UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

FACULDADE DE DIREITO

DEPARTAMENTO DE CIÊNCIAS PENAIS (DIR1)

Leonardo Garcia de Mello

APLICAÇÃO DA TEORIA DO DOMÍNIO DO FATO A CRIMES CIBERNÉTICOS DO TIPO *RANSOMWARE*

Porto Alegre

2021

Leonardo Garcia de Mello

APLICAÇÃO DA TEORIA DO DOMÍNIO DO FATO A CRIMES CIBERNÉTICOS DO TIPO *RANSOMWARE*

Trabalho de Conclusão de Curso apresentado como requisito parcial para a obtenção do grau de Bacharel em Ciências Jurídicas e Sociais pela Faculdade de Direito da Universidade Federal do Rio Grande do Sul.

Orientador: Prof. Dr. Ângelo Roberto Ilha da Silva

Porto Alegre

2021

CIP - Catalogação na Publicação

MELLO, LEONARDO GARCIA DE
APLICAÇÃO DA TEORIA DO DOMÍNIO DO FATO A CRIMES CIBERNÉTICOS DO TIPO RANSOMWARE / LEONARDO GARCIA DE MELLO. -- 2021.
52 f.
Orientador: ANGELO ROBERTO ILHA DA SILVA.

Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Faculdade de Direito, Curso de Ciências Jurídicas e Sociais, Porto Alegre, BR-RS, 2021.

1. DIREITO PENAL. 2. CRIMES CIBERNÉTICOS. 3. RANSOMWARE. 4. CONCURSO DE PESSOAS. 5. TEORIA DO DOMÍNIO DO FATO. I. SILVA, ANGELO ROBERTO ILHA DA, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
Setor de Graduação da Gerência Administrativa da Faculdade de Direito - GRADDIR
Av. João Pessoa, 80 - Bairro Centro - CEP 90040000 - Porto Alegre - RS - www.ufrgs.br
Prédio 11108

ATA

Aos doze dias do mês de maio do ano de dois mil e vinte e um, no Departamento de Ciências Penais da Faculdade de Direito da Universidade Federal do Rio Grande do Sul – UFRGS, às dez horas e quarenta minutos, reuniu-se, por meio digital, a Comissão Examinadora composta pelos professores **ÂNGELO ROBERTO ILHA DA SILVA, MAURO FONSECA ANDRADE e MARCUS VINÍCIUS AGUIAR MACEDO** para, sob a presidência do primeiro, na qualidade de orientador, arguirem o acadêmico **LEONARDO GARCIA DE MELL**O, a fim de avaliarem a Monografia de Conclusão do Curso de Ciências Jurídicas e Sociais, na forma da Resolução Nº 2 de 2004 da Comissão de Graduação da Faculdade de Direito. O trabalho de título **"APLICAÇÃO DA TEORIA DO DOMÍNIO DO FATO A CRIMES CIBERNÉTICOS DO TIPO *RANSOMWARE*"** foi apresentado à Comissão Examinadora, que, após a arguição do acadêmico, atribuiu-lhe o conceito final **"A"**. Nada mais havendo a tratar, foi encerrada a sessão e lavrada a presente ata, que vai assinada pelos membros da Banca Examinadora.

Porto Alegre, 12 de maio de 2021.

Documento assinado eletronicamente por **ÂNGELO ROBERTO ILHA DA SILVA**, **Chefe do Departamento de Ciências Penais**, em 14/05/2021, às 18:38, conforme art. 7º, I, da Portaria nº 6954 de 11 de setembro de 2015.

Documento assinado eletronicamente por **MARCUS VINICIUS AGUIAR MACEDO**, **PROFESSOR DO MAGISTÉRIO SUPERIOR**, em 17/05/2021, às 18:50, conforme art. 7º, I, da Portaria nº 6954 de 11 de setembro de 2015.

Documento assinado eletronicamente por **MAURO FONSECA ANDRADE**, **PROFESSOR DO MAGISTÉRIO SUPERIOR**, em 18/05/2021, às 08:36, conforme art. 7º, I, da Portaria nº 6954 de 11 de setembro de 2015.

A autenticidade do documento pode ser conferida no site https://sei.ufrgs.br/sei/verifica.php informando o código verificador **2781112** e o código CRC **99253BF0**.

DEDICATÓRIA

Dedico este trabalho para a minha Família,

em especial à minha mãe Maria Eva e ao meu filho Henrique.

AGRADECIMENTOS

Primeiramente eu agradeço a Deus, citando um versículo do Novo Testamento do qual eu gosto bastante e muitas vezes é mal interpretado: “Posso todas as coisas em Cristo, que me fortalece!” (Filipenses 4:13). Mesmo sabendo não se tratar de uma frase motivacional, peço licença para retirá-lo de seu contexto original na Carta da Alegria pela força dessas palavras.

Agradeço muito a toda minha Família, mas em especial aos meus pais Maria Eva e Luiz Carlos por haverem zelado pela nossa educação de maneira que eu e meus irmãos pudéssemos vir a estudar em instituições de prestígio. Sou grato à minha mãe por ter cuidado do meu filho enquanto eu fazia o curso, sem o seu apoio teria sido impossível! E agradeço ao meu filho Henrique por ter se sacrificado ao deixar de contar com a presença do pai durante parte da sua infância enquanto eu estudava. Mas acima de tudo sou grato por ele ser a grande motivação para eu me esforçar buscando qualificação a fim de atendê-lo cada vez melhor.

Agradeço à Universidade Federal do Rio Grande do Sul por ser uma instituição pública, gratuita e de qualidade. Tenho bastante orgulho por haver estudado aqui desde o ensino técnico até o pós-graduação. Não tenho palavras apropriadas para agradecer a todos os professores e funcionários da UFRGS com os quais tive a honra de conviver durante minha formação nesta Universidade.

Agradeço ao Ministério Público Federal, em especial a os colegas da Procuradoria Regional da República da 4ª Região (PRR4) e da Assessoria Nacional em Perícias de Tecnologia da Informação e Comunicação (ANPTIC). Frequentar esta Faculdade de Direito fez eu compreender melhor a importância de nosso trabalho como *custos legis*.

Agradeço aos colegas do grupo de pesquisa em Neurociências e Direito Penal, com quem eu tenho aprendido bastante ao longo dos anos. Sou grato especialmente ao Professor Ângelo Ilha, nosso coordenador, pelas oportunidades em participar do grupo de pesquisa, trabalhar como monitor, tutor e conteudista em suas disciplinas e ter acesso a suas publicações - as quais foram fundamentais para a realização deste trabalho.

Por fim agradeço aos amigos, novos e antigos. Mas em especial ao meu amigo de longa data, Dr. Marcos Eduardo dos Santos, por ter sido o grande incentivador para eu estudar Direito. E às minhas colegas de curso Mariana Wengler de Oliveira e Natália Fraga Maciel, a quem tenho a satisfação de acompanhar desde o meu primeiro dia de aula nesta Faculdade de Direito e por quem tenho um carinho enorme.

RESUMO

O presente trabalho tem por objetivo estudar como a teoria do domínio do fato pode ser aplicada para os crimes cometidos em ataques cibernéticos por meio de *ransomware*. Esse tipo de delito, por sua vez, ocorre quando usuários maliciosos sequestram o acesso ou a arquivos ou a recursos computacionais de organizações exigindo o pagamento de um resgate. Tal situação refere-se aos incidentes de segurança da informação ocorridos entre os anos de 2020 a 2021 em vários tribunais brasileiros incluindo STJ, TSE, TJPE e mais recentemente TJRS. Levando em conta aspectos técnicos na área de Ciência da Computação, teremos que dentro da concepção de Claus Roxin existirá um concurso de pessoas com três tipos de agentes: a) usuários maliciosos (ou *hackers*) agindo na forma de autoria indireta (ou mediata), exercendo uma posição de domínio "final" do fato típico; b) usuários das máquinas (ou *hosts*) comprometidas em decorrência das ações de usuários maliciosos sendo usados como meros instrumentos na forma de domínio da vontade e agindo em erro; e c) organizações especializadas em prestar apoio material para usuários maliciosos empreenderem esse tipo de ação, as quais podem ser consideradas: 1) cúmplices dos usuários maliciosos para o crime de invasão de dispositivo informático; 2) coautoras dos usuários maliciosos na forma do domínio funcional para o crime de extorsão; e 3) autoras para o crime de associação criminosa, sem o prejuízo de enquadramento da conduta em outros tipos penais conforme forem as circunstâncias.

Palavras-chave: Direito Penal. Crimes Cibernéticos. *Ransomware*. Concurso de pessoas. Autoria e participação. Teoria do Domínio do Fato.

ABSTRACT

This work aims to study about how the theory of fact domain can be applied to crimes committed during cyberattacks by way of ransomware. This species of delict, in turn, occurs when malicious users kidnaps access to computer files and resources demanding ransom payment. Its refers to information security incidents occurred between years of 2020 and 2021 in several brazilian courts including STJ, TSE, TJPE and more recently TJRS. Taking into consideration technical aspects concerning Computer Science area, accordingly with Claus Roxin conception we'll gonna have three kind of agents acting concurrently: a) malicious users (aka hackers) accordingly to indirect (or mediated) mode of authorship, holding a position of "finalistic" dominance of the delituous fact; b) users of machines (or hosts) which was compromised as a result of malicious user attacks being used as mere instruments accordingly to willness domain form and acting in error state; e c) organizations specialized in task of providing material support for malicious users to perform this type of action, which may be considered: 1) accomplices of malicious users in computer device invasion crime; 2) co-authors of malicious users in extortion crime accordingly to functional domain form; e 3) authors in criminal association crime, also being possible to attribute the conduct to other crimes accordingly to circumstances.

Keywords: *Criminal Law. Cybercrimes. Ransomware. Agents Concurrence. Authorship and participation. Theory of Fact Domain.*

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CF	Constituição Federal
CP	Código Penal
CPP	Código de Processo Penal
DNS	*Domain Name System*
DoD	*US Department of Defense*
IP	*Internet Protocol*
MAC	*Media Access Control*
RFC	*Request for Comments*
STF	Supremo Tribunal Federal
StGB	*Strafgezetzbuch*
STJ	Superior Tribunal de Justiça
TCP/IP	*Transmission Control Protocol/Internet Protocol*
TJPE	Tribunal de Justiça do estado de Pernambuco
TJRS	Tribunal de Justiça do estado do Rio Grande do Sul
TSE	Tribunal Superior Eleitoral
VPN	*Virtual Private Network*

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho aborda a autoria e a participação no âmbito do direito penal brasileiro, visando contribuir para a compreensão adequada do concurso de agentes para os crimes relacionados a ataques cibernéticos do tipo *ransomware*. *Ransomware* é o nome dado aos ataques cibernéticos nos quais usuários maliciosos sequestram o acesso ou aos arquivos, ou aos recursos do ambiente computacional da vítima; exigindo o pagamento de um resgate (do inglês *ransom*).

Tal situação refere-se aos incidentes em segurança da informação[1] ocorridos entre os anos de 2020 e 2021 em vários órgãos do Poder Judiciário brasileiro incluindo-se STJ[2], TSE[3], TJPE[4] e mais recentemente TJRS[5]. De acordo com relatório da empresa Chainalysis, ataques desse tipo renderam aos autores cerca de R$ 2,1 bilhões apenas em 2020[6]. Todavia, esse valor pode ser ainda maior pois inúmeras organizações optam por tratar o assunto com discrição a fim de preservarem sua credibilidade.

O Código Penal adota uma teoria monista temperada, mas o ordenamento jurídico pátrio não faz uma definição das figuras de autor e partícipe. Esse critério é deixado isso a cargo da doutrina. Nesse sentido uma das abordagens mais empregadas é por meio da teoria do domínio do fato, dentro do sistema diferenciador.

Desse modo, levando em conta aspectos técnicos em Ciência da Computação, o objetivo desse trabalho é determinar como cada um dos agentes deve ser punido dentro da concepção de Claus Roxin[7] para a teoria do domínio do fato. Com base nisso é feita uma categorização como autor, coautor, partícipe e instrumento para a situação de cada um dos envolvidos nesse fato delituoso. O entendimento dessas figuras é de importância fundamental,

[1] Um incidente de segurança da informação é indicado por um simples evento ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação (ABNT NBR ISO/IEC 27002:2013, 2013).
[2] (NEOTEL, 2020)
[3] (OLHAR DIGITAL, 2020)
[4] (TILT, 2020)
[5] (ADVISOR, 2021)
[6] (CNN BRASIL, 2021)
[7] (SILVA, 2020, p. 386-390)

uma vez que cada qual traz uma consequência jurídica distinta na aplicação de penas.[8] Essa diferença reside justamente no *quantum* de pena a ser atribuído ou não.[9]

Em ataques cibernéticos do tipo *ransomware* teremos vários crimes relacionados a esse tipo de ação, com três tipos de agentes agindo em concurso de pessoas: a) usuários maliciosos (ou *hackers*[10]) como autores mediatos ou indiretos, possuindo "domínio final do fato" (ou *finalen Tatherrschaff*); b) usuários das máquinas comprometidas nas ações de usuários maliciosos agindo em erro[11], sendo meros instrumentos na forma de domínio da vontade e; e c) organizações especializadas em prestar auxílio material para usuários maliciosos empreenderem ações desse tipo, tal como a REvil[12], as quais podem ser consideradas: 1) cúmplices dos usuários maliciosos para o crime de invasão de dispositivo informático[13]; 2) coautoras dos usuários maliciosos para o crime de extorsão[14] na forma do domínio funcional; e 3) autoras para o crime de associação criminosa[15], sem o prejuízo do enquadramento de sua conduta em outros tipos penais.

A Internet é uma rede de computadores onde o mecanismo principal para identificação unívoca de seus elementos constituintes (ou *hosts*[16]) são os endereços IP. Desse modo observa-se reiteradamente na doutrina, legislação e jurisprudência o entendimento de que

---

[8] Em observância ao princípio de individualização da pena (SILVA, 2020, p. 53), insculpido no inciso XLVI, artigo 5º, CF.

[9] É o que nos informa o art. 29, caput, CP: "quem, de qualquer modo, concorre para o crime incide nas penas a este cominadas, na medida de sua culpabilidade". Em seguida, o parágrafo primeiro do referido dispositivo consagra: "se a participação for de menor importância, a pena pode ser diminuída de um sexto a um terço".

[10] Esse trabalho considera a palavra *hacker* no sentido usualmente empregado pelos meios de comunicação como sendo autor de crimes virtuais. Todavia essa definição não é correta, pois *hacker* é qualquer pessoa quem se dedique intensamente em alguma área específica da computação e eventualmente descubra utilidades além daquelas previstas nas especificações de sistemas – não necessariamente brechas de segurança. (MCCLURE, SCAMBRAY e KURTZ, 2017, p. 29)

[11] "Roxin desenvolve uma teoria escalonada dos vários erros que fundamentam autoria mediata, que vão desde o erro de tipo até o erro de proibição evitável". (GRECO (ORG.), LEITE, *et al.*, 2014, p. 26)

[12] "O REvil não é um *ransomware* operado por uma pessoa ou uma gangue. Na verdade trata-se de uma plataforma de *ransomware* cujo autor ou autores vendem o acesso a quem quiser. Ele já atacou empresas grandes tal como a Quanta Computer - fornecedora terceirizada da Apple em Taiwan e que, na verdade, é uma das maiores fabricantes de laptops do mundo." (ADVISOR, 2021)

[13] CP, 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:".

[14] CP, art. 158, *caput*: "Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa. Pena - reclusão, de quatro a dez anos, e multa". Sendo que: "§ 1º - Se o crime é cometido por duas ou mais pessoas, ou com emprego de arma, aumenta-se a pena de um terço até metade"

[15] CP, art. 288, *caput*: "Associarem-se 3 (três) ou mais pessoas, para o fim específico de cometer crimes. Pena - reclusão, de 1 (um) a 3 (três) anos"

[16] A definição de *host* refere-se a máquina conectada na Internet, e será tratada em detalhes na seção 4.1.1

endereços IP (ou *IP Addresses)* constituem vestígio[17] bastante importante com relação a autoria de crimes cibernéticos.

Há uma tendência bastante forte de que endereços IP sejam usados como vestígio de autoria direta ou imediata. Todavia esse trabalho salienta de que em ataques cibernéticos do tipo *ransomware* estarão envolvidos endereços IP de agentes agindo em concurso.

Além disso é preciso considerar que atualmente 65% dos *hosts* conectados à Internet no Brasil ainda empregam o protocolo de rede IPv4[18]. Isso representa uma dificuldade para determinação da autoria, posto que endereços do tipo IPv4 não contém nenhuma informação relacionada ao *host* de origem. Ao passo que endereços do tipo IPv6 mantém dados do endereço de nível físico (ou MAC), sendo mais confiáveis[19].

Com relação ao método de pesquisa, primeiramente esse trabalho realizou pesquisa bibliográfica nas áreas de Ciência da Computação e Direito. Isso foi essencial para uma fundamentação precisa dos conceitos apresentados. Foi utilizada a pesquisa qualitativa para compreender os crimes cibernéticos a fim de criar um processo e uma linha de raciocínio a ser seguida, adotando-se o método dedutivo para chegar até os ataques do tipo *ransomware*.

O primeiro capítulo apresenta uma fundamentação teórica acerca do concurso de pessoas. Nesse ponto são trabalhados os requisitos do concurso de pessoas, autoria e participação, formas de autoria e a participação *strico sensu* por instigação e cumplicidade.

O segundo capítulo fala sobre a teoria do domínio do fato: suas origens e as concepções de Hans Welzel e Claus Roxin. Dentro da concepção de Roxin, é feita uma discussão em torno das três formas de domínio, a saber: domínio da ação, domínio da vontade e domínio funcional. [20 e 21]

No terceiro capítulo são apresentados conceitos essenciais para o entendimento deste trabalho envolvendo redes de computadores e Internet. Dentro do modelo de referência TCP/IP, é feita uma descrição das funções do nível de rede e dos protocolos IPv4 e IPv6 em

[17] CPP, art. 158-A, § 3º, "Vestígio é todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal"
[18] (APNIC, 2021)
[19] Tanto no *link-local* quanto no ULA (IPV6.BR, 2012)
[20] (ALFLEN, 2014)
[21] (GRECO (ORG.), LEITE, *et al.*, 2014, p. 19-45)

seus esquemas de endereçamento.[22] Também é feita uma discussão acerca do tratamento dispensado em nosso ordenamento jurídico aos endereços IP na legislação e na jurisprudência.

No quarto capítulo são feitas definições a respeito de crimes cibernéticos. Aqui também é feita uma análise dos crimes cibernéticos do tipo r*ansomware* em seus aspectos técnico e jurídico.

Por fim, na conclusão são feitas indicações de tópicos nos quais esse trabalho pode vir a ser estendido futuramente. Também são feitas ponderações acerca do tratamento dispensado para essa classe de delito no ordenamento jurídico brasileiro, ainda mais levando-se em conta o fato de que o Brasil é participante da Convenção de Budapeste[23] e, por força deste tratado, deve adequar sua legislação e adotar estratégias conjuntas de enfrentamento de crimes praticados na Internet.

[22] (TANENBAUM e WETHERALL, 2011)
[23] (BRASIL, 2020)

2 CONCURSO DE PESSOAS

Este capítulo trata sobre o concurso de pessoas. São apresentados os requisitos para o concurso de pessoas, bem como as figuras centrais do concurso de agentes: autoria e participação. Busca-se estabelecer uma diferença entre ambas, apresentar o conceito e as formas de autoria bem como a participação em sentido estrito (ou *stricto sensu*).

2.1 Sobre o concurso de pessoas

O concurso de agentes é um dos assuntos mais difíceis e polêmicos na doutrina jurídica do delito. O assunto encontra-se representado no CP dentro do "Título IV – Do Concurso de pessoas", em seus arts. 29 a 31, desde a Reforma da Parte Geral de 1984. A expressão concurso de pessoas abrange as formas delitivas em que haja a concorrência de mais de um agente.

"O concurso de pessoas pode ser de mais de um autor (coautoria), um autor e um partícipe (admitindo também vários partícipes) ou, ainda, diversos autores concorrendo com um ou vários partícipes". [24] Até a Reforma de 1984, a redação no CP de 1940 abordava o assunto no "Título IV – Da Co-Autoria" em seus arts. 25 a 27, pelo qual tratava todos os concorrentes de um crime como coautores. Isso deve-se ao fato de orientar-se por um critério conhecido como causal-extensivo, subjetivo-causal ou extensivo dentro da teoria unitária[25] por uma escolha do legislador. Esse entendimento não era o ideal porque não contemplava a participação *stricto sensu* (instigação e cumplicidade).

2.2 Requisitos do concurso de pessoas

2.2.1 Identidade de infração penal

Só pode existir concurso de pessoas em relação a uma obra comum, a um fato punível. Isso porque em doutrina fala-se em uma concepção monista (monística ou unitária) do concurso de pessoas. Tanto é que a própria expressão monismo diz respeito "com o título de

[24] (SILVA, 2020, p. 376)
[25] (SILVA, 2020, p. 382-383)

imputação em delitos praticados por vários intervenientes".[26] Portanto, monismo significa que todos os concorrentes (quer sejam autores, quer sejam partícipes) responderão pelo mesmo crime. Todavia é importante que o CP possibilita excepcionalmente, no concurso de pessoas, que determinado concorrente responda por crime menos grave[27].

2.2.2 Pluralidade de agentes

Trata-se de requisito imprescindível à caracterização do concurso de pessoas. É intuitivo e decorre logicamente a necessidade de mais de um agente[28].

2.2.3 Assunção subjetiva para o empreendimento delitivo comum

O acordo de vontades, o *pactum sceleris,* ou vínculo subjetivo é outro requisito a caracterizar o concurso de pessoas.[29] Um exemplo desse tipo de associação é aquela que acontece entre *hackers* e organizações que oferecem apoio material para a realização de ataques do tipo *ransomware*.

2.2.4 Relevância causal das condutas

Para que haja concurso de pessoas, a conduta do participante deve concorrer[30] para dar causa ao crime[31]. Isso significa que se a conduta não contribuir para a geração do resultado, então ela não será passível de incriminação. [32]

2.3 Autoria e participação

O Código Penal brasileiro não fornece os conceitos de autoria e participação. Entretanto temos que autoria[33] é o conceito central a partir do qual são formulados outros conceitos tais da autoria em suas variadas formas (direta, mediata, coautoria e colateral), bem

---

[26] (GRECO (ORG.), LEITE, *et al.*, 2014)
[27] CP, art. 29, "Se algum dos concorrentes quis participar de crime menos grave, ser-lhe-á aplicada a pena deste; essa pena será aumentada até metade, na hipótese de ter sido previsível o resultado mais grave"
[28] (SILVA, 2020, p. 399)
[29] (SILVA, 2020, p. 399)
[30] CP, art. 29, "Quem, de qualquer modo, concorre para o crime incide nas penas a este cominadas, na medida de sua culpabilidade."
[31] CP, art. 13, caput, "O resultado, de que depende a existência do crime, somente é imputável a quem lhe deu causa. Considera-se causa a ação ou omissão sem a qual o resultado não teria ocorrido"
[32] (SILVA, 2020, p. 399)
[33] *Apud* (SILVA, 2015, p. 38)

como de participação em sentido estrito (instigação e cumplicidade).[34] Em matéria de concurso de pessoas, a autoria é autônoma ao passo que a participação é acessória. Vale dizer que só existirá participação punível se houver ao menos um autor de fato tipificado como crime.[35]

2.3.1 Autoria

Para obter uma compreensão a esse respeito é preciso ter em conta que a diferenciação das pessoas quem contribuem para a realização de uma obra comum é algo que decorre da natureza das coisas. Desse modo temos que se um pedreiro constrói uma casa, valendo-se do auxílio de alguém encarregado de comprar o material de construção, não se pode dizer que este último construiu a casa. Transpondo essa ideia para o direito penal, autor é aquele quem pratica o fato ao passo que o partícipe contribui para o fato sem ser o autor.

Desse modo, em que pesem discrepâncias observadas nas legislações consideradas dentre as mais atuais, teremos que *autor* será aquele quem realiza o fato: a) por si mesmo, como no caso de quem desfere tiros (autoria direta ou imediata); b) por intermédio de outrem, como no caso do agente que vale de alguém não culpável, denominado instrumento (autoria indireta ou mediata); em conjunto e em acordo com outro autor ou outros coautores (coautoria); ou, d) de forma concomitante com outro ou outros autores sem estar em uma relação de coautoria em face da ausência de acordo, ou *pactum sceleris* (autoria colateral)[36].

2.3.2 Participação

Há de se distinguir entre a participação em sentido amplo (ou *lato sensu*), a qual vem da idéia de “tomar parte” no empreendimento delitivo; daquela participação em sentido estrito (ou *stricto sensu*), a qual compreende a instigação e a cumplicidade.

Instigador é aquele quem determina a prática do crime. Entretanto a doutrina brasileira faz distinção entre induzimento e instigação. “O induzimento ocorreria quando o indutor faz nascer no autor o propósito delitivo, ao passo que a instigação se daria quando o autor já estivesse predisposto à prática do crime e o instigador viesse tão somente a reforçar tal

[34] (SILVA, 2020, p. 377)
[35] (SILVA, 2020, p. 398)
[36] (SILVA, 2020, p. 378)

intento".[37] Essa distinção pode ser encontrada na fórmula de tipificação do crime de induzimento, instigação ou auxílio ao suicídio.[38]

Por sua vez, cúmplice é o partícipe que presta auxílio ou material, ou moral de forma dolosa para a prática de crime doloso por outrem (neste caso, o autor). Auxílio material é aquele em que, por exemplo, o cúmplice fornece a arma para o autor cometer homicídio – mas não pratica a conduta prevista no tipo penal. O auxílio moral ocorre quando, por exemplo, o cúmplice ensina o autor a fazer uma substância tóxica possibilitando ao autor cometer homicídio por envenenamento.

[37] (SILVA, 2020, p. 378)
[38] CP, art. 122

3 TEORIA DO DOMÍNIO DO FATO

Este capítulo trata sobre a teoria do domínio do fato. Aborda seu conceito, as concepções de Hans Welzel e de Claus Roxin com relação aos delitos de domínio.

3.1 Origens

A teoria do domínio do fato é uma resposta a um problema concreto sobre distinguir entre autor e partícipe. Ela é aplicável aos crimes dolosos e possui mais de diversas concepções incluindo-se as de Welzel, Maurach, Gallas e Roxin.

Por seu intermédio não se busca determinar se um agente será punido ou não, e sim se o será ou como autor, ou como mero partícipe. Os códigos penais alemães exigem que se faça essa distinção.[39] Neste sentido vide a tradução sobre autoria (ou *Täterschaft*) do Código Penal Alemão (ou Strafgezetzbuch StGB)[40]:

> *§ 25. Autoria*
> *(1) Será punível como autor quem cometer fato punível por si ou por meio de outrem*
> *(2) Se vários cometerem o fato punível em comum, cada um será punido como autor (coautor)*
> *§ 26. Instigação*
> *Será igualmente punido como autor, quem dolosamente determinou a outrem o cometimento de um fato típico e doloso.*
> *§ 27. Cumplicidade*
> *(1) Será punido como cúmplice quem dolosamente presta auxílio a outrem para o cometimento de um fato ilícito doloso.*
> *(2) A pena para o cúmplice é determinada com base na pena prevista para o autor. A pena deve ser reduzida conforme o § 49, inciso I.*

A expressão domínio do fato foi usada pela primeira vez por August Hegler em 1915, mas não possuía a conotação atual. Na época estava mais atrelada aos fundamentos da culpabilidade e não era critério para divisar a autoria da participação *stricto sensu.*

[39] (GRECO (ORG.), LEITE, *et al.*, 2014, p. 22)
[40] (GRECO (ORG.), LEITE, *et al.*, 2014, p. 22)

3.2 Concepção de Hans Welzel

A primeira formulação da ideia central da teoria do fato no plano da autoria ocorreu efetivamente em 1933, por Lobe. Entretanto apenas produziu eco quando Welzel mencionou-a em um estudo de 1939 no trabalho intitulado *Studiem zum Sytem des Strafrechts*[41], referindo-se a um domínio final do fato como critério determinante de autoria[42].

Welzel estabeleceu que autor final, diversamente do partícipe, é o senhor e dono da decisão e da execução, dono e senhor do "seu" fato, ao passo que o partícipe não possui domínio sobre o fato criminoso, possuindo tão somente um certo domínio sobre sua contribuição. Dentro de sua perspectiva de conduta como atividade final, Welzel refere-se ao autor como aquele que possui o "domínio final do fato" (*finalen Tatherrschaft*).[43]

Em síntese, para Welzel, nos crimes dolosos o autor possui as seguintes características: 1) característica geral: o domínio final do fato; 2) características especiais, tais como: a) subjetivo-pessoais: as quais consistem em intenções especiais, tendências ou tipos de ânimos; e b) objetivo-pessoais: como a posição especial de dever o autor, em certos crimes.[44]

3.3 Concepção de Claus Roxin

Atualmente a concepção mais debatida é a de Roxin, publicada em 1963. "Deve-se a Roxin um acatado delineamento das diversas formas de domínio (ao lado de construção específica para os delitos de infração de dever e de mão própria). Para o autor, nos delitos de domínio, ele dá-se fundamentalmente de três formas, quais sejam, domínio da ação, domínio da vontade e domínio funcional, sendo por isso denominado de concepção tripartida".[45]

3.3.1 Domínio da ação

De acordo com a doutrina de Roxin, o domínio da ação (ou *Handlungsherrschaft*) está presente na autoria imediata ou direta. Ou seja, nos casos em que o autor executa o fato ele

---

[41] (GRECO (ORG.), LEITE, *et al.*, 2014, p. 21)
[42] (GRECO (ORG.), LEITE, *et al.*, 2014, p. 11)
[43] (SILVA, 2020, p. 386)
[44] (SILVA, 2020, p. 387)
[45] (SILVA, 2020, p. 387)

mesmo. Trata-se da hipótese do StGB, § 25, item 1[46]. Nesse ponto é muito importante trazer a lume as palavras de Roxin[47].

3.3.2 Domínio da vontade

Domínio da vontade (ou *Willensherrschaft*) ocorre nos casos de autoria mediata ou indireta, valendo-se o autor de um executor material reduzido a mero instrumento. As razões desse tipo de domínio são fundamentalmente três: a) a coação exercida sobre o homem da frente, algo a que Roxin chama de princípio da responsabilidade (ou *Verantwortungsprinzip*) ao exculpá-lo em certos casos de coação[48]; b) o segundo grupo de razões para autoria mediata está no erro, escalonados por Roxin desde o erro de tipo até o erro de proibição evitável; e c) aparato organizado de poder, para aquele servindo-se de uma organização que seja: 1) verticalmente estruturada; 2) apartada do Direito; e 3) fungibilidade dos executores.

3.3.3 Domínio funcional

"O domínio funcional é aquele que se refere à coautoria, em que diversos (co)autores, em repartição de tarefas, realizam a execução comum, de uma decisão comum, em que cada coautor determina sua respectiva parte na execução do crime".[49] Consiste em uma ação coordenada, com pelo menos mais uma pessoa. Se duas ou mais pessoas, partindo de uma decisão conjunta de praticarem o fato, contribuírem para a sua realização com um ato relevante de um delito, elas terão o domínio funcional.do fato (ou *funktionaleTatherrschaft*). Isso fará de cada qual coautor do fato como um todo, ocorrendo o que se chama imputação recíproca.[50]

---

[46] No original: *(1). Als Täter wird bestraft, wer die Straftat selbst oder durch einen anderen begeht.*

[47] "Quem aperta o gatilho tem o domínio da ação e nunca poderá ser mero partícipe, ao contrário do que, como vimos, muitas vezes decidirá a jurisprudência alemã, partindo de uma teoria subjetiva extrema. Aquele que domina a ação permanece autor ainda que aja a pedido ou a mando de outrem, ou mesmo em erro de proibição inevitável determinado por um terceiro (StGB, § 17; art. 21 do CP); será um autor exculpado, mas ainda assim autor do fato típico, ainda que não necessariamente o único." (GRECO (ORG.), LEITE, *et al.*, 2014, p. 25)

[48] StGB, § 35 e CP, art. 22

[49] (SILVA, 2020, p. 387)

[50] (GRECO (ORG.), LEITE, *et al.*, 2014, p. 31)

4 REDES DE COMPUTADORES E INTERNET

Este capítulo trata sobre redes de computadores e Internet. É apresentado um histórico sobre o surgimento do modelo de referência TCP/IP, uma descrição das funções do nível de rede e os protocolos IPv4 e IPv6 em seus esquemas de endereçamento. Ao término é feito uma discussão a respeito de como endereços IP são tratados na legislação e jurisprudência brasileiros.

4.1 Rede de computadores

4.1.1 Conceito

Uma rede de computadores é uma associação entre duas ou mais máquinas autônomas (ou *hosts)* interligadas. Neste sentido pouco importa a tecnologia por meio da qual os *hosts* estejam sendo interligados: fibra ótica, *cablemodem*, cabos de par-trançado, cabos coaxiais, microondas, infravermelho e até mesmo via satélite.[51]

4.1.2 Finalidade

A finalidade de uma rede de computadores é compartilhar dados e/ou recursos computacionais. Através do compartilhamento de dados é possível, por exemplo, informar as partes de um processo sobre alguma decisão de modo simultâneo - afetando a contagem de prazos processuais.[52] E ao compartilhar recursos computacionais é possível promover um uso mais racional e eficiente dos mesmos. Por exemplo, uma impressora *laser* é um elemento com custo total de propriedade (de *total cost ownership*, ou *TCO*) elevado devido às despesas com manutenção preventiva, consumo de *toner* e papel. Mas usando a mesma em uma rede de computadores é possível fazer um equipamento desses atender vários usuários.[53]

4.1.3 Segurança

Também é possível melhorar a segurança da informação por meio de uma rede de computadores, reduzindo-se o número de pontos onde deve ser exercido o controle.

[51] (TANENBAUM e WETHERALL, 2011, p. 26)
[52] (ALMEIDA FILHO, JOSÉ CARLOS DE ARAÚJO , 2010)
[53] (TANENBAUM e WETHERALL, 2011, p. 30)

Considerando a existência de componentes com vulnerabilidades[54] em qualquer organização, devem ser implantados controles de segurança[55] a fim de protegê-la de ameaças[56] com base em um processo de gestão de riscos[57]. Usando-se como exemplo um enlace para acesso à Internet, torna-se mais simples coibir abusos com relação aos *downloads* excessivos e eventualmente implantar dispositivos de segurança cibernética tais como *firewalls*[58] e antivírus.

4.1.4 Protocolo de rede (ou *network protocol*)

O simples fato de existir uma interligação entre *hosts* não é condição suficiente para que a comunicação aconteça. A fim de que uma rede de computadores cumpra sua finalidade, é necessário que os integrantes estejam utilizando protocolos de rede compatíveis.

Esses protocolos de rede, por sua vez, consistem em regras e convenções a serem estritamente observadas a fim de que a comunicação ocorra. Caso algum *host* não observe um protocolo de rede, estará impedido de comunicar-se com os demais para usar um serviço.

Um exemplo de protocolo é o DNS, encarregado de traduzir nomes em endereços IP[59]: o protocolo é do tipo *request/reply*, exigindo que seja fornecido um parâmetro de consulta a fim de que seja retornado um endereço IP como sendo a resposta.

4.1.5 Hierarquia de protocolos de rede (ou *protocol hierarchy)*

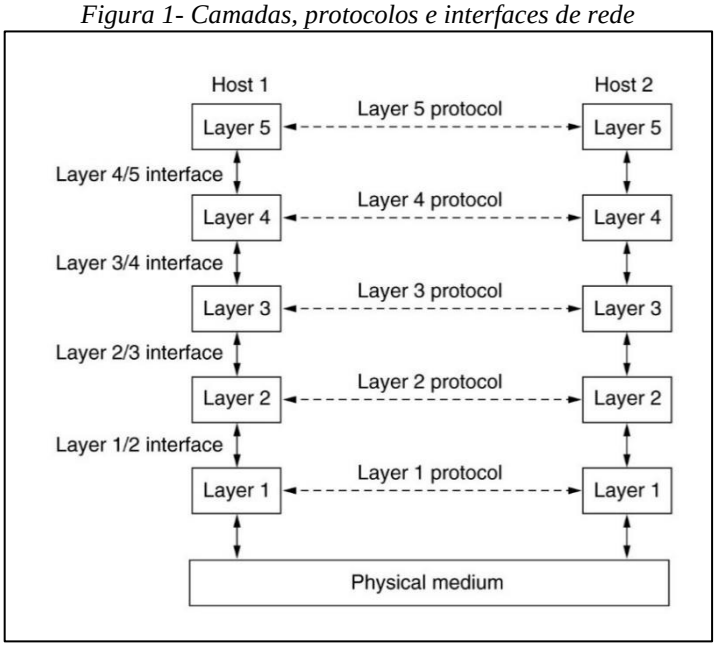
Rede de computadores são organizadas como sendo uma pilha (ou *stack*) de camadas (ou *layers)* ou níveis de abstração (ou *levels*).[60] Logo, a grande diferença entre uma rede de computadores e outra está justamente no número, nome, conteúdo e funções de cada camada.

---

[54] Uma vulnerabilidade "é uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças" (ISO/IEC, 2004, p. 22)
[55] "Um controle de segurança é uma salvaguarda ou contramedida de natureza gerencial, operacional ou técnica, prescrita para um sistema de informações, de modo a proteger a confidencialidade, integridade e disponibilidade do sistema de sua informação". (NIST, 2006)
[56] Uma ameaça "é uma causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização" (ISO/IEC, 2004, p. 22)
[57] Risco de Segurança da Informação] é o "Potencial que uma ameaça explore vulnerabilidades de um ativo ou conjunto de ativos e desta forma prejudique uma organização. Um risco é mensurado em termos de probabilidade de materialização do risco e seus impactos" (ISO/IEC, 2004, p. 18)
[58] Um *firewall* é um dispositivo em um determinado ponto da rede, na forma de um programa ou de equipamento físico, o qual tem por objetivo aplicar uma política de segurança entre ambientes diferentes – geralmente a organização e a Internet (CHAPMAN, ZWICKY e COOPER, 1999)
[59] (TANENBAUM e WETHERALL, 2011, p. 611)

O motivo para o assunto ser tratado dessa forma é diminuir a complexidade, fazendo cada camada implementar um conjunto de serviços a serem oferecidos para as camadas acima usando-se, para isso, dos serviços prestados pela imediatamente camada.[61] Esta situação encontra-se representada na Figura 1- Camadas, protocolos e interfaces de rede:

Figura 1- Camadas, protocolos e interfaces de rede



Fonte: Figura 1-13 (TANENBAUM e WETHERALL, 2011)

Sob o ponto de vista dos *hosts* quem participam da comunicação, cada uma de suas camadas interagindo diretamente com a camada de mesmo nível na contraparte da comunicação por intermédio dos protocolos de rede.

4.1.6 Arquitetura de redes

O conjunto de camadas e protocolos é chamado de arquitetura da rede (ou *network architecture*). A especificação de uma arquitetura de rede deve conter informações o suficiente para permitir a criação de *hardware* e *software* que venham a funcionar adequadamente nessa rede de computadores.

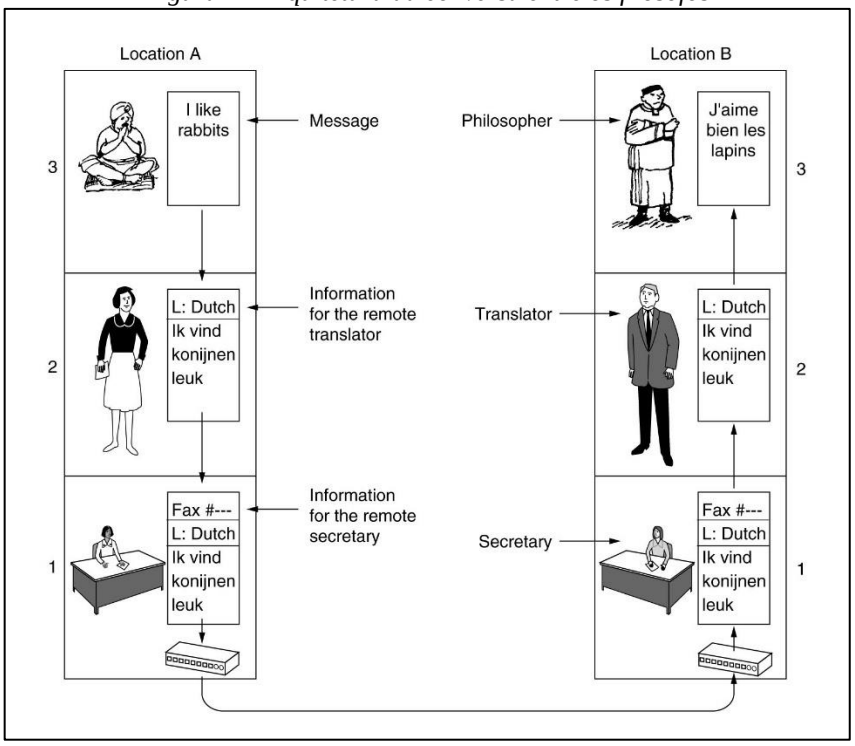
---

[60] "*To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.*" (TANENBAUM e WETHERALL, 2011, p. 53)

[61] *"The purpose of each layer is to offer certain services to the higher layers while shielding those layers from the details of how the offered services are actually implemented. In a sense, each layer is a kind of virtual machine, offering certain services to the layer above it.*" (TANENBAUM e WETHERALL, 2011, p. 53)

A proposta de uma arquitetura de rede dividida em camadas pode ser compreendida melhor fazendo-se uma analogia da conversa entre dois filósofos. Enquanto um deles domina os idiomas urdu e inglês, o outro domina os idiomas francês e chinês. Desse modo, utilizam-se do serviço prestado por tradutores. Esses, por sua vez, utilizam-se do serviço de secretárias para o envio de mensagens por fax. Essa situação está representada na Figura 2 - Arquitetura da conversa entre os filósofos:

Figura 2 - Arquitetura da conversa entre os filósofos



Fonte: Figura 1-14 (TANENBAUM e WETHERALL, 2011)

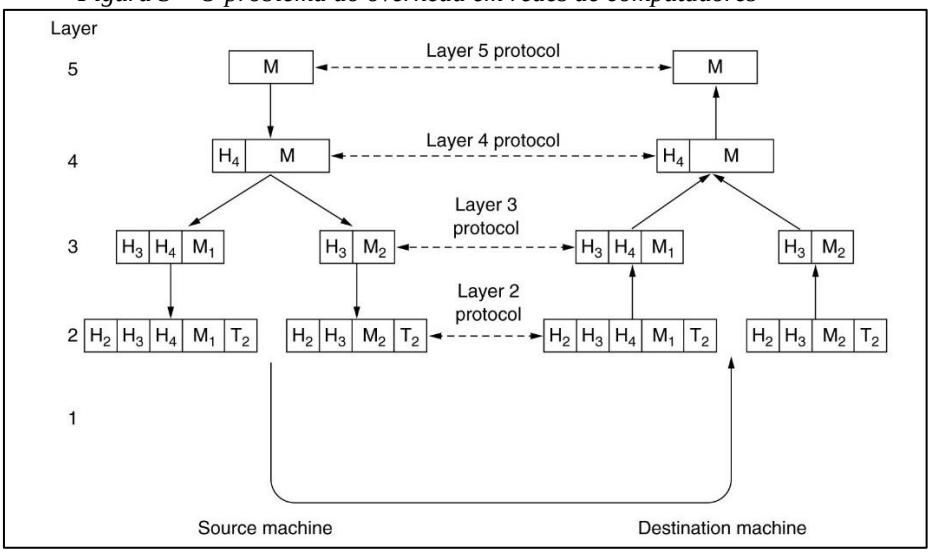
Importante notar que a medida que a mensagem percorre as camadas, cada uma delas acrescenta informações de controle destinadas a sua contraparte no interlocutor: neste exemplo, os tradutores informam que o idioma empregado é o holandês. Na implementação das pilhas de protocolos em redes de computadores reais, essa informação é implementada ou como sendo predecessora (ou *header*) ou sucessora (ou *trail*), constituindo elemento indispensável para a comunicação entre as camadas nos *hosts* adjacentes.

Embora a presença de informações de controle seja indispensável para a comunicação entre as camadas dos *hosts*, a existência de um volume muito grande pode afetar o desempenho. Essa informação redundante é denominada *overhead* da comunicação, eventualmente representando uma parcela considerável de todo o volume de tráfego.

Para transmitir uma mensagem M entre origem e destino, existe a necessidade de atravessando camadas existentes na arquitetura de rede dos *hosts*. Informações de controle na forma de prefixos e sufixos vão sendo adicionados a essa mensagem M a medida que ela é remetida para as camadas inferiores. E quando o conteúdo é recebido no destinatário, as informações de controle vão sendo removidas a medida que a mensagem M é remetida para as camadas superiores.

A existência das informações de controle intercaladas ao longo das camadas é algo de relevância para a área jurídica, especialmente em Direito do Consumidor. E isso porque as ofertas dos provedores de conexão induzem a erro na medida que fazem referência a uma vazão na perspectiva da camada mais baixa de todas: em um anúncio de Internet operando a 100 Mbps, na realidade significa um tráfego fluindo em cerca de 60 Mbps devido à existência do *overhead*. Esta situação encontra-se representada na Figura 3 – O problema do overhead :

Figura 3 – O problema do overhead em redes de computadores



Fonte: Figura 1-15 (TANENBAUM e WETHERALL, 2011)

4.2 Modelos de referência

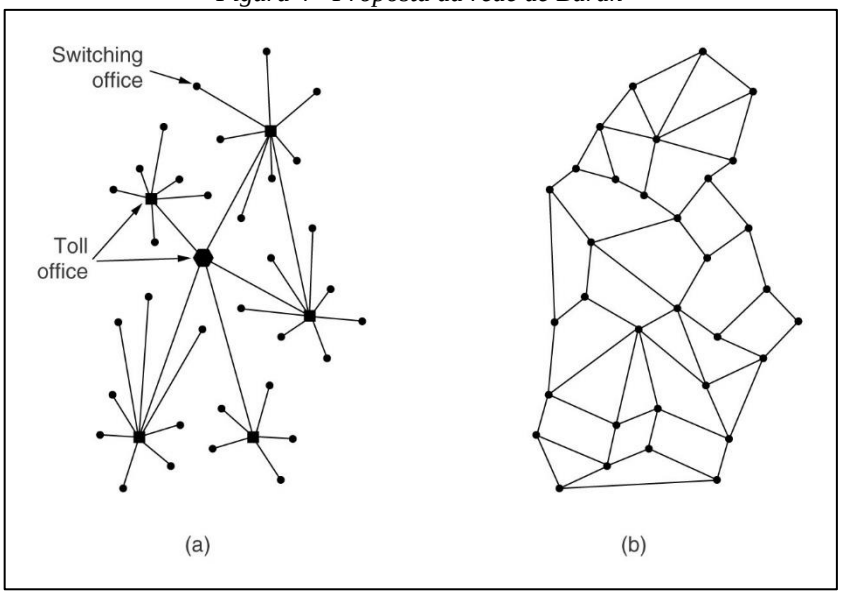
Apesar de existirem uma infinidade de arquitetura de redes, existem duas que representam os assim chamados modelos de referência principais: OSI e TCP/IP. O modelo de referência OSI é meramente teórico e não possui nenhuma implementação, mas o modelo de referência TCP/IP é aquele empregado pela Internet.

4.2.1 Breve histórico do modelo de referência TCP/IP

O modelo de referência TCP/IP teve origem dentro de um período histórico denominado Guerra Fria, o qual ocorreu na segunda metade do século XX. Nessa época havia uma animosidade muito grande entre as maiores potências militares da época, EUA e URSS. Em vista disso surgiu o temor nos EUA de que a eventualidade de um ataque nuclear viesse a comprometer sua capacidade de comunicação de longa distância.[62]

E de fato, na Figura 4 - Proposta da rede de Baran, para impossibilitar a comunicação na parte a bastaria que algum dos pontos de comutação (ou *toll offices*) fosse atingido. Desse modo, por volta de 1960 o DoD contratou a empresa RAND Corporation para que resolvesse esse problema. Jim Baran elaborou uma solução, a qual empregava enlaces redundantes para criar um cenário tolerante a falhas. Essa técnica foi denominada rede de Baran e está representado na parte b.

Figura 4 - Proposta da rede de Baran



Fonte: Figura 1-25 (TANENBAUM e WETHERALL, 2011)

Baran propôs a mudança no modelo de comunicação do tipo orientada a conexão (ou *connection-oriented*) para orientada a pacote (ou *packet oriented*). Entretanto, embora a proposta de Baran agradasse ao DoD ela não foi aceita pela AT&T[63]. A empresa alegou que a implantação teria custos elevados e não iria funcionar, fazendo a ideia de Baran ficar de lado.

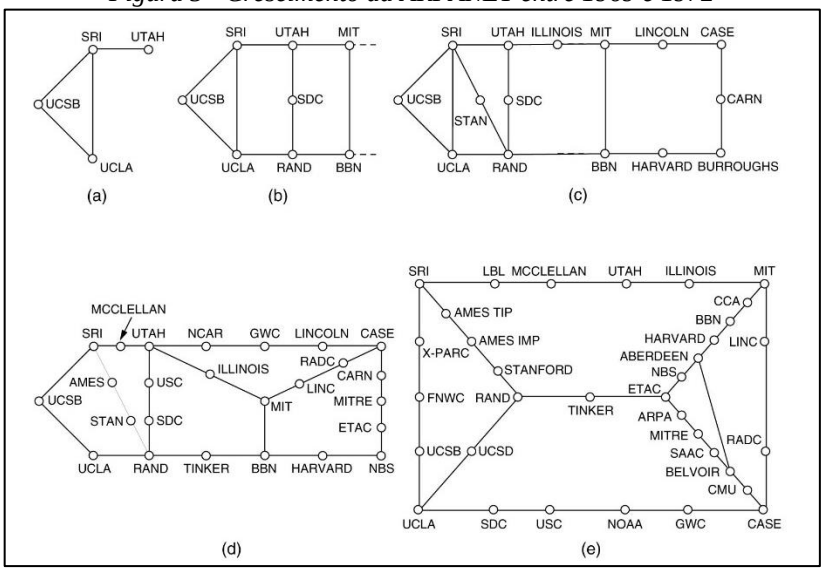
[62] (TANENBAUM e WETHERALL, 2011, p. 79)
[63] Essa organização detinha praticamente o monopólio da comunicação de longa distância dos EUA na década de 70.

Logo após o lançamento do satélite Sputnik pelos soviéticos em 1957, o presidente norte-americano Eisenhower determinou a criação de uma agência de pesquisa destinada a atender as demandas das forças armadas e desse modo surgiu a *Advanced Research Projects Agency* (ou ARPA). A ARPA não possuía cientistas ou laboratórios, mas atuava por meio de parcerias com a comunidade acadêmica.

Em 1967 um de seus integrantes da ARPA chamado Larry Roberts precisou interligar computadores. Foi Wesley Clark quem sugeriu usarem o modelo de conexão orientada a pacotes de Baran. Ele redigiu um artigo a respeito desse experimento e quando apresentaram o mesmo no evento *ACM SIGOPS Symposium on Operating System Principles* ocorrido em Gatlinburg descobriram que a proposta de Baran funcionava e já estava sendo usada por Donald Davies no *National Physical Laboratory* da Inglaterra.

Desse modo houve início a ARPANET, interligando computadores do tipo IMP. Inicialmente ela estava limitada apenas a uma sala, mas logo estendeu-se para as instituições que atuavam em parceiras com a ARPA. O número de participantes cresceu vertiginosamente ao longo de apenas 3 anos conforme demonstrado na Figura 5 - Crescimento da ARPANET entre 1969 e 1972, onde esse é o número de participantes em (a) dezembro de 1969, (b) julho de 1970, (c) março de 1971, (d) abril de 1972 e (e) setembro de 1972.

Figura 5 - Crescimento da ARPANET entre 1969 e 1972



Fonte: Figura 1-27 (TANENBAUM e WETHERALL, 2011)

Em última análise a ARPANET era uma rede de computadores formada pela interligação das redes de computadores de várias outras organizações. Seus protocolos

funcionavam bastante bem ao permitirem a interligação das redes de computadores de várias organizações por meio de enlaces com vazão de 56 kbps, conforme demonstrado na Figura 6.

Entretanto começaram a surgir problemas quando enlaces de vazão maior começaram a ser empregados, baseados em tecnologias de transmissão via satélite e ondas de rádio. Desse modo foram feitos ajustes em protocolos da ARPANET e o modelo TCP/IP surgiu em 1974[64]. Posteriormente os protocolos desse modelo TCP/IP tornaram-se um padrão Internet[65].

Em resumo foi essa arquitetura da rede da ARPANET, com alguns ajustes, que serviu de base para a Internet tal como conhecemos hoje. O cenário atual é de uma rede de computadores com extensão planetária formada pela interligação das redes de computadores de várias organizações (ou *Autonomous Systems*) segundo o modelo de referência TCP/IP.

A Internet originou-se de uma rede de computadores projetada para interligar poucos participantes, entre os quais havia confiança e parceria. Em contrapartida atualmente a Internet possui bilhões de *hosts* interligados, os quais lidam com dados sensíveis.

O fato de a segurança da informação não ter sido uma premissa no projeto da arquitetura de rede que deu origem à Internet é vários problemas, especialmente com relação a ameaças de usuários maliciosos como *hackers*[66]. Esses indivíduos podem vir a comprometer uma organização com relação a seus dados, recursos computacionais e reputação.[67]

4.3 Nível de rede (ou *internet*)

Dentro do modelo de referência TCP/IP, quando existe a necessidade de comunicação entre *hosts* o nível de rede possui a função de dividir o conteúdo recebido do nível de transporte em datagramas e fazer a transmissão entre origem e destino. O nível de rede mantém um esquema para endereçamento dos *hosts* e conhece as rotas para fazer o encaminhamento dos datagramas de modo que cada um deles trafega de modo independente em relação aos demais.

---

[64] (CERF e KAHN, 1974)
[65] Uma vez que algo é definido como sendo um padrão para uso na Internet, a descrição é publicada em documentos denominados Request for Comments (ou RFCs). Desse modo é possível para outros indivíduos e organizações fazerem implementações capazes de interagir via rede de computadores. Para que isto seja possível, basta seguir à risca as especificações contidas nas RFCs.
[66] (MCCLURE, SCAMBRAY e KURTZ, 2017)
[67] (CHAPMAN, ZWICKY e COOPER, 1999, p. 18)

Fazendo-se uma analogia, pode-se dizer que o conteúdo recebido do nível de transporte é um relatório com várias folhas. Elas deverão ser enviadas pelo nível de rede que, para fazer isso, divide-o em várias cartas. Logo, pouco importa o caminho percorrido pelos envelopes desde que estes cheguem até o destino.

Eventualmente podem vir a ocorrer contratempos relacionados com o envio de datagramas: a) alguns deles podem chegar ao destino em uma sequência diferente daquela de onde partiram, posto que percorrem caminhos distintos e algumas rotas podem estar transmitindo mais rapidamente; b) as máquinas intermediárias podem estar com recursos insuficientes para encaminhar os datagramas (congestionamento); e c) alguns datagramas podem vir a ser extraviados, sendo preciso identificar isso e solicitar o reenvio.

4.4 Protocolos de rede IPv4 e IPv6

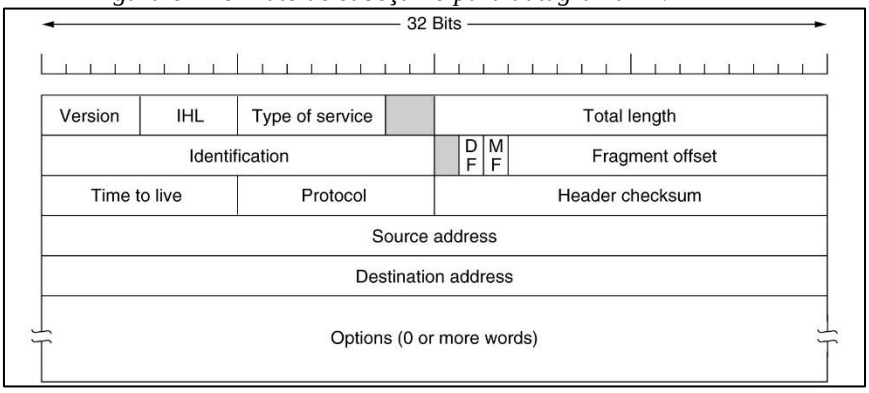
Na Internet o protocolo usado como sendo um padrão *de facto* para a comunicação é o IP (de *Internet Protocol*) em suas versões 4 e 6. Ele encontra-se devidamente especificado nas RFCs 791 e 2460, bem como várias outras. Há uma série de diferenças entre ambos, mas para o escopo desse trabalho interessa o esquema de endereçamento: o modo como os *hosts* são identificados. Os datagramas IP referenciados na seção anterior colocam o endereço IP organizados em palavras de 32 bits.

4.4.1 Esquemas de endereçamento

No protocolo IPv4 o campo do cabeçalho reservado para o endereçamento possui 32 bits e isso permite um máximo de 4.294.967.296 (2^{32}) endereços distintos. Na época de seu desenvolvimento, esta quantidade era considerada suficiente para identificar todos os computadores na rede e suportar o surgimento de novas sub-redes.

Dentro do datagrama IP, o protocolo IPv4 atribui o valor 4 no campo *version* e utiliza apenas 1 palavra de 32 bits para os campos *source address* e *destination address* conforme consta na Figura 6 - Formato de cabeçalho para datagrama IPv4:

Figura 6 - Formato de cabeçalho para datagrama IPv4

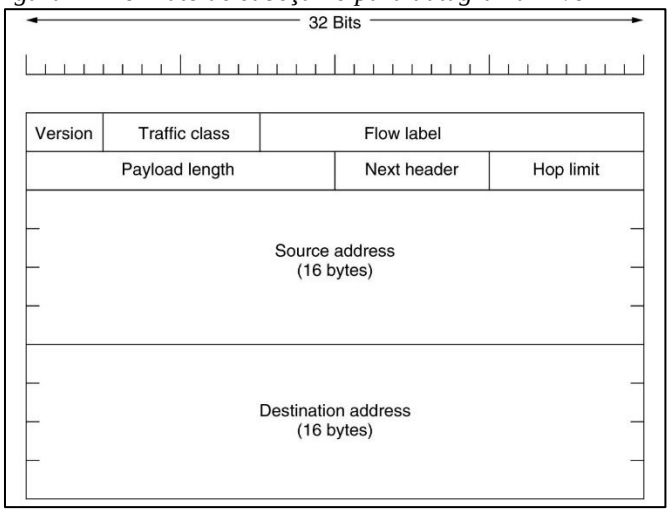


Fonte: Figura 5-53 (TANENBAUM e WETHERALL, 2011)

No entanto, com o rápido crescimento da Internet, surgiu o problema da escassez dos endereços IPv4, motivando a criação de uma nova geração do protocolo IP. O IPv6 utiliza um espaço para endereçamento de 128 bits, podendo obter 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços distintos (2^{128}).

Dentro do datagrama IP, o protocolo IPv6 atribui o valor 6 no campo *version* e utiliza apenas 4 palavras de 32 bits para os campos *source address* e *destination address* conforme consta na Figura 7 - Formato de cabeçalho para datagrama IPv6:

Figura 7 - Formato de cabeçalho para datagrama IPv6



Fonte: Figura 5-68 (TANENBAUM e WETHERALL, 2011)

Este esquema de endereçamento possibilita aproximadamente 79 octilhões ($7{,}9 \times 10^{28}$) de vezes a quantidade de endereços IPv4 e representa, também, mais de 56 octilhões ($5{,}6 \times 10^{28}$) de endereços por ser humano na Terra - considerando-se uma população estimada em 6 bilhões de habitantes.

4.4.2 Configuração do protocolo IP

Para que a comunicação aconteça é necessário que um endereço IP seja único dentro de um espaço de endereçamento. Neste sentido é importante ter em conta que conforme for a versão do protocolo IP ela será quase que totalmente parametrizável por *software*. Para que um *host* consiga comunicar-se ele precisa possuir ao menos três elementos configurados: a) um endereço IP que seja único no ambiente de rede; b) uma máscara de sub-rede; e c) um *gateway default*.

A fim de realizar esses ajustes existem duas possibilidades: a) isso pode ser feito através das opções de configuração da rede, existentes no sistema operacional dos *hosts*; ou b) uso de protocolos como o *Dynamic Host Configuration Protocol (DHCP)* e o *Bootstrap Protocol (bootp)* para ajustarem todos os *hosts* de uma rede de computadores. Somente a partir do momento em que um *host* dispor de configurações de rede apropriadas ao ambiente do qual participa será possível a este comunicar-se usando uma infraestrutura.

Uma vez configurado, o *host* pode usar os recursos da biblioteca *Sockets* para interagir com o *hardware* de rede e gerar datagramas. Quando isso acontece o endereço IP é associado a um endereço de nível físico (ou MAC) durante a transmissão.

4.5 Endereço IP públicos e privados

Conforme relatado anteriormente, o protocolo IPv4 possui limitações com relação ao número máximo de endereços IP disponíveis. Posto que existe uma escassez de endereços IP[68], teremos que eles irão dividir-se em públicos e privados[69]. Enquanto os endereços IP públicos devem ser únicos no espaço de endereçamento global da Internet, os endereços IP privados podem vir a ser empregados dentro de organizações que queiram usar o modelo TCP/IP sem a necessidade de estarem conectadas a ela diretamente.

A escolha entre o uso de endereços IPs públicos ou privados deve ser feita com base na finalidade a que o *host se destina*. Por exemplo: o servidor de e-mails de uma organização deve ser acessível para outras organizações e, desse modo deve possuir um endereço IP público que seja único no espaço de endereçamento global da Internet. Entretanto a máquina

[68] (IPV6.BR, 2012)
[69] Existem endereços IP privados de diferentes classes: a) da classe A, cujo primeiro octeto é 10; b) da classe B, cujo primeiro octeto é algo entre 172.16 até 172.31; e c) da classe C, cujo primeiro octeto é 192.168.

de um usuário navegando na Internet não precisa (e nem deveria) ser acessível publicamente, e desse modo pode possuir um endereço IP privado.

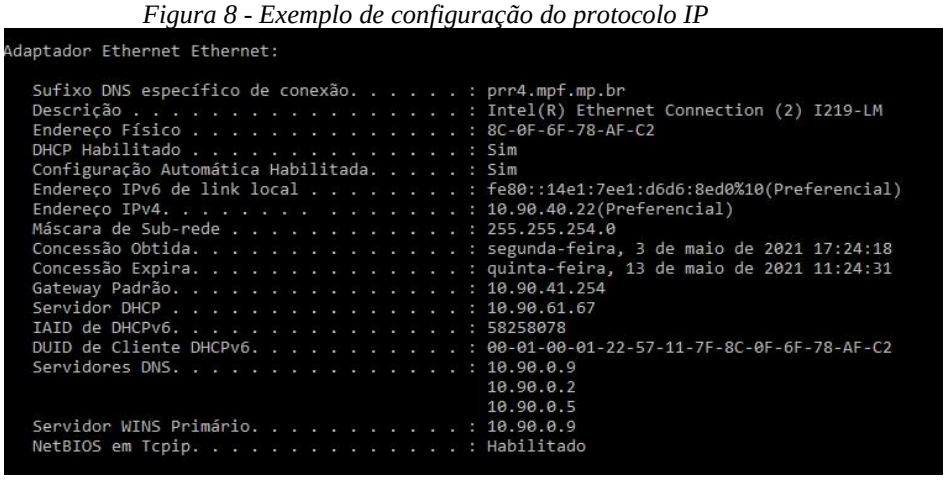
É relativamente simples determinar a autoria para quando um endereço IP é público. E isso porque existem entidades encarregadas de fazerem a delegação dos parâmetros de configuração do TCP/IP para cada organização que pretenda conectar-se na Internet global. Essas informações encontram-se mantidas em um banco de dados público, o qual pode vir a ser acessado por meio do serviço de *whois*. No caso brasileiro, isso é feito pelo organismo registro.br.

4.6 Endereços IP e determinação da autoria

Endereços do tipo IPv4 são bastante prejudiciais para determinação da autoria porque não contém nenhuma informação referente ao endereço de nível físico. Desse modo é possível a qualquer *host* que esteja no mesmo ambiente de rede forjar um datagrama, fazendo-se passar por qualquer origem, sem que o receptor perceba a diferença.

Um exemplo disso é o resultado do comando ipconfig executado em um *host* usando sistema operacional Microsoft Windows 10 e que segue na Figura 8 - Exemplo de configuração do protocolo IP.

Figura 8 - Exemplo de configuração do protocolo IP



Fonte: Resultado do comando ipconfig em *host*

O protocolo IPv4 agrupa os 32 bits que constituem o endereço em 4 octetos, representando-os de acordo com o sistema de numeração decimal e separados por ponto decimal. Nessa situação o *host* utiliza um endereço IPv4 do tipo privado, 10.90.40.22.

Entretanto, a máscara de sub-rede configurada como 255.255.254.0 indica que podem existir até outros 510 *hosts* distintos nessa mesma sub-rede. Desse modo, qualquer um deles poderia forjarem o endereço IP de origem de modo imperceptível ao *host* de destino, fazendo-se passar por essa máquina de endereço IP 10.90.40.22. Isso pode ser feito por meio de técnicas como o *IP Spoofing*[70]. Desse modo, temos que endereços IPv4 devem ser usados com ressalvas como indício de autoria.

Em contrapartida o protocolo IPv6 organiza os 128 bits que constituem o endereço em 8 grupos de 16 bits, representados de acordo com o sistema hexadecimal e separados por dois-pontos. Endereços IPv6 sempre fazem referência ao endereço físico (ou MAC) endereços IPv6 dos tipos *link-local* e *Unique Local Address (ULA)*[71]. Logo em seguida eles contêm um identificador de nível físico representado no formato IEEE EUI-64.

Na Figura 8 - Exemplo de configuração do protocolo IP teremos que alguns de seus endereços IPv6 serão o fe80::14e1:7ee1:d6d6:e8d0 e o 0001:0001:2257:117f:8c0f:6f78:afc2. É importante salientar que uma parte desse segundo endereço IPv6 faz referência ao "endereço físico" (ou MAC) de identificação 8c0f:6f78:afc2.

Em resumo endereços IPv6 são os mais apropriados para uma determinação da autoria na medida que é possível determinar a partir de qual interface de rede em um *host* a comunicação teve origem. Ao passo que endereços IPv4 podem ser forjados por meio de técnicas como o *IP Spoofing*, e o mero surgimento do meio como indício de autoria deve ser comprovado por meio de um trabalho pericial abrangendo os logs dos serviços de DHCP e *bootp*.

4.7 Endereços IP na legislação e jurisprudência

Via de regra apenas um endereço IP é o suficiente para ensejar a imputação de responsabilidade nas esferas administrativa, cível e até mesmo criminal. Todavia, em vista de tudo o que foi apresentado até esta seção está bastante claro de que tal postura é temerária para quando se trata do protocolo IPv4.

[70] (KASPERSKY, 2021)
[71] (IPV6.BR, 2012)

Nesse sentido, vide por exemplo como o assunto é tratado no Marco Civil da Internet (Lei 12.965/2014[72]):

- Art. 5º. Para os efeitos desta Lei, considera-se:
  III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;
  VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
  VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.
- Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
  § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
- Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
- Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.
- Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Com base nas definições constantes no Marco Civil da Internet, é possível demandar por informações junto aos Provedores de Conexão Internet e Provedores de Aplicação Internet com base na regulamentação pelo Decreto 8.771/2016[73]:

- Art. 11. As autoridades administrativas a que se refere o art. 10, § 3º da Lei nº 12.965, de 2014, indicarão o fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos dados cadastrais.
  § 2º São considerados dados cadastrais:
  I - a filiação;

[72] (BRASIL, 2014)
[73] (BRASIL, 2016)

> II - o endereço; e
> III - a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.

Mesmo assim, a despeito dos aspectos técnicos elencados até esse ponto, observa-se uma tendência muito forte na jurisprudência pátria no sentido de considerar endereços IP como sendo uma evidência de autoria imediata ou direta *prima facie*:

- APELAÇÃO CÍVEL. RESPONSABILIDADE CIVIL. E-MAILS COM CONTEÚDO CONSTRANGEDOR. IP DO COMPUTADOR ORIGINÁRIO DAS MENSAGENS IDENTIFICADO. RESPONSABILIDADE DO TITULAR DA ASSINATURA DA INTERNET/COMPUTADOR. AUTORIA. CULPA IN VIGILANDO. DANO MORAL CARACTERIZADO. QUANTUM REDUZIDO. I - A culpa in vigilando decorre da falta de atenção ou cuidado com o procedimento de outrem. Assim, responde o proprietário do computador, titular da assinatura da internet, do qual partiram as malfadadas mensagens eletrônicas à autora, pelos danos a ela ocasionados. II -Dano moral configurado em razão da evidente afronta.
  (TJ-RS - AC: 70025756222 RS, Relator: Artur Arnildo Ludwig, Data de Julgamento: 27/01/2011, Sexta Câmara Cível, Data de Publicação: Diário da Justiça do dia 11/02/2011)
- RECURSO ESPECIAL. AÇÃO DE OBRIGAÇÃO DE FAZER. PROVEDOR RESPONSÁVEL PELA HOSPEDAGEM DO BLOG. DISPONIBILIZAÇÃO DE MEIOS PARA IDENTIFICAÇÃO DE CADA USUÁRIO. DEVER. REGISTRO DO NÚMERO DE IP. SUFICIÊNCIA. PRECEDENTES. RECURSO ESPECIAL PROVIDO.
  (REspNº 1.676.049 /DF - RELATOR: Min. MARCO AURÉLIO BELLIZZE - TERCEIRA TURMA. DJe: 03/08/2017)
- APELAÇÃO CÍVEL. AÇÃO DE OBRIGAÇÃO DE FAZER E INDENIZATÓRIA. POSTAGEM COM CONTÉUDO OFENSIVO EM BLOG. SENTENÇA DE PROCEDÊNCIA PARCIAL DOS PEDIDOS. IRRESIGNAÇÃO DE AMBAS AS PARTES. 1. De acordo com o art. 19 aplicação de internet somente poderão ser responsabilizados civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tornar indisponível a publicação. 2. No caso concreto o pedido de tutela de urgência foi deferido, tendo o réu bloqueado o acesso ao blog. Considerando que o demandado adotou as providencias necessárias para tornar indisponível o conteúdo apontado como infringente, após a expedição de ordem judicial específica, afasta-se sua responsabilidade em indenizar o autor por eventuais danos morais sofridos. Precedentes do STJ. 3. O fornecimento do número do registro do protocolo de internet (IP) constitui meio satisfatório de identificação dos usuários. O demandado consiste em provedor de conteúdo, sendo incabível determinar que forneça dados pessoais do usuário, obrigação esta de responsabilidade do provedor de acesso. Julgados do STJ. 4. Reforma parcial da sentença. 5. NEGA-SE PROVIMENTO AO RECURSO DO AUTOR. 6. DÁ-SE PROVIMENTO AO RECURSO DO RÉU.
  (APELAÇÃO 0036036-06.2018.8.19.0002 - Des (a). SÉRGIO SEABRA VARELLA - Julgamento: 17/06/2020 - VIGÉSIMA QUINTA CÂMARA CÍVEL)

5 CRIMES CIBERNÉTICOS E DELITOS DO TIPO *RANSOMWARE*

Neste capítulo são feitas definições a respeito de crimes cibernéticos dentro do escopo desse trabalho: conceito e classificação. Também é feita uma discussão a respeito de tipos penais mais comuns associados a crimes cibernéticos. Por fim é feita uma análise dos crimes cibernéticos do tipo r*ansomware* em seus aspectos técnico e jurídico.

5.1 Definição

Primeiramente cumpre salientar que há divergência com relação a definição daquilo o que vem a ser crimes informáticos. E isso porque há vários autores denominam as infrações penais nas quais a tecnologia serviu apenas como mero instrumento na prática delitiva como sendo crimes cibernéticos. Desse modo, apesar de incorreta esta denominação tornou-se bastante popular tornando-se impossível desconsiderá-la e esse modo esse trabalho divide os crimes cibernéticos em sentido amplo (ou *lato sensu*) e em sentido estrito (ou *stricto sensu*).

Os crimes cibernéticos *lato sensu* abarcam toda e qualquer atividade criminosa executada por meios informáticos, quer seja ela direcionada a sistemas cibernéticos ou apenas empregando-os como um mero instrumento para a prática de crimes comuns. Este seria o caso, por exemplo, do envio de código-malicioso do tipo *phishingscam*[74] para aparelhos celulares a fim de cometer estelionato[75].

Os crimes cibernéticos *stricto sensu* contemplam apenas os delitos nos quais um elemento de natureza digital seja o bem jurídico tutelado pelo direito. Neste sentido, ainda para que um delito seja considerado crime cibernético seria necessário que o bem jurídico atingido fosse a inviolabilidade de dados e informações (consoante CF, artigo 5º, inciso X).[76]

5.2 Classificação

Este trabalho adota a classificação de Túlio Viana, segundo a qual os crimes cibernéticos podem vir a ser categorizados em:

---

[74] (MCCLURE, SCAMBRAY e KURTZ, 2017, p. 69)
[75] CP, art. 171, "Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento"
[76] (VIANNA e MACHADO, 2013)

5.2.1 Crimes informáticos *próprios* ou puros

São aqueles delitos onde o bem protegido pela norma é a inviolabilidade das informações em trânsito ou armazenadas. Um exemplo clássico desse tipo de delito seriam o crime de invasão de dispositivo informático[77] e o crime de inserção de dados falsos em sistema de informações por parte de funcionário público[78].

5.2.2 Crimes informáticos *impróprios* ou impuros

São aqueles onde o dispositivo computacional é utilizado como mero instrumento para a execução do crime, mas não existe ofensa à inviolabilidade da informação automatizada. Um exemplo seria o crime de ameaça[79], o qual e passível de ser executado via correio eletrônico ou rede social. Nesse caso, em regra, não há qualquer ataque à inviolabilidade de informações automatizadas.

5.2.3 Crimes cibernéticos *mistos*

Seriam os crimes conexos nos quais, além da proteção da inviolabilidade dos dados, a norma visa tutelar bem jurídica de natureza diversa. São delitos derivados do ataque ao sistema informatizado. Um exemplo dessa espécie é o ataque do tipo *ransomware* empreendido contra o TSE[80], no qual além do crime de invasão de dispositivo informático também houve crime eleitoral[81].

5.2.4 Crimes informáticos mediatos (ou indiretos)

São conceituados como delitos-fim não informáticos, pois herdaram essa característica do delito-meio informático que possibilitar a sua execução. Dessa forma, por exemplo, se determinada pessoa invadir o sistema computacional de um banco e transferir indevidamente

---

[77] CP, 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"

[78] CP, art. 313-A, "Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano"

[79] CP, art. 147, "Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave"

[80] (OLHAR DIGITAL, 2020)

[81] Código Eleitoral (Lei Nº 4.737 de 15 de julho de 1965), art. 296, "Promover desordem que prejudique os trabalhos eleitorais"

recursos financeiros para conta alheia; esse indivíduo estará cometendo dois crimes diferentes: o crime de invasão de dispositivo informático e o crime de furto, sendo que este é um delito contra o patrimônio enquanto aquele é um crime informático próprio. Nessa situação hipotética, o agente somente seria apenado pelo furto, aplicando-se ao caso o princípio da consunção[82].

5.3 Tipificação dos crimes cibernéticos

No Brasil, diferentemente de outros Estados, não existe lei única, própria ou especial para tipificar os crimes cibernéticos. Atualmente a tipificações dessas condutas está prevista em vários normativos, entre os quais merecem destaque:

Quadro 1: crimes cibernéticos mais frequentes e sua tipificação

Norma incriminadora	Crime
Lei Nº 9.296/96, art. 10.	Realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
Lei Nº 9.504/97, art. 72, incisos I a III.	Obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos. Desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral. Causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.
Lei Nº 8.069/90, arts. 241, 241-A, 241-B, 241-C e 241-D.	Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou

[82] Princípio da consunção, conhecido também como Princípio da Absorção, é um princípio aplicável nos casos em que há uma sucessão de condutas com existência de um nexo de dependência. De acordo com tal princípio o crime fim absorve o crime meio.

	outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso:
Lei Nº 7.716/1989, art. 20.	Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.
Lei Nº 9.609/1998, art. 12.	Violar direitos de autor de programa de computador.
Código Penal, arts. 138, 139 e 140.	Caluniar alguém, imputando-lhe falsamente fato definido como crime. Difamar alguém, imputando-lhe fato ofensivo à sua reputação. Injuriar alguém, ofendendo-lhe a dignidade ou o decoro.
Código Penal, art. 147.	Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave.
Código Penal, 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.
Código Penal, art. 171.	Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.
Código Penal, art. 266.	Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento.
Código Penal, art. 273.	Falsificar, corromper, adulterar ou alterar produto destinado a fins terapêuticos ou medicinais
Código Penal, arts. 286 e 287.	Incitar, publicamente, a prática de crime.

	Fazer, publicamente, apologia de fato criminoso ou de autor de crime.
Código Penal, arts. 313-A e 313-B.	Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente.

5.4 Forense computacional

Embora a volatilidade seja característica inerente a todos os dispositivos computacionais envolvidos em crimes cibernéticos, é oportuno citar o princípio da transferência criado pelo perito francês Edmond Locard: "Todo contato deixa uma marca"[83]. Indo adiante nesse raciocínio, os ensinamentos do perito francês foram sintetizados por Paulo Leland Kirk nas seguintes palavras[84]:

> Quaisquer que sejam os passos, quaisquer objetos tocados por ele, o que quer que seja que ele deixe, mesmo que inconscientemente, servirá como uma testemunha silenciosa contra ele. Não apenas as suas pegadas ou dedadas, mas o seu cabelo, as fibras das suas calças, os vidros que ele porventura parta, a marca da ferramenta que ele deixe, a tinta que ele arranhe, o sangue ou sémen que deixe. Tudo isto, e muito mais, carrega um testemunho contra ele. Esta prova não se esquece. É distinta da excitação do momento. Não é ausente como as testemunhas humanas são. Constituem, per se, numa evidência factual. A evidência física não pode estar errada, não pode cometer perjúrio por si própria, não se pode tornar ausente. Cabe aos humanos, procurá-la, estudá-la e compreendê-la, apenas os humanos podem diminuir o seu valor.

Enfim, a partir da teoria criada por Locard e do raciocínio desenvolvido por Kirk é possível concluir que os crimes cibernéticos, apesar de possuírem suas peculiaridades quando em comparação a outros tipos crimes, também deixam vestígios para os quais deve ser mantida a cadeia de custódia[85] a fim de que eventualmente venha a ser feito um trabalho de forense computacional buscando determinar materialidade e autoria.

---

[83] (TELLES, FILHO, *et al.*, 2020, p. 8)
[84] (VELHO(ORG.), 2016, p. 59)
[85] CPP, arts. 158-A, "Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear

5.5 Crimes cibernéticos do tipo ransomware

Ataques por meio de *Ransomware* constituem-se em um crime cibernético de tipo misto, na medida que pode atingir tanto dispositivos informáticos como outros bem jurídicos tutelados pelo direito. Ainda não se encontra tipificado em nosso ordenamento jurídico.

5.5.1 Aspecto técnico

Ransomware é um tipo de ataque envolvendo o uso de código malicioso, através da Internet, visando atingir elementos computacionais com vulnerabilidades que não estejam mitigadas.[86] O nome desse ataque deriva do fato de que é exibido o pagamento de um resgate (ou *ransom*), geralmente na forma de criptomoeda para reaver o controle do componente comprometido.

Enquanto uma parte do valor desse resgate fica com os autores, a outra é destinada para as organizações que prestam apoio material disponibilizando os recursos de sua plataforma para que esse tipo de ação seja empreendida. Há uma série de organizações desse tipo, tal como a REvil[87], as quais podem vir a ser contatadas por meio da *deepweb*[88].

Ataques desse tipo podem afetar tanto os equipamentos de usuários finais (ou clientes) quanto os equipamentos destinados a prestarem serviços para a rede de computadores (incluindo-se equipamentos e servidores). Isso acontece porque tão logo um *ransomware* invade um ambiente, procura disseminar-se ao máximo pela organização explorando serviços com vulnerabilidades de mitigação difícil.[89]

Um ataque do tipo *ransomware* pode comprometer os dados e recursos computacionais de uma organização com relação a seus atributos de disponibilidade e integridade. A disponibilidade refere-se à probabilidade de que um sistema estar operacional em um dado instante de tempo, apto a prestar o serviço para o qual foi concebido. E a

---

sua posse e manuseio a partir de seu reconhecimento até o descarte" e CPP, 158-B, "A cadeia de custódia compreende o rastreamento do vestígio nas seguintes etapas"

[86] (MCCLURE, SCAMBRAY e KURTZ, 2017, p. 177)

[87] "Assim, o REvil na verdade atrai afiliados para distribuir o ransomware. Como parte do acordo com esses afiliados, os desenvolvedores do ransomware dividem a receita obtida com o pagamento do resgate. É difícil, segundo os pesquisadores, apontar a localização exata dos desenvolvedores, mas acredita-se que eles estejam baseados na Rússia, devido ao fato de que o grupo não tem como alvo organizações russas ou aquelas em países do antigo bloco soviético." (ADVISOR, 2021)

[88] (SILVA, 2017, p. 255-270)

[89] Nesse sentido algumas das mais exploradas são soluções para VPN e virtualização de datacenters, por exemplo.

integridade refere-se às garantias de que uma informação não tenha sido adulterada, permitindo detectar caso isso ocorra.

Ataques do tipo *ransomware* afetam a integridade dos dados pois modificam o teor da informação original. A sua representação é alterada, passando a ser representada como sendo o resultado de um processo do tipo criptografia simétrica[90]. E eles podem afetar a disponibilidade dos recursos computacionais tornando-os inacessíveis total ou parcialmente por meio da exploração de vulnerabilidades que não estejam mitigadas.

5.5.2 Breve histórico

O primeiro código-malicioso foi criado no ano de 1989 por Joseph Popp[91]. Na época ele adquiriu 20 mil discos magnéticos e enviou-os pelo correio para os participantes de uma conferência da Organização Mundial da Saúde (OMS) sobre AIDS ocorrida em Estocolmo. Popp era um biólogo formado em Harvard e foi rastreado por meio de uma caixa postal, através da qual ele deveria receber o valor exigido como resgate de 189 dólares para liberar as máquinas.

Alguns relatórios indicam que Popp foi rejeitado pela OMS para uma oportunidade de trabalho. Após sua prisão no Aeroporto Schiphol, de Amsterdã, ele foi mandado de volta aos Estados Unidos e preso. Ele teria dito às autoridades que planejava doar o dinheiro do resgate para pesquisas sobre a AIDS. Popp morreu em 2007

Acusado de chantagem, Popp é considerado como sendo o inventor da categoria *ransomware*. Na época publicações técnicas em Ciência da Computação como o *Virus Bulletin* perceberam o conceito inovador em relação às técnicas usadas até então[92]. Para combaterem esse tipo de código malicioso, pesquisadores da época como John McAfee e Eugene Kaspersky criaram suas próprias empresas de antivírus em 1987.

---

[90] Onde uma única chave criptográfica deve ser empregada para cifrar e decifrar o conteúdo
[91] (CNN BRASIL, 2021)
[92] Os códigos-maliciosos até o momento eram dos tipos *keyloggers, horse-trojans,Worms, botnets, spywares, adwares* entre outros.

5.5.3 Aspecto jurídico

Sob o ponto de vista jurídico em relação à teoria do domínio do fato na concepção de Claus Roxin, teremos três agentes em concurso de pessoas: a) *hackers* como sendo autores mediatos ou indiretos; b) *hosts* afetados pelo *ransomware* sendo usados como mero instrumento pelos *hackers*, agindo em erro, na forma de domínio da vontade; e c) organizações criminosas que prestam apoio material para *hackers* empreenderem ações como essa, as quais podem ser consideradas: 1) cúmplices dos *hackers* para o crime de invasão; 2) coautoras dos *hackers* na forma do domínio funcional para o crime de extorsão; e 3) autoras para o crime de associação criminosa, sem o prejuízo do enquadramento em outros crimes conexos conforme forem as circunstâncias.

Os *hackers* autores mediatos ou indiretos por serem senhores e donos de sua decisão e da execução do acontecer típico, possuindo "domínio final do fato" (ou *finalen Tatherrschaff*). Escolhem qual será o alvo e decidem o momento em que o ataque irá acontecer.

Os *hosts* com vulnerabilidades não mitigadas usados pelos *hacker*si são meros instrumentos. Tão logo um *ransomware* consiga atingir um alvo, ele compromete o seu funcionamento para logo em seguida buscar disseminar-se pela organização afetada. Posto que isso acontece sem a consciência e vontade das vítimas, trata-se de uma situação de domínio da vontade onde existe um erro. Não há os elementos que subjazem o dolo dos tipos objetivos que associados aos crimes cibernéticos.

As organizações que mantém infraestrutura tecnológica e recursos humanos disponíveis para *hackers* empreenderem ataques do tipo *ransomware*, tal como a REvil[93], podem vir a ser consideradas partícipes, coautoras e autoras. Elas podem vir a ser consideradas partícipes por serem cúmplices no crime de invasão de dispositivo informático, pois prestam apoio material disponibilizando os recursos de suas plataformas.

Também podem ser consideradas coautoras quanto ao crime de extorsão[94] devido ao fato de serem remuneradas com uma porcentagem do valor exigido de resgates (ou *ransom*).

---

[93] Detalhes na URI https://www.tripwire.com/state-of-security/featured/revil-ransomware-what-you-need-to-know/

[94] CP, art. 158, caput: "Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa. Pena - reclusão, de quatro a dez anos, e multa". Sendo que: "§ 1º - Se o crime é cometido por duas ou mais pessoas, ou com emprego de arma, aumenta-se a pena de um terço até metade"

Com relação ao crime de extorsão há um *pactum sceleris* entre as organizações e os *hackers* quanto cada parte irá receber. Trata-se de uma situação de domínio funcional, dentro da teoria do domínio do fato.

E por fim elas podem vir a ser consideradas autoras em crimes como a associação criminosa[95] mas, conforme forem as circunstâncias, ainda também podem vir a responder por outros crimes. De acordo com as circunstâncias de cada caso concreto, eventualmente as organizações podem vir a ser consideradas autoras de crimes como até mesmo a Lei de Segurança Nacional.[96] E isso porque conforme for a magnitude dos danos, jurisdicionados podem ter o exercício da sua cidadania prejudicado pela impossibilidade de acesso aos poderes.[97]

[95] CP, art. 288, *caput*: "Associarem-se 3 (três) ou mais pessoas, para o fim específico de cometer crimes. Pena - reclusão, de 1 (um) a 3 (três) anos"
[96] (BRASIL, 1983)
[97] LSN, art. 18: "Tentar impedir, com emprego de violência ou grave ameaça, o livre exercício de qualquer dos Poderes da União ou dos Estados. Pena - reclusão, de 1 (um) a 3 (três) anos"

6 CONCLUSÃO

Ataques cibernéticos do tipo *ransomware* estão associados a crimes cibernéticos do tipo misto, na medida que afetam tanto um dispositivo informático quanto outros bens jurídicos tutelados pelo direito. Nesse tipo de delito haverá um concurso de pessoas e esse trabalho procurou aplicar a teoria do domínio do fato para determinação da autoria e participação dos agentes.

Como esse tipo de ação ocorre através da Internet, existirão os endereços IP associados a vários *hosts.* Todavia é importante salientar que nem todos esses endereços IP devem ser considerados posto que, conforme demonstrado, aqueles do tipo IPv4 são parametrizáveis por *software* e podem vir a ser forjados com facilidade. Neste sentido é recomendável o uso de endereços do tipo IPv6 para determinação da autoria.

Restou demonstrado que o tratamento dado pelo nosso ordenamento jurídico para coibir a prática de crimes cibernéticos no geral, e dos ataques do tipo *ransomware* em especial encontra-se muito aquém do ideal. E embora o nosso país faça parte da Convenção de Budapeste – tratado pelo qual obrigou-se a fazer a tipificação de condutas delitivas – ainda não efetuou as mudanças legislativas que seriam necessárias para o tratamento adequado de incidentes em segurança da informação. Nesse momento o único crime próprio encontra-se no art. 154-A do Código Penal, com pena cominada de detenção por até 1 ano e multa.

Na conclusão esse trabalho salienta a importância de uma manutenção apropriada da cadeia de custódia, a fim de permitir a distinção entre os agentes agindo em concurso por meio de um trabalho pericial na área de Tecnologia da Informação e Comunicação. Além da necessidade de uma tramitação célere da incorporação da Convenção de Budapeste ao nosso ordenamento jurídico junto ao Congresso Nacional, a fim de viabilizar a celebração de acordos de cooperação internacional.

REFERÊNCIAS

(ABNT NBR ISO/IEC 27002:2013, 2013) ABNT NBR ISO/IEC 27002:2013. **Tecnologia da informação - Técnicas de segurança - Código de prática para controles da segurança da informação**. Rio de Janeiro: ABNT, 2013. 99 p. Disponivel em: <https://www.abntcatalogo.com.br/norma.aspx?ID=306582>.

(ADVISOR, 2021) ADVISOR, C. Ransomware REvil está pedindo US$ 5 milhões de resgate ao TJRS. **CISO Advisor**, 2021. Disponivel em: <https://www.cisoadvisor.com.br/ransomware-revil-pede-us-5-milhoes-de-resgate-ao-tjrs/>. Acesso em: 03 maio 2021.

(ALFLEN, 2014) ALFLEN, P. R. **Teoria do Domínio do Fato**. São Paulo: Saraiva, 2014. Disponivel em: <https://app.minhabiblioteca.com.br/#/books/9788502210097/cfi/0>. Acesso em: 20 abr. 2021.

(ALMEIDA FILHO, JOSÉ CARLOS DE ARAÚJO , 2010) ALMEIDA FILHO, JOSÉ CARLOS DE ARAÚJO. **Processo Eletrônico e Teoria Geral do Processo Eletrônico – A Informatização Judicial no Brasil**. Porto Alegre: Editora Forense, 2010.

(APNIC, 2021) APNIC. IPv6 Capable Rate by Country (%). **IPV6 Measurement Maps**, 2021. Disponivel em: <https://stats.labs.apnic.net/ipv6>. Acesso em: 02 05' 2021.

(BRASIL, 1983) BRASIL. Lei Nº 7.170 de 14 de dezembro de 1983. Lei de Segurança Nacional., 14 dez. 1983. Disponivel em: <http://www.planalto.gov.br/ccivil_03/leis/l7170.htm>. Acesso em: 01 maio 2021.

(BRASIL, 2014) BRASIL. Lei Nº 12.965 de 23 de abril de 2014. Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil., 23 abr. 2014. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 26 abr. 2021.

(BRASIL, 2016) BRASIL. Decreto Nº 8.771 de 11 de maio de 2016, 11 maio 2016. Disponivel em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 18 abr. 2021.

(BRASIL, 2020) BRASIL. Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética. **Secretaria Geral da Presidência da República**, 2020. Disponivel em: <https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica>. Acesso em: 26 abr. 2021.

(CERF e KAHN, 1974) CERF, V.; KAHN, R. A Protocol for Packet Network Intercommunication. **IEEE Trans on Comms**, Com-22, 5 maio 1974. 637–648. Disponivel em: <https://ieeexplore.ieee.org/document/1092259>.

(CHAPMAN, ZWICKY e COOPER, 1999) CHAPMAN, B.; ZWICKY, E.; COOPER, S. **Building Internet Firewalls**. 2nd. ed. San Francisco: O'Reilly Press, 1999.

(CNN BRASIL, 2021) CNN BRASIL. A bizarra história do inventor do ransomware; vírus deixou parte dos EUA sem gás, 2021. Disponivel em: <https://www.cnnbrasil.com.br/amp/business/2021/05/16/a-bizarra-historia-do-inventor-do-ransomware-virus-deixou-parte-dos-eua-sem-gas>. Acesso em: 16 maio 2021.

(CNN BRASIL, 2021) CNN BRASIL. Ataques ransomware renderam R$ 2,1 bilhões a hackers em 2020, aponta estudo. **CNN Brasil**, 2021. Disponivel em: <https://www.cnnbrasil.com.br/tecnologia/2021/05/15/ataques-ransomware-rederam-r-2-1-bilhoes-a-hackers-em-2020>. Acesso em: 2021 maio 15.

(GRECO (ORG.), LEITE, *et al.*, 2014) GRECO (ORG.), L. et al. **Autoria como domínio do fato:** estudos introdutórios sobre o concurso de pessoas no direito penal brasileiro. São Paulo: Marcial Pons, 2014.

(IPV6.BR, 2012) IPV6.BR. Endereçamento. **NIC.br**, 2012. Disponivel em: <http://ipv6.br/post/enderecamento/>. Acesso em: 01 maio 2021.

(ISO/IEC, 2004) ISO/IEC. **ISO/IEC 13335-1:** 2004 - Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management. s.l.: [s.n.], 2004.

(KASPERSKY, 2021) KASPERSKY. O que é Spoofing? **Kaspersky Labs**, 2021. Disponivel em: <https://www.kaspersky.com.br/resource-center/definitions/ip-and-email-spoofing>. Acesso em: 17 abr. 2021.

(MCCLURE, SCAMBRAY e KURTZ, 2017) MCCLURE, S.; SCAMBRAY, J.; KURTZ, G. **Hackers expostos:** segredos e soluções para a segurança de redes. 4. ed. São Paulo: Bookman, 2017. 760 p.

(NEOTEL, 2020) NEOTEL, S. D. Sistema judicial do Brasil sob ataque maciço de ransomware RansomExx. **neotel Segurança Digital**, 2020. Disponivel em: <https://blog.neotel.com.br/2020/11/06/sistema-judicial-do-brasil-sob-ataque-macico-de-ransomware-ransomexx/>. Acesso em: 04 maio 2021.

(NIST, 2006) NIST. **FIPS PUB 200:** Minimum Security Requirements for Federal Information and Information Systems. S.L.: [s.n.], 2006.

(OLHAR DIGITAL, 2020) OLHAR DIGITAL. Após negar ataque, TSE tem bancos de dados expostos por hackers em dia de eleição. **Olhar Digital**, 2020. Disponivel em: <https://olhardigital.com.br/2020/11/15/seguranca/apos-negar-ataque-tse-tem-bancos-de-dados-vazado-por-hackers/>. Acesso em: 04 maio 2021.

(SILVA, 2017) SILVA, Â. R. I. D. (.). **Crimes Cibernéticos**. 1. ed. Porto Alegre: Livraria do Advogado, 2017.

(SILVA, 2015) SILVA, Â. R. I. D. O Domínio do Fato por meio de Aparatos Organizados de Poder e sua Aplicação à Criminalidade Empresarial. In: SILVA, Â. R. I. D., et al. **Temas de Direito Penal, Criminologia e Processo Penal**. Porto Alegre: Livraria do Advogado, 2015. p. 38.

(SILVA, 2020) SILVA, Â. R. I. D. **Curso de Direito Penal - Parte Geral**. Porto Alegre: Livraria do Advogado, 2020. 376-405 p.

(TANENBAUM e WETHERALL, 2011) TANENBAUM, A.; WETHERALL, D. **Redes de Computadores**. 5. ed. Rio de Janeiro: Pearson Education, 2011.

(TELLES, FILHO, *et al.*, 2020) TELLES, B. et al. Todo contato deixa uma marca. **Revista Brasileira de Criminalística**, v. 9, 2020. Disponivel em: <http://rbc.org.br/ojs/index.php/rbc/article/view/487>. Acesso em: 19 nov. 2020.

(TILT, 2020) TILT, C. D. T. RansomExx: vírus que atingiu STJ também atacou TJ-PE e outros países. **Conteúdo de Tecnologia TILT**, 2020. Disponivel em: <https://www.uol.com.br/tilt/noticias/redacao/2020/11/07/ransomexx-virus-que-atingiu-stj-tambem-atacou-tj-pe-e-outros-paises.htm>. Acesso em: 04 maio 2021.

(VELHO(ORG.), 2016) VELHO(ORG.), J. A. **Tratado de Computação Forense**. Campinas: Editora Millenium, 2016.

(VIANNA e MACHADO, 2013) VIANNA, T.; MACHADO, F. **Crimes cibernéticos**. Belo Horizonte: Fórum, 2013. 113 p.

ÍNDICE

A

C

D

F

H

I

M

N

P

R

S

T

V

W