PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

PROTEÇÃO DOS DADOS EXPOSTOS NA INTERNET

ORIENTANDO (A): DANILO LINHARES SANDES BARROS
ORIENTADORA: PROFA: Ma. ÉVELYN CINTRA ARAÚJO

GOIÂNIA-GO
2022

DANILO LINHARES SANDES BARROS

PROTEÇÃO DOS DADOS EXPOSTOS NA INTERNET

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Prof.(a) Orientadora: Ma. Évelyn Cintra Araújo.

GOIÂNIA-GO

2022

DANILO LINHARES SANDES BARROS

PROTEÇÃO DOS DADOS EXPOSTOS NA INTERNET

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____

Orientadora: Profa: Ma. Évelyn Cintra Araújo Nota

_____

Examinador (a) Convidado (a): Prof. (a): Titulação e Nome Completo Nota

Dedico esse trabalho para meus familiares e amigos que me apoiaram desde meu início da minha jornada acadêmica.

Agradeço a todos que me apoiaram durante todo esse período de aprendizado, como professores e colegas que me ajudaram muito em meus objetivos. Muito prazer em dedicar esse trabalho, que é algo que permite que eu finalize minha trajetória no bacharelado no curso de direito.

Grato por minha orientadora que me mostrou os melhores caminhos para realizar esse trabalho, me guiando para que eu consiga entregar da melhor forma.

SUMÁRIO

PROTEÇÃO DOS DADOS EXPOSTOS NA INTERNET

Danilo Linhares Sandes Barros [1]

O presente artigo científico tem como objetivo a analisar os chamados crimes cibernéticos e os riscos que eles trazem em suas diferentes espécies para os usuários. Em uma sociedade cada vez mais conectada, a utilização da Internet é uma ferramenta fundamental para trabalho ou simplesmente lazer, criando vários mecanismo para a atuação de criminosos que se utilizam do conhecimento virtual para praticar delitos. Serão abordados temas sobre leis já vigentes e aspectos relacionados a métodos de investigação e produção de provas para combater estes crimes. Serão apontadas também, inovações legislativas trazidas como Lei Geral de Proteção de Dados Pessoais (LGPD), LEI n°. 13.709/2018.

Palavras-chave: Ambiente Virtual, Crimes Virtuais, Legislação.

[1] Qualificação do autor.

INTRODUÇÃO

A modernidade trouxe para dentro da sociedade global, a facilidade de comunicar-se e interagir com pessoas sem mesmo conhecer pessoalmente, trouxe maneiras de compras em sites, aderindo qualquer produto com apenas alguns clicks, através de um equipamento eletrônico pela a rede mundial de computadores, navegando pela a internet.

Com a expressiva evolução e a expansão da tecnologia, e a sua utilização da sociedade na internet, não resta dúvidas sobre as pessoas se tornaram dependentes de dispositivos eletrônicos em razão da internet, construindo um mundo ainda novo para todos, com trocas de informações entre pessoas diferentes, em lugares diversos e em regiões em todo o mundo. Essa é a nova realidade, crescimento de trabalho e o aumento de relações envolvendo a internet, onde o Direito tem que se adequar para a garantia de segurança no ambiente virtual para que não se torne uma “terra sem lei”.

Essa adequação é de grande relevância para dentro do Direito Penal, com um aumento muito crescente em torno deste anos recentes de crimes virtuais, conhecido também como crimes cibernéticos, sendo assim, criando novas legislações para esta natureza em ambiente virtual, criando órgãos especializados nestes crimes, com a evolução da lei e da investigação para chegar no autor.

Estes crimes cometidos pelas as redes sociais, que na sua maioria há bastante dificuldade para a descoberta do autor, com a perca de provas, podendo ser facilmente apagadas, alteradas perdidas e a morosidade de aplicativos e sites para que se possa ser entregue as autoridades, dando uma maior instabilidade para a polícia.

A má utilização da tecnologia elevam as consequências e responsabilidades, sendo tratadas na segunda parte do texto. O uso sem o conhecimento do mundo virtual e por inocência pode proporcionar a prática de ofender a honra e a imagem das vítimas, trazendo o surgimento danos emocionais e psicológicos, além de danos materiais, sendo o Estado o maior responsável pela a proteção dos usuários em um mundo virtual.

Desde o surgimento destes crimes, a legislação tem o grande desafio de acompanhar destas práticas criminosas, muitas vezes sendo feitas fora de território nacional, mas colocando a população em riscos. A evolução lamentavelmente não

está no mesmo ritmo de crimes virtuais, assim há a necessidade de atualizações e a aplicação do Código Penal neste meio.

Será feita uma breve análise das principais leis referentes aos crimes virtuais, sendo as leis 12.737/2012 e 12.965/2014, onde a intenção foram ter uma punição maior para quem é responsável por estes crimes, e a lacunas ainda existentes sobre a nossa legislação.

Não foram citados todos os crimes e tipos de infrações cometidos em ambiente virtual, focando na evolução, como crimes próprios e impróprios, acontecimentos históricos e a evolução da legislação brasileira, em relação estes crimes, focando naqueles direcionados a honra, imagem, a moral e a necessidade da proteção legal sobre as vítimas.

A metodologia utilizada foram as pesquisas bibliográficas em livros, artigos científicos, sites e monografias. Acreditando em que esta questão deveria ter uma grande importância em toda a nossa realidade atual, como cada pessoa está ainda mais refém da internet agora e anos próximos.

1 COMO A INTERNET PODE FAVORECER OS RISCOS VIRTUAIS

Com a criação da internet em meados do século passado, durante a Guerra Fria, marcada por umas das grandes invenções da humanidade para realizar comunicações entre militares durante aquele período de confronto, ajudando essa relação sobre as bases passando informações se houvesse ataque de inimigo.

Durante anos foi se atualizando no final do século XX, com interligações, chamada hoje como e-mail com os Estados Unidos da América, Reino Unido e a Noruega.

Auriney Brito (2013, p.21) diz:

> A intenção dos criadores da internet era internalizar as comunicações durante as guerras. O projeto era denominado "*Arpanet*", que futuramente foi fundido pelos Estados Unidos com outro projeto, dando origem ao nome internet. Inicialmente, era utilizada restritamente. No entanto, após alguns anos, passou a ser comercializada.

De acordo com Fabrizio Rosa (2002, p.29):

> No fim de 1972, Ray Tomlinson inventa o correio eletrônico, até hoje a aplicação mais utilizada na NET. Em 1973, a Inglaterra e a Noruega foram ligadas à rede, tornando-se, com isso, um fenômeno mundial. Foi quando no mesmo ano veio a público a especificação do protocolo para transferência de arquivos, o FTP, outra aplicação fundamental na internet. Portanto, nesse ano, quem tivesse ligado a ARPANET já podia se logar. Como terminal em um servidor remoto, copiar arquivos e trocar mensagens. Devido ao rápido crescimento da ARPANET, Vinton Cerf e Bob Kahn propuseram o (Transmisson Control Protoco/internet Protocol– TCO/IP), um novo sistema que utilizava uma arquitetura de comunicação em camadas, com protocolos distintos, cuidando de tarefas distintas. Ao TCP cabia quebrar mensagens. Ao IP cabia descobrir o caminho adequado entre o remetente e o destinatário e enviar os pacotes.

No Brasil chegou conhecimento da internet no ano de 1988, logo após o grande salto tecnológico mundial, vem evoluindo e adaptando na vidas das pessoas cada vez mais forte e presente, com criação de máquinas tecnológicas e cada vez menores, podendo ser transportadas no dia a dia. Por volta dos anos 2000, dispararam os números de avanço tecnológico, com a esta evolução, a tecnologia está sendo fixado em nossa vidas, assim tende muito a crescer ainda mais o acesso e a necessidade de toda a sociedade com a internet e seus serviços.

Hoje a internet não possui nenhum órgão governamental que a regule rigidamente, ocorrendo livremente em toda parte do mundo a comunicação entre aparelhos tecnológicos.

Um dos marcos mundial, uma internet sem fronteiras e poderosa, que aconteceu em nossa história o ataque de 11 de setembro, com fins terroristas sobre o EUA, assim houve uma fiscalização e convenção, maior juntamente com a comunidade europeia, causando uma proximidade de legislação em âmbito mundial, estabelecendo pilares sobre o direito material e processual e classificando tipos de crimes da internet e estabelecendo controles de delitos cometidos nas redes.

Rede social é uma estrutura composta por pessoas ligadas um ás outras por uma relação amigável, política, comunitária ou profissional, possibilitando compartilhamento de informações, experiências, enfim. Relações que já existia antes da internet, agora de maneira global, de forma rápida podendo ser passada para qualquer lugar do mundo, tornando o ser humano sociável e ouvida por todos.

Uma realidade de desejo das pessoas, postar suas vidas e experiências para que todos possam ver, tornando-a onipresente com um instinto social. Este aumento trazem para os usuários maiores riscos, com o fornecimentos de seus dados para as plataformas, com a exposição de pessoas que tem o seu convívio e proximidade com familiares sendo expostos para todos.

Nesse sentido, Rossini (2004, p. 78):

> O conceito de ‘delito informático’ poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.

Crimes cibernéticos classificados em próprios e impróprios, expondo sujeitos ativos e passivos, com toda uma complexidade por trás deste assunto tão evidente e mais comum do que a população acham.

Sérgio José Barbosa Junior (2014) em seu artigo sobre crimes informáticos, discorre:

> “De forma simples, pode-se afirmar que crimes informáticos são aqueles praticados mediante a obtenção indevida de dados – informações – que foram ou estão sendo processados por um terceiro”.

O número de vítimas de pessoas que sofrem com a exposição de fotos íntimas, extorsões, invasões e diversos crimes em sites e aplicativos de smartphones, vem aumentando ano a ano. Os usuários usam a rede mundial para acessar informações diversas, às vezes em um número ilimitado de situações, onde a Internet pode fazer várias perguntas, o que vai acontecer, e as informações disponíveis ou

indisponíveis na Internet podem trazer punições para quem as usa sem autorização, nomeadamente, o direito à privacidade é uma restrição natural ao direito à informação.

Tratando de um acesso sem autorização da vítima, violando as medidas de segurança e invadindo sistema de informação, sendo ele individual ou um grupo de pessoas. Resultado no Brasil, para algumas doutrinas, as visitas ilegais estão sujeitas a penalidades criminais, a Lei n. 12.737/2012. Para outros autores, o Brasil os pune com arte.

Brasil (2008 p.23).

> Crime virtual ou crime digital pode ser definido como sendo termos utilizados para se referir a toda a atividade onde um computador ou uma rede de computadores são utilizados como uma ferramenta, uma base de ataque ou como meio de crime. Infelizmente, esta prática tem crescido muito já que esses criminosos virtuais têm a errada impressão que o anonimato é possível na Web e que a Internet é um “mundo sem lei.

Com os cybercrimes, existe dois tipos de criminosos que são os sujeitos ativos, que são aqueles utilizam de seus conhecimento avançados de informática e de internet, que praticam seus atos em vítimas leigas, que não tem este conhecimento aguçados ou sistemas de segurança de empresas de forma ilegal colhendo informações que possam ser sigilosas e que tomam proveito para si. É preciso separar as nomenclaturas e classificações de Hackers que utilizam estes conhecimento técnicos diferentes e habilidades para estes fins ilícitos.

Sujeitos ativos na práticas de crimes virtuais contra usuários.

a) Preaker

São fraudes que utilizam por meios de comunicação telefônica, para proveito para si, algum tipo de pagamento, instalando de forma ilegal escutas e outros dispositivos para ter acesso em conversas telefônicas de forma externas que possam colher informações confidenciais que enganam o sistema de telefonia. Pode ser usadas em dispositivos para rotear suas próprias chamadas e ignorar o acompanhamento do sistemas de empresas telefônicas, com permite chamadas gratuitas para outras pessoas. Esta modalidade foi mais comum antes dos computadores pessoais e é considerado antecessor do precursor do computador hacker, com a mudança da internet hoje poucos hackers tem este domínio.

b) Oracker

São os sujeitos que não tem o mesmo o conhecimento de um hacker, porém buscam formas de certa forma leigas para praticar crimes virtuais, geralmente são pessoas que começam se aventurar nesta modalidade de crimes.

c) Hacker

Pessoas sábios de inteligências que utilizam de grande sabedoria da tecnologia que ameaça contas pessoais e empresariais, quanto sistemas de segurança e utiliza para invadir sistemas por desafios pessoais que muitas das vezes nem causa danos para o próximo.

d) Cracker

Possui os mesmo conhecimento de inteligência virtual e aparelhos e sistemas empresariais, mas utilizam para ter prejuízo a outrem, bem como lucrar com esses tipos de práticas de crimes.

Wilson José de Oliveira (2006. p.26) explica:

> Hacker: pessoa que possui grande facilidade de análise, assimilação e compreensão, aplicadas ao trabalho com um computador. Ele sabe perfeitamente (como todos nós sabemos) que nenhum sistema é completamente livre de falhas, e sabe onde procurá-las utilizando técnicas das mais variadas. Cracker: possui tanto conhecimento quanto aos hackers, mas com a diferença de que, para eles, não basta entrar em sistemas, quebrar senhas e descobrir falhas: precisam deixar um aviso de que estiveram por lá. Geralmente são recados malcriados, mas, algumas vezes, podem destruir partes do sistema, ou aniquilar tudo o que veem pela frente. Também são atribuídos aos crackers programas que retiram travas de softwares, bem como os que alteram suas características, adicionando, ou modificando, opções, muitas vezes relacionadas à pirataria.

Sujeitos passivos é aquele que vem a receber prejuízo com alguma conduta delituosa virtual, titular de um bem jurídico lesado ou ameaçado seus patrimônios ou não, possivelmente pessoas jurídicas ou físicas de natureza tanto privada, como de natureza pública.

Molina (2011. p. 54).

> Podemos citar ainda, as vítimas de pedofilia, de pirataria de software, de dano, contra a honra, entre muitas outras vítimas de crimes praticados pela Internet. A agilidade que a Internet proporciona ao seu usuário para realização de diversas tarefas, como entretenimento, trabalho, pagamentos de despesas, entre outras, facilita também a ação de pessoas inescrupulosas que se aproveitam do anonimato e da falta de segurança existente na rede para conseguir informações sobre os usuários, principalmente senhas que são digitadas durante essas transações. Os atos ilícitos praticados via Internet, a cada dia que passa, aumentam a sua prática e sua diversificação. Temos crimes antigos, que agora são praticados pela rede mundial, assim

> como, temos novas modalidades. No entanto, alguns desses crimes já estão tipificados no nosso ordenamento jurídico, por exemplo: o furto, estelionato e etc.

Suas classificações doutrinárias sobre a natureza jurídica de crimes cibernéticos caracterizando em próprio e impróprio.

a) Próprio

Onde o agente utiliza o meio de execução essencial que seria o computador do sujeito passivo, para cometer um delito utilizando como objeto e meios de invasão de dados não autorizados. Com isso gerando prejuízo aos bens jurídicos pelos os crimes de dados em outra rede ou sistema.

b) Impróprio

Não é essencial a máquina ou computador para cometer o crime, podendo ser afetado o bem jurídico de várias maneira e atingindo o mundo físico, além da informática, como crimes de ameaça, furto, estelionato calúnia, pedofilia e outros. Crimes tipificados que são cometidos em meio informático, onde o autor se vale conhecimento do meio informático para produzir o resultado naturalístico, atingindo o mundo real e virtual, onde a ferramenta internet é somente uma ferramenta para a execução. Também não se faz necessários conhecimentos técnicos, entretanto, para a pratica de delitos considerados próprios, há a necessidade deste conhecimentos da computação.

Nesse sentido, podemos dizer que todas as condutas praticadas contra bens jurídicos informáticos (sistema, dados) são delitos de risco informático ou próprios. Ao passo que aquelas outras condutas que se dirigirem contras bens jurídicos tradicionais (não relativos à tecnologia) são crimes digitais impróprios.

Os crimes virtuais estão ganhando mais espaço em jornais e noticiários do mundo inteiro, pela quantidade de pessoas e empresas que são vítimas, devido uma mal orientação de algum uso de aplicativos e sites ou por enganos de contas fakes feitas pelos os criminosos, e invasões que buscam ter dados pessoais. Com toda essa facilidade com que a internet permite que os autores podem prejudicar o próximo, tanto com transmissão de dados e que podem os tornar anônimos

Esta prática ilícita tende piorar, caso não sejam fiscalizadas de forma abrangente e eficaz, com o passar dos anos e efeitos da pandemia que muitas

pessoas passam usufruir das tecnologias para sua sobrevivência, aumentando para grande maioria de pessoas conectadas online em seus domicílios e trabalhos.

Faz-se necessário um estudo aprofundado sobre a rede mundial de computadores e a evolução seja coerente com a normas que assegura uma melhor utilização de seus usuários. O Estado tem esta missão de não permitir que atos oriundos de pessoas más intencionadas ferem o bens jurídicos tutelados, reduzindo p aumento de criminalidade virtual.

Em Agosto de 2017, teve uma decisão inédita do TJPI – Tribunal de Justiça do Piauí, de estupro virtual, onde o homem com o perfil falso em uma rede social ameaçava uma ex-namorada a mandar exibindo fotos e vídeos íntimos, assim o julgado entendeu como extorsão, que seria uma junção da palavra sexo e extorsão, prática sexual ou pornográfica.

Houve uma alteração recentemente do Código Penal, onde se encaixa perfeitamente neste caso, devido que não houve uma conjunção carnal e sim um ato libidinoso, o juiz nesta decisão adequou o crime virtual ao tipo penal que foi o estupro.

> Art. 213.Código Penal - Constranger alguém, mediante violência ou grave ameaça, a ter conjunção carnal ou a praticar ou permitir que com ele se pratique outro ato libidinoso:
> Pena - reclusão, de 6 (seis) a 10 (dez) anos.

Quando STJ reconhece a tipificação e a gravidade de que é utilizado por instrumento moderno e expansão muito grande e pode atingir uma multidão de pessoas, é uma contribuição específica para interpretação e julgamento de crimes graves como pedofilia pela internet.

Os crimes cibernéticos vão ocorrendo de forma muito rápida, que a um descompasso com a profissão da Lei que é muito mais lenta, e com isso a legislação tem um desafio de acompanhar o amparo jurídico com a evolução tecnológica da sociedade.

Com essa evolução crescente acaba influenciando na privacidade de todos usuários, se tornando a cada dia mais existente no meio virtual.

> 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> 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;

Precisa de uma mão de obra de policiais que tenha um acompanhamento na rede, aqueles que visam prevenir o crimes antes que aconteçam, como acesso a (IP) Internet Protocol, uma versão numérica do nome do hospedeiro, onde todo computador de rede tem um endereço de IP, que seria a localização do autor e acessos a sites que possam levar a crer que tenha uma eventual pratica de crime e em loco, que são acompanhamento de criminosos pessoalmente. Muitas das vezes os criminosos usam provedores para movimentar seus atos de outros países que dificultam a sua localização, que é um grande desafio para as investigações devido a ter um acesso pacífico e que grandes empresas que usam e desenvolve estes provedores, é resistentes para estas quebras de sigilos de contas de seus usuários. Além da dificuldade que tem a investigação tem a burocracia que não oferece uma cobertura melhor para os envolvidos.

André Giachetta ainda afirma em Consultor Jurídico no site conjur.com.br:

> Há graus de dificuldade para indicar o culpado, mas não é impossível." Para ele, o número do IP hoje é muito mais relevante do que qualquer outro dado do internauta. “Em um crime de internet, ter o RG do suspeito é menos importante do que o endereço de IP, que prova o momento e local em que o ato foi cometido.

Emerson Wendt e Higor Vinicius Nogueira Jorge (2014.p.54) pesclarecem:

> quando ocorre a conexão de um computador ou dispositivo similar à internet (como celular, tablet etc.), o endereço de IP (Internet Protocol) é atribuído exclusivamente para aquele internauta. Da mesma forma que dois corpos não ocupam o mesmo lugar no espaço, não existem dois usuários com o mesmo IP durante a navegação na internet (mesmo dia e hora e fuso horário), independentemente do endereço IP ser estático ou dinâmico.

Hoje existe uma dificuldade muito evidente, que não tem tipificações penais adequada para tamanha e complexas de atos criminosos pela a internet.

Nós temos alguns tipos penais que são praticados através da internet, mas não tipificado e se usa uma analogia no processo penal, que tem comparações de crimes, que isto para o direito penal é muito sensível e pode trazer uma atipicidade e com isso causando uma nulidade para o processo, beneficiando os criminosos em esfera penal.

Entre uns dos mais comuns de crimes estão as fraudes virtuais, que é definido uma conduta de invasão, alteração ou modificação, pagamento ou supressão de dados ou alteração em sistemas. Ficou muito conhecido nacionalmente após uma famosa teve o seu computador invadido por hacker e teve suas fotos divulgadas. Assim criando uma lei voltada para este tipo de delito.

Nos últimos anos, a incidência de fraudes virtuais ou eletrônicas tem sido alarmante, principalmente no furto por fraude (artigo 155 da Lei Penal), que se caracteriza pelo envio de e-mails falsos aos usuários (phishing) e pela instalação de programas no acesso à Internet dispositivos para obter ilegalmente dados de suas contas bancárias.

Esta dificuldade decorre pela a manipulação de dados que são exclusivo de conhecimento de computação e intermédio de computadores com programação, que permite alterar horários interno, programando o computador invadir algum sistema com a data em um horário diferente certo.

Nas fraudes, os usuários precisam fornecer seus dados pessoais e financeiros, que geralmente ficam ocultos atrás de páginas suspeitas. Os usuários são chamados de páginas fraudulentas. Os fraudadores geralmente usam as mídias sociais e tentam induzir os usuários a fornecer suas informações pessoais de várias maneiras.

Em relação à fraude de computador, temos dois tipos de fontes:

a) Interna - é realizada por um funcionário ou terceiro no site da fraude;

b) Externa - o fraudador não tem nada a ver com o relacionamento do site da fraude, mas tem não significa que o agente fraudulento um dia não terá um relacionamento com a vítima.

Notamos que atualmente estas decisões envolvendo as redes sociais e invasões de sistemas, como persecução penal, vem se atualizando na base do empirismo, de caso a caso, surgindo decisões antagônicas. Como por exemplo citando o aplicativo whatsapp, onde acontece de instantes e verificamos decisões judiciais de bloquear nacionalmente o funcionamento do mesmo, prejudicando todos os usuários, devido alguns descumprimento de determinações do Estado, para um meio de troca de mensagens entre delituosos que comentem crimes.

> É imprescindível que que busque sempre a persecução dos criminosos porém utilizando todas ferramentas para que não seja necessário a ilegalidade da violação dos direitos fundamentais do investigado, levando sempre em consideração que, o direito penal é a última razão na busca do equilíbrio social (OLIVEIRA,2013).

Daniel Burg diz em entrevista a Consultor Jurídico no site conjur.com.br:

> A legislação brasileira não está adequada e, muitas vezes, o crime prescreve sem que haja um avanço significativo nas investigações. Nos crimes contra a honra, por exemplo, há uma enorme dificuldade para se identificar o autor de ofensas realizadas na internet, e sem a identificação sequer é possível oferecer queixa-crime;

A impessoalidade é uma fato no mundo do crime cibernético, onde é difícil chegar ao ator e comprovar a relação dele com a materialidade do crime. Não somente as tipificações, como competências que não são bem claras, como estes crimes podem ocorrer em dois estado ou países diferentes, que isto caso ocorra dependem de cooperação internacionais e que internamente a legislação é muito branda com crimes de internet, que podem causar uma enorme prejuízo para a sociedade. Assim, esses crimes em ambientes virtuais merecem as mesmas punições de uma crime real.

É necessário observar a territorialidade do delito, seja ela nacional, o crime será julgado pela Justiça Federal ou internacional, assim afetando os bens jurídicos em outros países, é direcionado aos tratados internacionais de acordo com a Constituição Federal.

2 COMO O AUMENTO DE TECNOLOGIA ATIGE A SEGURANÇA DO USUARIO

Com o crescimento dos produtos digitais, como smartphones, computadores, brinquedos, vídeo games, o futuro já deixa-nos convictos que vai aumentar bem mais com o passar dos anos, plataformas que de certa forma dominam, como Facebook, Whatsapp, Instagram, Twitter, sites de compras online e várias outras redes sociais popularizadas, são hoje como documentos das pessoas, dificilmente há pessoas desta nova geração que não tem esses serviços digitais e usam tanto para a vida pessoa, como sites de relacionamento, quanto profissional.

De acordo com Wendt, (p.230, 2013):

> “Se deve à “A evolução tecnológica e o barateamento dos computadores e dispositivos móveis de acesso à rede mundial”

Nos últimos anos, a transformação da internet se difundiu expressivamente, com o aumento de sua velocidade de navegação, sua popularidade e possibilitando seus assessores mais ações em um período de tempo bem menor. Abre os olhos para a sociedade que inevitavelmente caracteriza a internet como necessidade para população com plataformas informatizadas e conectadas a rede.

É incrível como a velocidade de avanços tecnológicos está sendo notado em nossas vidas, com variedade de aparelhos remotos são fabricados e vendidos para a sociedade, tornando todos conectados à internet quase 24 horas por dia.

Toda esta evolução é um marco mundial e histórico para a sociedade, denominada como a ‘‘Era da Informação”, que esta ferramenta nos propõem diversos benefícios para a humanidade que tem boas intenções, mas também abre espaço para o perigo de pessoas más intencionadas, onde criminosos acham brechas para praticar delitos e causar prejuízo a sociedade, inúmeras formas e complexas situações.

Já para Sydow (2015, p.115)

> Também é uma prática bastante comum nas redes informáticas a indução de vítimas futuras e eventuais a instalarem arquivos que geram falhas de segurança ou criam verdadeiras portas de acesso livre nos dispositivos alheios. Uma vez instalados tais códigos maliciosos, o delinquente pode ingressar no sistema.

Diante destes fatos as pessoas recorrem as ferramentas eletrônicas para informar arquivos importantes de dados e documentos pessoais, como CPF, endereço de suas casas, cartões bancários, telefones pessoais e profissionais, solicitados para cadastramento e identificar o visitante que usa estas plataformas. É solicitado esses dados para trazer maior segurança ao usuários, em caso de uma invasão de outrem, estas informações possam ser usadas pelos sites para bloquear o uso de algum hacker.

Porém em que ponto essa segurança é real para os usuários, nem todos os sites são confiáveis e apropriados para receber estas informações e não dão a seguridade para quem a utiliza. Vemos hoje, tantos casos de pessoas prejudicadas por ser expostos por aplicativos, e-mails invadidos, com cartões sendo clonados, utilizando CPF ou endereço para compras de produtos de forma ilícita em comércios eletrônicos que não se previne com a segurança e só visam os lucros.

Sites comerciais trazem cookies, arquivos criados a partir de um momento adentra em alguma plataforma, que seriam utilizado por meio de um navegador para

personalizar a página de acordo com o perfil do visitante, transportando dados para dentro do computador do cliente e obtendo os endereços online. É uma estratégia de vendas de produtos, mantendo o histórico da navegação de produtos visto pelo o usuário anteriormente e os anunciando quando a pessoa muda para outro site com tempo estipulado. No entanto é comum que sites com cookies, não tenha prazo algum para serem removidos, e se mantenha na navegação, retirando a privacidade e fornecendo o seu perfil para outros sites.

Quanto à segurança da informação sobre quem utiliza sites de e-commerce, mesmo de forma não ameaçadora é, a coleta de dados como frequência que você compra, a quantidade de produtos que você precisa e a maiorias de seus hábitos de consumo expostos para organizações virtuais e terceiros desconhecidos que se utilizam dessa ferramenta para obter seus dados.

Já a definição de redes sociais que vamos usar é a de que são os sites empregados cujo material principal é a troca de informações e experiências.

De acordo com Recuero (2009, p.29)

> Uma das evoluções mais utilizadas são de sites de relacionamento, como Tinder, Facebook ou Instagram, que trazem uma boa ideia que você possa se conectar com outras pessoas para se interagir, entretanto com pouco esforço detalhes pessoais são revelados para desconhecidos, sabendo sua rotina, localização e dados para aplicação de golpes.

Pessoas que visam ter relacionamentos buscam esses aplicativos de internet, conhecendo novas pessoas sendo ela localizada em lugares próximos ou distantes, para isso é preciso entregar diversos dados pessoais para os aplicativos em seu cadastro, tornando o vulnerável.

Com publicação de algo íntimo de vítimas que recebem chantagem, extorsão e abuso digital de autores que consegue sua confiança com conversas amigáveis ou amorosas, sem mesmo ter a visto, é um método de ataque que é possível com a fragilidade emocional de pessoas que são persuadi-las a lhe encaminhar dinheiro, números de documentos e até com links com vírus que adentra ao computador ou smartphones com o acesso, muito comum nessas redes sócias. O autor deste delito nem é reconhecido pela a sua pratica golpista devido à complexidade de o localizar e a morosidade de quem é responsável por punir.

Peck (2002 p.129)

> que muitas pessoas que não cometem crimes no mundo real por medo de serem pegas acabam, de algum modo, interessando-se pela prática delituosa virtual. É o caso, por exemplo, do grande número de adolescentes de classe média, com grande conhecimento de informática, que praticam atos ilegais na

> rede e sentem-se bastante seguros em fazê-lo. Esse tipo de crime tem um traço cultural que se aproxima do vandalismo.

Contextualizando os perigos que possam causar estes, por falta de regramento deste aumento das tecnologias. A problemática de diversas maneiras possíveis de realizar uma infração, que notoriamente não são tutelas como deveria pelas autoridades e empresas fornecem esses serviços, altos índice de impunidades com seus usuários que o ordenamento jurídico não os assegura seus direitos.

Diz Jesus (2016, p.24)

> fala que enquanto no Brasil pouco se faz em estrutura investigativa, nos Estados Unidos o FBI convoca especialistas de segurança para o que anuncia ser uma “Guerra cibernética”, eis que o crime informático estaria se tornando uma ameaça maior que o próprio terrorismo. rime informático não é só questão o de segurança pública, mas de defesa nacional.

3 A SEGURANÇA DOS USUÁRIOS À LUZ DA LGPD

Hoje temos uma imagem que há uma falsa impunidade para quem pratica crimes envolvendo tecnologia e redes sociais, o Brasil dispõe algumas normas e projetos de leis que tenham como objetivo prevenir, e ter uma punição mais severa em novos delitos, que tenha a proteção dos direitos fundamentais de liberdade e privacidade dos indivíduos, inibindo o uso desenfreado de informações pessoais em sites e plataformas, sendo cuidadosos e transparentes com os fluxos de dados.

Dispõem Soprana (2018)

> A lei estimula a transparência das empresas e organizações que lidam com os dados pessoais. Em seu teor obrigam-nas a estarem ‘‘aptas a comunicar sua responsabilidade sobre o ciclo de vida dos dados: coleta, tratamento, compartilhamento, armazenamento e descarte”

A Lei Geral de Proteção de Dados Pessoais (LGPD), LEI n°. 13.709/2018, acompanha um movimento internacional também gerado para a proteção de dados de cidadãos por todo o mundo, trabalhando para o controle sobre as empresas e organizações atuantes em ambientes virtuais que captam, armazenam e utilizam dados em excessos de seus clientes, sendo ele de forma online ou até mesmo off-line. Ela surgiu para estabelecer regras sobre as coletas de dados e os compartilhamento de seus usuários, após oito

anos de debates e redações o presidente Michel Temer sancionou em 2018, com o objetivo de preencher lacunas complementando o regulamento de uso de dados, para caso descumprimento havendo sansões e multas, assim vigorando em agosto de 2020.

Martins (2014, p. 270)

> No plano internacional, a título comparativo, existem regulamentos divergentes quanto ao momento de obtenção do consentimento, em relação o início do tratamento dos dados. Nos Estados Unidos a Direct Marketing Association (DMA) regulamentou o consentimento posterior – negative option, enquanto que na União Europeia o Conselho Europeu instituiu o consentimento prévio – positive option.

Foi escrita em base de sete fundamentos, delimitando a legalidade e a ilegalidade do que concerne a proteção, descritos os princípios legais da lei. De acordo com o artigo 2° da LGPD, dispõem:

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

É de grande interesse para os titulares destes dados, a clareza, exatidão e a transparência no meio virtual, ditando quais dados podem ser coletados e estando de acordo com a finalidade informada de cada um, e quais são as informações autorizadas tendo a ciência do que está compartilhando, sendo livre a retirada de qualquer dados do titular da base pessoal em posse de empresas de prestação de serviços e e-commerce.

Gonçalves (2017, p. 102).

> A necessidade de cautela na guarda e manuseio dos dados de registros dos usuários decorre porquanto ‘‘não é somente importante protegê-los formalmente, mas sim materialmente” e sem os ‘‘procedimentos de segurança não há segurança jurídica

No ensinar de Marcel Leonardi (2007, p. 52)

> Por outro lado, antes mesmo da publicação da LGPD, a doutrina já apontava que a responsabilidade civil do provedor de serviços de Internet deve partir do pressuposto de que existem deveres específicos a eles impostos.

Por tanto, o objetivo é a transparência e a garantia de privacidade que as empresas coletam de dados como (nome, RG, CPF, endereço e etc), tenha que estar limitada para atuar em seu mercado e prestação de serviço, prezando sua imagem ao público e respeitando as informações que as organizações mantêm como confidenciais juntamente ás legislações brasileiras.

A lei considerada primordial e a mais famosa é a Lei N°. 12.737/2012 e é uma alteração no Código Penal Brasileiro voltada para crimes virtuais, com isso o judiciário viu a necessidade de tipificar estes crimes. Esta lei ficou conhecida como um nome de uma atriz, chamando a de Lei Carolina Diekmann, quando em maio de 2011 um hacker invadiu seu computador pessoal e teve o acesso a 36 fotos íntimas da atriz.

> 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 03 (três) meses a 01 (um) ano, e multa.

Tavares diz (2013, p. 40).

> O que se percebe neste artigo acima citado é a tutela da privacidade e da intimidade, bens tão valiosos ao ser humano, como também a proteção de dados particulares do proprietário deste dispositivo. Cabe lembrar que na respectiva lei, “prevê que o dono de seus próprios dados deva colocar meios ou medidas que impeçam ou dificultem a invasão desses dados, gerando assim a sua proteção, para que assim, demonstre que esses arquivos não sejam de conhecimento público.

Considerada um marco inicial para a proteção dos dados pessoais dos usuários, com a repercussão chegou em todo o país, ao Congresso Nacional para a criação desta lei assinada pelo a presidente Dilma Rousseff, mas tem a necessidade de que evolua ainda mais as normas sobre o assunto.

Wendt e Jorge (2013. P.54).

> A quantidade de policiais capacitados e treinados na investigação de crimes virtuais ainda é escassa, e isso passa a tornar-se problemático, ao passo que dificulta a persecução penal dos responsáveis e, inevitavelmente, resulta na impunidade.

> Além da lei anterior, pode mencionar a Lei nº 12.965/2014 que instituiu o Marco Civil da Internet. Assim como a lei supracitada mencionada, essa também veio em decorrência do aumento de ataques a websites oficiais do governo, de empresas públicas e de contas privadas. Devido a esta situação, buscou-se por meio do Marco Civil da Internet a tutela da informação. Assim, no texto da presente norma encontra-se as garantias individuais dos internautas e os direitos e deveres para o uso da internet no Brasil. (BRASIL, 2014).

A legislação brasileira a chamou de Constituição da Internet, com um grande avanço da norma quando se trata de crimes em ambiente virtual, estabelecendo princípios, garantias, direitos e deveres para quem usa a internet, assinada pela a presidente Dilma Rousseff em 11 de maio de 2016.

De acordo com Augusto Marcacini (2016, p. 31):

> A Lei de fato encontrou e regulou alguns fatos sociais que são fruto exclusivo da Internet – como é o caso das disposições que estabelecem a neutralidade da rede ou a responsabilidade dos provedores de Internet – mas resvalou também, e pretendeu regular, situações jurídicas que não são uma exclusividade do ciberespaço – como a privacidade, a proteção a dados pessoais ou a liberdade de expressão – embora essas possam encontrar na rede uma larga amplitude de casos concretos e, consequentemente, obter maior visibilidade midiática quando ligadas a fatos ocorridos online. Mas é difícil restringir tais situações apenas ao universo da Internet, no que o Marco Civil deixa uma sensação de incompletude, ou de um encaixe imperfeito, no trato dessas matérias.

Segundo Otoboni cita em artigo no site Jus brasil (2019)

> Este decreto prescreveu que tivesse procedimentos para armazenar e proteger os dados dos usuários da rede, elencando também que as garantias da transparência quando houvesse requisição por parte da Administração Pública para conferir dados cadastrais dos respectivos usuários fossem assegurados de forma segura.

Para o Direito do Consumidor, o ato de uma simples navegação não configura relação de consumo com o provedor das aplicações de internet para os seus usuários. Porém sendo específico o Código Civil do Consumidor trata dos arquivos de consumidores em seu art. 43 do CPC.

Benjamin (1998, p. 329) ensina que:

> De plano, é necessário esclarecer que referidas disposições da legislação consumerista abordam de forma ampla o manejo de “arquivos de consumo”,

> efetivamente, um gênero, do qual se afiguram as espécies (i) banco de dados; e (ii) cadastro de consumidores;

Leonardi (2004, p. 27) diz que:

> A Internet se constitui num meio de comunicação, o qual serve para veiculação de informações e de manifestação de vontades. Nesse sentido, para o Direito do Consumidor, o ato de simples navegação na Internet não configura relação de consumo entre o provedor de aplicações de Internet e o usuário, o qual possui liberdade para escolher qual conteúdo acessar.

Na prática há uma grande dificuldade de se obter provas no mundo virtual com a instabilidade, de um crime ser facilmente apagado, alterada ou perdida, colocando as investigação policial em um enorme desafio de um crime sem fronteiras, com um esforço ao acesso dos vestígios na análise criminal, devido a diferença de crimes comuns no mundo real, onde as evidências das ações de um criminoso é mais difícil de exterminar por completo.

Discorre Corrêa (2008, p. 74):

> O grande problema relacionado aos “crimes” digitais é a quase ausência de evidências que provem contra o autor, a inexistência da arma no local do crime. Uma gloriosa invasão a sistema alheio não deixaria nenhum vestígio, arquivos seriam alterados e copiados, e nenhum dano seria prontamente identificado. Um crime perfeito, sem traços, e, portanto, sem evidências. Justamente por essa qualidade da perfeição há a dificuldade em presumir o provável número desses “crimes”.

Em virtude disto, é necessário provedores de aplicação que visem seus websites, para a adequação dos termos de uso, com contratos de adesão adequados e privativos, atendendo a LGPD e o Código Civil do Consumidor, na prática sendo feita de forma efetiva e segura para as informações compartilhadas dos internautas e cidadãos consumidores.

CONCLUSÃO

O presente trabalho procurou abordar a evolução da Internet apresentando desde o momento de sua criação e passando por momentos históricos e de grande relevância para o crescimento e a sua evolução na vida de seus usuários.

Além desta abordagem no trabalho realizando estudo das principais ameaças, cada vez mais as medidas que aumentam o número de pessoas que utilizam desta ferramenta, deixa claro a necessidade de conhecimento dos usuários em meio virtual, para que crimes cometidos virtualmente não evolua com tanta rapidez.

Analisando crimes mais praticados pelos meios informáticos, sendo ele em computadores, celulares ou qualquer outro dispositivo, abordando suas formas de tipificação bem como as classificações publicadas por doutrinadores sobre os métodos investigativos e sobre espécies de crimes.

Jovens e adultos, por inocência, excesso de confiança em outras pessoas e sites, ou até mesmo por necessidade, utilizam estas ferramentas para trocar imagens, documentos, vídeos de caráter íntimo ou sexual, criando a possibilidade do criminoso executar seu delito, com ameaças ou adentrar em documentos que o levam a ter lucros de forma ilegal.

Crimes diversos, com diferentes meios de investigação e principais meios de produção de provas, tratando de maneiras que impossibilita a eficácia e a facilidade para chegar até o autores de crimes virtuais, apresentando especial relevância neste contexto o conteúdo fático de um crime informático.

Assim, há muitas discussões sobre o que pode ser feito para o controle do uso da internet e empresas e-commerce no Brasil. Houve casos em que o Poder Judiciário chegou a retirar sites e contas, depois de visitantes se sentiram ofendidos com vídeos publicados.

Se tratando de uma ramo do direito ainda muito novo em relação a outros, analisando a realidade a partir de uma abordagem crítica sobre os fatos para o caso concreto e das maiores soluções efetivas no direito digital ainda carece de muitos estudos que visam trazer informações para os usuários, em relação a Direito, em especial do Direito Penal com o ambiente Virtual.

Por tanto, com o tempo foram criadas Leis n° 12.737/12 e 12.965/14, como para o objetivo de diminuir os delitos em âmbito virtual, buscando um meio de punir os delituosos. Fazendo em decorrer do texto, é necessário da certificação de novas leis mais justas para a punição desses infratores, com penas mais severas, que de a sensação de punição para a população, que realmente precisa ser ensinada e orientada a como agir em relação a tecnologia e as redes sociais.

PROTECTION OF DATA EXPOSED ON THE INTERNET

REFERÊNCIAS

ARTIGO19. Proteção de dados pessoais no Brasil: ANÁLISE DOS PROJETOS DE LEI EM TRAMITAÇÃO NO CONGRESSO NACIONAL. 2017. Disponível em: . Acesso em 01 Abril de 2022.

BARRETO, Erick Teixeira. Crimes Cibernéticos sob a égide da Lei 12.737/2012. Disponível em: . https://ambitojuridico.com.br/edicoes/revista-159/crimes-ciberneticos-sob-a-egide-da-lei-12-737-2012/#:~:text=A%20Lei%20Federal%20n%C2%B0,pela%20falta%20de%20comina%C3%A7%C3%A3o%20legal.. Acesso em 01 Abril de 2022.

BEZERRA, Arthur Coelho. Privacidade em perspectivas: Os Reflexos do Grande Irmão no Admirável Espelho Novo de Black Mirror. Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

Compugraf -https://www.compugraf.com.br/tudo-sobre-a-lei-geral-de-protecao-de-dados-lgpd/. Aceso em 01 Abril de 2022.

CONTEÚDO JURÍDICO: https://conteudojuridico.com.br/consulta/Artigos/55631/crimes-cibernticos-exposio-ntima-sem-o-consentimento-da-vtima-na-internet. Acesso em 02 Abril de 2022.

CONTEÚDO JURÍDICO https://conteudojuridico.com.br/open-pdf/phpKRSh7A.pdf/consult/phpKRSh7A.pdf. Acesso em 25 mar. de 2022.

CORRÊA, Gustavo Testa. Aspectos Jurídicos da Internet. 4 ed. São Paulo, Saraiva, 2008.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

ESTABELECE PRINCÍPIOS, GARANTIAS, DIREITOS E DEVERES PARA O USO DA INTERNET NO BRASIL.. Marco Civil da Internet. Brasília, Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm>. Acesso em: 17 out. 2016.. Acesso em 25 mar. de 2022.

Filho, W. Teoria dos Círculos Concêntricos na Esfera da Vida Privada MAGISTRADO TRABALHISTA, 2016. Disponível em: <http://www.magistradotrabalhista.com.br/2016/03/teoria-dos-circulos-concentricos-da.html>. Acesso em: 10 set. 2021

https://jus.com.br/artigos/29634/crimes-informaticos

https://www.techtudo.com.br/noticias/2018/10/o-que-sao-cookies-entenda-os-dados-que-os-sites-guardam-sobre-voce.ghtml - site sobre Cooks. Acesso em 25 mar. de 2022.

LEI A PROTEÇÃO DE DADOS: https://www.pontotel.com.br/lei-protecao-de-dados-pessoais/. Acesso em 25 Jan. de 2022.

MONOGRAFIA BRASIL ESCOLA: https://monografias.brasilescola.uol.com.br/computacao/a-importancia-privacidade-na-internet.htm. Acesso em 25 Fev. de 2022.

OTOBONI, Gustavo Henrique dos Santos. Crimes Cibernéticos: Phishing. 2019. Disponível em: < https://ambitojuridico.com.br/edicoes/revista-191/crimesciberneticos-phishing/> Acesso em 25 Jan. de 2022.

PECK, Patrícia. Direito digital. São Paulo: Saraiva, 2002.

RECUERO, Raquel. Redes Sociais na Internet. Porto Alegre: Editora Sulina, 2009.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Crimes cibernéticos: ameaças e procedimentos de investigação. 2ª. ed. Rio de Janeiro: Brasport, 2013.