O DIREITO FUNDAMENTAL DE PROTEÇÃO AOS DADOS PESSOAIS E A POSSÍVEL AUSÊNCIA LEGISLATIVA NO TRATAMENTO DE CRIMES À LUZ DO ORDENAMENTO JURÍDICO BRASILEIRO NO SÉCULO XXI

Pedro Henrique Caetano Scharra
Graduando em Direito FDCI
pedrohenriquescharra@hotmail.com

Lorena Borsoi Agrizzi
Mestre em Cognição e Linguagem- UENF, Professora Pesquisadora- FDCI
lorena@fdci.edu.br

RESUMO

O presente artigo versa sobre a proteção de dados pessoais diante dos complexos desafios, destinando-se seu enfoque a proteção de dados e ao direito à privacidade, presentes na atual constituição. Sabe-se que umas das características dos direitos fundamentais são o seu semblante não absoluto, proporcionando, de tal maneira, divergências entre tais direitos. Nesse contexto, a análise do artigo 5º incisos IV, X, XXXIII da Constituição Federal, está diante de um conflito constitucional, tendo em vista a liberdade de pensamento e a violação da privacidade, trazendo consigo a vida privada. Necessário considerar que tais direitos são um exemplo clássico da colisão dos direitos fundamentais, ressalta-se dessa forma a importância da liberdade de pensamento em conjunto com o direito à informação. A globalização é peça fundamental deste esquema, visto que, a difusão da informação atualmente é dada de forma imediata, relevando acontecimento a uma velocidade quase instantânea. Em contrapartida, o direito à privacidade se faz, mas que necessário, tendo em vista como base fundamental a Constituição Federal em seu inciso X, e juntamente com o novo código civil, Lei 10.406/02 em seus artigos 11 ao 21 bem como a Lei 13.709, que trata da Proteção de Dados. Analisando-se a pertinência destes conflitos, faz mister a utilização de um meio eficaz e alternativos para correção. Assim sendo, a problemática sobre a qual se desdobrará a análise é a respeito dos desafios destinados a proteção de dados e ao direito a privacidade tendo em vista também um olhar sobre o viés da tutela penal a respeito do presente tema, possuindo como base doutrinas modernas, revistas jurídicas e sites remetentes ao conteúdo. Bem como planeja analisar pontos da Constituição Federal, do Código Civil e Código Penal, em conjunto com leis referentes às infrações e suas atualizações.

PALAVRAS CHAVE- Hacker. Cracker. Dados pessoais. Crimes virtuais. LGPD. Liberdade de pensamento. Privacidade.

1. INTRODUÇÃO

A Constituição da República Federativa do Brasil de 1988, traz em seu rol dentro do título dos direitos e garantias fundamentais a presença do dever de proteção das pessoas, bem como de seus bens patrimoniais e a preservação da ordem econômica. Importante mencionar que além do amparo constitucional, há no âmbito penal, a presença de crimes as quais se fazem presente desde o século XVIII na sociedade, com a denominada *"Escola Clássica*" da criminologia, como na obra de *Cesare Beccaria.*

Entretanto, "O mundo global vive em uma era da informação, tendo iniciado na década de 1990, a qual introduz a internet como parte do dia a dia da sociedade." (HIAVENATO 2014) Dessa forma, devido ao aumento significativo dos usuários presentes nas redes, os crimes comuns cometidos pela sociedade passaram a possuir outro campo de incidência, o ambiente virtual. Nesse ambiente, os usuários possuem propriedades, entretanto, imateriais, o que diferencia dos demais crimes cometidos em sociedade, que se caracterizam pela materialidade. A obscuridade que esse ambiente possui é um grande desafio para o Direito, pois é essa ligação entre o mundo material e o imaterial, que faz um indivíduo cometer um crime, de furto, por exemplo, contra várias pessoas sem que ninguém saiba quando, onde e como ocorreu. Dessa forma, tais crimes possuem como objeto, por vezes, atentar contra a privacidade de usuários da rede mundial de computadores.

Ademais, além do aumento expressivo de usuários, outro fator que influência o grande acervo de crimes praticados virtualmente é a sensação de impunidade. Uma vez que a carência de legislação adequada para normatizar tais crimes se mostra irremediáveis e insuficientes. Enquanto o Brasil permanece retrógrado, outros países têm tentado reconstruir suas leis para eliminar os crimes cibernéticos, com ênfase para os Estados Unidos, bem como a Europa, pela elaboração da Convenção sobre o *Cibercrime*, também conhecida como *Convenção de Budapeste* – A Convenção de Budapeste é um tratado internacional de direito penal e direito processual penal, firmado no âmbito do Conselho da Europa para definir de forma harmônica os crimes praticados por meio da Internet e as formas de persecução.

Entretanto, nos últimos meses, muito se tem falado em tais crimes, uma vez que o prejudicado vem sendo pessoas jurídicas de grande porte nacional e internacional, bem como órgãos e entidades governamentais. Há de observar que o objetivo nem sempre é visando o lucro que tais crimes podem fornecer, existem também outras inúmeras consequências, sejam elas políticas ou econômicas dos países envolvidos. Podendo de certa forma resultar até mesmo em guerras ou atos terroristas, causando prejuízos incalculáveis para o governo e toda a população.

Além dos prejuízos econômicos, nota-se também a presença de violações constitucionais contra princípios básicos dos Direitos Humanos. Observa-se com veemência a transgressão ao Direito a privacidade bem como a liberdade de pensamento. Constata-se ainda que devido a acentuada constância dos crimes virtuais, dados estão sendo furtados e divulgados, corroborando assim para uma maior gravidade das ações de determinados indivíduos.

Diante da relevância do tema, importante frisar o quão grande deve ser incentivado o aprendizado a respeito da segurança na rede, assim como as ferramentas de proteção a serem usadas, de modo a dar mais comodidade aos usuários, a fim de que possam se sentir livre e seguro quanto a preservação de seus dados e direito individuais ao utilizar as várias ferramentas e facilidades que a internet proporciona.

Dessa forma, o trabalho objetiva a análise do ramo do direito, conhecido como direito digital, e suas repercussões nas esferas criminais, bem como uma análise a respeito da proteção de dados, e seu amparo constitucional. De maneira a demonstrar as diferenças

existentes entre as atividades criminosas virtuais, e os demais tipos de invasores, bem como objetiva analisar o tratamento jurídico brasileiro, e sua eficácia ao combate dos crimes virtuais.

Ainda será problematizada a aplicação da LGPD em sua interface referente ao período pandêmico e dos ataques cibernéticos emergentes deste recorte, uma vez que durante o longo período o qual o mundo atravessava o vírus da COVID-19, milhares de dados de pessoas físicas e jurídicas foram vasados, infringindo princípios e normas básicas inerentes aos seres humanos. Dessa forma, o persente artigo visará de forma clara e sucinta contribuir através de doutrinas e jurisprudências modernas, revistas jurídicas e sites remetentes ao conteúdo. Bem como analisará pontos da Constituição, do Código Civil e Código Penal, em conjunto com leis referentes às infrações violadas.

2. DO DIREITO FUNDAMENTAL AOS DADOS PESSOAIS

2.1.A segurança e o valor dos dados pessoais e seu amparo constitucional

Constata-se hoje que, "Os dados do século XXI são como o petróleo do século XVIII: um ativo imensamente inexplorado e valioso" (TOONDERS, 2018) os quais possuem um tratamento diferenciado, bem como as mercadorias. Tal nomenclatura deriva do seu alto valor e sua influência na economia digital. Anos atrás, o petróleo se destacava com seu alto valor de comércio, no entanto, atualmente o ouro negro foi substituído pelos dados pessoais. *Google*, *Facebook*, *Amazon*, entre tantas outras Big Techs que tomaram conta do mercado, se destacam com seu alto valor de mercado.

Tais empresas como Google e o próprio *Facebook*, não cobram nada para seu acesso à suas plataformas, no entanto, vendem seus dados a empresas privadas. Atualmente todo site têm *cookies*,até mesmo as redes sociais.

> "Os serviços fornecidos de modo aparentemente gratuito, na verdade são pagos com a troca por um bem altamente valorizado: dados sobre o consumidor. Por exemplo, empresas como Facebook, Google e Youtube recolhem informações sobre o usuário e rastreiam sua navegação para personalizar anúncios e conteúdo de suas plataformas. Esses dados pessoais permitem a elaboração de perfis dos usuários a partir de algoritmos, que podem aprender padrões de comportamento e influenciar as escolhas dos usuários." (CUNHA, Carolina.2018)

Aquela propagada relacionada à sua pesquisa na semana passada, tudo tem a ver com a venda de dados e o controle de suas atividades. Por exemplo, informações sobre um carro que você deseja comprar ao final do ano, a viagem em família nas férias, ofertas irão aparecer, é claro que de modo filtrado conforme seu campo de pesquisa selecionado. Tudo isso engloba a venda de dados, os seus dados. Importante ressaltar o que seria "*cookies",* de forma concreta e direta esses poderiam ser conceituados, sendo "pequenos arquivos criados por sites visitados e que são salvos no computador do usuário, por meio do navegador." (ALVES,2018). Os quais contêm informações que servem para identificar o visitante, seja para personalizar a página de acordo com o perfil ou para facilitar o transporte de dados entre as páginas de um mesmo site.

2.2. Fundamentos jurídicos

O crescente número de pessoas conectadas à internet, e o seu altíssimo valor que cada pessoa possui, requereu que houvesse a inclusão da proteção de dados no rol dos direitos fundamentais. Há de observar que no ano de 2019 foi aprovado pelo Senado uma

Emenda Constitucional, que inclui a proteção de dados pessoais disponíveis em meio digital, a Proposta de Emenda à Constituição (PEC)17/2019. A emenda deixa clara a competência da união para legislar sobre a proteção de dados pessoais. No entanto, tal PEC, só entrou em vigor em meados de 2020.

Entretanto, a constituição no rol dos direitos fundamentais expressos, engloba a inviolabilidade do sigilo de dados (art.5º, XII) em complemento a inviolabilidade da intimidade e da vida privada (art.5º, X). Importante ressaltar a presença da proteção de dados ainda no artigo 5º, no inciso LXXII, onde é assegurado ao particular o conhecimento de informações relacionadas à sua pessoa bem como a possibilidade de retificação de tais informações.

Conforme o entendimento Alexandre de Moraes a respeito de tais disposições constitucionais, temos que;

> A defesa da privacidade deve proteger o homem contra: (a) a interferência em sua vida privada, familiar e doméstica; (b) a ingerência em sua integridade física ou mental, ou em sua liberdade intelectual e moral; (c) os ataques à sua honra e reputação; (d) sua colocação em perspectiva falsa; (e) a comunicação de fatos relevantes e embaraçosos relativos à sua intimidade; (f) o uso de seu nome, identidade e retrato; (g) a espionagem e a espreita; (h) a intervenção na correspondência; (i) a má utilização de informações escritas e orais; (j) a transmissão de informes dados ou recebidos em razão de segredo profissional. (MORAES, 2016, p. 74).

Por outro lado, necessário frisar, que o Brasil em 2018, na vigência do mandado do Ex-presidente Michel Temer, promulgou a Lei Geral de Proteção de Dados, LGPD, que entrou em vigor no ano de 2020, sancionada dessa vez pelo presidente, Jair Messias Bolsonaro. Tal lei busca efetivar e regular de forma mais ampla a coleta e o tratamento de dados bem como a proteção do usuário, devido ao grau de importância e seu crescimento na atualidade. A respectiva lei será aprofundada mais à frente.

3. OS PRINCIPAIS CRIMES VIRTUAIS PRATICADOS POR HACKERS E CRACKERS

3.1. Diferença das atividades hacker e cracker

Frequentemente, tem-se ouvido falar em atividades de hacker. “Um grupo de hacker invadiu o sistema do banco X”, “Hackers invadiram dispositivos eletrônicos e conseguiram acesso a contas bancárias”. No entanto, o modo usado para representar tais atividades criminosas, e os indivíduos a que praticaram nos remete, a saber, de forma coerente qual vocábulo ideal a se usar.

Em primeiro lugar, convém destacar que “Hackers é uma pessoa que possui um grande conhecimento informático e que se encontra em constante estudo sobre a área, capaz de invadir o sistema de outrem para entretenimento e aprendizagem.” (ARIMURA, 2016) Da mesma forma, o conceito de Cracker, conforme Leandro, pode ser disposto como “O termo usado para designar quem pratica a quebra de um sistema de segurança.” (FERMINO, 2020,). Na prática, ambos servem para explicar as pessoas que têm habilidades com computadores, porém, cada um dos "grupos" usa essas habilidades de formas bem diferentes.

Com o surgimento, nos Estados Unidos, “hack”, como é a nomenclatura em inglês, de acordo com Mark começou a ser utilizada em meados da década de 50 e 60, serviam com solução inspirada ou elegante para qualquer problema. (WARD, 2011)

Pode se conceituar esse grupo de “anônimos” como, pessoas com um conhecimento profundo de informática e computação que trabalham desenvolvendo e

modificando softwares e hardwares de computadores, não necessariamente para cometer algum crime. (GONÇALVES, 2021)

Importante salientar a visão negativa que um hacker possui hoje em nossa sociedade, haja vista o desconhecimento das nomenclaturas corretas. Hoje se pode relatar que o objetivo em comum dos hackers é ajudar, sem ter "fama" de suas ações. A ideia principal é beneficiar a sociedade de alguma forma, por meio da tecnologia. Muito se tem falado na qualidade de produtos da Apple, entretanto, atrás da marca há hackers envolvidos em achar erros, falhas, a fim de melhorar a produtividade tecnológica.

Os hackers, também são conhecidos como, *white hats,* traduzido do inglês, chapéu branco, fazendo uma analogia a filmes de faroestes americanos, a qual denominava os mocinhos os quais utilizavam o chapéu branco. Os hackers "bons" assim denominados trabalham atualmente em empresas, normalmente nos setores de TI, como especialistas de sistemas, bem como em outros ramos da informática.

A nomenclatura Crackers, a qual pouco se houve falar, foi criada em 1985 por hackers em defesa ao uso jornalístico infamante do termo *"hacker*". O termo vem de do verbo em inglês "to crack", quebrar, rachar.

Desse modo, crackers, esse sim pode ser considerado "criminoso", uma vez que é ele quem infringiu leis, atribuindo e cometendo verdadeiras atividades ilícitas. Obtendo acesso por meio de quebras nas falhas dos sistemas, seja público ou privado.

O conceito mais aceito hoje é que Crackers "são definidos como criminosos, eis que operam em fraudes bancárias e eletrônicas, furto de dados, golpes, entre outros." (ARIMURA, 2016)

Importante ressaltar que atitude de um cracker é sempre prejudicial, maldosa, visando à quebra de um sistema em beneficio "próprio" ou de um terceiro.

Crackers também são conhecidos como *black hats*, os quais podem ser conhecidos por serem diferentemente dos white hats.

> "Os black hats se utilizam das vulnerabilidades que encontram para obter dados sigilosos, como dados pessoais, senhas, dados bancários, etc. São definidos, por alguns autores, como subcategoria dos crackers". (ARIMURA, Mayumi.2016)

Em muitos aspectos podemos diferenciar as atividades de um hacker e um cracker. Como já mencionado, esse se refere a atividades maldosas perante a sociedade ou ao um grupo seleto, ao contrário daqueles que possuem um posicionamento, em prol/benefício da tecnologia de modo amplo.

Ressalta-se ainda que tais indivíduos possuem aspectos em comum, que podem ser amplamente visualizados no ambiente cibernético.

> "No ambiente cibernético, especialmente na Internet, diversos termos podem ser encontrados para classificar os piratas cibernéticos. Tais piratas, que em sua maioria têm em comum algumas características, como: são homens jovens, autodidatas, gostam de ultrapassar os limites, são apaixonados por informática, têm conhecimentos em segurança, em auditoria e em ferramentas para quebra de sistema, dentre outras características específicas de cada categoria. No entanto, embora haja semelhança em algumas características, em outras, como por exemplo, o nível de conhecimento e o objetivo que os impulsiona à pirataria, diferem nas diversas terminologias." (BACH,2001,p.3)

Um ponto importante que difere tais atividades tidas como criminosas ou não, é a falta de ética presente no trabalho. Ambos visam achar falhas e erros nos sistemas operacionais, no entanto, quando um hacker acha tal erro ele trabalha a fim de melhorar, visando que tal erro não exista, melhorando de tal forma o funcionamento. Contudo, isso os difere dos crackers, que ao achar o erro, a falha no sistema, em vez de buscar a melhoria, invadem, com intuito de se beneficiar perante aquele erro.

A diferença básica é esta: “os hackers constroem coisas, crackers as destroem.” (RAYMOND, 2000).

Importantíssimo comentar que tais falhas ocasionadas por ambos indivíduos podem conduzir a invasões, as quais, poderão levar ao acesso não somente de contas bancarias, caracterizando um fato típico, mas também poderá levar ao acesso de fotos pessoais, infligindo à privacidade individual.

3.2. Demais tipos de invasores

Analisando-se esse ponto, temos que ter em mente que com o crescimento e o avanço da tecnologia, a todo o momento surgem indivíduos com intuitos secundários em seus dados. Com isso, é importante salientar os tipos de invasores mais conhecidos, bem como o que é cada um deles.

Consoante ao exposto anteriormente sobre a divisão de hackers e crackers, os quais se diferenciam por suas intenções, principalmente. Enquanto aquele visa achar uma falha no sistema e concertar, a fim de beneficiar a todos, esse tem o intuito de achar da mesma forma a falha no sistema, porém com intuito de se beneficiar.

Dessa forma, conforme o site backup garantido, há alguns tipos de invasores;

> - Ataque DDOS, esse tipo de ataque consiste no sobre carregamento de um servidor, onde um único computador mestre controla milhares de computadores, a fim de sobrecarregar e deixar o site indisponível para o uso.
> - *Ransomware*, esse ataque é conhecido como sequestrador virtual, e tem como objetivo bloquear o acesso a todos os arquivos do servidor, sendo liberado somente por meio de pagamento, como valor de resgate.
> - Cavalo de troia, esse tipo de ameaça é uma das mais conhecidas mundialmente, normalmente, o usuário deve “autorizar”. Caso mais comuns são de anexos, downloads e links pelo próprio e-mail pessoal os usuários. O objetivo aqui é roubar informações pessoais e interromper algumas funções do computador.
> - *Phishing*, é considerado um crime virtual. Aqui os invasores laçam uma isca ao indivíduo. Links, que levam o usuário a inserir dados. O caso mais comum é por meio do email, a qual os usuários revelam informações pessoais, incluindo senhas e até mesmo dados bancários.
> - *Cryptojaking*, esse tipo de invasão é mais recente, onde o invasor tem como objetivo usar o computador ou dispositivo de outra pessoa para fazer remotamente a “coleta” de criptomoedas, as moedas virtuais.
>
> (BACKUP GARANTIDO, 2018.)

Como se vê, são múltiplas as formas de ataques que colocam em riscos os dados e os direitos consagrados na Constituição Federal, desta forma, é congruente ressaltar a importância do Direito como ferramenta para colaborar no oferecimento de possíveis respostas no que tangem a segurança dos direitos inerentes ao ser humano.

3.3. Principais redes comumente invadidas

Importante mencionar que todas as redes e meios de comunicação estão sujeitas a invasão devido ao grandioso crescimento virtual nos últimos anos.

É claro que empresas de certas magnitudes são mais visadas, como é o caso da *Google*, *Apple*, *Microsoft*, *Ebay*, *DropBox*, *Instagram*, *Twitter* e milhares de outras que já até sofreram com tais problemas.

Recentemente o Twitter teve casos de hackers a redes privadas do alto escalão mundial.

> "Entre as contas hackeadas estavam a de líderes políticos, como o candidato presidencial democrata Joe Biden, o ex-presidente Barack Obama, mas também de grandes empresários, como Jeff Bezos, fundador da Amazon, Elon Musk, chefe da Tesla, ou ainda Bill Gates, fundador da Microsoft." (PRESSE, France,2020)

Além de casos recentes, como os citados anteriormente, o ano de 2014 também ficou marcado por várias invasões. Desde a empresa *Sony Pictures*, a fotos íntimas de celebridades. Nessa época, um aplicativo era muito utilizado mundialmente, o *snapchat*. A partir dessa plataforma de entretenimento, milhares de indivíduos, comuns e mundialmente conhecidos tiveram suas contas invadidas e seus dados pessoais e suas privacidades violadas e divulgadas.

Casos mais comuns do que os mencionados, são aqueles que acontecem diariamente por toda parte do planeta. Casos de cartões de créditos e débitos clonados. Segundo uma pesquisa feita pela G1, aproximadamente 40 milhões tiveram seus dados roubados após uma invasão na rede de varejo norte americana. "Só no caso da Target, as estimativas mais conservadoras apontam a violação de 40 milhões de dados de cartões de crédito, podendo chegar a 100 milhões." (ALTIERES, 2014)

4. TRATAMENTO JURÍDICO NO BRASIL

4.1. Lei Carolina Dieckmann- 12.737/2012

Com o grande avanço dos crimes virtuais, os debates a respeito do tema começaram a surgir com mais frequência. Em meados de 2011, foi analisado no congresso um projeto de lei (PL 2793/2011).

A lei Carolina Dieckmann, foi assim apelidada, pois um ano após a PL 2793, a atriz foi alvo de crackers, que invadiram seu computador por meio de hackers *phishing,* como já visto anteriormente. O cracker conseguiu acesso a dados e fotos pessoais da famosa, o caso na época ficou bem conhecido por todos.

> Sancionada em dezembro de 2012, a alteração do Código Penal foi apelidada com o nome da atriz, após fotos em que Carolina Dieckmann aparecia nua terem sido divulgadas na internet. Ao todo, 36 imagens da atriz foram publicadas na web em maio de 2012. Ela recebeu ameaças de extorsão para que pagasse R$ 10 mil para não ter as fotos publicadas. (G1,2013).

Após o surgimento da lei 12.737/2012, oriunda da PL 2793, houve também a promulgação de uma nova lei, que ordenava que os órgãos da polícia judiciariam criassem equipes especializadas no combate de crimes cibernético devido sua grande amplitude nos últimos anos.

A denominada lei Carolina Dieckmann, alterou alguns pontos do Código Penal, introduzindo o artigo 154-A e 154- B.

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1ºNa mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º-Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra.
> I - Presidente da República, governadores e prefeitos
> II - Presidente do Supremo Tribunal Federal
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (BRASIL,2012)

Assim, como se torna perceptível, esta norma oferece a gênese da proteção no que tange a invasão dos dispositivos no Brasil. Desta forma, com a inovação oferecida pelo Código Penal, há por parte do usuário uma maior segurança no que se refere a toda dinâmica das redes de computadores.

Importante mencionar a serventia do legislador ao fazer uma comparação do crime tipificado no artigo 154-A e no crime tipificado no artigo 155 do código penal, vemos que há disparidade das penas cominadas.

> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
> Pena - reclusão, de um a quatro anos, e multa.
> § 1º - A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno.
> § 2º - Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa.
> § 3º - Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico. (BRASIL,2012)

Temos em mente que a subtração aqui irá ocorrer em ambos os casos, causando prejuízos de qualquer forma. O critério utilizado no artigo 154-A, inserida pela lei 12. 737/2012 não é muito consistente. Haja vista na maioria das vezes o crime aqui tipificado resultar danos muitos maiores do que o praticado no rol do artigo 155.

4.2 Lei Geral de Proteção de Dados Pessoais - LGPD

No ano de 2019, foi dada uma nova redação a lei de proteção de dados. A qual anteriormente era conhecida como "Marco Civil da Internet". A atual e denominada lei geral de proteção de dados - LGPD. Lei nº. 13.709 dispõem sobre a coleta e o tratamento de dados pessoais.

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL,2019)

Importantíssimo aludir que sua vigência foi em meados de 2020, sendo por sua vez "adiada" apenas sua sanção, devido a omissão na estruturação da ANPD (Autoridade Nacional de Proteção de Dados) é, portanto, o principal problema de implementação da LGPD, não só do ponto de vista interno, de regulamentação e *enforcement*, como do

ponto de vista externo, de reconhecimento do Brasil conforme padrões internacionais de proteção de dados pessoais.

Em síntese, a LGPD mudará o mecanismo de funcionamento e as regras para operações de coleta, armazenamento, compartilhamento de dados pessoais. Dados pessoais são entendidos como quaisquer informações provenientes de pessoas naturais.

Para melhor ilustrar a finalidade da lei 13.709 analisaremos a imagem:

IMAGEM 1- LGPD ESQUEMATIZADA

Fonte: (SERPRO,2020)

Observa-se também, que a lei 13.709, corrobora com o ensinamento ao trazer alguns pontos fundamentais para sua interpretação. Constata-se a presença de fundamentos, os quais relatam que essa lei é expressamente regulada por;

I – o respeito à privacidade;
II - a autodeterminação informativa;
III – a liberdade de expressão, de informação, de comunicação e de opinião;
IV – a inviolabilidade da intimidade, da honra e da imagem;
V – o desenvolvimento econômico e tecnológico e a inovação;
VI – a livre-iniciativa, a livre concorrência e a defesa do consumidor;

> VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2019)

Importante ressaltar também que a Lei em sua atualidade apresenta requisitos para o tratamento correto dos dados, elencados por sua vez sendo:

> I. Mediante o fornecimento de consentimento pelo titular;
> II. Para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III. Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV. Para a realização de estudos por órgão de pesquisa – garantida, sempre que possível, a anonimização dos dados pessoais;
> V. Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei n. 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII. Para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII. Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX. Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X. Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (BRASIL, 2019)

Por fim ressalta-se que a Lei Geral de Proteção de Dados Pessoais- 13.709- elenca que, o possuidor tem direito a informação bem como ao acesso facilitado às informações no que se trata do tratamento de seus dados pessoais. Constata-se ainda que tais informações devam constar sempre disponíveis de maneira clara e adequada, de forma que consiga esclarecer pontos como a finalidade do tratamento, a identificação do controlador, as responsabilidades dos agentes que realizarão o tratamento e os direitos da pessoa interessada.

4.3 A Lei Geral de Proteção de Dados e a proteção ao período pandêmico

Observa-se que no momento atual em que vivemos, cada vez mais torna-se frequente a invasão de dispositivos e a configuração do crime previsto no artigo 154-A e 154B do Código Penal brasileiro.

Durante o ano de 2019 até o presente momento, muito tem falado sobre os ataques cibernéticos sofridos por parte governamental em virtude da implantação do auxílio emergencial bem como da ferramenta de pagamento eletrônico instantâneo e gratuito oferecido pelo Banco Central- PIX. Menciona-se dessa forma, que tais mecanismos tornaram-se meios de obtenção por parte de Hackers.

Segundo Fabio Assolini, analista de segurança da Kaspersky,

> Alguns dos golpes usam o Pix como tema. Nessa modalidade, os bandidos alertam a vítima de que a ferramenta está com um problema que precisa ser corrigido por meio de um link. Ao clicar, entretanto, a pessoa é direcionada a um site falso, onde é induzida a informar os dados bancários. (MUNHOZ,2021)

Outro caso muito frequente durante esse período foi no que diz respeito aos golpes ocorridos perante a ajuda oferecida pelo governo federal com o Auxílio emergencial, segundo a Polícia Federal;

> O golpe foi aplicado da seguinte forma: a quadrilha realizava o cadastro da conta-vítima no aplicativo da Caixa, banco responsável por distribuir o auxílio emergencial. Quando o recurso era disponibilizado (na conta-vítima), os criminosos realizavam imediatamente pagamentos e transferências, como forma de camuflar a fraude, direcionando os valores, ao final das operações, para contas dos investigados. Quando as vítimas, que tinham seus dados usados pelos investigados, requeriam o benefício, descobriam que supostamente já tinham recebido. (FIGUEIREDO,2021)

Consoante a isso, nota-se a audácia existente por parte de indivíduos que enfrentam a tutela penal exposta atualmente no pais, que apesar de rígida, não apresenta muita eficácia para sanar eventos como os dos golpes realizados por quadrilhas especializadas no PIX.

4.4 Política e técnicas eficientes de proteção

Há que se afirmar que o legislador ao editar a mudança feita pela lei 12.737/2012, obteve um descuido, deixando de certa forma vaga sua interpretação quanto à punição. Uma vez que ao analisar o disposto nos artigos 154-A e 155 do Código penal, o preceito secundário não se equipara.

É notório que a legislação brasileira em demasia não colabora para a efetiva atuação das normas vigentes, haja vista ser consideras pequenas e até mesmo, irrelevantes, ao serem comparadas com países a qual a lei de proteção de dados se demonstra altamente satisfatórias, como é o caso dos "países membros" da União Europeia.

Evidente que os crackers, são problemas de segurança mundiais. Deste modo, a interferência de tratados internacionais se faz necessário, visando uma maior amplitude de punibilidade para o cometimento de tais crimes.

O Brasil em especial vem se moldurando em novas leis de combate a crimes cibernéticos, entretanto é questionável até onde vai o poder punitivo da união em tais crimes. Como mencionado, a legislação tem deixado a desejar, na elaboração e na efetuação de medidas coercitivas eficazes de modo geral aos crimes praticados.

Nos crimes em gerais, os quais hoje vêm assolando excessivamente todo o país, a sensação de impunidade toma conta, de modo que com isso os criminosos tomem coragem e força para continuar bem como agravar a pratica dos diversos crimes. Haja vista terem conhecimento da ineficácia da legislação, bem como na punição das diferidas leis vigentes. No entanto, ao abordamos a respeito de crimes cibernéticos, os legisladores e contribuintes da justiça, tem que se utilizar de ferramentas satisfatórias, a fim de adequá-las a seu caráter punitivo.

Há que se ressaltar que atualmente no Brasil, o caráter punitivo é tido como um fator desestimulante ao agente, de forma a impor um valor suficiente, que possa por sua vez servir como uma efetiva punição, de modo a evitar novas práticas lesivas do mesmo ou de diversas infrações. Sendo assim, visa-se de modo efetivo diminuir ou até mesmo extinguir tais ataques, sem que haja dessa forma o mesmo caráter de impunidade e ineficácia que as leis brasileiras transmitem, seja contra pessoas físicas ou jurídicas, do baixo ou alto escalão, do Brasil ou do mundo de forma geral.

Diante disso, temos que ter em mente a ideia de uma efetiva lei, bem como afirma Beccaria, o qual "É melhor prevenir os crimes do que ter de puni-los." (BECCARIA,1764) De maneira que tais leis efetivas busquem inibir novos atos de tais

crimes virtuais, bem como visar influenciar a criação de legislações aspirando ao amparo tecnológico dos poderes existentes no país.

Ademais, constata-se ser de suma importância equipar a polícia judiciária com tais recursos eficientes ao combate da criminalidade virtual, importante também ensinar através de cursos gratuitos, visando toda a coletividade, o correto uso das redes sociais, bem como os modos viáveis de evitar que tais ataques se tornem mais comuns. Uma vez que, segundo o IBGE, 79% da população tem acesso à internet. Dentre os quais, segundo o IBOPE, 42% das pessoas possuem mais de 35 anos, e 15% desse percentual são pessoas menores de 15 anos. (IBGE,2019)

Analisando desse ponto, podemos alegar que a elaboração de cursos para o correto manuseio para o uso de internet, de certa forma poderia ocasionar em melhoras significativas nos acontecimentos de crimes virtuais. Visando dessa forma contribuir de ambos os lados, tanto no lado do manuseio pelos clientes das redes sociais, como no lado legislativo, visando medidas coercitivas mais severas e eficazes.

Diante disso, é notório a necessidade de ampliação de medidas eficazes ao combate do cibercrime por parte do governo, como dito, através de cursos, publicidade, bem como maiores informações a respeito do uso adequado das redes sociais, visando amplamente atingir todas as faixas etárias. Com intuito de beneficiar a sociedade na diminuição de vítimas de tais crimes.

CONCLUSÃO

Levando-se em consideração os aspectos apresentados, conclui-se que o presente artigo cumpriu sua finalidade de repassar, informar e exemplificar de forma clara e didática ao público leitor, a respeito de determinados pontos atualmente em foco na sociedade moderna tecnológica, no que tangem os direitos postergados perante a Constituição Federal e ainda ressaltar os atos criminosos através de redes de computadores, os quais atuam contrariamente à carta magna de 1988, utilizando-se dessa forma embasamentos legais e fatídicos coerentes.

Em um primeiro momento a questão envolvendo o atual valor, e a importância dos dados pessoais pertencentes aos usuários das redes sociais e demais plataformas on-line foi abordada, de forma a mencionar o aumento em demasia dos usuários a internet e o crescente número dos crimes virtuais, que se torne cada vez mais frequentes na sociedade.

Adiante, o foco é voltado para a questão de o espaço cibernético ser um grande centro da criminalidade digital. Necessário mencionar que em momentos atuais, o uso da internet além de facilitador é também um meio eficaz de se manter em alta perante as mudanças globais. A criminalidade virtual favorece muitas vezes a impunidade dos agentes infratores, os quais nem sempre visam obter somente vantagem monetária em cima das vítimas, mas também causar prejuízos sociais, por exemplo, a membros do alto escalão, como apontado no decorrer do artigo.

É importante frisar que o artigo contém, de forma sucinta, uma espécie de crítica em relação ao Brasil pela forma legislativa ainda atrasada para lidar com o aumento da prática de crimes em âmbito digital, quando comparada a demais potências. Ainda assim, as medidas já existentes são explicadas e apontadas em seus pontos positivos e eficazes, bem como as que ainda estão sendo preparadas para entrar em vigor e seus pequenos avanços, de acordo com a legislação brasileira, conforme as leis, 13.709 e 12.737/2012 e suas alterações.

Além da importância de conscientizar a respeito do aumento da ocorrência de crimes digitais, o texto ainda apresenta importantes diferenças entre certos agentes os

quais praticam tais ilícitos, para acrescentar ao intelecto do leitor, fatores extremamente interessantes para saber em pleno século XXI.

Sendo assim, é possível concluir que através da pesquisa foi possível perceber que devido ao presente momento em que se encontra a sociedade, abordar tal tema se torna extremamente essencial, tanto do ponto de vista jurídico quanto informativo, para todos os tipos de público.

REFERÊNCIAS

A LGPD em um giro, Serpro.gov, 2020. Disponível em:<https://www.serpro.gov.br/lgpd/noticias/2020/lgpd-giro> Acesso em: 27, jul. 2021

ALVES, Paulo. **O que são cookies? Entenda os dados que os sites guardam sobre você,** São Paulo, 2018. Out.2018. Disponível em:<https://www.techtudo.com.br/noticias/2018/10/o-que-sao-cookies-entenda-os-dados-que-os-sites-guardam-sobre-voce.ghtml.> Acesso em: 23 de jul. 2020.

ARIMURA, Mayumi. **Saiba a diferença entre Hackers, Crackers, White Hat, Black Hat, Gray Hat, entre outros,** 2016. Disponível em:<https://egov.ufsc.br/portal/conteudo/saiba-diferen%C3%A7a-entre-hackers-crackers-white-hat-black-hat-gray-hat-entre-outros.> Acesso em: 25, jul 2021.

BACH, Sirlei Lourdes. **Contribuição do hacker para o desenvolvimento tecnológico da Informática**, 2001. Disponível em:<https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/82176/184565.pdf?sequence=1&isAllowed=y> Acesso em: 02,ago. 2021.

BACKUP GARANTIDO**. 7 tipos de ataques hacker que você precisa conhecer, Belo Horizonte,** 2018. Disponível em:<https://blog.backupgarantido.com.br/tipos-de-ataque-hacker/.>Acesso em: 26, jul.2021

BRASIL, Superior Tribunal de Justiça, Lei geral de proteção de dados, Disponíviel em:<https://www.stj.jus.br/sites/portalp/Leis-e-normas/lei-geral-de-protecao-de-dados-pessoais-lgpd.> Acesso em : 14, abr. 2022.

BRASIL. **Constituição** (1988). **Constituição** da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988. Disponível em:<http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 24, jul.2021.

BRASIL; **Convenção sobre cibercrime**. Budapeste, MPF. 2001. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-egislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf.> Acesso em: 21, jul. 2021.

BRASÍLIA. **Projeto de lei N.º 9.744**, Câmara dos Deputados, 2018. Disponível em:<https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=5DEF326188F36A860A2636622A1B4569.proposicoesWebExterno1?codteor=1645590&filename=Avulso+-PL+9744/2018.> Acesso em: 23, jul. 2021.

CNJ; **Crimes digitais: quais são, quais leis os definem e como denunciar,** 2018. Disponível em: <http://www.justificando.com/2018/06/25/crimes-digitais-quais-sao-quais-leis-os-definem-e-como-denunciar/.> Acesso em: 21, jul. 2021.

CUNHA, Carolina. **Proteção de dados - a questão da privacidade dos cidadãos na internet.** 2018. Disponível em: <https://vestibular.uol.com.br/resumo-das-

disciplinas/atualidades/protecao-de-dados-a-questao-da-privacidade-dos-cidadaos-na-internet.htm> Acesso em: 24, jul. 2021.
FIGUEIREDO, Fabiana**. Grupo que teria aplicado golpes no auxílio emergencial e desviado R$ 65,5 mil é alvo de operação da PF**.2021 Disponível em: <https://g1.globo.com/ap/amapa/noticia/2021/07/20/grupo-que-teria-aplicado-golpes-no-auxilio-emergencial-e-desviado-r-655-mil-e-alvo-de-operacao-da-pf.ghtml> Acesso em: 08, jan. 2022.
G1. **Lei 'Carolina Dieckmann', que pune invasão de PCs, entra em vigor**, 2013. Disponível em: <http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html>Acesso em: 02, ago. 2021.
G1. **Lei 'Carolina Dieckmann', que pune invasão de PCs, entra em vigor,** São Paulo, Abr, 2013. Disponível em: <http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html>Acesso em: 02,ago. 2020.
IBGE-Instituto Brasileiro de Geografia e Estatística. **Uso de Internet, televisão e celular no Brasil,** Brasil**.** 2018. Disponível em:<https://educa.ibge.gov.br/criancas/brasil/2697-ie-ibge-educa/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular-no-brasil.html.>Acesso em: 23,jul. 2021.
MORAES, Alexandre de. **Direito Constitucional. São** Paulo: Atlas, 2016, 32ª ed., p. 74
MUNHOZ, Fábio. **Criminosos usam pix para dar golpes**. Folha de São Paulo, 2021. Disponível em:<https://agora.folha.uol.com.br/grana/2021/07/criminosos-usam-o-pix-para-dar-golpes-saiba-como-se-proteger.shtml> Acesso em : 08,jan.2022
PRESSE, France. **Twitter afirma que hackers 'manipularam' funcionários para conseguir acesso a contas, 2020.** Disponível em:<https://g1.globo.com/economia/tecnologia/noticia/2020/07/18/twitter-afirma-que-hackers-manipularam-funcionarios-para-conseguir-acesso-a-contas.ghtml.>Acesso em: 01,ago. 2020.
ROHR, Altieres. Cartões de crédito dos EUA são fraudados a partir do Brasil, 2014**.** Disponível em: >http://g1.globo.com/tecnologia/noticia/2014/11/cartoes-de-credito-dos-eua-sao-fraudados-partir-do-brasil.html> Acesso em: 23, jul. 2020.
Senado Federal. **Proteção de dados pessoais deverá ser direito fundamental na Constituição,** 2019. Disponível em:<https://www12.senado.leg.br/noticias/materias/2019/07/02/protecao-de-dados-pessoais-devera-entrar-na-constituicao-como-direito-fundamental> Acesso em: 23, jul.2021**.**
SUPREMO TRIBUNAL DE JUSTIÇA.**Justiça usa Código Penal para combater crime virtual,** 2009. Disponível em:<https://stj.jusbrasil.com.br/noticias/234770/justica-usa-codigo-penal-para-combater-crime-virtual.>Acesso em: 22, jul. 2021.
TOONDERS, Joris; **Data is the new oil of the digital economy**. Wired Cnmn collectio, California. 2018. Disponível em: <https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/.> Acesso em: 14, set. 2021.
WARD, Mark. **Saiba mais sobre a história dos hackers,** 2011**.** Disponível em:<https://www.bbc.com/portuguese/noticias/2011/06/110623_historiahacking_is#:~:text=A%20origem%20do%20termo%20hacker,ou%20elegante%20para%20qualquer%20problema.> Acesso em: 27, jul.2021.

FERMINO, Leandro, Hacker: o que é, o que faz e qual a diferença de um cracker?, 2020. Disponivel em: <https://canaldosul.com.br/hacker-o-que-e-o-que-faz-e-qual-a-diferenca-de-um-cracker/> Acesso em: 10, set.2022.
GONÇALVES, Mariana Sbaite, **Conheça o Ethical Hacking**. 2021. Disponivel em:https://www.lgpdbrasil.com.br/conheca-o-ethical-hacking/ Acesso em 10, jun.2022.
BECCARIA, Cesare de**.** ***Dos Delitos e das Penas. Capítulo XLI.*** *1764.* Edição Ridendo Castigat Mores. Iniciativa de Nélson Jahr Garcia. Disponivel em:https://www.oab.org.br/editora/revista/revista_08/e-books/dos_delitos_e_das_penas.pdf Acesso em: <10.set.2022)