CRIMES CIBERNÉTICOS: Roubo e proteção de dados

Adriany Raiumy Tanaka Custodio[1] – ETEC Professora Nair Luccas Ribeiro

Ana Laura dos Santos[2] – ETEC Professora Nair Luccas Ribeiro

Edimary de Oliveira Rabaiolli[3] – ETEC Professora Nair Luccas Ribeiro

Yara Rodrigues Branquinho[4] – ETEC Professora Nair Luccas Ribeiro - Orientadora

RESUMO

Este artigo tem como objetivo atestar os impactos iminentes que os crimes cibernéticos vêm causando na sociedade atual. O roubo de dados é a obtenção não autorizada de informações, como dados pessoais, financeiros ou corporativos, que pode acontecer através de diversos métodos, incluindo "*phishing, malware"*, engenharia social e vulnerabilidades em sistemas de segurança. O roubo e a proteção de dados são questões proeminentes na era digital, afetando pessoas, organizações e governos. Enquanto roubo de dados envolve a aquisição não autorizada de informações confidenciais que, na maioria dos casos, resulta em perdas financeiras e violações de privacidade, a proteção de dados envolve medidas para prevenir o acesso não autorizado e reduzir os impactos de possíveis violações. Os métodos comuns de roubo incluem ataques cibernéticos. Portanto, a proteção de dados torna-se vital, incluindo práticas políticas de segurança ainda mais rigorosas. Além disso, legislações como a LGPD (Lei Geral de Proteção de Dados Pessoais) impõem obrigações rígidas quanto à coleta, armazenamento e tratamento de dados, visando reduzir riscos e proteger os direitos dos usuários. A segurança dos dados continua a ser um desafio constante que exige inovação e consciência das práticas de segurança

Palavras-chave: Roubo. Proteção. Digital. Segurança.

ABSTRACT

This article aims to attest to the imminent impacts that cybercrimes are causing in today's society. Data theft is the unauthorized obtaining of information, such as personal, financial or corporate data, which can occur through various methods, including phishing, malware, social engineering and vulnerabilities in security systems. Data theft and protection are prominent issues in the digital age, affecting people, organizations and governments. While data theft involves the unauthorized acquisition of confidential information that, in most cases, results in financial losses and privacy violations, data protection involves measures to prevent unauthorized access and reduce the impacts of potential breaches. Common theft methods include cyber attacks. Therefore, data protection becomes vital, including even stricter security policy practices. Furthermore, legislation such as the LGPD (General Personal Data Protection Law) imposes strict obligations regarding the collection, storage and processing of data, aiming to reduce risks and protect users' rights. Data security continues to be a constant challenge that requires innovation and awareness of security practices

Keywords: *Robbery. Protection. Digital. Security.*

[1] - Técnico em Serviços Jurídicos – *e-mail*: adriany.custodio@etec.sp.gov.br

[2] - Técnico em Serviços Jurídicos – *e-mail*: ana.santos2283@etec.sp.gov.br

[3] - Técnico em Serviços Jurídicos – *e-mail*: edimary.rabaiolli@etec.sp.gov.br

[4] - Espec. em Direito Público e Licenciada em Direito e Pedagogia – *e-mail*: yara.branquinho01@etec.sp.gov.br

1 INTRODUÇÃO

O presente artigo tem como estudo o roubo e proteção de dados, que envolve a transferência ou acesso ilegal de informações pessoais, confidenciais ou financeiras, que podem incluir desde senhas e códigos de programas até informações mais sensíveis, como CNH, números de RG, CPF, documentos médicos e contas bancárias.

Este trabalho se propõe a investigar e analisar através de pesquisa aplicada qualitativa, dados coletados por meio de pesquisa bibliográfica o conceito de roubo de dados pessoais e empresariais, suas causas, consequências e possíveis medidas de prevenção e apresentado por meio de estudo de campo os maiores roubos da história que influenciaram na evolução da legislação e desenvolvimento de medidas de segurança. Serão apresentadas por meio de várias abordagens técnicas as implicações éticas, legais e tecnológicas relacionadas ao roubo de dados, fornecendo uma visão abrangente sobre um tema de extrema relevância na sociedade contemporânea.

Contudo, temos como objetivo analisar os crimes cibernéticos relacionados ao roubo e proteção de dados, compreender as principais modalidades desses crimes, suas consequências e as medidas de segurança que podem ser adotadas. Pretende-se fornecer uma visão abrangente das práticas criminosas, das legislações vigentes e das melhores práticas de proteção de dados no ambiente digital.

A relevância deste estudo se justifica pela crescente incidência de crimes cibernéticos e pelo impacto significativo que eles causam em diversos setores da sociedade. O roubo de dados pode resultar em perdas financeiras substanciais, danos à reputação e violações de privacidade. Além disso, com a promulgação de leis como a Lei Geral de Proteção de Dados (LGPD) no Brasil, torna-se essencial entender as obrigações legais e as estratégias de proteção de dados para garantir conformidade e segurança.

Diante do atual crescente número de incidentes de segurança cibernética e da sofisticação das técnicas utilizadas pelos cibercriminosos, é importante analisar as estratégias mais eficazes para proteger dados sensíveis e pessoais e garantir a privacidade dos usuários em um mundo que está cada vez mais digital e interconectado.

2 DEFINIÇÃO DE ROUBO DE DADOS

O roubo de dados, também chamado de roubo de informações, corresponde à transferência ou retenção ilegal de dados pessoais, confidenciais ou financeiros, o que pode envolver senhas, códigos de programas ou algoritmos, assim como procedimentos ou tecnologias exclusivas. A ação de roubar dados é vista como uma violação séria da segurança e da privacidade, podendo acarretar consequências graves para pessoas e empresas.

Esta definição refere-se ao roubo de ativos digitais armazenados em computadores, servidores ou dispositivos eletrônicos para obter ou divulgar informações confidenciais que foram roubadas podendo ser contas bancárias, senhas online, números de passaporte, números de carteira de motorista, números de seguro social, registros médicos, assinaturas online, entre outras.

O termo “roubo de dados” não significa literalmente roubar ou excluir informações, mas também pode ser configurado quando, invasores copiam ou duplicam as informações para uso próprio.

Essa definição se diferencia de vazamento de dados que ocorre quando dados sensíveis são acidentalmente expostos na Internet ou através de discos rígidos ou dispositivos perdidos, que facilita o acesso não autorizado às informações por criminosos. E a violação de dados é diferenciada em razão de se referir a ataques cibernéticos intencionais.

Na perspectiva de Nucci:

> “A nova figura típica de invasão de dispositivos informáticos, insere-se no contexto de crimes contra a liberdade individual, sendo este o bem jurídico mediato tutelado. No entanto, de forma imediata, ingressou-se no campo dos crimes contra a inviolabilidade dos segredos, com proteção acerca da intimidade, da vida privada, da honra, da inviolabilidade de comunicação e correspondência, enfim, da livre manifestação do pensamento, sem nenhuma intromissão de um terceiro.” (NUCCI, Guilherme de Souza, 2014, p. 811).

2.1 Dados passíveis de roubo

Qualquer informação armazenada por um indivíduo ou organização pode ser um alvo potencial para os ladrões de dados, como por exemplo Registros de clientes, Dados financeiros (como informações de cartão de crédito ou de débito), os Códigos fonte e algoritmos, as Descrições de processos e metodologias operacionais próprias, as Credenciais de rede, tais como nomes de usuário e senhas, os Registros de RH e dados de empregados e Documentos particulares armazenados em computadores.

Infelizmente, muitas empresas do mundo todo estão perdendo sua segurança sobre seus próprios dados, há mais tempo do que podemos imaginar, tanto por falhas no gerenciamento, quanto por fraudes.

3 ESTRATÉGIAS E FALHAS UTILIZADAS PARA PRÁTICA DE ROUBO DE DADOS

Com a evolução e a chegada da era cibernética tem-se percebido falhas no gerenciamento e fraudes que tem colocado em risco, a segurança dos dados de muitas empresas.

Atualmente as maiores falhas acontecem pelo acesso a computadores, redes ou dispositivos, onde para obter informações, criminosos realizam ataques cibernéticos e furto de dispositivos físicos e de acordo com os dados levantados as mais comuns incluem as seguintes:

3.1 Engenharia social

"*Phishing*" a palavra é derivada da palavra inglesa "*fishing*", que significa pescar. Este termo ilustra bem o conceito deste tipo de ameaça digital: tentativas de "phishing" nos dados pessoais da vítima através de contas de e-mail, redes sociais etc. É o que ocorre quando um invasor usa uma entidade de confiança para defraudar a vítima, fazendo com que abra mensagens de texto, mensagens instantâneas ou e-mails.

3.2 Ameaças internas

Normalmente os funcionários que trabalham para uma organização têm acesso às informações pessoais de seus clientes. Em razão disso, funcionários ou contratados que estejam mal-intencionados podem copiar, modificar ou roubar conteúdo. Importa ressaltar que essa situação pode ser praticada também por antigos funcionários, empreiteiros ou parceiros que tenham acesso aos sistemas de uma organização ou a informações sensíveis.

3.3 Erro humano

As violações de dados nem sempre são frutos de ações maliciosas, por vezes podem estar associadas a algum erro humano. Estes erros são comuns e incluem o envio de informação sensível à pessoa errada, como o envio de um e-mail por engano para o endereço errado, anexar o documento errado ou entregar um arquivo físico a alguém que não deveria ter acesso à informação.

Portanto, o erro humano pode não ser intencional, como por exemplo quando um funcionário deixa um banco de dados contendo informações confidenciais online sem proteger o seu acesso por meio de senha, ou quando são usadas em várias contas diferentes, a mesma senha, permitindo, assim com que criminosos tenham acesso a esses dados, ou ainda quando são cadastradas senhas de fácil adivinhação que também cooperam para a ação de pessoas mal-intencionadas.

3.4 Downloads comprometidos

Fazer “download” ou baixar programas ou dados de sites não confiáveis podem facilitar o acesso não autorizado por criminosos aos seus dispositivos, permitindo-lhes roubar dados.

3.5 Ações físicas

Algumas ações físicas como roubo, furto ou ainda perda de documentos e equipamentos como laptops, telefones celulares ou dispositivos de armazenamento também facilitam práticas de golpes e/ou roubo de dados, que tem aumentado muito com a crescente modalidade do trabalho remoto.

Importa ressaltar que existem outras ações físicas que contribuem para prática maliciosa como a clonagem de cartões, na qual os criminosos colocam dispositivos em leitores de cartões e caixas eletrônicos para coletar informações de cartões de pagamento e ainda quando se trabalha em um local público, como um restaurante por exemplo, e alguém visualiza a tela e teclado que estão expostos para se conectar e roubar informações.

4 OS 9 MAIORES ROUBOS DE DADOS DA HISTÓRIA

Segundo o site de notícias CRYPTOID os maiores roubos de informações da história são:

4.1 Nasdaq, 2005–2012: 160 milhões de pessoas afetadas:

Um grupo de hackers composto por cinco russos e um ucraniano foi responsável por roubar números de cartões de crédito e débito de mais de 160 milhões de pessoas, além de acessar 800 mil contas de bancos e invadir servidores usados pela bolsa de valores Nasdaq, que é uma das maiores bolsas de valores do mundo (CRYPTOID, 2015).

4.2 Heartland Payment Systems, 2008–2009: 130 milhões de pessoas afetadas:

Em 2009 houve uma das maiores brechas de segurança do mundo, onde um serviço computacional utilizado para realizar ações nos sistemas de computadores foi implantado no

sistema da Heartland Payment Systems que é uma empresa que gravava informações de cartões de crédito assim que eles chegavam dos varejistas que processava o pagamento de mais de 250 mil empresas nos Estados Unidos, sendo o suficiente para que os dados de 130 milhões de pessoas fossem roubados. Pelo crime, Albert Gonzalez foi condenado a 20 anos de prisão (CRYPTOID, 2015).

4.3 Target Stores, 2013: 110 milhões de pessoas afetadas:

Em dezembro de 2013, a Target, uma das grandes redes varejistas dos Estados Unidos, anunciou que informações de cerca de 40 milhões de clientes haviam sido roubadas, incluindo endereço, telefone, cartão de crédito e e-mail. Logo depois, a empresa revisou o número e afirmou que na verdade foram 110 milhões de clientes afetados com a brecha (CRYPTOID, 2015).

4.4 Sony, 2011: 102 milhões de pessoas afetadas:

Em Abril de 2011, a Sony sofreu o maior ataque de hackers da sua história, o que a obrigou a tirar a PlayStation Network do ar por três semanas, causando a insatisfação de milhões de usuários. Onde houve o comprometimento de informações de mais de 77 milhões de usuários, incluindo login, nomes, endereços, telefones e e-mails. Logo após o ocorrido, a empresa descobriu também que a Sony Online Entertainment (SOE) também havia sido violada, permitindo acesso a dados de mais 25 milhões de usuários. No total, foram 102 milhões de dados de usuários expostos pelos hackers (CRYPTOID, 2015).

4.5 AOL, 2004: 92 milhões de pessoas afetadas:

A quebra de segurança da AOL aconteceu em 2004, por culpa de um ex-funcionário, a AOL ainda era uma das grandes empresas da internet, o engenheiro de software Jason Smathers roubou os e-mails e nomes de usuário de 92 milhões de clientes. Os e-mails foram vendidos, calcula-se que enviaram mais de 7 bilhões de spams. Smathers pegou 1 ano e três meses pelo crime cometido (CRYPTOID, 2015).

4.6 Epsilon, 2011: 60 milhões de pessoas afetadas:

A Epsilon é uma empresa responsável pela comunicação de e-mails de muitas das maiores empresas do mundo. Em 2011, a empresa anunciou que os bancos de dados de cerca de 50 clientes haviam sido roubados. Com isso, os e-mails de ao menos 60 milhões de clientes

acabaram nas mãos de criminosos que usam fraude e induzem ao engano para manipular as vítimas (CRYPTOID, 2015).

4.7 Home Depot, 2014: 56 milhões de pessoas afetadas:

A Home Depot é uma rede de artigos de materiais de construção. Em setembro de 2014, a empresa admitiu que os dados dos cartões de crédito de 56 milhões de pessoas haviam sido violados. Os hackers usaram um programa criado especialmente para evitar os sistemas de detecção. Mas felizmente, os códigos de segurança dos cartões dos clientes não foram comprometidos (CRYPTOID, 2015).

4.8 Livingsocial, 2013: mais de 50 milhões de pessoas infectadas:

A Living Social é a maior concorrente do Groupon, site de descontos. Em abril de 2013, hackearam dados de 50 milhões de usuários, incluindo nomes, senhas e data de nascimento, mas não dados de cartões de crédito (CRYPTOID, 2015).

4.9 Evernote, 2013: 50 milhões de pessoas afetadas:

Endereços de e-mail e senhas criptografadas de usuários do Evernote foram expostas em fevereiro de 2013. Nenhum dado financeiro foi violado, e nem mesmo conteúdo que foram gerados por usuários, segundo a empresa. Por precaução, a Evernote restaurou a senha de 50 milhões de usuários (CRYPTOID, 2015).

5 FORMAS DE PROTEÇÃO E PREVENÇÃO

Existem diversas medidas que podem ser tomadas para evitar que os criminosos roubem dados, das quais merecem destaques as seguintes:

5.1 Uso de senhas seguras

Uma senha forte deve conter pelo menos 12 caracteres e letras maiusculas e minúsculas, bem como símbolos e números. Quanto mais curta e menos complexa for a sua senha, mais fácil é para os criminosos cibernéticos de quebrá-la. Deve-se evitar selecionar informações de identificação, como números de série ("1234") ou informações pessoais que as pessoas saibam que podem identificar (como aniversários e nomes de animais de estimação). Para tornar senhas mais complexas, pode-se considerar a criação de uma ‘frase secreta’. Frases secretas envolvem a escolha de uma frase significativa que seja fácil de lembrar e depois usar a primeira letra de cada palavra para formar a senha.

5.2 Evitar usar a mesma senha

Se for um costume usar a mesma senha para várias contas, o hacker também terá acesso a muitas outras. Lembrar de mudar as senhas regularmente a cada seis meses evita esse tipo de situação.

5.3 Evite anotar senhas

Escrever senhas em pedaços de papel, planilhas ou aplicativos de notas deixa suscetível de ser encontrada por criminosos. Se houver muitas senhas para se lembrar, pode-se considerar o uso de um gerenciador de senhas para auxiliar a manter o controle.

5.4 Autenticação multifator

A autenticação multifator (MFA, na sigla em inglês) é uma ferramenta que dá aos usuários da Internet um nível adicional de segurança de conta para além da combinação padrão de endereços de e-mail/nome de usuário mais senha. A autenticação de dois fatores requer duas formas separadas e distintas de identificação para acessar algo. O primeiro fator é uma senha, e o segundo geralmente inclui um texto com um código enviado para seu smartphone ou biometria usando sua impressão digital, rosto ou retina.

5.5 Limitar o compartilhamento em redes sociais

Se familiarizar com configurações de segurança de cada plataforma de rede social e assegurar que estas são definidas a um nível com o qual se sinta segura. Além de evitar divulgar informações pessoais como endereço em redes sociais, os criminosos podem utilizar informações pessoais para construir uma imagem falsa e se passar por qualquer indivíduo.

5.6 Excluir contas não utilizadas

Se inscrever em serviços online que não são mais utilizados, onde essas contas ainda existem, elas provavelmente contêm uma mistura de dados pessoais, detalhes de identidade e números de cartão de crédito, informações estas que possuem valor para criminosos cibernéticos. Para proteger a privacidade, é aconselhável remover os seus dados privados dos serviços que já não usa.

5.7 Eliminar informações pessoais

Eliminar documentos que contenham dados pessoais, como seu nome, data de nascimento ou número do fundo de previdência. Além disso, é importante monitorar e-mail

pessoal, pois ele pode alertar sobre uma violação de dados que passou despercebida. Como por exemplo, receber uma mensagem de texto informando a localização de um médico desaparecido, isso pode ser um sinal de que seus dados foram comprometidos.

5.8 Sistemas e programas atualizados

Manter sistemas operacionais e software instalando regularmente atualizações de segurança, monitoramento, sistema operacional e software (se disponíveis).

5.9 Monitorar contas

Verificar regularmente os extratos do banco, cartão de crédito e outras contas, para que se possa verificar se houve alguma cobrança não autorizada. Em diversos casos é comum não ser notificado quando uma transação é efetuada. Por isso é necessário manter sob vigilância contas de instituições que usam aplicativos.

6 CRIMES CIBERNÉTICOS - EVOLUÇÃO DA LEGISLAÇÃO BRASILEIRA

O aumento da tecnologia nas últimas décadas junto ao custo-benefício dos aparelhos tecnológicos têm possibilitado uma grande participação de usuários na rede mundial de computadores, conhecida como Internet.

De acordo com os dados das Nações Unidas, o Brasil ocupa o 4º lugar em números de usuários de Internet, com mais de 120 milhões de pessoas conectadas à rede. Já ultrapassando o número de 236 milhões de aparelhos e 210 milhões de habitantes, segundo os dados de 2018.

Essa quantidade atraiu pessoas dispostas a cometer todo tipo de crime no mundo virtual, como: vendas fraudulentas ou produtos ilegais, clonagem de cartões, roubo de dados pessoais, a divulgação de notícias falsas (“fake News”), pedofilia, crimes contra a honra, racismo e muito mais.

O relatório anual de atividades de segurança no mundo da Norton Cyber Security, do início de 2018 colocou o Brasil sendo o segundo país em números de casos de crimes cibernéticos, ficando só atrás da China.

Em 2017, 62 milhões de brasileiros foram afetados por algum tipo de crime cibernético, sendo os mais afetados os usuários do WhatsApp.

O Phishing é uma prática muito comum utilizada por golpistas, que consiste em enviar conversas geralmente falsas com links falsos, quando esses links são abertos ocorre o roubo de informações, direcionamento para lojas falsas com vírus.

O mundo jurídico não soube acompanhar no mesmo ritmo o crescimento da internet e seus crimes, apenas no ano de 2008 a Lei nº 11.829, de 25 de novembro, alterou o ECA (Estatuto da Criança e do Adolescente) para a penalizar a pornografia infantil em redes sociais, introduzindo vários artigos para combater e criminalizar a posse desse tipo de material e condutas relacionadas na internet.

Essa lei também institui a pena de reclusão de 3 a 6 anos para quem oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio de contato registros que contenham cenas de sexos explícito ou pornografias envolvendo crianças e adolescentes.

A Lei no 13.718, que entrou em vigor em 24 de setembro de 2018, adicionou novos crimes ao Código Penal, tornando a conduta de Pornografia por Vingança crime. A figura do crime de divulgação de cena de estupro ou de cena de sexo ou pornografia foi criada entre eles.

O artigo 218-C define como condutas criminosas oferecer, trocar, disponibilizar, transmitir, vender, expor à venda, distribuir, publicar ou divulgar por qualquer meio fotos, vídeos ou material que contenham conteúdo relacionado ao estupro ou com cenas de sexo, nudez ou pornografia sem o consentimento da vítima.

Já o artigo 153 do Código Penal Brasileiro, descreve como crime “divulgar a alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem”, eventualmente levando a uma pena de um a seis meses de detenção ou multa.

Em seu parágrafo primeiro:

> § 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: (Incluído pela Lei nº 9.983, de 2000) Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.

Em completude seu segundo parágrafo diz:

> “§ 2º. Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada. (Incluído pela Lei nº 9.983, de 2000)” (BRASIL, 2000).

Somente com a promulgação da Lei nº 12.737 de 30 de novembro de 2012, que teve origem após o episódio onde vazaram 36 fotos da atriz em 2011. Na época, a atriz Carolina Dieckmann teve seu computador invadido por hackers, que o fizeram através de seu e-mail. Antes de ter suas fotos vazadas, os hackers tentaram extorqui-la, pedindo dinheiro em troca da não publicação das fotos.

Foi então que surgiu a primeira lei que visava proteger a informação e dados individuais no ambiente digital, que trata da invasão de computadores por hackers e acrescenta os artigos ao Código Penal, originando o tipo penal "Invasão de dispositivo informático", além de modificar os artigos 266 e 298. É importante frisar que o parágrafo único do Art. 298 penaliza a falsificação de documentos com a pena de reclusão de até 5 anos e multa, uma vez que se trata da invasão de computadores que ficou conhecida como Lei Carolina Dieckmann, por ter sido sancionada após o caso da atriz brasileira que teve fotos íntimas que estavam em seu computador furtadas e divulgadas virtualmente. A enorme repercussão do fato acima descrito, e a inexistência de leis ou artigos jurídicos para ajudar no caso foram os fatores determinantes para acelerar a criação desta Lei.

Dentre as penas previstas pela Lei estão:

A Detenção de três meses a um ano, e multa para invasão de dispositivos informáticos aleatórios, conectados ou não à rede de computadores, na violação indevida de mecanismos de segurança com o fim de obter, adulterar ou destruir dados ou informações sem autorização do titular do dispositivo.

Reclusão de seis meses a dois anos, e multa se a conduta não constitui crime mais grave se dá pela razão da invasão resultar na obtenção de conteúdo de comunicações eletrônicas particulares ou públicas, segredos comerciais ou industriais, informações sigilosas definidas na lei ou o controle não autorizado de dispositivos invadidos. Tudo segundo ao Artigo 154-A do Código Penal - Decreto -Lei nº 2.848, de 7 de dezembro de 1940.

Já a Lei 12.735 também de 2012, determinou a estruturação e especialização das polícias judiciárias para combate a delitos na rede e modificou a Lei 7.716 (Lei de Crime Racial), através do inciso II do § 3º do artigo 20, objetivando a cessação de transmissões de rádios, televisões ou publicações por qualquer tipo de meio como, indução ou incitação de discriminação de raça, cor, etnia, religião ou procedência nacional. Esta lei trouxe não só proteção e inclusão para as pessoas prejudicadas por estes tipos de crime, como, também trouxe melhorias para possíveis

incentivos a políticas de segurança da informação e práticas aplicadas ao combate a discriminação digital.

O Decreto 7.962 de 2013 regulamentou o Código de Defesa do Consumidor em relação ao Comércio Eletrônico (e-commerce) e as vendas on-line, visando proteger o consumidor de insatisfações com os produtos e possíveis fraudes. Foram impostas aos fornecedores algumas obrigações como disponibilizar em local de fácil visualização do site de vendas, o nome empresarial e número no CNPJ e fornecer o endereço físico e eletrônico ao consumidor. O Decreto também criou regras específicas para ofertas em sites de compra e obrigou a apresentação de um contrato ao consumidor, ficando também o fornecedor responsável por informar os meios para o direito de arrependimento da compra pelo consumidor.

De grande importância, considerado o grande marco civil da internet, a Lei 12.965/2014 trouxe diversas inovações para o mundo digital como a garantia da liberdade de expressão, comunicação e manifestação de pensamento na internet em termos da Constituição Federal; proteção da privacidade e a proteção dos dados pessoais, sendo proibida a utilização no comércio de dados pessoais dos internautas sem o consentimento do usuário e a neutralidade da rede, não podendo os provedores de acesso discriminarem ou dar privilégios a tipos de conteúdo, tratando de forma igual qualquer tipo de pacote de dados.

Foi determinada que a quebra de dados ou informações particulares dos usuários, assim como a retirada de conteúdos de sites ou redes sociais só poderiam ser autorizadas mediante determinação judicial. Exceção feita aos casos de “pornografia de vingança” que é quando fotos ou conteúdos íntimos de uma pessoa são vazados para a rede, então nesse caso a própria vítima da violação poderia solicitar a retirada diretamente a quem estivesse com tal conteúdo.

Outra modificação interessante é que as partes interessadas poderiam pedir ao juiz com o propósito de formar prova em processo judicial cível ou penal que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações da internet.

Em 2016 foi publicado o Decreto 8.771 que regulamenta pontos do Marco Civil como uma neutralidade da rede e a proteção de registros de acesso e dados pessoais.

Os avanços alcançados pelas leis aqui faladas, dividem os especialistas da área jurídica. Alguns concordam com a necessidade de uma lei específica de combate aos crimes cibernéticos mais aprofundada, conforme destaca LIMA(2005, apud ARAÚJO, 2023, p. 7):

> "A maioria dos crimes que ocorrem na rede também existem no mundo real, o que ocorre é que tipos com devidas peculiaridades, o que faz com que seja necessária uma adequação quanto ao seu tipo penal" (LIMA, Paulo Marco Ferreira, 2005, p. 134 apud ARAÚJO, Iran Carlos da Silva, 2023, p. 7).

Já para SILVA (2021, p. 30):

> "Na opinião de política criminal de vigilância, não é eficaz apenas uma legislação que forneça um tipo penal, é preciso a formação de um programa de política criminal de precaução, apoiando-se na educação, na integração social e melhoria do estilo de vida, que qualifica o cidadão a impedir ou evitar eventuais conflitos." (SILVA, Eva Cristina de Souza, 2021, p. 30).

Outros citam como exemplo crimes como ameaça, calúnia, injúria e difamação, visto que a repercussão de tais crimes é muito maior quando é praticado por redes sociais, tendo correlação aos prejuízos e transtornos ocasionados às vítimas, uma vez que as sentenças estão previstas por artigos do Código Penal que é de 1940, retratando uma realidade de um mundo completamente diferente.

7 PROCEDIMENTOS METODOLÓGICOS

Para edição deste artigo foi realizada pesquisa aplicada com abordagem qualitativa com coleta de dados por meio de pesquisa bibliográfica sobre os crimes cibernéticos, roubos de dados e informações no Google Acadêmico e sites jurídicos e estudo de campo sobre roubos que impactaram a história.

8 DESENVOLVIMENTO

Este artigo foi desenvolvido para levantar dados através de pesquisa bibliográfica sobre roubo de dados e crimes cibernéticos no intuito de trazer conscientização e informações para o desenvolvimento de leis específicas. Durante a investigação foi utilizada e apresentado estudo de campo sobre casos verídicos que influenciaram a história e a evolução ao seu respeito.

9 RESULTADOS E DISCUSSÃO

Conforme o avanço da tecnologia houve o aumento dos crimes cibernéticos, causando muitos problemas para a sociedade e empresas. Contudo, neste trabalho buscamos a conscientização para que as pessoas saibam se proteger e se prevenir desses ataques.

10 CONSIDERAÇÕES FINAIS

Com a realização deste trabalho, foi identificado que é preciso prevenir o vazamento dos dados, uma vez que é importante se manter informado sobre notícias e sites de segurança para estar sempre atualizados sobre novos golpes e formas de prevenção, porém cumpre informar que a maneira mais usual de se manter seguro é usando um antivírus confiável, que protege o dispositivo, encontra vulnerabilidades e ameaças, bloqueia, isola e remove qualquer ameaça à segurança, antes mesmos que ela se instale no aparelho.

A implementação dessas estratégias resultará em uma infraestrutura de proteção eficaz e capaz de resistir a ameaças iminentes.

Portanto, conclui-se que o objetivo foi plenamente alcançado, uma vez que foram identificadas e discutidas estratégias eficazes para enfrentar os crimes cibernéticos e proteger os dados. Com a adoção das estratégias apresentadas nesse artigo e a contínua evolução das práticas de segurança, é possível reduzir significativamente as vulnerabilidades e construir um ambiente digital mais seguro e confiável.

REFERÊNCIAS

CONTROLE NET. O que é proteção de dados e como esse processo impacta nossas vidas. São Paulo, 2000. Disponível em: https://www.controle.net/faq/o-que-e-protecao-de-dados-e-como-esse-processo-impacta-nossas-vidas#:~:text=Prote%C3%A7%C3%A3o%20de%20dados%20%C3%A9%20o,dados%20de%20forma%20n%C3%A3o%20autorizada . Acesso em: 15 Mar. 2024.

CLICK COMPLIANCE, HELEN LUGARINHO. Roubo de dados pessoais pela internet: A empresa pode ser responsabilizada?. São Paulo, 2023. Disponível em: https://clickcompliance.com/roubo-de-dados-pessoais-pela-internet-a-empresa-pode-ser-responsabilizada/#:~:text=O%20roubo%20de%20dados%20pessoais,Roubo%20dos%20dispositivos%20f%C3%ADsicos. Acesso em: 17 Mai. 2024.

JUSBRASIL, GALVÃO E SILVA ADVOCACIA. Vazamento e roubo de dados: como evitá-lo. Disponível em: https://www.jusbrasil.com.br/artigos/vazamento-e-roubo-de-dados-como-acontecem-e-como-se-precaver/1384159456. Acesso em: 11 Mai. 2.

KARSPERSKY. O que é roubo de dados e como evitá-lo. Disponível em: https://www.kaspersky.com.br/resource-center/threats/data-theft. Acesso em: 11 Mai. 2024.

PUC GOIÁS. SILVA, EVA CRISTINA DE SOUZA. Proteção contra os Crimes Cibernéticos no Brasil: A necessidade de uma Legislação Específica e Atualizada. Artigo, p. 30. Goiás,

2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1487. Acesso em: 30 Mai. 2024. Acesso na Internet

JUSBRASIL, LIMA, UESLEI DE MELO RODRIGUES, TESSMANN, DAKARI FERNANDES, VENTURIN, EDILEUZA VALERIANA DE FARIAS.Violação dos Direitos Fundamentais em Crimes Cibernéticos e a Necessidade de Inclusão do Direito Eletrônico como Legislação Específica. São Paulo, 2018. Disponível em: https://www.jusbrasil.com.br/artigos/violacao-dos-direitos-fundamentais-em-crimes-ciberneticos-e-a-necessidade-de-inclusao-do-direito-eletronico-como-legislacao-especifica/653015456. Acesso em: 10 abril. 2024.

JUSBRASIL, ALBERTO DIWAN.O crime de invasão de dispositivo de informática - Art. 154-A do Código Penal. São Paulo, 2015. Disponível em: https://www.jusbrasil.com.br/artigos/o-crime-de-invasao-de-dispositivo-de-informatica-art-154-a-do-codigo-penal/199631200#:~:text=%E2%80%9CSe%20da%20invas%C3%A3o%20resultar%20a,se%20a%20conduta%20n%C3%A3o%20constitui. Acesso em: 10 Mar. 2024.

ASCENTY. Os 12 tipos de ataques cibernéticos mais perigosos para sua empresa. São Paulo. Disponível em: https://ascenty.com/blog/artigos/ataques-ciberneticos/. Acesso em: 10 Mar. 2024.

JUSBRASIL, PAULO ROBERTO MOREIRA. O que são crimes cibernéticos. São Paulo, 2022. Disponível em: https://www.jusbrasil.com.br/artigos/o-que-sao-crimes-ciberneticos/1583984125. Acesso em: 25 Maio. 2024.

EMGETIS, JÂNIO OLIVEIRA. Artigo: A Internet como local de crimes virtuais, os cibercrimes: como se proteger. Sergipe, 2017. Disponível em: https://emgetis.se.gov.br/artigo-a-internet-como-local-de-crimes-virtuais-os-cibercrimes-como-se-proteger/. Acesso em: 30 Mai. 2024.

LIMA, Paulo Marco Ferreira. Crimes de computador e segurança computacional. Livro, p. 134. Campinas, SP: Ed. Millennium, 2005 apud ARAÚJO, Iran Carlos da Silva. Os Crimes Cibernéticos e o Direito Penal Brasileiro. Artigo, p. 7. Picos, 2023. Disponível em: https://www.jusbrasil.com.br/artigos/os-crimes-ciberneticos-e-o-direito-penal-brasileiro/1894019562. Acesso em: 21 Mai. 2024.

NUCCI, Guilherme de Souza. Código Penal Comentado. 14ª ed. Rio de Janeiro: Forense, 2014, p. 811

CRYPTOID. Os 9 maiores roubos de dados da história. São Paulo, 2015. Disponível em: https://cryptoid.com.br/criptografia-identificacao-digital-id-biometria/os-9-maiores-roubos-de-dados-da-historia/. Acesso em: 16 Mar. 2024.

BRASIL. Lei nº 9.983, de 2000. Dos crimes contra a inviolabilidade dos segredos. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 14 de Abri. 2024.