PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Instituto de Ciências Exatas e Informática
***Campus* Betim**
Bacharelado em Sistemas de Informação

Pesquisadores:

Sabrina Matos Rodrigues (Aluna)

Fábio Martins de Oliveira (Orientador)

DIREITO DIGITAL E PROTEÇÃO DE DADOS

Betim
2021

Sabrina Matos Rodrigues

DIREITO DIGITAL E PROTEÇÃO DE DADOS

Monografia apresentada ao Programa de Bolsas de Iniciação Científica, Tecnológica e Inovação da Pontifícia Universidade Católica de Minas Gerais, *campus* Betim

Orientador: Prof. Fábio Martins de Oliveira

Betim
2021

RESUMO

Este trabalho aborda um estudo sobre o Direito Digital brasileiro e a Proteção de Dados. O tema foi escolhido devido ao interesse em compreender se porventura a atual legislação brasileira pode ser atendida com as ferramentas tecnológicas existentes.

A elaboração deste trabalho se deu por pesquisa bibliográfica nas áreas relacionadas ao tema, a fim de possibilitar a contribuição da autora por observação e consideração das definições encontradas. A bibliografia em sua maior parte foi obtida pela biblioteca virtual da PUC, outra parte pela biblioteca física e outra parte no *Google Play* Livros.

A partir do desenvolvimento dessa pesquisa foi possível constatar que a legislação brasileira de fato contempla muitos dos conflitos tecnológicos atuais, porém a complicação está na falta de educação digital para todos os cidadãos, considerando que leis como o Marco Civil da Internet e a Lei Geral de Proteção de Dados requerem que o titular dos dados seja proativo em relação aos seus direitos, capaz de revogar consentimento previamente concedido e de solicitar remoção de conteúdo de plataformas.

Existe a necessidade de uma maior conscientização sobre como a Internet funciona e quais são os direitos e deveres digitais que o brasileiro possui, em mídias acessíveis como televisão, programas de educação pública e outras possibilidades similares.

Palavras-chave: Direito digital. Dados. Segurança da Informação. Internet. Legislação brasileira.

ABSTRACT

This monography is about a study of brazilian's Digital Law and Data Protection. This subject was chosen due to the interest in understanding if perhaps the current brazilian law can be attended with the existent technological tools.

The elaboration of this work was through bibliographic research in the fields related to the subject, in order to allow the author contribuition by observance and consideration of the found definitions. The bibliography was mostly obtained through the virtual library of PUC, another part through the physical library and another on the Google Play Books.

From this research development it was possible to find out that the brazilian digital law in fact contemplate many of the current technological conflicts, although the complicated part stays in the missing digital education for all the citizens, considering that laws such as the Marco Civil da Internet and the Lei Geral de Proteção de Dados requires that the data owner be proactive regarding your rights, capable of revoking consent previously granted and of requesting remotion of content on platforms.

Exists the necessity of a bigger awareness about how does the Internet works and what are the digital rights and duties that the brazilian citizen has, in acessible media such as television, public education programs and other similar possibilities.

Keywords: Digital law. Data. Information Security. Internet. Brazilian's law.

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

IBGE	Instituto Brasileiro de Geografia e Estatística
LGPD	Lei Geral de Proteção de Dados
ANPD	Autoridade Nacional de Proteção de Dados
ABNT	Associação Brasileira de Normas Técnicas
OWASP	Projeto Aberto de Segurança em Aplicações Web (*Open Web Application Security Project)*
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
DoS	Negação de Serviço (*Denial of Service)*
DDoS	Negação de Serviço Distribuído (*Distributed Denial of Service)*
MiTM	Homem no Meio (*Man in The Middle*)
TCU	Tribunal de Contas da União
ISO/IEC	Organização Internacional para Padronização/ Comissão Eletrotécnica Internacional (*International Organization for Standardization / International Electrotechnical Commission)*
XML	*Extensible Markup Language*
XXE	*XML External Entity*
HTTP	Protocolo de Transferência de Hipertexto (*Hypertext Transfer Protocol)*
XSS	*Cross-Site Scripting*
API	Interface de Programação de Aplicações (*Application Programming Interface)*
URL	Localizador Uniforme de Recursos *(Uniform Resource Locator)*
JSON	*JavaScript Object Notation*
SOAP	Protocolo Simples de Acesso a Objetos (*Simple Object Access Protocol)*
JWT	*JSON Web Token*
CNJ	Conselho Nacional de Justiça

SUMÁRIO

1 INTRODUÇÃO

A Internet se expandiu sobremaneira mundialmente nas últimas décadas, permitindo à maioria das pessoas o acesso à rede e aos recursos por ela oferecidos. O Instituto Brasileiro de Geografia e Estatística (IBGE) realizou a Pesquisa Nacional por Amostra de Domicílios Contínua. Segundo o IBGE (2017), 3 a cada 4 domicílios brasileiros têm acesso à Internet.

Há comércio, entretenimento, fácil socialização com pessoas ao redor do mundo, compartilhamento instantâneo de informações e de arquivos. Assim, observa-se que o ambiente virtual é um espelho da realidade e, como tal, também precisa do amparo das leis para que os indivíduos sejam protegidos e tenham seus direitos garantidos.

São fatores a se considerar que existe conectividade em tempo real dos continentes, que as leis de cada país são diferentes, que conflitos entre pessoas de diferentes países acontecem. O ambiente de interação entre as partes amplia-se para além das fronteiras físicas; é preciso atender a essa realidade.

De acordo com Pinheiro (2016, p.79), a rapidez das transformações tecnológicas é maior que a velocidade de definição de novas legislações, considerando que a durabilidade e território dessas leis teriam vigência afetada em função da dinâmica dessas mudanças. Assim, o direito digital é amparado pelo Direito Codificado e pelo Direito Costumeiro, não havendo uma nova área, mas uma absorção das já existentes de elementos que contemplem o mundo virtual.

Muitos crimes que acontecem no espaço físico também ocorrem no ciberespaço; da primeira forma, é possível identificar os criminosos por meio da declaração de testemunhas, vestígios como digitais e fluídos corporais ou com o auxílio tecnológico a partir de imagens de câmeras de segurança ou registros de conversas e tráfego. Já no ambiente virtual, esses vestígios e provas são compostos por dados virtuais, armazenados em diversos bancos de dados na rede, o que permite o rastreio e identificação dos criminosos.

As possibilidades, oportunidades e vantagens que o espaço cibernético proporciona são interessantes para a economia, a educação e a democracia, portanto ele não deve ser desconsiderado. Diante desta oportunidade, novos desafios e preocupações surgem, como por exemplo a segurança dos dados.

No Brasil, foi sancionada em 2019 a Lei Geral de Proteção aos Dados (LGPD). Algumas iniciativas anteriores já haviam sido estabelecidas como, por exemplo, em 2014 a lei do Marco Civil da Internet estabeleceu direitos, deveres, princípios e garantias para o uso da Internet no Brasil e, em 2012, a lei Carolina Dieckmann também abordou tipificação criminal de delitos informáticos.

A LGPD é a mais recente lei a regular o tratamento de dados no Brasil. Ela define a relação das empresas que realizam tratamento de dados com os cidadãos quanto a forma de uso de seus dados dentro do território brasileiro. É preciso observar as exceções em relação a quais tipos de empresas e seus fins pois essa lei não se aplica a todas as empresas, por exemplo, aquelas que não realizam tratamentos de dados. Esse tratamento de dados não é apenas dos clientes, externos à organização, mas também dos funcionários ali dentro da empresa.

A LGPD visa instaurar um maior controle sobre os próprios dados pessoais aos donos (titulares) dos dados, definindo a necessidade de um consentimento explícito do titular à finalidade proposta pela empresa. Para intermediar a relação empresa-titular, e para orientar acerca do novo cenário do direito digital, foi criada a Autoridade Nacional de Proteção de Dados (ANPD).

Também ocasionou uma mudança na estrutura das empresas, que precisam nomear três figuras, a saber: o Controlador, o Operador e o Encarregado; sendo que o último pode ser uma empresa (terceirizada) contratada para realizar as funções a ele atribuída.

A falta de conhecimento básico do funcionamento da Internet é uma vulnerabilidade para a sociedade, pois esse conhecimento é necessário para ter noção dos perigos virtuais, de como se proteger deles, o que evitar e o que fazer.

Assim, percebe-se a necessidade de conscientizar as pessoas que utilizam os recursos da Internet sobre as possíveis falhas de segurança, os métodos de proteção e a legislação vigente aplicada neste ambiente. Essa conscientização se torna relevante partindo do pressuposto de que a divulgação de informações relacionadas aos direitos e deveres nem sempre são incentivadas em ambientes escolares ou mesmo comunitários, o que leva a um desconhecimento do assunto de parte da população. Para estar consciente da realidade é importante adquirir informação externa, visto que uma sociedade é composta não apenas pelo “*eu*”,

mas de vários indivíduos e suas perspectivas, por hora divergentes, em outras convergentes, ou ainda paralelas, mas harmonizadas pelo Direito.

Diante deste cenário apresentado, a proposta deste trabalho consiste em explorar o campo da segurança da informação na Internet. A partir de uma discussão sobre as falhas de segurança, métodos de ataque e proteção de dados pessoais e do mapeamento sobre a legislação e demais matrizes normativas aplicadas ao Direito Digital, espera-se com isso orientar e conscientizar acerca da segurança da informação na Internet e dos direitos e deveres de cada indivíduo neste ambiente. Além disso, espera-se discorrer acerca da efetividade e da aplicabilidade da legislação na Internet, com base em uma análise não somente crítica, mas também do ponto de vista técnico.

1.1 Tema

Direito digital e proteção de dados: orientação e conscientização da sociedade.

1.2 Ideia

A proposta deste trabalho consiste em apresentar uma cartilha informativa sobre Segurança e Proteção de Dados e o Direito Digital que regula a Internet no Brasil, a fim de comunicar pontualmente sobre os direitos e deveres das pessoas na Internet.

1.3 Objetivo geral

O objetivo geral deste trabalho é trazer à consciência sobre como a Internet se relaciona com a regulamentação do Direito Digital no Brasil ao fornecer uma base para possíveis futuras campanhas de educação nas redes de computadores e, dessa forma, orientar as pessoas com relação a segurança da informação, a legislação e demais normativas, bem como a sua efetividade e aplicabilidade do ponto de vista técnico.

1.4 Objetivos específicos

Os objetivos específicos deste trabalho são:

1) Compreender os aspectos relevantes sobre a segurança da informação na Internet;
2) Investigar as falhas de segurança métodos de proteção de dados;

3) Fazer um levantamento da legislação vigente e demais normativas aplicadas ao direito digital;
4) Analisar crítica e tecnicamente a efetividade e aplicabilidade da legislação atual aplicada à Internet;
5) Realizar um estudo de caso sobre crimes virtuais;
6) Investigar penalidades aos crimes mais comuns.

1.5 Justificativa

A motivação para desenvolver este trabalho veio da percepção, por senso comum, que muitas pessoas não conhecem a maneira como o direito regula a Internet. Assim como no cotidiano físico, nem sempre as pessoas têm consciência de seus deveres e direitos como parte da sociedade nas variadas circunstâncias da vida.

Muitas vezes o conhecimento do direito do cidadão é adquirido por meio de ambientes escolares, da comunidade em si, de cartilhas, de propagandas seja em televisões ou jornais, por divulgação por meio de pessoas que ouviram em algum lugar, por informativos como disque-denúncia, entre outros.

Com a presença estabelecida da Internet no mundo atualmente, é perceptível a necessidade de comunicar a maneira como esse ambiente virtual é regulado, assim como o ambiente físico tem sido para que as relações humanas possam acontecer harmoniosamente.

Nesse contexto, este trabalho se torna relevante por trazer uma discussão acerca dos direitos e deveres das pessoas no Brasil ao utilizarem a Internet, sobre a realidade dos crimes virtuais mais recorrentes e como proteger os dados durante a navegação. Além da orientação da sociedade em geral acerca dos seus direitos e deveres no ambiente digital, ressalte-se a necessidade de uma análise técnica da eficácia e da irrefutabilidade da legislação aplicada à Internet.

2 REFERENCIAL TEÓRICO

Neste capítulo é apresentada uma breve revisão de literatura, em que são abordados conceitos relacionados ao objeto de pesquisa. Na seção 2.1 é apresentada a conceituação de Espaço Cibernético. A seção 2.2 apresenta a definição de Direito Digital. A seção 2.3 aborda a regulação jurídica da Internet no Brasil. A seção 2.4 aborda a Segurança da Informação, e especificamente trata na seção 2.4.1 sobre Falhas de Segurança, na seção 2.4.2 sobre Ameaças na Internet e na seção 2.4.3 sobre Mecanismos de Proteção de Dados e Informações. Por fim, na seção 2.5 é abordado sobre o tema crimes virtuais.

2.1 Espaço Cibernético

O espaço cibernético é descrito pela ABNT (2015, p.12) como um ambiente virtual consequente da Internet, aonde pessoas, organizações, atividades, dispositivos e redes estão presentes.

2.2 Direito Digital

Segundo Pinheiro (2016, p.77), o Direito Digital consiste na evolução do próprio direito. A velocidade das transformações no ambiente virtual impõe barreira à legislação, sendo necessário recorrer ao estabelecimento de um relacionamento entre o Direito Codificado e o Direito Costumeiro, para solucionar as questões da sociedade digital, tendo em mente que os fatores tempo e território restringem a formulação de leis específicas. Essas leis específicas podem ser geridas ao se estabelecer um contrato de serviço.

2.3 Regulação jurídica da Internet no Brasil

Aplicar a justiça na Internet não é tão simples quanto em outros meios de telecomunicação, devido à complexidade das redes de computadores. Muitas vezes, é necessária a cooperação de empresas para encontrar provas sobre crimes, pois os rastros comprovatórios estão nos bancos de dados que guardam os dados dos serviços da empresa.

Dentre as leis que falam sobre o direito digital estão:

A. A lei n° 9.507, de 12 de Novembro de 1997, que "*Regula o direito de acesso a informações e disciplina o rito processual do habeas data.*" (BRASIL, 1997);
B. A lei n° 12.527, de 18 de Novembro de 2011, que

> "regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências." (BRASIL, 2011);

C. A lei Carolina Dieckmann, que foi sancionada em 30 de Novembro de 2012, e segundo a ementa, "*dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências."* (BRASIL, 2012);
D. O decreto n° 7962 de 15 de Março de 2013, que segundo a ementa, "*regulamenta a Lei no 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico.*" (BRASIL, [2013]);
E. A lei do Marco Civil da Internet, sancionada em 23 de Abril de 2014, que "*estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.*" (BRASIL, 2014);
F. O decreto n° 8.771 de 11 de Maio de 2016, que

> "regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações." (BRASIL, [2016]);

G. O decreto n° 8.777 de 11 de Maio de 2016, que "*Institui a Política de Dados Abertos do Poder Executivo federal.*" (BRASIL, [2016]);
H. A Lei de Proteção de Dados Pessoais, sancionada em 9 de Agosto de 2018 e "*dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).* " (BRASIL, 2018);
I. O decreto N° 9.637 de 26 de Dezembro de 2018 que

> "institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e

> dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional" (BRASIL, [2018]);

J. O decreto N° 9.854, de 25 de Junho de 2019, que

> "institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas." (BRASIL, [2019]).

2.4 Segurança da Informação

Conforme a ABNT (2005, p. x), a segurança da informação se trata de manter a informação protegida de ameaças, garantindo que o negócio continue com o mínimo de riscos e o máximo de retorno sobre o investimento. Para Fontes (2006), ela busca proteger as informações através de orientações, normas, políticas e outras ações para que a organização alcance seus objetivos.

A segurança no espaço cibernético, segundo a ABNT (2015, p5), é possível através da preservação da confidencialidade, integridade e disponibilidade das informações.

Para o Tribunal de Contas da União (TCU) do Brasil (2012), a segurança da informação é importante pois a informação é valiosa. Se ela não é confidencial, nem íntegra, nem disponível, pode prejudicar os processos da instituição e sua imagem.

2.4.1 Falhas de segurança

As falhas de segurança permitem que ameaças causem danos ao que se busca proteger.

Segundo Cabral e Caprino (2015, p.12), atualmente se produz mercadoria para que dure até que outro produto inovador a substitua, isso rapidamente, assim é inviável tampar todas as brechas antes de vender o produto, pois isso pode prejudicar a venda.

2.4.2 Ameaças na Internet

A ABNT (2015, p.8) define como ameaça aquilo que pode causar um incidente indesejado que afete negativamente sistemas, indivíduos ou organizações.

Segundo a ABNT (2019, p.12), elas podem ser naturais ou humanas, propositais ou não, sendo importante identificá-las.

Conforme CERT (2012, p.101), na Internet se está sujeito a ameaças diversas, onde os dados podem ser roubados, os recursos computacionais utilizados

sem conhecimento do proprietário, ataques para descobrir credenciais como o de força bruta, dentre outros.

A seguir, são enumeradas dezenove ameaças na Internet:

1. **Adware**: Um *adware* é, para a ABNT (2015, p.2) um programa que apresenta publicidade não requisitada para os usuários, ou ainda pode coletar informação sobre como o usuário se comporta na Internet;
2. **Bot**: Conforme a ABNT (2015, p.4), um *bot* é um *software* automatizado, que realiza tarefas específicas, para um usuário ou outro programa;
3. **Botnet**: Um *botnet*, para a ABNT (2015, p.4), é uma coleção de *bots*, que funcionam de forma autônoma em computadores comprometidos;
4. **Malware**: Segundo a ABNT (2015, p.7), um *malware* é um *software* malicioso, que pode prejudicar o usuário ou o computador do usuário;
5. **Conteúdo malicioso**: Conteúdos maliciosos, conforme a ABNT (2015, p.7), são recursos computacionais acompanhados ou contaminados por recursos maliciosos;
6. **Phishing**: *Phishing* para a ABNT (2015, p.7) é tentar obter informações confidenciais de um alvo numa comunicação, fingindo ser alguém confiável;
7. **Spam**: Segundo a ABNT (2015, p.8), *spam* é quando se usa de sistemas mensageiros para enviar mensagens não solicitadas em massa;
8. **Spyware**: Para a ABNT (2015, p.8), um *spyware* é um *software* que coleta informações confidenciais de uma pessoa, como por exemplo as senhas;
9. **Trojan**: Um *trojan* é um *malware* que parece desempenhar uma função desejável (ABNT, 2015, p.8);
10. **Varredura em redes (*scan*)**: Conforme o CERT (2012, p.18), a varredura em redes é buscar identificar computadores ativos e informações sobre eles, e então associar com possíveis vulnerabilidades dos serviços e dos programas instalados;
11. **Interceptação de Tráfego (*sniffing*)**: Segundo o CERT (2012, p.19), a interceptação de tráfego é a inspeção dos dados trafegados em redes com o uso de programas chamados *sniffers*. Pode ser feito maliciosamente se for para capturar informações confidenciais;
12. **Exploração de vulnerabilidades:** Um ataque de exploração de vulnerabilidades, segundo o CERT (2012, p.18), acontece quando um

atacante usa de uma vulnerabilidade para tentar executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível;

13. **Ataque de negação de serviço (DoS e DDoS):** Conforme o CERT (2012, p.21), negação de serviço (*DoS)* é usar um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet. É uma negação de serviço distribuído (*DDoS)* se for usado um conjunto de computadores;
14. **Ataque de força bruta (*brute force*):** O ataque de força bruta, conforme o CERT (2012, p.20), se dá através da adivinhação, por tentativa e erro, de um nome de usuário e senha, levando a executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário;
15. **Desfiguração de página (*defacement*):** A desfiguração de página, conforme o CERT (2012, p.21), é uma técnica que altera o conteúdo da página *web* de um *site*, através da exploração de erros da aplicação *web*, de vulnerabilidades do servidor da aplicação *web* e da linguagem de programação ou dos pacotes utilizados no desenvolvimento da aplicação *web*, podendo invadir o servidor onde a aplicação *web* está hospedada e alterar diretamente os arquivos que compõem o *site*, e furtar senhas de acesso à interface *web* usada para administração remota;
16. **Credential Stuffing**: "*Credential stuffing*" é coletar credenciais vazadas (geralmente roubadas em um vazamento de dados) e usar em várias outras contas, esperando conseguir acesso (AVAST, 2021);
17. **Man in The Middle (MiTM)**: No ataque *Man in The Middle*, "O invasor se posiciona entre duas partes que tentam comunicar-se, intercepta mensagens enviadas e depois se passa por uma das partes envolvidas." (MALENKOVICH, 2013);
18. **Keylogger**: Um *keylogger* é "capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador." (CERT, 2012, p. 27);
19. **Screenlogger**: Um *screenlogger* é "capaz de armazenar

> a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado.” (CERT, 2012, p. 27).

2.4.3 Mecanismos de proteção de dados e informações

É preciso usar mecanismos que protejam as informações e os próprios dispositivos quanto às ameaças que podem danificá-los, tendo em vista que para além do dano aos arquivos do computador, existem ameaças que podem até mesmo sobrecarregar o computador de tal maneira que afete fisicamente seus componentes, com superaquecimento e dentre outros.

Segundo o CERT (2012, p.48), alguns exemplos de mecanismos de segurança são: a criptografia, política de segurança, o *backup*, registros de eventos (*logs*), ferramentas *antimalware*, filtro *antispam*, notificação de incidentes, contas e senhas, *firewall*, antivírus e filtro de bloqueio de propagandas.

A seguir, a descrição de dez mecanismos de segurança:

1. **Criptografia:** Para o CERT (2012, p.67), a criptografia é a escrita cifrada ou por código, e dependendo do tipo de chave usada, os métodos criptográficos podem ser simétricos ou assimétricos:
    1. Métodos simétricos: Segundo o CERT (2012, p.68), uma única chave é usada para codificar e decodificar;
    2. Métodos assimétricos: São usadas, segundo o CERT (2012, p.68), uma chave pública e uma chave privada. Uma informação codificada com uma das chaves só pode ser decodificada com a outra chave.

    Ainda segundo o CERT (2012, p.69), uma outra forma de criptografar é a função de resumo (*hash*), que gera um identificador de tamanho fixo, usado, por exemplo, para verificar se a integridade de um arquivo foi preservada;
2. **Política de Segurança:** A política de segurança define os direitos e as responsabilidades de cada um em relação à segurança dos recursos computacionais que utiliza e as penalidades às quais está sujeito, caso não a cumpra (CERT, 2012, p.48);
3. **Cópias de Segurança (*Backup*):** O “*backup”* é definido como “uma cópia que se destina a guardar dados armazenados no caso de uma eventual perda de informação.” (BACKUP, 2021). *“*Permitem a proteção de dados, a recuperação de versões e o arquivamento” (CERT, 2012, p.51 e p.52);

4. **Registros de eventos (*Logs*):** O *log* é, conforme CERT (2012, p. 53), o registro de atividades de um computador, que pode ficar armazenado em arquivos, na memória do computador ou em bases de dados;
5. **Ferramentas *antimalware:*** “Ferramentas *antimalware* são aquelas que procuram detectar

> e, então, anular ou remover os códigos maliciosos de um computador. Antivírus, antispyware, antirootkit e antitrojan são exemplos de ferramentas deste tipo.” (CERT, 2012, p. 55);

6. **Filtro *antispam:*** “Os filtros *antispam* já vem integrado à maioria dos *Webmails* e programas leitores de *e-mails* e permite separar os *e-mails* desejados dos indesejados (*spams*).” (CERT, 2012, p.74);
7. **Notificação de incidentes e abusos:** Um incidente de segurança, para o CERT (2012, p.50), é qualquer evento contrário a segurança do sistema ou das redes, e notificá-lo aumenta a segurança da Internet e ajuda que outras pessoas detectem problemas;
8. **Contas e senhas:** Para tratar da autenticação a fim de determinar a qual função e informações o usuário tem acesso, é necessário o uso de contas e senhas. Conforme o CERT (2012, p.51), uma conta de usuário é o que permite a identificação do usuário em um computador ou serviço.

   “Na autenticação, o usuário deve apresentar algo que só ele saiba ou possua, podendo até envolver a verificação de características físicas pessoais.” (Brasil, 2012, p.19);
9. ***Firewall* pessoal:** “*Firewall* pessoal é um tipo específico de *firewall* que é utilizado para proteger um computador contra acessos não autorizados vindos da Internet.” (CERT, 2012, p. 57);
10. **Filtro de bloqueio de propagandas:** “Filtros, como o *Adblock*, permitem o bloqueio de *sites* conhecidos por apresentarem propagandas” (CERT, 2012, p. 58).

2.5 Crimes virtuais

Conforme o artigo primeiro do decreto da lei n° 3.914 de 9 de dezembro de 1941, considera-se crime

> “[...] a infração penal que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente

> com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente.” (BRASIL, 1941, art. 1º)

De acordo com o Dicionário Priberam da Língua Portuguesa, “cibercrime” é definido como “crime cometido através da comunicação entre redes de computadores, notadamente através da Internet” (CIBERCRIME, 2021).

No mundo virtual, a existência de trilha de auditoria (arquivos de *log*) são fundamentais para consultas sobre fatos que aconteceram. Mas as informações gravadas devem ser efetivas, corretas e íntegras. (FONTES, 2006, p. 18).

Segundo o SAFERNET (2018), as principais violações para as quais os internautas brasileiros pediram ajuda no ano 2018 foram a exposição de imagens íntimas, *ciberbullying* ou ofensa, fraude ou golpes ou *e-mails* falsos, problemas com dados pessoais e o conteúdo ou discurso de ódio.

3 METODOLOGIA

A princípio, foi realizada uma revisão bibliográfica sobre definições e conceitos de Segurança da Informação, Proteção de Dados e Informações, Métodos de prevenção de falhas de segurança, Direito Digital e regulação jurídica da Internet no Brasil. Essa revisão se fez necessária para compreensão dos aspectos conceituais envolvidos na temática do trabalho que serviram de base para as análises e conclusões.

Em seguida foi feito um mapeamento sobre a legislação e demais matrizes normativas aplicadas ao Direito Digital, previamente conceituado. A importância desta etapa consiste no entendimento acerca das normas e leis aplicadas aos crimes cometidos na Internet, bem como as responsabilidades e penalidades envolvidas. Uma análise técnica da aplicabilidade e efetividade dessas leis e regulamentações foi realizada.

Na sequência foi realizado um estudo dos mecanismos de prevenção de ataques e falhas de segurança, a partir da exploração de softwares e ferramentas existentes. Esse estudo serviu de base para definição dos métodos de segurança mais eficazes na atualidade, de acordo com cada falha de segurança identificada.

Por fim, a exploração e análise de casos reais de falhas de segurança e medidas adotadas foram realizadas. Consistiu de uma etapa de levantamento de situações do cotidiano em que pessoas e/ou empresas podem estar sendo vítimas de ataques virtuais. A partir deste levantamento, com base nos mecanismos de segurança estudados na etapa anterior, foi feita uma avaliação crítica e técnica das causas das falhas ocorridas.

4 MAPEAMENTO DA LEGISLAÇÃO

Neste capítulo serão resumidas e analisadas as principais legislações referentes ao direito digital, que são a Lei Carolina Dieckmann que foca na invasão de dispositivo informático, o Marco Civil da Internet que foca no uso da Internet no Brasil e a Lei Geral de Proteção de Dados Pessoais que foca no tratamento de dados pessoais.

4.1 Lei Carolina Dieckmann

Na atualidade, as pessoas carregam nos smartphones muitos dados pessoais, de fotos, conversas, *e-mails*, dados de contas, *sites* visitados, aplicativos utilizados e arquivos como comprovantes, extratos e arquivos sigilosos empresariais. Essas informações podem ser acessadas em situação de invasão de dispositivo, causando danos ao proprietário.

A lei Carolina Dieckmann trata principalmente da invasão de dispositivo informático, acrescentando no Decreto-Lei n°2.848 os artigos 154-A e 154-B, mas também acresce redação neste Decreto-Lei sobre a interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, e também sobre a falsificação de documento particular, acrescendo na seção de falsificação de cartão que o cartão de crédito ou débito se equiparam a documento particular.

Esta lei, ao definir o crime de invasão de dispositivo informático, diz que

> “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: [...]” (BRASIL, 2012, Art. 154-A)

Segundo Brasil (2012), as penas para a invasão de dispositivo informático podem ser de detenção e de reclusão, e existem agravantes na lei. As penas para a interrupção ou perturbação de serviço telegráfico, telefônico informático, telemático ou de informação de utilidade pública tem como agravante o caso de ser cometido em ocasião de calamidade pública.

4.2 Marco Civil da Internet

O consentimento do usuário e a justificativa do uso dos dados são parte da temática desta lei. São definidas responsabilidades do provedor de Internet e direitos do usuário.

A seguir, um quadro mostra a estrutura da lei do Marco Civil da Internet:

Quadro 1 — Estrutura do Marco Civil da Internet

CAPÍTULO	TEMA	SEÇÕES	ARTIGOS
1	Disposições preliminares	-	1 ao 6
2	Dos direitos e garantias dos usuários	-	7 e 8
3	Da provisão de conexão e de aplicações de Internet	I. Da neutralidade da rede II. Da proteção aos registros, aos dados pessoais e às comunicações privadas • Da guarda de registros de conexão • Da guarda de registros de acesso a aplicações de Internet na provisão de conexão • Da guarda dos registros de acesso a aplicações de Internet na provisão de aplicações III. Da responsabilidade por danos decorrentes de conteúdo gerado por terceiros IV. Da requisição judicial de registros	9 ao 23
4	Da atuação do Poder Público	-	24 ao 28
5	Disposições finais	-	29 ao 32

Fonte: Elaborado pela autora com dados extraídos de BRASIL (2014).

Esta lei se aplica quando uma operação de coleta, ou armazenamento, ou guarda e tratamento de registros ou de dados pessoais, ou de comunicações por provedores de conexão e de aplicações de Internet **aconteça em território nacional,** devendo ser respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros, conforme o artigo 11.

A disponibilização ao requerente dos registros de conexão deve vir de uma autorização judicial, conforme o quinto inciso do artigo 13.

Em se tratando da responsabilidade civil das plataformas, é necessário que o reclamante entre com ordem judicial específica para que a lei se aplique sobre o provedor de aplicações de Internet, conforme o artigo 19, exceto em

situação de conteúdo de nudez ou de atos sexuais, em que o provedor de conteúdo para terceiros pode ser responsabilizado subsidiariamente mesmo sem a ordem judicial, caso não indisponibilize o conteúdo após notificação do participante ou representante legal, conforme o artigo 21.

4.3 Lei Geral de Proteção de Dados Pessoais

O conhecimento atual e tecnologias existentes permitem o acesso a um montante de dados e informação sobre as pessoas nunca antes possíveis. Essa possibilidade auxilia na personalização da experiência de venda das empresas e extração de conhecimento relevante acerca de diversos assuntos. Esse acesso pode configurar, no entanto, invasão de privacidade ou ainda risco de exposição ao armazenar dados pessoais que podem ser vazados.

Conforme Brasil (2018), a LGPD contempla o tratamento realizado com dados pessoais que são informações sobre as pessoas, por pessoa natural ou jurídica do direito público ou privado, a fim de proteger os direitos fundamentais de liberdade e privacidade, e o livre desenvolvimento da personalidade da pessoa. Com algumas exceções, é preciso que as organizações peçam o consentimento das pessoas para tratarem seus dados pessoais, consentimento esse que pode ser aceito, negado ou revogado pela pessoa futuramente.

O tratamento de dados pessoais envolve o proprietário dos dados (chamado de *titular*), os agentes de tratamento (nomeados *controlador* e *operador*) e o *encarregado*, que atua como canal de comunicação entre o controlador, os titulares e a ANPD (*Autoridade Nacional de Proteção de Dados*).

Segundo Brasil (2018), a LGPD pode ser aplicada se o tratamento for feito no Brasil, ou se o objetivo do tratamento for ofertar ou fornecer bens ou serviços ou tratar dados de pessoas localizadas no Brasil, ou caso os dados pessoais do tratamento tenham sido coletados no Brasil, enquanto o titular também estava no Brasil.

A seguir, um quadro mostra a estrutura dessa lei:

Quadro 2 — Estrutura da Lei Geral de Proteção de Dados

(continua)

CAPÍTULO	TEMA	SEÇÕES	ARTIGOS
1	Disposições preliminares	-	1 ao 6

Quadro 2 – Estrutura da Lei Geral de Proteção de Dados

(conclusão)

CAPÍTULO	TEMA	SEÇÕES	ARTIGOS
2	Do tratamento de dados pessoais	I. Dos requisitos para tratamento de dados pessoais II. Do tratamento de dados pessoais sensíveis III. Do tratamento de dados pessoais de crianças e adolescentes IV. Do término do tratamento de dados	7 ao 16
3	Dos direitos do titular	-	17 ao 22
4	Do tratamento de dados pessoais pelo poder público	I. Das regras II. Das responsabilidades	23 ao 32
5	Da transferência internacional de dados	-	33 ao 36
6	Dos agentes de tratamento de dados pessoais	I. Do controlador e do operador II. Do encarregado pelo tratamento de dados pessoais III. Da responsabilidade e do ressarcimento de danos	37 ao 45
7	Da segurança e das boas práticas	I. Da segurança e do sigilo de dados II. Das boas práticas e da governança	46 ao 51
8	Da fiscalização	I. Das sanções administrativas	52 ao 54
9	Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade	I. Da Autoridade Nacional de Proteção de Dados II. Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade	55 ao 59
10	Disposições finais e transitoriais	-	60 ao 65

Fonte: elaborado pela autora com dados extraídos de BRASIL (2018).

5 ANÁLISE TÉCNICA DA LEGISLAÇÃO

O Marco Civil da Internet e a LGPD trazem muitos direitos e controle ao cidadão sobre seus próprios dados tratados em território brasileiro. No entanto, este respaldo jurídico advém de uma postura proativa do titular em defender seu direito, vide a necessidade de entrar com ordem judicial para remoção de conteúdo de provedores de serviços a terceiros do Marco Civil ou cancelar consentimento da LGPD, o que pressupõe uma consciência da legislação e conhecimento do funcionamento da Internet, o que não é maioria e nem predominância na realidade brasileira a julgar pela parcela da população que não concluiu o ensino fundamental, constatando-se que são legislações que precisam ser consideravelmente divulgadas e esclarecidas de maneira didática.

Conforme Brasil (2018, art. 5º, XI), tem-se o conceito de anonimização, que é usar tecnologias disponíveis no momento do tratamento a fim de tornar impossível que esse dado seja associado a uma pessoa. Um dado anonimizado não se trata de um dado pessoal, porém, **dependendo do montante de informação armazenada sobre uma mesma pessoa, é possível deduzir igualmente a quem se refere** através de associações, em outras palavras, conforme excetua o artigo 12, revertendo o processo de anonimização ao qual foram submetidos.

Outra situação em que o cumprimento da LGPD acontece, mas a falta de instrução e educação cibernética do brasileiro afeta a própria participação de seus direitos e deveres é no **momento de dar consentimento de uso de seus dados ao provedor da aplicação ou conexão**, em seu contrato de instalação ou de acesso ao site, em que a enfadonha e aparentemente sem propósito leitura de seus termos longos e em letras minúsculas não convidativas, impulsiona um "*concordo*" para breve deleite do propósito inicial da instalação ou acesso ao site, objetivamente assinando um contrato que não foi lido.

Uma solução para isso é que o governo divulgue informação acessível e de fácil entendimento em meios viáveis e produtivos, e as empresas utilizem de suas habilidades de *marketing* para destacar devidamente as palavras que precisam ser destacadas, ilustrar para capturar a atenção de cerca de poucos segundos para este propósito, para numa primeira tela sem precisar de rolagem o objetivo, a necessidade, a importância, a causa, estarem explícitas, e detalhadas apenas

embaixo necessitando de rolagem, isto tanto para poupar a própria empresa de exaustões judiciais quanto ao próprio utilizador do serviço das mesmas situações.

Conforme recomenda a ABNT (2015, p.34), convém que os provedores de serviços orientem os consumidores sobre como se manter seguro *online.* Tanto a LGPD quanto o Marco Civil trazem em seus artigos a expressão “no âmbito e nos limites técnicos” ao se referir de medidas tecnológicas para realização de uma operação, como tornar indisponível conteúdo infringente (BRASIL, 2014, art. 19 e art. 21), eliminação dos dados pessoais após término de tratamento (BRASIL, 2018, art. 16), tornar dados afetados ininteligíveis para terceiros não autorizados a acessá-los (BRASIL, 2018, art. 48, § 3º). Estas operações dizem respeito aos princípios da segurança da informação, que são a integridade, confidencialidade e disponibilidade.

Tornar indisponível um conteúdo infringente e eliminar dados pessoais após o término de tratamento se refere a disponibilidade da informação. A consideração de que se tenha limites técnicos para a realização desta operação se pauta na redundância e conectividade naturais à Internet. Terceiros com acesso a uma informação podem armazená-las em diferentes dispositivos, impossibilitando ou dificultando o rastreamento para total remoção do conteúdo da Internet.

Tornar dados afetados ininteligíveis para terceiros não autorizados a acessá-los se refere a confidencialidade da informação. Medidas como a criptografia atendem melhor a este objetivo, pois o texto original com o auxílio tecnológico se altera de uma maneira aleatória incompreensível e de muito complexa reversão.

Outro problema observado é a falta de educação digital para todos, ou a falta de divulgação destes projetos e de sua importância, em meio facilmente acessível para todos, tendo em vista que para reivindicar ou fazer valer os direitos em muitas circunstâncias, requer uma ação proativa do cidadão, ação essa respaldada por um conhecimento mínimo em informática, como é o caso de solicitar remoção de conteúdo aos provedores de aplicação em caso de divulgação por terceiros de fotos de nudez, ou revogação de consentimento quanto ao tratamento de dados por uma empresa.

6 DIREITOS E GARANTIAS DIGITAIS DO BRASILEIRO

Existem direitos e garantias digitais que os brasileiros precisam estar conscientes que possuem, para um melhor respaldo jurídico em caso de lesão aos seus dados.

6.1 Direitos e garantias dos usuários no Marco Civil da Internet

Os direitos e garantias definidos no artigo 7º do Marco Civil da Internet foram aqui separados por aqueles que são fundamentais, aquele que depende de requerimento, aqueles referentes ao relacionamento com o responsável pelo tratamento de dados e aqueles que dependem do consentimento.

6.1.1 Direitos e garantias fundamentais

A seguir, estão listados direitos e garantias que podem ser considerados fundamentais, pois são para todos e são uma base geral e não para situações mais específicas:

- “inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação.” (BRASIL, 2014, art. 7º, I);
- “inviolabilidade e sigilo do fluxo de suas comunicações pela Internet, salvo por ordem judicial, na forma da lei.” (BRASIL, 2014, art. 7º, II);
- “inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial.” (BRASIL, 2014, art. 7º, III);
- “não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização.” (BRASIL, 2014, art. 7º, IV);
- “manutenção da qualidade contratada da conexão à Internet.” (BRASIL, 2014, art. 7º, V);
- “acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e.” (BRASIL, 2014, art. 7º, XII);
- "aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.” (BRASIL, 2014, art. 7º, XIII).

6.1.2 Direito e garantia dependente de requerimento

O direito e garantia que depende do requerimento se trata do que solicita exclusão de dados pessoais, conforme a lei, “exclusão definitiva dos dados pessoais que tiver fornecido

> a determinada aplicação de Internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei.” (BRASIL, 2014, art. 7º, X).

6.1.3 Direitos e garantias referentes ao relacionamento com o responsável pelo tratamento de dados

O provedor de conexão à Internet precisa ter como responsabilidade no relacionamento de cliente e provedor a transparência acerca do que envolve o tratamento dos dados do cliente. Seguem dois direitos e garantias acerca desse tema:

- “Informações claras e completas constantes dos contratos

> de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de Internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade.” (BRASIL, 2014, art. 7º, VI);

- "publicidade e clareza de eventuais políticas de uso dos provedores de conexão à Internet e de aplicações de internet.” (BRASIL, 2014, art. 7º, XI);
- Informações

> “claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta, não sejam vedadas pela legislação e estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de Internet.” (BRASIL, 2014, art. 7º, VIII).

6.1.4 Direitos e garantias dependentes do consentimento

Os direitos e garantias dependentes do consentimento são aqueles que tratam da autorização por parte do titular do uso de seus dados pelo provedor, são os que seguem:

- "não fornecimento a terceiros de seus dados pessoais,

> inclusive registros de conexão, e de acesso a aplicações de Internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei.” (BRASIL, 2014, art. 7º, VII);

- "consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais.” (BRASIL, 2014, art. 7º, IX).

6.2 Direitos do titular na Lei Geral de Proteção de Dados Pessoais

Os direitos do titular definidos nos artigos 17 ao 22 da LGPD são aqui separados por aqueles que são fundamentais, aqueles que dependem de requerimento e aqueles acerca da solicitação de revisão de tomada de decisão baseada em tratamento automatizado.

6.2.1 Direitos fundamentais

Considera-se aqui como fundamental os direitos que se referem a todos e são menos específicos, como os que seguem:

- “Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade nos termos desta lei.” (BRASIL, 2018, art. 17º);
- “Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.” (BRASIL, 2018, art. 21º);
- “A defesa dos interesses e dos direitos dos titulares de dados

> poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.” (BRASIL, 2018, art. 22º).

6.2.2 Direitos dependentes de requerimento

Considera-se aqui como dever dependente de requerimento os deveres que pressupõem uma proatividade, que tratam do controle do titular concomitante à transparência por parte de quem realiza o tratamento, como os que seguem:

- “O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:” (BRASIL, 2018, art. 18º);
- “a confirmação da existência de tratamento” (BRASIL, 2018, art. 18º, I);
- “acesso aos dados” (BRASIL, 2018, art. 18º, II);
- “correção de dados incompletos, inexatos ou desatualizados” (BRASIL, 2018, art. 18º, III);
- “anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei” (BRASIL, 2018, art. 18º, IV);
- “portabilidade dos dados a outro fornecedor de serviço ou produto,

> mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial” (BRASIL, 2018, art. 18º, V), portabilidade essa que “não inclui dados que já tenham sido anonimizados pelo controlador.” (BRASIL, 2018, art. 18º, § 7º);

- "eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei” (BRASIL, 2018, art. 18º, VI);
- “informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados” (BRASIL, 2018, art. 18º, VII);
- “informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa” (BRASIL, 2018, art. 18º, VIII);
- “revogação do consentimento, nos termos do § 5º do art. 8º desta Lei” (BRASIL, 2018, art. 18º, IX);
- “O titular dos dados pessoais tem o direito de peticionar

> em relação aos seus dados contra o controlador perante a autoridade nacional” (BRASIL, 2018, art. 18º, § 1º)., direito esse que “também poderá ser exercido perante os organismos de defesa do consumidor.” (BRASIL, 2018, art. 18º, § 8º);

- “O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.” (BRASIL, 2018, art. 18º, § 2º);
- “Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento” (BRASIL, 2018, art. 18º, § 3º)., requerimento esse que “será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.” (BRASIL, 2018, art. 18º, § 5º). Segundo Brasil (2018, art. 18º, § 4º), caso seja impossível adotar imediatamente a provisão requerida, o controlador enviará ao titular resposta em que poderá comunicar que não é agente de tratamento dos dados e indicar o agente sempre que possível, ou indicar as razões de fato ou de direito que impedem a adoção imediata da providência;
- “O responsável deverá informar, de maneira imediata,

  > aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.” (BRASIL, 2018, art. 18º, § 6º);

- Segundo Brasil (2018, art. 19º, I e II), a confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular em formato simplificado imediatamente, ou por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até quinze dias, contado da data do requerimento do titular;
- “Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.” (BRASIL, 2018, art. 19º, § 1º);

- Segundo Brasil (2018, art. 19º, § 2º), o titular escolhe se prefere que as informações e os dados são fornecidos por meio eletrônico (seguro e idôneo para esse fim) ou sob forma impressa;
- “Quando o tratamento tiver origem

> no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.” (BRASIL, 2018, art. 19º, § 3º);

- “A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.” (BRASIL, 2018, art. 19º, § 4º).

6.2.3 Direitos acerca da solicitação de revisão de tomada de decisão baseada em tratamento automatizado

A empresa ou organização pode tratar automaticamente os dados pessoais para realizar definições de perfil, e o titular pode solicitar informações ou revisão sobre esses tratamentos. Seguem os direitos do titular acerca desse tema:

- “O titular dos dados tem direito a solicitar

> a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.” (BRASIL, 2018, art. 20º);

- “O controlador deverá fornecer, sempre que solicitadas,

> informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.” (BRASIL, 2018, art. 20º, § 1º);

- “Em caso de não oferecimento de informações

> de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.” (BRASIL, 2018, art. 20º, § 2º);

7 FALHAS DE SEGURANÇA NO DESENVOLVIMENTO DE APLICAÇÕES

Conforme Cabral e Caprino (2015, p.2), é inviável prever todas as possíveis falhas de segurança, considerando que há necessidade de rápida inovação para participar do mercado.

Segue a lista das *top* dez falhas definidas pela OWASP 2017:

1. **Injeção:** Segundo OWASP (2017, p. 8), falhas de injeção ocorrem quando se faz consultas ou comandos com dados hostis em um espaço para consulta normal, para executar comandos não esperados nem tratados pelo programador da aplicação, ou ver dados sem autorização;
2. **Quebra de autenticação:** A quebra de autenticação, segundo OWASP (2017, p.8), acontece quando as funções da aplicação que tratam da autenticação e gestão de sessões estão implementadas incorretamente, permitindo que um atacante possa ter acesso às senhas, chaves, *tokens* de sessão, ou ainda assumir a identidade de outros usuários;
3. **Exposição de dados sensíveis:** A exposição de dados sensíveis está muito ligada ao escopo que a Lei Geral de Proteção de Dados Pessoais trata. Conforme OWASP (2017, p.8), quando os dados sensíveis das pessoas não são adequadamente protegidos, os atacantes podem roubá-los ou modificá-los. Dados sensíveis precisam estar criptografados quando armazenados ou em trânsito, precisam também de precauções especiais quando em contato com o navegador *web;*
4. **Entidades externas de XML (XXE):** Falhas de entidades externas de XML, segundo OWASP (2017, p.8) acontecem devido a muitos processadores de XML mais antigos ou mal configurados avaliarem referências a entidades externas dentro dos documentos XML;
5. **Quebra de controle de acessos:** A quebra de controle de acessos, segundo OWASP (2017, p.8), acontece quando as restrições sobre o que cada pessoa autenticada está autorizada a fazer não são corretamente verificadas, os atacantes podem assim conseguir acesso a funcionalidades ou dados aos quais não é autorizado;
6. **Configurações de segurança incorretas:** Configurações de segurança incorretas, segundo OWASP (2017, p.8), normalmente são devido a configurações padrão inseguras, incompletas ou *ad hoc (*sem padronização,

documentação e controle regulatório), armazenamento na nuvem sem restrição de acesso, cabeçalhos *Hypertext Transfer Protocol* (HTTP) mal configurados ou mensagens de erro com informações sensíveis;

7. **Cross-site scripting (XSS):** A falha de *cross-site scripting* ocorre, segundo OWASP (2017, p.8), quando uma aplicação inclui dados não confiáveis numa nova página *web* sem que tenha validação ou filtragem apropriadas, ou quando atualiza uma página *web* existente com dados enviados por um usuário através de uma API do navegador que possa criar *JavaScript*. O XSS permite que atacantes possam executar scripts no navegador da vítima, os quais podem roubar sessões do usuário, descaracterizar *websites* ou redirecionar o usuário para *websites* maliciosos;
8. **Desserialização insegura:** A falha de desserialização insegura, para OWASP (2017, p.8), normalmente leva à execução remota de código. Pode também ser usada para realizar ataques como os de repetição, injeção e elevação de privilégios;
9. **Utilização de componentes vulneráveis:** Conforme OWASP (2017), o abuso de um componente vulnerável pode levar a uma séria perda de dados, ou no controle completo de um servidor. Aplicações e APIs que usem componentes com vulnerabilidades conhecidas podem enfraquecer as defesas da aplicação possibilitando ataques;
10. **Registro e monitoração insuficientes:** “O registro e monitorização insuficientes,

> em conjunto com uma resposta a incidentes inexistente ou insuficiente permite que os atacantes possam abusar do sistema de forma persistente, que o possam usar como entrada para atacar outros sistemas, e que possam alterar, extrair ou destruir dados.” (OWASP, 2017, p.8).

8 MECANISMOS DE PREVENÇÃO NO DESENVOLVIMENTO DE APLICAÇÕES

Existem mecanismos que ajudam a impedir que ameaças explorem as falhas de segurança e que aconteçam danos aos dados. Seguem neste capítulo alguns dos mecanismos propostos pela OWASP 2017 para as dez falhas previamente listadas:

1. **Para a Injeção:** Para OWASP (2017, p.9), para detectar se a aplicação é vulnerável a injeções, pode-se se fazer revisão de código e testes automáticos que cubram todos os parâmetros, cabeçalhos, URL, *cookies*, JSON, SOAP e dados de entrada para XML;
2. **Para a quebra de autenticação:** Para prevenir que ameaças quebrem a autenticação, segundo OWASP (2017, p.10), é importante implementar autenticação multifatores para prevenir ataques automáticos de *credential stuffing*, força bruta e reutilização de credenciais roubadas;
3. **Para a exposição de dados sensíveis:** Segundo OWASP (2017, p.11), para proteger os dados sensíveis de exposição, é importante que os dados processados, armazenados ou transmitidos por uma aplicação sejam identificados e classificados. Não armazenar dados sensíveis sem necessidade, e garantir que todos os dados armazenados são criptografados;
4. **Para as entidades externas de XML (XXE):** Para OWASP (2017, p.12), algumas das formas de se proteger de entidades externas de XML são: treinar os programadores, optar por um formato mais simples como o JSON e corrigir ou atualizar todos os processadores e bibliotecas de XML usados pela aplicação, dependências ou sistema operacional;
5. **Para a quebra de controle de acessos:** O controle de acessos só é efetivo, segundo OWASP (2017, p.13), se realizado por código confiável processado no servidor ou pelas APIs em arquiteturas *serverless.* São exemplos o registro de falhas de controle de acesso junto ao alerta aos administradores sempre que necessário e a invalidação de JSON *Web* Tokens (JWT) após desconectar do sistema (*logout*);
6. **Para configurações de segurança incorretas:** As configurações de segurança incorretas podem ser prevenidas, segundo OWASP (2017, p. 14), instalando por exemplo a plataforma mínima necessária, sem funcionalidades desnecessárias, realizando a gestão das correções e um processo

automático para verificar a eficácia das configurações e definições em todos os ambientes;

7. **Para cross-site scripting(XSS):** Para prevenir o *cross-site scripting*, segundo OWASP (2017, p.15), é necessário separar os dados não confiáveis do conteúdo ativo do navegador, por exemplo, através do uso de frameworks que ofereçam nativamente proteção para XSS, como as versões mais recentes de *Ruby on Rails* e ReactJS;
8. **Para desserialização insegura:** Conforme a OWASP (2017, p.16), a única forma segura de utilizar serialização pressupõe que não são aceitos objetos serializados de fontes não confiáveis, e que só são permitidos tipos de dados primitivos. De outra maneira, para se proteger pode-se fazer, por exemplo, implementar verificações de integridade como a assinatura digital nos objetos serializados, ou isolar e executar o código que desserializa em ambientes de baixo privilégio;
9. **Para utilização de componentes vulneráveis:** Para a prevenção da utilização de componentes vulneráveis, o processo de gestão de correções e atualizações deve, segundo OWASP (2017, p.17), remover dependências, funcionalidades, componentes, arquivos e documentações desnecessários, ou ainda, obter componentes apenas de fontes oficiais e de ligações seguras, preferindo pacotes assinados para mitigar componentes modificados ou maliciosos;
10. **Para registro e monitoração insuficientes:** Para prevenir o registro e monitoração insuficientes, segundo OWASP (2017, p.18), dependendo do risco inerente à informação é preciso, por exemplo, garantir que as transações mais críticas têm uma trilha de auditoria dos registros com controles de integridade para prevenir adulteração ou remoção, e definir processos de monitoração e alerta capazes de detectar atividade suspeita e resposta em tempo oportuno.

9 CRIMES DIGITAIS E SUAS PENALIDADES

Segundo o CNJ (2018), os crimes mais comuns cometidos na internet são calúnia, difamação, injúria, injúria qualificada, ameaça, falsa identidade. Este capítulo foi escrito usando como fonte o artigo do CNJ, a lei do Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais. A seguir são enumerados seis crimes e suas penalidades, conforme o CNJ:

1. Calúnia:

> "Atribuir a alguém a autoria de um fato definido em lei como crime quando se sabe que essa pessoa não cometeu crime algum – Trata-se do crime Calúnia, previsto no artigo 138 do Código Penal e cuja pena pode variar de seis meses a dois anos de prisão além do pagamento de multa." (CNJ, 2018);

2. Difamação:

> "Atribuir a alguém fato ofensivo à sua reputação ou honra (por exemplo, espalhar boatos que prejudiquem a reputação da pessoa na empresa em que ela trabalhe ou na comunidade em que ela vive) – Trata-se do crime de Difamação, previsto no artigo 139 do Código Penal e cuja pena pode variar de três meses a um ano de prisão além do pagamento de multa." (CNJ, 2018);

3. Injúria:

> "Ofender a dignidade de alguém (por meio de insultos, xingamentos, humilhações etc) – Trata-se do crime de Injúria, previsto no artigo 140 do Código Penal e cuja pena pode variar de um a seis meses de prisão além do pagamento de multa." (CNJ, 2018);

4. Injúria qualificada:

> "Ofender a dignidade de alguém utilizando-se de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência – Trata-se do crime de Injúria qualificada, previsto no parágrafo terceiro do artigo 140 do Código Penal (é um tipo mais grave de injúria), cuja pena pode variar de um a três anos de prisão além do pagamento de multa." (CNJ, 2018);

5. Ameaça:

> “Ameaçar alguém de causar-lhe mal injusto e grave por meio de palavras (faladas ou escritas), gestos, ou qualquer outro meio simbólico (por exemplo, ameaçar uma pessoa dizendo que vai agredir a ela ou alguém da família dela) – Trata-se do crime de Ameaça, previsto no artigo 147 do Código Penal e cuja pena pode variar de um a seis meses de prisão além do pagamento de multa.” (CNJ, 2018);

6. Falsa Identidade:

> “Mentir sobre sua identidade ou sobre a identidade de outra pessoa para obter alguma vantagem indevida ou para causar dano a alguém – Trata-se do crime de Falsa Identidade, previsto no artigo 307 do Código Penal e cuja pena pode variar de três meses a um ano de prisão além do pagamento de multa.” (CNJ, 2018).

Conforme o CNJ (2018), seguem cinco dos crimes previstos na Lei Carolina Dieckmann (Lei 12.737/2012) e inclusos no Código Penal (artigo 154-A e art. 298) e suas penalidades:

1. *“Violar*

> sistema de segurança (senhas, travas, sistemas de criptografia etc) para invadir computador, rede, celular ou dispositivo similar sem autorização (independente de estar ou não conectado à internet) para obter, adulterar ou destruir dados ou informações ou, ainda, para instalar vírus ou vulnerabilidades no dispositivo – a pena pode variar de três meses a um ano de prisão além do pagamento de multa.” (CNJ, 2018);

2. *“Se, ao cometer o crime definido acima, o criminoso obter*

> conteúdo de comunicações eletrônicas privadas (senhas, conteúdo de e-mails, mensagens, fotos etc), segredos comerciais ou industriais, informações sigilosas ou o controle remoto não autorizado do dispositivo invadido o crime é considerado mais grave – neste caso, a pena pode variar de seis meses a dois anos de prisão além do pagamento de multa.” (CNJ, 2018);

3. *“Se, depois de obter*

> conteúdo sem autorização (fotos, senhas, e-mails, mensagens etc) o criminoso divulgar, vender ou transmitir os dados ou informações

> obtidas a qualquer pessoa – neste caso, aumenta-se a pena de um a dois terços.” (CNJ, 2018);

4. *“Produzir, oferecer, distribuir, vender ou difundir*

> dispositivo ou programa de computador que sirva para cometer o crime definido acima (ou seja, criar ou vender programas de roubo de senhas etc) – a pena pode variar de três meses a um ano de prisão além do pagamento de multa.” (CNJ, 2018);

5. *“Falsificar cartão de crédito ou débito* – a pena pode variar de um a cinco anos de prisão além do pagamento de multa (art. 298 CP).” (CNJ, 2018).

Também é crime, conforme Brasil (1940), o que está definido no artigo 266, § 1º e § 2º, onde é dito que interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento possui pena de detenção, de um a três anos, e multa, incorrendo da mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento, sendo dobradas as penas se o crime for cometido por ocasião de calamidade pública.

Quanto as penalidades previstas na LGPD, conforme Brasil (2018, art. 52º), os agentes de tratamento de dados que infringirem às normas da lei, ficam sujeitos às seguintes nove sanções administrativas aplicáveis pela autoridade nacional:

1. “Advertência, com indicação de prazo para adoção de medidas corretivas” (BRASIL, 2018, art. 52º, I);
2. “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” (BRASIL, 2018, art. 52º, II);

3. “Multa diária, observado o limite total a que se refere o inciso II” (BRASIL, 2018, art. 52º, III);
4. “Publicização da infração após devidamente apurada e confirmada a sua ocorrência” (BRASIL, 2018, art. 52º, IV);
5. “Bloqueio dos dados pessoais a que se refere a infração até a sua regularização” (BRASIL, 2018, art. 52º, V);

6. “Eliminação dos dados pessoais a que se refere a infração” (BRASIL, 2018, art. 52º, VI);
7. “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” (BRASIL, 2018, art. 52º, X);

8. “Suspensão do exercício da atividade de tratamento de dados pessoais a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período” (BRASIL, 2018, art. 52º, XI);
9. “Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.” (BRASIL, 2018, art. 52º, XII).

O Marco Civil da Internet segundo Brasil (2014, art. 12º) estabelece como penalidades às infrações às normas previstas nos artigos 10 e 11, as seguintes quatro sanções, aplicadas de forma isolada ou cumulativa:

1. “Advertência, com indicação de prazo para adoção de medidas corretivas” (BRASIL, 2014, art. 12º, I);
2. “Multa

> de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção” (BRASIL, 2014, art. 12º, II);

3. “Suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou” (BRASIL, 2014, art. 12º, III);
4. “Proibição de exercício das atividades que envolvam os atos previstos no art. 11” (BRASIL, 2014, art. 12º, IV).

10 ANÁLISES DE CASOS REAIS

Neste capítulo será realizada uma análise técnica e crítica sobre as causas de falhas ocorridas nas situações do cotidiano em que pessoas e/ou empresas podem estar sendo vítimas de ataques virtuais.

10.1 Uma pessoa mal intencionada tenta acessar a conta pessoal de outra em uma aplicação

Na situação em que uma pessoa mal intencionada tenta acessar a conta de outra em uma aplicação, o atacante tentará acertar a combinação de ID e senha a fim de ter acesso aos privilégios e dados relativos a conta atacada.

Tanto o proprietário da conta como o servidor da aplicação podem estabelecer mecanismos protetivos para tampar as brechas.

O servidor pode definir limite de tentativas erradas para realizar bloqueio de tentativas, ou ainda, enviar *e-mail* ao proprietário da conta informando sobre acesso em endereço ou dispositivo diferente, permitindo o bloqueio ou permissão desse acesso; pode estabelecer exigência de senha forte para efetuar criação de contas.

O proprietário da conta precisa compreender que senhas não devem ser compartilhadas ou anotadas em lugares pouco seguros, bem como ser proativo em buscar saber se porventura suas credenciais de acesso já foram vazadas. O *website* "*haveIbeenpwned?*" permite ver se isso já ocorreu, por exemplo. Assim, se o usuário utiliza da mesma credencial que já foi vazada me algum momento, é simples de ter sua conta violada.

10.2 Uma pessoa mal intencionada envia e-mails disfarçados de autênticos para obter informações da vítima

Uma pessoa mal intencionada que deseja obter informações da vítima pode se passar por alguém confiável para solicitar informações. Pode acontecer de um *e-mail* aparentemente autêntico e de fonte respeitada ser, na verdade, um método enganoso usado por atacantes para obter informações da vítima e até mesmo realizar ataques de engenharia social com as informações fornecidas.

Nesta situação, é necessário que as pessoas desconfiem de *e-mails* que receberem, pois dizer que considerar apenas as fontes conhecidas já é uma afirmação com brecha, tendo em vista que atacantes se passam por fontes conhecidas. Ao clicar em um *link* de *e-mails* desse tipo, a vítima provavelmente será

direcionada para um *website* similar ao original na aparência, mas, na verdade, quem está recebendo os dados inseridos é o atacante.

Dificilmente uma pessoa com pouco conhecimento informático vai deduzir ou intuir que o *e-mail* do remetente não é o oficial da empresa, mesmo porque a pessoa mal pode ter ideia de um padrão de nomenclatura, e considerar um "*@gmail*" ou "*@outlook*" verídico para endereço virtual de um banco de grande porte. Assim, ter essas noções de segurança só é possível com a educação e, portanto, essa precisa ser estimulada e acessível para todos.

10.3 Uma pessoa solicita um código enviado por mensagem de celular ou por e-mail para concluir um processo qualquer

As aplicações podem enviar códigos para o *e-mail* ou por mensagem de celular para alteração de senha ou recuperação de conta, esses aspectos são muito pessoais e dizem respeito apenas a pessoa proprietária da conta, nunca se deve informar esses códigos a uma pessoa para concluir qualquer processo comum. Informar códigos assim pode resultar em perda de conta, *WhatsApp* clonado, e diversas situações estressantes e propícias a prejuízos financeiros e sociais.

10.4 Uma pessoa faz download de arquivo ou aplicação contaminado com malware

Arquivos e aplicações disponibilizados para *download* na Internet podem estar ou não contaminados com *malwares*.

O servidor da aplicação pode prover proteção ao realizar verificações automáticas para cada arquivo que for feito *upload*; fornecer teclado virtual para inserção de senha, para dessa forma contornar *keyloggers*.

Já o usuário, necessita ter em seu dispositivo um antivírus, *antimalware* e *firewall* ativo, no mínimo, para barrar os excessos. Precisa manter atualizado seu dispositivo e programas instalados, para que as correções de falhas pelos desenvolvedores sejam baixadas. Também evitar baixar arquivos de fontes desconhecidas, e aqui entra novamente a necessidade de educação digital, pois é uma boa prática pesquisar sobre a reputação de um site antes de baixar arquivos e aplicações dele, e buscar discernir uma avaliação verdadeira de uma falsa. Isso pode ser feito analisando se há similaridade nas avaliações, se foram feitas por perfil de rede social, a quantidade de curtidas com a relevância do que foi escrito, estilo de escrita dos comentários, dentre outros.

Nunca se deve baixar arquivos recebidos por *e-mail* de pessoas desconhecidas.

Essas são situações que requerem uma análise precedendo o objetivo, que é baixar o arquivo ou aplicação e utilizá-lo. Sem educação digital, uma pessoa pode nem mesmo ter ideia da necessidade de uma postura preventiva.

Para evitar espionagem por câmera de dispositivo, é interessante que a câmera física seja coberta. Existem atualmente objetos com este objetivo, tanto para celular quanto para computador ou *notebook*, diferente de outrora em que um adesivo era o recurso viável a ser usado, mas não é prático por perder a cola se for necessário remover e, novamente, colocar.

11 CONCLUSÃO

Com a realização desta pesquisa, foi possível constatar que a legislação brasileira melhorou muito no que concerne os crimes digitais. Muitos dos crimes digitais tendem a ser os mesmos crimes já conhecidos fora da rede, com o adendo de que o meio em que ocorrem é virtual, observação essa que não reduz as diferenças entre os crimes, pelo contrário, a Internet proporciona um alcance exponencial de divulgação e compartilhamento, agravando crimes que fora dela não alcançariam tal proporção em tão pouco tempo.

A maior necessidade de melhoria observada é a questão da educação pública acerca da legislação digital e do funcionamento da Internet.

Para os dados efetivamente serem protegidos em nível conforme a legislação brasileira estabelece, é crucial que o zelo pela integridade, confidencialidade, disponibilidade e autenticidade dos dados seja um objetivo constante e diário por parte de todos que realizam tratamento de dados pessoais.

REFERÊNCIAS

ABNT. **Norma ABNT NBR ISO/IEC 27002**. 2005. Disponível em: <http://www.fieb.org.br/download/senai/NBR_ISO_27002.pdf>. Acesso em: 28 jun. 2019.

ABNT. **Norma ABNT NBR ISO/IEC 27032**. 2015.

ABNT. **Norma ABNT NBR ISO/IEC 27005**. 2019.

AVAST. **O que é "credential stuffing" e por que minha câmera de segurança inteligente é vulnerável?** Avast Blog, 2019. Disponível em: <https://blog.avast.com/pt-br/credential-stuffing-and-web-cams>. Acesso em: 28 mai. 2021.

BACKUP. *In:* PRIBERAM, **Dicionário Priberam da Língua Portuguesa**. Disponível em: <https://dicionario.priberam.org/backup>. Acesso em: 19 jul. 2021.

BRASIL. **Decreto-lei n. 2.848, de 7 de dezembro de 1940**. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-lei/Del2848compilado.htm>. Acesso em: 28 mai. 2021.

BRASIL. **Decreto n. 7.962, de 15 de março de 2013**. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Brasília, DF: Presidência da República, [2013]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm>. Acesso em: 21 jun. 2019.

BRASIL. **Decreto n. 8.771, de 11 de Maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF: Presidência da República, [2016] Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm >. Acesso em: 5 jan. 2020.

BRASIL. **Decreto n. 8.777, de 11 de Maio de 2016**. Institui a Política de Dados Abertos do Poder Executivo federal. Brasília, DF: Presidência da República, [2016]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8777.htm >. Acesso em: 5 jan. 2020.

BRASIL. **Decreto n. 9.637, de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília, DF: Presidência da República, [2018]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm>. Acesso em: 28 jun. 2019.

BRASIL. **Decreto n. 9.854, de 25 de Junho de 2019**. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas. Brasília, DF: Presidência da República, [2019]. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9854.htm>. Acesso em: 19 jul. 2021.

BRASIL. **Lei n. 9.507, de 12 de novembro de 1997**. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm >. Acesso em: 5 jan. 2020.

BRASIL. **Lei n. 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm >. Acesso em: 5 jan. 2020.

BRASIL. **Lei n.12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 21 jun. 2019.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 21 jun. 2019.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da

Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 21 jun. 2019.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação** / Tribunal de Contas da União. – 4. ed. – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012. Disponível em: <https://portal.tcu.gov.br/biblioteca-digital/cartilha-de-boas-praticas-em-seguranca-da-informacao-4-edicao.htm>. Acesso em: 22 set. 2019.

CABRAL, C.; CAPRINO, W. **Trilhas em segurança da informação - caminhos e ideias para a proteção de dados** / Carlos Cabral, Willian Caprino, organizadores. Rio de Janeiro: Brassport, 2015.

CERT. **Cartilha de Segurança para Internet, versão 4.0** / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf> Acesso em: 24 set. 2019.

CIBERCRIME. *In:* PRIBERAM, **Dicionário Priberam da Língua Portuguesa**. Disponível em: <https://dicionario.priberam.org/cibercrime> Acesso em: 23 jul. 2021.

FONTES, Eduardo. **Segurança da informação: o usuário faz a diferença** / Edison Fontes. - São Paulo: Saraiva, 2006.

IBGE. Pesquisa Nacional por Amostra de Domicílios Contínua (Pnad), realizada em 2017 pelo IBGE sobre Tecnologia da Informação e Comunicação: **Internet chega a três em cada quatro domicílios do país**. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/23445-pnad-continua-tic-2017-Internet-chega-a-tres-em-cada-quatro-domicilios-do-pais>. Acesso em: 5 jun. 2019.

CNJ. **Crimes digitais: quais são, quais leis os definem e como denunciar**. [S.l.]; Justificando, 2018. Disponível em: <https://www.justificando.com/2018/06/25/crimes-digitais-quais-sao-quais-leis-os-definem-e-como-denunciar/>. Acesso em: 19 jul. 2021.

MALENKOVICH, Serge. **O que é um Ataque Man-in-the-Middle?** [S.l.]: Kaspersky daily, 2013. Disponível em: <https://www.kaspersky.com.br/blog/what-is-a-man-in-the-middle-attack/462/>. Acesso em: 19 jul. 2021.

OWASP. OWASP Top 10 - 2017: **The Ten Most Critical Web Application Security Risks (versão portuguesa)**. Disponível em: <https://wiki.owasp.org/images/0/06/OWASP_Top_10-2017-pt_pt.pdf>. Acesso em: 13 fev. 2021.

PINHEIRO, Patrícia Peck. **Direito Digital**. 6. ed. rev., atual. E ampl. - São Paulo: Saraiva, 2016.

SAFERNET. **Número de atendimentos por tópico da conversa em 2018**.

Disponível em: <https://helpline.org.br/indicadores/>. Acesso em: 27 jun. 2019.