INTERFACE TECNOLÓGICA

O IMPACTO DAS PEGADAS DIGITAIS NA SEGURANÇA E PRIVACIDADE ON-LINE DO USUÁRIO

THE IMPACT OF DIGITAL FOOTPRINTS ON THE USER'S ONLINE SECURITY AND PRIVACY

Gabriel Oliveira Silva – contatogabrieloliveira@outlook.com
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – SP – Brasil

Giuliano Scombatti Pinto – giuliano.pinto@fatectq.edu.br
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – SP – Brasil

DOI: 10.31510/infa.v21i2.2015
Data de submissão: 05/09/2024
Data do aceite: 23/11/2024
Data da publicação: 20/12/2024

RESUMO

Como uma consequência da evolução da tecnologia e a democratização do acesso à Internet, os usuários estão se tornando cada vez mais dependentes de aplicativos e serviços on-line. Contudo, na contemporaneidade digital, toda interação com esses recursos gera dados que são coletados para análise e personalização de serviços. Sabendo disso, este artigo teórico tem como objetivo discutir a coleta de dados pessoais, o conceito de pegada digital e o impacto que ela gera na segurança e privacidade on-line do usuário, afinal, é a intimidade do utilizador exposta como resultado de sua interação com o ambiente virtual. Este estudo se trata de uma revisão bibliográfica, o que inclui a utilização de livros, teses, dissertações e artigos científicos. Dessa forma, foi possível concluir que a exploração e o uso indevido de dados pessoais podem provocar danos significativos à vida pessoal, social e financeira dos indivíduos, sendo necessária a conscientização digital.

Palavras-chave: Pegadas digitais. Big Data. Dados pessoais. Segurança. Privacidade.

ABSTRACT

As a consequence of the evolution of technology and the democratization of Internet access, users are becoming increasingly dependent on online applications and services. However, in the digital age, every interaction with these resources generates data that is collected for analysis and service personalization. With this in mind, this theoretical article aims to discuss the collection of personal data, the concept of digital footprint and the impact it has on users' online security and privacy, after all, it is the user's intimacy that is exposed as a result of their interaction with the virtual environment. This study is a bibliographic review, which includes the use of books, theses, dissertations, and scientific articles. Thus, it was possible to conclude that the exploitation and misuse of personal data can cause considerable damage to individuals' personal, social and financial lives, and that digital awareness is necessary.

Keywords: Digital footprints. Big Data. Personal data. Security. Privacy.

1 INTRODUÇÃO

Com uma origem datada há milhares de anos, a humanidade deixa os rastros de sua existência por onde quer que passe. Tais vestígios traçam o caminho percorrido, relatam como os humanos moldam o seu entorno e podem ser encontrados em todo o planeta. Com o advento da Internet, iniciou-se uma nova fase: o espaço físico foi transportado para o espaço virtual e começou-se a gerar rastros a partir de interações sociais on-line, assim como dos novos hábitos de consumo, a forma de absorver produções culturais, a relação homem-trabalho, entre outros aspectos do dia a dia. Sendo assim, é inevitável obter marcas da interação entre o ser humano e o ambiente – seja ele físico ou digital.

Nesse sentido, surge o conceito de pegada digital que, por sua vez, também é conhecida como sombra digital ou rastro eletrônico, sendo isso um conjunto de dados deixados por uma pessoa ao utilizar a Internet, abrangendo desde os sites visitados pelo usuário até os e-mails enviados e as informações compartilhadas on-line, resultando em uma enorme fonte de dados pessoais que são coletados diariamente e que, em concordância com o matemático britânico Clive Humby (2006), os dados podem ser considerados o novo petróleo, uma vez que por meio deles é possível ditar comportamentos e induzir ao consumo, por isso eles se tornam ativos importantes para os negócios e a sua obtenção é incentivada.

Atualmente, com a democratização do acesso à Internet, os usuários geram milhões de dados sobre seu comportamento digital que são compartilhados entre organizações para que estratégias sejam definidas. Logo, surge uma nova preocupação: a segurança e a privacidade on-line do indivíduo. Portanto, este artigo teórico tem como objetivo discutir a coleta de dados pessoais, o conceito de pegada digital e o impacto gerado na segurança e privacidade do usuário. Além disso, pontuar como esses rastros são utilizados por organizações para fins comerciais e as consequências da exposição virtual, visto que resultam na criação de mais pegadas e, consequentemente, mais dados.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Conceito de pegadas digitais

De acordo com a ONU News (2022), serviço oficial de notícias da Organização das Nações Unidas (ONU), existem 5,3 bilhões de usuários de Internet no mundo. No Brasil, segundo o NIC.br (Núcleo de Informação e Coordenação do Ponto BR) (2022), por meio da

pesquisa TIC Domicílios 2021, elaborada pela sua área de indicadores, o Cetic.br (Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação), foi apresentado que 138,8 milhões de pessoas estão conectadas no Brasil praticamente o tempo todo.

Ainda segundo a pesquisa divulgada pelo NIC.br, os participantes da análise afirmaram que utilizam a Internet com a intenção de enviar ou receber mensagens de texto (93%), conversar por chamadas de vídeo (82%), acessar redes sociais (81%), assistir à vídeos e ouvir músicas (73%), ler jornais, revistas ou notícias (54%), acompanhar transmissões ao vivo (50%) e para buscar informações sobre saúde (50%).

Na contemporaneidade digital, efetuar tais atividades gera um rastro conhecido como pegada digital. Conceitualmente, Weaver e Gahegan (2007) classificam a pegada digital como um espaço de alta dimensão e em constante expansão, caracterizado por transações digitais, amplificado pela vigilância e moldado por associações e padrões que se desenvolvem ao longo do espaço e do tempo. Popularmente, esse rastro é visto como uma marca deixada na Internet toda vez que se utiliza sites, redes sociais ou qualquer outra plataforma.

Portanto, cada ação on-line deixa uma marca, isto é, um rastro eletrônico que define a pegada digital do usuário. Sendo assim, há diferentes maneiras de coletar essas pegadas, dessa forma, é de suma importância conhecer os tipos de pegadas digitais e como são coletadas. Nesse sentido, Girardin *et al*. (2008) definem duas categorias principais para esses rastros: pegada digital ativa e pegada digital passiva.

2.1.1 Pegadas digitais ativas

A primeira categoria corresponde às pegadas digitais ativas que, por sua vez, referem-se aos rastros deixados voluntariamente pelos usuários, justamente com o propósito de compartilhar informações sobre si mesmos, isto é, estando cientes de sua coleta (Arakerimath; Gupta, 2015). Nesse cenário, o indivíduo compartilha intencionalmente informações pessoais durante suas interações on-line, o que pode incluir uma variedade de situações, sendo as redes sociais um dos principais exemplos.

De acordo com Galdino (2016), os dados são predominantemente obtidos de fontes web e redes sociais, abrangendo desde fluxos de cliques, blogs, *posts* e até *feeds* de notícias. Isso acontece, pois, ao compartilhar uma atualização de status, uma foto, um vídeo ou um comentário em uma plataforma de mídia social, blog ou fórum, o usuário está deixando uma pegada digital ativa que revela traços de sua personalidade, opinião e interesse em relação a um determinado assunto no momento de sua interação.

As operações transacionais também são mencionadas por Galdino (2016), como registros de chamadas, reclamações empresariais e compras com cartão de crédito. Isso acontece, pois, ao fazer compras on-line, o usuário fornece informações pessoais, como nome, endereço de e-mail, número de telefone, endereço de entrega, detalhes de pagamento e preferências de compra, bem como outras informações envolvidas na transação, como recibos e históricos, sendo essas informações importantes para diferentes organizações.

2.1.2 Pegadas digitais passivas

A segunda categoria corresponde às pegadas digitais passivas que, por outro lado, são criadas automaticamente, muitas vezes sem a participação consciente do usuário, sendo coletadas implicitamente durante suas atividades on-line (Arakerimath; Gupta, 2015). Dessa forma, esse é o cenário que merece maior atenção, pois é um processo oculto em que o usuário pode não perceber o que está acontecendo, uma vez que são utilizados identificadores e rastreadores para monitorar a sua atividade em tempo real durante a utilização.

Para isso, sabe-se que cada dispositivo conectado à Internet possui um endereço IP que identifica de forma única o equipamento (Tanenbaum, 2003), o que pode revelar informações como a localização geográfica, o provedor de Internet e detalhes da rede local. Além disso, os *cookies*, que "são marcadores digitais introduzidos no disco rígido dos computadores dos usuários pelos sites visitados" (Marques, 2019, p. 11), armazenam dados como preferências de idioma, histórico de navegação entre outras atividades dentro do navegador.

Ademais, para Galdino (2016), há os dados biométricos que são usados para identificação automática, como DNA, impressões digitais e reconhecimento facial, além dos dados *machine-to-machine*, que são gerados diretamente por máquinas, como sensores, dispositivos de GPS e medidores. Portanto, com a evolução da tecnologia e o surgimento de novos dispositivos, os usuários estão cada vez mais dependentes desses serviços e, por consequência, gerando dados que revelam sobre a sua interação com o ambiente.

2.2 Utilização das pegadas digitais

Ao analisar o cenário atual, é possível afirmar que a humanidade está vivendo em uma era em que os dados, quando devidamente tratados, manipulados e interpretados, geram informações que, quando testadas, validadas e codificadas, se transformam em conhecimento (Rodriguez, 2001). Logo, este conhecimento é essencial, pois proporciona respostas para diversas questões e são fundamentais na tomada de decisões.

Contudo, essa grande abundância de dados exige técnicas avançadas de armazenamento e processamento para extrair informações relevantes e, dessa forma, gerar conhecimento útil. Sendo assim, surge o conceito de *Big Data*, uma vez que a sua aplicabilidade está no tratamento de um grande volume de dados, oriundos de variadas fontes e que demandam alta velocidade de processamento na busca por um valor (Taurion, 2013).

2.2.1 *Big Data* e dados pessoais

Conceitualmente, *Big Data* se refere a um conjunto de dados cujo tamanho está além da capacidade das ferramentas típicas de software e de banco de dados de capturar, armazenar, gerenciar e analisar esses registros (Manyika *et al*., 2011). Sabendo disso, a capacidade de análise aprofundada é a principal vertente explorada pelas organizações, permitindo-lhes compreender melhor o mercado e seus consumidores.

Em suma, a capacidade de coletar, analisar e interpretá-los se tornou essencial para as organizações que buscam se adaptar e prosperar em um mundo cada vez mais orientado por dados. Dessa forma, o *Big Data* "está causando uma revolução em como empresas, governos e organizações coletam e analisam os dados para a tomada de decisão, tanto no âmbito governamental quanto no empresarial" (Coneglian; Segundo; Sant'ana, 2017, p. 62).

Nesse caso, os dados pessoais se tornam fundamentais para o crescimento das empresas, uma vez que, ao ter conhecimento do perfil de seus potenciais consumidores, podem direcionar com mais precisão as suas atividades e criar estratégias personalizadas para influenciar o consumo. No entanto, o uso excessivo e descontrolado dos dados pessoais pode acarretar prejuízos à privacidade e à vida íntima dos usuários (Marques, 2019).

2.2.2 Regulamentação dos dados pessoais

No Brasil, de acordo com a Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD), o dado pessoal pode ser definido como "informação relacionada à pessoa natural identificada ou identificável". Dessa forma, a lei reconhece que a proteção de dados não se aplica apenas a informações óbvias que identificam uma pessoa, mas também a dados que, mesmo de forma indireta, podem levar à identificação de alguém.

No contexto das pegadas digitais, coleta-se informações diretas, como nome completo, endereço residencial, número de telefone, endereço de e-mail, CPF e data de nascimento, além de informações indiretas, como dados bancários, informações de cartão de crédito,

geolocalização e identificadores on-line. Por isso, Galdino (2016) afirma que os dados privados, isto é, aqueles que são gerados por pessoas, devem ser protegidos por legislação.

Sendo assim, o uso de dados pessoais a partir das pegadas digitais estão sujeitos a regulamentações de privacidade, como a LGPD, que estabelecem regras sobre como as empresas podem coletar, armazenar, processar e compartilhar os dados que possam identificar direta ou indiretamente um indivíduo. Com isso, busca-se assegurar a privacidade e os direitos dos usuários, mitigando os riscos associados à exploração indevida dessas informações.

2.3 Segurança e privacidade on-line

Na realidade digital, é importante compreender os conceitos de segurança e privacidade, uma vez que são utilizados como sinônimos, porém possuem significados distintos. De um lado, segurança se refere às práticas e medidas adotadas para proteger a autenticidade de uma informação, que deve possuir três características fundamentais: confidencialidade, integridade e disponibilidade (Whitman; Mattord, 2017).

Por outro lado, para o conceito de privacidade, Westin (1967) aponta que privacidade das informações é definida como “o direito de indivíduos, grupos ou instituições de determinar por si mesmos quando, como e em que medida as informações sobre eles são comunicadas a outros”, ou seja, refere-se ao controle que os indivíduos têm sobre como suas informações pessoais são coletadas, usadas, compartilhadas e armazenadas na Internet.

Por isso, no contexto de pegadas digitais e da utilização de dados pessoais, é necessário proteger os sistemas digitais contra ameaças como vírus, ataques cibernéticos, roubo de identidade e outras atividades maliciosas, assegurando as três características da informação, bem como o uso adequado dessas informações e uma comunicação clara entre o usuário e o sistema, garantindo, portanto, a segurança e a privacidade on-line.

2.3.1 Danos à vida íntima do usuário

Os dois conceitos apresentados anteriormente são fundamentais para a proteção dos indivíduos na Internet, pois a falha em garantir esses aspectos pode resultar em impactos profundos. Segundo Weber (2010), “a proteção de dados pessoais deve ser considerada uma questão-chave”, afinal, ter os dados comprometidos é um grande risco tanto no caráter pessoal quanto no profissional. Dessa forma, quando a segurança é comprometida, seja por conta de vazamentos ou ataques cibernéticos, dados pessoais, como informações bancárias e documentos de identidade, podem ser expostos, aumentando o risco de fraudes, roubo de

identidade e outras atividades maliciosas, bem como o acesso a informações sensíveis, como histórico de navegação e comunicações privadas (Such; Pereira; Silva, 2020).

Nessas situações, segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), por meio da Cartilha de Segurança para Internet (2012), é esperado um aumento nas tentativas de golpes por diferentes meios, como mensagens de texto, e-mails e ligações telefônicas. Portanto, essa exposição indevida pode resultar em situações de chantagem e extorsão, assim como perdas financeiras e estresse emocional. Em contrapartida, esse tema transcende a esfera de golpes ou situações de constrangimento, uma vez que grandes empresas também se beneficiam do vazamento de dados pessoais. Um dos casos mais notórios ocorreu em 2018, quando dados de aproximadamente 87 milhões de usuários do Facebook foram vazados e usados para propaganda política (Carvalho; Tagliaferro, 2020).

Essas informações foram acessadas pela Cambridge Analytica, uma empresa de análise de dados, por meio de brechas na política de privacidade do Facebook. A empresa utilizou esses dados para construir perfis psicográficos detalhados, direcionando campanhas personalizadas com o objetivo de influenciar comportamentos eleitorais e decisões políticas, como as eleições presidenciais dos Estados Unidos. Em resposta, o Facebook implementou medidas para reforçar a proteção dos dados pessoais dos usuários. Após esse acontecimento, intensificaram-se as discussões sobre o impacto dos vazamentos de dados, uma vez que a influência dos algoritmos é evidente no comportamento dos utilizadores (Carvalho; Tagliaferro, 2020). Contudo, mesmo que medidas sejam aplicadas, é fundamental que cuidados adicionais sejam adotados.

2.3.2 Métodos de segurança

Com o objetivo de aumentar a segurança do usuário e de protegê-lo de potenciais ameaças, o CERT.br, por meio da já mencionada Cartilha de Segurança para Internet (2012), destaca a importância de algumas ações, como por exemplo ajustar as configurações de privacidade em redes sociais, aplicativos e serviços, bem como ter cautela com as informações compartilhadas na Internet e monitorar regularmente a presença on-line.

Ainda nesse sentido, a Cartilha afirma que, para minimizar os rastros deixados e preservar o anonimato, recomenda-se o uso do modo de navegação anônima, a limpeza regular de *cookies* e caches, assim como adoção do uso de uma Rede Privada Virtual (VPN),

uma vez que ela oculta o endereço IP e criptografa as interações on-line, dessa forma oferecendo uma camada adicional de segurança e privacidade.

Ademais, manter um software de antivírus atualizado é uma prática vital para detectar e bloquear ameaças à privacidade. Por fim, o uso de senhas fortes e únicas por meio de gerenciadores de senhas, combinado com a ativação da autenticação de dois ou múltiplos fatores, pode proteger o usuário contra possíveis invasões. Portanto, manter-se seguro exige uma combinação de boas práticas, ferramentas de segurança e conscientização.

3 PROCEDIMENTOS METODOLÓGICOS

Para a realização deste estudo, foi adotada a metodologia de revisão bibliográfica, a qual se caracteriza pelo uso e análise de documentos de domínio científico, tais como livros, periódicos, enciclopédias, ensaios críticos, dicionários e artigos científicos (Oliveira, 2007). Sendo assim, realizou-se uma busca criteriosa de materiais científicos publicados nos últimos dez anos ou mais, utilizando bases de dados como o Periódicos CAPES, Google Acadêmico e Scielo. As buscas realizadas incluíram combinações como "pegada digital", "*digital footprint*", “dados pessoais”, "*big data*", "privacidade", "segurança".

A seleção do conteúdo seguiu alguns critérios, como a relevância para o tema, medida pela relação com o escopo do estudo, a originalidade dos resultados, medida pela contribuição inovadora ao debate sobre pegadas digitais, e a qualidade metodológica dos materiais, medida pelo seu detalhamento. Por fim, as informações coletadas foram organizadas e analisadas de forma crítica, com base em critérios como a consistência entre os conteúdos apresentados, a relação direta com os objetivos deste estudo e a aplicabilidade prática dos resultados para entender os impactos das pegadas digitais na privacidade e segurança dos usuários.

4 RESULTADOS E DISCUSSÃO

Diante do exposto pelo estudo, torna-se evidente que a Internet se consolidou como uma extensão da vida real, transformando-se em um órgão vital para a vivência em sociedade. Sabendo disso, o sociólogo brasileiro Bernardo Sorj (2013) pontua que a Internet se faz presente nas relações pessoais, familiares, na educação, na cultura, na economia e na política, possibilitando a comunicação, a transmissão de imagens e informação em tempo real e, assim, eliminando a barreira do espaço e colocando à disposição dos usuários o acervo de, praticamente, todo o conhecimento humano.

A revolução tecnológica da conectividade já é uma realidade. Nesse sentido, nadar contra a corrente é uma tratativa errônea, principalmente no que tange à contenção da evolução da tecnologia e as mudanças que ela causa no cotidiano. Logo, a probabilidade de que os indivíduos deixem de comprar on-line, usar redes sociais, consumir conteúdo ou demonstrar seus interesses é praticamente inexistente, dado que essas atividades se tornaram parte do dia a dia de milhões de pessoas. Sendo assim, é necessário reconhecer que o ambiente digital é uma extensão do ambiente físico e não regular esse ambiente pode ter repercussões sob a esfera pessoal do usuário, tanto nos direitos pessoais quanto nos coletivos (Zingales, 2023).

Portanto, as pegadas digitais são uma consequência que precisa ser compreendida e disseminada, pois, mesmo que medidas regulatórias sejam tomadas, elas são implicações que estarão ativamente presentes e, dessa forma, terão seu impacto no dia a dia, no consumo, nos algoritmos das redes sociais e em todos os aspectos na vida digital e cotidiana. Diante disso, surge a necessidade da educação e da conscientização digital, pois, dessa forma, ambas desempenharão um papel crítico na promoção da segurança e da privacidade, uma vez que, quando combinadas, capacitam os indivíduos a navegarem na Internet de forma segura.

5 CONSIDERAÇÕES FINAIS

Constata-se que as pegadas digitais trazem implicações éticas significativas relacionadas à privacidade, ao consentimento e ao uso responsável dos dados, uma vez que a coleta e o uso de informações pessoais, muitas vezes sem o devido consentimento ou entendimento dos usuários, geram um dilema ético entre a proteção da privacidade e a utilização desses dados para fins comerciais ou estratégicos.

Nesse sentido, a discussão sobre o impacto das pegadas digitais não visa afastar os indivíduos do mundo digital, mas analisar como potencializar os benefícios e amenizar os malefícios da conectividade no ambiente on-line. Trata-se de compreender os riscos associados à exposição de dados e buscar alternativas para equilibrar inovação tecnológica e proteção de direitos. Além disso, incentivar uma convivência digital mais segura.

Sendo assim, por meio da revisão bibliográfica, foi possível investigar como a literatura aborda a questão das pegadas digitais, assim como o uso do *Big Data* nesse contexto e, principalmente, o impacto do uso indevido de dados pessoais na vida íntima dos indivíduos. O estudo também abordou a necessidade de regulamentações, como a LGPD, e apresentou recomendações práticas para aumentar a segurança digital.

Acredita-se que, para enfrentar esses desafios, é fundamental que os usuários sejam orientados sobre práticas de privacidade, e que as empresas adotem políticas claras, limitem a coleta de dados e desenvolvam serviços com um foco ético. Portanto, há a necessidade de estimular um ambiente consciente, tanto por parte dos usuários quanto por parte das organizações, compreendendo a influência de suas ações no mundo virtual.

Por fim, o acesso ao conhecimento sobre pegadas digitais e seus impactos é crucial para educar os usuários quanto aos riscos e cuidados necessários na interação com o mundo digital. A disseminação de informações e a promoção da conscientização permitem capacitar os indivíduos para adotar comportamentos mais prudentes e informados, contribuindo para a construção de um ambiente virtual mais seguro e colaborativo.

REFERÊNCIAS

ARAKERIMATH, A. R.; GUPTA, P. K. **Digital Footprint: Pros, Cons, and Future**. International Journal of Latest Technology in Engineering, Management & Applied Science, v. 4, p. 52-56, out. 2015.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 28 abr. 2024.

CARVALHO, W. W. S.; TAGLIAFERRO, E. **A influência dos vazamentos de dados pessoais para a construção da legislação atual**. Revista Intraciência, v. 20, dez. 2020.

CERT.BR. **Cartilha de Segurança para Internet**. São Paulo: Comitê Gestor da Internet no Brasil, 2012.

CONEGLIAN, C. S.; SEGUNDO, J. E. S.; SANT'ANA, R. C. G. **Big Data: fatores potencialmente discriminatórios em análise de dados**. Em Questão, v. 23, n. 1, p. 62, 22 dez. 2017.

DW BRASIL. **A era das redes sociais está acabando?** 2023. Participação de: Nicolo Zingales. Disponível em: <https://www.youtube.com/watch?v=HtJNioMltpk>. Acesso em: 17 mai. 2024.

GALDINO, N. **Big Data: Ferramentas e Aplicabilidade**. Associação Educacional Dom Bosco, 31 out.-01 nov. 2016.

GIRARDIN, F; BLAT, J; CALABRESE, F; DAL FIORE, F; RATTI, C. **Digital Footprinting: Uncovering Tourists with User-Generated Content**. DSpace@MIT, 1 out. 2008.

HUMBY, Clive. **Data is the new oil**. Proc. ANA Sr. Marketer's Summit. Evanston, IL, USA, 2006.

INSTITUTO CPFL. **Como a internet está mudando nossas vidas?** 2013. Participação de: Bernardo Sorj. Disponível em: <https://institutocpfl.org.br/play/series/como-a-internet-esta-mudando-nossas-vidas/>. Acesso em: 16 ago. 2024.

MANYIKA, J; CHUI, M; BROWN, B; BUGHIN, J; DOBBS, R; ROXBURGH, C; BYERS, A. H. **Big data: The next frontier for innovation, competition, and productivity**. Disponível em: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation>. Acesso em: 12 de ago. 2024.

MARQUES, L. P. L. N. C. A. **Análise da Regulação do Uso da Ferramenta de Cookies no Brasil e na União Europeia**. Biblioteca Digital da Produção Intelectual Discente da Universidade de Brasília, 2019.

NIC.BR. **Na Mídia - 3 em cada 4 brasileiros acessam a Internet todos os dias ou quase diariamente**. Disponível em: <https://www.nic.br/noticia/na-midia/3-em-cada-4-brasileiros-acessam-a-internet-todos-os-dias-ou-quase-diariamente/>. Acesso em: 25 nov. 2024.

OLIVEIRA, M. M. **Como fazer pesquisa qualitativa**. Petrópolis: Vozes, 2007.

ONU NEWS. **Crescimento da internet desacelera e 2,7 bilhões ficam fora da rede**. 2022. Disponível em: <https://news.un.org/pt/story/2022/09/1801381>. Acesso em: 25 fev. 2024.

RODRIGUEZ, M. V. R. **Gestão do Conhecimento: reinventando a empresa para uma sociedade baseada em valores intangíveis**. Rio de Janeiro: IBPI Press. 2001.

SUCH, G. M; PEREIRA, G. H. B; SILVA, K. A. A. **Segurança e Privacidade na Internet**. Revista das Faculdades Santa Cruz, v. 11, n. 1, 1 jan. 2020.

TANENBAUM, A. S. **Redes de Computadores**. São Paulo: Editora Campus, 2003.

TAURION, C. **Big Data**. Rio de Janeiro: Brasport, 2013.

WEAVER, S. D.; GAHEGAN, M. **Constructing, Visualizing, and Analyzing a Digital Footprint**. Geographical Review, v. 97, n. 3, p. 324–350, 2007.

WEBER, R. H. **Internet of Things - New security and privacy challenges**. Computer Law & Security Review, v. 26, n. 1, p. 23-30, 2010.

WESTIN, A. F. **Privacy and Freedom**. New York: Atheneum, 1967.

WHITMAN, M. E; MATTORD, H. J. **Principles of Information Security**. Massachusetts: Cengage Learning, 2017.