O DIREITO À PROTEÇÃO DE DADOS SOB A ÓTICA DAS VULNERABILIDADES DO USUÁRIO

THE RIGHT TO DATA PROTECTION FROM THE VIEW OF USER VULNERABILITIES

Emanuelle Ricardo Finger[1]
Sabrina Favero[2]

RESUMO

Este texto tematiza a legislação referente à proteção de dados na perspectiva da vulnerabilidade dos usuários a ataques cibernéticos que ocorrem no Brasil. A partir da constatação de que o país é um dos que mais sofrem esse tipo de ocorrência, o objetivo é verificar se as normas positivadas prestam-se a garantir a segurança dos dados. Ao confrontar as normas postas com os dados estatísticos, percebe-se que grande parte das vulnerabilidades são produto do fator humano, daí porque a simples regulamentação tem sido insuficiente para atingir o objetivo da legislação. Nesse sentindo, a educação digital, como política pública a ser implantada em todos os níveis de ensino e a contemplar todas as faixas etárias, forma, juntamente com a legislação, um amálgama necessário para a proteção deste novo direito. O estudo foi subsidiado por pesquisa bibliográfica, documental e jurisprudencial, com utilização do método dedutivo e com a sucessão de quatro etapas. Na primeira, apresentaram-se as razões pelas quais é necessária proteção jurídica aos dados pessoais; posteriormente, a proteção de dados foi apresentada como um novo direito fundamental; na terceira etapa, discorreu-se sobre as vulnerabilidades do usuário de internet a ataques cibernéticos; no último tópico, tratou-se sobre a educação digital.

Palavras-chave: Proteção de dados; vulnerabilidades; educação digital.

ABSTRACT

This text discusses the legislation regarding data protection from the perspective of the vulnerability of users to cyber attacks that occur in Brazil. Based on the fact that the country is one of the countries that suffers the most from this type of occurrence, the

[1]Acadêmica do Curso de Direito da Universidade do Contestado (UNC). Campus Concórdia. Santa Catarina. Brasil. E-mail: emanuellefinger@gmail.com.
[2]Doutoranda em Direito pela Universidade do Oeste de Santa Catarina (UNOESC). Possui graduação em Direito pela Universidade do Contestado (2004) e Mestrado em Direito pela Universidade do Oeste de Santa Catarina (2016). Atualmente é celetista da Universidade do Contestado e estatutário - Tribunal de Justiça do Estado de Santa Catarina. E-mail: sabrinafavero1000@gmail.com.

objective is to verify if the positive norms lend themselves to guaranteeing data security. When comparing the rules set with the statistical data, it is clear that most vulnerabilities are the product of the human factor, hence why simple regulation has been insufficient to achieve the objective of the legislation. In this sense, digital education, as a public policy, to be implemented at all levels of education and to include all age groups, forms, together with the legislation, a necessary amalgamation for the protection of this new right. The study was supported by bibliographic, documentary and jurisprudential research, using the deductive method and with the succession of four stages. The first presented the reasons why legal protection of personal data is necessary; later, data protection was presented as a new fundamental right; in the third stage, the vulnerabilities of the internet user to cyber attacks were discussed; in the last topic, it was about digital education.

Key words: Data protection; vulnerabilities; digital education.

Artigo recebido em: 29/07/2022

Artigo aceito em: 07/10/2022

Artigo publicado em: 28/05/2024

Doi: https://doi.org/10.24302/acaddir.v6.4347

1 INTRODUÇÃO

A Humanidade está, desde sempre, em um contínuo ciclo de mudanças. Nas últimas décadas, contudo, esse processo intensificou-se em razão da revolução tecnológica. A velocidade das transformações parece ser o paradigma de nossa sociedade, que, com uma periodicidade cada vez menor, vê entendimentos serem superados, novas rotinas adquiridas e uma profunda transformação das relações humanas sendo construída. Apoiadas na popularização da internet, a comunicação e a sociabilidade parecem estar migrando do meio físico para o digital, o que rompe com barreiras físicas e temporais.

Nesse contexto, ao mesmo tempo em que surge a necessidade de se tutelarem novos direitos, há uma revisitação de outros que, embora já assentados no ordenamento jurídico, precisam ser adaptados às novas dinâmicas sociais, na medida em que, como esclareceu Miguel Reali, o Direito não é apenas norma, como também, fato e valor.

O objeto deste estudo é a proteção de dados pessoais, um desses novos direitos que emergiram do processo de digitalização do mundo[3]. Recentemente alçado à categoria de direito fundamental pela Emenda Constitucional 115, de 10 de fevereiro de 2022, representa um marco histórico da tutela da privacidade no Brasil.

Ainda que de inequívoca atualidade, a problemática adquiriu maior relevância diante do cenário pandêmico ocasionado pela COVID-19, quando, subitamente, milhões de pessoas viram-se obrigadas a utilizar plataformas virtuais, tornando suas vidas mais digitais, na mesma proporção em que suas vulnerabilidades também aumentaram.

Sob essa perspectiva, o artigo propõe-se a analisar se a proteção jurídica fornecida pelo ordenamento brasileiro é (ou pode vir a ser) suficiente para resguardar a proteção de dados do usuário da Internet, tendo em conta sua vulnerabilidade, que está relacionada ao conhecimento dos riscos que a rede pode oferecer.

Para a consistência e fundamentação, foram consultadas bases legislativas nacionais, com referencial teórico especializado sobre o assunto. A metodologia para a elaboração da investigação foi subsidiada por pesquisa bibliográfica, documental e jurisprudencial, com utilização do método dedutivo e com a sucessão de quatro etapas. Na primeira, analisaram-se os motivos pelos quais a proteção de dados é importante; na segunda, procedeu-se ao exame da evolução da proteção de dados à categoria de direito constitucional; posteriormente, discorreu-se sobre as vulnerabilidades do usuário de internet; no último tópico, tratou-se sobre a educação digital.

2 POR QUE PROTEGER DADOS PESSOAIS?

Compreender a necessidade jurídica de proteção de dados passa, previamente, pelo entendimento desse novo paradigma da comunicação surgido do desenvolvimento das tecnologias da informação, que criaram um meio ambiente virtual.

[3]A digitalização do mundo é a conversão de processos, ações, informações, migrando do meio físico para o virtual, fomentando a globalização. Um dos seus princípios balizadores é florescer a relação humana através da tecnologia.

Foi Lévy (1999) que cunhou os termos “ciberespaço” e “cibercultura” para designar essas novas formas de comunicação surgidas a partir da internet. Ciberespaço – também chamado de rede – é, segundo ele, a forma de comunicação surgida a partir da interconexão mundial dos computadores, compreendendo não apenas a infraestrutura material, como também as informações e as pessoas que utilizam esse universo. Já cibercultura é a cultura surgida no ciberespaço, isto é, são as técnicas, práticas, atitudes, valores e modos de pensar que se desenvolvem no ciberespaço.

Essa nova dinâmica de comunicação fez surgir as redes sociais, estruturadas na interconexão proporcionada pela internet. As comunidades virtuais orientaram o crescimento inicial do ciberespaço. Elas são fruto de afinidades de interesses, de conhecimento e de cooperação, apoiado na interconexão e independente de proximidade geográfica, representam, ainda, uma nova maneira de expor opinião pública (LÉVY, 1999).

Nesse cenário, os dados das pessoas circulam cada vez mais em ambientes virtuais, sendo uma valiosa fonte de extração de informações. Os usuários que trafegam na rede, por muitas vezes, possuem a sua privacidade comprometida pela exposição de seus dados pessoais, sem a consciência do quão frágil isso pode torná-lo frente a um *hacker* (BARBOSA et al., 2021).

É que os ambientes virtuais, além de abarcarem enorme fluxo de interação e interconexão entre as pessoas, são palco de manifestação de ideias, pensamentos e informação. Como exemplos, citam-se Facebook, YouTube, Instagram, Twitter, entre outros, todas geridas por grandes empresas de tecnologia que almejam lucro. Mas não só. Há hoje um modelo de negócios que se desenvolve no ciberespaço, seja na prestação de serviços, seja no comércio, na educação e até mesmo nos serviços públicos e de cidadania.

Todos os usuários estão, portanto, propícios a terem os seus dados pessoais utilizados de forma indevida, na medida em que, para consumirem serviços oferecidos pela internet, muitas vezes é-lhes exigido o compartilhamento dados e permissões, sob pena de restrição ou mesmo impedimento de acesso ao serviço (LIGUORI, 2022).

Percebe-se, dessa forma, que esses serviços, muitos dos quais tidos como gratuitos, na realidade apropriam-se dos dados pessoais dos usuários, sob a falácia de uma “permissão”, para comercializá-los posteriormente.

Além dessa prática, já conhecida, há também o denominado “sequestro” de dados, prática utilizada por *hackers*. Segundo Liguori (2022, p. 18) o *hacker* é o indivíduo que quebra a criptografia ou a segurança de qualquer meio informatizado para obter informações. As consequências, quando o *hacker* obtém êxito em sua investida, são incalculáveis e vão desde a manipulação do usuário com base em seu perfil de interesses, até mesmo a insegurança financeira.

O uso de um ataque poderá conceder ao sequestrador de dados acesso a contas bancárias, senhas de cartões, contas virtuais e informações sobre a sua atividade laboral (OLIVEIRA; LANZILLO, 2021).

Com a popularização da internet foi necessária a implementação de lei específica para estabelecer o uso, garantias e deveres da utilização desta ferramenta no Brasil. O Marco Civil da Internet (MCI), introduzido na legislação por meio da Lei 12.965/2014, foi criado para exteriorizar garantias fundamentais da Constituição Federal e atrelar responsabilidade ao usuário no momento da utilização da rede (LEITE; LEMOS, 2017).

O MCI prevê novos direitos ao usuário, mas o grande foco da referida lei está nos seus artigos 10 e 11. Esses artigos priorizam a manutenção da integridade dos dados, desde a sua coleta até a disponibilização a outro órgão, deixando evidente que esse dado somente será disponibilizado mediante ordem judicial ou requisição de órgão competente. Evidenciam a importância de preservar o sigilo e a confidencialidade das informações dos usuários em um ambiente controlado e seguro, prescrevendo que qualquer irregularidade ao acesso sem a devida ordem judicial enquadra-se como um comportamento ilegal e o usuário responsável arcará com os ônus de expor/coletar dados de forma indevida. Neste sentido, é possível vislumbrar que um dos principais objetivos da lei, além da tutela de todas essas garantias, é assegurar um ambiente digital digno e saudável aos seus usuários (LEITE; LEMOS, 2017).

Além de prever garantias e deveres na rede, o MCI também elencou no seu art. 26 o dever de as instituições de ensino prestarem educação digital para todas as idades. Assim, desde cedo as crianças deveriam entender a importância do uso responsável e consciente da internet, compreendendo quais os limites entre a liberdade de expressão e os discursos de ódio, além da apresentação de temas como segurança da informação e a proteção de dados (JESUS, 2014).

Importante destacar que, a incorporação do termo “proteção de dados” na legislação é recente, apesar da constatação de que esse direito sempre foi relacionado a direitos fundamentais da Constituição Federal. O embasamento legal para suprir a falta de legislação especial sobre o tema estava atrelado ao direito à privacidade, ao *Habeas Data*, ao MCI e até mesmo ao Código de Defesa do Consumidor (DONEDA, 2018).

Após alguns anos da entrada em vigência do MCI, foi promulgada a Lei 13.709/2018 – a Lei Geral de Proteção de Dados (LGPD) que representou um marco histórico na legislação brasileira no que concerne à proteção da privacidade.

É que os dados pessoais se relacionam, à toda evidência, com a privacidade dos indivíduos, direito fundamental previsto no art. 5º, X: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 2022).

Anteriormente à referida lei, só existiam legislações esparsas sobre o tema, hoje, a LGPD regulamenta todo e qualquer tratamento de informações referente a dados pessoais, normatizando princípios, direitos e obrigações no manuseio, armazenamento e coleta dessas informações (PINHEIRO, 2020).

A LGPD, ao dispor sobre o tratamento de dados, tem como objetivo a proteção da liberdade, privacidade e desenvolvimento da pessoa natural. Sublinhe-se: a lei não se destina à tutela de direitos da pessoa jurídica, apenas da pessoa natural. Dentre seus fundamentos, estão o respeito à privacidade e a autodeterminação informativa.

Expressamente conceitua dado pessoal como “informação relacionada a pessoa natural identificada ou identificável”. O conceito é abrangente para abarcar todas as espécies de dados. Dados que podem apresentar pouca relevância, se conectados com outras informações do indivíduo podem construir um perfil completo do usuário, chegando em dados específicos, inclusive, de caráter sensível (VIOLA; TEFFÉ, 2020).

A origem do direito à autodeterminação informativa remonta ao julgamento, pelo Tribunal Constitucional Alemão, do “BVERFGE 65, 1”. O caso remonta à discussão levada à Corte da Lei do Censo (*Volkszählungsgesetz*) de 1983, de 25 de março de 1982 (BGBl. I, p. 369), que determinou, “[...] o recenseamento geral da população, com dados sobre a profissão, moradia e local de trabalho para fins estatísticos”. Diversas reclamações foram ajuizadas com fundamento na violação ao

livre desenvolvimento da personalidade, tendo o Tribunal, no mérito, declarado nulos alguns dispositivos da lei, principalmente os que tratavam da "[...] comparação e trocas de dados e sobre a competência de transmissão de dados para fins de execução administrativa" (SCHWABE, 2002, p. 233-234).

Hoje, compreende-se como o direito de titularidade da pessoa natural de proteção contra coleta, tratamento e revelação de seus dados pessoais (LEONARDI, 2011).

A autodeterminação informativa, como um dos princípios balizadores da LGPD, está intrinsecamente ligada a outros princípios constitucionais, como a dignidade da pessoa humana, visto que proporciona ao usuário o livre desenvolvimento de sua personalidade e autonomia em relação aos seus dados pessoais. Para estar em conformidade, a autodeterminação informativa deve estar ancorada em um consentimento livre e informado, motivo pelo qual o usuário deve ter clareza do que está consentindo (BACHUR, 2021).

Não obstante, o direito à autodeterminação informativa soa como um devaneio nos dias atuais, tendo em vista que o consentimento livre e esclarecido é inerente à sua concretização. Todos os dias há, entretanto, uma massiva disseminação de propagandas que são criadas a partir mapeamento do perfil de interesse dos usuários, advindos de permissões concedidas de forma consciente ou inconsciente. Outro exemplo que pode ser citado são os termos de adesão de produtos e serviços, que não deixam muitas escolhas ao usuário, isto é, ou ele aceita todas as condições de uso, que são redigidas de forma técnica e por muitas vezes de complexa compreensão ou ele não poderá dispor daquele determinado produto/serviço (LUGATI; ALMEIDA, 2020).

Daí porque é possível questionar até que ponto, de fato, existe consentimento, e, por consequência, autodeterminação informativa, no compartilhamento dos dados pelos indivíduos, havendo mesmo aqueles que defendem tratar-se de um mito.

3 PROTEÇÃO CONSTITUCIONAL DE DADOS

Os riscos advindos do compartilhamento de dados no ambiente virtual desencadearam uma reação constituinte. Se, historicamente, o constitucionalismo surgiu como uma teoria (ou ideologia) de limitação do poder estatal por meio de

constituições escritas e de declaração de direitos fundamentais, hoje percebe-se que, não apenas os atores estatais podem abusar do exercício de poder.

Um alerta, no entanto, é necessário. Quando se analisa a internet, há que se ter em conta duas faces distintas: a da potencialização de algumas garantias fundamentais, como a liberdade de expressão e a manifestação política; e, por outro lado, outros riscos emergem, como o abuso do direito da liberdade de expressão, encontrando-se diversos discursos odiosos em ambientes virtuais ou até disseminação de notícias falsas, colocando-se em choque os benefícios e malefícios da Internet (MENDES; FERNANDES, 2020).

Atualmente, há um enorme poder nas mãos de quem tem conhecimento para adquirir informações. E dados pessoais são informações valiosíssimas, são, com efeito, fontes de poder. E o advento da LGPD trouxe novas luzes sob o direito à privacidade e a proteção de dados na Jurisdição Constitucional.

Em 2020, o Supremo Tribunal Federal (STF) referendou a Medida Cautelar concedida pela Ministra Rosa Weber, relatora das Ações Diretas de Inconstitucionalidade (ADIs) n. 6.387, 6.388, 6.390, 6.393. As ações questionavam a Medida Provisória (MP) n. 954/2020 ao argumento de que ela contrariava princípios e garantias constitucionais, como a dignidade da pessoa humana e a inviolabilidade da intimidade e da vida privada (MENDES; RODRIGUES JÚNIOR; FONSECA, 2020).

É que a MP 954/2020 previa que empresas de telecomunicação prestadoras de serviço de telefonia fixo, comutado e de serviço móvel pessoal deveriam disponibilizar diversos dados pessoais de seus consumidores ao Instituto Brasileiro de Geografia e Estatística (IBGE). A argumentação utilizada pela defesa da MP n. 954/2020 é que com a pandemia do COVID-19 o acesso a entrevistas presenciais foi restringido, dessa forma, com a disponibilização dos dados pessoais pelas empresas de telecomunicação traria a produção de estatísticas oficiais (PAVANI; HERMES, 2021).

A MP possuía vícios formais e materiais, ou seja, tanto em sua redação quanto a sua consonância com a Constituição Federal. A redação, extremamente genérica e vazia, não contemplava argumentos plausíveis para tratar de dados pessoais, somente informava que seu objetivo era criar uma produção estatística para fins de emergência e saúde pública em decorrência da pandemia do coronavírus (COVID-19). Também não informava quais medidas seriam adotadas para zelar pela

segurança da informação dos dados coletados, sem garantias que esses dados realmente seriam tratados de forma congruente e que o IBGE teria os meios de segurança adequados para proteger e impedir o vazamento de dados (MENDES; RODRIGUES JÚNIOR; FONSECA, 2020).

A relatora, Ministra Rosa Weber, deferiu a medida cautelar requerida, suspendendo a eficácia da MP, para prevenir a exposição de milhões de dados, resguardando a intimidade e a vida privada dos indivíduos. No mérito, retomou os argumentos ensejadores da concessão da liminar, dentre os quais: o direito à privacidade e à autodeterminação informativa são os fundamentos da proteção dos dados pessoais; a MP não agrega interesse público legítimo a justificar o compartilhamento de dados, pois não define a forma de utilização de tais dados nem mecanismos de proteção contra acessos não autorizados; o estado de emergência sanitária deflagrado pela pandemia não pode justificar, assim, enfraquecimento de direitos fundamentais. Após o voto da Ministra Rosa Weber, mais dez ministros acompanharam o seu voto. Não há somente a conquista do direito à proteção de dados exposto nesta decisão, mas essa foi a primeira vez que o Supremo Tribunal Federal reconheceu explicitamente o direito à proteção de dados (BRASIL, 2020).

Este julgamento foi paradigmático, na medida em que reconheceu a proteção de dados como corolário de direitos fundamentais quais sejam: liberdade individual, a privacidade e livre desenvolvimento da personalidade.

De fato, a invocação do direito à privacidade (já consagrado na Constituição Federal desde 1988) para suprir lacunas atinentes à proteção de dados era frequente, apesar de, quando do julgamento da ADI 6.387, já tramitar no Congresso Nacional Proposta de Emenda Constitucional (PEC) com o objetivo de inserir expressamente no texto constitucional a proteção de dados como um direito fundamental.

Na justificativa da PEC n. 17/2019, apresentada pelo Senador Eduardo Gomes (MDB-TO), ponderou-se que a privacidade estava sendo o ponto de partida para discussão em torno da proteção de dados pessoais, mas que, com a evolução histórica da sociedade e o avanço da tecnologia, esse direito já possui autonomia valorativa a ponto de merecer tratamento constitucional específico (SENADO FEDERAL, 2022).

Na proposta apresentada, também existiu a necessidade de estabelecer a competência constitucional para legislar sobre o tema, dada a pluralidade política da

matéria, o que poderia acarretar insegurança jurídica, por existirem diversos conceitos e entendimentos sobre a proteção de dados pessoais (GOMES, 2019).

Assim é que, em 11 de fevereiro de 2022 foi promulgada a Emenda Constitucional n. 115 que acrescentou ao rol dos direitos e garantias fundamentais a proteção de dados e estabeleceu a competência da União para legislar sobre a matéria. Hoje, nos termos do art. 5º, LXXIX da Constituição Federal: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (BRASIL, 2022).

O reconhecimento da proteção de dados como um direito fundamental é um marco regulatório e uma sinalização de que o Estado reconhece a complexidade e fragilidade dos ambientes virtuais. Após a positivação constitucional, o desafio agora é a implementação de mecanismos para fomentar a segurança da informação e fortalecer o conhecimento do usuário sobre as suas vulnerabilidades, sob pena de a proteção constitucional representar tão-somente uma normatização simbólica[4].

4 VULNERABILIDADES DO USUÁRIO DE INTERNET

Nos termos já expostos anteriormente, as plataformas digitais estão se tornando cada vez mais presentes no cotidiano dos indivíduos, vive-se um processo de hibridização do mundo[5], as pessoas transacionam financeiramente via aplicativos, exercem suas atividades laborativas mediante a utilização da internet, socializam pela rede. Com o aumento de usuários utilizando plataformas digitais, também existe o aumento de dados trafegando de um ambiente a outro, o que gera constantes vulnerabilidades aos titulares desses dados.

As vulnerabilidades do usuário de internet estão relacionadas com sua fragilidade em relação à rede. As inseguranças atreladas a rede estão lincadas a softwares falhos, hardwares desprotegidos e falhas humanas, todos estes elementos

[4] Constituição simbólica, na lição de Neves (1996, p. 326), ocorre quando "[...] à atividade constituinte e à emissão do texto constitucional não se segue uma normatividade jurídica generalizada, uma abrangente concretização normativa do texto constitucional.

[5] Hibrido, segundo o Dicionário Michaelis (2022) é: "Que ou que é composto de elementos distintos ou disparatados". A hibridização do mundo está ligada a processos que estão em fase de migração do mundo físico para o virtual, de conexões palpáveis, para conexões virtuais.

criam vulnerabilidades ao usuário, aumentando a probabilidade de existirem vazamentos de dados.

A despeito da complexidade dessas vulnerabilidades, que contemplam desde cyberbullyings, vulnerabilidades de grupos específicos (como crianças, idosos, do consumidor), da autonomia informativa, da perfilização, dentre outras, este trabalho atenta para a vulnerabilidade humana oriunda da falta de conhecimento do usuário sobre segurança na internet, que torna a rede um locus propício para atuação de cibercriminosos, que afeta não apenas indivíduos, como também organizações (públicas e privadas).

Segundo a Organização das Nações Unidas (ONU) mais 782 milhões de pessoas ficaram online no período de 2019 a 2021, os acessos foram intensos devido a pandemia do COVID-19. No Fórum de Governança da Internet da ONU foram abordados os crescentes números de ciberataques, 7 mil violações de dados foram registradas em 2019, expondo mais de 15 milhões de registros.

No Brasil, é cada vez mais recorrente as notícias sobre o vazamento de dados. Em setembro de 2021, a Associação Nacional dos Profissionais de Privacidade de Dados (ANPPD) noticiou que mais de 400 milhões de dados pessoais foram vazados, expondo a vida e a privacidade dos brasileiros.

A proliferação do acesso à internet tornou inevitável que o ataques e vazamentos de dados sejam cada vez mais recorrentes, muito devido à falta de conhecimento e consciência das pessoas sobre o risco de expor a sua vida pessoal em redes sociais. Essa brecha é utilizada por hackers, que encontram vulnerabilidades e informações confidenciais de forma mais célere e direcionada.

Segundo Mitnick e Simon[6] (2003, p. 15) “o fator humano é o elo mais fraco da segurança”. A segurança digital é construída quando o usuário toma conhecimento de que um simples firewall[7] não irá proteger a sua privacidade. Segurança digital pressupõe a compreensão de que os dados e as rotinas disponibilizadas em redes

[6]Kevin Mitnick é um *hacker* estadunidense conhecido mundialmente. Foi um dos *hackers* mais procurados pelo *Federal Bureau of Investigation* (FBI). Sua técnica mais utilizada foi a engenharia social. Desta forma, por mais que a referência seja antiga, Mitnick apresenta amplo conhecimento e experiência nesta técnica.

[7]*Firewall* é uma ferramenta utilizada para identificar e prevenir ataques cibernéticos, criando um filtro do que é confiável e barrando as ameaças da rede (VARTOUNI; TESHNEHLAB; KASHI, 2019)

sociais acarretam a construção de um perfil, que poderá ser utilizado na obtenção de senhas, rotinas, rotas, dados e demais informações.

Através da engenharia social, é possível manipular pessoas, compelindo-as a praticar atos que podem ou não ser de seus interesses. Trata-se assim, não especificamente de uma ação, mas de uma habilidade, que nem sempre é utilizada de forma nociva. Algumas pessoas tem um talento natural para elas, outras, a adquirirem (HADNAGY, 2011).

Quando utilizada de forma danosa, a engenharia social é uma das práticas mais recorrentes no sequestro de dados, quando o hacker utiliza da confiabilidade do alvo para persuadi-lo e fazer com que ele exponha as suas vulnerabilidades de forma voluntária e inconsciente. O engenheiro social explora seus alvos e os manipula para que estes forneçam os seus dados, em uma conversa que aos olhos do usuário parece ser despretensiosa (SILVA; ARAÚJO; AZEVEDO, 2013).

A engenharia social é uma técnica simplificadora para qualquer tipo de ataque cibernético, seja ele um ransomware ou um phishing[8]. Entender o alvo e quais são as formas mais eficazes de realizar o ataque tornam a iniciativa mais assertiva. Neste sentido, muitas vezes a engenharia social é utilizada em conjunto com outros métodos de ataque, potencializando a sua efetividade.

Os indivíduos possuem um fator biológico que tem forte impacto em suas vulnerabilidades e que induz de forma inconsciente ao erro humano no que tange à segurança da informação: o ser humano é sociável; necessita da cooperação dos demais e essa característica o torna flexível para seguir os hábitos dos indivíduos que possui como referência. Assim, o indivíduo tende a seguir o comportamento daqueles que o circundam, para neutralizar o sentimento de exclusão social (LANNES, 2020).

A nova dinâmica de comunicação construída pela evolução das tecnologias da informação fez surgir as redes sociais, estruturadas na interconexão proporcionada pela internet. As comunidades virtuais orientaram o crescimento inicial do ciberespaço. Elas são fruto de afinidades de interesses, de conhecimento e de cooperação, apoiado na interconexão e independente de proximidade geográfica, representam, ainda, uma nova maneira de expor opinião pública (LÈVY, 1999).

[8] *Phishing* é um ataque de engenharia social utilizado para obter dados confidenciais, geralmente é efetuado por meio de e-mails falsificados, direcionando o assunto aos interesses do usuário (ABROSHAN, 2021).

Constituem um facilitador para os indivíduos incrementarem as relações humanas; não obstante, a carência pela socialização e pela aprovação social acarreta em um bombardeio de informações diárias em ambientes virtuais. O próprio usuário expõe a sua vida e a sua rotina em troca de atenção generalizada (SILVA; ARAÚJO; AZEVEDO, 2013).

Essa forma de comportamento na rede impulsiona ataque aos dados pessoais. Um deles é o phishing, que utiliza o perfil de interesse do usuário explorando a sua necessidade, desde a contratação para uma atividade laboral, até compras em lojas online. Usualmente o phishing é feito mediante e-mails, mas não se limita a esta plataforma, podendo ser realizado através das redes sociais, como Facebook e Instagram. Os jovens são mais propensos a sofrerem este ataque, porque a sua tomada de decisão é instantânea, ou seja, sem reflexão sobre o conteúdo apresentado (ABROSHAN et al., 2021).

Existem diversas espécies de phishing, porém, a mais perigosa para o usuário é o que carrega um ransomware. O ransomware é utilizado como meio de extorsão, no qual o sequestrador de dados chantageia o usuário a efetuar pagamento de forma não rastreável, geralmente em criptomoeda, em troca da descriptografia dos arquivos. O ransomware é uma atividade lucrativa, visto que o sequestrador vende as informações obtidas ao principal interessado, o proprietário dos dados (FORNASIER; SPINATO; RIBEIRO, 2020).

O ransomware é feito em larga escala, atingindo cerca de 3% da população mundial. Após detectada a vulnerabilidade do software, o sequestrador tem acesso a todos os arquivos do computador, além de possuir acesso a webcam da vítima, podendo direcionar a chantagem a momentos íntimos. Os ataques tornam-se cada vez mais aprimorados, não só na questão técnica, mas também na estratégia e persuasão da chantagem (FORNASIER; SPINATO; RIBEIRO, 2020).

A tecnologia é disruptiva, rompendo barreiras do conhecimento e evoluindo diariamente. Os hackers se aprimoram da mesma forma, criando novos mecanismos e utilizando técnicas de inovação aprimoradas para tornar o ataque cada vez mais refinado. Por outro lado, o usuário está cada vez mais vulnerável, sofrendo ataques diários e ficando à mercê de cibercriminosos.

Alguns ataques são efetuados de forma automatizada, como nos casos de ataque de “força bruta”, em que incansavelmente o software tenta todas as

combinações alfanuméricas possíveis para alcançar a senha pretendida. Alcançando as senhas, o sequestro se estende às demais informações desejadas. Quanto mais "fraca" é a senha, mais frágil torna-se o usuário, concretizando o objetivo do hacker de forma célere. Existem algumas situações que podem obstruir a realização deste ataque, como a criação de uma senha "forte" e a autenticação em dois passos, são fatores que vão dificultar a investida do hacker, mas não irão garantir a falibilidade na execução do sequestro (LIGUORI, 2022).

Algumas falhas dos usuários também podem ser encontradas na forma que as informações são repassadas. Em 14 de dezembro de 2021 a ANPPD divulgou em seu sítio da internet uma matéria sobre o vazamento de dados do Ministério da Saúde. A intenção da matéria era enfatizar a autonomia da Autoridade Nacional de Proteção de Dados (ANPD) na fiscalização da LGPD. Ao longo da matéria, no entanto, percebe-se que a própria ANPD reporta dificuldades em identificar os danos que os ataques cibernéticos podem causar. A ANPD parece admitir não ter "braços" para apurar todos os ataques que acontecem no Brasil, tornando-se um chamariz para hackers.

Em 2018 a IBM Security[9] divulgou uma pesquisa em escala global calculando os índices e os custos médios de uma violação de dados. O estudo foi dirigido a 500 empresas de 15 países distintos. Foram constatadas mais de 50 milhões de violações, e a estimativa financeira em torno dessas violações é de US$350 milhões de dólares na economia, em comparação com o ano de 2017 houve uma crescente de 6,4% de violações.

A pesquisa ainda relata quais são as maiores falhas na segurança da informação, advindo de falhas no sistema e erro humano, novamente sendo constatadas as vulnerabilidades do usuário frente a cibercriminosos. O tempo médio para detectar e conter essas violações foi de 365 dias, tempo este que os hackers tiveram disponível para explorar os dados da empresa, dos funcionários e de seus clientes. O estudo ainda relata que o Brasil é o país com maior probabilidade de sofrer violações de dados, possuindo uma estimativa de 43%, a média global é de 27%.

O Brasil é, portanto, um país frágil em segurança da informação. Segundo a IBM Security, a taxa de erros humanos é de 32%, quando a média de outros países

[9] A IBM é uma empresa estadunidense voltada para o ramo da informática. É uma empresa consolidada no mercado e referência em segurança da informação, sua fundação foi em 1911.

chega a 25%. Daí porque, além das melhorias que são feitas em sistemas, o Brasil precisa capacitar seus usuários da internet (LANNES, 2020).

Como se vê, os resultados das pesquisas demonstram que as maiores vulnerabilidades em segurança da informação são resultado do fator humano, ou seja, do comportamento do usuário.

Desta forma, além de órgãos competentes para fiscalização, que protegem dados por meio de sanções administrativas, como multas, publicização de infrações, suspensão do exercício da atividade da empresa penalizada, a mitigação das vulnerabilidades passa, necessariamente pela educação digital.

5 EDUCAÇÃO DIGITAL

O ambiente digital jamais será 100% seguro ou imune a práticas nocivas de uns em detrimento de outros. Como bem pondera Hadnagy (2011), a segurança total somente seria possível com a desconexão de todos os dispositivos eletrônicos e com a mudança para as montanhas.

Se, como se viu, o fator humano é o que mais propicia ataques cibernéticos, é evidente que as pessoas devem ser estimuladas ao conhecimento sobre segurança digital.

Nesse sentido, o MCI elencou em seu art. 26 o dever do Estado na prestação de educação digital em todos os níveis de ensino. A educação digital, como produto da transformação tecnológica, tem como premissa capacitar o usuário para a utilização consciente e responsável da rede, primando pela segurança da informação em ambientes virtuais.

Segundo a Base Nacional Comum Curricular (BNCC), disponibilizada pelo Ministério da Educação (MEC, 2022) as matérias obrigatórias no nível médio de ensino são: I – linguagens e suas tecnologias; II – matemática e suas tecnologias; III – ciências da natureza e suas tecnologias; IV – ciências humanas e sociais aplicadas; V – formação técnica e profissional.

A maioria das disciplinas ministradas no ensino médio aprofundam os conhecimentos adquiridos no ensino fundamental. Pode-se observar que não há exigências do MEC para existir educação digital nas grades curriculares, tornando a

matéria de previsão discricionária por parte dos Estados e Municípios. Isso vai de encontro ao dever estatal de prestar educação digital.

Com a alfabetização digital nas escolas, os alunos seriam impulsionados a pensar de forma crítica e analisar diversas situações corriqueiras no ambiente virtual. A inserção da segurança digital como disciplina obrigatória nas grades curriculares assegura aos estudantes o direito de adquirir conhecimentos interdisciplinares. Assim, seria possível a compreensão de como funciona um ataque cibernético e como o usuário pode construir sua defesa (NICOLETE et al., 2021).

A educação deve acompanhar a evolução tecnológica, o Estado tem a obrigação de fornecer aos indivíduos um meio de adquirir conhecimento conforme os avanços ocorrem no mundo. Estar consciente dos riscos da internet, entender como esses riscos se manifestam e o porquê eles são cada vez mais frequentes são fundamentais para o usuário evoluir. Essa evolução só é possível através do aprendizado, que poderia ser repassado com método e assertividade nas escolas (GILL, REDEKER; GASSER, 2015).

A tecnologia cria, modifica e evolui todos os dias, a educação precisa conter essa volatilidade, possibilitando ao aluno a oportunidade de programar e manipular dados. Não há como estabelecer um método para a prevenção de ataques cibernéticos, sem que o usuário tenha experiência e convívio com essas formas de ataque. Direcionar e ensinar o usuário sobre quais possibilidades existem e como elas podem evoluir pode reduzir drasticamente o percentual de vazamento de dados no Brasil. O pensamento crítico e o entendimento de como funciona a cabeça de um hacker são primordiais para maximizar a cibersegurança. Atualmente as salas de aula possuem métodos obsoletos e padronizados, o que dificilmente gera interesse no aluno. Outro ponto crucial é a necessidade atual de esmiuçar a matéria, transcorrendo sobre um assunto em diversas aulas. Hoje, o aluno possui acesso imediato ao conhecimento através da Internet, o que ele precisa é ser instigado a se desenvolver em aulas dinâmicas e que aproximem o aprendizado dos anseios de seu cotidiano (MIZUSAKI, 2021).

No cenário atual, o Estado não dispõe de possibilidades acadêmicas nos primeiros anos de ensino para os indivíduos se desenvolverem e buscarem conhecimento sobre proteção de dados. Assim como a disciplina de linguagens, que

é vital para desenvolver a comunicação do aluno, a educação digital é indispensável para o usuário entender em qual mundo está inserido.

A pandemia COVID-19 serviu como promotora de mudança, avanços que possivelmente demorariam anos para acontecer, ocorreram de 2020 a 2022. Pode-se dizer que a realidade “pós” pandemia alterou a forma como as pessoas socializam, consomem ou estudam. A educação foi direcionada para plataformas virtuais, e mesmo com essas alterações a BNCC não promoveu alteração curricular para contemplar a educação digital.

De fato, a necessidade do distanciamento social no período de pandemia, as escolas foram compelidas a se reinventar, criando novas metodologias de ensino para a educação a distância (EaD). Esse movimento descortinou as dificuldades e falta de compreensão de como funcionam as tecnologias da informação e comunicação (TIC), tanto dos docentes como dos discentes. O uso das TIC são um desafio, a maioria das pessoas as utilizam como meio de entretenimento e não como uma ferramenta para adquirir conhecimento (CASTAMAN; RODRIGUES, 2020).

Se a educação digital já estivesse agregada à base curricular, grande parte das dificuldades acadêmicas enfrentadas na pandemia poderiam ter sido mitigadas. Os esforços que nesse período foram necessários ao aprendizado do que são e como funcionam as TIC, teriam sido aproveitados.

A pandemia serviu como alicerce para identificar as fragilidades do sistema educacional brasileiro. Os desafios enfrentados ao longo do período pandêmico só afirmaram que os métodos de ensino obsoletos devem ser superados, dando oportunidade a novas estratégias de ensino, munidas de tecnologia e informação. A constatação de que docentes e discentes tiveram dificuldades em utilizar as TIC, serve como meio afirmativo de que a educação precisa passar por um processo de reestruturação (CASTAMAN; RODRIGUES, 2020).

O Ensino Remoto Emergencial foi uma medida rápida para proporcionar educação em meio a pandemia, mas tornou-se precário por não haver planejamento sobre as etapas de implantação deste processo. Pontos primordiais como acesso à internet e desigualdade social afetam intrinsecamente o aproveitamento acadêmico do estudante, gerando prejuízos no seu desenvolvimento intelectual (MIZUSAKI, 2021).

Existe uma disparidade entre a educação privada e a pública, enquanto diversos jovens passaram por um período desassistidos de educação, as escolas privadas continuaram oferecendo ensino através de plataformas virtuais. A pandemia foi um período para as instituições de ensino repensarem sobre a sua metodologia e o seu conceito de educação. Refletindo sobre os impactos e os anseios dos jovens sobre a internet é possível traçar uma rota de melhorias e qualidade no cenário atual (CARDOSO; FUHR; DIAS, 2020).

Frisa-se que o princípio de inserir a segurança digital como matéria básica na educação não se limita aos jovens, pois a tecnologia está presente na vida das pessoas de todas as idades. A consciência sobre qual é a importância de proteger dados pessoais e quais os riscos eminentes de utilizar uma plataforma virtual deve, assim, estar presente no cotidiano de todos os indivíduos.

Os idosos, por exemplo, têm utilizado cada vez mais as plataformas virtuais, embora grande parte deles possua certa dificuldade em lidar com essas novas ferramentas e entender a sua extensão e complexidade. Caracterizados como imigrantes digitais, nasceram em um mundo que foi moldando-se e evoluindo com a necessidade da população; a tecnologia desabrochando e ganhando força na sociedade e ao longo dos anos os idosos se adaptam a ela, cada um em sua linha do tempo (ANDRADE, 2019).

Diferente dos imigrantes digitais, os nativos digitais são pessoas que já nasceram em meio a tecnologia e possuem facilidade em utilizá-la. Por mais que os idosos tenham adquirido experiência com os avanços tecnológicos, o fato é que o mundo se atualiza todos os dias, de modo que uma grande diferença entre um nativo digital de um imigrante digital, é que os nativos já nasceram em um mundo acelerado e o seu aprendizado acompanha essa celeridade. Os imigrantes digitais por muitas vezes conflitam com essa agilidade, preferindo processos mais vagarosos e elucidativos (ANDRADE, 2019).

Por tais razões, necessário direcionar a educação digital de forma alternativa, com metodologias adequadas à diversidade e à necessidade de cada faixa etária, na medida em que, conforme o art. 7º do MCI “o acesso à Internet é essencial ao exercício da cidadania”, mas não saber como utilizá-la torna vazio o texto da lei, gerando somente uma expectativa de direito aos idosos.

A necessidade da educação digital ao grupo da terceira idade foi visível na pandemia do COVID-19. Os idosos foram considerados como um grupo de risco, sendo intensificado o distanciamento social após os 60 anos de idade. Os serviços que antes eram físicos, migraram para plataformas digitais, como consultas médicas, entrega de produtos ou até mesmo os saques emergenciais do fundo de garantia. Sem o conhecimento destas ferramentas a terceira idade encontra-se vulnerável a sociedade como um todo (JOAQUIM; OLIVEIRA; PESCE, 2021).

O letramento digital do idoso também pode ser visto sob uma perspectiva de inclusão social atualmente, visando a transformação de diversos processos que ocorreram em período pandêmico. A utilização das TIC e a compreensão dos riscos inerentes a ela, são necessários para o idoso usufruir do novo mundo que está sendo construído.

Ainda que exista legislação que tutele os dados pessoais, a implementação de uma efetiva educação digital é imprescindível para que a legislação não seja meramente simbólica. É necessário que o Brasil adentre no conceito de constitucionalismo transformador, promovendo a mudança social através da aplicação da lei. A interpretação da legislação deve emergir com estruturação de projetos e políticas públicas que sanem a raiz do problema, concretizando objetivos constitucionais. O constitucionalismo transformador transcende o texto da lei e cria diretrizes para sanar os problemas sociais. No caso de vazamento de dados, os esforços seriam guiados pela conscientização e educação digital, visando a fragilidade do usuário na rede. A sua essência está direcionada a alcançar os objetivos traçados em lei, criando a resolução das problemáticas envolvidas (BOGDANDY; URUEÑA, 2021).

A educação digital configura, assim, política pública de efetivação do direito fundamental à tutela de dados pessoais. O Estado atua, aqui, não como órgão que impõe limites a si mesmo e aos demais (dimensão negativa), mas também como aquele que impulsiona o direito (dimensão positiva), de forma que, a positivação da proteção de dados precisa da educação digital para ser efetiva. Ambas podem ser tidas como um amálgama, uma a depender da outra.

6 CONSIDERAÇÕES FINAIS

O avanço tecnológico modificou o paradigma das relações sociais, na medida em que possibilitou a interação humana através de ambientes virtuais. Isso potencializou a dinâmica da comunicação, mas também fez surgir uma série de ofensas a direitos.

A promessa de que a internet se constituiria em um ambiente neutro e livre, não se confirmou. Rapidamente relações de poder entre atores públicos e privados se estabeleceram no ciberespaço.

A dinâmica do poder na rede está intrinsecamente relacionada com os dados pessoais compartilhados pelos usuários, tendo em vista o modelo de negócios que se desenvolve no ciberespaço que se utiliza dos dados pessoais. Ele compreende entretenimento, prestação de serviços, comércio, educação e até mesmo nos serviços públicos e de cidadania. Nesse novo modelo de interação, os usuários podem, muitas vezes, terem os seus dados pessoais utilizados de forma indevida.

No Brasil, a necessidade de regulamentação do ciberespaço levou à promulgação do Marco Civil da Internet (MCI), que estabeleceu princípios, direitos e deveres para o uso da Internet no país. Posteriormente, em 14 de agosto de 2018, foi publicada a Lei n. 13.709, a Lei Geral de Proteção de Dados (LGPD) que regula especificamente sobre o tema a proteção de dados pessoais.

Os riscos advindos do compartilhamento de dados no ambiente virtual desencadearam uma reação constituinte, que culminou com a promulgação, em 11 de fevereiro de 2022, da Emenda Constitucional n. 115 que acrescentou o direito à proteção dos dados pessoais, inclusive nos meios digitais ao rol dos direitos e garantias fundamentais do art. 5º.

Esse movimento é produto da preocupação cada vez maior com as vulnerabilidades dos usuários de internet, tendo em vista que o Brasil é o país mais propenso a sofrer ataques cibernéticos.

A maior parte desses ataques são produto da engenharia social, uma técnica de manipulação de pessoas que se serve do desconhecimento ou mesmo da confiabilidade do alvo para persuadi-lo à prática de ações. O fator humano é, assim, a principal causa das vulnerabilidades a ataques cibernéticos.

Por essa razão, ainda que o Brasil detenha um arcabouço normativo consistente para a proteção de dados pessoais, é ingênua a ideia de que a lei seja suficiente para a segurança dos dados.

Nesse sentindo, além de impor comportamentos negativos e regulamentar o tratamento de dados pessoais, a implementação de uma política pública de educação digital parece ser o caminho para, de fato, minimizar as vulnerabilidades do usuário de internet.

REFERÊNCIAS

ABROSHAN, Hossein, et al. Phishing happens beyond technology: the effects of human behaviors and demographics on each step of a phishing process. **IEEE Access**, v.9, p. 44928-44949, Mar 17, 2021. Disponível em: http://ieeexplore.ieee.org/document/9380285. Acesso em: 15 abr. 2022.

ANDRADE, Cristian Ricardo. **Letramento digital na terceira idade:** Estudo de caso do projeto de inclusão digital para terceira idade da Fatec Garça. 2019. Tese (Mestrado em Mídia e Tecnologia) - Universidade Estadual Paulista, Bauru, 2019.

BACHUR, João Paulo. Proteção de Dados Pessoais na Educação. In: BIONI, Bruno et al (Coords.). **Tratando de proteção de dados pessoais**. Rio de Janeiro: Forence, 2020.

BARBOSA, Juliana Souza, et al. A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional. **Research, Society and Development**, v.10, n.2, 2021. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/12557. Acesso em: 15 abr. 2022.

BOGDANDY, Armin Von; URUEÑA, René. Constitucionalismo transformador internacional na América Latina. **Revista Brasileira de Políticas Públicas**, Brasília, v.11, n.2, p. 27-73, ago. 2021. Disponível em: https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/7762/pdf. Acesso em: 04 mai. 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25 jan. 2022.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 16 jan. 2022.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 31 jan. 2022.

BRASIL. **Medida Provisória n. 954,** de 17 de abril de 2020. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 31 jan. 2022.

BRASIL, Ministério da Educação. Base nacional comum curricular. Brasília: **MEC**, 2018. Disponível em: http://basenacionalcomum.mec.gov.br/abase/#medio. Acesso em: 23 abr. 2022.

BRASIL. Senado Federal. **Proposta de Emenda** à Constituição nº 17, de 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em: 02 abr. 2022.

CARDOSO, Maykon Dhonnes de Oliveira; FUHR, Heliana Pereira Portilho; DIAS, Kátia Gonçalves. Covid 19 e educação: reflexões e possíveis caminhos. **Revista Observatório**, v.6, n.2, abr./jun. 2020.

CASTAMAN, Ana Sara; RODRIGUES, Ricardo Antônio. Educação a distância na crise Covid-19: um relato de experiência. **Research, Society and Development**. v.9, n.6, jun./jun. 2020. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/3699 .Acesso em: 27 abr. 2022.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: BIONI, Bruno et al (Coords.). **Tratando de proteção de dados pessoais**. Rio de Janeiro: Forence, 2020.

ESTUDO IBM: Gastos com violações de dados caem no Brasil, mas o país é o mais provável a ter ataques de hackers entre os pesquisados. **IBM**, São Paulo, 12 de jul. de 2018. Disponível em: https://www.ibm.com/blogs/ibm-comunica/estudo-ibm-gastos-com-violacoes-de-dados-caem-no-brasil/. Acesso em: 21 de abr. 2022.

GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards digital constitutionalism? mapping attempts to craft an internet bill of rights. **Research Publication** No. 2015-15 November 9, 2015, v. 7641, 2015. Disponível em: https://dash.harvard.edu/bitstream/handle/1/28552582/SSRN-id2687120.pdf?sequence=1 . Acesso em: 03 abr. 2022.

HADNAGY, Christopher. **Social Engineering**: the art of human hacking. Indianapolis: Wiley Publishing, 2011.

HIBRIDO. In: DICIO, Dicionário Michaelis. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/hibrido/. Acesso em: 18 mai. 2022.

JESUS, Damásio. **Marco Civil da Internet:** comentários à Lei n. 12.965/14**.** São Paulo: Saraiva, 2014.

JOAQUIM, Bruno dos Santos; OLIVEIRA, Werley Carlos; PESCE, Lucila. Inclusão e letramento digital do idoso na perspectiva da educação ao longo da vida. **Revista Conhecimento Online**, Novo Hamburgo, v.1, jan./abr. 2021. Disponível em: https://periodicos.feevale.br/seer/index.php/revistaconhecimentoonline/article/view/2363. Acesso em: 04 mai. 2022.

LANNES, Yuri Nathan da Costa. **Nova privacidade no Brasil e os impactos jurídicos e econômicos:** uma análise do big data e da responsabilidade empresarial. 2020. Tese (Pós-graduação em Direito Público e Econômico) - Universidade Presbiteriana Mackenzie, São Paulo, 2020.

LEITE, George Salomão; LEMOS, Ronaldo. **Marco Civil da Internet**. São Paulo: Atlas S.A, 2014.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011.

LÈVI, Pierre. **Cibercultura**. São Paulo: Ed. 34, 1999.

LIGUORI, Carlos. **Direito e Criptografia**. São Paulo: SaraivaJur, 2022.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito**. v.12, n.2, p.1-33, jun./jul. 2020. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10597. Acesso em: 05 fev. 2022.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. **Revista Brasileira de Direito**, Passo Fundo, v.16, n.1, p.1-33, jan./abr. 2020. Disponível em: https://seer.imed.edu.br/index.php/revistadedireito/article/view/4103. Acesso em: 26 mar. 2022.

MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otavio Luiz; FONSECA Gabriel Campos Soares. O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo. In: BIONI, Bruno et al (Coords.). **Tratando de proteção de dados pessoais**. Rio de Janeiro: Forence, 2020.

MITNICK, Kevin; SIMON, William, MITNICK**. A arte de enganar**. São Paulo: Pearson Education, 2003.

MIZUSAKI, Lucas Eishi Pimentel. **O ensino hacker: o digital divide e o professor como inventor**. 2021. Tese (Pós-Graduação em Informática na Educação) - Universidade Federal do Rio Grande do Sul, Porto Alegre, 2021.

NICOLETE, Priscila C., et al. Informática na educação básica pública brasileira: análise sobre sua importância, tendências e desafios. **EDT - Educação Temática Digital**, Campinas, v.23, n.3, p.794-815, jul./set. 2021.

OLIVEIRA, Fabiane Araújo; LANZILLO, Anderson Souza da Silva. Estado, novas tecnologias e proteção de dados pessoais como direito fundamental. **Revista de Direito, Governança e Novas Tecnologias**, v.7, n.1, p.92-107, jan./jul. 2021.Disponível em: https://www.indexlaw.org/index.php/revistadgnt/ article/view/7901. Acesso em: 25 fev. 2022.

ONU - Organização das Nações Unidas. As internet user numbers swell due to pandemic, UN forum discusses measures to improve safety of cyberspace. **United Nations**, 2021. Disponível em: https://www.un.org/en/desa/internet-user-numbers-swell-due-pandemic-un-forum-discusses-measures-improve-safety-cyberspace. Acesso em: 02 abr. 2022.

PAVANI, Giorgia; HERMES, Manuellita. A emergência da Covid-19 nas experiências federais: o caso do Brasil. **Novos Estudos Jurídicos**. v.26, n.3, set./dez, 2021. Disponível em https://vlex.com.br/vid/emergencia-da-covid-19-897111775. Acesso em: 21 de mar. 2022.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais:** Comentários à Lei 13.709/2018 (LGPD). 3. ed. São Paulo: Saraiva, 2020.

SCHWABE, Jürgen. **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal alemão**. Tradução: Beatriz Henning et al. Montevideo: Fundación Konrad-Adenauer, 2005.

SILVA, Narjara Xavier; ARAÚJO, Wagner; AZEVEDO, Patrícia. Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. **Revista Ibero-americana de Ciência da Informação**, Brasília, v.6, n.2, p. 37-55, ago./dez. 2013. Disponível em: https://periodicos.unb.br/index.php/RICI/article/view/1782. Acesso em: 04 abr. 2022.

VARTOUN, Ali Moradil; TESHNEHLAB, Mohammad; KASHI, Saeed Sedighian. Leveraging deep neural networks for anomaly-based web application firewall. **IET Information Security.** v.12, Is.4, p. 352-361, jul./nov. 2019. Disponível em: https://ietresearch.onlinelibrary.wiley.com/doi/epdf/10.1049/iet-ifs.2018.5404. Acesso em: 06 maio 2022.

VIOLA, Mario; TEFFÉ, Chiara Spadaccini. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11º. In: BIONI, Bruno et al (Coords.). **Tratando de proteção de dados pessoais**. Rio de Janeiro: Forence, 2020.