UNIVERSIDADE SANTA CECÍLIA
FACULDADE DE CIÊNCIAS EXATAS, ENGENHARIAS E ARQUITETURA
SISTEMAS DE INFORMAÇÃO

GABRIEL OLIVEIRA DE LIMA
IVO PRADO PEREIRA FILHO
JOÃO VITOR FERNANDES LIMA
LEON DENNIS SOARES DE LIRA
LEONARDO DOS SANTOS GOMES DA SILVA

VAZAMENTO DE DADOS PESSOAIS DE PESSOAS FÍSICAS

Santos – SP
Junho/2022

UNIVERSIDADE SANTA CECÍLIA
FACULDADE DE CIÊNCIAS EXATAS, ENGENHARIAS E ARQUITETURA
SISTEMAS DE INFORMAÇÃO

GABRIEL OLIVEIRA DE LIMA
IVO PRADO PEREIRA FILHO
JOÃO VITOR FERNANDES LIMA
LEON DENNIS SOARES DE LIRA
LEONARDO DOS SANTOS GOMES DA SILVA

VAZAMENTO DE DADOS PESSOAIS DE PESSOAS FÍSICAS

Monografia apresentada à disciplina de "Trabalho de Conclusão de Curso II – TCC II", para fins de avaliação final.
Orientador: Prof. Me. Luiz Antonio Ferraro Mathias.
Coorientadora: Profa. Me. Ana Carolina Caetano Senger.

Santos – SP
Junho/2022

GABRIEL OLIVEIRA DE LIMA
IVO PRADO PEREIRA FILHO
JOÃO VITOR FERNANDES LIMA
LEON DENNIS SOARES DE LIRA
LEONARDO DOS SANTOS GOMES DA SILVA

VAZAMENTO DE DADOS PESSOAIS DE PESSOAS FÍSICAS

Trabalho de Conclusão de Curso apresentado como exigência final para obtenção do título de Bacharel em Sistemas de Informação à Faculdade de Ciências Exatas, Engenharias e Arquitetura da Universidade Santa Cecília.

Data da aprovação: 14/07/2022 APROVADO (X) REPROVADO ( )

Banca Examinadora

_____
Prof. Me. Luiz Antonio Ferraro Mathias

_____
Profa. Me. Ana Carolina Caetano Senger

_____
Prof. Me. Claudio Ferreira de Carvalho

_____
Prof. Me. José Avelino dos Santos Moura

DEDICATÓRIA

Aos amigos e familiares que de alguma forma contribuíram seja por meio de conhecimento ou por incentivo moral para que conseguíssemos concluir esta importante e árdua etapa do curso.

AGRADECIMENTOS

Agradecemos inicialmente a Deus pelas nossas vidas e por ter nos auxiliado a vencer todos os obstáculos que tivemos durante o desenvolvimento deste trabalho.

Aos nossos amigos e familiares que de alguma forma contribuíram e nos incentivaram para que conseguíssemos concluir este trabalho.

Ao nosso orientador Luiz Antonio Ferraro Mathias e a nossa coorientadora Ana Carolina Caetano Senger por toda a instrução que nos foi dada não só do decorrer do curso, mas também durante toda a elaboração deste trabalho afim de que fosse feito da melhor forma possível e atendendo a todas as normas necessárias.

Agradecemos também todos aqueles que contribuíram direta ou indiretamente para a realização deste trabalho.

Agradecemos aos nossos colegas estes que convivemos intensamente durante todo o curso e na elaboração deste trabalho.

EPÍGRAFE

A nossa privacidade está sendo atacada em várias frentes.

Tim Cook, CEO da Apple.

RESUMO

Nos dias atuais, diante do cenário altamente tecnológico, vazamentos de dados são cada vez mais comuns no mundo todo, tanto entre empresas como entre indivíduos. A tecnologia está em todo lugar e todas as pessoas estão conectados de alguma maneira, e desta forma, é quase impossível que alguém não tenha informado algum dado por meio da internet, de maneira voluntária ou não. O trabalho tem como objetivo contribuir para o conhecimento já existente sobre o tema, bem como informar assuntos relevantes a qualquer área que tenha contato direto ou indireto com a tecnologia. Essas metas são cumpridas por meio da exposição de tópicos relevantes ao assunto, como a exposição de situações e acontecimentos que resultam em vazamentos de dados, bem como a recomendação de métodos e soluções de como se pode evitar ou mitigar o vazamento de informações, problema esse que tem se consolidado como uma das principais ameaças à segurança da informação. Para tais fins, a partir da pesquisa bibliográfica, feita por meio de artigos e notícias relevantes ao tema, uma contextualização sobre a importância da proteção dos dados, bem como uma discussão acerca das leis que tornam isso possível é feita nos primeiros tópicos, onde em seguida há uma discussão sobre a atual situação da proteção dos dados pessoais no Brasil e no mundo, apresentando em seguida as causas e efeitos de vazamentos de dados, terminando então com a proposta de soluções e recomendações de segurança, tanto para empresas como para pessoas físicas. De acordo com o presente trabalho, fica claro que muitos países dispõem de uma sólida base para a proteção de dados, pela forma de leis e utilização de boas práticas, mas ainda assim, há muitas medidas a serem tomadas na questão da proteção dos dados no mundo, principalmente no Brasil, que agora dispõe de uma Lei Geral de Proteção de Dados (LGPD), mas que não está sendo muito bem cumprida e regulamentada por todas as empresas que lidam com as informações de seus usuários, visto que o Brasil é um dos países que sofreu e mais sofre com vazamentos de dados. Por outro lado, pode-se chegar à conclusão de que nem todos os usuários de serviços online têm noção ou se importam com a segurança de suas contas, visto que fora identificado que muitas senhas de diversos serviços no mundo consistem em nomes pessoais ou simples combinações do teclado, como “qwerty” ou “123456”.

PALAVRAS-CHAVE: Leis de Proteção de Dados; Prevenção de vazamentos;

Vazamento de dados.

ABSTRACT

In today's highly technological scenario, data leaks are increasingly common around the world, both among companies and individuals. Technology is everywhere and everyone is connected in some way, and thus, it is almost impossible that someone has not informed some data through the Internet, voluntarily or not. This work aims to contribute to the existing knowledge on the subject, as well as to inform relevant issues to any area that has direct or indirect contact with technology. These goals are met through the exposure of topics relevant to the subject, such as the exposure of situations and events that result in data leakage, as well as the recommendation of methods and solutions on how to avoid or mitigate information leakage, a problem that has been consolidated as one of the main threats to information security. To these ends, based on a bibliographical research, made through articles and news relevant to the theme, a contextualization about the importance of data protection, as well as a discussion about the laws that make this possible is made in the first topics, where next there is a discussion about the current situation of personal data protection in Brazil and in the world, then presenting the causes and effects of data leakage, ending then with the proposal of solutions and security recommendations, both for companies and individuals. According to this work, it is clear that many countries have a solid foundation for data protection, by the form of laws and use of best practices, but still, there are many measures to be taken on the issue of data protection in the world, especially in Brazil, which now has a General Law of Data Protection (LGPD – Lei Geral de Proteção de Dados), but it is not being very well complied with and regulated by all companies that deal with the information of their users, since Brazil is one of the countries that has suffered and suffers most from data leaks. On the other hand, one can conclude that not all users of online services are aware or care about the security of their accounts, since it was identified that many passwords for various services in the world consist of personal names or simple keyboard combinations such as "qwerty" or "123456".

KEYWORDS: Data Protection Laws; Data Leak Prevention; Data Leaks.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

Ao início do século 21, os volumes de dados armazenados e coletados por diversos serviços conectados à rede não param de crescer, de maneira exponencial. Dados define-se como valores concedidos a algo, porém não são apenas valores numéricos, os dados podem conter qualquer tipo de informação.

Um vazamento de dados acontece quando informações confidenciais de pessoas ou empresas são expostas sem a sua permissão. CPF, telefone, endereço, senhas diversas e dados bancários são apenas alguns exemplos de dados que podem ser vazados na internet.

Com tudo, como os dados são vazados, salienta-se que os motivos por trás disso acontecem por diversas maneiras, como o uso de *spyware*, *malware*, por meio de *phishing* e entre outros ataques cibernéticos que vazem dados. Esses malwares infectam o computador por meio de arquivos baixados da internet, links, e-mails ou pela rede.

O malware, quando infecta uma máquina ele vai em busca de outras máquinas através da rede, caso haja outra máquina que contenha falhas como a ausência de firewall e antivírus, o vírus irá infectar outras máquinas até ele ser eliminado, mas enquanto o malware está na sua máquina, ele vai roubar e vazar todos os seus dados disponíveis e sem proteção.

No geral, os dados são roubados para serem vendidos na internet, com isso poderão ser expostos na *deep web* ou o próprio hacker irá utilizar esses dados para benefício próprio. O domínio de contas e informações pessoais pode permitir muitos outros golpes, como roubo de identidade, uso indevido de cartões de crédito, entre outros crimes (SANTOS, 2020). A metodologia a ser empregada no projeto de pesquisa consiste em revisão bibliográfica, como também a aplicação de estudos de casos que apresentam o emprego da LGPD, leis de proteção de dados de outros países, a menção de notórios vazamentos e boas práticas de prevenção de vazamentos para pessoas físicas e jurídicas.

O trabalho foi dividido em sete capítulos elaborados com base em material coletado em pesquisas, notícias, artigos científicos, legislações nacionais e estrangeiras

relevantes ao tema. O primeiro capítulo do trabalho tratará da relevância em se investir na privacidade de dados.

Em seguida, o segundo capítulo abordará o atual tema da LGPD - Lei Geral de Proteção de Dados, lei brasileira mais recente sobre o tema, onde será demonstrado um resumo das leis, suas aplicações, finalidades e afins. Será apresentado também a situação das leis de proteção de dados no Brasil e em outros países, como a Índia. O capítulo descreve que as leis brasileiras de proteção de dados são extremamente importantes, mas muitas empresas não se comprometem a seguirem os valores e regras delas, causando uma situação em que os sistemas do país acabam tendo seus dados comprometidos, principalmente aqueles que funcionam em serviço do sistema público.

A seguir, o quarto capítulo trata da causa (origem) e efeito (consequência) dos vazamentos de dados, trazendo consigo informações sobre técnicas aplicadas em tais situações, como o SQL Injection.

Posteriormente, o quinto capítulo traz um estudo de caso sobre o tema, trazendo consigo exemplos de notórios vazamentos de dados. Imediatamente, o sexto capítulo trata de boas práticas de prevenção de vazamentos, É exposto também práticas de segurança ao se navegar pela internet. E por fim, o último tópico trata de soluções de mercado para mitigar vazamentos.

2 A IMPORTÂNCIA DA PRIVACIDADE DE DADOS

Atualmente, a privacidade dos dados pessoais é uma preocupação, tanto para os clientes, usuários, parceiros e colaboradores, como para a própria empresa, principalmente, após a Lei Geral da Proteção de Dados (LGPD) ter entrado em vigor. Muitas empresas investem na segurança "física" de seus estabelecimentos e filiais, investindo suas economias com guardas, câmeras, portas de segurança com senhas ou reconhecimento facial, dentre outros métodos físicos de segurança, para que não corram o risco de serem invadidas por criminosos, como também para evitar danos e perdas em geral, mas com o crescimento da Tecnologia da Informação (T.I), e as informações sendo armazenadas dentro de computadores e servidores, também é de suma importância investir na segurança digital, visto que a tecnologia facilitou a violação da privacidade de dados, como também, a transferência de informações e dados para as mãos erradas.

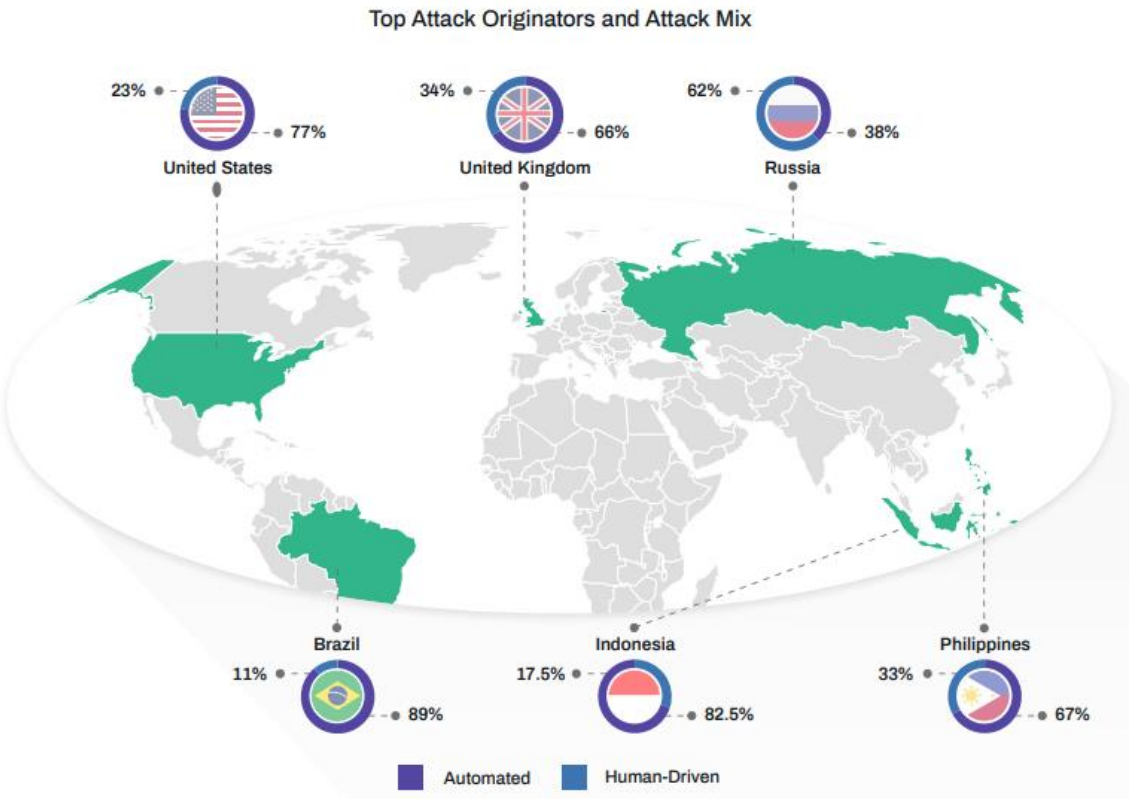
A privacidade e segurança de dados é extremamente importante, pois existem inúmeros tipos de informações que ficam armazenadas dentro dos servidores de empresas, organizações e multinacionais. Informações sensíveis e valiosas que não podem, de jeito nenhum, cair nas mãos de terceiros, ou isso poderia causar inúmeras consequências, para os clientes da empresa, parceiros, colaboradores, e para a própria empresa ou organização, podendo comprometer sua reputação, causar transtornos, e gerar multas milionárias, com esses sendo uns dos principais motivos no qual é importante investir na segurança e proteção de dados e informações.

Há de exemplo as empresas do setor bancário, que possuem informações pessoais e sensíveis armazenadas em seus bancos de dados, como nomes completos, endereços, telefones, informações de cartões e informações financeiras de seus clientes.

E por mais que seja um avanço tecnológico poder coletar dados e os deixar salvos e armazenados corretamente, ainda é necessário para as organizações ter muito cuidado ao gerenciar os dados. Ainda mais tendo noção de que no Brasil, ataques cibernéticos acontecem com cada vez mais frequência, as empresas precisam investir cada vez mais, para manterem seguros seus sistemas, dados de clientes, colaboradores, parceiros, fornecedores e informações financeiras, como movimentações e investimentos, pois, segundo o relatório *Fraud & Abuse Report* da Arkose Labs, o Brasil permaneceu no ranking dos cinco países mais afetados por fraudes digitais ainda no primeiro trimestre de 2020.

Como mostrado na Figura 1, de acordo com os dados estatísticos do Centro Global de Fraudes (Global Center Hubs) de 2020, foi realizada uma comparação de ataques cibernéticos causados por humanos e ataques causados por robôs.

Figura 1 - Gráfico estatístico de origem de ataques cibernéticos



Fonte: 2020 Q2 Fraud Report – Arkose Labs (2020).

2.1 DEFINIÇÃO DE PRIVACIDADE DE DADOS DE DADOS E SEUS PRINCÍPIOS

A privacidade é o direito que os titulares dos dados têm de manter anônimos suas informações pessoais e da própria vida. Ou seja, a privatização de dados atua para que empresas não obtenham, utilizem ou disponibilizem tais informações indevidamente para terceiros. É importante manter reservado certas informações, pois é normal um desconhecido perguntar o nome de outra pessoa, mas não seria normal perguntar dos seus dados biométricos, e essa seria uma pergunta sem resposta. E a

privacidade de dados funciona dessa maneira, pois se os dados ou as informações forem de grande importância, devem ser tratadas com segurança.

Também é importante manter até mesmo dados pessoais básicos protegidos, como nomes, CPF, endereços, telefones, e-mail, dentre outros. Pois apenas com essas informações pessoais básicas, já seria possível de algum criminoso cometer um roubo de identidade.

"Assegurar a privacidade aos usuários durante todo o ciclo de vida dos dados é um dos princípios mais relevantes da LGPD". (ARICETO, 2020)

"Prevenir e não remediar: Adotar ações preventivas de segurança de tratamento de dados pessoais". (ARICETO, 2020)

"Proteção durante o ciclo de vida completo: A proteção de privacidade deve ser pensada de ponta a ponta, durante todo o ciclo de vida dos dados". (ARICETO, 2020)

"Visibilidade e transparência: Permitir que o titular dos dados conheça o processo de coleta com maior transparência possível". (ARICETO, 2020)

2.2 CONSEQUÊNCIAS DA FALTA DE PRIVACIDADE DE DADOS

A ausência da proteção e privacidade de dados pode gerar consequências como:

Roubo de identidade: quando os criminosos utilizam indevidamente a identidade da vítima que teve seus dados vazados, se passando por essa pessoa para praticar atos criminosos e fraudulentos, como também dando-os a oportunidade de fazer transferências monetárias e compras indesejadas.

Pedidos de estorno: o meliante se aproveita de possuir os dados de uma pessoa e exige uma quantidade monetária em troca dos dados roubados. Graças a isso eles podem mudar informações, como senhas, fazendo com que a vítima não tenha mais acesso à própria conta, como também, possibilita-os de interceptar mercadorias que foram compradas pela vítima.

2.3 O QUE É A SEGURANÇA DE DADOS

A segurança de dados é a proteção de informações e dados confidenciais que são de grande valor para uma empresa. Essa proteção deve ser feita em computadores, sistemas, provedores, servidores, e nas redes da empresa, e para isso, é necessário que essa empresa tenha uma gestão de segurança da informação, que esteja

preferencialmente de acordo com as normas ISO/27001[1]. Com isso, apenas com uma equipe que possua conhecimento na área, seria possível ter uma garantia maior que os dados estejam seguros, e que teriam uma melhor proteção contra-ataques cibernéticos, evitando assim os vazamentos de informações.

A segurança da informação opera o princípio de certas boas práticas, na qual temos:

Confidencialidade: A garantia de que qualquer informação armazenada não seja acessada, ou liberada para pessoas indesejadas.

Integridade: Tentar evitar que as informações armazenadas não sejam alteradas indevidamente, ou caso sejam alteradas, ser possível detectar qual alteração foi feita, e onde ela ocorreu.

Disponibilidade: Garantia de que os usuários legítimos tenham o direito de acessar as informações, e recursos do sistema a qualquer momento.

Autenticidade: Garantir que o autor de uma mensagem seja identificado corretamente pelo destinatário.

Irretratabilidade: Onde o emissor, ou destinatário não possam negar de terem feito algo, evitando a negação de envios, recepções e posses de informações e mensagens (SIMPLICIO, Marcos).

De acordo com as normas da LGPD**,** é de responsabilidade do controlador (pessoa física/jurídica que faz as decisões referentes ao tratamento de dados pessoais) e seus agentes (o operador e o encarregado) a utilização da prática da adoção de medidas técnicas e administrativas eficazes o suficiente para a proteção dos dados pessoais dos titulares e restringir o acesso indevido ou ainda possíveis acidentes que possam vir a ocorrer com essas informações, como por exemplo a exclusão, perda, alteração, comunicação e tratamento inadequado ou ilícito.

A ANPD[2] poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos na LGPD.

---

[1] A norma ISO/27001 é uma padronização utilizada para prover requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI). Mais informações em: <https://www.27001.pt>.

[2] Sigla para “Agência Nacional de Proteção de Dados”.

2.4 A PRIVACIDADE DE DADOS NAS REDES SOCIAIS

Deve-se ter cuidado para não compartilhar detalhes pessoais e certas informações de contato na internet, pois elas podem cair nas mãos erradas. Quando se trata de segurança e privacidade nas redes sociais, pode-se citar publicações de fotos, publicações de texto e compartilhamento de localização, mas principalmente, senhas, pois elas são o que mantém os dados protegidos nas redes, e por isso, é necessário ter atenção com senhas fracas. Por exemplo, não teria de muita utilidade usar a opção de "Conta privada" nas redes sociais (opção onde o usuário permite apenas pessoas consideradas de confiança para ver o que o dono da conta publica), e a conta ter uma senha fraca, que seria de fácil acesso para criminosos com más intenções. Caso contrário, pessoas indesejadas poderiam ver dados que apenas o proprietário da conta tem acesso.

Compartilhar informações pessoais nas redes sociais pode prejudicar a privacidade do indivíduo. Mesmo a LGPD legislando sobre a proteção de dados no Brasil, é muito importante que alguns cuidados sejam tomados pelos usuários para proteger ainda mais a privacidade nas redes sociais, como:

- Verificar a configuração de privacidade das redes sociais. Assim, é você quem decide quais informações serão públicas;
- Evitar usar armazenamentos públicos para dados privados. Não coloque senhas e ou informações de documentos importantes em aplicações como o Google Drive ou Dropbox;
- Ao navegar em um site, utilize o modo anônimo e evite o rastreamento das suas preferências;
- Aplicativos de troca de mensagens devem ser usados com criptografia de ponta a ponta;[3]
- Evite disponibilizar seus números pessoais como e-mail e telefone para lojas. Afinal, a única coisa que você pode ganhar com isso é uma caixa de entrada lotada de spam;
- Criar um endereço de e-mail especialmente para compras e serviços online;
- Muito cuidado ao informar os lugares que frequenta em posts nas redes sociais.

[3] Um recurso de segurança que protege os dados durante uma troca de mensagens, fazendo com que o conteúdo seja acessível apenas para o remetente e o destinatário.

3 A LEI GERAL DE PROTEÇÃO DE DADOS

De acordo com o cenário estabelecido anteriormente, de um mundo altamente tecnológico e conectado, torna-se importante a discussão sobre as leis que tornam a proteção de dados possível no nosso país. Inicialmente será exposto a atual situação da proteção de dados no Brasil, com leis que foram complementadas pela Lei Geral de Proteção de Dados (LGPD), o tema mais recente a respeito de legislação de dados no Brasil. Haverá também uma contextualização sobre leis de outros países, como a GDPR, que é o regulamento europeu de dados pessoais.

3.1 A PROTEÇÃO DE DADOS NO BRASIL

O Brasil dispõe de diversas leis que tratam da privacidade e proteção de dados pessoais de pessoais naturais (físicas), como o Marco Civil da Internet (Lei n° 12.965) e o Código Brasileiro de Defesa do Consumidor (Lei 8.078/1990), ambos sendo complementados pela atual Lei Geral de Proteção de Dados Pessoais – LGPD (Lei 13.709/2018), o primeiro regulamento geral sobre a proteção de dados pessoais no Brasil.

A LGPD entrou em vigor em 18 de setembro de 2020, com suas sanções administrativas passando a valer em 01 de agosto de 2021. A lei é de interesse nacional e prevalece sobre qualquer lei municipal ou estadual, e tem como objetivo fornecer aos indivíduos um maior controle sobre seus dados pessoais, dando aos titulares dos dados a possibilidade de solicitar a qualquer momento a exclusão de suas informações armazenadas, e das empresas, a exigência de uma maior segurança, transparência e controles sobre toda e qualquer coleta, uso, armazenamento e compartilhamento de dados pessoais, dados sensíveis e afins, com isto sendo feito por meio de regras e multas no caso do descumprimento das mesmas.

Ainda assim, é necessário o comprometimento das companhias brasileiras e as que operam em território brasileiro de seguirem as regras da Lei da devida maneira, atitude que não é feita por todas elas. Segundo uma pesquisa realizada pela empresa de privacidade e segurança online Surfshark, no ano de 2021, o Brasil foi um dos países que mais sofreu com vazamento de dados:

> De janeiro a novembro de 2021, 24,2 milhões de perfis de brasileiros tiveram suas informações expostas na internet a partir de ataques ou brechas em sistemas. Com isso, o Brasil assumiu o 6º lugar no ranking de países com mais vazamentos de dados no mundo [...] no total global, o crescimento de vazamentos foi de 3,4%. (ISTOÉ, 2022)

O Brasil é altamente suscetível a casos de vazamento de dados por conta da dificuldade da implementação de boas práticas do setor de TI[4] de algumas empresas, conforme exemplificado por Dias:

> [...] não só de vazamento ou exposição de dados estamos vulneráveis, há incontáveis empresas que compartilham irregularmente dados pessoais antes mesmo do início da vigência da LGPD, da qual refletiam justamente o que seria acompanhado com atenção redobrada pela SENACON[5]: captura de informações, sem consentimento, para fins comerciais.
>
> Em razão da intensificação do acompanhamento de práticas que possam constituir os chamados "ilícitos de consumo" no ambiente digital, a SENACON, após uma semana da vigência da LGPD já contava com 34 processos administrativos em andamento envolvendo o uso indevido de dados pessoais de usuários de plataformas digitais, destes, boa parte dos processos envolvendo os principais gigantes americanas de tecnologia, como as empresas Tinder e Facebook (que atualmente se chama Meta). (CAMAROTTO, 2020 apud DIAS, 2021, p. 30, adaptação nossa).

O País figura na 56ª posição – no "National Cyber Security Index", um ranking global para avaliar a situação digital de países. "[...] Temos diversas e acessíveis tecnologias que podem nos auxiliares, no entanto, a segurança depende de um conjunto de fatores como: campanha de conscientização dos usuários, investimento em softwares genuínos, adição de ferramentas de controle baseados em comportamento dos usuários, aumento do nível de segurança adicionando múltiplos fatores de autenticação etc." (LOPES, 2020). Os motivos para a fraqueza da segurança dos dados no país variam, de acordo com Reis (2013):

> 1. O País investe pouco em segurança. Muitas das grandes empresas brasileiras, públicas e privadas, além do governo (administração direta, autarquias etc.), não possuem sequer um profissional responsável por segurança; várias destas não possuem orçamento para segurança; em tempos de crise, ou no caso de necessidade de cortes orçamentários, os investimentos em segurança são os primeiros da lista;
>
> 2. O País investe errado em segurança. O pouco dinheiro que sobra para a área é, em muitos casos, investido de forma incorreta. Empresas e governo ainda acreditam que projetos pontuais de consultoria resolverão o problema para sempre; ainda pensam que antivírus resolve sozinho o problema de vírus, que firewall evita completamente invasões, e assim por diante. É como colocar um band-aid numa ferida de câncer;
>
> 3. Uma minoria leva segurança a sério. A segurança não é levada a sério porque não se entende a extensão do problema, não se compreende que a falta de segurança pode colocar tudo a perder, que pode significar a derrocada de uma empresa, ou até mesmo de um país. (REIS, 2013, adaptação nossa).

---

[4] TI: Tecnologia da Informação, um termo genérico para uma pessoa que trabalhe com tecnologia.

[5] SENACON: Sigla da Secretaria Nacional do Consumidor, órgão público responsável pela gestão, disponibilização e manutenção da plataforma <consumidor.gov.br>, site do governo que é utilizado para consumidores brasileiros se comunicarem diretamente com empresas participantes do site.

Um exemplo de falta de boas práticas pode ser visto no caso que expôs os dados de pacientes do Hospital Albert Einstein, em 2021, onde um funcionário munido de boas intenções e com o objetivo de compartilhar informações pessoais (nomes completos e dados pessoais) dos pacientes com seus colegas de trabalho acabou fazendo o *upload* (o envio) de uma planilha no GitHub[6] com todas as informações em texto puro (ou seja, sem utilizar métodos de encriptação[7]), em um repositório público, onde qualquer indivíduo podia acessar e baixar o arquivo (ISTOÉ, 2020).

Além do exposto acima, outro fato que contribui para a vulnerabilidade da segurança das informações dos brasileiros é o grande uso de tecnologias defasadas, principalmente em sistemas do setor público. A Syhunt, empresa brasileira de cibersegurança, apontou que, em 2021, o Brasil ficou em quarto lugar entre as nações que mais tiveram senhas vazadas de domínios do órgão público:

> O banco de dados publicado que circula na internet oculta expõe senhas de e-mails de órgãos como Banco Central do Brasil, Polícia Militar de São Paulo, Supremo Tribunal Federal (STF), Câmara dos Deputados, Ministério dos Transportes, entre outros [...] Segundo Daragon, fundador da Syhunt, o vazamento de domínios relacionados a órgãos públicos é especialmente delicado porque um hacker[8] pode ter acesso a informações sensíveis dos cidadãos. "Se, em algum momento, a senha de um funcionário é capturada por um hacker, a conta pode ser tomada e ele se faz passar pelo funcionário. Se o funcionário utiliza a mesma senha em outros serviços sem um fator adicional de proteção, o problema se torna ainda mais sério", afirma o especialista. (CORACCINI, 2021, adaptação nossa).

Um exemplo deste tipo de incidente envolveu os serviços armazenados pelo Ministério da Saúde, que já foi invadido diversas vezes: Em 2016, um hacker acessou o site e alterou a agenda de compromissos do então ministro da saúde Ricardo Barros para anunciar uma falsa renúncia do então presidente Michel Temer (BRITO, 2016) e em 2020, o site foi vandalizado, removido do ar e algumas máquinas tiveram seus dados encriptados (DEMARTINI, 2020). A invasão mais recente do site do Ministério da Saúde ocorreu em 2021. Não houve nenhum dano, mas o hacker fez questão de deixar uma mensagem para os administradores do sistema, apontando as vulnerabilidades do site e pedindo que sejam arrumadas (VARGAS, 2021).

As ameaças cibernéticas associadas ao sensível momento causada pela Pandemia da Covid-19 têm gerado efeitos negativos em todos os usuários de tecnologia, independente do grau de entendimento sobre boas práticas de navegação na Internet. O

---

[6] GitHub: Site de compartilhamento de softwares (programas) e de código-fonte deles.
[7] Encriptação: Codificar ("embaralhar") uma informação de modo que ela só possa ser lida por algo ou alguém que tenha a capacidade de descriptografá-la ("desembaralhar").
[8] Hacker: Pessoa que possui amplo conhecimento na área da tecnologia e que utiliza tal experiência para fins ilícitos (invasão de sistemas, vazamento de dados etc.)

enorme aumento no número de ataques durante a pandemia não é coincidência (IBLISS, 2020). “Redes sem certificação, roteadores abertos, maior volume de conexões na vizinhança, tudo isso pode se tornar portas de entradas para pessoas mal-intencionadas. Mesmo as empresas que ofereceram uma VPN (rede de comunicação privada) não estão totalmente seguras, já que ela é um túnel direto para o coração da rede de uma empresa”, alertou Carlos Sampaio, gerente de TI do Centro de Transformação Digital e Inovação.

“Além disso, é importante notar que a confiança dos clientes diminui conforme acontecem incidentes cibernéticos, o que pode fazê-los buscar empresas concorrentes. Problemas de reputação causam prejuízos para além de dados vazados ou multas, podem reduzir o valor de mercado de uma companhia e sua imagem junto aos clientes”, explica Pedro Silveira, vice-presidente de Vendas e Marketing da GC Security (INFOMONEY, 2021).

3.2 LEI GERAL DE PROTEÇÃO DE DADOS - LGPD

A Lei Geral de Proteção de Dados (LGPD) é uma lei brasileira, desenvolvida com o objetivo de proteger os dados de pessoas físicas contra o mal uso ou o compartilhamento indiscriminado de informações sem que o titular tenha fornecido o consentimento para utilização delas, e é válida para toda e qualquer informação coletada em território nacional.

Ela foi desenvolvida a partir do modelo da GDPR (*General Data Protection Regulation*) ou Regulamento Geral de Proteção de Dados, da União Européia, que é considerado referência internacional no quesito de privacidade de dados.

A LGPD estabelece que empresas, órgãos públicos e organizações sem fins lucrativos que ofereçam bens e serviços ou ainda que façam a coleta, análise ou processamento de dados em território nacional estejam sujeitas ao seu cumprimento. Ela aplica-se somente em relações que haja negociação econômica e a qualquer operação de tratamento[9] que seja realizada por pessoa natural ou por pessoa jurídica, seja de direito público ou privado. Independente do meio ou da localização de sua sede, nos demais casos a lei não é empregada, conforme exemplos das situações a seguir:

[9] O “tratamento” de dados se refere a toda e qualquer operação realizada com dados pessoais, como por exemplo a coleta, distribuição, processamento e armazenamento dos mesmos.

- Tratamento feito por pessoas naturais por interesse próprio e sem fins econômicos.
- Tratamento feito exclusivamente para fins jornalísticos, artísticos ou acadêmicos.
- Tratamento feito para fins de segurança pública, defesa nacional, segurança do estado ou ações de investigações e repressão de infrações penais.

No contexto da LGPD, um dado pessoal é toda informação capaz de identificar uma pessoa. Dados capazes de nos identificar são nomes, RG, CPF, gênero, data e local de nascimento, filiação política, convicção religiosa, telefone, celular, endereço residencial, dados bancários e afins. Esses dados são divididos em dois grupos: Os estruturados e não estruturados. Os dados estruturados são dados que seguem um determinado padrão e podem ser facilmente processados e identificados, como por exemplo, um nome ou endereço. Já os dados não estruturados, eles são aqueles que não possuem um determinado padrão ou sequência e são compostos por diferentes elementos, como por exemplo, um e-mail ou postagens feitas em redes sociais.

Dentro desse contexto, há também os dados sensíveis, que são aqueles que podem vir a discriminar uma pessoa, ocasionando certo constrangimento e possível dano moral a quem tiver esses dados utilizados sem seu prévio e expresso consentimento e/ou autorização do portador. Eles devem seguir normas legais e, por isso, necessitam de cuidados especiais. Dados sensíveis incluem:

- Informações sobre religião.
- Informações Genéticas.
- Informações de raça ou etnia.
- Informações sobre saúde ou vida sexual.

Portanto, para que os dados citados acima sejam tratados, eles devem ser manipulados de forma extremamente cuidadosa e sigilosa, a fim de que não sejam usados de forma discriminatória e quem estiver na posse deles não venha a sofrer nenhum tipo de sanção e/ou punição pelo vazamento, fornecimento ou compartilhamento para utilização deles a terceiros sem que estes estejam autorizados por quem os possui por direito.

Visando ainda uma maior proteção dos dados dos titulares, a lei obriga que a organização ou prestadora de serviço faça a nomeação de um colaborador que será

encarregado de fazer a proteção dessas informações, ou seja, um encarregado de dados que será responsável em não só proteger, como também, em caso de ocorrer algum incidente em que os dados possam vir a ser vazados ele será responsabilizado pelo ocorrido, ficando obrigado a imediatamente dar publicidade do fato juntamente com seus dados de contato, onde essa obrigatoriedade se dá quando o ocorrido for em uma organização pública, exceto nos tribunais que estejam no exercício de suas funções jurisdicionais, quando as informações exijam um controle contínuo e em grande escala e quando as informações também sejam de grande escala e tratem de assuntos referentes a delitos ou condenações criminais.

A LGPD estabelece um conjunto de princípios norteadores do tratamento dos dados pessoais pelos controladores, pessoa natural ou jurídica de direito público ou privado a quem compete as decisões referentes ao tratamento de dados pessoais, ou também pelos operadores, pessoa natural ou jurídica de direito público ou privado que realiza o tratamento dos dados pessoais em nome do controlador. Ambos devem observar e realizar suas tarefas seguindo alguns princípios da LGPD, listados a seguir:

- **Finalidade**: o controlador compromete-se de forma clara e específica a realizar com os dados somente o que foi informado ao titular no momento da coleta deles, ficando excluídas qualquer possibilidade de utilização para outros fins.
- **Transparência**: o controlador deve garantir aos titulares informações claras e fácil acesso a realização do tratamento dos dados e possíveis agentes de tratamento.
- **Adequação**: o tratamento a ser realizado com os dados coletados deve ser compatível com as suas finalidades informadas no ato da coleta.
- **Segurança**: o controlador e seus agentes de tratamento comprometem-se a proteger os dados de acessos não autorizados e possíveis incidentes que podem ocasionar a perda ou destruição deles.
- **Necessidade**: fica limitado o controlador a efetuar com os dados coletados somente o que apresentar ser necessário para alcançar sua necessidade.
- **Livre acesso**: o controlador deve garantir aos titulares facilidade de acesso as informações de forma gratuita e informações sobre a duração do tratamento e integridade dos dados.

- **Não Discriminação**: os dados não poderão ser utilizados para qualquer que seja o tipo de discriminação, ato ilícito ou abusivo dos dados.
- **Responsabilização e Prestação de Contas**: O controlador e seus respectivos agentes deverão demonstrar a adoção de medidas e comprovar sua observância ao cumprimento de normas e eficácia das medidas.

3.2.1 TRATAMENTO DE DADOS PESSOAIS

A Lei faz com que o titular tenha maior controle de quem poderá utilizar seus dados, tendo em vista que ele deverá autorizar por escrito ou por outro meio seu uso. O tratamento dessas informações poderá ser feito nas situações a seguir:

a) A partir da autorização voluntária e expressa do titular.
b) Cumprimento de obrigação legal ou regulatória pelo controlador.
c) Tratamento por parte da administração pública.
d) Tratamento e compartilhamento dos dados para execução de políticas públicas.
e) Realização de estudos por órgão competente.
f) Para exercício regular de direitos em processo judicial ou arbitral.
g) Para proteção da vida ou da incolumidade física do titular ou de terceiros; ou para tutela de saúde.
h) Obtenção para proteção de crédito.

Ainda a respeito sobre o fornecimento de consentimento do titular para tratamento de dados, devem ser observados os seguintes requisitos:

a) O consentimento deve ser fornecido por escrito ou outro meio que demonstre a manifestação expressa do titular.
b) Em caso de o consentimento ser fornecido por escrito esse deverá constar cláusula com destaque sobre os dados consentidos.
c) O controlador arcará com o ônus da prova sobre o que foi consentido e em conformidade com a LGPD.
d) É vedado o tratamento de dados pessoais mediante vício de consentimento.
e) O consentimento deve se referir a finalidades específicas e as autorizações genéricas serão nulas.

f) O titular pode a qualquer momento revogar seu consentimento sobre os dados consentidos e isso deve ser feito de maneira imediata, facilitada e gratuita pelo controlador ou seus agentes.

A aplicação da lei se dará em qualquer tipo de território, seja ele nacional ou estrangeiro, desde que a atividade que a originou tenha ocorrido em território nacional.

3.2.2 TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

Conforme dito anteriormente, dados pessoais sensíveis devem ser manipulados de forma extremamente cautelosa e sigilosa, a fim de que não sejam usados de forma discriminatória e quem estiver na sua posse não venha a sofrer nenhum tipo de sanção e/ou punição pelo vazamento, fornecimento ou compartilhamento para utilização por terceiros. Estes dados poderão ser tratados somente nas seguintes possibilidades:

- Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas.
- Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
  - Cumprimento de obrigação legal ou regulatória pelo controlador.
  - Tratamento por parte da administração pública.
  - Tratamento e compartilhamento dos dados para execução de políticas públicas.
  - Realização de estudos por órgão competente, garantindo sempre que possível a anonimização dos dados pessoais sensíveis.
- Para exercício regular de direitos em processo judicial ou arbitral nos termos da lei nº 9.307/1996.
- Para proteção da vida ou da incolumidade física do titular ou de terceiros; ou para tutela de saúde.
- Para tutela de saúde, exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.
- Garantia de prevenção à fraude e à segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

3.2.3 DIREITOS DO TITULAR DOS DADOS PESSOAIS

É assegurado ao titular dos dados os direitos e garantias fundamentais de liberdade, de intimidade e de privacidade nos termos da LGPD independente do que esteja sendo solicitado no consentimento, pois os dados pessoais são individuais e intransferíveis e sempre pertencerão a pessoa a que se referem.

O titular poderá obter do controlador os dados que por ele estejam sendo tratados a qualquer momento e mediante sua solicitação:

a) Para acesso aos dados.

b) Confirmação da existência do tratamento por ele designado.

c) Para correção de dados incompletos, incorretos ou desatualizados.

d) Para anonimização, bloqueio ou eliminação de dados desnecessários, excessivos, ou tratados em desconformidade com o que é exposto pela LGPD.

e) Portabilidade a terceiros mediante solicitação expressa e de acordo com a regulamentação da ANPD observados os sigilos comercial e industrial.

f) Exclusão dos dados pessoais tratados conforme consentimento conferido pelo titular, exceto nas hipóteses previstas na LGPD.

g) Para informação de entidades públicas ou privadas com as quais o controlador realizou uso compartilhado de dados.

h) Para informação sobre a possibilidade de não fornecer consentimento e consequências da negativa.

i) Revogação do consentimento mediante solicitação expressa do titular de forma gratuita e facilitada.

Ao final do período acordado entre o titular e o controlador e/ou seus agentes os dados pessoais deverão ser destruídos de forma efetiva e segura para que não haja mais a possibilidade de utilização deles.

3.2.4 SANÇÕES ADMINISTRATIVAS

Há fiscalização por parte da Autoridade Nacional de Proteção de Dados Pessoais (ANPD), que é um órgão integrante da administração pública federal e da presidência da república, com o objetivo de assegurar que o tratamento dos dados está sendo feito de forma adequada e em conformidade com a LGPD. Os agentes de tratamento

(controlador e operador), em caso de cometerem alguma infração face as normas da LGPD, estarão sujeitas as seguintes sanções administrativas:

- Multas diárias limitadas a até R$ 50.000.000,00 (cinquenta milhões de reais) milhões de reais por infração.
- Publicitação da infração após a devida apuração e confirmação da sua ocorrência.
- Multa de 2% sobre o percentual do seu último faturamento anual da empresa limitada a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.
- Bloqueio dos dados pessoais até sua regularização.
- Exclusão dos dados pessoais a que se refere a infração.
- 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.
- 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.
- Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Antes da aplicação da sanção, a autoridade competente notificará a empresa e estipulará um prazo para que ela se adeque às normas exigidas, e se decorrido o prazo e em nova auditoria a empresa não se adequar ao que é exigido, a multa será aplicada. Elas poderão ser aplicadas após procedimento administrativo, que dá ao controlador a oportunidade de ampla defesa, de forma gradativa, isolada ou cumulativa, conforme as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

- A gravidade e a natureza das infrações e dos direitos pessoais afetados.
- A boa-fé do infrator.
- A vantagem auferida ou pretendida pelo infrator.
- A sua condição econômica.
- A reincidência.
- O grau de dano.
- A cooperação do infrator.
- A adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de

dados em consonância com as medidas para reverter ou mitigar os efeitos do incidente.

- A proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Conforme a notícia a seguir, pode-se observar que a LGPD já vem sendo utilizada pelo poder judiciário como instrumento de se fazer cumprir com suas determinações, vide o caso do vazamento de dados da empresa Uber:

> Em **2016 a Uber decidiu esconder um vazamento de dados que aconteceu em sua plataforma** e afetou 7 milhões de motoristas e 57 milhões de usuários – destes, 196 mil eram brasileiros. O caso foi descoberto e punido em 2018, com uma multa de 148 milhões de dólares.
> O vazamento aconteceu devido a um ataque de hackers ao sistema da empresa. Na época, a **Uber tentou esconder o caso embaixo do tapete, oferecendo 100 mil dólares para os hackers responsáveis,** que concordaram manter em segredo o escândalo.
> A revelação do ataque veio a público quando o ex-diretor de segurança da empresa foi demitido e, durante uma auditoria externa no setor, encontrou-se o vazamento de telefones, nomes, e-mails e carteiras de motoristas expostas no ataque. (SOFTWALL, 2021)

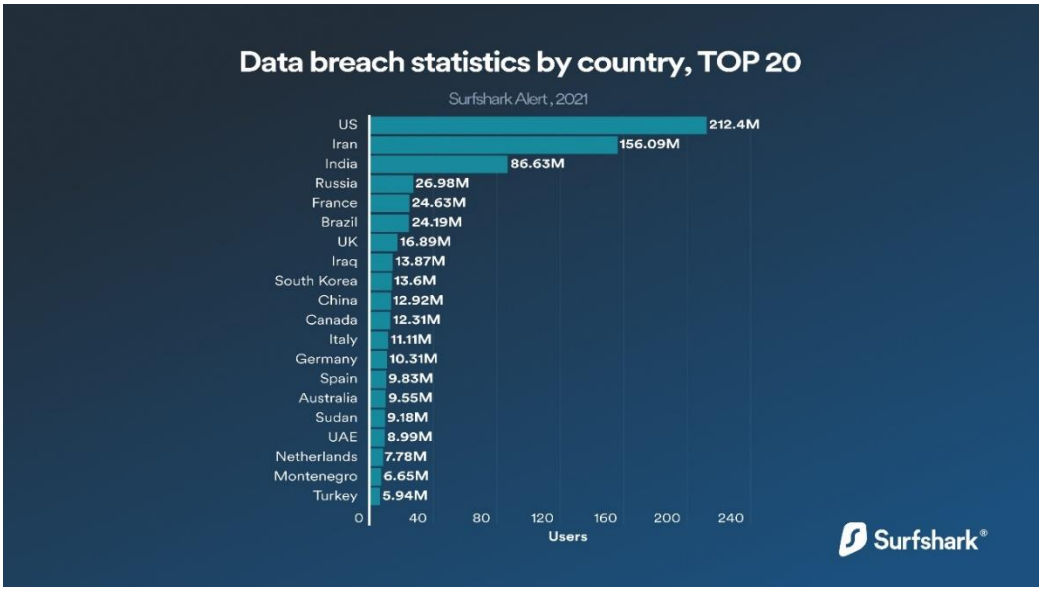
3.3 A PROTEÇÃO DE DADOS EM OUTROS PAÍSES

Conforme exposto anteriormente, o Brasil é um dos países que mais sofre com vazamento de dados, atitude que não é coincidência se considerarmos a falta de boas práticas de usuários corporativos e de seus respectivos setores de TI quanto à segurança da informação. O país, por outro lado, não está sozinho nessa, já que 19% dos países do mundo (SECURITY REPORT, 2021) ainda não possuem nenhuma legislação sobre privacidade de dados:

> [...] Segundo informações da United Nations Conference on Trade and Development (UNCTD), organização intergovernamental ligada à ONU, 66% dos países no mundo possuem legislação relacionada a proteção de dados e privacidade nas redes; 10% possuem legislação em elaboração ou em tramitação; 19% não possuem nenhuma legislação e 10% não disponibilizam dados relacionados ao tema (SECURITY REPORT, 2021).

A situação da segurança dos dados no mundo fica bem representada na Figura 2, onde “users” representa “usuários” e os números representam, por país, a quantidade de usuários que tiveram seus dados (informações pessoais e privadas) vazados:

Figura 2 - Top 20 de Países com a maior quantidade de dados vazados



Fonte: Adaptado de SURFSHARK no Twitter[10], 2021.

A quantidade de vazamentos em um determinado período depende do contexto da tal época. Utilizando o gráfico acima como base, os Estados Unidos estão em primeiro lugar de maior quantidade de dados vazados por conta de seu longo território e ampla influência mundial, o que os torna grandes alvos para tentativas de ataques, mesmo apesar de todas as leis de proteção de dados e uma enorme quantidade de verba direcionada para tal que o país possui. A título de exemplo, destaca-se o exemplo da Índia, no qual, desde 2019, tramita uma proposta de Lei sobre proteção de dados, que ainda está para ser aprovada. Enquanto isso o país inteiro sofre com problemas relacionados à invasão de dados, como em 2021, que cerca de 4,5 milhões de clientes da Air India, do mundo todo, tiveram seus dados roubados, entre nomes, números de cartão de crédito e dados de passaporte. (SECURITY REPORT, 2021).

O país inteiro não possui uma adequada estrutura para a tecnologia no geral, muito menos sobre a proteção de dados e, em decorrência destes fatos, a prática de fraudes e roubo de informações se torna rampante no território inteiro, até mesmo afetando cidadãos de outros países, com duas técnicas sendo bastante utilizadas pelos golpistas de lá: fraudes de sites falsos e call centers (centrais de atendimento de usuários).

[10] Disponível em: <https://twitter.com/surfshark/status/1476619594500476929/photo/1>. Acesso em: 22 abr. 2022.

Por outro lado, países com uma economia mais desenvolvida (chamados de “primeiro mundo”) conseguem pagar por uma estrutura mais robusta, e com isso eles também conseguem lidar melhor com a proteção de seus dados, como é o caso dos países da União Europeia, que em sua grande maioria já tinham implementado a *General Data Protection Regulation* (GDPR).

4 VAZAMENTO DE DADOS: CAUSA E EFEITO

De acordo com o dicionário Michaelis (s.d), o significado de causa é “Aquilo que determina a existência de uma coisa ou de um acontecimento; razão, motivo, explicação [...]”, e a consequência, de acordo com o mesmo dicionário, significa “Resultado natural, provável ou forçoso de uma causa; efeito, resultado [...] Conclusão obtida a partir de um raciocínio lógico; inferência, ilação, dedução.”

Em resumo, a causa é a origem de uma ação e a consequência é o efeito dele. Ambos estão presentes no conceito filosófico da causalidade, explicado melhor por Maciel (s.d):

> A causalidade é o agente que liga dois processos, sendo um a causa e outro o efeito, em que o primeiro é entendido como sendo, ao menos em parte, responsável pela existência do segundo, de tal modo que o segundo é dependente do primeiro. Diz-se "em parte" porque um efeito pode ter mais de uma causa em seu passado. Esta é ainda uma relação continua e replicável, já que um efeito pode vir a ser causa de outros efeitos, do mesmo modo que a causa de um efeito pode ela mesma ser efeito de um processo causal anterior.

No contexto do vazamento de dados, há inúmeras causas para este acontecimento, com a consequência diferindo dependendo da maneira do ocorrido, sendo mais comumente alguma vulnerabilidade ou brecha em um sistema. Existem falhas que dão a um invasor a capacidade de influenciar, visualizar ou alterar dados sensíveis, como o método SQL Injection, explicitado a seguir.

4.1 SQL INJECTION

A sigla SQL significa "*Structured Query Language*", que em sua tradução significa Linguagem de Consulta Estruturada, uma linguagem padrão de gerenciamento de dados que interage com os principais bancos de dados baseados no modelo relacional.[11]. Ela possibilita a criação de tabelas para armazenamento de dados e dispõe de diversos comandos para a manipulação deles, como *INSERT* (inserção), *SELECT* (consulta), *UPDATE* (atualização) e *DELETE* (exclusão) (SIGNIFICADOS, s.d).

As consultas SQL, como são chamadas as execuções de comando da linguagem, “[...] são capazes de passar, indetectadas, por controles de acesso, portanto desviando da

[11] Banco de dados relacional: Um tipo de banco que armazena e fornece acesso a pontos de dados relacionados entre si.

autenticação padrão e de checagens de autorização, e algumas vezes consultas SQL podem permitir acesso à comandos no nível do sistema operacional do servidor. (PHP, s.d).

O SQL Injection, do português, injeção de SQL, é uma técnica de ataque em que são criados ou alterados comandos de um código SQL existente para expor dados escondidos, sobrescrever dados valiosos, ou ainda executar comandos de sistema perigosos no servidor. Um ataque de SQL injection bem-sucedido pode resultar em acesso não autorizado a dados confidenciais, como senhas, detalhes de cartão de crédito ou informações pessoais do usuário. Muitas violações de dados de alto perfil nos últimos anos foram resultado de ataques de SQL injection, levando a danos à reputação e multas regulatórias. Em alguns casos, um invasor pode obter um *backdoor*[12] persistente nos sistemas de uma organização, levando a um comprometimento de longo prazo, que pode passar despercebido por um longo período.

Existem várias possibilidades de um ataque acontecer explorando as vulnerabilidades de um código SQL, sendo que cada um pode surgir em diferentes situações. Dentre elas temos:

4.1.1 ATAQUE DE SQL INJECTION PELA TELA DE LOGIN:

Uma das técnicas mais comuns de SQL injection é através de um formulário de login de uma aplicação. Quando o usuário digita o login e a senha, a aplicação web consulta as informações do usuário, mantidas em um banco de dados. A figura 3 mostra como este formulário é exibido para o usuário:

Figura 3 - Exemplo de formulário web de login

[12] Backdoor: Significa “porta dos fundos”, e no contexto da tecnologia, significa uma porta de acesso a um sistema que não foi documentada.

Fonte: Adaptado de DevMedia, 2007.

De acordo com a figura no anexo A, o código demonstra como a informação digitada pelo usuário nos campos inseridos na figura 1 será processada na aplicação web.

“Ao digitar o nome e senha (ver Figura 1), a aplicação web dispara uma consulta na tabela “USERS” para confirmação do cadastro do usuário. Se um registro for encontrado, o *username* será retornado e esta é a confirmação de que o usuário foi autenticado com sucesso. Se a consulta na tabela “USERS” não retornar registros, o usuário não será autenticado.” (DevMedia, 2007).

No exemplo abaixo, há um código em que não é realizada uma validação e o atacante é capaz de coletar dados dos usuários e assim burlar a digitação da senha.

var sql = "select * from users where username = '" + username +
"' and password = '" + password + "'";

Adaptado de DevMedia, 2007.

Quando o código é digitado dessa forma, o atacante ganha uma margem para acessar os dados apenas inserindo o nome de usuário, colocando “--” após a digitação. Isso faz com que todo o comando após a sequência seja considerado um comentário e assim não processado. Por outro lado, caso o atacante não tenha conhecimento de um *username*, poderá autenticar-se com as credenciais do primeiro usuário cadastrado na tabela “USERS”. (Dev Media, 2007).

Em 2021, duas falhas de segurança foram encontradas em plataformas digitas da Universidade de São Paulo (USP):

> Duas falhas de segurança encontradas em plataformas digitais da Universidade de São Paulo (USP) podem ter exposto os dados

> pessoais de até 188,6 mil pessoas, entre alunos, professores, funcionários e servidores. As brechas estavam disponíveis em sistemas de acesso a serviços internos da universidade e em uma plataforma de ensino, com materiais como aulas gravadas e provas online. (Demartini, 2021).

Segundo o pesquisador Giovanni Zadinello, da GZ Segurança (2021):

> "Utilizando as credenciais de acesso [aos sistemas] da USP, ataques direcionados poderiam ser realizados, visando acessar outros serviços com os mesmos dados", explica Zadinello. Ele aponta, também, a própria exposição das informações como um problema, com a disponibilização aberta de um banco de dados desse tipo também podendo levar a tentativas de golpes contra alunos e servidores, em busca de dados financeiros ou de cartão de crédito.

Em outro caso, que está relacionado com o portal e-Disciplinas, estavam expostos dados pessoais como nomes, endereços completos e números de telefone de alunos, além de dados de acesso a plataforma como *login*, senhas e detalhes da conta, como a data de criação do perfil e o endereço de IP do último local onde a conta foi acessada. Tudo isso seria possível com o SQL Injection. (DEMARTINI, 2021)

4.2 VULNERABILIDADE DAS SENHAS

Hoje em dia, muitas pessoas acabam por colocar senhas fracas e que podem ser facilmente descobertas por hackers, causando uma situação em que os dados do usuário estejam correndo perigo sem nem mesmo ele saber, pois as senhas são a porta de entrada para o mundo digital, visto que através delas podemos acessar contas de bancos, e-mails, redes sociais, redes corporativas etc.

> Mesmo com aumento de investimento em segurança digital, empresas ainda sofrem com a reutilização e adoção de senhas fracas adotadas por colaboradores, aponta o 3º Relatório Anual Global de Segurança de Senhas da LastPass by LogMeIn. O estudo oferece informações sobre o comportamento de adoção de senhas por funcionários, além de analisar tendências em ascensão nas áreas de gerenciamento de identidade e acesso de empresas ao redor do mundo.
> De acordo com o relatório, mesmo com 57% das empresas analisadas relatarem que usam soluções de autenticação multifatorial (MFA), funcionários ainda adotam senhas fracas em sistemas corporativos. Outro problema identificado pelo estudo é a reutilização de senhas, como quando um usuário cria sempre senhas iguais aos seus pessoais, além de reutilizar senhas de outros funcionários. (MAIS DADOS DIGITAL, 2021)

Em um estudo feito em 50 países pela Nord VPN, uma empresa que é especializada em segurança cibernética, foi descoberta que combinações como

“123456” e palavras simples são uma das mais usadas por usuários comuns. Uma pesquisa analisou que em nove de dez senhas fracas levam 1 segundo para serem descobertas e assim conseguir acesso a dados pessoais e de empresas. Outras necessitam de mais algumas horas de esforço para que o hacker tenha acesso a conta e a dados pessoais. (PACHECO, 2021).

Segundo o site showmetech, o Brasil não ficou de fora de lista de países que seguem utilizando a combinação “123456” como uma opção de acesso para suas contas, e apenas em terras tupiniquins, há 1.003.925 de contas analisadas que utilizam esta simples combinação. “[...] Dentro do top 10 de senhas fracas mais usadas no Brasil, apenas uma opção leva “mais tempo” para ser descoberta: “senha” (apenas 10 segundos). As demais poderiam ser acessadas pelos hackers em literalmente, menos de 1 segundo.” (PACHECO, 2021). O quadro 1 a seguir mostra as 25 senhas fracas mais utilizadas no Brasil:

Quadro 1 - As 25 mais senhas fracas mais utilizadas no Brasil:

Senha utilizada	Tempo para ser descoberta	Quantidade de ocorrências
123456	Menos de um segundo	1,003,925
123456789	Menos de um segundo	326,815
Brasil	Menos de um segundo	154,075
12345	Menos de um segundo	143,513
102030	Menos de um segundo	106,217
senha	10 segundos	103,500
12345678	Menos de um segundo	85,973
1234	Menos de um segundo	85,158
10203	Menos de um segundo	62,649
123123	Menos de um segundo	54,441
123	Menos de um segundo	51,725
1234567	Menos de um segundo	49,286
654321	Menos de um segundo	45,459
1234567890	Menos de um segundo	42,703
gabriel	5 segundos	42,532
q1w2e3r4t5y6	Menos de um segundo	40,939

101010	Menos de um segundo	40,244
159753	Menos de um segundo	38,013
123321	Menos de um segundo	37,380
Senha123	17 minutos	34,061
mirantte	3 horas	33,801
Flamengo	3 horas	32,770
felicidade	12 dias	30,901
qwerty	Menos de um segundo	30,789

Fonte: Adaptado de ShowMeTech, 2021.

Como analisado, os brasileiros ainda estão muito atrás na criação de boas senhas para suas redes sociais, e-mails, portais e outros canais na internet. Ainda é necessário melhorar muito nesse aspecto, No total, 125.012.161 senhas brasileiras foram consideradas pelos especialistas para que o estudo fosse feito (PACHECO, 2021).

4.2.1 KEYSTROKE LOGGING

Keystroker Logging é uma ação de gravar as teclas pressionadas em um teclado de maneira secreta, para que assim seja possível registrar tudo que está sendo digitado pelo usuário em um computador. Assim, acessar sites que requerem uma autenticação é um grande perigo já que qualquer pessoa pode acessar computadores púbicos, fazendo com que qualquer um possa instalar softwares maliciosos, como o Keystroke logger. (MITNICK; SIMON, 2003).

Existem dois tipos de Keyloggers, como também é conhecida a prática, o tipo de software e o tipo de hardware. Um *Keylogger* de software é um programa instalado em um dispositivo para monitorar a atividade realizada pelo usuário. O *Keylogger* de software é subdivido em outras categorias: Kernel, API, JavaScript e Injeção de memória.

- O tipo Kernel fica escondido dentro do sistema operacional, o que dificulta a sua detecção. Ainda mais quando é utilizado aplicativos instalados pelo usuário.
- O tipo API se utiliza de funções da APIS do próprio Windows para poder registrar toda a atividade realizada pelo usuário no teclado.

- No tipo de JavaScript, o Keylogger se aproveita do código feito em JavaScript para injetá-lo em uma página web. Isso é feito por meio de um ataque conhecido como *Cross-Site-Scripting*, que irá executar ações maliciosas como copiar cookies, tokens ou roubar dados de acesso registrado no navegador web.
- As injeções de memória funcionam através de modificações de tabelas da memória que está vinculada as funções do sistema e navegadores de internet. Por ele é possível ignorar o controle de conta do usuário do Windows. (TAVELLA, 2021, adaptação nossa).

No caso dos *Keyloggers* de hardware existem três tipos: o *Keylogger* de *fireware, keyboard hardware* e *Wireless Keyboard sniffers.*

- O *fireware* se baseia em uma modificação na BIOS[13] do computador para poder registrar eventos enquanto eles acontecem. Isso só irá funcionar caso o software que for carregado for programado para um hardware específico.
- O *Keyboard hardware* funciona com um dispositivo que é conectado entre o teclado e alguma outra porta de entrada para o computador, como por exemplo a entrada USB.
- *Wireless Keyboard Sniffers* ocorre quando as informações digitadas no teclado são enviadas para o receptor através de pacotes, criptografados ou não.

4.2.2 SNIFFING

O *Sniffing* é uma forma de monitorar o tráfego da rede através de capturas de pacotes de rede. Ao se utilizar de redes públicas, ou seja, redes WI-FI sem senhas, pode haver usuários mal-intencionados que estejam tentando descobrir nomes de usuários e senhas ao enviar estas informações para o servidor, por esse motivo, é importante evitar acessar contas pessoais em redes de terceiros, ou os dados correm risco de serem capturados por um analisador de pacotes (MITNICK; SIMON, 2005)

[13]BIOS: “Basic Input/Output System”, ou “sistema básico de entrada e saída”. Ele é um dos principais componentes de um computador, por ser o responsável pela execução de tarefas indispensáveis para o funcionamento dele.

4.2.3 VAZAMENTO DE DADOS DE CONTAS DO LINKEDIN

Em 2012, um foi exposto em um fórum popular uma lista com 6,5 milhões de senhas de usuários do LinkedIn, uma rede social focada no campo profissional, onde é possível se conectar com profissionais de todo o mundo e mostrar seu perfil para empresas que buscam novos funcionários, nesse fórum membros eram contratados para hackear senhas complexas. Segundo a empresa estimasse que esse vazamento afetou mais de 117 milhões de contas. Após serem contratados, os hackers perceberam a identificaram muitas senhas com uma variação da palavra “LinkedIn” nelas. (KREBS, 2016)

Após a descoberta desse vazamento, o LinkedIn forçou uma redefinição de senhas em todas as 6,5 milhões de contas afetadas, porém, logo depois foi descoberto que existia um movimento de vendas desses dados:

> O LinkedIn respondeu forçando uma redefinição de senha em todas as 6,5 milhões de contas afetadas, mas parou por aí. Mas hoje cedo, surgiram relatos sobre um segmento de vendas em um bazar de crimes cibernéticos on-line no qual o vendedor se ofereceu para vender 117 milhões de registros roubados na violação de 2012. Além disso, o mecanismo pago de busca de dados hackeados LeakedSource afirma ter uma cópia pesquisável do banco de dados de 117 milhões de registros. (KREBS, 2016).

4.2.4 SPYWARE

Spyware é um termo para um software malicioso que tenta infectar seu computador ou dispositivo móvel e que coleta informações sobre você, sua navegação e seus hábitos de uso da Internet, bem como outros dados. Ou seja, ele monitora e copia tudo que está sendo digitado, carregado, baixado e armazenado no dispositivo. Quanto mais tempo ele ficar sem ser detectado, mais prejudicial pode ser, pois o *spyware* foi projetado para ser indetectável via formas comuns, como o escaneamento de antivírus. (SEGUIN, 2021, adaptação nossa).

Existem algumas empresas que o utilizam como forma que monitoramento de seus funcionários, como cita o trecho a seguir:

> De fato, existem alguns casos em que o uso de spyware é justificado. Por exemplo, seu empregador pode ter uma política de segurança que permita usar software para monitorar o uso de computadores e dispositivos móveis dos funcionários. O objetivo do spyware empresarial geralmente é proteger informações proprietárias ou monitorar a produtividade dos funcionários. O controle dos pais que limita o uso do dispositivo e bloqueia o conteúdo adulto também é uma forma de spyware. (SEGUIN, 2021)

Como dito acima, o *spyware* é usado para espionar e registrar as atividades que o usuário está fazendo em seu dispositivo. Uma vez instalado no dispositivo, o *spyware* tem variedade de opções de coletar as informações, como gravar áudio e capturar a tela, observar o conteúdo de redes sociais, e-mails e mensagens e capturar o histórico do navegador (SEGUIN, 2021).

A variedade de tipos de *spyware* existem para diversas opções, que vão desde monitorar e armazenar as atividades online até exibir anúncios indesejados enquanto navega pelo dispositivo. Há diversos tipos de *spyware*, como por exemplo:

> - ***Adware*** exibe anúncios automaticamente enquanto você navega na internet ou usa um software financiado por publicidade.
> - ***Infostealers*** coletam informações do seu computador ou sistema móvel, verificando seu computador em busca de informações específicas e coletando seu histórico de navegação, documentos e mensagens.
> - ***Cookies*** podem ser úteis. Por exemplo, eles fazem o login instantaneamente em seus sites favoritos e veiculam anúncios de produtos e serviços de acordo com seus interesses. Porém, **cookies de rastreamento** podem ser considerados spyware, pois monitoram a navegação, compilam o histórico de navegação e registram tentativas de login. Com o conhecimento e as ferramentas certas, um hacker "maligno" pode usar esses cookies para recriar suas sessões de login.
> - ***Rootkits*** permitem que criminosos se infiltrem em computadores e dispositivos móveis e os acessem em um nível muito profundo. Para isso, eles podem explorar vulnerabilidades de segurança, usar um cavalo de Troia ou fazer login de administrador em um computador. (AVAST, 2021).

4.2.5 BRASIL É PRINCIPAL ALVO DE ROUBOS DE DADOS BANCÁRIOS

De acordo com um levantamento da ESET, uma empresa de companhia de segurança de informação, o Brasil é o primeiro colocado em número de casos de *spyware* entre os países da América Latina:

> [...] O país concentra a maior distribuição de programas espiões (27%), seguido do México (21%) e Peru (14%). A pesquisa analisou os casos de spyware na América Latina de setembro de 2018 a setembro de 2019 e concluiu que as ameaças mais comuns no país são Mekotio (24%) e Amavaldo (89%). (Ribeiro, 2019)

O Mekotio e o Amavaldo são exemplos de um trojan bancário, cuja finalidade é o roubo de dados bancários e informações financeiras de clientes e quando acessados pelos dispositivos já infectados. (TRUST CONTROL, 2021)

No caso do "Mekotio", o invador se passa por uma empresa para enviar um e-mail com um link armadilha para o usuário. Ao baixar o conteúdo do link, ele sem sabendo acaba

por instalar um trojan sem perceber. O “Amavaldo” trabalha com o roubo de credenciais bancárias e informações financeiras, além de monitorar as abas abertas no navegador. (RIBEIRO, 2019)

> Entre setembro de 2018 e setembro de 2019, o Brasil ficou na segunda posição em relação a quantidade de ataques com o trojan bancário Mekotio, com 24%, atrás apenas do Chile, que tem 70%. Esse tipo de vírus se passa por uma empresa que envia um link para uma fatura. Quando o usuário baixa o arquivo, instala o trojan no computador.
> Já no caso do spyware Amavaldo, o Brasil liderou como o país da América Latina com o maior número de ataques, representando 89%, no período de janeiro de 2019 a setembro de 2019. A ameaça está presente no Brasil e no México (10%) e finge ser um programa legítimo para roubar credenciais bancárias e dados financeiros. Por exemplo, ele monitora as abas ativas no computador da vítima e mostra uma janela pop-up falsa que imita o banco para roubar dados privados da pessoa. O Amavaldo também captura fotos pela webcam, keylogger, executa códigos, entre outros. (RIBEIRO, 2019)

5 ESTUDO DE CASO

Todos os anos são publicadas notícias de empresas e corporações que sofreram de invasões virtuais ou, que tiveram as informações armazenadas em seus bancos de dados vazadas por criminosos virtuais, mais conhecidos como "*hackers*". Estes dados que seriam da própria corporação incluem informações financeiras, informações de funcionários, colaboradores, parceiros, como também, informações pessoais de seus usuários e de pessoas que utilizam de seus serviços.

Nenhuma empresa está 100% segura de um vazamento de dados, com isto ocorrendo até mesmo em empresas de grande porte, que já foram vítimas de ataques virtuais, como Facebook, Zoom, Banco Inter, Netshoes, Adobe e Uber.

Esses acontecimentos demonstram que qualquer empresa pode ser vítima de invasões virtuais ou de dados, que são assuntos de extrema importância, já que tanto a reputação da empresa, como a reputação de seus funcionários, usuários, e colaboradores pode ser desfavorecida, uma vez que suas informações sensíveis podem ser utilizadas por terceiros, uma situação que poderia trazer inúmeras complicações a todas as vítimas dos vazamentos.

Um exemplo que ocorreu no dia 7 de março de 2022 publicado no site da Olhar Digital, foi o caso da empresa Mercado Livre, uma empresa Argentina, que é o maior e-commerce da América Latina, especializado no setor de comércio eletrônico. A empresa tem mais de 140 milhões de usuários ativos únicos, e cerca dos 300 mil deles tiveram seus dados acessados, representando 0,2 por cento (%) do total de usuários da companhia. (LIMA, 2022).

A empresa alega que sofreu um acesso indevido no código-fonte de sua plataforma Web, uma brecha que foi aproveitada pelos invasores para causar esse crime virtual, mas nenhuma evidência foi encontrada de que seus sistemas de infraestrutura tenham sido prejudicados ou comprometidos. E que, também, as senhas de seus usuários, saldos em contas, investimentos, informações financeiras, e informações de cartões de crédito, ou débito estão seguras. Após esse ataque, a empresa afirmou que tomará medidas rigorosas para evitar novos incidentes parecidos, e que esse vazamento será investigado. (LIMA, 2022).

5.1 O MAIOR VAZAMENTO DE DADOS DA HISTÓRIA DO BRASIL

No início de 2021, foi descoberto um caso sem precedentes no nosso país: Intitulado de "O maior vazamento de dados da história do Brasil" (HIGA, 2021), a

empresa de serviços de crédito Serasa sofreu com uma grave exposição de dados, pois as informações de mais de 220 milhões de brasileiros foram expostas, incluindo dados sigilosos como nome e endereço completo, renda, CPF, fotos dos indivíduos e diversas informações adicionais, contendo até mesmo dados sobre pessoas falecidas.

Ventura (2021) explica que são dois vazamentos iguais, distintos apenas pelo hacker que decidiu expor tais informações ao público. Este vazamento "possui dados de 223,74 milhões de CPFs distintos, e aparentemente foi compilado em agosto de 2019", mas ele só foi exposto no ano seguinte, em 2020. De início, todas estas informações foram divulgadas na *Deep Web* (uma seção oculta da internet comum, com conteúdos sensíveis e acessíveis apenas para usuários avançados), mas logo depois esta base de dados intitulada "Serasa Experian" começou a aparecer na "internet comum", sendo indexada em serviços de pesquisa, como o Google. Os redatores do site Tecnoblog, unidos com um grupo da tecnologia da informação intitulado de *DataBreaches* fizeram um resumo das informações que constam de cada um dos 223 milhões de brasileiros afetados, informações básicas e sensíveis como:

> I. Nome, RG, CPF, gênero, data de nascimento, nome do pai, nome da mãe e estado civil.
> II. E-mails, telefones e fotos do rosto.
> III. Endereços, logradouro, número, bairro, cidade, estado e CEP.
> IV. Nível de escolaridade.
> V. Salário, emprego, local de trabalho e CNPJ.
> VI. Título de eleitor, número de inscrição, zona e seção.
> VII. INSS: nome do segurado, número do benefício e data de início.
> X. Devedores: nome, tipo do devedor (principal ou corresponsável), situação (ativa, em cobrança ou ajuizada), e tipo de dívida.
> XI. Óbitos: Data de falecimento, idade, nome e endereço do cartório (RODRIGUES, 2021, adaptação nossa).

Em reação a este vazamento, alguns meses depois, em março de 2021, a Polícia Federal iniciou a Operação *Deepwater*, e eles identificaram e localizaram o principal suspeito e o prenderam com sucesso por cometer crimes de obtenção, divulgação e comercialização de dados. Além disso, ele é suspeito de ter participado de um ataque ao Sistema do Tribunal Superior Eleitoral (TSE), em 2020. (HIGA, 2021)

Essa invasão *hacker* aos sistemas do Tribunal Superior Eleitoral (TSE) foi motivo da criação de um novo mandato e busca de apreensão, com a nova Operação

"*Exploit"*, a operação que prendeu em novembro de 2020, um dos suspeitos de invadir os sistemas do Tribunal Superior Eleitoral.

"Ele é investigado por ter participado da invasão que expôs informações administrativas de ex-servidores e ex-ministros do TSE antes do 1º turno das eleições municipais do ano passado." (G1, 2020)

De acordo com o jornal R7, em uma notícia publicada em março de 2021, a Operação *Deepwater* foi uma operação que investiga os fatos criminosos relacionados à obtenção, divulgação e comercialização de dados pessoais de brasileiros, dentre esses, diversas autoridades públicas. E que, em janeiro de 2021, essas investigações apuraram que, por meio da internet, inúmeros dados sigilosos, tanto de pessoas físicas como jurídicas, tais como: CPF/CNPJ, nome completo, e endereço foram disponibilizados para terceiros, em um fórum na internet especializado em trocas de informações.

5.2 VAZAMENTOS DE CHAVE PIX

O Pix, um serviço de pagamento eletrônico instantâneo, e gratuito, que é oferecido pelo Banco Central do Brasil, tanto para pessoas físicas como jurídicas. Ele funciona por 24 horas, sete dias por semana, com este serviço sendo disponibilizado no dia 16 de novembro de 2020, com o princípio de facilitar e agilizar o processo de transferência monetária entre contas.

No dia 21 de janeiro de 2022, o Banco Central comunicou que 160 mil dados cadastrais de clientes foram vítimas de vazamento. Esse incidente ocorreu entre os dias 3 e 5 de dezembro de 2021 e é o segundo caso de vazamento ocorrido e informado pelo Banco Central.

> Não foram expostos dados sensíveis, tais como senhas, informações de movimentações e saldos financeiros em contas transacionais, ou quaisquer outras informações sobre sigilo bancário. As informações obtidas são de natureza cadastral, que não permitem movimentação de recursos, nem acesso às contas ou outras informações financeiras (G1, 2022).

O Banco Central também informou que, aqueles que tiveram seus dados cadastrais vazados serão informados exclusivamente através do próprio aplicativo, ou pela internet banking de seu próprio banco.

No dia 30 de setembro de 2021, ocorreu o primeiro vazamento de dados registrado pelo Banco Central. Dados cadastrais que estavam sob a guarda e segurança do Banco do Estado de Sergipe, a Banese, foram vazados devido a um ataque virtual por *hackers*.

Segundo a direção da empresa, o vazamento ocorreu por conta de “falhas pontuais em sistemas da instituição financeira, e envolveu informações de natureza cadastral, que não dão margem à movimentação de recursos ou acesso a contas”. (G1, 2021)

“Não foram expostos dados sensíveis, tais como senhas, valores, movimentados e saldos nas contas. Os telefones de clientes, no entanto, foram capturados por pessoas de fora da instituição”. (MÁXIMO, 2021)

De acordo com o G1, em uma notícia publicada em janeiro de 2022, o Banco Central reiterou que o vazamento não afetou a confidencialidade de senhas, histórico de transações, ou demais informações financeiras dos clientes, e destacou que está trabalhando na apuração dos fatos e na implementação de mecanismos de segurança para evitar que casos semelhantes não voltem a ocorrer.

5.3 BANCO PAN SOFRE VAZAMENTO DE MILHARES DE CLIENTES

O Banco Pan confirmou, no dia 15 de abril de 2022, um vazamento parcial de dados e informações pessoais de seus clientes devido a uma invasão, mas a empresa afirma que informações de cartões como senhas não foram vazadas, apenas outras informações, como: nome completo data de nascimento, CPF, endereço de residência e saldo devedor (VALTRICK, 2022).

O banco disse que “ocorreram cópias não autorizadas dos dados cadastrais dos clientes” assim como o limite disponível e do saldo devedor. Também foi afirmado que “os órgãos competentes já foram notificados, conforme exige a Lei Geral de Proteção de Dados (LGPD)”, e que “não houve risco financeiro direto para os clientes” (BARROS, 2022).

O Banco Pan apresenta aproximadamente 17 milhões de clientes cadastrados em seus sistemas, e que ao menos 64 mil desses 17 milhões de clientes tiveram seus dados vazados, e que o problema aconteceu através de uma empresa terceirizada, responsável pela central de atendimento ao cliente (VALTRICK, 2022). De acordo com a Polícia Civil de Minas Gerais, um homem do mesmo Estado estaria “exigindo” resgate dos dados que foram vazados, pedindo que as vítimas realizassem pagamentos em *Bitcoins* (moeda virtual para transações financeiras) para o meliante (BARROS, 2022, adaptação nossa).

5.4 FACEBOOK (META) SOFRE VAZAMENTO DE 533 MILHÕES DE USUÁRIOS

Na data de 3 de abril de 2021, a empresa Facebook (hoje conhecida pelo novo nome, "Meta") foi mais uma vítima de ataque *hacker*, onde os criminosos acessaram e vazaram os dados de 533 milhões de usuários do Facebook. No banco de dados da empresa, estão armazenadas informações como, nome completo, telefone, data de nascimento, endereço e endereço de e-mail (FANTINATO, 2021).

O acesso indevido dos criminosos ocorreu por uma brecha na plataforma da empresa, que já foi corrigida. Mas só pelo fato de as informações dos usuários já terem sido disponibilizadas em fóruns de *hackers*, elas ainda podem ser usadas por criminosos virtuais, dando-os a oportunidade de cometer golpes e fraudes usando as informações das pessoas que foram vítimas do vazamento.

5.5 ANONYMOUS VAZA BANCO DE DADOS DE MINISTÉRIO DE COMUNICAÇÕES DA RÚSSIA

Em março de 2022, o grupo de ativistas *Anonymous* aplicou mais um golpe contra o governo da Rússia para mostrar sua oposição contra os ataques russos à Ucrânia. (DEMARTINI, 2022)

Esse grupo é formado por um conjunto de pessoas desconhecidas, por isso possuem o nome de "*Anonymous*", que remete ao termo "anônimo", ou "anonimato", ou seja, total desconhecimento da identidade dos participantes. O grupo é uma espécie de "coletivo *hacker*", onde os membros se intitulam como "ativistas da liberdade digital", pois são a favor de favorecer o povo. Os *Anonymous* são mundialmente conhecidos devido as suas atividades benéficas à liberdade, e ataques considerados criminosos.

De acordo com uma publicação de março de 2022 no site Canaltech, os arquivos vazados teriam uma quantidade maior que 526 GB (Gigabytes), com um total de 43,5 mil diretórios com informações pertencentes a atos do ministério e informações do setor de recursos humanos, onde também podem possuir dados pessoais de servidores, e integrantes do governo, como também, pesquisas relacionadas à mídia e tecnologias de comunicação usadas na Rússia (DEMARTINI, 2022).

“A agência reguladora tem sido um dos principais alvos das ações do grupo, que afirmam lutar pela liberdade do povo Ucraniano, e desejar mostrar à população russa a verdade sobre a invasão do país vizinho” (DEMARTINI, 2022).

De acordo com o Canaltech, o grupo *Anonymous* tinha declarado guerra à Rússia desde o final de fevereiro, realizando ataques de negação de serviço e desfiguração contra sites e agências do governo, como também outros vazamentos de dados.

6 BOAS PRÁTICAS DE PREVENÇÃO DE VAZAMENTOS

No contexto das tecnologias do presente mundo, a segurança e as medidas de prevenção contra vazamento dos dados que se encontram na internet se tornam cada vez mais necessárias, se considerarmos o fato de que as tecnologias estão cada vez mais presentes no dia-a-dia das pessoas, o que torna necessário também a inserção de dados pessoais, como CPF, RG, endereço e nome completo para a utilização de tais benefícios, como um acesso a um site de compras online ou para realizar transações bancárias, por exemplo.

Porém, na maioria dos casos, tais dados pessoais ficam salvos nos servidores e endereços de tal empresa, atitude que pode tornar seus clientes suscetíveis a sofrerem uma ilegal exposição de seus dados online, mediante a invasão e a exposição dos dados por terceiros. Graças a isso, a privacidade das informações pessoais não depende somente do usuário, mas também da corporação que os detém. É de se considerar também que, da mesma maneira que as tecnologias estão mais avançadas e presentes no cotidiano comum, as técnicas de invasão e brecha de sistemas, bancos de dados etc. estão avançando também, atitude que necessita de cautela extra, tanto por parte das empresas como por parte de seus usuários.

Apesar de tudo, a responsabilidade da segurança da conta e as informações contidas na mesma ainda continuam sendo do indivíduo que a usa, já que existem métodos e ferramentas para prevenção e identificação de vazamentos.

6.1 A IMPORTÂNCIA DE SE ESCOLHER UMA FORTE SENHA

O objetivo de se escolher uma boa senha vem da proteção que ela providencia contra técnicas de invasão comuns, como os ataques de força bruta, que consistem em “[...] tentativa de violar uma senha ou um nome de usuário, encontrar uma página da Web oculta ou descobrir uma chave usada para criptografar uma mensagem, usando uma abordagem de tentativa e erro [...]” (KASPERSKY, s.d).

Isso é feito por meio de ferramentas especializadas para ataques deste tipo, onde o programa percorre as palavras de um dicionário e as tenta utilizar como login ou senha de usuário, tentando tanto as próprias palavras como também permutações dela com caracteres e números. O programa também pode-se utilizar de algum banco de

dados com diversos usuários e senhas, provenientes de diversos vazamentos de dados online, para então testar todas as combinações e catalogar quais delas ainda funcionam.

6.1.1 METODOLOGIAS E RECOMENDAÇÕES PARA A CRIAÇÃO DE UMA FORTE SENHA

De acordo com Charlotte Empey, Diretora de Marketing da Avast, uma respeitável empresa de antivírus, uma senha forte deve conter:

I. A senha deve ser longa. Este é o ponto mais importante. Não crie uma senha abaixo de 15 caracteres, e use mais se possível.
II. Utilize uma mistura de caracteres. Misture letras maiúsculas, minúsculas, números e símbolos, pois isso irá fortalecer bastante a sua senha, e tornar um ataque de força bruta mais difícil de suceder.
III. Evite substituições comuns. Hackers estão cientes de substituições comuns que pessoas utilizam como senha, por exemplo, trocar algumas letras de uma palavra comum por números (trocar “senha” por “s3nh4”). Hoje em dia, uma senha eficaz é mais forte com distribuições aleatórias de caracteres do que com substituições de letras com números [...].
IV. Não utilize sequências comuns do teclado. Semelhante a dica acima, não utilize sequências do teclado na sua senha, como “qwerty”, pois estas são fáceis de se advinhar. (EMPEY, 2018, tradução nossa)

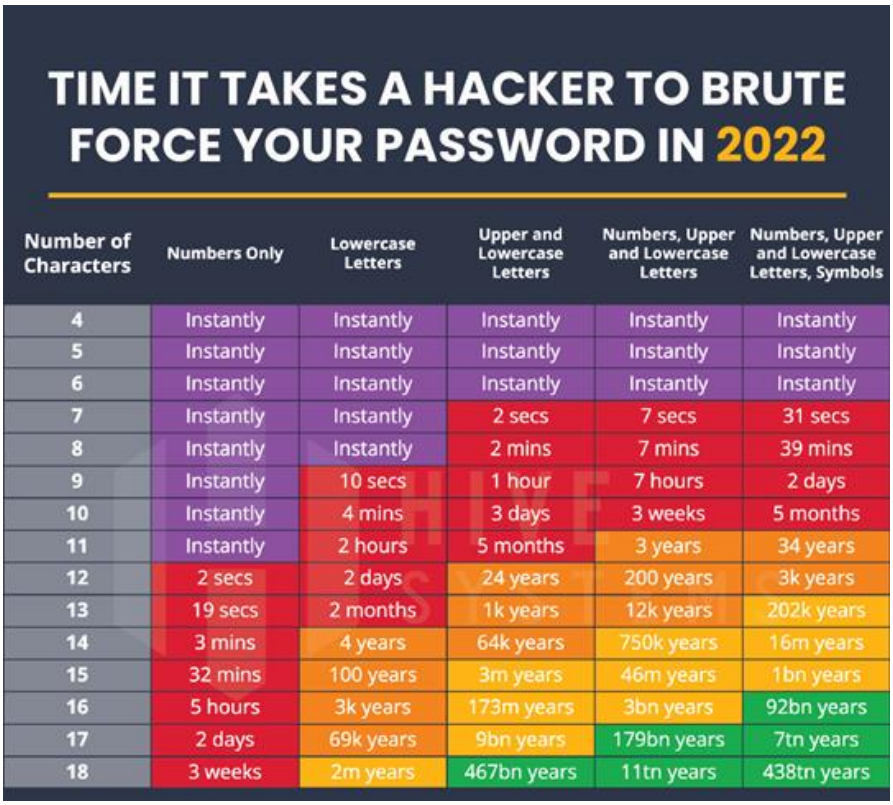
E para complementar as informações acima, Empey sugere metodologias para a criação de uma senha completamente eficaz contra este tipo de ataque:

I. Método da “senha revisada”: Uma variante do método de múltiplas palavras em uma senha, que consiste em utilizar palavras bizarras e incomuns. Utilize nomes próprios, nomes de figuras históricas, palavras em outras línguas etc. (exemplo: “QuagmireHancockMerciDeNada”). Você deve compor uma frase que seja longa, mas simples de lembrar, e para aumentar a complexidade da senha, você pode também adicionar caracteres (números, símbolos) no meio ou entre as palavras selecionadas.
II. Método da “sentença”: Este método consiste em criar uma frase aleatória e então definir uma senha nela por meio de uma regra criada por você mesmo. Por exemplo, retirando as três primeiras letras de cada palavra na frase “Uma trinca de trancas trancou Tancredo.” lhe dá a sentença “UmatridetratraTan”. Uma pessoa que

> observar esta frase não entenderá nada, mas para você fará todo sentido por saber da regra definida. Lembre-se de formar uma sentença que seja o mais pessoal e menos possível de se advinhar. (EMPEY, 2018, tradução e adaptação nossa)

Em resumo, quanto mais forte a sua senha for, mais difícil será dela ser adivinhada ou até mesmo impossível de o fazer, conforme a Figura 4, que ilustra a quantidade de tempo necessária para um hacker adivinhar sua senha por ataque de força bruta, em 2022:

Figura 4 - a quantidade de tempo necessária para um hacker adivinhar sua senha por ataque de força bruta, em 2022



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Fonte: Adaptado de HIVE SYSTEMS, 2022.

6.2 CUIDADOS AO SE NAVEGAR PELA INTERNET

Por mais que todas as dicas acima sejam extremamente úteis para proteger a conta do indivíduo, infelizmente uma forte senha, o uso da verificação em duas etapas e qualquer outro método de segurança feita pelo usuário ainda não é o suficiente, pois basta apenas um acesso indevido aos sistemas do tal site ou função para que os seus dados possam ser expostos na internet, atitude essa que ocorreu recentemente com o site

de compras online Americanas e outros sites gerenciados pela mesma empresa[14]. O consumidor não pode fazer nada quanto a este tipo de invasão, já que a segurança dos servidores e afins são de responsabilidade exclusiva da empresa dona e/ou empresa contratada para o gerenciamento do setor tecnológico.

Além disso, existem também métodos de brechas que conseguem burlar senha e autenticação, como o *phishing*, que é o tipo de golpe mais comum na Internet, de acordo com um artigo do Banco Pan (2021), que explica: "[...] uma das fraudes mais corriqueiras na internet [...] é um tipo de fraude eletrônica, caracterizada por tentativas de adquirir dados pessoais de vários tipos: nome de usuário, senhas, números de cartões de crédito e conta bancária e outras informações de cadastro." Belcic (2021) comenta sobre a origem do nome, como também do significado:

> Por isso phishing recebe seu nome: O cibercriminoso vai "pescar" (em inglês, "fishing") com uma atraente "isca" para fisgar as vítimas do vasto "oceano" dos usuários da internet. O ph em "phishing" vem de "phreaking de telefone" que surgiu em meados de 1900, no qual os "phreaks", ou seja, entusiastas, faziam experimentos com as redes de telecomunicações para descobrir como elas funcionavam. Phreaking + fishing = phishing.

Este golpe é um dos mais perigosos da Internet, por se tratar de um método de engenharia social feita especialmente para roubar as informações de usuários, onde os principais alvos são grupos de pessoas que têm tendência a não saberem utilizar os recursos da internet, como idosos e pessoas em situação vulnerável (por conta de dívidas, falta de emprego etc.). O golpista entra em contato com a vítima, mais comumente por e-mail ou raramente por ligação de celular alegando alguma razão totalmente chamativa e absurda, como por exemplo, que a pessoa ganhou na loteria ou recebeu uma herança de algum indivíduo de status de realeza, notavelmente sendo um "Príncipe Nigeriano" ou algum "parente" dele, conforme o exemplo da Figura 5:

[14] Em fevereiro de 2022, a empresa Americanas registrou um "acesso não autorizado" aos servidores do site de mesmo nome e de outros gerenciados por eles, e graças a isso a companhia decidiu remover seus sites do ar temporariamente, o que causou prejuízos ao lucro da empresa. Mais informações em: <https://g1.globo.com/tecnologia/noticia/2022/02/22/sites-da-americanas-e-do-submarino-seguem-fora-do-ar-pelo-terceiro-dia-seguido.ghtml>. Acesso em: 22 abr. 2022.

Figura 5 - Exemplo de e-mail de phishing – Príncipe Nigeriano

Fonte: Adaptado de USECURE.IO, s.d.

Estes tipos de golpes existem em diversas formas, mas no seu núcleo, a atitude é sempre a mesma: Alguma pessoa que você nunca ouviu falar na vida está te prometendo uma enorme quantia, mas para obtê-lo você deve realizar um depósito para o seu "beneficiário", e é assim que o golpista lucra pois o dinheiro prometido a você nunca existiu desde o início. Este estilo de golpe não é comum no Brasil, mas ainda assim é recomendado a cautela do usuário, principalmente porque há outra modalidade deste mesmo esquema que é mais comum no nosso país, o *phishing* por link falso.

Ele opera somente pelo e-mail e consiste no farsante enviar e-mails falsos, mas com a aparência de que se fossem legítimos e de grande urgência, como algum aviso de brecha em algum serviço usado pelo leitor ou alguma falha em uma transação ou serviço bancário. Nesse sentido, Ariane enfatiza as quatro principais características deste método:

> 1. O senso de urgência é uma característica comum dos criminosos virtuais. Eles pedem que você aja rápido para criar o sentimento de urgência e, se você não fizer o que ele pediu naquele momento, você vai perder esta super chance da sua vida. Ignore estes e-mails.
>
> 2. Frases de efeito como "seu serviço será suspenso se…" ou "sua conta foi bloqueada, clique aqui para verificar" são abordagens comuns de phishing. Mais uma vez, verifique diretamente com a instituição referida, seja banco ou

> órgão governamental (os mais usados), antes de qualquer medida. Empresas sérias nunca dão prazos curtos e com esse tipo de abordagem aos clientes e usuários.
>
> 3. Estes e-mails ou mensagens vêm acompanhados de links externos para que você clique e então abra as portas para a invasão. Um jeito de verificar a intenção deste link antes de clicar é passar o mouse em cima do link para ver a URL. Mas fique atento. Os criminosos registram domínios muito parecidos com o domínio original da empresa em que fingem ser.
>
> 4. Ao receber e-mails de desconhecidos, que já são por si só suspeitos, fique atento quanto aos anexos da mensagem. Extrato de conta, comprovante de depósito, multa ou até propostas de trabalho são gatilhos usados para induzir o usuário a clicar em links que contém vírus e roubam dados. (ARIANE, 2021)

A Figura 6 exemplifica como que um e-mail desses aparece para o usuário e mostra também meios de identificá-lo. 1) Endereço falso, com o nome de uma notória empresa mas que não há relação nenhuma com a mesma; 2) Mensagem escrita com um senso de urgência, para o usuário achar que deve tomar ação imediata; 3) Link fraudulento, que pode ser verificado ao passar o ponteiro do mouse no botão, sem clicar ele, pois se clicado ele poderá causar danos aos dados e/ou computador do usuário.

Figura 6 - Exemplo de e-mail de phishing – Site falso

Fonte: MILLANEZ, Eduardo. 2019, adaptação nossa.

Felizmente, para o usuário comum, este tipo de mensagem costuma ser rapidamente filtrada pelos próprios sistemas do provedor, que as enviam direto para a caixa de spam (e-mails desnecessários), que logo após são deletados automaticamente.

E ainda assim, caso um e-mail considerado suspeito pelo sistema seja aberto, uma mensagem destacada na tela imediatamente avisa os perigos de se comunicar um remetente desconhecido. Por exemplo, no serviço Gmail da empresa Google, a seguinte mensagem é mostrada: “Esta mensagem parece perigosa. Mensagens semelhantes foram usadas para roubar informações pessoais. Não clique em links, não faça o download de anexos nem responda com informações pessoais.” (GOOGLE, 2022).

Há de se considerar também que o *phishing* não ocorre necessariamente de uma interação entre indivíduos, ele pode acontecer também sem contato de ambas as partes uma com a outra, atitude que pode ocorrer quando a vítima conecta o seu dispositivo (computador, notebook, smartphone) em uma rede WiFi[15] pública. Esta atitude é uma coisa altamente perigosa e uma coisa que deve ser evitada sempre que possível, dado que uma rede dessas tem pouca ou nenhuma segurança contra invasões, afirmação feita por TAGIAROLI, HYPPOLITO et. al (2015).

> Segundo Thiago Hyppolito, engenheiro de produtos da McAfee no Brasil, cibercriminosos costumam aproveitar falhas de segurança (às vezes dos próprios roteadores, aparelhos que distribuem a internet) para bisbilhotar as atividades online dos usuários.
>
> Em computadores, um dos problemas mais simples é não configurar a rede Wi-Fi de forma apropriada. De acordo com Rodrigo Paiva, gerente de produto da D-Link (fabricante de roteadores), além da necessidade de senha, o usuário deve informar ao sistema operacional que está conectando-se a uma rede pública e que não quer compartilhar arquivos com outras pessoas.
>
> [...] Jordão afirma [...] que uma rede Wi-Fi pública há dezenas ou até mesmo centenas de conexões simultâneas. O firewall dos roteadores entende que todos os dispositivos conectados sejam “amigos” e com isto, não impede a conexão entre os dispositivos, permitindo invasão com possibilidades de captura, exclusão ou alteração de dados do dispositivo infiltrado. (MARTINS, CANCELA et. al, p.3, s.d, adaptação nossa)
>
> Uma tática comum de alguns atacantes é criar redes Wi-Fi próximas de estabelecimentos públicos. A ideia é tentar chamar a atenção do usuário com uma rede aberta e com nome semelhante à do local original. Após a pessoa efetuar o login, os cibercriminosos podem ter acesso facilmente às informações da vítima. (TAGIAROLI, 2015)

Ainda assim, se o uso de uma rede pública se tornar realmente necessário, como em uma emergência, falta de serviço de sua provedora de dados móveis etc., recomenda-se o uso de um serviço de antivírus combinado com uma VPN. “*Virtual Private Network*”, são serviços de encriptam o tráfego de Internet do dispositivo, dificultando ou impossibilitando que eles sejam vistos por outros. Além disso, as VPNs

[15] WiFi: “Wireless Fidelity”, é uma tecnologia de troca de informações (rede) sem fio.

mascaram o local onde o computador está se conectando, fazendo com que o servidor ache que ele está em outra região ou país, ação que pode permitir acesso à serviços bloqueados por região, como séries ou serviços de streaming que ainda não estão disponíveis no Brasil (TAGIAROLI, 2015).

O último risco relacionado à recursos públicos são os cuidados a se tomar em utilizar uma porta USB[16] pública, como em um ônibus ou computadores de lan-house. Rodrigues explica que este ataque é conhecido como "*juice jacking*", como também sugere também uma medida bem simples de como evitá-lo:

> É um golpe que usa o carregador USB para copiar informações de seu smartphone ou mesmo instalar arquivos maliciosos enquanto você usa uma porta USB pública para carregar a bateria do aparelho. Para evitar, use um carregador USB conectado a uma tomada ou um cabo USB somente de energia. (RODRIGUES, 2020)

6.3 FERRAMENTAS PARA SE VERIFICAR VAZAMENTOS DE DADOS

Como dito no tópico do capítulo anterior, o vazamento de dados é um mal inevitável, pois basta apenas um acesso indevido aos sistemas do tal site ou função para que os seus dados sejam expostos na internet. Entretanto, para estes fins, existem sites extremamente úteis para se verificar a proteção de suas contas, como também monitorar vazamentos recentes.

O principal e mais conhecido deles se chama "Haveibeenpwned", com o significado do nome do site sendo explicado melhor por Renato Guedes:

> "Pwned (pronuncia-se "powned") é um termo inglês que significa que algo foi dominado. A expressão como sinônimo para dados comprometidos devido a violação de bases de dados foi popularizada pelo site "have i been pwned?", um serviço que coleta e analisa informações de bilhões de contas vazadas na internet." (GUEDES, 2020)

A verificação da situação dos dados pode ser feita no site[17], onde pode-se preencher tanto o e-mail ou alguma senha utilizada em algum serviço, e então ele irá pesquisar em seu gigantesco banco de dados de vazamentos para então avisá-lo se houve alguma correspondência com algum dado armazenado, conforme o exemplo da Figura 7. 1) Tela inicial do site, traduzida para português. Basta apenas preencher um e-

[16] USB: "*Universal Serial Bus*", é uma entrada para a conexão de um periférico com dispositivos compatíveis, como um computador podendo ter conectado um mouse, um teclado, um monitor.
[17] https://haveibeenpwned.com

mail, apertar o botão “pwned?” e o site dirá se alguma conta associada ao e-mail já foi comprometida, e se sim, ele te dirá onde e quais dados foram vazados, e adicionalmente, pode-se verificar da mesma maneira as senhas que já foram comprometidas na opção “Passwords” (senhas). 2) Aviso de que o e-mail ou senha já foi comprometida (ou não), junto com os locais onde o site encontrou correspondências; 3) A quantidade atual de sites, contas e repositórios nos quais sofreram vazamentos e foram detectados pelo site.

Figura 7 - Haveibeenpwned, exemplo de verificação de vazamentos por e-mail

Fonte: HAVEIBEENPWNED, 2022, tradução e adaptação nossa.

A quantidade de informações que o site mostra que foram vazadas é impressionante e é um número que cresce mais a cada dia. Santos explica que isso não acontece por acaso, sempre há um motivo por trás:

> Em geral, dados são roubados para serem vendidos no mercado negro, expostos na dark web ou por interesse específico de hackers em determinados conjuntos de dados. O domínio de contas e informações pessoais pode viabilizar muitos outros golpes, tais como extorsão, roubo de identidade, spam de phishing ou malware, uso indevido de cartões de crédito ou das credenciais de acesso em outros sistemas online. (SANTOS, 2020)

Em conclusão, caso o e-mail tenha sido verificado e o usuário tenha percebido que alguma das contas associada a ela foi “pwnada”, o primeiro passo é entrar na tal conta do tal serviço para alterar a senha (ou melhor ainda, deletar a conta caso seja um serviço que você não utilize mais).

Logo em seguida, mesmo que a tal pessoa não tenha sido afetada é altamente recomendado ativar a autenticação de dois fatores quando possível e utilizar senhas únicas para cada site. Este último ponto é muito importante, visto que se alguma conta de um serviço tiver a senha exposta na internet, o invasor não conseguirá acessar nenhuma outra conta de outros serviços pertencente à mesma pessoa apenas por tentar logar com a senha do vazamento, como também ele não conseguirá acessar o e-mail (que é a central de todas as outras contas) e consequentemente causar um problema maior, coisa que não acontecerá com alguém que utiliza a mesma senha para todos os serviços que usa.

7 SOLUÇÕES DE MERCADO PARA MITIGAR VAZAMENTOS

No momento atual em que vivemos, prevenir uma pessoa física ou jurídica de ter seus dados vazados pode ser algo complicado, pois na internet, os dados são muito valiosos e altamente procurados. Possuir o CPF (Cadastro de Pessoa Física), CNPJ (Cadastro de Pessoa Jurídica), o nome completo, a data de nascimento, e-mail ou até mesmo o número da pessoa, permite se passar por ela em sites, cadastrar a pessoa em lugares da internet que ela não quer e até mesmo burlar o site e entrar nas contas que ela já possui cadastro. Por isso, nenhum site deve expor os dados do usuário e para isso necessita-se de uma segurança reforçada.

Há inúmeras formas de mitigar esses vazamentos com soluções disponíveis no mercado, para diversos fins, como a hard wallet, firewall, a VPN, autenticação de 2 fatores, tokens e alguns serviços de senhas como o Lastpass. Entretanto, todas as organizações que trabalhem com dados precisam de um chefe de segurança ou de um encarregado dos dados, porque são eles que devem estar em contato com o CEO para influenciar e abordar a importância da segurança de dados e a importância de seguir a Lei Geral de Proteção aos Dados.

7.1 HARD WALLET

A hard wallet é uma carteira de hardware ou carteira física," [...] é um dispositivo físico eletrônico, desenvolvido com o único propósito de guardar e proteger seus Bitcoins [...]" (bitPreço, s.d). As *hard wallets* não são apenas para proteger Bitcoins[18], elas servem para proteger todas as criptomoedas[19] existentes.

As "carteiras rígidas" usam um dispositivo separado para armazenar as chaves privadas dos tokens mantidos e são considerados muito mais seguros do que as carteiras baseadas em software (KOGON, 2017, tradução nossa). Ou seja, de acordo com Kogon, as *Hard wallets* são a melhor maneira de proteger tokens e criptomoedas.

[18] Bitcoins são moedas virtuais – a primeira criada no mundo – e pode ser usado para a compra de serviços, produtos e quaisquer outros itens em estabelecimentos que aceitem ser pagos com ele.
[19]Criptomoeda é o nome genérico para moedas digitais descentralizadas, criadas em uma rede blockchain, a partir de sistemas avançados de criptografia que protegem as transações, suas informações e os dados de quem transaciona.

[19]A blockchain é um livro-razão compartilhado e imutável que facilita o processo de registro de transações e o rastreamento de ativos em uma rede empresarial.

A hard wallet é similar a um pendrive e é um dispositivo que conecta ao computador para a transferência de fundos de criptomoedas. Após o uso da *hard wallet*, o recomendado é que o dispositivo seja guardado em um local seguro e sem estar conectado à internet, onde ela funciona armazenando a chave privada ou senha que dá acesso à carteira de criptomoedas.

” [...]Conhecido como Cold Storage (armazenamento frio), sua principal função é mitigar as chances de ataques de hackers[...]” (bitPreço, s.d). O *hacker* pode entrar no seu computador ou no servidor da sua empresa, mas se o ele não possuir a hard wallet em mãos, ele não conseguirá fazer nenhuma transação e não terá êxito em roubar as criptomoedas.

O grande diferencial é que esses dispositivos ficam permanentemente desconectados da internet e caso ele seja extraviado ou roubado, ainda assim é possível recuperar suas chaves privadas no próprio software da *hard wallet*.

A maioria destes dispositivos custa entre R$ 600,00 e R$ 1.900,00 e as marcas mais famosas são a Trezor, a Ledger e a Digital BitBox, onde o custo é relativamente baixo quando se fala na segurança dos seus investimentos digitais. Em suma, é altamente importante que todas as empresas e pessoas físicas que compram e vendem criptomoedas utilizem *hard wallets* para a proteger as moedas digitais que ele possui.

A figura 8 mostra alguns exemplos de Hardwallets como o 1) Trezor, que há uma tela para ver as informações das transações e confirmar no botão da direita ou cancelar no botão da esquerda. Ele Possui um software para ver informações da carteira e não tem limite de criptomoedas para ser adicionado. 2) Ledger, tem a forma de um pendrive e guarda as chaves privadas da carteira digital. Há também uma tela no interior e dois botões na parte de baixo para aceitar ou cancelar as transações. 3) Digital BitBox, é uma hardwallet nova no mercado, que tem o seu código aberto e tem um diferenciado das demais: o possuimento de um chip (secure element ou chip de elemento seguro).

Figura 8 - Hard wallets

Fonte: Blog da BitPreço. **O que é Hardwallet: Vale a pena comprar?** S.d.

7.2 FIREWALL

Na computação, o firewall pode ser tanto um hardware, software ou ambos. Ele é um "[...] dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança. [...]" (Cisco, s.d)

É oportuno criar e gerenciar previamente, controles de segurança interna representando uma camada primária a segurança de dados composta por implementações de soluções de segurança e controle como: firewall, proxy, sistema de detecção de intrusão e políticas de segurança. (Correa, Luz, Ferreira, 2020)

> Os firewalls são elementos centrais na segurança da rede. No entanto, o gerenciamento de regras de firewall, especialmente para redes empresariais, tornou-se complexo e propenso a erros. Filtragem de regras do firewall devem ser cuidadosamente escritas e organizadas para implementar corretamente a política de segurança. Além disso, inserir ou modificar uma regra de filtragem requer uma análise completa da relação entre esta regra e outras regras, a fim de determinar a ordem adequada desta regra e confirme as atualizações.
>
> Firewalls não são softwares ou equipamentos que podem simplesmente serem retirados da caixa, conectados na rede e utilizados instantaneamente. Precisam ser devidamente configurados, geralmente seguindo uma política de segurança da informação corporativa, para que possam atender necessidades específicas de cada rede. Além disso, a configuração é dinâmica e precisa ser revista periodicamente, seja quando novas vulnerabilidades são descobertas, quando são efetuadas alterações na

> arquitetura da rede ou ainda quando a política de segurança da informação corporativa é modificada. (AL-SHAER, 2003, tradução nossa).

Um dos grandes desafios encontrados é a validação da configuração de sistemas de firewalls para que operem de maneira satisfatória seguindo as regras estabelecidas na política de segurança da informação da empresa. As configurações do firewall devem ser feitas pelo administrador da rede, que na maioria das vezes é um chefe de segurança da área da tecnologia da informação.

7.3 USO DE VPN (VIRTUAL PRIVATE NETWORK)

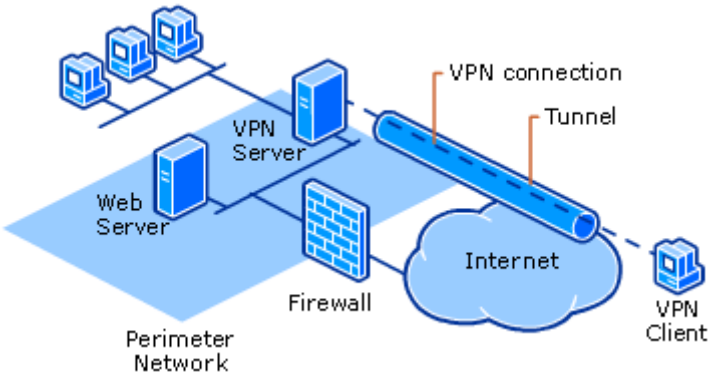
VPN é uma rede virtual que permite a duas redes se conectarem de forma segura utilizando um canal público de comunicação, onde essa tecnologia cria tuneis que transmitem os dados criptografados entre as redes. (Borges, Fábio. E.T. 2019).

Com o aumento de serviços que utilizam redes, há também o surgimento de diversos problemas de segurança. Uma forma segura de se garantir acesso remoto a uma rede é o uso de algum protocolo de Virtual Private Network (VPN) ou Rede Privada Virtual. Em VPN, a palavra Private corresponde a forma como os dados trafegam, ou seja, os dados são criptografados garantindo a privacidade das informações. O termo Virtual indica que as máquinas conectadas na rede não fazem, necessariamente, parte da rede. (Borges, Fábio. E.T. 2019)

A classificação do tráfego dos dados pode ser categorizada com base em seu objetivo final: associar tráfego com criptografia (por exemplo, tráfego criptografado), encapsulamento de protocolo (por exemplo, encapsulado por meio de VPN). (Wang et al., 2014 ; Rao et al., 2011 ; Coull e Dyer, 2014. Tradução nossa).

A VPN opera sob uma estrutura personalizada, de acordo com a figura 9. Ao criar uma conexão VPN estamos criando um túnel (Tunnel) entre as extremidades da conexão, assim os dados trafegam seguros de uma ponta até a outra. A ponta da VPN do cliente (VPN Client) entra no túnel, que faz uma proteção para o cliente navegar na internet e o IP (Internet Protocol ou Protocolo de Internet) do usuário fica localizado no servidor da VPN (VPN Server).

Figura 9 - Estrutura de uma VPN



Fonte: GTA/UFRJ. **Arquitetura de VPN. S.d**

A VPN deve dispor de ferramentas para permitir o acesso de clientes remotos autorizados aos recursos da rede corporativa e viabilizar a interconexão de redes geograficamente distantes, de forma a possibilitar acesso de filiais a matriz. Em geral, uma VPN deve estar sempre possibilitando o compartilhamento de recursos e informações, além de assegurar privacidade e integridade dos dados que trafegam pela Internet. (Borges, Fábio. E.T. 2019)

> No processo de tunelamento, o protocolo de comunicação VPN estabelece um túnel, através de vários roteadores, entre dois pontos que querem se comunicar. Depois, as mensagens são envidas de forma criptografada por dentro do túnel. Dessa forma, são formadas duas camadas de segurança sobre os dados que serão transferidos. Um ponto interessante sobre o VPN é que caso seja identificada uma tentativa de quebra da segurança, o túnel inteiro é desfeito e é então traçada uma nova rota e formado um novo túnel através de roteadores diferentes.
>
> Os túneis VPN podem ser criados dentro da rede da organização ou no próprio equipamento do usuário. O primeiro caso é chamado de gateway-to-gateway, e é muito utilizada no meio corporativo para simular uma intranet VPN. Já o segundo, chamado client-to-gateway, pode ser utilizado para criar um extranet VPN, conectando a organização a clientes e fornecedores que necessitem de acesso remoto. (GTA/UFRJ. S.d)

Somente a VPN não é o suficiente, para permitir que usuários externos tenham acesso aos recursos da rede de forma segura, é extremamente recomendado possuir outras formas de proteção, como o firewall e uma política de segurança elaborada por um chefe de segurança da informação.

7.4 TOKENS DE ACESSO

Um token de acesso é uma cadeia de caracteres randômicos que identifica um usuário, aplicativo ou Página. (Developers Facebook. s.d). Tokens de acesso são

utilizados frequentemente quando o usuário quer mudar ou excluir senhas, e-mail ou telefone. Esse tipo de autenticação é bem comum, porém é importante para a segurança de um usuário ou empresa pois, o token gerado e enviado para e-mail do usuário ou gerado em um aplicativo terceiro, comprova que aquele usuário está autenticado, ou seja, que é realmente ele que está usando o perfil ou serviço.

Com o objetivo de fortalecer ainda mais a segurança de uma conta, recomenda-se o uso dele, que também é conhecido como "Autenticação de dois fatores": De acordo com a empresa Google (2022), "Com a verificação em duas etapas, também conhecida como autenticação de dois fatores, você adiciona uma camada a mais de segurança à sua conta para o caso de a senha ser roubada."

No contexto de sites e serviços online, esta "camada a mais de segurança" mencionada pela Google é uma verificação se a pessoa que está tentando logar[20] na conta é realmente o dono da mesma, ação que normalmente tem a forma de uma mensagem SMS enviada para o número de celular cadastrado previamente na conta, contendo um código ou link (ambos de uso único) no qual o usuário precisa digitar (no site) ou acessar, respectivamente.

Esta autenticação é opcional, mas ainda assim, muitas empresas estão aderindo a este tipo de verificação, implementando-as nos seus serviços e afins, já que a conta se mantém protegida mesmo que aconteça de alguém acabar descobrindo a senha dela. Há também serviços de 2FA[21] disponíveis em aplicativos e programas, como o Authy e o Google Authenticator.

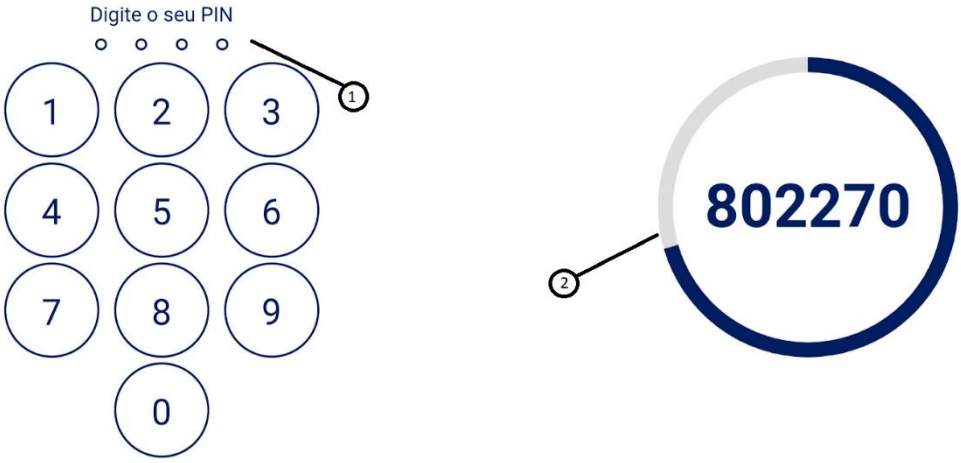
Todavia, por mais que esta tecnologia seja o suficiente em proteger contas de invasões comuns, ela ainda não é desprovida de falhas. Fazendo uma comparação com o mundo real, a autenticação de dois fatores serve como se fosse o detector de metais de um aeroporto: É uma medida adicional de segurança que serve para fazer a verificação do indivíduo que deseja entrar em um avião, permitindo ou barrando a entrada do mesmo caso ele esteja portando algo proibido... Que contenha metal em sua composição, por exemplo. O detector de metais pode ser burlado caso o objeto não seja feito de metal, ou tenha quantidades insignificantes deste material.

[20] "logar": Vem de "login" e significa o ato de entrar, "logar" em uma conta.
[21] 2FA: Significa "two-factor authentication", uma sigla em inglês para "Autenticação de dois fatores".

E quanto a verificação em duas etapas, a lógica é a mesma: É uma medida adicional de segurança que serve para fazer a verificação de uma solicitação de login, permitindo o acesso apenas se o dono confirmar que é ele mesmo que está tentando entrar na conta... Exceto se alguém usar, furtar ou hackear o celular ou dispositivo de autenticação, ou que clonem o número de celular, ou que interceptem as mensagens SMS... Assim sendo, são muitas possibilidades que necessitam da cautela do usuário a todo momento.

A figura 10 demonstra dois exemplos de tokens de acesso/autenticação de dois fatores. 1) Senha somente com números para entrar no token randômico. 2) Tokens sendo gerados de 10 em 10 segundos para acessar uma aplicação

Figura 10 - Autenticação de dois fatores



Fonte: Autoria Própria, 2022.

7.5 GERENCIADORES DE SENHAS

Um gerenciador de senhas mantém guardado todas as senhas que você guardar nele, com exceção de uma: A senha mestra que você deverá definir para acessar as tais senhas guardadas. Você também pode utilizar um gerador de senha, como o Avast Random Password Generator[22] que cria sentenças aleatórias misturando letras, números e caracteres.

[22] Mais informações em: https://www.avast.com/random-password-generator

Há também o LastPass, serviço de gerenciador de senhas, gratuito, mas também há uma versão paga com serviços adicionais, como monitoramento da dark web[23] entre outros serviços, desenvolvido pela LogMeIn. Ele é disponível como um plugin para os navegadores, Internet Explorer, Mozilla Firefox, Google Chrome, Opera e Safari.

Um gerenciador de senhas como o LastPass administra as senhas de usuários e empresas. Quando o usuário conecta suas contas ao serviço de gerenciador de senhas, as senhas passam a ser geradas aleatoriamente e isso torna sua conta mais segura, por utilizar uma senha forte e difícil de ser descoberta ou advinhada.

7.6 VIRUSTOTAL

VirusTotal é um site online gratuito que analisa arquivos, links, endereços IP [24]e arquivos HASH[25], podendo assim, identificar, se o arquivo ou o link em questão, possui conteúdos maliciosos. O "vírus" em questão é escaneado pelo antivírus e assim alerta o usuário do conteúdo malicioso.

O proprietário da VirusTotal é a empresa Chronicle Security que é uma empresa de segurança cibernética que faz parte do Google Cloud Platoform (Plataforma de Nuvem do Google). A Chronicle cria ferramentas para empresas prevenirem de cibercrime em seus serviços.

[23]Dark web: O termo Internet obscura (dark web) ou endereço sombrio refere-se a servidores de rede disponíveis na Internet, acessíveis somente através de ferramentas, configurações ou autorizações específicas.
[24] IP: Sigla para "Internet Protocol", ou "Endereço de Protocolo da Internet".
[25] A função **hash** é um algoritmo matemático para a criptografia, na qual ocorre uma transformação do dado (como um arquivo, senha ou informações) em um conjunto alfanumérico com comprimento fixo de caracteres.

8 CONCLUSÃO

Em resumo, esse projeto ensinou sobre o quão importante é a segurança da informação e porque deve-se investir tempo e dinheiro nela, pois é com a segurança dos dados que evitarmos golpes de roubo de dados, crimes e roubos de dados na internet.

Pode-se dizer que este trabalho irá ajudar em todos os âmbitos que ele for inserido e praticado. Em ambientes corporativos, a segurança ajuda no combate de vazamentos de dados que pode ocorrer por falhas e invasões de hackers, mas com o auxílio da LGPD, a organização irá obter uma maior compreensão das leis que defendem os dados de pessoais físicas, assumindo que a lei seja seguida da devida maneira.

Em suma, para a comunidade acadêmica a pesquisa traz informações sobre os mais recentes vazamentos de dados pelo mundo em 2021, contribuindo também com informações de leis e formas de mitigar casos de vazamento de dados em sites e aplicativos criados para pesquisas acadêmicas.

Ao longo das pesquisas, foi recolhido muitas informações sobre diversos países do Mundo e da América latina. Comparando os países da América latina, nota-se que o Brasil é o país que mais tem vazamento de dados da América latina e é o sexto no ranking mundial de vazamentos de dados, tornando altamente evidente que o Brasil necessita investir na segurança de seus dados no geral.

Para novas abordagens no futuro, os pesquisadores deverão acompanhar todas as tecnologias novas lançadas, pois nelas existem erros e brechas, mas de qualquer modo, via a análise das tecnologias, novas formas de proteger os dados serão lançadas no futuro.

9 REFERÊNCIAS

A GAZETA. **Ministério da Saúde sofre nova invasão de hacker: "Arrumem esse site porco".** 18 fev. 2021. Disponível em: <https://www.agazeta.com.br/brasil/ministerio-da-saude-sofre-nova-invasao-de-hacker-arrumem-esse-site-porco-0221/>. Acesso em: 08 abr. 2022.

Advogados, Giarllarielli. **O que são dados pessoais.** Giarllarielli Advogados, mar. 2022. Disponível em: <https://www.giarllarielli.adv.br/o-que-sao-dados-pessoais/>. Acesso em: 15 mar. 2022.

ALEXANDRE, Luana. **Empresas que já tiveram vazamentos de dados pessoais.** Disponível em:<https://advluanaalexandre.jusbrasil.com.br/artigos/1481020484/empresas-que-ja-tiveram-vazamento-de-dados-pessoais> Acesso em: 02 maio 2022.

ALEXANDRE, Luana. **Empresas que já tiveram vazamentos de dados pessoais. 29 abr. 2022.** Disponível em: <https://advluanaalexandre.jusbrasil.com.br/artigos/1481020484/empresas-que-ja-tiveram-vazamento-de-dados-pessoais>Acessado em: 02 mai. 2022

ARIANE, G. **O que é phishing e como se proteger de golpes na internet.** 23 jul. 2021. Disponível em: <https://www.hostinger.com.br/tutoriais/o-que-e-phishing-e-como-se-proteger-de-golpes-na-internet>. Acesso em: 17 mar. 2022.

ARICETO, Natascha. **7 princípios de privacidade do cliente.** 04 ago. 2020. Disponível em: <https://administradores.com.br/artigos/7-princípios-de-privacidade-do-cliente> Acesso em: 10 mai. 2022.

Arkose Labs. **Fraud & Abuse Report Q2 2020.** 2020. Disponível em: <https://www.arkoselabs.com/wp-content/uploads/Fraud-Report-Q2-2020.pdf> Acesso em: 30 abr. 2022.

BANCO PAN. **O que é phishing: veja como ele pode te prejudicar e como se proteger.** 17 ago. 2021. Disponível em: <https://www.bancopan.com.br/blog/publicacoes/o-que-e-phishing-e-como-se-proteger.htm>. Acesso em: 09 mar. 2022.

Barbosa, Ákio Nogueira. **Um sistema para análise ativa de comportamento de firewall.** 2006. Disponível em: < https://www.teses.usp.br/teses/disponiveis/3/3142/tde-

13122006-145140/publico/UMSISTEMAPARAANALISEATIVADECOMPORTAMENTODEFIREWALL.pdf>. Acesso em: 21 mar. 2022

BARROS, Bruno Luis. **Após ataque hacker ao Banco Pan, polícia cumpre mandados nesta 2° feira.** 19 abr. 2022. Disponível em: <https://www.em.com.br/app/noticia/economia/2022/04/25/internas_economia,1362204/apos-ataque-hacker-ao-banco-pan-policia-cumpre-mandados-nesta-2-feira.shtml> Acessado em: 25 abr. 2022.

BATISTELLA, Carla. **Privacidade nas redes sociais: o que muda com o vigor da LGPD?** 02 mar. 2021. Disponível em: <https://www.certifiquei.com.br/privacidade-redes-sociais/#:~:text=O%20que%20é%20privacidade%20nas,para%20pessoas%20conhecidas%20e%20desconhecidas> Acesso em: 11 mai. 2022.

BELCIC, Ivan. **O guia essencial sobre phishing: Como funciona e como se proteger.** 20 set. 2021. Disponível em: <https://www.avast.com/pt-br/c-phishing>. Acesso em: 10 mar. 2022.

Blog da BitPreço. **O que é Hardwallet: Vale a pena comprar?** S.d. Disponível em: <https://blog.bitpreco.com/o-que-e-uma-hardwallet/#:~:text=Uma%20carteira%20de%20hardware%2C%20tamb%C3%A9m,para%20a%20transfer%C3%AAncia%20de%20fundos.>. Acesso em: 19 mar. 2022.

Borges, Fábio, Alves Fagundes, Bruno e Nunes da Cunha, Gerson. "**Vpn: Protocolos e segurança.**" 2019. Disponível em: < https://www.lncc.br/~borges/doc/VPN%20Protocolos%20e%20Seguranca.pdf>. Acesso em: 27 mar. 2022

Brasil, HSC. **O que é GDPR e o que muda para as empresas e os brasileiros?** HSC Brasil, 1º abr. 2019. Disponível em: <https://www.hscbrasil.com.br/gdpr>. Acesso em: 08 abr. 2022.

Brasil, LGPD. **O que muda com a nova lei de dados pessoais**. LGPD Brasil, mar. 2022. Disponível em: <https://www.lgpdbrasil.com.br/o-que-muda-com-a-lei/>. Acesso em: 19 mar. 2022.

Brasil, SAP. **Sete Princípios Fundamentais da GDPR.** SAP Brasil, 21 mai. 2019. Disponível em: <https://news.sap.com/brazil/2019/05/gdpr-sete-principios-fundamentais-bl0g/>. Acesso em: 06 mai. 2022.

BRAVO, Luís. **A importância da privacidade de dados.** 20 jan. 2021. Disponível em: <https://www.dinheirovivo.pt/opiniao/a-importancia-da-privacidade-de-dados-13253922.html> Acesso em: 30 abr. 2022.

BRITO, R. **Hackers invadem site do Ministério da Saúde e incluem agenda de 'renúncia' de temer.** 27 set. 2016. Disponível em: <https://politica.estadao.com.br/noticias/geral,hackers-invadem-site-do-ministerio-da-saude-e-incluem-agenda-de-renuncia-de-temer,10000078490>. Acesso em: 07 abr. 2022.

Cisco. **O que é firewall?** s.d. Disponível em: <https://www.cisco.com/c/pt_br/products/security/firewalls/what-is-a-firewall.html>. Acesso em: 21 mar. 2022

COMPLIANCE ADVISORY BRAZIL. **O QUE É COMPLIANCE? ENTENDA A SUA IMPORTÂNCIA E COMO IMPLEMENTAR.** 2 de junho de 2020**.** Disponível em: < https://www.techedgegroup.com/pt/blog/o-que-%C3%A9-compliance-entenda-a-sua-import%C3%A2ncia-e-como-implementar>. Acesso em 15 abril 2022

CONHEÇA as 200 senhas fracas mais usadas em 2021. *In*: PACHECO, Victor. **Conheça as 200 senhas fracas mais usadas em 2021**. [*S. l.*], 13 dez. 2021. Disponível em: https://www.showmetech.com.br/senhas-fracas-mais-usadas-em-2021/. Acesso em: 26 abr. 2022.

CORACCINI. **Brasil é o quarto país que mais tem senhas de órgãos públicos vazadas.** 26 abr. 2021. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/brasil-e-o-quarto-pais-do-mundo-que-mais-tem-senhas-vazadas-de-orgaos-publicos/>. Acesso em: 22 abr. 2022.

Correa, Gabriel, Luz, Gabriel, e Ferreira, Lucas. **BYOD E DLP: IMPLEMENTANDO SOLUÇÕES DE SEGURANÇA PARA PREVENÇÃO DE PERDA DE DADOS**. 2020. Disponível em: < http://ric.cps.sp.gov.br/bitstream/123456789/5256/1/19_Edna_20200630.pdf >. Acesso em: 29 de abril 2022.

Cruz, Fio. **Princípios Fundamentais do Marco Civil da Internet**. Fio Cruz, 2022. Disponível em: https://portal.fiocruz.br/documento/principios-fundamentais-do-marco-civil-da-internet>. Acesso em: 26 abr. 2022.

Delelopers Facebook. **Tokens de acesso**. S.d. Disponível em:<https://developers.facebook.com/docs/facebook-login/access-tokens/?locale=pt_BR>. Acesso em:28 mar. 2022

DEMARTINI, F. **Sistemas do Ministério da Saúde são desfigurados por hackers.** 06 nov. 2020. Disponível em: <https://canaltech.com.br/seguranca/sistemas-do-ministerio-da-saude-sao-desfigurados-por-hackers-174177/>. Acesso em: 08 abr. 2022.

DEMARTINI, Felipe, e CLAUDIO, Yuge. **Anonymous vaza banco de dados de ministério de comunicações da Rússia**. 11 mar. 2022. Disponível em: <https://canaltech.com.br/seguranca/anonymous-vaza-banco-de-dados-de-ministerio-de-comunicacoes-da-russia-211300/> Acesso em: 25 mar. 2022

DEMARTINI, Felipe, e CLAUDIO, Yuge. **Anonymous vaza banco de dados de ministério de comunicações da Rússia**. 11 mar. 2022. Disponível em: <https://canaltech.com.br/seguranca/anonymous-vaza-banco-de-dados-de-ministerio-de-comunicacoes-da-russia-211300/> Acesso em: 25 mar. 2022.

DEMARTINI, Felipe. **Universidade de São Paulo tinha falha que expôs dados de alunos e funcionários**. Canaltech: Claudio Yuge, 17 ago. 2021. Disponível em: https://canaltech.com.br/seguranca/usp-tinha-falha-que-expos-dados-de-alunos-e-funcionarios-193007/. Acesso em: 27 abr. 2022.

DIAS, José. **AS SANÇÕES ADMINISTRATIVAS DA LGPD, RESPONSABILIDADE E RESSARCIMENTO DE DANOS: UMA ÓTICA A PARTIR DA VIOLAÇÃO AOS DADOS PESSOAIS PELO COMPARTILHAMENTO IRREGULAR E FALTA DE SEGURANÇA DA INFORMAÇÃO.** 2021. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/1648/1/JOSÉ%20LUCAS%20DA%20COSTA%20DIAS.pdf>. Acesso em: 01 maio 2022.

EDSON, Kaique**. Vazamento expõe dados de 300 mil usuários do Mercado Livre.** 09 mar. 2022. Disponível em: <https://olhardigital.com.br/2022/03/07/seguranca/vazamento-expoe-dados-de-300-mil-usuarios-do-mercado-livre/> Acesso em: 08 mar. 2022.

EDSON, Kaique**. Vazamento expõe dados de 300 mil usuários do Mercado Livre.** 09 mar. 2022. Disponível em: <https://olhardigital.com.br/2022/03/07/seguranca/vazamento-expoe-dados-de-300-mil-usuarios-do-mercado-livre/> Acesso em: 08 mar. 2022.

Ehab S. Al-Shaer , e Hazem H. Hamed. **FIREWALL POLICY ADVISOR FOR ANOMALY DISCOVERY AND RULE EDITING**. 2003. Disponível em: < https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.71.9582&rep=rep1&type=pdf>. Acesso em: 21 mar. 2022. Tradução própria.

EMPEY, Charlotte. **How to create a strong password.** 15 ago. 2018. Disponível em: <https://blog.avast.com/strong-password-ideas>. Acesso em: 08 mar. 2022.

FANTINATO, Giovanna**. Grande vazamento do Facebook: saiba se você foi afetado.** 05 abr. 2021. Disponível em: <https://www.tecmundo.com.br/seguranca/214964-saiba-conta-parte-vazamento-dados-do-facebook.htm> Acesso em:18 abr. 2022.

FANTINATO, Giovanna**. Grande vazamento do Facebook: saiba se você foi afetado.** 05 abr. 2021. Disponível em: <https://www.tecmundo.com.br/seguranca/214964-saiba-conta-parte-vazamento-dados-do-facebook.htm> Acesso em:18 abr. 2022.

Federal, Ministério Público. **O que é a LGPD?.** Ministério Público Federal, mar. 2022. Disponível em: <http://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd/>. Acesso em: 16 mar. 2022.

Federal, Tribunal Regional-PR. **O que são dados pessoais?.** mar. 2022. Disponível em: <https://www.tre-pr.jus.br/transparencia-e-prestacao-de-contas/lei-geral-de-protecao-de-dados/o-que-sao-dados-pessoais/ >. Acesso em: 14 mar. 2022.

Ferreira, Tamires. **LGPD qual a diferença entre dados pessoais, sensíveis e anonimizados?** Olhar Digital, 17 ago. 2021. Disponível em: <https://olhardigital.com.br/2021/08/17/tira-duvidas/lgpd-qual-a-diferenca-entre-dados-pessoais-sensiveis-e-anonimizados/>. Acesso em: 16 mar. 2022.

FSB Comunicação. **Compliance**. 24 de outubro de 2020. Disponível em:<https://www.fsb.com.br/noticias/compliance/>. Acesso em 15 abril 2022

G1. **As senhas mais comuns em vazamentos de dados no Brasil em 2021**. 18 nov. 2021. Disponível em: <https://g1.globo.com/tecnologia/noticia/2021/11/18/as-senhas-

mais-comuns-em-vazamentos-de-dados-no-brasil-em-2021.ghtml>. Acesso em: 22 abr. 2022.

G1. **Entenda o caso de Edward Snowden, que revelou espionagem dos EUA**. G1**,** 14 fev. 2014. Disponível em: <https://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html/>. Acesso em: 2 abr. 2022.

G1. **PF prende hackers suspeitos de participação no vazamento de dados de 223 milhões de brasileiros.** 19 mar. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/03/19/policia-federal-deflagra-operacao-contra-divulgacao-e-comercializacao-de-dados-pessoais-de-brasileiros.ghtml Acesso em: 16 abr. 2022.
G1. **PF prende hackers suspeitos de participação no vazamento de dados de 223 milhões de brasileiros.** 19 mar. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/03/19/policia-federal-deflagra-operacao-contra-divulgacao-e-comercializacao-de-dados-pessoais-de-brasileiros.ghtml Acesso em: 16 abr. 2022.
G1. **Pix: BC relata vazamento de dados cadastrais de 159,6 mil clientes de Acesso Soluções de Pagamento**. 21 jan. 2022. Disponível em: < https://g1.globo.com/economia/pix/noticia/2022/01/21/pix-bc-relata-vazamento-de-dados-cadastrais-de-clientes-da-acesso-solucoes-de-pagamento.ghtml> Acesso em: 18 abr. 2022
G1. **Pix: BC relata vazamento de dados cadastrais de 159,6 mil clientes de Acesso Soluções de Pagamento**. 21 jan. 2022. Disponível em: < https://g1.globo.com/economia/pix/noticia/2022/01/21/pix-bc-relata-vazamento-de-dados-cadastrais-de-clientes-da-acesso-solucoes-de-pagamento.ghtml> Acesso em: 18 abr. 2022
GATEFY. **Como funcionam as leis de proteção de dados nos Estados Unidos.** 23 mar. 2021. Disponível em: <https://gatefy.com/pt-br/blog/como-funcionam-leis-protecao-dados-estados-unidos/>. Acesso em: 08 abr. 2022.

Geral, Secretaria. **Regulamento Geral de proteção de dados.** Secretaria Geral, 2018. Disponível em: <https://www.sg.pcm.gov.pt/sobre-nos/regulamento-geral-de-prote%C3%A7%C3%A3o-

dedados.aspx#:~:text=O%20Regulamento%20(UE)%202016%2F,relativos%20a%20pessoas%20na%20UE>. Acesso em: 06 abr. 2022.

GONZÁLEZ, Mariana. **Conheça o cenário das leis de proteção de dados ao redor do mundo.** 14 fev. 2020. Disponível em: <https://blog.idwall.co/protecao-de-dados-cenario-mundial-das-leis/>. Acesso em: 08 abr. 2022.

GOOGLE. **Ativar a verificação em duas etapas.** S.d. Disponível em: <https://support.google.com/accounts/answer/185839?hl=pt-BR>. Acesso em: 10 mar. 2022.

GTA/UFRJ. **Arquitetura de VPN**. S.d. Disponível em:<https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2015_2/Seguranca/conteudo/Redes-Privadas-Virtuais-VPN/Arquitetura-VPN.html>. Acesso em: 27 mar. 2022

HIGA, P. **Polícia Federal prende suspeito de vazar dados de 223 milhões de brasileiros**. **Tecnoblog**, ano 2021, 19 mar. 2021. Disponível em: <https://tecnoblog.net/422817/policia-federal-prende-suspeito-de-vazar-dados-de-223-milhoes-de-brasileiros/>. Acesso em: 14 abr. de 2022.

HIGA, P. **Polícia Federal prende suspeito de vazar dados de 223 milhões de brasileiros**. **Tecnoblog**., 19 mar. 2021. Disponível em: <https://tecnoblog.net/422817/policia-federal-prende-suspeito-de-vazar-dados-de-223-milhoes-de-brasileiros/>. Acesso em: 14 abr. de 2021.

HIGA, Paulo. **Descubra se alguma senha sua já vazou na internet**. Tecnoblog, 12 jan. 2017. Disponível em: https://tecnoblog.net/responde/senha-vazada-internet/. Acesso em: 27 abr. 2022.

HORNE, Lorax e BEST, Emma. **Release: Roskomnadzor (820 GB).** 10 mar 2022. Disponível em: <https://ddosecrets.substack.com/p/release-roskomnadzor-820-gb?s=r> Acesso em: 25 mar. 2022.

IBLISS. **Ataques cibernéticos aumentam em meio à pandemia da COVID-19.** 14 abr. 2021. Disponível em: <https://www.ibliss.com.br/ataques-ciberneticos-aumentam-em-meio-a-pandemia-da-covid-19/>. Acesso em: 08 abr. 2022.

IBM.**O que é a tecnologia blockchain**. s.d. Disponível em: <https://www.ibm.com/br-pt/topics/what-is-blockchain >. Acesso em: 20 mar. 2022

INFOMONEY. **Segurança digital: a prevenção é mais barata que a cobertura dos danos para as empresas.** 13 jul. 2021. Disponível em: <https://www.infomoney.com.br/patrocinados/empresas-e-tecnologia/seguranca-digital-a-prevencao-e-mais-barata-que-a-cobertura-dos-danos-para-as-empresas/>. Acesso em: 26 abr. 2022.

ISTOÉ. **Segurança de dados: Brasil é o 6º país com mais vazamentos, diz pesquisa.** 17 mar. 2022. Disponível em: <https://www.istoedinheiro.com.br/seguranca-de-dados-brasil-e-o-6o-pais-com-mais-vazamentos-diz-pesquisa/>. Acesso em: 26 abr. 2022.

ISTOÉ. **Vazamento expõe dados de 16 milhões de pacientes de Covid-19.** 26 nov. 2020. Disponível em: <https://www.istoedinheiro.com.br/vazamento-expoe-dados-de-16-milhoes-de-pacientes-de-covid-19/>. Acesso em: 07 abr. 2022.

KASPERSKY. **O que é um ataque de força bruta?.** S.d. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/brute-force-attack>. Acesso em: 08 mar. 2022.

KISSELL, J. Aprendendo a proteger suas senhas. Tradução: BrodTec. 1. ed. São Paulo: Novatec, 2017. 176 p.

Kogan, Jeffrey. **Blockchain Technology: An Analysis of Potential Applications and Uses**.12 de Dez. 2017. Disponível em: <https://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1164&context=honorscollege_theses>. Acesso em 29 abril 2022.

KREBS, Brian. **As Scope of 2012 Breach Expands, LinkedIn to Again Reset Passwords for Some Users**. Krebsonsecuity, 18 maio 2016. Disponível em: https://krebsonsecurity.com/2016/05/as-scope-of-2012-breach-expands-linkedin-to-again-reset-passwords-for-some-users/. Acesso em: 27 abr. 2022.

LEITE, Victor. **O que é criptomoeda? Entenda de uma vez**.23 abril 2020. Disponível em:<https://blog.nubank.com.br/o-que-e-criptomoeda/>. Acesso em: 20 mar. 2022

LOPES, Henrique. **Internet segura: falta muito para o Brasil chegar lá?.** 03 mar. 2020. Disponível em: <https://canaltech.com.br/seguranca/internet-segura-falta-muito-para-o-brasil-chegar-la-161258/>. Acesso em: 26 abr. 2022.

Macedo, Luís. **Câmara aprova projeto que disciplina tratamento de dados pessoais.** Câmara, 29 mai. 2018. Disponível em: <https://www.camara.leg.br/noticias/539266-camara-aprova-projeto-que-disciplina-tratamento-de-dados-pessoais/>. Acesso em: 03 abr. 2022.

Mendes, Assis e. **5 áreas que devem ser impactadas pela LGPD**. Assis e Mendes, 2020. Disponível em: https://assisemendes.com.br/lgpd-areas-impactadas/>. Acesso em: 14 abr. 2022.

MENDONÇA, Jâmison, BOCARD, Lucas, DIAS, Luciano, DOS REIS, Maxwel. **WI-FI PÚBLICO RISCOS E SOLUÇÕES.** S.d. Disponível em: <http://www.periodicos.letras.ufmg.br/index.php/anais_linguagem_tecnologia/article/viewFile/12198/10395> Acesso em: 21 mar. 2022.

MILLANEZ, Eduardo. **5 DICAS PARA RECONHECER E-MAILS MALICIOSOS.** 16 abr. 2016. Disponível em: <https://www.tradesys.com.br/2019/04/16/5-dicas-para-reconhecer-e-mails-maliciosos/>. Acesso em: 17 mar. 2022.

MITNICK, K. D.; SIMON, W. L. A arte de enganar. São Paulo: Pearson, 2003. 286 p.

MULLER, F. **Como o vazamento de dados acontece.** 17 fev. 2021. Disponível em: <https://www.nsctotal.com.br/noticias/como-o-vazamento-de-dados-acontece/>. Acesso em: 08 abr. 2022.

Nacional, Congresso. **PLC 53/2018**. Congresso nacional, 2018. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7738705&ts=1630450891439&disposition=inline>. Acesso em: 14 abr. 2022.

Nones, Fernanda. **LGPD: o que diz a lei brasileira de proteção de dados e como ela pode impactar a estratégia de marketing de sua empresa.** Resultados Digitais, 1º ago. 2021. Disponível em: < https://resultadosdigitais.com.br/marketing/o-que-e-lgpd/>. Acesso em: 17 mar. 2022.

Oitchau, Blog. **GDPR: Como se aplica ao Brasil? Saiba mais!.** Oitchau, 06 jan. 2022. Disponível em: <https://www.oitchau.com.br/blog/gdpr-como-se-aplica-ao-brasil/>. Acesso em: 06 mai. 2022.

On-line, Valor. **Cyrela é multada em R$ 10 mil por infração à Lei Geral de Proteção de Dados.** G1, 30 set. 2020. Disponível em: <https://g1.globo.com/economia/noticia/2020/09/30/cyrela-e-multada-em-r-10-mil-por-infracao-a-lei-geral-de-protecao-de-dados.ghtml>. Acesso em: 27 mar. 2022.

Planalto. **Lei 12965/2014**. Brasil, 23 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm/>. Acesso em: 03 abr. 2022.

Planalto. **Lei 13.709/2018.** Brasil, 14 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm/>. Acesso em: 27 mar. 2022.

PONTES, F. **STJ é alvo de um ataque de hacker e Polícia Federal investiga o sistema.** 04 nov. 2020. Disponível em: <https://agenciabrasil.ebc.com.br/justica/noticia/2020-11/stj-e-alvo-de-ataque-de-hacker-e-policia-federal-investiga-o-sistema/>. Acesso em: 08 abr. 2022.

Portal de corregedorias. **Lei Anticorrupção.** S.d. Disponível em:<https://corregedorias.gov.br/assuntos/PAR/lei-anticorrupcao>. Acesso em 15 abril 2022

Privacy, Secure. **Tudo o que você precisa saber sobre multas da lei GDPR**. Secure Privacy, 29 set. 2021. Disponível em: <https://secureprivacy.ai/pt/blog/o-que-voce-precisa-saber-sobre-multas-da-lei-gdpr>. Aceso em: 08 abr. 2022.

Privicy, Get. **20 exemplos práticos e reais de aplicação da LGPD.** Get Privicy, mar. 2022. Disponível em: <https://getprivacy.com.br/exemplos-praticos-e-reais-de-aplicacao-da-lgpd/>. Acesso em: 26 mar. 2022.

R7. **Operação combate vazamento ilegal de dados pela internet**. 19 mar. 2021. Disponível em: https://noticias.r7.com/brasil/pf-operacao-combate-vazamento-ilegal-de-dados-pela-internet-19032021?amp#aoh=16503018322914&referrer=https%3A%2F%2Fwww.google.com&amp_tf=Fonte%3A%20%251%24s Acesso em: 16 abr. 2022

R7. **Operação combate vazamento ilegal de dados pela internet**. 19 mar. 2021. Disponível em: https://noticias.r7.com/brasil/pf-operacao-combate-vazamento-ilegal-de-dados-pela-internet-

19032021?amp#aoh=16503018322914&referrer=https%3A%2F%2Fwww.google.com&amp_tf=Fonte%3A%20%251%24s Acesso em: 16 abr. 2022

REBITTE, Leonardo. **Brasil é um dosum dos países com mais fraudes por ataques virtuais no mundo.** 13 abr. 2022. Disponível em: <https://www.combateafraude.com/post/brasil-fraudes-ataques-virtuais#:~:text=Ao%20lado%20dos%20Estados%20Unidos,ataques%20cibernéticos%20ano%20a%20ano> Acesso em: 30 abr. 2022.

REIS, Rogério. **Por que a segurança da informação no Brasil é frágil?.** 07 ago. 2013. Disponível em: <https://webinsider.com.br/seguranca-da-ti-no-brasil-muito-falatorio-pouca-evolucao/>. Acesso em: 26 abr. 2022.

RIBEIRO, Carolina. **Brasil é principal alvo de spywares que roubam dados bancários**. TechTudo, 22 out. 2019. Disponível em: https://www.techtudo.com.br/noticias/2019/10/brasil-e-principal-alvo-de-spywares-que-roubam-dados-bancarios.ghtml. Acesso em: 28 abr. 2022.

RODRIGUES, Carlos. **O guia essencial sobre phishing: Como funciona e como se proteger.** 24 jan. 2020. Disponível em: <https://cryptoid.com.br/banco-de-noticias/autenticacao-de-dois-fatores-esta-entre-as-medidas-de-ciberseguranca-que-voce-deve-aplicar-em-2020/>. Acesso em: 13 mar. 2022.

SANTOS, Rahellen. **O que é o Marco Civil da Internet?** Politize, 06 ago. 2021. Disponível em: <https://www.politize.com.br/marco-civil-da-internet/>. Acesso em: 04 abr. 2022.

SANTOS, Renato. **';--‘; --você foi pwned?.** 27 abr. 2020. Disponível em: <https://renatogsantos.jusbrasil.com.br/artigos/835870313/voce-foi-pwned> Acesso em: 21 mar. 2022.

Saturo, Ares. **Senado vota PLC 53/2018, lei que regulamenta o uso de dados pessoais no Brasil.** Canaltech, 03 jul. 2018. Disponível em: <https://canaltech.com.br/governo/senado-vota-plc-532018-lei-que-regulamenta-o-uso-de-dados-pessoais-no-brasil-117178/>. Acesso em: 14 abr. 2022.

Sávio Vale. **Definição, funcionamento e as aplicações do hash, a função popular da criptografia.** Disponível em: <https://www.voitto.com.br/blog/artigo/o-que-e-hash-e-como-funciona>. Acesso em 03 abril 2022

Scognamiglio, Heloísa**. Entenda o que é compliance e como as empresas podem se beneficiar dos investimentos nessa área**.14 de abril de 2022.Disponível em:<https://economia.estadao.com.br/noticias/governanca,o-que-e-compliance-beneficios-investimentos,70004038286>. Acesso em 15 abril 2022

SECURITY REPORT. **19% dos países do mundo ainda não possuem nenhuma legislação sobre privacidade de dados.** 04 abr. 2021. Disponível em: <https://www.securityreport.com.br/overview/19-dos-paises-do-mundo-ainda-nao-possuem-nenhuma-legislacao-sobre-privacidade-de-dados/>. Acesso em: 08 abr. 2022.

SEGUIN, Patrick. **Spyware: Detecção, prevenção e remoção**. Avast Academy, 13 set. 2021. Disponível em: https://www.avast.com/pt-br/c-spyware. Acesso em: 28 abr. 2022.

Senado. **Projeto de Lei da Câmara n° 53, de 2018**. Congresso Nacional, 31 ago. 2021. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/133486>. Acesso em: 14 abr. 2022.

SENHAS fracas ainda são obstáculos essenciais à segurança corporativa. [*S. l.*], 16 jun. 2021. Disponível em: https://www.maisdados.com.br/senhas-fracas-ainda-sao-obstaculos-essenciais-a-seguranca-corporativa/. Acesso em: 26 abr. 2022.

SIMPLICIO, Marcos. **Segurança da informação – Aula 01 – Introdução.** 21 jun. 2018. Disponível em: <https://www.youtube.com/watch?v=JrVS7YsGw8w&feature=youtu.be&ab_channel=UNIVESP> Acesso em: 06 mai. 2022.

SoftWall. **8 casos de vazamentos de dados tratados com a LGPD.** SoftWall, 23 ago. 2021. Disponível em: <https://www.softwall.com.br/blog/vazamentos-de-dados-tratados-com-a-lgpd/>. Acesso em: 29 mar. 2022.

Souto Maior, Alexandra. **O consentimento na proteção de dados pessoais: análise do PL4060/2012 e sua conjuntura legislativa.** Arca, 2018. Disponível em: <https://www.arca.fiocruz.br/handle/icict/40407>. Acesso em: 03 abr. 2022.

SQL Injection Tutorial: O que é SQL Injection? Como Evitar? Veja!. Dev Media, 12 jul. 2007. Disponível em: https://www.devmedia.com.br/sql-injection/6102. Acesso em: 18 mar. 2022.

TAGIAROLI, Guilherme. **Usar rede Wi-Fi aberta oferece riscos aos usuários; veja como se proteger.** 29 jan. 2015. Disponível em:

<https://www.uol.com.br/tilt/noticias/redacao/2015/01/29/usar-wi-fi-aberto-oferece-riscos-aos-usuarios-veja-como-se-proteger.htm>. Acesso em: 21 mar. 2022.

Tools, Privacy. **10 casos famosos de multas com a GDPR.** Privacy Tools, 2022. Disponível em: <https://privacytools.com.br/10-casos-famosos-de-multas-com-a-gdpr/#.>. Acesso em: 08 abr. 2022.

TRUST CONTROL, Marketing (ed.). **O ataque via Trojan bancário: 03 soluções que aumentam a segurança contra esse malware**. Trust Control, 24 nov. 2021. Disponível em: https://www.trustcontrol.com.br/blog/o-ataque-via-trojan-bancario-03-solucoes-que-aumentam-a-seguranca-contra-esse-malware/. Acesso em: 28 abr. 2022.

Valtrick, Bruna. **Banco Pan confirma vazamento de dados de milhares de clientes.** 18 abr. 2022. Disponível em: <https://seucreditodigital.com.br/banco-pan-vazamento-de-dados/> Acessado em: 25 abr. 2022

VARGAS, M. **Ministério da Saúde sofre invasão e hacker debocha: 'Este site está um lixo!'**. 03 fev. 2021. Disponível em: <https://brasil.estadao.com.br/noticias/geral,ministerio-da-saude-sofre-invasao-e-hacker-debocha-este-site-esta-um-lixo,70003603976/>. Acesso em: 08 abr. 2022.

VELLA, Fernando. **Keylogger: uma ferramenta usada para espionar**. Welivesecurity, 5 mar. 2021. Disponível em: https://www.welivesecurity.com/br/2021/03/05/keylogger-uma-ferramenta-usada-para-espionar/. Acesso em: 27 abr. 2022.

VENTURA, Felipe. **Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava.** 22 jan. 2021. Disponível em: <https://tecnoblog.net/noticias/2021/01/22/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/>. Acesso em: 05 abr. 2022.

VENTURA, Felipe. **Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava.** 22 jan. 2021. Disponível em: <https://tecnoblog.net/noticias/2021/01/22/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/>. Acesso em: 05 abr. 2022.

VirusTotal. **VirusTotal**. Disponível em: <https://www.virustotal.com/gui/home/upload>. Acesso em 03 abril 2022

Wang, D., Zhang, L., Yuan, Z., Xue, Y., e Dong, Y. **Characterizing application behaviors for classifying p2p traffic**.2014. In International Conference on Computing, Networking and Communications, ICNC'14, pages 21–25. IEEE. Acesso em: 29/04/2022

YASIR, S, KUMAR, H. **Indian Call-Center Plot Fooled Americans Into Paying Over $14 Million.** 17 dez. 2020. Disponível em: <https://www.nytimes.com/2020/12/17/world/asia/india-call-center-scam.html>. Acesso em: 08 abr. 2022.

10 ANEXO A - CÓDIGO BACKEND[26] QUE REALIZA LOGIN DE USUÁRIO

```
<HTML>
<BODY bgcolor='000000' text='ffffff'>
<FONT Face='tahoma' color='ffffff'>
<STYLE>
p { font-size=20pt ! important}
font { font-size=20pt ! important}
h1 { font-size=64pt ! important}
</STYLE>
<%@LANGUAGE = JScript %>
<%
function trace( str )
{
if( Request.form("debug") == "true" )
Response.write( str );
}
function Login( cn )
{
var username;
var password;
username = Request.form("username");
password = Request.form("password");
var rso = Server.CreateObject("ADODB.Recordset");
var sql = "select * from users where username = '" +
username + "' and password = '" + password + "'";
trace( "query: " + sql );
rso.open( sql, cn );
if (rso.EOF)
{
rso.close();
%>
<FONT Face='tahoma' color='cc0000'>
<H1>
<BR><BR>
<CENTER>ACCESS DENIED</CENTER>
</H1>
</BODY>
</HTML>
<%
Response.end
return;
}
else
{
Session("username") = "" + rso("username");
%>
<FONT Face='tahoma' color='00cc00'>
<H1>
<CENTER>ACCESS GRANTED<BR>
<BR>
Welcome,
<% Response.write(rso("Username"));
Response.write( "</BODY></HTML>" );
Response.end
}
}
function Main()
{
//Set up connection
var username
var cn = Server.createobject( "ADODB.Connection" );
cn.connectiontimeout = 20;
cn.open( "localserver", "sa", "password" );
username = new String( Request.form("username") );
if( username.length > 0)
{
Login( cn );
}
cn.close();
}
Main();
%>
```

Fonte: Adaptado de DevMedia, 2007.

[26] Backend: A “parte de trás” de toda e qualquer aplicação ou site, é a estrutura mantida pelo computador que possibilita que o sistema funcione corretamente.