

DESAFIOS DA PROTEÇÃO DOS DIREITOS FUNDAMENTAIS NO BRASIL FRENTE À CIBERCRIMINALIDADE E À CONVENÇÃO DE BUDAPESTE

Antonio Donizetti de Resende¹

Xenofontes Curvelo Piló²

1 INTRODUÇÃO

Não é novidade a afirmativa que as novas tecnologias de informação e comunicação (TIC), internet, marcam de maneira duradoura a sociedade contemporânea, estabelecendo assim novas formas de relação interpessoal e novos modos de compreensão das noções de tempo e espaço. O fluxo de conexões apresenta-se de modo avassalador que um dos principais desafios da contemporaneidade passará inevitavelmente pela regulação das múltiplas e variadas esferas de poder, que emergem do enorme leito comunicacional que pauta a sociedade em rede.

Com a pandemia do Covid-19 que assolou o mundo, o espaço laboral foi perfeitamente transladado para o espaço virtual, não ocorrendo grandes perdas na qualidade dos serviços e das atividades realizadas. A importância das TIC- tecnologias de informação e comunicação- na sociedade Contemporânea, os termos ciberespaço e cibercultura já integram o nosso vocabulário cotidiano. Onde o ciberespaço potencializa agregações eletrônicas em torno de interesse comuns que conectam sujeitos, que, de outro, modo talvez nunca se encontrariam pessoalmente (LÉVY, 2016).

Manuel Castells professa, que a criminalidade é um fenômeno que acompanha a humanidade desde os seus primórdios. No entanto, a formação de

¹ Doutorando e Mestre em Proteção dos Direitos Fundamentais pela Universidade de Itaúna. Mestre em Engenharia Geotécnica pela Universidade Federal de Ouro Preto. Especialista em Engenharia Rodoviária pela Pontifícia Universidade Católica de Minas Gerais. Especialista em Direito Material e Processual do Trabalho pela Faculdade Pitágoras de Divinópolis. Especialista em Engenharia de Segurança do Trabalho pela Pontifícia Universidade Católica de Minas Gerais. Especialista em Direito Processual Constitucional pela Faculdade de Pará de Minas. MBA em Mercado de Capitais e Derivativos pela Pontifícia Universidade Católica de Minas Gerais. Bacharel em Engenharia Civil pela Fundação de Ensino e Tecnologia de Alfenas. Bacharel em Direito pela Faculdade Pitágoras de Divinópolis. Advogado. E-mail: resende36@yahoo.com.br.

² Doutorando e Mestre em Proteção dos Direitos Fundamentais pela Universidade de Itaúna/MG (2021). Bacharel em Direito pela Faculdade Promove (2008), Bacharel em Ciências Contábeis pela Faculdade Newton Paiva (1988). Especialização Direito Público lato sensu pelo CEAJUF (2009). Especialização em Ciências Penais lato sensu pelo Centro Universitário Newton Paiva (2011), membro da ABJD - Associação Brasileira de Juristas pela Democracia. Advogado. Email: xenopilo@yahoo.com.br Currículo Lattes: <http://lattes.cnpq.br/8570712885711499>.

redes entre organizações criminosas e associados, com atividades em todo o planeta, fazem surgir o fenômeno do “crime global”, o qual “afeta profundamente a economia no âmbito internacional e nacional, a política, a segurança e, em última análise, as sociedades em geral”. (CASTELLS, 2007).

Os Tratados e/ou Convenções internacionais poderiam, e deveriam, ser mais efetivos quando da solução de crimes informáticos, tendo em vista que, em sendo a internet um meio de comunicação que ultrapassa limites e fronteiras de qualquer país, seria pouco provável que somente leis nacionais de cada Estado conseguissem definir como, quando, onde e qual legislação seria responsável por determinada conduta delituosa de um indivíduo.

A Convenção de Budapeste, conhecida como Convenção sobre o Cibercrime -CETS nº 185, foi elaborada em 21 de setembro de 2001 com mais de quarenta países-membros signatários, dentre os quais Estados Unidos da América, Canadá, Japão e África do Sul, postula a produção de uma política criminal comum para fornecer proteção à sociedade contra a criminalidade no espaço virtual, enfatizando a necessidade de se ter uma legislação adequada com o desenvolvimento tecnológico atual.

A convenção de Budapeste tem contribuído para dar respostas coordenadas a uma forma de criminalidade que não reconhece barreiras espaço-geográficas e que desafia para o seu combate, novas formas de persecução penal, que perpassam pela cooperação internacional.

2 A CIBERCRIMINALIDADE E A CONVENÇÃO DE BUDAPESTE

A preocupação com a Cibercriminalidade, como não poderia deixar de ser, rompe barreiras e alcança um patamar global. Spencer Sydow chama à atenção para a necessidade no combate ao cibercrime incluir as agências privadas. O autor se refere que interesses comerciais por parte das agências privadas acabam por impedir um combate mais contundente. Ainda afirma o autor que há uma descrição de diferentes estratégias internacionais de combate à cibercriminalidade, destacando a urgência no estabelecimento de parcerias de cooperação entre governos, empresas e universidades. (SYDOW, 2022).

O conceito de cibercrime é fluido e a sua definição não é consensual, uma vez que, tendo em conta a diversidade de oportunidades proporcionadas

pela tecnologia e pelos diferentes equipamentos eletrônicos para adotar comportamentos desviantes e/ou cometer crimes, como “burlas em plataformas de venda online, divulgação ilícita de fotografias, crimes contra honra, difusão de pornografia infantil ou crimes contra o direito do autor. (GOMES, 2021).

No âmbito internacional a Convenção sobre cibercrime, é conhecida como Convenção de Budapeste, trata-se de um tratado internacional de direito penal e processual penal firmado na Hungria, em 2001, no âmbito do Conselho da Europa, tendo por objetivo definir, harmonicamente os crimes praticados através da Internet e as formas eficazes para a sua persecução. (Conselho da Europa, 2001).

A Convenção de Budapeste preconiza uma política criminal tendo por objetivo de proteger a sociedade contra a criminalidade no ciberespaço, especificamente através da adoção de legislação adequada e da melhoria da cooperação internacional, sem deixar de reconhecer a necessária cooperação entre os Estados e a indústria privada, com a finalidade específica de combater os crimes no ciberespaço.

Um dos pontos mais relevantes da Convenção de Budapeste é o texto legal estabelecendo conceitos que permitem identificar objetivamente aspectos relacionados com a Internet e os fornecedores de serviços. Obrigando assim os países signatários a estabelecerem jurisdição sobre os delitos previstos na Convenção, através dos respectivos sistemas judiciais e administrativos, de modo a poder declarar-se competentes, a perseguir e processar com base no território, os cometedores de atos ilícitos no ciberespaço, a bordo de embarcações e aeronaves matriculadas de um Estado e com base na nacionalidade, independentemente do lugar onde foi praticada a infração. (VELASCO, 2012).

A Convenção de Budapeste, sugere e não obriga, não tem vinculação coercitiva, servindo de parâmetro a ser observado pelos Estados, a fim de uniformizar as várias legislações internas. Também, recomenda acerca da cooperação internacional e de aspectos relacionados à investigação criminal e a procedimentos de processo penal.

Destaca-se que a discussão acerca da dificuldade de se definir o tempo e o lugar de determinada conduta cibernética criminosa, está no fato de estarem correlacionados com o local em que se consumam, e, por consequência,

podendo englobar a jurisdição de vários países distintos. É imprescindível que esses crimes sejam investigados e identificados em escala mundial, mas qual o país competente para processar, julgar e penalizar os infratores, essa seria a grande pergunta.

Praticada uma infração penal, o Estado, através de seus agentes legitimados, será o responsável pela averiguação e esclarecimento da autoria (quem praticou a ação do tipo penal) e da materialidade (qual o resultado naturalístico juridicamente relevante para o direito penal) do fato delitivo. Apesar dos avanços na investigação sobre o cibercrime ocorridos na última década, ainda há aspectos que tem limitado o seu conhecimento científico. Uma das limitações consiste na insuficiência de dados oficiais que permitam estimar a prevalência e a incidência destas ofensas na população em geral. (GOMES,2021).

A Convenção de Budapeste é atualmente o único instrumento jurídico de caráter global para o combate hábil aos cibercrimes. Contudo, acredita-se que a Convenção peca por tratar todos Estados signatários de forma idêntica não levando em consideração as discrepâncias e os hiatos tecnológicos de cada país. Pode-se afirmar que no que diz respeito à cibercriminalidade, é colocado de modo evidente, a questão sobre a possibilidade ou não de enfrentar com leis nacionais(internas) os desafios criminais derivados do uso de tecnologias da informação o que deveria ser atendido a partir de uma plataforma legislativa internacional com a possibilidade de transpassar as fronteiras territoriais.

Considerando-se a natureza jurídica, os sujeitos, o tempo e o lugar do seu cometimento e as provas obtidas, os cibercrimes possuem particularidades que fazem com que a investigação preliminar desenvolvida a partir do ciberespaço seja *sui generis*. Nem sempre as técnicas, praticas ou métodos usados diariamente em investigações do universo offline podem ser aplicados em ambiente online.

No contexto brasileiro, a investigação de cibercrimes não possui legislação específica, ou seja, o Brasil não possui uma lei de cunho processual penal destinada exclusivamente a regulamentar procedimentos, métodos, instrumentos, limites e critérios para investigação em ambiente online.

Decorridos mais de vinte anos desde a entrada em vigor na ordem internacional, a Convenção de Budapeste se mantém relevante e atual, tendo

sido ratificada por 68 Estados, membros e não membros do Conselho da Europa. O Brasil ratificou a Convenção em 2022 e a promulgou internamente com o Decreto 11.491/2023, em 12 de abril de 2023.

Conforme dispõe o art. 37º da Convenção de Budapeste, o Brasil, por não ser um dos países que participaram da elaboração do tratado, deveria receber o convite de um dos Estados membros para aderir à resolução, além de receber a aprovação unânime entre os demais Estados membro, o que ocorreu no final do ano de 2022. A adesão do Brasil à Convenção de Budapeste era uma necessidade que o país almejava. Contudo a assunção de obrigações internacionais para o combate ao cibercrime não basta, sendo necessário adotar medidas internas em matéria penal e processual penal para torná-las efetivas.

A Convenção de Budapeste tem como objetivo facilitar a cooperação internacional para combater o cibercrime. Elaborado pelo Comitê Europeu para os Problemas Criminais, com o apoio de uma comissão de especialistas, o documento lista os principais crimes cometidos por meio da rede mundial de computadores e foi o primeiro tratado internacional sobre crimes cibernéticos. A Convenção já foi assinada por mais de 60 países e é utilizada por outros cerca de 160 como orientação para as legislações locais. Essa cooperação com outros Estados no combate aos crimes cibernéticos tem a finalidade precípua de proteção aos direitos fundamentais.

3 DIREITOS FUNDAMENTAIS VERSUS CIBERCRIMINALIDADE

Os direitos fundamentais estão ligados, como o próprio nome já informa, a sua fundamentalidade, podendo ser analisados tanto no aspecto material como no aspecto formal. Para Ruthenburg (2000, p. 146), essa fundamentalidade colocada dentre uma das características dos direitos fundamentais revela-se pelo conteúdo do direito – referência aos valores supremos do ser humano e preocupação com a promoção da dignidade da pessoa humana – e também pela posição normativa, expressa no ordenamento jurídico como norma da Constituição. Tais direitos possuem aplicação imediata, conforme preceitua o art. 5º, § 1º da Constituição brasileira e são direitos fundamentais protegidos tanto pelo legislador como pelo poder constituinte, considerando as cláusulas pétreas. Porém, a fundamentalidade material está ligada à estrutura do Estado e às

sociedades, levando em consideração o § 2º do mesmo art. 5º, o qual prevê os direitos e garantias constitucionais.

O termo cibercrime não significa mais do que a ocorrência de um comportamento danoso, que está, de alguma forma, relacionada com um computador e que não tem uma referência específica na lei. Embora ao longo dos últimos anos, diversos países, tenham previstos tipos legais de cibercrime na sua legislação. São também múltiplas expressões que têm sido usadas para designar a prática complexa de ofensas cibernéticas: crime informático, crime digital, crime informático-digital, entre muitas outras. (GOMES, 2021).

No âmbito internacional, os direitos e as garantias fundamentais têm como base fundamental a Declaração Universal dos Direitos Humanos, adotada e proclamada pela resolução 217-A da Assembleia Geral das Nações Unidas, em 10 de dezembro de 1948.

O direito internacional dos direitos humanos é aquele que, conforme afirma Mazzuoli (2018, p. 66), visa proteger todos os indivíduos, qualquer que seja a sua nacionalidade e independentemente do lugar onde se encontram. Trata-se da disciplina encarregada de estudar o conjunto de normas internacionais convencionais e consuetudinárias, na qual são estipulados o comportamento e os benefícios que as pessoas ou grupos de pessoas podem esperar ou exigir dos governos, tendo por objeto de estudo o conjunto de normas previstas pelas declarações, tratados ou convenções sobre direitos humanos, adotados pela Comunidade Internacional em nível universal ou regional. São aquelas normas internacionais que consagram os direitos humanos, que criam e regulam os sistemas supranacionais de promoção e proteção dos direitos humanos, assim como as que regulam os procedimentos possíveis de serem levados ante os ditos organismos para o conhecimento e consideração das petições e denúncias e queixas pela violação dos direitos humanos.

De acordo com a espécie de obrigação gerada, é possível elencar na ótica interna e internacional os direitos humanos mais basilares, e, assim, aproximar-se de uma definição. Poderiam ser citados, como exemplos de direitos já reconhecidos, os seguintes: vida, liberdade, não ser escravizado, não ser torturado, privacidade (direitos-liberdade), segurança pessoal, propriedade, educação básica, lazer, (direitos-pretensão) personalidade, honra,

nacionalidade, direitos políticos (direitos-poder/imunidade). Todos citados são reconhecidos na Declaração Universal dos Direitos Humanos.

Com a finalidade precípua em prejudicar terceiros, o Cibercrime vem sendo utilizado para descrever um amplo conjunto de infrações, incluindo os crimes contra dados e sistemas (denominado de "hacking"), crimes relacionados a falsificação e fraude (denominado "phishing"), ofensas de conteúdo (tais como divulgação de pornografia infantil), e infrações de direitos autorais (como por exemplo a disseminação de conteúdo pirata). (SYDOW, 2022).

De acordo com o Relatório NORTON Symantec (Antivírus) divulgado em 2015, quase dois terços da população adulta mundial já fora vítima de algum crime cibernético. O mesmo relatório indica que pelo menos 79% dessas pessoas não esperam que haja alguma punição aos criminosos. As principais espécies de cibercrimes praticadas em larga escala são a pedofilia, as fraudes de cartões de crédito ou bancárias e o estelionato, a subtração de valores e informações ou sua destruição. (NORTON, 2015).

Os crimes cibernéticos são, portanto, uma das formas de violação de direitos humanos mais básicos, como a propriedade e a intimidade. O pacto internacional dos direitos civis e políticos prevê em seu artigo 17 que “ninguém será objeto de intervenções ilegais ou arbitrárias em sua vida privada”, com a clara intenção de proteger a privacidade do indivíduo.

Nesse sentido ao se tratar o direito à privacidade como um direito humano, trazem a lume a teoria de William Prosser, ao afirmar que existem quatro meios básicos de afrontar a privacidade, a saber: 1) intromissão da reclusão do indivíduo; 2) exposição pública de fatos privados; 3) exposição do indivíduo a uma falsa percepção do público (false light) e 4) apropriação do nome e da imagem da pessoa, sobretudo para fins comerciais. Fica claro, nesse âmbito, que a cibercriminalidade tem o potencial em suas variadas vertentes de violar substancialmente o direito à privacidade. (MENDES, 2012).

Outro direito fundamental violado é o direito à propriedade pois o objetivo da maioria dos delinquentes virtuais é a obtenção de lucro às custas de subtrações e fraudes bancárias, bem como, lavagem de valores obtidos de forma criminosa, especialmente com a conversão de valores em criptomoedas (moedas digitais) como o bitcoin. Calderon esclarece que se trata de uma espécie de “cambio do novo milênio” em que se troca a moeda real por uma

moeda existente apenas no mundo virtual, tudo com vistas a lograr as autoridades estatais. (CALDERON, 2017).

Diante de ameaças que despontam no mundo informatizado, por meio do cibercrime, a segurança da informação (também denominada segurança cibernética), ou cibersegurança, é o novo desafio da comunidade internacional. A cibersegurança não só é essencial à garantia dos direitos individuais fundamentais de todos que tem acesso à rede, como também é tida como função estratégica de Estado. (MANDARINO JUNIOR; CANONGIA, 2010).

A conservação de infraestruturas sensíveis à defesa nacional, como energia, telecomunicações, finanças e a própria informação estratégica, por exemplo, exigem uma política de cibersegurança consolidada e resistente aos constantes ataques de hackers e crackers, que agem de forma autônoma ou até mesmo prestando serviços a outros governos ou corporações.

Para o cidadão comum que utiliza a internet para suas atividades do dia-a-dia, a segurança do terminal utilizado pode prevenir muitos golpes e ataques e se torna tão essencial quanto a segurança física proporcionada por muros, portões e fechaduras. A existência do Direito está intimamente ligada à prestação da jurisdição estatal.

Aury Lopes professa que estatuído por fundamento constitucional, o monopólio da jurisdição estatal serve à resolução de conflitos entre particulares, inclusive no campo penal. (JUNIOR, 2003).

Para Carnelutti, a investigação assume também uma função garantista, pois representa um mecanismo apto a evitar e a filtrar acusações, infundadas contra o sujeito passivo, afastando dele o risco da estigmatização. (CARNELUTTI 2020).

Dentre os principais fundamentos garantistas subjacentes à investigação preliminar, está a possibilidade de se evitarem acusações infundadas. A bem da verdade, os resultados decorrentes de uma acusação imputada a um inocente têm consequências que maltratam não apenas esse indivíduo, como também a sociedade da qual faz parte, já que faz brotar a incerteza e a insegurança coletiva nos órgãos, responsáveis pela investigação. (GOMES, 2021).

Deilton Brasil professa que os direitos fundamentais previstos em normas constitucionais que têm a natureza de regras ou de princípios não são absolutos podendo ser relativizados em face da necessidade de consideração de

outros direitos fundamentais ou de interesses públicos constitucionalmente protegidos.

A presunção de não culpabilidade é um direito fundamental que impõe o ônus da prova à acusação e impede o tratamento do réu como culpado até o trânsito em julgado da sentença. (BRASIL, 2016)

O mundo cibernético tornou-se um âmbito no qual o ordenamento jurídico brasileiro ainda se surpreende com situações sem precedentes, vez que padece de lacunas nesta seara, muito embora, nos últimos dois anos, o Congresso Nacional tenha editado duas importantes leis que tratam de cibercrime, as Leis n.º 12.735 e 12.737, de 30 de novembro de 2012, e, a disposição normativa que regula as relações civis na internet, Lei n.º 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, conhecida como Marco Civil da Internet.

A realidade brasileira, perante constatação inarredável de que a criminalidade cibernética aumenta na proporção das novas tecnologias digitais, a ausência de uma legislação penal específica, para tratar das novas condutas ilícitas praticadas no ambiente virtual, constitui um privilegiado elemento catalisador e estimulador da prática de ilícitos que, em última instância, atinge o direito fundamental à segurança, compromete o papel estatal da prevenção e da persecução penal e, enfim, conduz ao descontrole e à impunidade.

A bem da verdade, em que pese a escassez legislativa no que toca aos mecanismos de investigação de cibercrimes no ordenamento jurídico brasileiro, há que se considerar que a atuação dos órgãos investigativos estará, na maioria das vezes, pautada pela discricionariedade que faz parte do “poder geral de cautela” do magistrado criminal. O que significa que, mesmo inexistente, a previsão legal de medidas cautelares para cibercrimes, a eficácia probatória dependerá da habilidade do agente investigador, com capacidade postulatória, em requerer ao juiz criminal a produção de determinada prova digital. (GOMES, 2021).

Destaca-se que na investigação de cibercrimes, está no deferimento, após o pedido do órgão investigador, do espelhamento de unidades de armazenamento de dados de computadores. Não há previsão expressa de tal medida na norma processual penal brasileira, mas, novamente, se a legislação

não acompanha a velocidade da evolução dos meios de comunicação, cabe ao magistrado criminal a adoção da medida apta a garantir a prova.

A investigação de cibercrime é uma atividade que requer conhecimento especializado. Exige-se conhecimento técnico dos dispositivos utilizados para o seu propósito, conhecimento a computadores, celulares, mídia e outros meios de comunicação. Esclarecendo que o maior problema para a investigação brasileira de cibercrimes está na ausência de difusão de domínio técnico sobre esses novos dispositivos, já que a maioria dos agentes têm em sua rotina equipamentos obsoletos.

Recordando que em abril de 2023, o Brasil passou a ser signatário da Convenção de Budapeste onde autoridades brasileiras podem obter informações atualizadas em relação a crimes cibernéticos, e crimes que demandam provas eletrônicas/ digitais em outros países, facilitando muito a investigadores brasileiros ao combate aos crimes cibernéticos como também na coleta e preservação de provas digitais.

4. CONSIDERAÇÕES FINAIS

O sistema universal de proteção aos Direitos Humanos, não possui mecanismos suficientes ou mesmo órgão voltado ao combate aos crimes cometidos por meio da internet. Embora inicialmente se imagine que essa pauta diga respeito à cooperação jurídica internacional pura e simples, ponderando-se a acerca dos direitos humanos que merecem tutela especial, como a intimidade, a propriedade e a dignidade da pessoa humana.

A convenção de Budapeste, a despeito de tratar especificamente do cibercrime, foi firmada apenas no sistema regional europeu, e mesmo aberta à assinatura de outros países, não dispõe de mecanismos de monitoramento ou sanções ao descumprimento de suas diretrizes, funcionando apenas como um tratado de cooperação jurídica internacional na matéria.

Essas novas formas de violação aos direitos fundamentais tendem a ampliar-se com o advento da tecnologia, com potencial para desfigurar a organização político-administrativa que hoje é conhecida, o que deve ser o foco de atenção da comunidade internacional. O crime cibernético é uma realidade que está às portas da comunidade internacional, devendo ser combatido com

vigor, caso não seja, poderá trazer sérios danos não só aos Estados enquanto organização política, como a toda a população mundial.

Perante a carência na legislação, o avanço das redes tem continuado e com isso as brechas do sistema virtual podem ser facilmente manipuladas, pois sabemos que o direito nem sempre versa sobre todas as condutas, a menos que haja conhecimento de alguma ação que reforce a necessidade de uma legislação mais dura e ampla, como é o caso brasileiro. A partir do momento que excede a liberdade de expressão na internet deve haver responsabilização uma vez que em dado momento a vítima teve sua honra insultada ou a insegurança das redes trouxe prejuízos financeiros, e outros.

Mas um importante passo foi dado pelo governo brasileiro em ser signatário da Convenção de Budapeste, a troca de informações e experiências com outros países muito importante será ao combate à Criminologia.

REFERÊNCIAS

BRASIL. **Decreto nº 11.491**. de 12 de abril de 2023. Presidência da República. Disponível em:
https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em 11.07.2024.

BRASIL, Deilton Ribeiro. **A garantia do princípio constitucional da presunção de inocência (ou de não culpabilidade)**: um diálogo com os direitos e garantias fundamentais- Revista de Direito Brasileira, 2016, p. 393.

BRASIL. **Lei n.º 12.735**, de 30 de novembro de 2012. Disponível em:
http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em 17 jul. 2024.

BRASIL. **Lei n.º 12.737**, de 30 de novembro de 2012. Disponível em:
https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 17 abr. 2023.

CALDERON, Barbara. Deep e Dark Web: **A internet que você conhece é apenas a ponta do iceberg**. Rio de Janeiro: Alta Books, 2017, p. 77-78.

CARNELUTTI, Francesco. **As misérias do Processo Penal**. Leme: Edijur, 2020, p.45.

CASTELLS, Manuel. **Fim do Milênio**. V. III. São Paulo: Paz e Terra, 2007.

EUROPA. Conselho da Europa. **Convenção de Budapeste**. Disponível em:
<https://www.coe.int/pt/web/about-us>. Acesso em 07.07.2024.

GOMES, Marcus Alan de Melo; GUEDES, Inês Sousa. **Cibercriminalidade, novos desafios, ofensas e soluções**. Lisboa: Pactor Edições de Ciências; Sociais, Forense, 2021, p.5.

JUNIOR, Aury Lopes. **Sistemas de investigação preliminar no Processo Penal**. Rio de Janeiro: Lúmen Juris, 2003, p. 48.

LEMONS, André. A utopia da sociedade em rede: um mundo sem fronteiras? **Instituto Humanitas Unisinos**. 16 de setembro de 2008. Disponível em: www.ihu.unisinos.br/159-noticias/entrevistas/16737-. Acesso em 02.07.2024.

LÉVY, Pierre. **As tecnologias da Inteligência o futuro do pensamento na era da informática**. Tradução de Carlos Irineu Costa. 2. ed. São Paulo: Editora 34, 2016, p.154.

MANDARINO JUNIOR, Raphael; CANONGIA, Cláudia. (Org.). **Livro verde: segurança cibernética no Brasil**. Brasília: GSIPR/SE/DSIC, 2010, p.25

MAZZUOLI, Valério de Oliveira. **Curso de direitos humanos**. 6. ed. São Paulo: Método, 2018.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 7. ed. rev. São Paulo: Saraiva, 2012, p. 320.

NORTON. **Relatório de Crimes Cibernéticos: O impacto humano**. Disponível em: https://www.broadcom.com/404-symantec?sourceURL=http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_Portuguese-Human. Acesso em 18 jul. 2024.

OEA. Organização dos Estados Americanos. **Convenção Americana sobre Direitos Humanos, de 22 de novembro de 1969**. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm. Acesso em 15 jul. 2024.

ROTHENBURG, Walter Claudius. Direitos fundamentais e suas características. **Revista do Direito Constitucional e Internacional**, São Paulo, ano 8, p.146-151, jan./mar. 2000. Disponível em: <https://sismpbva.mpsp.mp.br/consulta/ArquivoList.aspx?idDocumento=6532084>Acesso em 18 jul. 2024.

SYDOW, Spencer Toth. **Curso de Direito Penal Informático**. São Paulo: Juspodium, 2022.

VELASCO, San Martin C. **La jurisprudência y competencia sobre delitos cometidos através de cómputo e internet**. São Paulo: Tirant to Blanch Brasil, 2012, p. 42.