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

LEI GERAL DE PROTEÇÃO DE DADOS

RESPONSABILIDADES CIVEIS E CRIMINAIS

ORIENTANDO(A): Felipe Vasconcelos Carvalho

ORIENTADORA: Profª. MS. Ysabel del Carmen Barba Balmaceda

GOIÂNIA

2022

FELIPE VASCONCELOS CARVALHO

LEI GERAL DE PROTEÇÃO DE DADOS

RESPONSABILIDADES CIVEIS E CRIMINAIS

Artigo Científico apresentado à disciplina Trabalho de Curso I da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).

Profª. Orientadora: Ms. Ysabel del Carmen Barba Balmaceda

GOIÂNIA

2022

FELIPE VASCONCELOS CARVALHO

LEI GERAL DE PROTEÇÃO DE DADOS

RESPONSABILIDADES CIVEIS E CRIMINAIS

Data da Defesa: 25 de maio de 2022

BANCA EXAMINADORA

_____

Orientadora: Profª. Ms. Ysabel del Carmen Barba Balmaceda nota

_____

Examinador Convidado: Gabriela Pugliesi Calaça nota

Primeiramente agradeço a meus familiares, principalmente meus pais, por todo apoio e amparo que me deram ao longo de toda minha jornada universitária. Agradeço também a Deus, por toda ajuda nos momentos em que mais precisei. E por fim e não menos importante agradeço a Professora Ysabel del Carmen, por todos os ensinamentos transmitidos e por sua dedicação.

RESUMO

O presente estudo pretende examinar sobre a criação da internet, e como essa nos últimos anos tem se tornado um dos instrumentos mais utilizados por todas as pessoas do mundo. Outro ponto a ser debatido no trabalho são os crimes e prejuízos que estes podem causar aos usuários, que utilizam deste meio de comunicação. Enfim, será abordado o porquê da importância da criação da Lei Geral de Proteção de Dados, e quais são as responsabilidades criadas e impostas por esta lei. Como foco de análise, optou pela alusão histórica observando a criação da internet, dados estatísticos expondo números de usuários na internet e quais são os meios mais comuns de acesso a internet. Por fim será tratada sobre a Lei de Proteção de dados, tratando questões como por que foi necessária, quais são os objetivos da mesma, quais as responsabilidades que a mesma criou, e quais foram os resultados que a mesma já obteve após sua criação

Palavras-chaves: Lei de Proteção de Dados, internet, usuários.

LEI DE PROTEÇÃO DE DADOS
RESPONSABILIDADES CÍVEIS E CRIMINAIS

Felipe Vasconcelos Carvalho

INTRODUÇÃO

A escolha do tema se deu graças a importância de se ter uma lei como a Lei Geral de Proteção de Dados, em uma era onde a tecnologia é indispensável na vida de grande maioria das pessoas. Em uma era onde o número de dados colocados na rede de internet cresce proporcionalmente a quantidade de usuários que utilizam deste benefício. Sendo esta citada acima um marco de suma importância para as pessoas que se utilizam da internet.

O trabalho foi elaborado a partir de três seções. A primeira seção aborda sobre o surgimento da internet, e como ocorreu o advento da mesma. Sendo que essa antes era utilizada apenas por algumas pessoas em todo o mundo, e só se podia trocar alguns e-mails, e atualmente é utilizada por aproximadamente 4,7 bilhões de pessoas em todo o mundo.

Já a segunda seção aborda a respeito dos crimes que geralmente ocorrem na internet, abordando principalmente a respeito da forma que esses atos são cometidos, os danos que podem ser causados as vítimas, e por fim a respeito de como ocorre a investigação e a coleta de provas de um crime cibernético.

Na terceira e última seção deste artigo, é abordado sobre a Lei Geral de Proteção de Dados. Sendo exposto o porquê a mesma se fez necessária, sobre as responsabilidades cíveis e criminais criadas com o advento desta lei, e os resultados que esta tem proporcionado.

A metodologia utilizada para o desenvolvimento deste artigo foi o método dedutivo e pesquisa teórica, sempre nos limites dos objetivos propostos.

1 – COMO A INTERNET SURGIU E COMO OCORREU O ADVENTO DA MESMA

Será abordado nesta seção os aspectos históricos da internet, e os fatores sociais que fizeram com que houvesse o advento da mesma. Advento este que culminou na necessidade de se criar uma legislação específica para o assunto, uma vez que com o advento problemas como os crimes cibernéticos surgiram, mas este será um assunto que será tratado nos próximos capítulos deste artigo.

1.1– COMO OCORREU O SURGIMENTO DA INTERNET

A rede mundial de computadores surge no ano de 1958, em meio a Guerra Fria protagonizada por Estados Unidos e União Soviética, segundo o site RockContent (2020, p. 1), em uma tentativa dos americanos de proteger informações e seus meios de comunicações em caso de um ataque nuclear por parte dos nazistas. A primeira nomenclatura que recebeu foi DARPA (Defense Advanced Research Projects Agency, ou Agência de Projetos de Pesquisa Avançada de Defesa, em português).

Após a criação da DARPA, muitas pesquisas se iniciaram com o fim de aprimorar cada vez mais este dispositivo, e em 1965 ocorreu um grande avanço na internet mundial, Thomas Merrill que estava na California, e Lawrence G. Roberts que estava em Massachusetts conseguiram conectar um computador TX2 a um Q-32, por meio de uma linha telefônica. Este acontecimento é um grande marco da internet mundial, pois foi a primeira conexão de longa distância já registrada.

As tentativas de aprimoramento não pararam, e em 1966 Lawrence juntamente com mais 2 cientistas, Howard Frank e Robert Kahn, criaram um plano denominado ARPANET, que tinha como objetivo a criação da primeira rede de comutação de pacotes. Este plano obteve êxito 3 anos depois, quando um computador da Universidade da Califórnia (UCLA) conseguiu se conectar com grande estabilidade a outro do Stanford Research Institute (SRI). Meses depois deste incrível feito quatro faculdades americanas já se encontravam interconectadas por meio do que ficou conhecido como ARPANET. RockContent (2020, p. 1).

No ano seguinte o ARPANET já era um sucesso e já estava em centenas de computadores. Ainda no ano seguinte uma equipe de Network Working desenvolveu um comando nos computadores que permitia a criação de softwares e aplicativos através do ARPANET. Foi então que em 1972 Ray Tomlinson criou um software de e-mail. O uso do aplicativo criado por Ray foi tão impactante que este foi o aplicativo mais importante da década, e mudou a forma de colaboração e comunicação entre as pessoas. Então o uso ARPANET, que antes era de uso majoritário para fins militares, começou gradativamente a ser utilizado por pessoas normais, como um novo meio de comunicação, sendo utilizado principalmente pelas faculdades).

No Brasil, a chegada da internet se deu de fato em outubro de 1988, quando o Laboratório Nacional de Computação Científica, localizado no Rio de Janeiro, se conectou a um computador da Universidade de Maryland, nos Estados Unidos, a conexão se deu por meio de um sistema chamada Bitnet, as únicas ações eram trocar e-mails e compartilhar arquivos. A conexão era individual, por linha telefônica, e não era necessário que houvesse discagem. As empresas pagavam taxas para a Empresa Brasileira de Telecomunicações, a EMBRATEL. Daniela Diana (2019, p. 1):

> No Brasil, a Internet surgiu no final da década de 80, quando as universidades brasileiras começam a compartilhar algumas informações com os Estados Unidos. Entretanto, foi a partir de 1989, quando se fundou a Rede Nacional de Ensino e Pesquisa (RNP), que o projeto de divulgação e acesso ganhou força. O intuito principal era difundir a tecnologia da Internet pelo Brasil e facilitar a troca de informações e pesquisas.

As evoluções não pararam tendo várias outras mudanças, até que em 1989 Tim Berners-Lee criou a World Wide Web, ou como é popularmente conhecida a WWW. Este sistema facilitaria a busca por documentos na internet, já que o mesmo funciona como um mecanismo de distribuição de documentos de hipertexto interconectados e acessíveis por meio de um navegador web conectado à Internet.

Por sua vez, comenta Paulo Alves (2019, p. 1):

> A World Wide Web (WWW), foi criada por Tim Berners-Lee em 12 de março de 1989. Naquela data, o engenheiro britânico criava o método

> pelo qual seria possível obter acesso público à Internet, tecnologia que havia sido desenvolvida nos anos de 1960 por militares dos EUA.

Em abril de 1989, mesmo que o número de pessoas com acesso a internet no Brasil ainda fosse muito pequeno, é criado o domínio .BR, que era pra designar os sites brasileiros e para conta de brasileiros. Outros domínios surgem em 1991 como o .GOV, o .COM.BR, e o .ORG, porém no ano em questão o grande feito foi a primeira conexão do Brasil com a internet, que ocorreu na Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), quando trocaram pacotes com a rede mundial de computadores.

1.2 – COMO SE INICIOU E POR QUE SE INTESIFICOU TANTO

Após a criação do WWW, a criação do Google foi uma das mais importantes. Criado em 1997 o Google foi e é até hoje uma das maiores plataformas de busca da internet. Esta plataforma revolucionou a internet na época, uma vez que atingia um grande público e possuía um sistema amigável e de fácil acesso. Atualmente o Google possui mais de 1 bilhão de páginas indexadas, e fornece ao usuário uma certa facilidade no acesso de seus dados, graças aos algoritmos.

A chegada das redes sociais, como o Facebook, Instagram, WhatsApp, Twitter e Youtube, além dos que não estão mais em operação como o Orkut e o MSN, foi um dos maiores, se não o maior, acontecimentos da internet. Essas redes sociais foram e ainda são uma febre entre seus usuários, muito disso se deve ao serviço que é ofertado pela grande maioria, serviços como acesso a informações em tempo real, e como um meio de comunicação em tempo real, são ofertados gratuitamente em praticamente todas as redes citadas acima.

No Brasil a internet chega em oito de dez domicílios, segundo dados do Instituto Brasileiro de Geografia e Estatística (IBGE), site do Governo Federal Brasileiro (2021, p.1), em 2019 cerca de 82,7% dos domicílios brasileiros possuíam internet, quando se leva em consideração apenas os domicílios localizados nas áreas urbanas este número cresce ainda mais, chegando a

86,7%. Sendo as pessoas entre 14 e 39 anos os maiores usuários deste advento tecnológico.

Outro dado importante para se levar em conta, é por onde as pessoas acessam a internet, segundo dados fornecidos pelo IBGE em 2019, cerca de 98,6% utilizavam o celular para acessar a internet, enquanto 46,2% utilizavam computadores, 31,9% televisões e 10,9% tablets, para acessar a internet.

Em um cenário mundial o percentual é um pouco mais baixo, porém o número ainda sim é muito grande, segundo pesquisas dados disponíveis no site Statista, VIEIRA, Douglas (2021, p.1), no primeiro semestre de 2020 aproximadamente 4,66 bilhões de usuários estavam ativos nas redes.

Estes dados são de suma importância para transparecer o quão importante e utilizada a internet é nos dias hodiernos. Como já foi exposto anteriormente a internet possui inúmeros pontos positivos, que ajudam milhares de pessoas ao redor do mundo todo os dias, com seus mais variados serviços disponíveis.

1.3 – INTERNET UM LUGAR PERIGOSO

Porém por outro lado, a internet também deve ser considerada um lugar perigoso, onde deve se agir com uma certa cautela, para que não se tenha dados e/ou informações roubadas/vazadas. Os chamados crimes cibernéticos são aqueles praticados via computadores ou dispositivos eletrônicos conectados a internet, e que vão desde bullying digital à até mesmo a furtos e fraudes.

GARRET, Filipe (2021, p. 1) define crimes cibernéticos como:

> Crimes cibernéticos são aqueles que utilizam computadores, redes de computadores ou dispositivos eletrônicos conectados para praticar ações criminosas, que geram danos a indivíduos ou patrimônios, por meio de extorsão de recursos financeiros, estresse emocional ou danos à reputação de vítimas expostas na Internet.
> A classificação é ampla e compreende desde ações relacionadas a bullying digital e ataques à reputação em redes sociais até crimes que usam malwares para, por meio de engenharia social ou vulnerabilidades técnicas, provocar danos ou prejuízos financeiros.

Por sua vez, DOS SANTOS, Douglas Ribeiro (2021, p. 1): “São exemplos de crimes cibernéticos: a fraude, o furto e o estelionato quando praticados digitalmente, ou seja, mediante utilização de smartphones, notebooks, tablets etc.”

Os três principais perigos da internet são os softwares maliciosos, popularmente conhecidos como vírus, os spams e as páginas falsas. Estes que são praticados através do uso de malwares, ou seja, praticados por softwares utilizados para interceptar informações, danificar sistemas, ou até mesmo para causar prejuízos financeiros.

Os softwares maliciosos, agem como um vírus biológico, por isso o nome vírus, uma vez que quando infectam o sistema operacional, começam a se multiplicar com a intenção de se espalhar para outros computadores. Eles podem chegar nos computadores de várias formas, como por um pen drive infectado, pelo download de músicas, filmes e jogos em páginas que não são seguras, ou até mesmo pela abertura de um anexo infectado

Por sua vez, os spams nada mais são do que e-mails que não são solicitados pelo usuário e chegam até sua conta. Em muitos casos os spams são enviados à uma grande quantidade de destinatários aleatórios, com mensagens falsas que tentam persuadir o usuário, para conseguir informações pessoas, ou até mesmo dados bancários.

As páginas falsas na maioria das vezes, possuem o mesmo objetivo dos spams, a única diferença é que elas possuem uma plataforma semelhante ou até mesmo igual a de grandes plataformas conhecidas como sites de notícias ou de bancos, e sempre tentam persuadir o usuário, fazendo com que este disponibilize dados bancários, informações pessoais, ou qualquer tipo de informação que tenha algum valor.

GARRET, Filipe (2021, p. 1) sobre os crimes cibernéticos:

> Crimes cibernéticos podem assumir várias formas, mas há dois tipos mais praticados: crimes que visam ao ataque a computadores — seja para obtenção de dados, extorsão das vítimas ou causar prejuízos a terceiros — ou crimes que usam computadores para realizar outras atividades ilegais — nesses casos, dispositivos e redes servem como ferramentas para o criminoso

2 – CRIMES NA INTERNET

Já nesta seção serão abordados sobre os crimes cibernéticos, estes que por sua vez têm aumentado de forma surpreendente que nos últimos anos. No Brasil, em 2020, o número de denúncias contra esses crimes mais que dobrou se comparado ao número de denúncias que ocorreram no ano de 2019, dados estes que foram disponibilizados pela Central Nacional de Denúncias de Crimes Cibernéticos, com base nas notificações que os mesmos receberam.

2.1 – COMO OCORREM

Praticamente todos os crimes que ocorrem na internet, ocorrem por meio de *Malwares,* que nada mais são do que softwares maliciosos, que adentram nos computadores por meio de redes, e tem como objetivo muitas das vezes danificar dados dos usuários, ou até mesmo furtar dados e/ou dinheiro dos usuários.

Esses softwares ilícitos são classificados pelo objetivo que cada um possui, Tulio Lima Vianna (2001, págs. 53-58) em sua tese de mestrado, classificou os *Malwares* em: Cracker de Sistema, que são aqueles que invadem outros computadores através da rede; Cracker de Programas, estes por sua vez violam proteções dos *softwares* legais, e utilizam-se dos mesmos como se fossem cópias autenticas; Phreakers são os que causam danos a rede de telefonia; os Vírus que são os utilizados para causar certo prejuízo e/ou dano a outrem; os Piratas de Programas, estes que por sua vez copiam programas, não respeitando os direitos autorais do verdadeiro criador; e por último e não menos importante, os Distribuidores de Warez, estes que utilizam de redes para disponibilizar software, que são pagos de forma gratuita, sem autorização dos criadores e/ou detentores dos direito autorais de tal programa.

Os *malwares* podem infectar os dispositivos de diferentes modos, segundo o site de suporte da Microsoft (2022, p. 1), que é uma das maiores empresas no ramo da tecnologia atualmente, responsável pela criação e desenvolvimento dos principais softwares do mundo, os meios mais comuns de um software malicioso invadir um computador são: E-mails de spam; Macros

Office mal-intencionados; Unidades removíveis infectadas; Junto com outros softwares; e em páginas da web comprometidas ou que foram invadidas.

O mais comum dessas maneiras são os e-mails que contêm spans, segundo a empresa norte americana Mashable cerca de 145 bilhões de e-mails são enviados em todo mundo por dia, e desse total cerca de 65% destes contêm spans.

Para se ter noção da dimensão desses números, pode-se utilizar como base a pesquisa realizada pelo Yahoo, em 2020, onde observa-se que esse meio de comunicação conta com mais de 4 bilhões de usuários, e que os trabalhadores recebem em média cerca de 120 e-mails por dia. E ainda tomando como base essa pesquisa feita pelo Yahoo, existe um prognóstico que o número de mensagens enviadas por este meio de comunicação tão famoso, chegue a incrível marca de 347 bilhões de mensagens enviadas por dia no ano de 2023.

O site de suporte da Microsoft (2022, p. 1) alerta sobre essas mensagens, e diz que:

> Os autores de malware geralmente tentam enganar você para baixar arquivos mal-intencionados. Pode ser um e-mail com um arquivo anexado que diz ser a nota fiscal de uma entrega, um reembolso de taxa ou o boleto de um ingresso. Talvez a mensagem diga que você precisa abrir o anexo para receber dinheiro ou para que os itens sejam entregues a você.

Observando-se estes números, é importante abordar a respeito dos danos que podem ser causados caso um dispositivo seja afetado por estes softwares que possuem más intenções.

2.2 – QUAIS SÃO OS DANOS QUE PODEM SER CAUSADOS

A maioria das pessoas que utilizam o sistema mundial de computadores com algum fim, se não todas as pessoas, estão sujeitas a pelo menos algum tipo de problema. Seja esse problema mais simples como por exemplo a falha no funcionamento de um aplicativo por conta de algum malware, seja um problema mais grave como um vazamento de dados confidenciais, ou até mesmo um ataque a uma conta bancária.

O site Kaspersky (2021, p. 1) em um artigo publicado no ano de 2020 separa os malwares em dois tipos, os que são para usuários de redes

domésticas, e os que são para uma rede corporativa. E ainda expões os danos que ambos esses “dispositivos” podem causar para os usuários:

> - **Para usuários domésticos**, uma infecção pode envolver a perda de informações não tão importantes, que podem ser facilmente substituídas, ou resultar na perda de informações que permitem ao criminoso virtual acessar a conta bancária do usuário
> - **Em uma rede corporativa**, um cavalo de Troia que envia spam pode aumentar um pouco o tráfego das comunicações, enquanto outros tipos de infecções podem resultar na parada total da rede corporativa ou na perda de dados críticos para os negócios.

Segundo um artigo publicado por Leonardo Gurjao Margotti (2020, p. 1), graduado em Ciências da Computação na Universidade do Sul de Santa Catarina em 2005, no blog Backup Dados, em 2020, grandes empresas já tiveram problemas com suas plataformas virtuais por conta de ataques cibernéticos. Empresas como Yahoo, Uber, Facebook, e até mesmo bancos como foi o que aconteceu com o banco digital popularmente conhecido como Banco Inter, foram alvos desse tipo de ataque que comprometeu tanto o funcionamento, como também dados de milhões de usuários.

Neste mesmo artigo, o autor dá uma breve explicação de como ocorreu o ataque a um dos aplicativos de transporte mais conhecidos em nível mundial, se não o mais, que existe atualmente, o Uber. Leonardo Margotti (2020, p. 1) pontua que:

> ... em 2016, a Uber, uma das principais empresas de transporte de pessoas, teve a sua segurança invadida por hackers. Segundo dados divulgados na imprensa, 57 milhões de pessoas, entre usuários e motoristas, tiveram seus dados vazados. Apesar de toda a ação ter ocorrido no ano de 2016, as informações saíram na mídia apenas em 2017. A Uber tentou esconder a invasão das autoridades e ofereceu US$100 mil aos hackers para que eles apagassem as informações que haviam roubado. No entanto, foi exatamente o contrário que aconteceu. No ano de 2018, o aplicativo entrou em um acordo judicial que custou US$148 milhões aos seus cofres, o maior pagamento de indenização da história.

Nem mesmo as prefeituras municipais estão protegidas, segunda notícia divulgada no site do G1, no dia 22 de dezembro de 2021, as contas bancárias da prefeitura de Euclides da Cunha Paulista, no estado de São Paulo, na madrugada do dia 21 de dezembro de 2021 foram alvo de um grupo de

hackers, os quais conseguiram desviar mais de meio milhões de reais dos cofres públicos. Ataque este que até o presente momento não foi resolvido.

O vazamento de dados, ou até mesmo o roubo dos mesmos, também é muito comum no mundo virtual. Em um artigo publicado por Alessandra Montini, mestre em estatística pela USP-IME, e doutora pela FEA-USP, pode-se observar o quão recorrente é o problema com vazamento de dados, no artigo a mesma cita um vazamento ocorrido no mês de janeiro, que expôs na internet o Cadastro de Pessoa Física (CPF) de mais de 223 milhões de brasileiros, e outro ocorrido no início de fevereiro o qual disponibilizou na rede a conta telefônica de mais de 100 milhões de cidadãos brasileiros, divulgando até mesmo o número de telefone do presidente Jair Bolsonaro.

MONTINI, Alessandra (2021, p.1) pontua que:

> Pode ser que os meus ou os seus dados também estejam em meio a esses vazamentos, o que mostra o quanto esse assunto é sensível e merece cuidado especial tanto de nós, que deixamos rastros pela internet, além de disponibilizarmos uma série informações quando fazemos uma compra ou cadastro, e das empresas que são as que guardam todos esses dados. Mas os casos ocorridos evidenciam o quanto não estamos preparados para lidar com o número de informações que temos disponível e o quanto as empresas também não se adequaram para respeitar a LGPD (Lei Geral de Proteção de Dados), que já está em vigor e nem deu a importância necessária ao profissional Data Protection Officer (DPO), uma espécie de xerife de dados, que está previsto na lei.

Segundo artigo publicado pela Associação do Ministério Público de Minas Gerais (2012, p. 1), cerca de 54 crimes cibernéticos são cometidos por minuto no Brasil. Graças a esse grande aumento no número de casos de ataques cibernéticos, e a falta de cuidado que muitos bancos de dados possuem com dados dos usuários, fez se necessário a revisão da legislação, bem como a criação da Lei Geral de Proteção de Dados, lei esta que será mais bem desenvolvida na próxima seção.

2.3 – INVESTIGAÇÃO E OBTENÇÃO DE PROVAS DE CRIMES CIBERNÉTICOS

Faz se necessário debater a respeito deste tema, pois investigar crimes cibernéticos para muitos é de uma complexidade muito grande. Na grande maioria das vezes os criminosos possuem um vasto conhecimento em tecnologia, fazendo com que seja de extrema dificuldade a descoberta. Em

muitas das vezes os infratores agem com o endereço IP de seus computadores alterados, ou até mesmo camuflam seus IPS, fazendo com que os mesmos não possam ser encontrados. TEIXEIRA, Ronaldo (2013, p.43) define endereço de IP como: “O endereço IP, também conhecido como endereço lógico, é um sistema de identificação universal onde cada computador possa ser identificado exclusivamente, independente da rede em que esteja operando”.

Um outro fator que dificulta bastante as investigações, e que grande parte destes crimes são cometidos na *Deep Web*, acerca dessa internet Garret, Felipe (2019, p 1) disserta que:

> Deep Web (Internet Profunda, em tradução livre) é uma área da Internet que fica “escondida” e tem pouca regulamentação. O termo ficou mais conhecido no Brasil depois do massacre de Suzano, em que dois jovens invadiram uma escola, mataram oito pessoas e depois se suicidaram. A polícia vê indícios de que os assassinos tenham recebido apoio do Dogolachan, fórum criado em 2013 e que não requer login para participar.

Como já foi discutido anteriormente, o acesso a dados para a investigação de crimes que ocorre na “Internet Profunda” é algo de uma exorbitante dificuldade na maioria das vezes, e é justamente por esta certa segurança para praticarem crimes, que nesta rede vários crimes são cometidos. Segundo Artigo Científico publicado por OLIVEIRA, William e FERNANDO, Caio, é possível encontrar nessa rede crimes como: pornografia infantil, tráfico de drogas, fraudes virtuais, tráfico de armas, e é possível também encontrar-se assassinos de aluguel.

O site Olhar Digital (2016, p. 1) publicou um artigo onde pode se observar sete maneiras de identificar um criminoso na *Deep Web,* o site elencou da seguinte maneira:

> **Agentes infiltrados** - Essa tática é simples: investigadores se passam por vendedores de produtos ilegais, identificando compradores em potencial. Há um endereço de entrega registrado para os produtos, o que facilita o trabalho da polícia. Em operações do tipo, foram presos compradores de veneno, armas e pedófilos do mundo todo.
>
> **Hack** - Uma maneira de burlar o Tor é atacar os computadores dos usuários. Isso foi o que o FBI fez com um grande site de pornografia infantil da deep web. A agência implantou um malware que enviava o IP verdadeiro de usuários que clicassem em fóruns relacionados à pornografia infantil. Depois de possuir o endereço IP, a polícia intima o provedor ou o centro de dados responsável por ele para conseguir informações sobre o cliente.

> **Rastros na internet** - Especialistas afirmam que há “migalhas” digitais na internet comum que podem levar a criminosos na deep web. São postagens em fóruns, por exemplo, que conduzem a um suspeito. (...)
> **Vigilância em larga escala** - Em alguns países há o monitoramento de informações em massa para encontrar criminosos. Esse tipo de dados geralmente não é contestado.
> **Mercadorias apreendidas** - A prisão de traficantes ou a apreensão de mercadorias pode gerar pistas que levem a consumidores. Em alguns casos, a polícia encontrou junto com traficantes algumas listas com todos os pedidos de clientes e dados de contato.
> **Rastreamento de moedas virtuais** - Transações na deep web costumam usar a bitcoin para garantir o anonimato dos envolvidos no processo, mas isso pode acabar em breve. A Agência de Investigações em Segurança Interna dos Estados Unidos (HSI) criou uma força-tarefa para rastrear a lavagem de bitcoins e outras moedas virtuais.
> **Correios** - O tráfico de drogas da deep web ainda precisa de um serviço de entregas, como os correios. Além de terem que embalar os produtos de maneira que eles não sejam descobertos, remetentes e destinatários correm o risco de serem descobertos e, consequentemente, presos. Nesses casos, a polícia pode criar uma “entrega falsa”, apreendendo o suspeito em flagrante.

Por outro lado, na internet comum, a qual as pessoas estão mais habituadas a utilizar, a descoberta de um crime é um processo também complexo, porém a descoberta pode ser um pouco mais fácil. Tal fato se dá, haja vista que a internet faz parte de uma grande estrutura controlado por agências provedoras. Agências estas que absorvem as informações de todas as ações de seus usuários, desde uma postagem em uma rede social, até as informações bancárias que um usuário utilizou para fazer uma compra na internet.

TEIXEIRA, Fernanda e COSTA, Priscila (20, p.63) apontam que:

> São essas informações que em geral permitem, de forma precisa, desvendar um crime cibernético ou obter uma prova digital para elucidar um crime real. O que tem aturdido o mundo jurídico é a obtenção dessas informações, desses dados que consubstanciam a prova digital. As empresas provedoras de Internet, englobando todos os tipos envolvidos nessa atividade, passaram a ser assoberbadas de pedidos de informações sobre os dados, recebendo solicitações e ordens de toda parte do mundo.

3 – LEI GERAL DE PROTEÇÃO DE DADOS

O artigo 1º da Lei nº 13.709, 14 de agosto de 2018, tem como objeto a Lei Geral de Proteção de Dados, ou simplesmente LGPD, e nele diz que:

> 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.

> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

No decorrer deste tópico esta lei será debatida com mais detalhes acerca do porquê foi criada, quais as principais mudanças ela causou, quais direitos e deveres a mesma criou aos cidadãos, quais são os resultados obtidos por ela até o momento etc.

3.1 – POR QUE FOI NECESSÁRIA?

Em 2018 quando a lei que protege os dados dos cidadãos europeus entrou em vigor, conhecida como General Data Protection Regulation (GDPR), fez com que os legisladores brasileiros se atentassem para a importância de se ter uma regulamentação como esta no Brasil. Além disso deve-se modificar a legislação brasileira, haja vista que com a criação desta lei na Europa, afetaria diretamente a transferência de dados dos europeus para o Brasil. O site brasileiro Compugraf aponta que: "(...) E diante de todas as possibilidades, nasceu a LGPD, Lei Geral de Proteção de Dados que é explicitamente baseada na versão europeia, embora possua suas próprias características para se adaptar ao cenário brasileiro."

A Lei Geral de Proteção de Dados foi criada com o intuito principal de proteger o dado pessoais tanto dos cidadãos brasileiros, quanto por pessoa jurídica, inclusive nos meios digitais, que é o que está exposto no artigo 1º da lei. O site do Ministério Público Federal ainda completa dizendo que:

> A Lei Geral de Proteção de Dados (13.709/2018) tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Também tem como foco a criação de um cenário de segurança jurídica, com a padronização de regulamentos e práticas para promover a proteção aos dados pessoais de todo cidadão que esteja no Brasil, de acordo com os parâmetros internacionais existentes.

A lei em questão começou a entrar em vigor no dia 18 de setembro de 2020, e teve sua total vigência marcada no dia 1 de agosto de 2021, porém foi sancionada no dia 14 de agosto de 2018, surgiu para uma maior segurança das pessoas e/ou empresas para com seus dados existentes na internet.

Como foi exposto nas seções anteriores, o vazamento de dados confidenciais por parte dos bancos infelizmente é um problema recorrente, e um

dos principais objetivos da Lei Nº 13.709, 14 de agosto de 2018, é tentar minimizar esses vazamentos, além de fazer com que as pessoas coloquem apenas os dados necessários, e também explicite com qual finalidade aquele dado está sendo solicitado, quando forem criar uma conta em uma rede social ou até mesmo fazer uma compra com cartão de crédito pela internet, por exemplo.

Também é valido dizer que os dados que a lei trata são dados como telefone, endereço, número de identidade, registro geral, CPF, CNPJ no caso das empresas, e qualquer outro tipo de dado que possa revelar a identidade de alguém ou de alguma empresa.

3.2 – QUAIS FORAM AS RESPONSABILIDADES CIVEIS E CRIMINAIS QUE ESTA CRIOU?

Com a entrada da Lei Geral de Proteção de dados em vigor, praticamente todas as empresas com sede no Brasil, e todas aquelas que vendem serviços e bens no país tiveram que se adequar as novas normas impostas por ela.

Como foi exposto no último tópico a última parte da lei entrou em vigor em agosto de 2021, e é justamente nessa parte que a lei aborda a respeito das responsabilidades penais. Em seu artigo 52 onde se lê a respeito das penas que quem descumpre essa norma recebe, penas essas que vão desde apenas penas que são de caráter socioeducativo, até multas que podem chegar a 50 milhões de reais. As sanções impostas pela LGPD estão presentes nos artigos 52 e 54:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> – advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II – multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III – multa diária, observado o limite total a que se refere o inciso II;
>
> IV – publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V – bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

> VI – eliminação dos dados pessoais a que se refere a infração;
>
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
>
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
>
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

"Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional."

É possível também notar uma semelhança entre a Lei Geral de Proteção de Dados com o artigo 153 do Código Penal Brasileiro, haja vista que o artigo 153 do CP denota que, é crime quando se é divulgado algum conteúdo, sem prévia autorização do detentor do mesmo, podendo assim causar dano a outrem, e tendo pena de detenção de um a seis meses, além de multa. Ou se forem divulgados conteúdos de posse da Administração pública a pena aumenta, resultando em uma pena de 1 a 4 anos, e multa.

GONÇALVES, Antônio (2021, p. 1) faz a seguinte analogia:

> O tipo objetivo protegido é a divulgação sem justa causa de conteúdo que possa trazer prejuízo a terceiro, assim, informações pessoais, dados sigilosos, prontuários médicos e a violação da proteção de dados digitais são alguns dos elementos que podem ser atingidos pela norma penal.

Porém, é necessário se atentar aos artigos 2º, 3º e 6º da LGPD, haja vista que os mesmos impõem critérios para que a mesma possa ser aplicada. O artigo 2º trata a respeito da disciplina dos fundamentos da proteção de dados, onde são apontados 7 fundamentos que fazem com que a LGPD seja necessária, os quais são: respeito à privacidade; autodeterminação informativa; liberdade de expressão, de informação, de comunicação e de opinião; inviolabilidade da intimidade, da honra e da imagem; desenvolvimento econômico e tecnológico e a inovação; e por fim e não menos importante a livre iniciativa, a livre concorrência a defesa do consumidor; direitos humanos, o livre desenvolvimento da personalidade, a dignidade, e o exercício da cidadania pelas pessoas naturais.

O artigo 3º expõe sobre quando a lei deve ser aplicada, entende se que a lei irá se aplicar a qualquer pessoa, seja ela jurídica ou natural, independente do meio ou local em que a mesma se encontra, desde que este tratamento seja realizado em território nacional, e/ou tem por objetivo a oferta de algum bem ou serviço utilizando-se de dados de individuo situados em território nacional, e/ou os dados utilizados tenham sido coletados em território nacional, vale ressaltar que é considerado território nacional, quando o titular dos dados está no território no momento da coleta.

Já o artigo 6º trata dos princípios impostos e considerados pela lei, e nele é exposto os seguintes princípios, além do princípio da boa fé que e enfatizado no *Caput* do artigo: finalidade, os dados quando utilizados deveram possuir uma finalidade exata; adequação, o tratamento dos dados utilizados, devem ser iguais foram informados ao titular dos mesmos; necessidade, apenas os dados de suma importância podem ser utilizados; livre acesso, esse princípio dá ao proprietário dos dados o direito de solicitar um certo relatório que comprove com quais fins seus dados estão sendo utilizados; qualidade dos dados, dados devem sempre estar atualizados; transparência, esse princípio é praticamente igual ao do livre acesso, e dá direito ao titular de saber das informações; segurança, os dados devem ser protegidos e mantidos em sua integridade; prevenção, esse princípio é a característica fundamental da proteção dos dados; não discriminação; e por ultimo a responsabilização e prestação de contas.

Além das responsabilidades criminais criadas pela LGPD, foram também criadas responsabilidades cíveis, as quais as empresas também que tiveram que se adequar. Estás que estão dispostas no capítulo VI, seção III da LGPD. Segundo Walter Aranha, que é professor e advogado, em um artigo publicado por ele, o mesmo afirma que existem dois tipos de responsabilidades de âmbito cível criados pela Lei Geral de Proteção de Dados.

ARANHA, Walter (2020, p. 3) afirma que:

> Dessa forma, é possível identificar duas situações de responsabilidade civil na LGPD: a) violação de normas jurídicas, do microssistema de proteção de dados; b) violação de normas técnicas, voltadas à segurança e proteção de dados pessoais. E, evidentemente, só caracterizará a responsabilidade civil, se a violação de norma jurídica

> ou técnica ocasionar dano material ou moral a um titular ou a uma coletividade.

O artigo 42 delimita de certa forma essa responsabilidade para somente o controlador e/ou o operador. Neste mesmo artigo ele fala que um ou outros dos agentes citados, respondem em tom de reparação, para quem desses em razão da atividade de cuidar de dados, causar danos patrimoniais, morais, individuais ou coletivos a alguém.

Já o paragrafo primeiro deste artigo trata a respeito de quando cada um dos sujeitos ativos nessas ações serão responsabilizados, e como estes serão responsabilizados, é possível entender que o operador responderá solidariamente quando houver danos causados e o mesmo não estiver cumprindo as obrigações impostas pela legislação, ou quando não estiver seguindo as orientações do controlador. Já o controlador responderá solidariamente em qualquer situação que houver dano

O artigo 43 por sua vez diz respeito à quando os agentes não serão responsabilizados pelos problemas com dados. Em geral é possível se entender que a responsabilidade não cairá sobre os agentes quando for provado que os problemas estão dentro das diretrizes, ou quando esses problemas foram provocados exclusivamente por culpa de seu proprietário.

O artigo 44 retrata sobre quando será irregular os serviços de armazenamento de dados. Nele fica explicito que este é irregular quando ele não fornece a segurança necessária pelo titular dos dados, e também quando ele deixa de observar a legislação.

Essa indenização tratada acima, é calculada observando-se alguns critérios, ARANHA, Walter (2020, p. 6) enumera esses critérios da seguinte forma:

> a) a quantidade de dados pessoais afetados;
> b) a natureza dos dados pessoais afetados: o vazamento de dados pessoais sensíveis, por exemplo, determinará uma indenização maior, especialmente se se tratar de dados biométricos, que não podem ser substituídos;
> c) a reincidência da conduta;
> d) a omissão em tomar medidas de segurança e técnicas para minorar o dano ou em colaborar com a Autoridade Nacional de Proteção de Dados;

e) a ausência de notificação dos usuários da ocorrência do incidente;
f) a comprovada utilização dos dados pessoais vazados de titulares por terceiros.

3.3 – RESULTADOS

Por ser uma lei um tanto quanto recente, já que apesar de ter sido criada em 14 de agosto de 2018, a mesma só entrar completamente em vigência no segundo semestre do ano de 2021. Logo a mesma não apresenta ainda resultados extremamente significativos.

A maioria das empresas já possuem um grande conhecimento sobre tal lei, porém muitas ainda não conseguiram a se adequar a mesma.

Segundo uma pesquisa feita no ano de 2021, pela empresa Resultados Digitais, onde os entrevistadores avaliaram a situação de 997 empresa, sendo 60% delas microempresas. Apenas 14% dos responsáveis pelas empresas disseram que não possuíram nenhuma dificuldade em se adequar as novas normas impostas.

Um outro grande problema apontado pela pesquisa, trata a respeito da capacitação dos funcionários para trabalharem conforme as novas regras, a pesquisa diz que quase 33% das empresas não sabem se vão, ou não vão investir na capacitação de seus funcionários para que se adequem.

CONCLUSÃO

O presente estudo partiu da análise do tema da Lei de Proteção de Dados Responsabilidades Cíveis e Criminais, passando a tratar com enfoque os usuários da internet, que já tiveram problemas com ataques de malwares aos seus softwares, e como os usuários são afetados pela lei em questão.

Pretendeu-se com esse trabalho verificar-se como ocorreu o advento da internet e porque esse dispositivo se tornou uma das ferramentas de comunicação mais importantes do mundo, além de entender um pouco mais a respeito dos crimes cibernéticos, que hoje são algo bastante normais em nossa sociedade, muito disso se devendo a grande utilização desta rede. Além de

discorrer sobre como a Lei de Proteção de Dados foi importante para que houvesse uma diminuição neste tipo de crime.

A partir de vastas pesquisas feitas, fica claro que hoje são raras as pessoas que não têm e/ou nunca tiveram contato com a internet, uma vez que atualmente a internet é um dos meios de comunicação mais importantes do mundo, se não o mais importante atualmente. Além do mais, fica evidente de como o crescimento no número de usuários influenciou diretamente no número de crimes cibernéticos cometidos, e também como a LGPD conseguiu diminuir os atos ilícitos cometidos na grande rede mundial de computadores, além de impor penas mais duras aos criminoso que agem na internet.

As hipóteses levantadas no projeto de pesquisa foram confirmadas.

REFERÊNCIAS

- ALVES, Paulo. Rede mundial de computadores faz 30 anos e Google comemora com Doodle. Tech Tudo. Disponível em: < https://www.techtudo.com.br/noticias/2019/03/rede-mundial-de-computadores-faz-30-anos-e-google-comemora-com-doodle.ghtml> Acesso em: 10 nov 2021

- ARANHA, Walter. A responsabilidade civil na Lei Geral de Proteção

de Dados. **Direito**, Cadernos Jurídicos, São Paulo, 2021, nº 53, p. 163-170. Disponível em: <https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=637250347559005712> Acesso em: 24 fev 2022

- ASSOCIAÇÃO DO MINISTÉRIO PÚBLICO DE MINAS GERAIS. Brasil registra 54 crimes virtuais por minuto. 2012. Disponível em: <https://amp-mg.jusbrasil.com.br/noticias/3125198/brasil-registra-54-crimes-virtuais-por-minuto> Acesso em 15 jan 2022

- BLOG SAN. Perigos da internet. Quais são e como se prevenir. 2021. Disponível em: <https://blog.saninternet.com/perigos-da-internet> Acesso em: 11 nov 2021

- BRANDÃO, Gustavo Koury Maues; CAMPOS, Kaique Duarte; CARDOSO, Wladirson Ronny da Silva. CRIMES VIRTUAIS: Uma análise sobre a adequação da legislação penal brasileira. **Direito**, 2018. Disponível em: <https://www.unirios.edu.br/revistarios/media/revistas/2018/18/crimes_virtuais.pdf> Acesso em: 14 jan 2022

- BRASIL. Constituição Federal da República Federativa do Brasil de 1988. Promulgada em 05 de outubro de 1988.

- BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez.

- BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). Promulgada em 14 de agosto de 2018.

- BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil.

- CRUZ, Diego; RODRIGUES, Juliana. Crimes Cibernéticos E A Falsa Sensação De Impunidade. **Direito**, Garça, v.13, 2018.

- DIANA, Daniella. **História da internet**. Toda Matéria. Disponível em: <https://www.todamateria.com.br/historia-da-internet/> Acesso em: 9 nov 2021

- DOMINGOS, Fernanda Teixeira Souza; RÖDER, Priscila Costa S. Obtenção de provas digitais e jurisdição na Internet. **Direito**, São Paulo, v. 1, 2017, p. 63-65. Disponível em: < https://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf> Acesso em: 19 fev 2022

- GARRETT, Filipe. **Crimes cibernéticos: entenda o que são e como se defender**. 2021. Tech Tudo. Disponível em: <https://www.techtudo.com.br/noticias/2021/08/crimes-ciberneticos-entenda-o-que-sao-e-como-denunciar.ghtml 15/11/21> Acesso em: 12 nov de 2021

- GARRET, Filipe. O que é a Deep Web. 2019. Disponível em: <https://www.techtudo.com.br/noticias/2019/03/o-que-e-deep-web.ghtml> Acesso em: 13 jan 2022

-GONÇALVES, Antônio. Lei Geral de Proteção de Dados Pessoais, as responsabilidades e os aspectos penais. 2021. Disponível em: <https://www.conjur.com.br/2021-out-01/goncalves-lgpd-responsabilidades-aspectos-penais> Acesso em 25 fev 2022

- GONZÁLEZ, Mariana. LGPD comentada. GuiaLGPD. 2019. Disponível em: < https://guialgpd.com.br/lgpd-comentada/> Acesso em: 14 dez 2021

- G1. Ataque hacker desvia mais de R$ 500 mil de contas bancárias da Prefeitura de Euclides da Cunha Paulista. 2021. Disponível em: < https://g1.globo.com/sp/presidente-prudente-regiao/noticia/2021/12/22/ataque-hacker-desvia-mais-de-r-350-mil-de-contas-bancarias-da-prefeitura-de-euclides-da-cunha-paulista.ghtml> Acesso em: 15 jan 2022

- G1. Denúncias de crimes cometidos pela internet mais que dobram em 2020. 2021. Disponível em: < https://g1.globo.com/economia/tecnologia/noticia/2021/02/09/numero-de-denuncias-de-crimes-cometidos-pela-internet-mais-que-dobra-em-2020.ghtml>

- IBGE EDUCA. Uso de internet, televisão e celular no Brasil. 2019. Disponível em: <https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular-no-brasil.html> Acesso em 10 de nov 2021

- KASPERSKY. Danos causados por malware. 2021. Disponível em: < https://www.kaspersky.com.br/resource-center/threats/malware-damage> Acesso em: 23 fev 2022

- MARGOTTI, Leonardo. 11 empresas que sofreram ataques cibernéticos. 2020. Disponível em: <https://backupdados.com.br/blog/11-empresas-que-sofreram-ataques-ciberneticos> Acesso em: 18 jan 2022

- BRASIL. MINISTÉRIO PÚBLICO FEDERAL. O que é a LGPD?. Disponível em: <http://mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd> Acesso em: 14 fev 2022

- NOLETO, Cairo. LGPD: o que é, por que foi criada e o que muda?. 2020. Disponível em: <https://blog.betrybe.com/tecnologia/lgpd-lei-geral-de-protecao-de-dados/> Acesso em: 22 fev de 2022

- NUCCI, Guilherme de Souza. Manual de Direito Penal 11ª Ed. 2015

- RESULTADOS DIGITAIS. Empresas e LGPD: Cenários, desafios e caminhos. Como a entrada em vigor das sanções previstas na Lei Geral de Proteção de Dados Pessoais afetará as empresas. 2021. Disponível em: <https://d335luupugsy2.cloudfront.net/cms%2Ffiles%2F2%2F1628275980relatorio-adequacao-lgpd-rd-manar.pdf> Acesso em 1 mar 2022

- RIBEIRO, Douglas. Crimes cibernéticos serão punidos com mais severidade. Migalhas. Disponível em: < https://www.migalhas.com.br/depeso/350424/crimes-ciberneticos-serao-punidos-com-mais-severidade> Acesso em: 10 nov 2021

- ROCKCONENT. Conheça a história da internet, sua finalidade e qual o cenário atual. 2020. Disponível em: <https://rockcontent.com/br/blog/historia-da-internet/> Acesso em: 10 nov 2021

- TECH MUNDO. Microsoft. 2020. Disponível em: < https://www.tecmundo.com.br/microsoft> Acesso em: 27 dez 2021

- TEIXEIRA, Ronaldo de Quadros. Os Crimes Cibernéticos no Cenário Nacional. Escola superior aberta do Brasil – ESAB, 2013 (Curso de pós-graduação lato sensu em engenharia de sistemas).

Acesso em: 10 jan 2022

- YAHOO ESPORTES. Quantos e-mails são enviados por dia?. 2020. Disponível em: <https://esportes.yahoo.com/video/quantos-e-mails-s%C3%A3o-enviados-154333487.html> Acesso em: 29 dez 2021

Acesso em: 18 dez 2021