltiplo) a bens jurídicos individuais graças à força propulsora da informática”. Ele ainda diz:

Os bens jurídicos já protegidos e que são lesados por meio do uso da tecnologia – como, por exemplo, a honra atacada por uma mensagem de texto remetida por celular – não merecerão nova roupagem, por já serem objeto de proteção. Mas as condutas praticadas merecem alternativas de agravamento, vez que praticadas por meio facilitador e com alta capacidade lesiva e, mais especialmente, por serem uma tendência da criminalidade (2015, p. 86).

Apesar de estes antigos valores não necessitarem de uma nova roupagem, a segurança da rede impõe uma nova visão quanto aos valores que devem ser preservados. Caso isso não seja feito, “permanece a ideia de que tais condutas em nada prejudicam a sociedade em qualquer segmento, sendo que, na realidade, transformam o ambiente informático, que é difuso em certos aspectos, em um ambiente inseguro” (SYDOW, 2015, p. 87 e 88).

Compreendido o bem que se visa a tutelar, devem-se entender alguns dos crimes cibernéticos tipificados em nosso Código Penal.

### **3.4 Crimes cibernéticos próprios tipificados no Brasil**

Com relação aos crimes cibernéticos, Martín dispõe que:

Brasil no cuenta con una legislación específica que castigue y sancione delitos informáticos, sin embargo el Código Penal contiene algunas disposiciones que tipifican y castigan conductas cometidas a través de sistemas de información y bases de datos pertenecientes a la administración pública<sup>62</sup> (2012)

Até então, em razão do advento da Lei nº 9.983/00, o Código Penal passou a prever alguns delitos que utilizam o aparato tecnológico para se concretizarem, mas eles se limitavam a proteger os dados que pertencentes à Administração Pública. Por este motivo, o autor mencionou apenas a existência destes delitos.

Após esta Lei, somente em 2012, com a edição das Leis nº 12.735 e 12.737, o Brasil passou a prever em seu ordenamento jurídico tipos que incriminassem condutas que utilizassem o meio virtual ou tivessem como intuito atingir algum bem jurídico vinculado a este ambiente.

Ainda que a Lei nº 12.735/12 seja breve, ela trouxe a possibilidade, ao se tratar de crime de racismo, que o Juiz determine, após ouvido o Ministério Público, “a cessação das respectivas transmissões radiofônicas televisivas, eletrônicas ou da publicação por qualquer meio” (BRASIL, 2012).

Além disso, esta Lei determinou no artigo 4º que “os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes, especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado” (BRASIL, 2012).

A Lei ainda pretendia modificar o Código Penal e o Código Penal Militar, mas os dispositivos que realizavam a modificação foram vetados.

A Lei nº 12.737/12 que realmente introduziu os crimes cibernéticos contra toda e qualquer pessoa, não somente em face da Administração Pública. Independente da motivação para a edição do normativo apelidado Lei Carolina Dieckmann, este representa uma evolução para a defesa dos interesses da sociedade no ambiente virtual.

Os crimes que o Código Penal passa a prever são os que seguem abaixo.

### *3.4.1 Invasão de dispositivo informático*

---

<sup>62</sup> Brasil não conta com legislação específica que castigue e sancione delitos informáticos, porém o Código Penal contém algumas disposições que tipificam e castigam condutas cometidas através de sistemas de informação e bases de dados pertencentes à Administração Pública.

Este crime vem tipificado no artigo 154-A do Código Penal, sendo ele integrado ao nosso ordenamento em virtude da lei mencionada acima. Este possui o intuito de criminalizar a conduta de invasão de dispositivo informático, uma novidade em relação ao direito penal clássico, devendo-se atentar ao seu teor:

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:  
Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa (BRASIL, 2012).

Primeiramente, o legislador optou por definir a invasão de dispositivo informático alheio como ilícita, gerando a dúvida quanto ao que esta abrange. No dizer de Jesus (2016, p. 86 e 87), dispositivo informático é “todo o dispositivo capaz de tratar informação, diga-se, armazenar ou processar dados”, enquanto que o acesso se configura por “qualquer interação de um indivíduo com um sistema informático”.

Ora, sendo o dispositivo informático qualquer dispositivo capaz de usar a informação, nota-se que temos uma definição deveras abrangente, admitindo diversos tipos, incluindo *software*, pelo qual se pode processar a informação.

Para Sydow (2015, p. 298), por outro lado, dispositivo informático é um conceito mais restrito, pois, na realidade, se refere a “qualquer *hardware* que trabalhe com o trato automático de informações e possua em si capacidade de armazenamento de dados confidenciais”, excluindo-se, desta forma “contas em serviços exclusivamente on-line (por ausência de suporte/dispositivo), *softwares* (bens imateriais)”, assim como aparelhos que não possuam como função específica o uso no direito informático e que seus dados não sejam resguardados pelo sigilo, como seria o caso do relógio digital.

Veja-se que esta segunda postura prejudica os usuários. Adotando-se a posição do Damásio de Jesus, tem-se que todas as informações agregadas a estes dispositivos são protegidas, desde que estes sejam capazes de armazenar ou processar os dados. Por outro lado, exige-se que sejam *hardwares*, mas há que se notar que, por exemplo, o serviço exclusivamente on-line depende de um *hardware*,

pois ele não simplesmente existe na internet, isto é, ele depende de um algum aparato que o possibilite funcionar e fornecer o serviço a que se propõe. Portanto, o crime poderia alcançar esta circunstância, pois, ainda que se exija a presença de *hardware*, ele é necessário para o funcionamento de qualquer serviço da internet.

O mesmo raciocínio se utiliza com relação ao *software*, já que este não poderá funcionar de forma isolada, sem ter algum *hardware* para lhe dar o suporte.

Na realidade, a dificuldade que se percebe com relação ao dispositivo informático é com relação àqueles que não apresentam mecanismo de segurança. Na visão de Damásio de Jesus (2016, p. 88), este deve ser considerado “uma barreira entre o invasor e os dados ou informações armazenadas ou contidas no dispositivo”, enquanto que para Sydow (2015, p. 300), mecanismos de segurança “são todos aqueles que têm como finalidade evitar o acesso de terceiro não legítimo”, assim como “garantir autenticidade do detentor legítimo de acesso”.

Desta forma, Jesus (2016, p. 88) está correto ao notar que o *pendrive* não está protegido, pois, usualmente, ele não apresenta qualquer mecanismo para impedir o acesso de terceiros. Portanto, inexistindo mecanismo de segurança, não haverá a incidência do tipo.

Outro empecilho à aplicação deste tipo se verifica com o dolo específico exigido, tendo em vista que requer “o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita” (BRASIL, 2012).

A dificuldade que se pode esbarrar é justamente com relação à visão de Sydow (2015, p. 299), que determina que o “objetivo seja ulterior ao desafio do ingresso não autorizado e, destarte, objetive dados específicos”, da mesma forma que “mudanças em arquivos ocorridas com a mera finalidade de ingresso no sistema, por si sós, não bastam para a caracterização do delito por serem meramente meio, e não finalidade do agente”. Sydow fecha o seu pensamento afirmando que o legislador não pretendeu criminalizar o mero acesso sem autorização e sem finalidade específica, devendo-se buscar ou a finalidade do agente no sentido de obter dados ou obter alguma vantagem.

Damásio de Jesus (2016, p. 90), inclusive, alerta que “é impossível acessar um dispositivo informático sem obter dados, por mais inúteis e imprestáveis que possam parecer” e é possível se questionar sobre a pretensão de um indivíduo em

acessar um dispositivo alheio ao seu, mediante a violação indevida de mecanismo de segurança.

A dificuldade também se encontra com relação ao sujeito passivo do crime, pois o artigo é explícito com relação à autorização expressa ou tácita do titular do dispositivo. Veja-se que esta norma “ignorou a existência de quaisquer outros sujeitos além do titular do dispositivo” (SYDOW, 2015, p. 304), ainda que diversas pessoas tenham acesso àquele computador, por exemplo.

Sydow alerta que, ainda que o titular possa ser apenas um, várias pessoas poderão fazer uso daquela máquina e possuírem diversas contas, com documentos e pastas particulares, o que poderia gerar uma situação em que, por exemplo, o titular anuisse com o acesso ao dispositivo, independente do real proprietário das outras informações que nele estão presentes.

Como se percebe, a tipificação deste delito acabou por gerar mais dúvidas do que trazer respostas, mas, como já se afirmou anteriormente, ao menos é um passo em busca da criminalização de atos ocorridos em meio virtual em busca de reprimir condutas lesivas no ambiente virtual.

De qualquer forma, tendo em vista a norma penal em questão, há que se questionar se este se trata de um crime material ou formal, isto é, se este requer a obtenção de resultado, eis que isto influencia diretamente com relação ao local do crime, que nos auxiliará posteriormente.

Assim como os outros pontos apresentados acima, a categorização deste crime quanto a esta questão é também polêmica. Nota-se que, apesar de Sydow não ser explícito quanto a isso, ao considerar que a mera invasão não pode ser considerada crime, compreende-se que se exige a obtenção de um resultado e, conseqüentemente, há que se falar em crime material.

No entanto, Damásio de Jesus (2016, p. 93) entende que se trata de um crime formal, tendo em vista que “muito embora o tipo traga qual deve ser a finalidade do agente na invasão, não exige que tal finalidade seja atingida para a consumação”, sendo suficiente a invasão para a caracterização do crime.

O §1º do artigo 154-A do Código Penal traz uma figura equiparada, criminalizando a produção, a distribuição, a venda, a difusão ou o oferecimento de produtos ou dispositivos que permitam a prática dos crimes apontados no *caput*.

O §2º deste mesmo artigo, por sua vez, trouxe uma causa de aumento referente ao prejuízo econômico da vítima, considerada questionável por Sydow em razão de sua abrangência, sendo demasiadamente genérica.

De acordo com o autor (2015, p. 311), deveria se adotar um parâmetro objeto para a aplicação desta causa de aumento, tendo em vista que o prejuízo econômico genérico sempre existirá, tendo em vista o “tempo dedicado ao inquérito, ao processo, seja pela contratação de um suporte técnico, pela compra de um antivírus etc”.

O §3º traz a forma qualificada do tipo, que se caracteriza pela obtenção de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, ou o controle remoto não autorizado do dispositivo.

Há que se notar que este não se confunde com o artigo 10 da Lei nº 9.296/96, pois esse tem como núcleo a interceptação, de forma diversa deste, que prevê a obtenção mediante o acesso não autorizado.

O §4º apresenta uma causa de aumento específica para a forma qualificada na eventualidade de estas informações obtidas, referidas no §3º, serem divulgadas, comercializadas ou transmitidas a terceiros, aumentando-se a pena de um a dois terços.

Por fim, o §5º prevê uma causa de aumento em razão da qualidade da vítima, aumentando-se a pena de um terço à metade no caso de o titular do dispositivo informático ser o Presidente da República, Governador de Estado, Prefeito, Presidente do STF, Presidente da respectiva Casa Legislativa ou dirigente máximo de administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Há que se notar, também, que o artigo 154-B do Código Penal, também acrescido em razão da Lei nº 12.737/12, estabelece que o crime somente se procede mediante representação, a não ser que ocorra contra a Administração Pública, direta ou indireta, de qualquer dos entes federados.

#### *3.4.2 Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública*

A Lei nº 12.737/12 acresceu os §§ 1º e 2º do artigo 266 do Código Penal, tipificando a conduta de interromper “serviço telemático ou de informação de

utilidade pública, ou impede ou dificulta-lhe o reestabelecimento” (BRASIL, 2012) e prevê um causa de aumento de pena no caso de o crime ser cometido em situação de calamidade pública, aplicando-se a pena em dobro.

Anteriormente, o *caput* do artigo 266 do Código Penal não fazia qualquer referência ao serviço informático, telemático ou de informação de utilidade pública, razão pela qual a referida Lei adicionou os referidos parágrafos acima referidos, garantindo a continuidade da prestação destes serviços.

Damásio de Jesus (2016, p. 111) alerta que esta norma penal possui “por escopo o funcionamento do serviço de comunicação, considerado em seu conjunto geral, no interesse coletivo e não individual”. Outro não poderia ser o entendimento, tendo em vista que o presente delito possui sua previsão no Título VIII do Código Penal, referente aos Crimes contra a Incolumidade Pública.

O mesmo autor (2016, p. 113) nota que, quanto ao resultado, trata-se de “crime material, exigindo para sua consumação o resultado previsto no tipo”.

### 3.4.3 Falsificação de cartão

Por fim, a Lei nº 12.737/12 incluiu o atual parágrafo único do artigo 298 do Código Penal, equiparando à figura do documento particular o cartão de crédito e de débito.

Em que pese a Lei busque tratar sobre os delitos cibernéticos, tal delito acabou por se distinguir dos demais justamente por não se enquadrar a estes.

Ao se pensar em crimes cibernéticos em que haja a utilização de cartões de crédito e de débito, normalmente a atenção se volta ao uso de senhas alheias para realizar saques ou compras pela própria internet, o que este artigo não protege.

Os crimes descritos acima são chamados de *phishing scam* e, conforme Damásio de Jesus (2016, p. 119 e 120), este delito veio para criminalizar a “clonagem física” de cartões, sendo que o intuito do infrator será determinante para a definição do crime, tendo em vista que os saques ensejam a qualificação do furto mediante fraude, enquanto que na hipótese de o agente realizar compras teremos a configuração do crime de estelionato.

## 3.5 Os crimes cibernéticos impróprios no Brasil

Como é possível perceber acima, os crimes cibernéticos próprios ainda são escassos no Brasil, mas isso não impossibilita a criminalização de certas condutas que se concretizam no ambiente virtual, pois eles apenas se apresentam como um novo meio para a realização de um crime.

Alguns exemplos que podem ser citados são os crimes contra a honra, pedofilia, estelionato, furto, ameaça, entre outros.

### **3.6 Os crimes cibernéticos e a jurisdição brasileira**

Em vista do estudo realizado acima, é possível se chegar às conclusões a seguir, que, em parte, representam um desafio a ser superado.

Primeiramente, compreendemos como a internet funciona, em sua maior parte, demonstrando que, apesar de possuir esta aparência etérea, na realidade, a internet é formada por diversas redes conectadas que possibilitam a comunicação entre as mais diversas máquinas.

Além disso, as máquinas que realizam as comunicações entre si podem ser qualificadas como servidores ou clientes, a depender do que foi estabelecido na conversa entre estes usuários. Portanto, nota-se que há algumas máquinas que são montadas justamente para fornecer um serviço, sendo elas os servidores, e aqueles que requisitam os seus conteúdos os clientes.

A partir deste momento temos o vislumbre da camada de aplicação, sendo ela a que permite a interação do usuário final com o serviço prestado por algum provedor de conteúdo. É aqui, inclusive, que podemos ter a maior parte dos crimes cibernéticos.

A seguir, nota-se que a jurisdição deixou de se apresentar conforme aquela fórmula clássica de lide e da atuação da vontade concreta da lei. A jurisdição atingiu o patamar de meio de tutela dos direitos fundamentais dos indivíduos, que deve ser realizado por meio da reconstrução da ordem jurídica, utilizando-se como base a necessidade do direito material.

Posteriormente, teceu-se a noção de que a nossa jurisdição é determinada, em matéria penal, conforme a territorialidade, aplicando-se a normal penal brasileira a casos que ocorrem no exterior tão somente em casos excepcionados por lei.

Compreendendo a jurisdição, passou-se à discussão com relação ao âmbito virtual, se seria possível a sua aplicação diante deste novo ambiente, e chegou-se à conclusão de que, apesar de sua aparência novel, há que se perceber que a não aplicação da ordem jurídica estatal acabaria por obstar a defesa dos direitos dos diversos indivíduos que participam das comunidades virtuais.

Na realidade, a utilização conforme a legislação atual, apesar de não ser a resposta mais eficiente e querida pela sociedade, tem-se como a única que possuímos no momento, não podendo o Estado se abster do seu dever de regular as relações entre os diversos particulares.

Por fim, no presente capítulo, notamos que os crimes cibernéticos ainda representam um estudo muito recente, eis que a Lei de maior representação desta categoria penal apenas foi editada em 2012, muitos anos após a introdução do meio virtual no cotidiano dos brasileiros.

Determinou-se que não se tratam apenas os bens jurídicos individuais, mas também coletivos, da sociedade em geral, etc.

Portanto, chega-se ao questionamento se todo e qualquer crime cibernético que ocorra, que possua como vítima um residente no território brasileiro, será protegido pelo nosso ordenamento jurídico.

Como qualquer outra categoria de crimes, existem os crimes que são materiais e os formais, tendo esta categoria influência direta para o momento da consumação e, por consequência, o local do crime. Diante do primeiro caso, importará tanto o local da conduta quanto o do resultado, enquanto que, no outro, este último será desconsiderado, pois sequer é necessário para a consumação do delito.

Desta forma, devemos nos ater a crimes específicos para compreendermos como eles lidam com a questão da territorialidade.

Primeiramente, diante de um crime de injúria, tem-se que a consumação ocorre “no momento em que a vítima toma ciência do teor do diálogo ultrajante” (ZANIOLO, 2016, p. 63).

Considerando esta informação, independente de onde os dois usuários estiverem, o infrator e o ofendido, assim como o servidor, o crime só se realizará com a ciência do crime, isto é, é um delito essencialmente material, exigindo-se que

haja a produção de um resultado que só poderá ocorrer com o conhecimento da vítima.

Veja-se, de nada adianta tentar ferir a honra de alguém, diretamente, sem que ela tenha ciência de que isso está ocorrendo, tornando-se um elemento lógico anterior à qualificação do crime.

Neste sentido, verifica-se que o crime de injúria não sofre qualquer prejuízo com relação às regras de territorialidade e extraterritorialidade brasileiras.

Por sua vez, a Lei nº 7.716/89 prevê o crime de racismo no seu artigo 20, que dispõe: “praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional” (BRASIL, 1989).

Considerando que um sítio eletrônico disponibilize diversas informações que tenham como intuito a disseminação do racismo, conforme Zaniolo (2016, p. 65), o local do crime é aquele “de onde partiram as manifestações tidas por racistas”.

Sendo assim, estando o sítio hospedado em um servidor no Brasil, este poderá exercer a sua jurisdição sobre o infrator, sem qualquer dúvida. Todavia, estando o sítio hospedado em outro território, como na Hungria, por exemplo, ainda que existissem diversos ofendidos no primeiro país, ele não poderia exercer a sua jurisdição.

A razão de ser desta distinção é muito simples. Trata-se, o racismo, de um crime de mera conduta, isto é, considera-se consumado tão somente com o adimplemento das elementares do tipo e, por esta razão, no momento em que a informação considerada racista é veiculada na internet, ele já se encontra consumado, independente do resultado que venha a causar.

Há outra razão para isso também. Conforme assinalado anteriormente, a internet não se encontra tão destacada do meio físico como diversos autores afirmam e o documento da internet se encontra armazenado em algum local.

Sendo assim, apesar de o acesso ser mundial, o documento ainda se encontra naquele servidor em específico, local em que a prática do racismo ocorre e, como efeito secundário, acaba afetando diversas outras pessoas.

Em face de outro crime, como o de estelionato, por exemplo, poderemos ter a situação a seguir.

Na hipótese de um sítio qualquer na internet apresentar diversos produtos para a compra de qualquer local do mundo, inclusive apresentando diversos

idiomas, além da promessa de um bom preço e a entrega em prazo razoável, um usuário brasileiro adiciona ao seu carrinho virtual diversos objetos, fornecendo, ao final, os números referentes ao seu cartão de crédito.

Caso o servidor e o infrator estejam presentes no território nacional, não há dúvida de que a jurisdição brasileira é a competente para a persecução penal. No entanto, devemos notar as repercussões no caso de eles estarem em localidades diferentes.

Primeiramente, a consumação do crime de estelionato ocorre com a obtenção da vantagem ilícita em prejuízo da vítima. Neste caso, para que isso ocorra, o ofensor deverá receber aquela vantagem.

Quando tratamos de uma situação comum, fora do meio virtual, a obtenção da vantagem é, usualmente, concomitante ao método utilizado pelo agente para incidir a vítima em erro. Na internet é diferente, eis que é possível, como neste caso, que o infrator simplesmente forneça a todo e qualquer usuário a fraude.

Sendo assim, considerando que a obtenção da vantagem é necessária para a consumação, reconhece-se que o crime é material, possibilitando que o local do resultado seja considerado para a determinação do local do crime.

Neste sentido, considerando que o infrator está em um país diverso, como a Argentina, estando o servidor no Brasil, há que se questionar se ele obtém ou não a vantagem.

Veja-se que certamente o infrator tem à sua disponibilidade a informação que ele deseja, que são os dados do cartão de crédito, mas ele não os possui diretamente com ele. Caso, por exemplo, o sítio deixe de funcionar por algum motivo, como o reconhecimento de que se trata de um utensílio para o crime, nota-se que ele não poderá mais ter acesso àquela informação.

Entretanto, como seria costumeiro, o servidor poderá enviar todas as informações percebidas para outra máquina, assim que as receber. Desta forma, percebe-se que o crime realmente só se consuma com o recebimento efetivo destas informações, considerando que o servidor não significa a obtenção da vantagem, sendo este apenas um utensílio ou um mecanismo para a obtenção.

Portanto, o local de interesse é justamente em que o infrator está, isto é, neste caso, estando ele na Argentina, por exemplo, o local da consumação seria este. Entretanto, como o servidor se encontra no Brasil, a sua ação de dispor o meio

fraudulento na internet só se torna possível pelo armazenamento do seu sítio neste Estado e, dessa forma, não poderá ser excluído como local do crime, concebendo-se a jurisdição brasileira como competente.

Por outro lado, em face de um autor de uma nacionalidade diversa da brasileira, no seu respectivo território, e um servidor em qualquer outro país, tem-se que o Brasil não poderia exercer a sua jurisdição, tendo em vista que a atividade e o resultado apenas se realizam no território de outro Estado.

Tanto as regras da territorialidade como da extraterritorialidade penal não são suficientes para abarcar tais casos, pois aqui não se adota o princípio da nacionalidade passiva.

Ainda que tal perspectiva possa parecer absurda, ela só subsiste numa consideração superficial. Veja-se que, a depender das informações propagadas em um sítio, vários poderão ser os ofendidos em diversas localidades do mundo, criando uma situação já apontada anteriormente, qual seja o conflito positivo de jurisdição de diversos países. Há que se questionar se esta conduta é a adequada.

O ponto principal que se tem que ter em mente, com relação aos delitos em geral, não são somente os cibernéticos, é que, na definição da jurisdição e competência, há que se prezar pela sua executividade. Afinal, pergunta-se a finalidade de se realizar um processo custoso e demorado para definir a materialidade e a autoria de um crime em um território estranho sem qualquer perspectiva de o condenado sofrer as suas devidas represálias.

O próprio Código Penal, na realidade, compreende esta circunstância, apenas concebendo a hipótese de extraterritorialidade de forma restrita, ainda que admita a chamada incondicionada, em que, independente da questão ter sido julgada noutro território, ela não será levada em consideração em razão da particularidade das pessoas a que se pretende proteger ou por se tratar de um genocídio, conforme o inciso I do artigo 7º deste códex.

Note-se, inclusive, que a alínea que se refere ao genocídio apenas possibilita que a matéria seja julgada no Brasil se o agente for brasileiro ou tenha domicílio neste território, demonstrando o mínimo de interesse necessário para que a jurisdição possa ser exercida.

Por outro lado, a única adoção do princípio da nacionalidade passiva no nosso Código Penal está nas alíneas 'a' a 'c' do inciso I do artigo 7º, em que, nestes

casos específicos, o que se pretende, na realidade, é preservar a soberania e este aparece como real limitador do exercício do puniendi.

Este se torna o ponto principal quando se questiona a atuação do Estado perante os seus jurisdicionados quando o crime, apesar de atingi-los, não pode ser conhecido no Poder Judiciário local. Justamente, sendo a soberania uma condição para o reconhecimento dos Estados, assim como um delimitador da atuação de uns sobre os outros, tem-se que o Brasil, por exemplo, não teria como ensejar a execução de uma sentença sua, por si só, perante outro Estado.

Isto, no entanto, não significa que os ofendidos estão desprotegidos ou que o Estado deve se manter na inércia. Na realidade, pelo contrário, desenvolveu-se o raciocínio de que a jurisdição, além de uma forma de reconstrução da ordem jurídica, é um meio de tutela dos direitos fundamentais, sendo este, afinal, um dos maiores deveres do próprio Estado, não apenas na sua expressão jurisdicional.

A defesa dos direitos fundamentais não ocorre tão somente quando o Judiciário disponibiliza a quem se interessar o aparato para que este possa pleitear os seus direitos perante um terceiro imparcial.

Esta visão seria extremamente restritiva e não teria qualquer sentido no Estado de Direito que vivemos hoje. Não só a expressão jurisdicional, mas também a executiva e a legislativa devem realizar a tutela dos direitos fundamentais, de acordo com as suas respectivas atividades.

Portanto, cabe ao Estado garantir que os direitos fundamentais sejam devidamente protegidos e, caso não seja possível, que ocorra a efetiva repulsa com relação ao violador.

Direcionando essa discussão ao tema, tem-se que a sociedade exige, cada vez mais, a certeza de que poderá acessar a internet de forma tranquila, pois o uso deste instrumento está crescendo.

Compreendendo-se que os usuários cada vez mais buscam a segurança na rede, que foram definidos, conforme a Convenção de Budapeste, como a confidencialidade, a integridade e a disponibilidade, sendo estes extremamente importantes para os usuários, o legislativo não se manteve de todo inerte, editando a Lei nº 12.965/14, a Lei do Marco Civil da Internet, em que há um capítulo específico para definir os direitos e garantias dos usuários.

Como foi visto anteriormente, ainda que o Brasil não participe da Convenção supracitada, há que se notar que os direitos assegurados por esta Lei, de certa forma, abordam os elementos básicos da segurança esperada no ambiente virtual.

Portanto, o Brasil deve assegurar que esses direitos sejam preservados e defendidos no ambiente virtual, chegando-se a questionar como seria possível fazer isso.

À primeira vista, seria interessante um esforço internacional no sentido de uniformizar a legislação relativa aos crimes cibernéticos, impossibilitando os refúgios por parte dos diversos agentes, além de possibilitar a maior segurança na rede.

Entretanto, trata-se de uma visão utópica, pois não se trata apenas de um desejo comum de repulsa aos delitos cibernéticos, mas é a tentativa de realizar a junção de diversas culturas e pensamentos num objetivo único que não necessariamente é perseguido por todos. Esta perspectiva se torna clara quando notamos a influência da cultura sobre a definição do que seria ou não crime, sendo possível, inclusive, a noção de que os fatos ocorridos por meio virtual não são merecedores de qualquer tipo de tutela, pois a sociedade em questão não o utiliza de forma demasiada, apenas gerando um encargo ainda maior para aquele Estado.

Esta não é a única dificuldade, conforme Berman explica:

*Both of these attempts at international harmonization reveal the principal drawback of attempting to establish international norms through multilateral treaties. Almost by definition, these treaties will demand prior consensus among many countries with different social policies and economic interests. Thus, the treaties will tend merely to codify painstakingly developed conventional wisdom about recognized problems. As a result, such treaties are rarely the best mechanism for developing new solutions to emerging issues on which there are widely divergent traditions and interests [...]. Accordingly, the classical model of public international lawmaking may not be the appropriate mechanism for achieving international harmonization in a fast-changing world<sup>63</sup> (2002)*

---

<sup>63</sup> Ambas as tentativas (refere-se às Convenções de Berne e Hague) de uma harmonização internacional revelam a principal desvantagem de uma tentativa de estabelecer normas internacionais por meio de tratados multilaterais. Quase por definição, estes tratados demandarão um consenso anterior entre os vários países com diferentes políticas sociais e interesses econômicos. Portanto, os tratados tenderão a meramente codificar o conhecimento convencional já meticulosamente desenvolvido sobre problemas reconhecidos. Como resultado, estes tratados são raramente o melhor mecanismo para desenvolver novas soluções para problemas emergentes em que há uma grande divergência de tradições e interesses (...). Por consequência, o clássico modelo de criação de leis internacional talvez não seja o mecanismo mais apropriado para atingir a harmonização internacional em um mundo que muda tão rápido (tradução livre).

Desta forma, diante de um mundo que tanto muda, que é o virtual, a legislação internacional seria, na realidade, um empecilho para a defesa dos interesses dos usuários, eis que, quando da ratificação do tratado, provavelmente, os agentes delitivos já teriam encontrado outra forma de atingir os bens jurídicos alheios.

A intenção, afinal, é boa, e pode ser suficiente para alguns casos. A uniformização seria a peça chave para impedir que existissem desacordos entre os diversos países com relação à quais atos devem ser concebidos como crimes. Entretanto, Berman (2002) refuta a necessidade de um ato legislativo internacional ao colocar que, usualmente, as convenções só ditam aquele conhecimento que já é aceito de forma comum, isto é, apenas diz o que os países já concordam, não gerando real eficácia.

Porém, os tratados não são a única forma de relação entre os Estados, existindo também a Cooperação Jurídica Internacional.

## 4 COOPERAÇÃO JURÍDICA INTERNACIONAL

Conforme visto anteriormente, a cooperação jurídica internacional se torna a resposta não só para os crimes cibernéticos, mas toda situação em que o Estado se vê impossibilitado de exercer a sua soberania, tendo em vista que ela se encontra em conflito com outra.

Tal instituto existe, conforme Milton Fornazari Junior (2016, p. 15), “desde o surgimento das fronteiras dos Estados”, sendo que os seus instrumentos foram se desenvolvendo ao decorrer do tempo.

Ainda conforme Fornazari Junior, ao mesmo tempo em que as tecnologias avançavam, principalmente de transporte, indivíduos conseguiam se utilizar desta facilidade de circulação para tentar se furtar da atividade punitiva de outro Estado, apresentando-se a cooperação como meio para garantir a aplicação da lei de um determinado Ente Estatal quando for pertinente.

A situação não é diferente hoje. A tecnologia possibilita o alcance de situações antes não previstas e, por consequência, o direito deve se adaptar. A possibilidade de se atingir atos praticados em território estranho ao do próprio Estado impede que atos criminosos fiquem impunes e impossibilite a criação de verdadeiros paraísos, em que o indivíduo poderia simplesmente se esconder.

O ambiente virtual, em razão de sua conectividade, possibilita a transgressão de diversas fronteiras em qualquer local do mundo e isso, definitivamente, é um desafio para o direito como um todo. No entanto, a existência de uma harmonia entre os diversos países, não somente com relação a elementos normativos, torna possível um ambiente mais seguro, seja ele o real ou o virtual, tendo em vista que os Estados irão contribuir uns com os outros no intuito de reprimir atividades ilícitas.

Nádia de Araújo (2014, p. 30), abordando a importância da cooperação jurídica internacional para o Estado brasileiro no Manual de Cooperação Jurídica Internacional e Recuperação de Ativos, reflete que, na realidade, não se deve ter em mente a perspectiva do Estado, isto é, a preocupação deste com a governabilidade e com a manutenção de suas relações internacionais, mas também há que se ter em conta a perspectiva ex parte Populi, “a dos que estão submetidos ao poder, e cuja preocupação é a liberdade, e tendo como conquista os direitos humanos”. Neste sentir, ela aduz:

Além disso, como pano de fundo da cooperação jurídica internacional, está presente a questão do respeito aos direitos humanos e direitos fundamentais do indivíduo, ponto axial de todo o ordenamento jurídico brasileiro, especialmente depois da proeminência que lhe foi dada pela Constituição de 1988 (2014, p.30)

Esta noção é justamente o que se trabalhou com relação à compreensão atual de jurisdição e o dever do Estado de assegurar a tutela dos direitos fundamentais. Ora, o ente estatal não deve se voltar à atuação internacional tão somente em razão de fazer valer a sua lei, mas sim também para preservar o interesse daqueles que estão em seu território, “mas cujas necessidades têm reflexos internacionais” (ARAUJO, 2014, p. 31).

No mesmo tom, Ricardo Andrade Saadi e Camila Colares Bezerra, que também escreveram um capítulo no Manual de Cooperação Jurídica Internacional e Recuperação de Ativos, apresentam a importância que este instituto tomou para os diversos Estados, como se vê abaixo:

Mudam-se os paradigmas, a cooperação jurídica internacional deixa de ser exclusivamente um ato de cortesia entre os Estados e, se antes podia ser vista como uma ameaça à soberania, hoje se apresenta como essencial à sua própria manutenção. Mais que isso, se antes a cooperação internacional se justificava somente pela necessidade de contribuir com a paz e o progresso da humanidade, atualmente o próprio exercício das funções soberanas por parte dos Estados depende vitalmente da ajuda internacional. A garantia dos direitos individuais, coletivos e difusos, a manutenção da segurança pública, o combate ao crime organizado, a estabilidade do sistema econômico-financeiro, e tantos outros temas a cargo dos Estados dependem cada vez mais da cooperação jurídica internacional (2014, p. 20).

Desta forma, os Estados encontraram uma forma amigável de se relacionarem, de modo que eles prestem assistência uns aos outros com relação, “sem que para isso tenha que empregar o uso da força contra outro Estado soberano” (FORZANARI JUNIOR, 2016, p. 15), estreitando as relações entre os entes soberanos, assim como resguardando o interesse dos particulares que se submetem a estes.

Diante desta breve introdução, devemos compreender melhor o que é a cooperação jurídica internacional, quais os seus instrumentos e como ela contribuiria

para o caso específico retratado neste trabalho, isto é, os crimes cibernéticos ocorridos em território diverso do da vítima.

#### **4.1 O conceito de cooperação jurídica internacional**

Com relação ao conceito de cooperação jurídica internacional, Nádía de Araújo (2016) definiu-a, em sentido amplo, como “o intercâmbio internacional para o cumprimento extraterritorial de medidas processuais provenientes do Judiciário de um Estado estrangeiro”, sendo que é possível se observar “um aumento da cooperação jurídica entre entes administrativos, mediante uma nova modalidade de cooperação, a assistência direta ou auxílio direto”.

Esta última colocação se torna relevante, tendo em vista que há que se ressaltar, conforme Fábio Ramazzini Bechara (2011), que existe “também a cooperação administrativa, entre órgãos investigatórios, que igualmente produzem efeitos jurídicos”, considerando-se que chamar a cooperação de jurídica se reputa mais em razão dos seus “efeitos que desta possam advir do que propriamente à natureza do objeto da cooperação ou à qualidade de quem coopera”.

Importante destacar um trecho do livro de Milton Fornazari Junior, que diz:

A prática do referido ato deve estar relacionada diretamente, mas de maneira incidental e acessória a uma investigação criminal (fase pré-processual), ou a um processo penal, ou ainda, vinculado à execução da pena (nesta hipótese, apenas na transferência de presos e condenados e na extradição), em observância ao devido processo legal (2016, p. 13).

Portanto, nota-se que a postura adotada por Nádía de Araújo se apresenta, de certa forma, restritiva à desenvoltura que a cooperação jurídica internacional tomou com o tempo.

De qualquer forma, Fornazari Junior (2016, p. 14) ressalta que são modalidades tradicionais da cooperação internacional a extradição, a homologação de sentença penal estrangeira e as cartas rogatórias, enquanto que são novas modalidades a transferência de presos e condenados e o auxílio direto. Realizada a conceituação, passamos a estas modalidades.

#### **4.2 Extradição**

A extradição como é hoje, na visão de Denise Neves Abade (2013, p. 48), só pode ser compreendida à luz de sua origem e como se desenvolveu posteriormente. Note-se que, primeiramente, “o instituto era nada mais do que consequência de acordos celebrados entre reis para servir de instrumento de punição contra seus inimigos pessoais”. Ela só teria se desenvolvido em 1765, no acordo entre Carlos III da Espanha e Luís XV da França, pois se ampliou a abrangência com a “entrega de condenados pelos crimes comuns mais graves”.

Ainda conforme esta autora (ABADE, 2013, p. 48) nota-se que, “com o advento do liberalismo e sob a influência do Iluminismo e da Revolução francesa”, a extradição tomou novas proporções, consagrando-se como modalidade de cooperação para o combate de crimes comuns. Além disso, o Constitucionalismo andava a passos largos, impondo limitações à atuação estatal. Neste contexto, as fronteiras passaram a significar cada vez menos, considerando que elas não eram suficientes “para conter nem a internacionalização do trabalho, nem a internacionalização do capital”, exigindo-se que o Estado adotasse uma alternativa para que “sua política criminal repressiva pudesse ser efetiva”.

Sendo assim, ainda no dizer de Abade (2013, p. 50), a extradição se desenvolveu, ainda com a marca de sua origem, tendo em vista que não se admite a extradição por crime político ou de opinião, assim como se impediu a fuga dos criminosos para outros territórios. Neste sentir, pode se definir a extradição como uma modalidade que objetiva “a entrega de indivíduo para determinado Estado solicitante, para fins de submissão a processo penal ou à execução de pena criminal”.

Para Hildebrando Accioly (2011, p. 539), por sua vez, tem-se que não se trata de qualquer crime, mas sim aquele que possua “certa gravidade”, assim como o Estado que realiza a extradição deve “haver-se certificado de que os direitos humanos do extraditando serão garantidos”. Portanto, nota-se que o principal objetivo deste instituto é justamente “evitar, mediante a cooperação internacional, que um indivíduo deixe de pagar pelas consequências de crime cometido”.

Compreende-se a possibilidade de a extradição ser ativa quando o “Brasil é o Estado requerente”, sendo ela “apresentada diretamente pelo Poder Executivo da União ao Estado requerido, observadas as cláusulas de tratado que eventualmente

o Brasil tiver firmado com o Estado requerido”, ou, na ausência destas, com base nos princípios da “cortesia e da reciprocidade” (FORNAZARI JUNIOR, 2016, p. 24). Enquanto isso, a passiva representa o contrário, isto é, quando o Estado estrangeiro realiza o requerimento para o brasileiro, seja com base no tratado estabelecido entre eles ou nestes princípios.

Como fontes do instituto temos, de acordo com Accioly (2011, p. 539), os tratados bilaterais ou multilaterais, sendo exemplos destes na América Latina a Convenção de Direito Internacional Privado de 1928, também conhecido como Código Bustamante, esta que foi posteriormente modificada pela Convenção sobre Extradicação de 1932 e o Tratado de Direito Penal Internacional de 1940. Com relação à legislação interna, a Constituição Federal de 1988 aborda o tema nos incisos LI e LII do artigo 5º, assim como a Lei nº 6.815/80 e o Decreto nº 86.715/81.

A Constituição Federal de 1988 restringe a extradicação no caso de se tratar de um brasileiro nato e, caso ele seja naturalizado, poderá ocorrer se o crime for comum e praticado antes de ocorrer a naturalização, ou se houver envolvimento com o tráfico ilícito de entorpecentes e drogas afins, conforme a lei, assim como não permite a extradicação de estrangeiro em razão de crime político ou de opinião.

Há que se notar, entretanto, que o §3º do artigo 77 da Lei nº 6.815/80 que, na apreciação realizada pela Corte Suprema, os crimes contra os Chefes de Estado ou autoridades, assim como atos de “anarquismo, terrorismo, sabotagem, sequestro de pessoa, ou que importem propaganda de guerra ou de processos violentos para subverter a ordem política ou social” (BRASIL, 1980), podem não ser considerados como crimes políticos.

Este mesmo artigo aborda, em seu *caput*, as hipóteses em que a extradicação não é admitida, sendo elas, além das previstas constitucionalmente: O fato não configurar crime no Brasil ou no Estado que fizer o requerimento, o Brasil possui competência para ele mesmo julgar o crime imputado, a pena do crime em questão for igual ou menor a um ano, o Brasil já estiver processando ou já tenha condenado ou absolvido o extraditando sobre o fato, o fato já tiver a sua punibilidade extinta pela prescrição de acordo com a lei brasileira ou do Estado requerente e se o extraditando tiver que responder perante um Tribunal ou Juízo de exceção.

O artigo 91 da Lei nº 6.815/80 ainda exige que o Estado assuma o compromisso de o extraditando não ser processado ou preso por fatos anteriores ao

pedido, de o tempo de prisão no Brasil ser computado, de haver a comutação da pena privativa de liberdade a pena corporal ou de morte, ressalvando-se, quanto a última, os casos em que a lei brasileira permite a sua aplicação, não entregar o extraditando a outro Estado sem o consentimento do Brasil e a impossibilidade de se considerar o motivo político para agravar a pena.

O artigo 78, da mesma lei, ainda define as condições para que a extradição seja concedida, requerendo-se que o crime tenha sido cometido no território do Estado que fez o requerimento ou esteja sob sua jurisdição em virtude das suas leis penais e que exista sentença final ou decisão que autorize a autoridade competente a realizar a prisão do indivíduo, excetuando-se apenas a prisão cautelar.

Por fim, há que se notar a competência do Supremo Tribunal Federal para a apreciação do caráter da infração, conforme estabelecido pelo §2º do artigo 77 da Lei nº 6.815/80.

Tendo em vista o afirmado, relevam-se as palavras de Fornazari Júnior (2016, p.23), que afirma que este instituto pode ser “considerado o de natureza mais gravosa, por envolver diretamente a liberdade do indivíduo”. Tal afirmação se revela em vista dos diversos requisitos para a sua concessão, devendo-se notar que não é toda e qualquer atividade criminal que pode ensejar a extradição.

Trata-se de uma hipótese extremamente específica em que se apresenta como uma forma extremamente custosa. Considerando as leis brasileiras com relação ao instituto, nota-se que esta modalidade não seria capaz de nos auxiliar, pois se requer que o judiciário local tenha conhecimento e julgue o acusado, sendo que, na situação anteriormente apreciada, não é possível que o Brasil possa exercer a sua jurisdição nestes casos.

Sendo assim, nota-se que a extradição não é um instrumento capaz de influenciar a situação, não só por este requisito, mas também pelas excessivas demandas que ele possui, ainda que justificáveis.

### **4.3 Cartas rogatórias**

As cartas rogatórias constituem, por sua vez, um instrumento “pelo qual se solicita a prática de diligência à autoridade judicial estrangeira” ou é aquele

necessário para a “comunicação de que atos processuais precisam ser realizados fora do território de um Estado” (BECHARA, 2011).

Fornazari Júnior também se refere ao instituto em seu livro, assinalando:

A carta rogatória é meio tradicional utilizado por um Estado soberano, por sua Jurisdição, para solicitar que se produza atos processuais em outro território soberano, visando a produção e coleta de provas ou de qualquer outro ato de instrução processual. A solicitação é sempre expedida por uma autoridade judicial à outra equivalente de outro país. Destina-se (sic) à citação de réu ou investigado domiciliado no exterior (com endereço certo), oitivas, intimações, etc. (2016, p. 27).

Em vista desta afirmação, é possível classificar as cartas rogatórias, conforme Nádia de Araújo (2016) como atos ordinatórios (citação, notificação e cientificação), instrutórias (coleta de provas) e executórias (aqueles que preveem medidas que possuem caráter restritivo). A autora ainda assinala o erro comum de se utilizar a carta rogatória para adquirir informações sobre o direito estrangeiro, sendo que não há previsão para tanto.

A princípio, de acordo com Bechara (2011) o Brasil executava as cartas rogatórias diretamente, não se exigindo muitas formalidades. Entretanto, com a edição do Aviso Circular nº 1 de 1987, “estipulou-se o recebimento das cartas rogatórias pela via diplomática ou consular, por apresentação do interessado ou a partir da comunicação direta entre juízes”.

No dizer deste mesmo autor, nota-se que a competência para o juízo de admissibilidade só passou a ser do Supremo Tribunal Federal com a Constituição Federal de 1934, ainda que não se admitissem medidas de caráter executório. Entretanto, em razão da Emenda Constitucional nº 45 de 2004, a competência “para a concessão do *exequatur* às cartas rogatórias passivas passou para o Superior Tribunal de Justiça”, sendo que o procedimento foi regulamentado pela Resolução nº 9 e, posteriormente, pelo Regimento Interno de 2014.

A análise por parte do Superior Tribunal de Justiça é chamada de juízo de delibação que, conforme Fornazari Junior (2016, p. 29), “restringe-se ao exame dos requisitos legais de admissibilidade da carta rogatória, sem a análise do mérito da demanda, a não ser que este se confunda com os requisitos de admissibilidade”. Desta forma, será de competência deste a aferição do cumprimento das

“formalidades exigidas no Código de Processo Penal, no Regimento Interno do STJ e no tratado internacional específico”.

Nádia de Araújo, no Manual de Cooperação Jurídica Internacional e Recuperação de Ativos, aprofunda um pouco mais na definição de juízo de delibação, devendo-se lembrar que ele é utilizado tanto na análise das cartas rogatórias como das sentenças estrangeiras a serem homologadas em território nacional. Ela assinala:

O modelo adotado no Brasil inspirou-se no italiano, chamado de sistema de delibação, pelo qual não se questionava o mérito da decisão a ser homologada, em sua substancia, senão para a verificação dos requisitos formais, além da ofensa à ordem pública, bons costumes e soberania nacional. Estabeleceu-se, assim, um processo de contenciosidade limitada, porque não é permitido discutir outras questões fora daquelas expressamente delimitadas (2014, p. 40)

Neste sentido, o artigo 784 do Código de Processo Penal estabelece a necessidade de que a carta rogatória não dependa de homologação e será atendida desde que o crime não exclua a extradição. Por sua vez, o artigo 216-P do Regimento Interno do Superior Tribunal de Justiça impede a concessão do *exequatur* quando houver ofensa à soberania nacional, a dignidade da pessoa humana ou à ordem pública.

Dessa forma, as cartas rogatórias passivas são aquelas recebidas pelo Brasil. Por sua vez, as cartas rogatórias ativas exigem, conforme Nádia de Araújo:

Nas cartas rogatórias ativas, há o envio direto do Tribunal rogante para o Ministério da Justiça (mais precisamente, para o Departamento de Recuperação de Ativos e Cooperação Internacional), o que procederá ao seu envio ao exterior, cuidando, inclusive, dos trâmites especiais com os países com os quais mantemos convênios especializados, de caráter multilateral ou bilateral (2016).

Especificamente quanto às cartas rogatórias de matéria penal, o Código de Processo Penal determina, em seu artigo 222-A, que elas só serão expedidas quando for demonstrada a sua imprescindibilidade, devendo-se a parte requerente arcar com os custos, notando-se que este possui o objetivo de “evitar o uso das cartas rogatórias como manobras protelatórias,

prolongando desnecessariamente o inquérito policial ou o processo penal” (FORNAZARI JUNIOR, 2016, p. 28).

O artigo 368 do mesmo códex estabelece, por sua vez, considerando o acusado que está em território estrangeiro, a suspensão do prazo de prescrição até que a medida seja concluída.

As cartas rogatórias, apesar de menos burocráticas do que a extradição, também não se apresenta como medida viável para atingir os acusados que praticam crimes cibernéticos contra brasileiros, tendo em vista que certos crimes não poderiam ser conhecidos pelo judiciário brasileiro.

#### **4.4 Homologação de sentença estrangeira**

No dizer de Abade (2013, p. 56), a homologação de sentença penal estrangeira “consiste em espécie de cooperação jurídica internacional na qual um determinado Estado executa, em seu território, sentença penal oriunda de outro Estado”. Portanto, reconhece-se como instituto tendente a evitar a impunidade, reconhecendo-se seu motivo de ordem humanitária, em que “os sentenciados poderiam cumprir a pena em seu país de origem”.

A forma como cada Estado trabalha com o instituto é diversa, sendo que cada qual conta com sua própria “sistemática para executar sentenças estrangeiras, e raros são os Estados que deixam de reconhecê-las” (ARAUJO, 2016).

Assim como em relação às cartas rogatórias, a Emenda Constitucional nº 45/04 acabou por transferir a competência do Supremo Tribunal Federal para o Superior Tribunal de Justiça para analisar a questão e, na legislação interna, temos dispositivos que tratam sobre o tema no Código Penal, no Código de Processo Penal, na Resolução nº 9 e do Regimento interno, ambos do STJ.

O Código Penal aborda a questão da sentença estrangeira no Brasil no artigo 9º, em que possibilita a homologação da sentença estrangeira nos casos em que “a aplicação da lei brasileira produz na espécie as mesmas consequências” (BRASIL, 1984), conforme redação entregue pela Lei nº 7.209/84, devendo-se ter como intuito obrigar a reparação do dano ocasionado, a restituir ou outros efeitos civis ou sujeitar o acusado à medida de segurança, conforme os incisos do dispositivo.

O parágrafo único do dispositivo, nas suas alíneas, especifica que, no caso de o interesse ser a obrigação de reparar, restituir ou alcançar outro efeito civil, a parte interessada deverá realizar o pedido. Enquanto isso, para os demais casos, deve haver tratado de extradição com o Estado requerente ou, na sua ausência, de requisição do Ministro da Justiça.

Portanto, verifica-se que as hipóteses conforme o Código Penal de 1940 são extremamente restritas, não se admitindo a possibilidade de a homologação ensejar, por exemplo, “a imposição de pena privativa de liberdade a brasileiro que tenha cometido crime no estrangeiro”, pois, neste caso, considerando que o fato também seja considerado como delito no Brasil, tem-se que ele “responderá a processo penal em território brasileiro e, em sendo condenado cumprirá a pena no Brasil” (FORNAZARI JUNIOR, 2016, p. 34 e 35).

Com relação ao Código de Processo Penal, a previsão da modalidade está nos artigos 787 a 790 e eles determinam que, além destas exigências, devem concorrer os seguintes requisitos, sendo eles: o revestimento das formalidades externas necessárias, segundo a legislação do Estado requerente; a sentença tenha sido proferida por juiz competente, mediante citação regular, também de acordo com a legislação alienígena, ter transitado em julgado, ter sido devidamente autenticada pelo cônsul brasileiro e estar acompanhada de tradução, realizada por tradutor público.

Conforme se nota, esta modalidade não se apresenta como meio capaz de possibilitar a tutela do interesse do ofendido brasileiro diante de crime cibernético ocorrido no exterior, tendo em vista que as hipóteses são restritas e o interesse seria o de conseguir processar o acusado no território brasileiro e homologar a sentença no exterior. Entretanto, como se viu anteriormente, as regras referentes à territorialidade e extraterritorialidade da lei penal limitam esta possibilidade, concebendo-se a impossibilidade de a justiça brasileira conhecer alguns crimes.

#### **4.5 Transferência de presos**

Como uma extensão da última modalidade, a partir da década de 70 do século XX, a transferência de presos começou a surgir e “passou a definitivamente fazer parte da agenda da Organização das Nações Unidas” (ABADE, 2013, p. 57).

Entretanto, apenas na década de 80 que se tornou possível a transferência destes, em vista da Declaração de Caracas, que explicitamente abordou o tema.

Conforme Fornazari Junior (2016, p. 38), trata-se de um “instituto humanitário, inspirado na dignidade da pessoa humana, que tem como finalidade propiciar que o condenado cumpra a pena em seu país de origem ou de residência, embora tenha praticado o crime no exterior”. Ainda, o mesmo autor, relata que o interesse não está restrito ao preso ou ao seu Estado, mas também o que efetuou a prisão, tendo em vista que este se vê desobrigado de arcar com as despesas que o detento ocasiona.

Com relação ao Brasil, este “possui dez tratados bilaterais dessa espécie em vigência, com os seguintes países: África do Sul, Argentina, Bolívia, Chile, Espanha, França, Holanda, Paraguai, Portugal e Reino Unido” (FORNAZARI JUNIOR, 2016, p. 38), além de estar obrigado com relação ao tratado multilateral realizado na Convenção Interamericana sobre o Cumprimento de Sentenças Penais no Exterior de 2007.

Infelizmente, assim como os demais instrumentos, este não se apresenta como suficiente para solucionar a situação em que os crimes cibernéticos ocorrem no território estrangeiro enquanto o ofendido é brasileiro localizado neste local, tendo em vista que a modalidade tem como pressuposto garantir melhor condições para o preso e retirar as despesas que ele possui perante o outro Estado.

#### **4.6 Auxílio direto**

Como visto anteriormente, as dinâmicas novas que regem as relações internacionais acabam por exigir uma nova postura dos Estados, tendo em vista que, além dos pontos positivos que estas trazem, os malefícios também se encontram presentes, “especialmente, a vulnerabilidade do Estado no combate aos crimes transnacionais”, pois estes são facilitados “justamente pela nova ordem mundial, com a facilitação do trânsito de bens e pessoas entre os países, bem como com o uso dos meios tecnológicos disponíveis”. (FORNAZARI JUNIOR, 2016, p. 40)

Diante desta situação, “ante a necessidade de respostas mais rápidas aos pedidos formulados”, outras modalidades começam a surgir para amparar os Estados, como o auxílio direto, que é “a cooperação efetuada entre autoridades

centrais de países-parte de convenções internacionais com previsão para essa modalidade de cooperação” (ARAUJO, 2014, p. 41).

Fornazari Junior (2016, p. 41) adianta que, apesar desta necessidade de facilitar a cooperação jurídica internacional, há que se ter em mente que é imprescindível “a criação de um sistema de normas, ou seja, de um regime jurídico que respeite e assegure os direitos fundamentais dos indivíduos frente à ação estatal, consoante os princípios básicos do Estado Democrático de Direito”.

Saadi e Bezerra, no Manual de Cooperação Jurídica Internacional e Recuperação de Ativos, apresentam o conceito de autoridade central, como se vê abaixo:

A autoridade central é um órgão técnico-especializado responsável pela boa condução da cooperação jurídica que cada Estado exerce com as demais soberanias, cabendo-lhe, ademais do recebimento e transmissão dos pedidos de cooperação jurídica, a análise e adequação destas solicitações quanto à legislação estrangeira e ao tratado que a fundamenta. Tem como função promover a efetividade da cooperação jurídica, e, principalmente, desenvolver conhecimento agregado acerca da matéria (2014, p. 21).

Há que se notar ainda que, além deste fundamento, isto é, a busca da celeridade com relação aos pedidos de cooperação jurídica, estes ainda buscam a “lisura da cooperação, dando ao Estado e aos cidadãos que dela se utilizam maior garantia da autenticidade e legalidade do que tramita”, tendo em vista que, quando realizados os tratados, reconhece-se que os participantes “comungam de preceitos e garantias processuais básicas comuns, independentemente do sistema jurídico por eles adotados” (SAADI; BEZERRA, 2014, p. 22).

Atualmente, conforme os mesmos autores (2014, p. 22 e 23) a Autoridade Central brasileira é o Ministério da Justiça, cujo papel é exercido diretamente pelo Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional e o Departamento de Estrangeiros, cabendo a este “analisar e tramitar os pedidos de extradição e transferência de pessoas condenadas”, enquanto que ao primeiro as demais espécies de pedidos de cooperação jurídica internacional sejam de matéria penal ou civil.

Entretanto, há que se notar duas exceções na esfera criminal, eis que cabe à Procuradoria-Geral da República o papel como Autoridade Central “nas questões relativas ao Tratado de Auxílio Mútuo em Matéria Penal entre o Governo da

República Portuguesa e o Governo da República Federativa do Brasil” (SAADI; BEZERRA, 2014, p. 23), assim como no Tratado de Assistência Mútua com o Governo do Canadá, conforme os Decretos nº 1.320/94 e 6.747/09, respectivamente.

Após o envio do pedido à Autoridade Central brasileira, este será “encaminhado ao órgão incumbido, internamente, dos poderes para a realização da diligência”, sendo que, na ocasião de esta necessitar de autorização judicial, o pedido será encaminhado “ao Ministério Público Federal, que proporá uma ação judicial solicitando o atendimento do pedido” (ABADE, 2013, p. 313).

Abade (2013, p. 313) aponta, ainda, três características consideradas básicas do auxílio direto. Primeiramente, ainda que seja oriundo do Poder Judiciário de outro Estado, tem-se que se trata de “uma demanda internacional da parte de outro Estado, da alçada do Poder Executivo brasileiro, na gestão das relações internacionais”, isto é, o requerente se apresenta como “sujeito de Direito Internacional que solicita cooperação”, aceitando que as diligências requeridas sejam realizadas conforme a legislação brasileira.

Tal perspectiva também se encontra na fala de Bechara ao reputar que a singularidade do instituto não se dá tão somente em razão do seu processamento pelas Autoridades Centrais, como se vê abaixo:

O que o singulariza, na realidade, é o fato de que o Estado estrangeiro não se apresenta na condição de juiz, mas de administrador, porquanto não encaminha um pedido judicial de assistência, mas sim uma solicitação para que a autoridade judicial do outro Estado tome as providências e as medidas requeridas no âmbito nacional (2011)

Além desta, tem-se que, diferentemente da carta rogatória e da homologação de sentença estrangeira, o auxílio direto não passa pelo juízo de delibação, pois o pedido tem o seu mérito verificado. Sendo assim, concebe-se que o auxílio direto é um procedimento “que é iniciado por solicitação de Estado estrangeiro para que um juiz nacional conheça de seu pedido e seja iniciada uma demanda interna, pelo órgão competente que na área criminal é o Ministério Público Federal” (ABADE, 2013, p. 314).

Para finalizar, a última característica se refere ao “papel que o Poder Executivo desempenha, de destaque, pois cabe a ele – no papel de Autoridade

Central – encaminhar ou não o pedido cooperacional para os órgãos internos, como o Ministério Público Federal” (ABADE, 2013, p. 314 e 315).

Fornazari Junior (2016, p. 47) também reconhece outra característica básica com relação ao instituto, tendo em vista que grande parte dos tratados exigem que o auxílio direto deve estar associado a uma persecução penal, exige-se que a expedição do pedido por este instrumento, “no Brasil, deve ter sido determinada obrigatória e incidentalmente no curso de uma das duas fases do processo criminal”, isto é, a pré-processual, o inquérito, ou na processual, que é a ação penal em si.

Ainda em vista do pedido de auxílio direto ativo, nota-se que “não somente os juízes brasileiros podem recorrer a este instrumento, mas também o Ministério Público, a defesa e a autoridade policial” (BECHARA, 2011).

Com relação ao seu objeto, nota-se que “toda e qualquer medida processual” poderá ser requerida por intermédio deste instituto, “excetuadas somente a extradição e a prisão”, devendo-se notar que os próprios tratados definem os limites das “questões que não se relacionem diretamente com a liberdade dos indivíduos, matéria afeta somente à extradição e transferência de presos” (FORZANARI JUNIOR, 2016, p. 51).

Como limites a este objeto têm-se aqueles determinados pelos próprios tratados, sendo que há que se ter em mente a dicção do artigo 17 da Lei de Introdução às normas do Direito Brasileiro, Decreto Lei nº 4.657/42, que dispõe como limitadores das leis, atos e sentenças estrangeiras, ou qualquer declaração de vontade, a soberania nacional, a ordem pública e os bons costumes.

Fornazari Junior (2016, p. 76 e 77) orienta no sentido de que o fato de o auxílio direto não importar na privação de liberdade do agente, a restrição à concessão do pedido deve ser menor do que com relação à extradição, por exemplo. Sendo assim, não teria que se falar no princípio da dupla incriminação, isto é, na necessidade de os dois Estados terem em suas respectivas legislações a tipificação daquele determinado crime.

Alguns tratados assumem que o princípio não deve realmente se aplicar, enquanto que outros determinam a aplicação para alguns tipos de crimes, assim como é possível que a relevância do princípio seja aferida com o pedido, conforme o autor acima.

Por fim, como limitador do auxílio direto, tem-se o princípio da especialidade, este que diz que a “prova obtida em inquérito policial ou no processo penal não pode ser utilizada novamente pelo Estado requerente para instruir outra persecução penal, visando apurar outro fato”, devendo-se, para fazer o uso, o Estado requerente formular “um pedido de extensão” para tal fim (FORNAZARI JUNIOR, 2016, p. 79).

#### **4.7 Como o auxílio direto permite o combate ao crime cibernético**

Diante das informações apresentadas acima, nota-se que o auxílio direto permite uma cooperação mais eficiente entre os Estados, possibilitando o combate ao crime transnacional de forma mais célere e menos burocrática, mas há a necessidade de haver um processo, ou ao menos um inquérito, para que ocorra a requisição por parte do Estado brasileiro.

Porém, já se assentou que o judiciário brasileiro não seria competente para conhecer este crime, assim como a competência da autoridade policial estaria perdida assim que tivesse conhecimento do local real do crime.

Desta forma, é possível se questionar sobre qual seria o papel do auxílio direto para garantir que não ocorra a impunidade e que, por consequência, com relação aos crimes cibernéticos, exista um ambiente virtual mais seguro.

Se observarmos a Convenção de Budapeste sobre o Cibercrime, o qual o Brasil não é signatário, mas possui um ponto interessante de partida que podemos utilizar, podemos notar que eles determinam a possibilidade de os Estados-Partes fazerem uso de um instituto chamado de informação espontânea, previsto no artigo 26. Este dispõe:

Uma Parte pode, dentro dos limites da sua legislação nacional e na ausência de pedido prévio, comunicar a outra Parte informações obtidas no quadro das suas próprias investigações, sempre que considerar que isso pode ajudar a Parte destinatária a iniciar ou a levar a cabo investigações ou procedimentos relativos a infrações penais, estabelecidas em conformidade com a presente Convenção, ou sempre que essas informações possam conduzir a um pedido formulado por essa Parte, nos termos do presente Capítulo (2001).

Além desta previsão, a Parte poderá solicitar para que a receptora da informação a mantenha confidencial ou que sejam utilizadas em certas condições,

devendo esta segunda informar quando não poderá anuir com a vontade da primeira.

Portanto, dependendo das informações obtidas por uma autoridade de certo País, nota-se que este não tem como exercer a sua jurisdição para a reprimenda do crime, podendo informar o Estado interessado para que este possa iniciar ou desenvolver as investigações ou iniciar o processo penal contra o autor.

Na realidade, um instrumento como este, da informação espontânea, soa como consequência inerente à cooperação jurídica internacional em matéria penal, tendo em vista que o maior motivo para a sua existência é, justamente, impedir que os crimes transnacionais ocorram com mais frequência.

Entretanto, não são todos os tratados que dispõem acerca desta possibilidade, sendo o instrumento mais predominante em acordos bilaterais, ainda que não exista esta previsão em todos.

Por exemplo, o acordo bilateral firmado com o Reino da Espanha sobre cooperação e auxílio jurídica em matéria penal, promulgado pelo Decreto nº 6.681/08, verifica-se a sua previsão no artigo 21, estabelecendo a possibilidade de as partes trocarem informações relativas a delitos, ainda que não haja solicitação prévia, caso se considere que a informação seja útil para o início ou a condução de investigações ou processos.

Interessante notar, como está disposto na Convenção de Budapeste, o Estado que apresentar esta informação espontânea poderá impor algumas condições para o uso destas, devendo o Estado receptor respeitar a demanda do outro desde que as aceite.

Alguns outros Estados também possuem a previsão deste instituto nos seus acordos bilaterais formados com o Brasil, sendo eles: República de Honduras, Estados Unidos Mexicanos, República Federal da Nigéria, República do Panamá, Governo do Reino Unido da Grã-Bretanha e Irlanda do Norte, Confederação da Suíça e República do Suriname<sup>64</sup>.

Ainda que não se haja previsão explícita deste instituto nos demais acordos, é possível considerar, no intuito da cooperação e na preservação da sociedade em geral, que a troca de informações de forma espontânea ocorra.

---

<sup>64</sup> Decretos nº 8.046/13, 7.595/11, 7.582/11, 7.596/11, 8.047/13, 6.974/09, 6.832/09, respectivamente.

Utilizando como exemplo o acordo realizado com o Governo do Canadá, tem-se que, no artigo 1, referente à obrigação de prestar assistência mútua, reconhece-se no parágrafo primeiro que ambos os Estados devem prestar a assistência mútua “em matéria penal na medida mais ampla possível” (BRASIL, 2009).

O parágrafo segundo, por sua vez, reflete o que é considerado como assistência mutua para os fins deste acordo, conforme se depreende abaixo:

Para os fins do parágrafo 1 deste artigo, será considerada assistência mútua qualquer assistência prestada pelo Estado requerido em relação a investigações ou processos judiciais no Estado requerente relativos a uma matéria penal, independentemente do fato da assistência ser solicitada ou dever ser prestada por um tribunal ou alguma outra autoridade (BRASIL, 2009).

O parágrafo quinto afirma, dentre outras hipóteses, a inclusão de outras formas de assistência desde que elas sejam coerentes com os objetivos do acordo.

Ora, tendo em vista que o objetivo destes acordos é justamente facilitar a comunicação entre os Estados e impedir que a impunidade se propague, há que se notar que a informação espontânea de um ente estatal ao outro representa justamente o intuito destes documentos.

O espírito destes acordos é basicamente o mesmo, considerando-se ainda que há previsão, na maior parte destes, com relação a esta concepção, ou similar, de assistência mútua e a possibilidade de serem utilizados outros instrumentos que permitam a cooperação.

É como se afirmou anteriormente, trata-se de uma consequência lógica da ideia de cooperação. Não é possível pensar no auxílio entre dois Estados na área penal e não haver a possibilidade de comunicação entre estes no caso de um deles ter conhecimento de crimes ocorridos no território do outro. Formar-se-ia um verdadeiro contrassenso, em que iria vigorar exatamente o que se pretende combater, que é a impunidade.

Como Martín compreende, a persecução destes infratores é uma tarefa por demasiada difícil, tendo em vista que:

*Se requiere de la cooperación regional e internacional de los organismos en la materia, las autoridades competentes, los gobiernos y el sector privado de los países involucrados, donde muchas veces se encuentran con serias limitantes como son*

*diferencias de los sistemas jurídicos; carencia de legislación penal adecuada tanto sustantiva como adjetiva para perseguir ciberdelitos y sobre todo la falta de acuerdos y consensos legislativos para armonizar las legislaciones de conformidad con los tratados, acuerdos y resoluciones internacionales más relevantes sobre la materia*<sup>65</sup> (2012).

O trabalho realizado na cooperação jurídica internacional já seria de grande valia para a superação dos problemas enfrentados na persecução penal, tendo que se ter em mente que outras medidas, internamente, também podem ser tomadas para à repressão aos crimes cibernéticos.

#### **4.8 Limites às informações espontâneas?**

Se pegarmos como exemplo o artigo 21 do acordo realizado entre o Brasil e a Espanha, tem-se a previsão da troca espontânea de informação, apresentando-se dois parágrafos, que dispõem:

- 1.As Partes poderão, sem solicitação prévia, trocar informação relativa a fatos delituosos, caso considerem que tal informação possa ser útil para iniciar ou conduzir investigações ou processos.
- 2.A parte que fornecer a informação poderá impor condições sobre o uso que a Parte receptora fará dessa. Ao aceitar a informação, a Parte receptora se compromete a respeitar as condições (BRASIL, 2008)

A primeira dúvida que surge perante estas disposições é reconhecer o que constituiria uma informação. Questiona-se a possibilidade de ser um mero indício ou se se requer uma prova de materialidade ou de autoria e como que ela pode ser utilizada.

Veja-se que, ainda com relação a este acordo em específico, o artigo 9º estabelece como as informações, entre outros, podem ser utilizados pelo Estado requerente, como se verifica:

---

<sup>65</sup> Requer-se da cooperação regional e internacional dos organismos na matéria, as autoridades competentes, os governos e o setor privado destes países envolvidos, em que muitas vezes se encontram sérias limitantes como são as diferenças entre os sistemas jurídicos; carência de legislação penal adequada, tanto substantivas quanto adjetivas para perseguir os crimes cibernéticos e, sobretudo, a falta de acordos e consensos legislativos para harmonizar as legislações em conformidade com os tratados, acordos e resoluções internacionais mais relevantes sobre a matérias.

1. Informações, documentos ou objetos obtidos mediante auxílio jurídico poderão ser utilizados em investigações na Parte requerente e ser empregados como meios de prova em outros procedimentos penais relativos a delitos pelos quais se possa conceder o auxílio jurídico (BRASIL, 2008)

Como se depreende do trecho acima, estas informações são capazes de constituir meio de prova nos processos penais, ou nos seus respectivos inquéritos, de forma a permitir que a persecução penal ocorra.

Quando estamos diante de uma requisição, tem-se que o Estado requerente tem a noção de que ele depende do outro ente estatal para a produção da prova necessária, adimplindo com a legislação do requerido.

Entretanto, diante de uma situação em que a informação é entregue de forma espontânea, o Estado receptor daquela não adimpliu com a forma com a qual o ente que a entregou formulou a prova.

Pode-se dizer que, por outro lado, nos casos em que o acordo foi celebrado com esta possibilidade, há certo assentimento tácito com relação às informações tácitas, prevalecendo, desta forma, o paradigma da confiança e do reconhecimento mútuo.

No dizer de Abade (2013, p. 63), este paradigma é aquele em que a cooperação internacional “é marcada pela confiança entre os Estados e reconhecimento mútuo das decisões, sem maiores avaliações nacionais de controle dos pedidos”, permitindo-se esta atitude entre os Estados com base na “homogeneização das normas processuais penais”.

Ora, tendo em vista que a intenção é justamente impedir o crescimento e a impunidade dos crimes transnacionais, concebe-se que a aproximação entre os diversos sistemas jurídicos ensejaria uma cooperação mais eficaz, pois facilitaria o intercâmbio de provas e homologações de sentenças.

Apesar de ser uma perspectiva interessante, esta não é a realidade que o Brasil vive. Tal afirmação pode ser realizada tão somente com a leitura do artigo 17 da Lei de Introdução às Normas do Direito Brasileiro, que dispõe que “as leis, atos e sentenças de outro país, bem como quaisquer declarações de vontade, não terão eficácia no Brasil, quando ofenderem a soberania nacional, a ordem pública e os bons costumes”.

A tendência do paradigma da confiança e do reconhecimento mútuo se verifica com maior clareza na União Europeia, mas, ainda assim, de forma limitada. Com relação ao Mercosul, Abade (2013, p. 63) nota que persiste a coexistência interessada, em que cabe ao Estado “avaliar as condições pelas quais a cooperação internacional penal se dá, em especial no que tange à proteção dos direitos fundamentais dos indivíduos sujeitos aos pedidos cooperacionais”.

Há, então, a vigência da desconfiança, em que os Estados devem realizar a sua própria análise com relação ao que se está sendo requerido.

Portanto, diante de um ambiente internacional como esse, em que requerimentos usualmente passam pelo crivo de certa autoridade previamente estabelecida, tem-se que, possivelmente, as informações espontaneamente entregues entre os Estados não seria utilizada sem uma análise prévia em face da legislação local, o que poderia ocasionar uma maior demora com relação às investigações e, conseqüentemente, o processo penal.

De qualquer forma, tem-se que, ainda que as informações sejam regularmente produzidas conforme a legislação de um local, isto pode não corresponder à legislação de outro Estado e, por esta razão, elas não poderiam ser utilizadas num eventual inquérito ou processo.

#### **4.9 A importância do Brasil no cenário internacional no combate ao crime cibernético**

Em 2012, Martín assinalou uma tendência preocupante em alguns países, como o Brasil, conforme se vê abaixo:

*Se cree que las economías emergentes tales como Rusia, China, India y Brasil albergan la mayoría de los ciberdelincuentes puesto que dichos países no cuentan todavía con un marco jurídico sólido para su persecución y sobre todo con instituciones y autoridades eficaces para la identificación de los ciberdelincios y su persecución<sup>66</sup> (2012).*

---

<sup>66</sup> Acredita-se que as econômicas emergentes como a Rússia, China, Índia e Brasil acolhem a maioria dos ciberdelinquentes, posto que estes países não contam ainda com um marco jurídico sólido para a perseguição daqueles e sobretudo com instituições e autoridade eficaz para a identificação dos crimes cibernéticos e sua persecução (tradução livre).

Note-se que a realidade aponta que o Brasil possui diversos autores de crimes cibernéticos que ocorrem ao redor do mundo, verificando-se a importância do Estado brasileiro neste cenário.

É muito importante, como já apontado, que o Estado brasileiro aja quando exista uma vítima brasileira e possibilite que o autor de certo crime cibernético sofra a sua devida punição.

Entretanto, a perspectiva acima não exclui a necessidade de o próprio Brasil trabalhar com os demais Estados no intuito de coibir as atividades delituosas advindas de seu interior.

Veja-se que, qualquer que seja o tipo de trabalho realizado pelas Autoridades Centrais, isto é, seja de forma ativa ou passiva, a relação entre os Países comunicantes se estreita e ajuda a, no futuro, verificar novas e melhores formas de cooperação, seja pela produção de determinadas provas ou nas condições em que possibilitam a condição da prova como legal no Estado receptor.

Todavia, não há como aceitar a legislação vigente sobre os crimes cibernéticos. A análise feita por alguns autores acima citados foram anteriores à Lei nº 12.737/12, mas com muita dificuldade seria possível acreditar que a inclusão de quatro artigos é suficiente para contribuir, efetivamente, na repressão aos crimes cibernéticos.

É um passo, de fato, mas não muito longo, devendo-se tentar acompanhar as ações criminosas realizadas na internet sempre que possível, ainda mais que as atividades são extremamente dinâmicas.

Não basta, também, apenas a inovação legislativa. Considerar que a legislação é suficiente para coibir a prática de crimes em um determinado território corresponde a um pensamento simplista e dissociado da realidade, apesar de importar em algum avanço.

Veja-se que as autoridades policiais devem caminhar no sentido de aperfeiçoar, cada vez mais, os seus procedimentos investigativos com relação a esta categoria de crimes, da mesma forma que devem ser aprimoradas as comunicações entre estas autoridades e a Autoridade Central, de forma que as informações circulem com maior rapidez.

## CONCLUSÃO

Primeiramente, compreendemos como a internet funciona por meio do entendimento do que são protocolos e como eles se articulam.

A internet é, de fato, uma rede de redes, em que diversas redes menores comunicam entre si dando a ideia de que se trata de uma grande rede, mas isso não passa de uma ilusão.

Esta não é a única ilusão, entretanto, tendo em vista que apesar de o ambiente virtual parecer dissociado de qualquer aspecto físico, ele é inteiramente dependente de seu aparato. Veja-se, por exemplo, que na ausência de um servidor específico para um sítio qualquer da internet, ele nunca poderia ser acessado.

Além disso, ainda que exista um servidor, caso não exista um caminho pelo qual os pacotes de dados possam trafegar, não teria qualquer propósito a sua existência, pois não haveria qualquer possibilidade de comunicação.

Compreendida a internet, passou-se a analisar a jurisdição. Este instituto determina a possibilidade de o Estado dizer o direito com relação a certo local e a sua compreensão foi se desenvolvendo com o tempo.

Como parâmetros clássicos, temos as posições de Carnelutti e Chiovenda, sendo que o primeiro partiu de um conceito de lide, ou conflito, enquanto que o segundo adota a posição de que a jurisdição se limita à atuação da vontade concreta do direito objetivo.

Em seguida, abordamos os escopos da jurisdição, conforme as lições de Dinamarco, sendo que estes se dividem em três perspectivas, os sociais, políticos e jurídicos.

Os sociais refletem a pacificação social e a educação da sociedade a qual se submete a esta jurisdição, enquanto que os políticos se referem à afirmação do poder estatal, a preservação das liberdades públicas e a garantia da participação do jurisdicionado no caminho da sociedade. Por fim, como escopo jurídico, tem-se a atuação da vontade concreta do direito, buscando-se a celeridade e a universalização da justiça.

Há que se notar que os escopos ou propósitos da jurisdição articulam entre si, denotando uma face diversa daquela esposada pelos conceitos clássicos. Ainda que Dinamarco tenha partido desta concepção de que a jurisdição tem como objetivo a atuação da vontade concreta do direito, tem-se que já se percebe um avanço com

relação aquele conceito clássico, em que se tem como propósito último do instituto a pacificação social e, de certa forma, a educação da sociedade, sem dizer que a expressão política dos escopos revela a preservação das liberdades pública.

Marinoni, Arenhart e Mitidiero, então, concebem o que podemos chamar de um conceito contemporâneo de jurisdição, em que não se trata tão somente da aplicação da vontade concreta do direito ao caso concreto, mas há a verdadeira reconstrução da ordem jurídica, em que o direito deve se conformar ao caso concreto de forma a garantir o seu objetivo último, qual seja, a tutela dos direitos. Busca-se, então, garantir que os direitos daqueles subordinados a determinada jurisdição sejam preservados, sejam com relação ao próprio Estado ou com relação à particulares que lesionam aqueles primeiros.

Tendo em vista o desenvolvimento da jurisdição, tendente à tutela dos direitos de seus jurisdicionados, nota-se que ela não representa tão somente um dever da jurisdição, mas sim do todo estatal. Considerando-se que o poder é uno, este instituto representa apenas uma parte do que compreendemos o Estado e, na realidade, os direitos fundamentais devem ser preservados por todo este ente, seja na sua manifestação executiva, legislativa ou jurisdicional.

De qualquer forma, a jurisdição penal é, sendo esta apenas uma distinção didática, aquela que se propõe a aplicar a pretensão punitiva, estabelecendo-se, como seu limite, justamente o local em que o crime ocorreu.

Para tanto, adota-se, como regra, o princípio da territorialidade, conforme o artigo 5º do Código Penal, em que a lei brasileira será aplicável aos crimes que ocorrerem no território nacional, com possíveis exceções.

No entanto, como visto no trabalho, somente esta concepção de territorialidade acabaria por ser ultrapassada, pois a dinâmica mundial mudou de tal forma que os meios de transportes e outras tecnologias avançaram de modo que os Estados tiveram que adotar uma postura diversa. Por esta razão, diante da possibilidade de um criminoso sair impune, tem-se que os Estados passaram a adotar regras que permitiam a aplicação extraterritorial de suas leis.

Os princípios regentes destas aplicações extraterritoriais pretendem defender os bens jurídicos de determinados Estados, punir crimes que devem ser reprimidos de forma internacional, preservar aqueles de sua nacionalidade ou punir aqueles

que realizam crimes em território estrangeiro, ou, ainda, alcançar delitos praticados em embarcações ou aeronaves que não estão no território nacional.

Tem-se, entretanto, que a lei brasileira adota uma série de requisitos para que ela seja aplicada às infrações penais que ocorrem no território estrangeiro, sendo elas previstas no artigo 7º do Código Penal.

Ainda que exista a possibilidade de se aplicar a lei penal brasileira a todo e qualquer caso, a chamada extraterritorialidade incondicionada, em que, principalmente, busca-se punir aqueles atos contra os bens jurídicos referentes ao Estado brasileiro, assim como a punição do genocídio quando o agente for brasileiro ou tiver domicílio neste local.

O inciso II deste mesmo artigo também não abarca a possibilidade de a lei penal brasileiro reprimir os crimes praticados contra brasileiro, ainda que no exterior, somente tendo esta previsão no §3º, em que, além dos requisitos do parágrafo anterior, devem estar presentes a ausência de pedido ou a negação da extradição e a requisição do Ministro da Justiça.

Tendo em vista a restrição de tal caso, é comum chamar esta hipótese de extraterritorialidade hipercondicionada, pois são vários os requisitos para a sua aplicação.

Com relação ao local do crime, o Brasil adota a teoria da ubiquidade, em que se considera tanto o local da ação ou omissão como o do resultado, abrangendo diversas situações, porém, como visto posteriormente, tal não é suficiente para abarcar alguns crimes cibernéticos praticados contra brasileiros.

Após esta discussão com relação a jurisdição no Brasil, passou-se a discutir como a jurisdição seria aplicada na internet, pois se trataria de um ambiente diverso daquele que tratamos usualmente.

Notando-se que a jurisdição é associada, usualmente, com o território, vê-se que a internet não apresentaria qualquer similaridade com o mundo real porque as suas comunidades não dependem de um território específico, entre outros motivos.

Todavia, notou-se que apesar das diferentes perspectivas com relação a este problema, a internet possui, sim, barreiras e as regras territoriais e extraterritoriais, apesar de não serem as mais desejáveis, podem fornecer a base para que o Estado possa realizar um dos seus objetivos, qual seja, a tutela dos direitos de seus administrados.

A discussão, então, dirigiu-se aos crimes cibernéticos em si, compreendendo o seu conceito, a sua classificação e alguns dos tipos penais específicos previstos no ordenamento jurídico brasileiro.

Viu-se, também, que não se trata da proteção dos bens jurídicos individuais, de extrema relevância, mas não únicos, porque a segurança da rede é um resultado pretendido por todos e, com a sua preservação, tem-se que os individuais, por consequência, também serão resguardados.

Apesar de não existir uma norma que prevê expressamente a defesa da segurança na rede no direito brasileiro, tem-se que os requisitos apreciados pela Convenção de Budapeste, quais sejam, a confidencialidade, a integridade e a disponibilidade estão todos previstos de forma implícita na Lei do Marco Civil da Internet, estabelecendo que estes correspondem aos direitos dos usuários.

Verificou-se, posteriormente, que a maior preocupação que se deve ter com relação aos crimes cibernéticos é a classificação deste como um crime material, formal ou de mão própria, além do local em que o agente delitivo se encontra, assim como do servidor.

Não será todo crime deste tipo, portanto, que será alcançado pela legislação brasileira, tendo em vista que o artigo 7º do Código Penal estabelece critérios rígidos para a aplicação extraterritorial nestes casos.

Há que se notar, entretanto, que apesar desta situação, tem-se que, diante das inovações da cooperação jurídica internacional, trata-se de uma resposta melhor do que o uso indiscriminado de um princípio da personalidade passiva, em que, por vezes, o autor do crime ainda permaneceria impune tendo em vista a falta de eficácia da sentença brasileira no exterior a depender das regras próprias do País a receber a homologação de sentença estrangeira, assim como as restritas hipóteses de extradição.

A cooperação jurídica internacional se torna relevante principalmente em face do auxílio direto, que possibilita uma via menos burocrática para os entes estatais comunicarem entre si, representando um verdadeiro avanço para impedir a impunidade.

Dentre as possibilidades decorrentes do auxílio direto, tem-se a previsão em alguns acordos da informação espontânea, em que, diante da produção de uma

informação que poderá ensejar uma investigação ou um processo em outro país, o produtor poderá enviar tais informações para o Estado interessado.

Volta-se à questão do objetivo do Estado ter como pressuposto a tutela dos direitos dos seus administrados, em que, apesar de ele reconhecer que ele não possui a competência para exercer a sua jurisdição, ele irá fornecer uma possibilidade para que aquele criminoso seja punido e, conseqüentemente, com o maior auxílio entre os diversos entes estatais, a segurança na rede irá aumentar.

Claramente, apesar de ser uma consequência lógica do auxílio direto, diversos acordos realizados pelo Brasil não preveem esta possibilidade da informação espontânea, mas acredita-se na possibilidade de ela ocorrer na mesma forma considerando que as formas de ajuda entre os Estados não representa um rol taxativo.

Além disso, não se dispensa a possibilidade de haver limitações, sejam elas processuais decorrentes da forma de produção da prova, podendo ela ser considerada ilícita no Estado receptor, assim como há a possibilidade de que o fato sequer seja considerado criminoso neste.

O que se percebe é a necessidade de os Estados, não só o Brasil, portanto, de atualizarem as suas respectivas legislações, de forma a acompanharem as tendências dos crimes cibernéticos, caso eles não consigam perseguir determinados fatos.

Talvez um dos casos mais emblemáticos para representar esta situação seja o do vírus conhecido como vírus *I love you*, *Loveletter* ou *Love bug*, em que, no ano de 2000, causou “bilhões de dólares de prejuízo”, fazendo com que “várias empresas e organizações, inclusive a NASA” (ROHR, 2010), desativassem seus servidores para que ele não causasse mais danos. A questão é que, como não havia legislação sobre o assunto nas Filipinas o autor acabou não sendo responsabilizado.

Portanto, há uma necessidade que os Estados trabalhem em conjunto para garantir a segurança da rede, não somente com relação ao auxílio em si, mas também com a atualização constante de suas legislações para evitar situações como estas.

De qualquer forma, depreende-se do estudo que, afinal, certos crimes cibernéticos, ainda que praticados contra vítimas brasileiras, não podem ser aqui julgados, devendo as autoridades brasileiras competentes realizarem as devidas

investigações e, comprovada a impossibilidade, que as informações sejam remetidas para o Estado que possa ter interesse sobre estas.

## REFERÊNCIAS

ABADE, Denise Neves. **Direitos fundamentais na cooperação jurídica internacional: extradição, assistência jurídica, execução de sentença estrangeira e transferência de presos**. São Paulo: Saraiva, 2013.

ACCIOLY, Hildebrando; CASELLA, Paulo Borba; SILVA, G. E. do Nascimento e. **Manual de direito internacional público**. 19. ed. São Paulo: Saraiva, 2011.

ARAÚJO, Nádia de. **Direito Internacional Privado: Teoria e Prática Brasileira**. 1. ed. Porto Alegre: Revolução eBook, 2016.

\_\_\_\_\_. A importância da cooperação jurídica internacional para a atuação do Estado brasileiro no plano interno e internacional. In: **Manual de Cooperação jurídica internacional e recuperação de ativos: cooperação em matéria penal**. 3. ed. Brasília: Ministério da Justiça, 2014.

BARLOW, John Perry. **A Declaration of the Independence of Cyberspace**. Disponível em: <<https://www.eff.org/cyberspace-independence>>. Acesso em: 15 abr. 2017.

BECHARA, Fábio Ramazzini. **Cooperação jurídica internacional em matéria penal: eficácia da prova produzida no exterior**. São Paulo: Saraiva, 2011.

BERMAN, Paul Schiff. **Law and Society Approaches to Cyberspace**. Disponível em: <<http://lsr.nellco.org/uconn/ucwps/papers/72>>. Acesso em: 20 abr. 2017.

\_\_\_\_\_. **The Globalization of Jurisdiction**. Disponível em: <[http://scholarship.law.upenn.edu/penn\\_law\\_review/vol151/iss2/1/](http://scholarship.law.upenn.edu/penn_law_review/vol151/iss2/1/)>. Acesso em: 28 abr. 2017.

BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte geral**. 15. ed. São Paulo: Saraiva, 2010.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm)>. Acesso em: 20 mar. 2017.

BRASIL, **Decreto nº 6.747, de 22 de janeiro de 2009**. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2007-2010/2009/decreto/d6747.htm](http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/decreto/d6747.htm)>. Acesso em: 15 maio. 2017.

BRASIL, **Decreto nº 8.048, de 11 de julho de 2013**. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2011-2014/2013/Decreto/D8048.htm](http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D8048.htm)>. Acesso em: 15 maio. 2017.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940.** Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/decreto-lei/De12848compilado.htm](http://www.planalto.gov.br/ccivil_03/decreto-lei/De12848compilado.htm)>. Acesso em: 19 mar. 2017.

BRASIL, **Decreto-Lei nº 3.689, de 3 de outubro de 1941.** Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/decreto-lei/De13689.htm](http://www.planalto.gov.br/ccivil_03/decreto-lei/De13689.htm)>. Acesso em: 20 maio. 2017.

BRASIL. **Lei nº 6.815, de 19 de agosto de 1980.** Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/leis/L6815.htm](http://www.planalto.gov.br/ccivil_03/leis/L6815.htm)>. Acesso em: 18 abr. 2017.

BRASIL. **Lei nº 7.209, de 11 de julho de 1984.** Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/leis/1980-1988/L7209.htm](http://www.planalto.gov.br/ccivil_03/leis/1980-1988/L7209.htm)>. Acesso em: 10 maio. 2017.

BRASIL. **Lei nº 7.716, de 5 de janeiro de 1989.** Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/leis/L7716.htm](http://www.planalto.gov.br/ccivil_03/leis/L7716.htm)>. Acesso em: 10 maio. 2017.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012.** Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/112735.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112735.htm)>. Acesso em: 19 abr. 2017.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/112737.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm)>. Acesso em: 18 abr. 2017.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/112965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm)>. Acesso em: 30 abr. 2017.

CÂMARA, Alexandre Freitas. **Lições de Direito Processual Civil, volume I.** 11. ed. Rio de Janeiro: Editora Lumen Juris, 2004.

CARVALHO, Ana Cristina Azevedo P. **Marco civil da internet no Brasil.** Rio de Janeiro: Alta Books, 2014.

COMER, Douglas E. **The internet book: everything you need to know about computer networking and how the internet works.** 4. ed. San Jose: Pearson Education, 2007.

DINAMARCO, Cândido Rangel. **A instrumentalidade do processo.** 13. ed. São Paulo: Malheiros Editores LTDA., 2008.

DINAMARCO, Cândido Rangel; GRINOVER, Ada Pellegrini; CINTRA, Antonio Carlos de Araújo. **Teoria geral do processo.** 29. ed. São Paulo: Malheiros Editores LTDA., 2013.

CONSELHO DA EUROPA. **Convenção sobre o Cibercrime.** Budapeste. 2001. Disponível em:

FACEBOOK. **102 milhões de brasileiros compartilham seus momentos no Facebook todos os meses.** Disponível em: <<https://pt-br.facebook.com/business/news/102-milhes-de>>

brasileiros-compartilham-seus-momentos-no-facebook-todos-os-meses>. Acesso em: 31 maio. 2017.

FORNAZARI JUNIOR, Milton. **Cooperação Jurídica Internacional: Auxílio direto penal**. Rio de Janeiro: Editora Lumen Juris, 2016.

GOLDSMITH, John; WU, Tim. **Who controls the internet? Illusions of a Borderless World**. New York: Oxford University Press, 2006.

GOMES, Luiz Flávio; BIANCHINI, Alice; DAHER, Flávio. **Curso de Direito Penal: parte geral (arts. 1º a 120)**. Salvador: Editora JusPodivm, 2016.

GRECO, Rogério. **Curso de Direito Penal**. 13. ed. Rio de Janeiro: Impetus, 2011.

JESUS, Damásio de.; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

KUROSE, Jim; ROSS, Keith. **Redes de computadores e a internet: uma abordagem top-down**. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz; MITIDIERO, Daniel. **Novo curso de processo civil: volume 1: teoria do processo civil**. São Paulo: Editora Revista dos Tribunais, 2015.

MARTÍN, Cristos Velasco San. **La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet**. Valencia: Tirant Lo Blanch, 2012.

MIRABETE, Julio Fabbrini. **Manual de direito penal**. 23. ed. São Paulo: Atlas, 2006.

MITIDIERO, Daniel; OLIVEIRA, Carlos Alberto Álvaro de. **Curso de Processo Civil: volume I: teoria geral do processo civil e parte geral do direito processual civil**. São Paulo: [s.n.].

NUCCI, Guilherme de Souza. **Manual de Direito Penal**. 7. ed. São Paulo: Editora Revista dos Tribunais, 2011.

POST, David G. Anarchy, State and the Internet: an Essay of Law-making in Cyberspace. **Journal of Online Law, article 3**, 1995.

ROHR, Altieres. **Vírus Loveletter, que infectou milhões de computadores, completa 10 anos**. Disponível em: <<http://g1.globo.com/tecnologia/noticia/2010/05/virus-loveletter-que-infectou-milhoes-de-computadores-completa-10-anos.html>>. Acesso em: 31 maio. 2017.

SAADI, Ricardo Andrade; BEZERRA, Camila Colares. A autoridade central no exercício da cooperação jurídica internacional. In: **Manual de Cooperação jurídica internacional e recuperação de ativos: cooperação em matéria penal**. 3. ed. Brasília: Ministério da Justiça, 2014.

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. 2. ed. São Paulo: Saraiva, 2015.

SYMANTEC. **Norton Cyber Security Insights Report 2016**. Disponível em: <<https://www.symantec.com/content/dam/symantec/docs/reports/2016-norton-cyber-security-insights-comparisons-brazil-en.pdf>>. Acesso em: 31 maio. 2017.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal**. 6. ed. Salvador: Editora JusPodivm, 2011.

TOLEDO, Francisco de Assis. **Princípios básicos de direito penal**. 5. ed. São Paulo: Saraiva, 2000.

TORRES, Gabriel. **Redes de Computadores**. 2. ed. Rio de Janeiro: Novaterra, 2014.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. 2. ed. Rio de Janeiro: Brasport, 2013.

WOODS, Andrew. K. **Against Data Exceptionalism**. Disponível em: <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2745038](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2745038)>. Acesso em: 15 abr. 2017.

ZANIOLO, Pedro Augusto. **Crimes modernos: o impacto da tecnologia no direito**. 3. ed. Curitiba: Juruá, 2016.