FACULDADE DE TECNOLOGIA DE SÃO PAULO
FELIPE PEREIRA ALEIXO

RASTROS DIGITAIS:
COMO O COMPARTILHAMENTO EXCESSIVO DE DADOS NA REDE PODE FACILITAR CRIMES CIBERNÉTICOS

SÃO PAULO
JUNHO / 2023

FACULDADE DE TECNOLOGIA DE SÃO PAULO
FELIPE PEREIRA ALEIXO

RASTROS DIGITAIS:
COMO O COMPARTILHAMENTO EXCESSIVO DE DADOS NA REDE PODE FACILITAR CRIMES CIBERNÉTICOS

Trabalho submetido como exigência parcial para a obtenção do Grau de Tecnólogo em Análise e Desenvolvimento de Sistemas.
Orientadora: Profª. Me. Edméa Pujol Cantón

SÃO PAULO
JUNHO / 2023

RES
ER
VA
DA

FACULDADE DE TECNOLOGIA DE SÃO PAULO

FELIPE PEREIRA ALEIXO

RASTROS DIGITAIS:
COMO O COMPARTILHAMENTO EXCESSIVO DE DADOS NA REDE PODE FACILITAR CRIMES CIBERNÉTICOS

Trabalho submetido como exigência parcial para a obtenção do Grau de Tecnólogo em Análise e Desenvolvimento de Sistemas.

Parecer do Professor Orientador
O Trabalho de Conclusão de Curso do aluno Felipe Pereira Aleixo atendeu a todos as exigências do Departamento de Tecnologia da Informação.

Conceito/Nota Final: 9.0 → nove inteiros

Atesto o conteúdo contido na postagem do ambiente TEAMS pelo aluno e assinada por mim para avaliação do TCC.

Orientadora: Profª. Me. Edméa Pujol Cantón

SÃO PAULO, 20 de Junho de 2023.

Edméa Pujol Cantón
Assinatura do Orientador

Felipe P. Aleixo

Assinatura do aluno

AGRADECIMENTOS

Agradeço minha família e minha namorada por todo o apoio crucial nesse fim de etapa.

À orientadora Edméa pelo auxílio durante o desenvolvimento deste trabalho.

Aos funcionários da FATEC-SP, DTI e professores, por todos esses anos de aprendizado.

"*Quando eu era jovem, sentíamos medo de bombas atômicas.*
Hoje, o que mais me amedronta são ataques cibernéticos."

Steve Wozniak, engenheiro eletrônico e cofundador da Apple.

RESUMO

ALEIXO, Felipe Pereira. **Rastros digitais**: Como o compartilhamento excessivo de dados na rede pode facilitar crimes cibernéticos. 2023. 30 f. Graduação. Tecnologia em Análise e Desenvolvimento de Sistemas. Faculdade de Tecnologia de São Paulo. FATEC-SP. São Paulo, 2023.

Esse estudo tem como objetivo apresentar o conceito e a origem dos rastros digitais assim como a sua utilização em crimes cibernéticos a fim de analisar a ocorrência de cibercrimes em relação ao compartilhamento e uso indevido dos dados digitais das pessoas. É importante também demonstrar os desafios encontrados pelos investigadores na coleta e análise desses rastros e as medidas mitigadoras e remediativas tomadas por parte das plataformas e órgãos governamentais com o intuito de proteger a identidade digital dos usuários.

Palavras-chave: Cibercrime; rastros; privacidade; segurança; dados

ABSTRACT

ALEIXO, Felipe Pereira. **Digital footprint**: How excessive data sharing on the internet could facilitate cybercrimes. 2023. 30 s. Graduation. Technology in Analysis and System Development. Faculdade de Tecnologia de São Paulo. FATEC-SP. São Paulo, 2023.

This study aims to present the concept and origin of digital traces, as well as their use in cybercrimes, in order to analyze the occurrence of cybercrimes related to the sharing and misuse of people's digital data. It is also important to demonstrate the challenges faced by investigators in collecting and analyzing these traces, as well as the mitigating and remedial measures taken by platforms and government agencies to protect users' digital identities.

Keywords: Cybercrime; footprint; privacy; security; data

LISTA DE ABREVIATURAS E SIGLAS

LGPD	Lei Geral de Proteção de Dados Pessoais
GDPR	*General Data Protection Regulation* (Regulamento Geral sobre a Proteção de Dados)
CCPA	*California Consumer Privacy Act* (Lei de Privacidade do Consumidor da Califórnia)
ANPD	Autoridade Nacional de Proteção de Dados

SUMÁRIO

Introdução

Contextualização

Com o aumento da utilização de dispositivos eletrônicos para acessar à Internet, principalmente daqueles de fácil acesso como o smartphone, o rastro digital deixado pelos usuários tornou-se uma preocupação crescente em relação à privacidade e segurança dos dados pessoais, especialmente a partir dos anos 2000 com o surgimento das redes sociais.

Em quaisquer seja o lugar na internet, os usuários sempre deixarão uma ampla variedade de informações sobre si mesmos, de forma voluntária ou não, através de ações realizadas ou processos automáticos encontrados na rede.

O rastro digital é definido pela autora Fernanda Bruno em “Rastros digitais sob a perspectiva da teoria ator-rede” (2012) como:

> “[...] o vestígio de uma ação efetuada por um indivíduo qualquer no ciberespaço. Há, certamente, rastros no ciberespaço que não derivam de ações realizadas por indivíduos, mas de processos automatizados.”

Como destacado pela autora, um rastro digital surge de ações não só individuais e conscientes dos usuários, mas também de processos automatizados. Esses processos são cadastros em sites ou até um simples acesso à uma página na *web*, e muitas informações são coletadas sem conhecimento do usuário. Os dispositivos de vigilância, órgãos governamentais e empresas interessadas coletam e analisam esses dados e têm visto nestes rastros uma valiosa base de dados (BRUNO, 2012).

Escândalos de vazamento de dados e espionagem por parte de governos e empresas para fins comerciais e políticos aumentaram essa preocupação significativamente quando em 2016, um dos maiores casos de vazamento de dados digitais veio à tona e atormentou ainda mais os usuários. Essa violação de dados ocorreu na plataforma da rede social *Facebook*, que se destaca como uma das mais ativas, contando com um estimado de 2,9 bilhões de usuários ativos em 2023 (DATA REPORTAL, 2023). O incidente teve início por meio de um quiz disponibilizado na plataforma, no qual a empresa *Cambridge Analytica* coletou informações dos usuários. Esses dados foram posteriormente manipulados e utilizados indevidamente, sem respeitar a privacidade das pessoas, sendo comercializados

para anunciantes envolvidos em campanhas políticas. O objetivo dessa ação era identificar eleitores, determinar melhores locais para campanhas, auxiliar na comunicação estratégica, direcionar anúncios e disseminar notícias personalizadas, principalmente *fakenews* na rede social americana (REHMAN, 2019). Cerca de 87 milhões de perfis no mundo todo foram afetados (DIXON, 2018). Este vazamento é só um dos exemplos que temos no mundo real. São conhecidos inúmeros casos não só no âmbito corporativo ou comercial, mas também vazamentos mais comuns de cunho pessoal, como de informações bancárias, fotos e acessos de redes, e-mails e aplicativos. De acordo com um levantamento realizado em 2022 pelo *Statista*, só no 3º trimestre de 2020 houve cerca de 125 milhões de dados vazados na internet (PETROSYAN, 2022).

Conforme a tecnologia avança, as pessoas também se aperfeiçoam e com isso surgem, fatalmente, novos métodos de utilização desses rastros tanto para o bem quanto para o mal. A cada ano que passa surgem novos dispositivos eletrônicos, protocolos de rede, *websites* e aplicativos e isso acaba tornando mais difícil ainda os desafios de coleta, análise, investigação e solução de crimes. Os profissionais de cibersegurança que atuarem sobre alguma prova digital, precisam ter o conhecimento técnico e as ferramentas necessárias, se não a prova pode se corromper ou ser invalidada (NASSIF, 2019).

Esses rastros que deixamos de forma excessiva na rede ou que são coletados de forma descontrolada, podem facilitar crimes cibernéticos?

Objetivo Geral

Essa monografia tem como objetivo apresentar o conceito de rastros digitais e seu impacto na privacidade e segurança de indivíduos e empresas, considerando também os desafios na coleta e análise desses rastros em investigações de crimes cibernéticos.

Objetivos Específicos

- Pesquisar as principais características dos rastros digitais, tais como sua natureza, origem e conceito.
- Entender o potencial de uso dos rastros em crimes cibernéticos e seus impactos na segurança pessoal e corporativa.
- Identificar e discutir os desafios associados à coleta e análise de rastros digitais em investigações de crimes cibernéticos.

Metodologia

Para a realização deste Trabalho de Conclusão de Curso utilizou-se como procedimento metodológico a pesquisa bibliográfica e consistiu na busca, seleção e análise da literatura relacionada aos temas de rastros digitais, crimes cibernéticos, privacidade e proteção de dados pessoais, legislações e regulamentos nacionais e internacionais. A pesquisa foi conduzida por meio de consulta a bases de dados eletrônicas, livros, artigos científicos, teses e dissertações e busca apresentar um estudo sobre os rastros digitais e tudo que o envolve, realizando uma análise considerável e conclusiva sobre o problema. (MARCONI; LAKATOS, 2019)

Justificativa

É necessário uma análise abrangente sobre o impacto dos rastros digitais na privacidade e segurança, considerando os desafios inerentes à coleta e análise desses rastros em investigações de crimes cibernéticos. Além disso, é fundamental investigar a aplicabilidade das leis e regulamentos existentes e emergentes na proteção dos dados pessoais diante do aumento na utilização de redes sociais e aplicativos digitais.

Nesse sentido, este trabalho de pesquisa se justifica pela importância de se compreender os impactos dos nossos rastros digitais na privacidade e segurança de indivíduos e empresas. A pesquisa poderá contribuir para a discussão sobre a necessidade de novas políticas públicas e legislações que possam garantir uma proteção adequada aos dados pessoais, em um cenário em que a tecnologia continua a avançar rapidamente.

1. O Rastro Digital

Os estudos sobre rastros digitais remontam às últimas décadas do século XX, época em que a internet começou a se popularizar. O advento das redes sociais e o desenvolvimento de dispositivos móveis, que permitem o acesso constante e instantâneo à internet, trouxe a discussão ainda mais à tona.

Os smartphones se tornaram uma extensão da nossa identidade. Nos celulares carregamos identidades pessoais, de veículo, habilitação, cartões de crédito, contas bancárias, perfis sociais e aplicativos de mensagem, que são essenciais hoje em dia. Nas mídias sociais compartilhamos nossos gostos, mensagens, fotos, música e *likes*, e geralmente não nos preocupamos com os rastros que estamos deixando nas redes.

As empresas estão sendo obrigadas por lei a cumprir com políticas de segurança e proteção de dados em suas plataformas e aplicativos, a fim de manter nossos rastros seguros. Com o avanço das regulamentações, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil, as organizações estão precisando ser mais responsáveis ao realizar o tratamento correto dos dados pessoais dos usuários. Essas leis visam conscientizar as empresas sobre a importância da privacidade e estabelecem direitos aos usuários para controlar o uso de seus dados (MONTEIRO; GOMES et al, 2019).

Origem e Conceito

A identidade digital do usuário é originada a partir dos seus rastros que podem incluir tanto rastros **ativos** quanto rastros **passivos:** (BURDOVA, 2023)**.**

- **Ativos:** são informações deixadas de forma intencional, como nome, telefone, endereço, documentos, fotos, vídeos e mensagens.
- **Passivos** são informações coletadas pelas aplicações sem intenção do usuário, como histórico de navegação, localização, informações do navegador e dispositivos utilizados.

Pode-se conceitualizar um rastro digital como um registro contínuo do comportamento e das interações do usuário no ambiente virtual (BRUNO, 2012). São uma forma de materialização do comportamento humano no espaço virtual e estão intimamente ligados às formas de percepção e cognição. Por meio deles, é

possível compreender como os usuários interagem no ambiente virtual e como suas ações podem ser interpretadas e utilizadas. Na maioria das vezes, mas não exclusivamente, os rastros são intangíveis e formatados de forma a não serem facilmente identificáveis por seres humanos, mas sim pelas aplicações que os manipulam.

Utilização em crimes cibernéticos

Sendo a rastreabilidade na internet uma característica inerente à sua natureza, nossos dados e informações pessoais estão constantemente expostos a potenciais violações de privacidade. A facilidade de compartilhamento excessivo de informações na era digital tem contribuído para a crescente ocorrência de crimes cibernéticos. Os rastros digitais deixados por usuários durante suas atividades online podem ser explorados por criminosos com o intuito de cometer uma série de delitos. Alguns dos principais tipos de crimes que se aproveitam de nossos rastros são:

- **Roubo de identidade:** Através da coleta e análise dos rastros digitais, como informações pessoais, histórico de navegação, registros de compras e interações em redes sociais, os criminosos podem se apropriar da identidade de uma pessoa, resultando em sérias consequências para as vítimas.
- **Roubo de contas e informações pessoais e bancárias:** Os rastros digitais, como senhas fracas, informações de login armazenadas em dispositivos ou mesmo a exposição acidental de informações sensíveis, podem ser utilizados para invadir contas de e-mail, redes sociais, sistemas bancários e outros serviços online.
- **Crimes fora do âmbito digital:** O rastreamento de informações pessoais e hábitos de navegação na internet pode ser usado para crimes como stalking, onde o agressor monitora e assedia a vítima online e offline, e engenharia social, onde o criminoso manipula pessoas para obter informações confidenciais ou acesso a sistemas (PERRY, 2012).

No Brasil, o compartilhamento excessivo de informações pessoais tem contribuído para um aumento significativo nos casos de roubo de contas e informações bancárias. Segundo um estudo realizado pela empresa de segurança

digital PSafe em 2022, houve mais de mil tentativas de roubos de dados financeiros por hora, através de phishing (DINIZ, 2022). Esses ataques, que geralmente ocorrem por meio do compartilhamento de links maliciosos e e-mails falsos, visam enganar as pessoas e levá-las a fornecer informações confidenciais, como senhas e números de cartão de crédito.

Relatos de stalking, que envolve a perseguição persistente e obsessiva de uma pessoa, tanto online quanto offline, têm se tornado mais comuns. No Brasil, foram registradas cerca de 63 mil denúncias de stalking só em 2022 (MONSERRAT; MARTINIUK, 2023). Em um estudo do Pew Research Center de 2020 realizado nos Estados Unidos da América, 14% dos adultos já experienciaram **ameaças físicas** pela internet, 11% sofreram com **stalking** e 11% já foram **assediados sexualmente** por pessoas nas redes.

O simples fato de compartilhar uma foto ou uma publicação comemorando algum evento já dá brecha para os criminosos. Em complementação à foto existem inúmeras informações que se pode extrair ao visualizar uma imagem: a localização da pessoa, se a pessoa compartilha uma foto em um mesmo lugar todo dia na mesma hora, as pessoas que ela acompanha, a rota que ela faz para viajar do trabalho à sua casa e vice-versa. Todas essas informações são dados que um criminoso, com habilidade, tempo e persistência, consegue extrair e usá-los a seu favor ao cometer um crime. Fatalmente, quanto mais imagens, vídeos e mensagens deixamos espalhados pela internet, maior o nosso rastro digital.

A engenharia social é uma estratégia que está em crescente, utilizada pelos criminosos para obter informações confidenciais ou acesso a sistemas. Essa estratégia se baseia em utilizar da boa fé humana e emoções para induzir a pessoa a fornecer informações ao atacante (SHIVANANDHAN, 2020).

2. Desafios na Extração e Análise de Rastros Digitais

A digitalização da sociedade tem resultado em uma quantidade maior de dados sendo gerados e armazenados online, criando uma grande quantidade de rastros digitais. Esses rastros são capazes de fornecer informações valiosas para investigações criminais, mas sua coleta e análise apresentam uma série de desafios.

Antes do advento da tecnologia digital *pessoal*, isto é, celulares, *wearables,* relógios inteligentes e computadores, a dificuldade que a ciência forense digital enfrentava era muito menor. As provas que os investigadores tinham que trabalhar se limitavam a apenas fontes de TV, jornais e relatos, mas hoje é bem diferente haja vista que qualquer pessoa de qualquer lugar do mundo consegue, do seu celular, enviar mensagens, compartilhar conteúdos, imagens, vídeos e áudios.

Para investigar e combater esses crimes, os órgãos de segurança e autoridades competentes enfrentam diversos desafios. A complexidade das infraestruturas tecnológicas e a rápida evolução das técnicas utilizadas pelos criminosos dificultam a identificação e rastreamento dos responsáveis pelos delitos.

A cooperação internacional também é essencial para lidar com os crimes cibernéticos, pois muitas vezes envolvem fronteiras e jurisdições diferentes. Contudo, segundo o art. 170 da Constituição Federal de 1988, assegura-se que toda empresa é livre para exercer atividade econômica no país independentemente de autorização de órgãos públicos, porém está condicionada ao respeito à soberania do Brasil mesmo hospedada em outro território a não ser nacional. Quaisquer delitos ocorridos no âmbito digital, se estiver ferindo os direitos de um cidadão brasileiro ou a soberania do país, está dentro da jurisdição brasileira e é passível de punição.

No capítulo 2 da coletânea de artigos sobre Crimes Cibernéticos (2018) do Ministério Público Federal, afirma-se:

> “Negar-se a cumprir decisão válida emanada de juiz brasileiro, para que sejam fornecidos os dados telemáticos armazenados em seus servidores, exigindo para tanto pedido de cooperação jurídica internacional, traduz-se em desrespeito à jurisdição brasileira como expressão da soberania nacional.” (TEIXEIRA; COSTA, 2018)

As dificuldades de prevenção, investigação e solução de casos digitais não ocorrem pela ausência de legislação. As condutas infratoras já são tipificadas por lei,

sendo a necessidade de melhorias e procura por meios mais eficazes e punitivos para os infratores mais importante do que simplesmente tipificar novas leis (ABREU, 2015).

Extração de Rastros Digitais

A coleta de rastros digitais é um processo complexo que exige conhecimento técnico específico. Alguns desafios enfrentados na coleta de rastros digitais são a falta de padronização dos procedimentos de coleta e a variedade de dispositivos e plataformas utilizados pelos usuários. De acordo com Lilian Nassif em seu artigo de 2019, “Desafios da Coleta de Dados e em Evidências Digitais”, os rastros deixados pelos usuários não seguem um padrão, de modo que é imprescindível a utilização de técnicas e ferramentas específicas para cada plataforma utilizada, sendo cada coleta única e específica.

A diversidade e quantidade de fontes e diferentes ramificações contribuem para a geração de rastros digitais e consequentemente dificulta ainda mais a coleta desses rastros. Cada fonte possui suas próprias peculiaridades e formatos de dados, o que dificulta a integração e análise conjunta dessas informações. Além disso, a diversidade de plataformas, aplicativos e tecnologias em constante evolução requer uma abordagem adaptativa para coletar os rastros digitais de forma eficiente.

Durante a coleta dos rastros digitais, existem procedimentos padrões a serem seguidos para que não se comprometa a veracidade das provas a fim de preservar as evidências. É definido os procedimentos padrões:

> “Os Procedimentos Operacionais Padrões (POP) devem ser definidos e seguidos durante a fase de coleta de evidências digitais, incluindo o uso de materiais específicos, como bolsas antiestáticas, luvas para retirada de discos rígidos (HDs) e bolsas Faraday para armazenar telefones celulares, para bloqueio de sinais eletromagnéticos e impedimento de acesso remoto ao celular.” (NASSIF, 2019)

Após a obtenção das provas digitais, é essencial tomar todo o cuidado na apreensão. Os indivíduos envolvidos normalmente estão alarmados e em estado de medo e é bem comum acontecer o apagamento das evidências a fim de dificultar o trabalho dos investigadores e consequentemente a solução do caso.

Os profissionais responsáveis pela coleta de evidências digitais em investigações criminais têm a possibilidade de coletar essas evidências tanto no

local do crime quanto online. Nas seções seguintes, será detalhado os desafios da extração para cada tipo de local (NASSIF, 2019).

Desafios para Extração *On-site*

A extração *on-site* requer o investigador presencialmente no local, e por conta disso requer uma tomada de decisões mais rápida pois o profissional está lidando com os equipamentos dos suspeitos na hora, e pode ser que provas sejam perdidas tanto por causa de algo programado pelo suspeito (uma limpa em massa dos arquivos do HD, por exemplo) ou podem ser simplesmente perdidas com o tempo, como postagens temporárias como vemos em alguns aplicativos de mensagens como *Snapchat* e *Instagram*.

Alguns dos desafios para extração presencial (NASSIF, 2019):

- **Impossibilidade de remoção física:** A impossibilidade de remover fisicamente um dispositivo que contém evidências digitais, como um *hardware*, depende das suas dimensões, peso e onde está alocado. Isso acarreta em perda de agilidade no processo. Após identificado esse problema, o investigador então recorre ao espelhamento da evidência ou tenta selecionar os dados relevantes diretamente do dispositivo.
- **Tamanho do disco:** O tamanho do disco também pode ser um empecilho, pois o investigador deseja realizar um espelhamento dos discos e ambos precisam ter o mesmo tamanho.
- **Quantidade de evidências:** Para realizar a extração dos rastros que estão contidos nos dispositivos evidências, a equipe de investigação necessita de ferramentas específicas para cada tipo e se for uma quantidade numerosa, terá que dispor de múltiplas dessas ferramentas para executar o trabalho com agilidade.
- **Transferência dos dados:** Para conseguir extrair os dados dos equipamentos, o investigador deverá utilizar algum meio de conexão entre as ferramentas de extração e o dispositivo propriamente dito. Pode ser via cabos, onde é necessário ter uma enorme variedade disponível para utilizar em diferentes padrões de entrada/saída, principalmente celulares de diferentes modelos e marcas. Também pode ser via *wireless*, porém a

extração por esse meio pode ser difícil devido a conexão da rede que os equipamentos estão conectados.

Desafios para Extração *Online*

A extração *online* depende de uma conexão com a rede para ser executada e pode envolver dados em aplicativos de mensagens, redes sociais e até dados armazenados em nuvem. Dos desafios encontrados para realizar a extração *online*, destacam-se (NASSIF, 2019):

- **Velocidade da rede:** O investigador realiza a cópia de todas as informações do dispositivo via rede. No entanto, a velocidade da rede depende de muitos fatores e pode ocorrer oscilações, o que pode causar lentidão ou até cancelamento da extração caso houver desconexão.
- **Alteração de dados:** Os dados digitais encontrados na rede não são uma cópia local. Portanto, tendo o devido acesso e autorização (*login*), qualquer um inclusive o suspeito pode acessar essas informações e manipulá-las. Isso pode incluir a exclusão ou modificação de arquivos, bloqueio de acesso remoto (do investigador) ou desativação das evidências, por exemplo. Essas ações podem comprometer a obtenção de dados confiáveis. O investigador especialista deve se atentar a isso ao tratar as evidências pela internet.
- **Privacidade:** É importante levar em conta os direitos, a segurança e privacidade dos usuários na internet. Por se tratar de provas digitais, muitas vezes podem ser informações sensíveis como mensagens privadas, fotos, áudios além também de informações pessoais. Esses dados são protegidos por lei e devem ser tratados e manipulados com cuidado, sem serem expostos.
- **Jurisdição:** O investigado muito provavelmente armazenou as informações em uma plataforma que hospeda seus dados em um data center alocado em outro país. Apesar da soberania do Brasil e a jurisdição além de fronteiras, como, diferentes leis podem ser aplicadas a diversas situações, e o investigador e a equipe devem considerar todos aspectos antes de prosseguir com a investigação.

Análise de Rastros Digitais

Um dos principais desafios na etapa da análise é a preservação da integridade dos dados coletados. É importante que as evidências digitais sejam preservadas em seu estado original, para garantir a autenticidade e a integridade dos dados, evitando a perda de informações importantes durante a análise.

A grande quantidade de informações disponíveis pode dificultar a identificação de padrões e relacionamentos relevantes para a investigação. Os analistas de segurança que atuarão sobre as provas digitais precisam ter habilidade para interpretar os dados coletados e extrair informações úteis para a investigação, evitando conclusões equivocadas que possam comprometer a validade das evidências (NASSIF, 2019). Devido ao uso de técnicas de anonimização e criptografia, as dificuldades em identificar o autor aumentam e exige o uso de técnicas e ferramentas avançadas.

A coleta e análise de rastros digitais apresentam desafios que precisam ser superados para garantir a validade das evidências. Ressalta-se então, a importância de que os profissionais envolvidos na investigação de crimes digitais possuam conhecimento técnico específico e utilizem técnicas adequadas para a coleta e análise de evidências digitais, além também da disponibilidade de infraestrutura e ferramentas atualizadas e seguras para a análise dessas evidências (NASSIF, 2019).

3. Proteção Digital

O surgimento das redes sociais principalmente após os anos 2000 aumentou o tráfego de rastros de uma forma significativa. A finada rede social *MySpace*, tida como pioneira, foi a primeira a atingir 1 milhão de usuários ativos mensalmente em 2004 (ORTIZ-OSPINA, 2019). Isso são milhões de pessoas trocando mensagens, compartilhando posts, fotos, vídeos, seus gostos para o mundo ouvir. Os rastros deixados através dessas informações são valiosos, críticos e muito sensíveis e devem ser protegidos e manipulados de forma adequada pelas plataformas que armazenam esses dados e também pelas pessoas que conseguem acesso a essas informações.

A proteção adequada dos rastros digitais e a conscientização sobre os riscos associados ao compartilhamento excessivo de informações são aspectos cruciais para mitigar essas ameaças. Tanto as plataformas de redes sociais e serviços online quanto os próprios usuários devem adotar medidas de segurança e privacidade para garantir que esses rastros digitais sejam utilizados de maneira responsável e segura. É necessário também um arcabouço legal efetivo que regulamenta a proteção de dados pessoais e estabeleça responsabilidades claras para as empresas que lidam com essas informações sensíveis.

Medidas Mitigadoras Adotadas por Plataformas e Legislações

As plataformas de redes sociais têm adotado uma série de medidas para mitigar crimes relacionados à exposição e ao roubo de dados pessoais. Uma dessas medidas é a implementação de configurações de privacidade que permitem aos usuários controlar o nível de visibilidade de suas informações. Por meio dessas configurações, os usuários podem definir quem pode visualizar seus perfis, posts e fotos, restringindo o acesso a pessoas confiáveis e limitando a exposição a possíveis criminosos.

Adicionalmente, as plataformas investem em recursos avançados de detecção de atividades suspeitas e de identificação de contas fraudulentas. Algoritmos de inteligência artificial são utilizados para analisar padrões de comportamento, identificar contas falsas ou atividades incomuns e notificar os usuários sobre possíveis ameaças (SINGH, 2019). Essas medidas visam proteger os usuários e prevenir a ocorrência de crimes cibernéticos.

No âmbito legislativo, várias regulamentações têm sido implementadas para forçar as empresas a protegerem mais os dados pessoais dos usuários. Conforme a tecnologia se enraíza mais e mais na vida das pessoas, a preocupação com nossos dados digitais aumenta, porque isso está atrelado a vida pessoal, ao trabalho, relacionamentos e praticamente tudo que está à nossa volta. Junta isso com o grande acesso à informações, estudos e opiniões de especialistas que conseguimos em uma distância de um clique do mouse, então temos uma revolta dos próprios usuários que começam a reivindicar seus direitos digitais e a terem maior consciência política e social. O Regulamento Geral de Proteção de Dados, em inglês *General Data Protection Regulation* (GDPR), aplicável na União Europeia, estabelece diretrizes rígidas sobre a coleta, o processamento e a segurança dos dados pessoais. Ele exige que as empresas obtenham consentimento explícito dos usuários para a coleta e o uso de seus dados, além de impor penalidades significativas em caso de violação (UNIÃO EUROPEIA, 2018).

Após a implementação da GDPR, o mundo inteiro entrou em uma discussão extensiva sobre privacidade e compartilhamento de dados. No Brasil, surgiu então a Lei Nº 13.709 - Lei Geral de Proteção de Dados Pessoais - LGPD. A LGPD estabelece princípios, direitos e deveres sobre a proteção de dados pessoais. Ela obriga as empresas a adotarem medidas de segurança adequadas para proteger os dados dos usuários e estabelece sanções para o descumprimento das normas (BRASIL, 2018). Da mesma forma, nos Estados Unidos a *California Consumer Privacy Act* (CCPA) busca garantir a privacidade dos dados dos consumidores e dá aos usuários o direito de optar por não permitir a venda de suas informações pessoais (DEPARTAMENTO DE JUSTIÇA DA CALIFÓRNIA, 2018). A CCPA também é de extrema importância, pois a maioria das empresas de tecnologia grandes tem suas plataformas hospedadas nos Estados Unidos da América ou na Califórnia, como Apple, Facebook, Google e Amazon (YU, 2018), então são obrigadas a seguir as diretrizes da CCPA em suas soluções.

Uma mudança que a GDPR e a CCPA trouxeram e foi imediatamente percebida pelos usuários, foi a solicitação de permissão para utilização dos *cookies*. Cookies são rastros que deixamos em todos websites que visitamos. Com esse rastro a aplicação consegue customizar a experiência do usuário durante sua navegação e também personalizar anúncios (NGUYEN; MCNALLY, 2023), mas

também podem ser compartilhados (ou vendidos) para outras empresas terceiras de publicidade, muitas vezes sem consentimento da pessoa que está acessando o website. Entretanto, de acordo com o GDPR, os websites devem obter o consentimento informado do usuário antes de coletar ou armazenar os cookies que contenham dados pessoais. Isso significa que os websites devem solicitar permissão aos usuários para utilizar cookies que rastreiam suas atividades online e coletam informações sobre eles. Além disso, as empresas devem fornecer informações claras e compreensíveis sobre o propósito dos cookies, quais dados são coletados, por quanto tempo serão armazenados e se serão compartilhados com terceiros (UNIÃO EUROPEIA, 2018).

Medidas Remediativas Adotadas por Plataformas e Legislações

As plataformas de redes sociais devem fornecer canais de denúncia eficientes e mecanismos para relatar incidentes de segurança, abuso ou violação de privacidade. Além disso, é importante que as plataformas estejam prontas para responder prontamente às denúncias, investigar os incidentes e tomar medidas corretivas, como a remoção de conteúdo ofensivo ou a suspensão de contas envolvidas em atividades criminosas.

Nos Estados Unidos, as *Big Techs* (gigantes da tecnologia como IBM, Google, Amazon, Meta, Apple e Microsoft) têm um importante papel na segurança dos indivíduos que utilizam de suas tecnologias, e isso não só em solo americano. O governo americano acredita que uma parceria entre os órgãos governamentais e as empresas de tecnologia poderia se formar uma espécie de Convenção de Genebra, estabelecendo normas internacionais entre os países para se tratar do direito digital das pessoas. Apesar dessa nova convenção ainda não ter saído do papel oficialmente, muitas dessas gigantes da tecnologia se comprometeram, juntamente ao governo americano, a realizar um significativo investimento na área de cibersegurança e abrir empregos relacionados, além de realizar parcerias com universidades, treinamentos, melhorias de segurança nos seus respectivos softwares e soluções *open source* (SAJJAD, 2022).

No aspecto legislativo, as leis devem garantir que as vítimas de crimes cibernéticos tenham acesso a mecanismos eficazes de reparação. Isso inclui a possibilidade de buscar indenização por danos sofridos, a criação de unidades

especializadas para lidar com crimes cibernéticos e a cooperação entre agências governamentais, empresas e organizações da sociedade civil para combater essas ameaças. No Brasil, segundo a LGPD, é previsto sanções administrativas e ações judiciais para as vítimas que tiverem seus dados pessoais violados (BRASIL, 2018).

Violações às regras de proteção de dados pessoais previstas na LGPD poderão ser punidas pela ANPD (Autoridade Nacional de Proteção de Dados) mediante as sanções do artigo 52, que variam desde advertência a multas de R$ 50 milhões (FECOMERCIO SP, 2023).

Conclusão

Nesta pesquisa, foi possível analisar a relação entre o compartilhamento excessivo desregrado de dados pessoais na rede e os crimes cibernéticos. Foi demonstrado que a forma de manipulação dos dados pessoais dos usuários pode sim expor os indivíduos a riscos de fraudes, roubo de identidade, phishing, ataques de engenharia social e invasões em sistemas e redes. Ressaltou-se que tais compartilhamentos não partem apenas dos próprios usuários, mas também das empresas que coletam esses dados.

A exposição de informações sensíveis de empresas pode resultar em prejuízos financeiros e danos à reputação. Os vazamentos de dados de clientes e usuários são comuns e tais ocorrências tornam ainda mais popular o tema segurança digital e proteção de dados, haja vista que mais pessoas têm acesso à Internet e estão mais interessadas em ter seus dados protegidos e manipulados de forma correta. A maneira como a vida pessoal e do trabalho estão intrinsecamente conectadas ao meio digital contribui para esse interesse e consequentemente no surgimento de novas políticas públicas e medidas tomadas pelas empresas.

Também foram analisados os desafios na extração e análise desses rastros para investigação dos crimes. A alta quantidade de dados deixados por um único indivíduo dificulta o trabalho do investigador e dos especialistas trabalhando no caso. Ademais, se tratando de rastros deixados na rede é bem complexo, pois esses rastros são deixados em diferentes formatos, por diversos dispositivos que são programados de várias maneiras e publicados em diferentes plataformas. Tudo isso é um obstáculo na hora de solucionar os crimes e encontrar suspeitos.

Solicitar aos usuários para que não compartilhem dados é utópico, assim como solicitá-los para que não cometam crimes. Os usuários precisam, impreterivelmente, de proteção no âmbito digital, partindo tanto pelas plataformas quanto pelo governo. Por isso, formas de mitigação e remediação foram impostas por movimento das próprias empresas de tecnologia, que também sofrem pressão pública para melhorarem seus serviços e segurança em suas plataformas. Regulamentos emergentes empurram as plataformas contra a parede e as obrigam a cumprir com normas de segurança a fim de tornar a experiência na rede menos nociva. Essas medidas vêm sendo bem sucedidas e visam aumentar o número de denúncias, filtros e o principal: evitar crimes cibernéticos.

SUGESTÕES PARA TRABALHOS FUTUROS

Seria interessante analisar mais tecnicamente os diferentes tipos de rastros (cookies, pixel de rastreamento, *local storage* e seus diversos usos e implementações.

Um estudo sobre stalking realizado através de rastros é um bom conteúdo também, podendo investigar mais a fundo engenharia social e stalking, conseguindo mesclar com o campo da psicologia para entender o comportamento humano por trás do criminoso e também da vítima exposta. Um indivíduo consegue entender muito da rotina e da vida de uma pessoa somente através da análise de seu rastro digital, então seria interessante um trabalho que entra mais em detalhes nesse sentido.

Referências Bibliográficas

ABREU, E. Os entraves à repressão dos crimes cibernéticos. 2015. Disponível em: http://edufranco91.jusbrasil.com.br/artigos/142294529/os-entravesarepressao-aos-crimes-ciberneticos. Acesso em 16 mai. 2023.

BRASIL. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf. Acesso em: 17 mai. 2023.

BRASIL. Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018.

BRUNO, F. Rastros digitais sob a perspectiva da teoria ator-rede. Revista FAMECOS. Porto Alegre, 2012. Disponível em: https://revistaseletronicas.pucrs.br/index.php/revistafamecos/article/view/12893/8601. Acesso em: 29 mar. 2023.

BURDOVA, C. O que é pegada digital e por que ela é importante?. AVG, 2023. Disponível em: https://www.avg.com/pt/signal/what-is-a-digital-footprint. Acesso em 15 mai. 2023.

DATA REPORTAL. Facebook users, stats, data & trends. Data Reportal, 2023. Disponível em: https://datareportal.com/essential-facebook-stats#:~:text=Essential%20Facebook%20statistics%20and%20trends,'active'%20social%20media%20platforms. Acesso em 17 jun. 2023.

DEPARTAMENTO DE JUSTIÇA DA CALIFÓRNIA. CCPA – California Consumer Privacy Act. 2018. Disponível em: https://oag.ca.gov/privacy/ccpa. Acesso em: 16 mai. 2023.

DINIZ, D. **Golpes financeiros**: mais de mil por hora, neste ano. PSafe, 2022. Disponível em: https://www.psafe.com/blog/golpes-financeiros/. Acesso em: 16 mai. 2023.

DIXON, S. Facebook accounts affected by Cambridge Analytica. Statista, 2018. Disponível em: https://www.statista.com/statistics/831815/facebook-user-accounts-affected-cambridge-analytica-by-country/. Acesso em 13 mai. 2023.

FECOMERCIO SP. **LGPD**: multas e sanções já estão valendo; saiba como se preparar. FECOMERCIO SP, 2023. Disponível em: https://www.fecomercio.com.br/noticia/lgpd-multas-e-sancoes-ja-estao-valendo-saiba-como-se-preparar#:~:text=As%20viola%C3%A7%C3%B5es%20%C3%A0s%20regras%20de,multas%20de%20R%24%2050%20milh%C3%B5es. Acesso em 17 jun. 2023.

MARCONI, M. A; LAKATOS, E. M. Fundamentos de Metodologia Científica. 8 ed. São Paulo: Atlas, 2019.

TEIXEIRA, F; COSTA, P. **Crimes Cibernéticos**: Coletânea de Artigos. Ministério Público Federal. 2018. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 17 maio 2023

MONSERRAT, D; MARTINIUK, T. Brasil registra mais de 63 mil denúncias de 'stalking' em 2022; SP é o estado com maior número de casos. 2023. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2023/04/04/brasil-registra-mais-de-63-mil-denuncias-de-stalking-em-2022-sp-e-o-estado-com-maior-numero-de-casos.ghtml. Acesso em: 16 mai 2023.

MONTEIRO, R. L; GOMES, M. C. O. et al. Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf. Acesso em 16 mai. 2023.

NASSIF, L. N. Desafios da coleta de dados e em evidências digitais. Revista O Alferes, Belo Horizonte, 74 (29): 89-107, 2019. Disponível em: https://revista.policiamilitar.mg.gov.br/index.php/alferes/issue/view/110. Acesso em 12 mai. 2023.

NGUYEN, S; MCNALLY. C. What Are Internet Cookies and How Are They Used?. 2023. Disponível em: https://allaboutcookies.org/what-is-a-cookie. Acesso em: 31 mai. 2023.

ORTIZ-OSPINA, E. The rise of social media. 2019. Disponível em: https://ourworldindata.org/rise-of-social-media. Acesso em 16 jun. 2023.

PERRY, J. **Digital stalking**: A guide to technology risks for victims. 2012, edição 2. Disponível em: https://www.saferderbyshire.gov.uk/site-elements/documents/pdf/digital-stalking-a-guide-to-technology-risks-for-victims.pdf. Acesso em: 22 mai 2023.

PETROSYAN, A. Data records breached worldwide. Statista, 2022. Disponível em: https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/. Acesso em: 12 mai. 2023.

REHMAN, I. Facebook-Cambridge Analytica data harvesting: What you need to know. Library Philosophy and Practice. 2019. Disponível em: https://digitalcommons.unl.edu/libphilprac/2497. Acesso em: 01 abr. 2023.

SAJJAD, S. The role of Big Tech in cyber defence. IDG Connect, 2022. Disponível em: https://www.idgconnect.com/article/3649770/the-role-of-big-tech-in-cyber-defence.html. Acesso em 16 jun. 2023.

SHIVANANDHAN, M. Social Engineering - The art of attacking humans. 2020. Disponível em: https://www.freecodecamp.org/news/social-engineering-the-art-of-hacking-humans/. Acesso em: 16 mai. 2023.

SINGH, A. Using AI to combat the menace of “Fake Accounts” on Social Media. 2019. Disponível em: https://ankitnsingh.medium.com/using-ai-to-combat-the-menace-of-fake-accounts-on-social-media-ffc4e66307c8. Acesso em: 31 mai. 2023.

UNIÃO EUROPEIA. General Data Protection Regulation (GDPR). União Europeia, 2018.

YU, W. The Tech Industry in California and Los Angeles. 2018. Disponível em: https://www.anderson.ucla.edu/documents/areas/ctr/forecast/reports/uclaforecast_Sept2018_Yu.pdf. Acesso em: 31 mai. 2023.

Referências Bibliográficas Complementares

ABC NEWS. Apple co-founder Steve Wozniak says cyber crime is world's greatest threat. 2016. Disponível em: https://www.abc.net.au/news/2016-04-18/apple-steve-wozniak-says-cyber-security-greatest-threat/7334954. Acesso em: 16 jun. 2023.

BRUNO, F. **Dispositivos de vigilância no ciberespaço**: duplos digitais e identidades simuladas. Revista Fronteiras. Porto Alegre, 2006. Estudos midiáticos, p. 152-159. Disponível em: https://revistas.unisinos.br/index.php/fronteiras/article/view/6129/3304. Acesso em: 03 abr. 2023.

CANTERBURY CHRIST CHURCH UNIVERSITY. Learning and Skills Hub: Your Digital Footprint, 2021. Disponível em: https://www.canterbury.ac.uk/learning-skills-hub/your-digital-footprint. Acesso em: 29 abr. 2023.

COSTA, T. Desafios para a investigação de crimes digitais. 2016. Disponível em: https://www.jusbrasil.com.br/artigos/desafios-para-a-investigacao-de-crimes-digitais/351838651. Acesso em 25 mai. 2023.

CURTIS, J; OXBURGH, G. Understanding cybercrime in ‘real world’ policing and law enforcement. The Police Journal, 2022. Acesso em: 02 abr. 2023.

SENADO FEDERAL. Lei com penas mais duras contra crimes cibernéticos é sancionada. 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contra-crimes-ciberneticos-e-sancionada. Acesso em: 13 abr. 2023.