UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ADMINISTRAÇÃO
DEPARTAMENTO DE CIÊNCIAS ADMINISTRATIVAS

BERNARDO FRANZOI

Privacidade Digital: uma abordagem sobre sua progressão, violação e preservação no contexto do Brasil

Porto Alegre
2022

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ADMINISTRAÇÃO
DEPARTAMENTO DE CIÊNCIAS ADMINISTRATIVAS

BERNARDO FRANZOI

Privacidade Digital: uma abordagem sobre sua progressão, violação e preservação no contexto do Brasil

Trabalho de conclusão de curso de graduação apresentado ao Departamento de Ciências Administrativas da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do grau de Bacharel em Administração.

Orientadora: Dra. Daniela Brauner

Porto Alegre
2022

Agradecimentos

Agradeço primeiramente a Deus, pelas graças que me proporcionou diante das dificuldades, superações e conquistas em toda minha vida: *Tuus totus ego sum, et omnia mea tua sunt*.

Aos meus pais pelo apoio em diversos aspectos que sempre me foi dado, principalmente de cunho material. Sempre estiveram presentes em todos os momentos, desde início dos meus estudos, por mais que tenham ficado distantes em grande parte do meu período acadêmico, recepcionaram-me com amor e me proporcionaram conforto.

À professora Daniela Brauner, por me orientar na realização deste trabalho, sendo precisa nas orientações que me foram necessárias para bem realizá-lo. Certamente não teria conseguido desenvolvê-lo sem esse imprescindível direcionamento.

À Lourdes Odete dos Santos que me auxiliou na metodologia e análise de dados.

Aos professores que tive no decorrer da minha formação, não somente aqueles com os quais tive contato direto, mas também aqueles que delegaram seus ensinamentos e sabedoria em seus livros.

Aos meus colegas de trabalho que me proporcionaram muito conhecimento de análise e manipulação de dados.

A quem dedicou parcela do seu tempo para responder ao questionário deste trabalho, compreendo que não era um questionário breve, portanto, a permanência de cada um até o final tornou possível a análise de dados.

Resumo

Com a disseminação da tecnologia, verifica-se um desenvolvimento social e jurídico da privacidade digital, evidenciando a mudança entre o cenário físico e o digital. A sociedade se digitalizou em um ritmo exponencial, apresentando um ambiente propício para coletores de dados, que adequaram seus modelos de negócios para usufruir desses dados. Em razão disto, é importante entender algumas medidas que estes coletores tomam e que violam diretamente a privacidade dos clientes de seus serviços. Muitos meios de coletas de dados são desconhecidos pelos usuários, principalmente os relativos à tecnologia internet das coisas (IoT), de modo que diversos dispositivos se tornam potenciais violadores de privacidade.Diante disso, este trabalho aborda variadas formas de coleta de dados, tentando apresentar alguns pontos que desafiam a manutenção da privacidade dos usuários digitais. O objetivo deste trabalho é analisar, sob o ponto de vista de usuários de serviços digitais, se suas preocupações quanto a preservação da privacidade digital condizem com seus conhecimentos e ações práticas no mundo digital. Para isso, este trabalho analisa a percepção de um conjunto de 116 pessoas a respeito da preservação e violação da privacidade digital, a partir de perspectivas como usuários de serviços digitais. Com ênfase nas práticas comumente adotadas pelos usuários digitais respondentes desta pesquisa, conclui-se que a maioria dos questionados se preocupa em alto grau com a privacidade digital, no entanto, estes demonstram ser pouco proativos para a preservarem, pois suas próprias escolhas no ambiente virtual acabam fragilizando sua privacidade.

Palavras-chave: Direito à Intimidade, Diretrizes da Privacidade Digital, Violação da Privacidade, Software Livre, Proatividade Digital

Lista de Figuras

Lista de Tabelas

Sumário

1 Introdução

A crescente presença de tecnologias que coletam dados digitais resulta em questionamentos quanto à privacidade dos usuários. Tais questionamentos necessitam de respostas, que dificilmente são concretas. Os precursores desse mundo digital são organizações que tradicionalmente não informavam por completo aos seus clientes como são tratados os seus dados, a não ser por termos de uso do serviço que, mais recentemente e por lei, devem apresentar brevemente algumas informações sobre o uso dos dados pessoais. No entanto, a maioria dos códigos fontes destes serviços, sistemas ou aplicativos são fechados, não modificáveis e não transmissíveis; em outras palavras, não são livres (GNU, 2022a), de modo que os usuários e a comunidade digital possam averiguar e auditar o que de fato é feito com o dado, identificando possíveis invasões de privacidade e corrigi-las se necessário.

Em acréscimo, redes sociais detêm substancial informação a respeito de seus usuários, de modo a tornar viável a criação de personalidades adstritas a cada um deles (MARKOVIKJ et al., 2013). Diante disso, nota-se a capacidade que as tecnologias modernas possuem para identificar pessoas na vida real, uma vez que proporcionam conclusões que somente seriam possíveis ao conhecer o usuário pessoalmente. Nesse contexto, não se trata meramente de uma ou outra organização com essa capacidade, ou um ou outro software, mas sim de um conjunto de organizações que atuam com um fim convergente de coleta de informações pessoais.

Trata-se de circunstância relativamente nova, tanto para os negócios, quanto para os consumidores. Do lado das organizações que satisfazem necessidades subjetivas, há o objetivo de incrementar as informações a respeito do mercado e de seus clientes; para isso, o uso de dados, inclusive de pessoais, torna-se relevante. Nem sempre, porém, como é demonstrado, os meios pelos quais se obtém tais dados são adequados à necessidade de privacidade do usuário digital. Muitos usuários digitais desaprovam práticas como a publicidade sob medida (TUROW et al., 2009), o que possivelmente implica que a criação de “personalidades virtuais”, ferramentas que viabilizam tal publicidade, é também mal vista.

É relevante permanecer em atualização, haja vista as mudanças constantes que ocorrem no meio digital. Temas como Internet das Coisas (IOT), indústria 4.0, outras tecnologias disruptivas, como Virtual Reality (VR) e até mesmo medidas governamentais recentes, como o Serviço de Identificação do Cidadão (BRASIL, 2021) impactam diretamente a privacidade digital da população.

Diante disso, este trabalho aborda variadas formas de coleta de dados, tentando apresentar alguns pontos que desafiam a manutenção da privacidade dos usuários digitais. O objetivo deste trabalho é analisar, sob o ponto de vista de usuários de serviços digitais, se suas preocupações quanto a preservação da privacidade digital

condizem com seus conhecimentos e ações práticas no mundo digital. Além disso, este trabalho visa explorar o desenvolvimento do tratamento do tema da privacidade, as violações que a afetam no ambiente digital, a relevância deste tópico para a administração de empresas, e os princípios que orientam desenvolvedores e usuários para maior privacidade e segurança digital. Por fim, para compreender a que extensão os usuários digitais do Brasil valorizam sua privacidade digital, um questionário é abordado, bem como os dados obtidos serão objeto de análises exploratórias.

2 Objetivo

O objetivo deste trabalho é analisar, sob o ponto de vista de usuários de serviços digitais, se suas preocupações quanto a preservação da privacidade digital condizem com seus conhecimentos e ações práticas no mundo digital.

Dentre os objetivos especificos, estão: – Analisar a problemática da violação da privacidade de dados digitais; – Compreender como algumas tecnologias digitais, oferecidas aos usuários por meio de softwares, aplicativos ou serviços Web, abordam as questões de privacidade digital, identificando práticas que possam auxiliar ou comprometer a privacidade; – Analisar mecanismos que atuem como orientadores das práticas de desenvolvimento de software que contribuem para preservação da privacidade; – Comparar se mecanismos orientadores de desenvolvimento de software são refletidos no uso prático que os usuários fazem das ferramentas.

Para analisar a problemática da violação da privacidade de dados digitais, é necessário apresentar algumas tecnologias inovadoras de coleta de dados que proporcionam uma cobertura substancial da vida digital e real dos indivíduos. A explicação dessas tecnologias demonstra que o fluxo de dados pessoais em diversos dispositivos é frequentemente violado, de modo a expor informações pessoais de seus usuários. Muitas dessas tecnologias são inerentes aos aparelhos, o que dificulta a prevenção dessas violações.

Essas violações da privacidade digital não se limitam a alguns agentes maliciosos. É visto neste trabalho que tanto organizações privadas, quanto organizações públicas são responsáveis por estruturas extensas de vigilância e coleta de informações pessoais. Diante disso, um dos focos do presente escrito é averiguar a progressão futura de tais violações, ainda mais com a constante implementação de sistemas digitais, patrocinados pelos governos, com o fim de controlar com maior intensidade as ações, pensamentos e tendências de sua população.

Espera-se verificar se as políticas, regulações e outras medidas tiveram efetividade diante do dinamismo e desprendimento regulatório do meio digital. Muitas leis de proteção de dados têm surgido em tempos recentes; essa tendência, porém, deve ser verificada com cautela, haja vista que é da natureza da internet a existência de descentralização e mecanismos que evitam o controle aplicável a contingências físicas, comumente existente no cotidiano estatal. Nessa conjuntura, deve-se considerar se o fim abordado pela lei, o de proteger os dados pessoais, pode ser alcançado pela via regulatória.

Em seguida, para contrapor coleta extensa de dados, convém a abordagem de tecnologias e práticas de privacidade de dados. Nesse tópico, serão analisadas práticas que facilitam o conhecimento do público concernente a dados coletados a seu respeito, como priorizar um Softwares Livres, ou que possuam código aberto. Além disso,

tecnologias alternativas às comumente usadas serão analisadas, como sistemas operacionais, navegadores, aplicativos de mensagem, redes sociais e outras ferramentas que auxiliam na manutenção da privacidade online.

Por fim, após a consideração teórica do trabalho, deve-se inquirir o público digital brasileiro a respeito de sua preocupação com a privacidade digital. Para isso, convém a utilização de questionários a respeito do uso de tecnologias mais seguras no que tange à privacidade digital. Perguntas relativas ao sistema operacional do celular e computador, navegador e aplicativo de mensagem utilizados; essas e outras questões serão orientadas para atingir o fim de verificar a familiaridade dos usuários digitais brasileiros com tecnologias adotáveis para evitar a extensiva coleta de dados pessoais.

Como objetivos específicos, a presente escrita visa à explorar as violações de privacidade, realizadas por organizações privadas e públicas, avaliar a efetividade regulatória das leis de proteção de dados, apresentar alternativas às ferramentas tipicamente utilizadas no cotidiano e compreender se o público brasileiro valoriza sua privacidade, conhece os softwares alternativos e os utiliza cotidianamente, mediante um questionário.

3 Revisão da Literatura

3.1 Cenário Atual da Privacidade Digital e da Coleta de Dados

3.1.1 Sobre a Privacidade

Muitas organizações emergentes na era pós-internet convergem para um ponto em comum: o uso de dados para a tomada de decisão. Isso ocorre porque todos os aspectos dos negócios estão abertos para a coleta de informações (FAWCETT; PROVOST, 2016). Não somente os aspectos dos negócios, mas cada vez mais, os aspectos pessoais dos consumidores estão disponíveis para comercialização digital.

Na contingência de digitalização atual, em que a vida pessoal e privada dos indivíduos passam a ser memorizadas em bancos de dados na internet, cada vez mais as organizações procuram obter vantagem competitiva por vias do uso de dados. Isso é um fenômeno relativamente recente, porém, já havia, de fato, preocupação quanto à coleta de dados pessoais crescente, pelo menos desde os anos 1960s, no que tange a massivos banco de dados governamentais (NISSENBAUM, 2010).

Isso, inevitavelmente, afeta o que se denomina como privacidade. Trata-se de um termo em discussão e, de fato, eivado de ambiguidades e inconsistências, no entanto, é possível estabelecer relação direta entre esse termo e o uso de informações pessoais, aquelas que são sensíveis ou concernem à intimidade do sujeito (NISSENBAUM, 2010, p. 5). As definições variaram conforme a época, mesmo porque em tempos remotos a sociedade estava organizada diferentemente. Para ressaltar tal afirmação, autores do século XIX descreviam o termo da seguinte forma: privacidade é "a proteção do espaço pessoal de alguém e do seu direito de ser deixado sozinho"(WARREN; BRANDEIS, 1890). Fica claro a partir dessa definição que a privacidade estava adstrita ao ambiente físico do sujeito, isto é, seu espaço privado, como seu quarto, suas propriedades e mesmo o local onde este sujeito se encontra de imediato. Não obstante essa constatação, o título do artigo, "O direito à Privacidade", já demonstrava uma tentativa de construção legal desse termo.

Essa definição, naturalmente, estava condizente à época dos autores. No século XIX, com o mundo muito menos interligado, as pessoas possuíam privacidade, na medida em que se encontravam sozinhas, ou fossem deixadas sozinhas; ora, os meios de locomoção eram diminutos, e a maioria das pessoas se encontrava circunscrita e limitada a certas localidades regionais, para ilustrar, os primeiros trilhos de trem foram construídos em 1844, na Suíça (4 JEAN-NICOLAS, 2016). Donde, tal definição era perfeitamente cabível para ilustrar a vida do cidadão mediano no século XIX.

Consoante as mudanças sociais, principalmente após o período da Segunda Guerra mundial (1945-), a definição desse termo também foi atualizada. Tendo em

vista que novas tecnologias informacionais surgiram e se disseminaram gradativamente, a definição de tal termo modificou o enfoque loco-regional para informacional: privacidade é "o controle e garantia de informações pessoais"(WESTIN, 2003). Nota-se que a privacidade passa a ser considerada do ponto de vista do que se conhece de determinado sujeito, não meramente do espaço a que ele está circunscrito, ou de suas ambições subjetivas de ser deixado a sós. Nesse contexto, há certa evolução em desvincular o termo a um ambiente físico, visto que há maior abrangência de violação da privacidade individual.

Por fim, com maior consolidação do significado apropriado de privacidade para os tempos modernos, passou-se a considerá-la diferentemente. Schoeman (1992) afirma que privacidade é "um aspecto da dignidade, autonomia, e uma liberdade humana". Diante dessa definição, o aspecto regulatório e, em certo grau demagógico, da privacidade emerge com maior ênfase. Para resguardar essa "liberdade humana"alguém deve protegê-la; assim, a evolução regulatória sobre a privacidade de cada indivíduo passou de um tema meramente doutrinário para um objeto de regulação. Isso foi potencializado com o incremento do uso de dados, bem como da facilitação de seu armazenamento, com tecnologias como cloud storage, que viabilizou a comercialização e distribuição segura de espaços de depósitos digitais.

3.1.2 Privacidade como um Direito

Entendimentos recentes, a partir de eventos regulatórios como a Lei Geral de Proteção de Dados (LGPD), já consideram a privacidade digital como um direito a ser resguardado pelas entidades estatais (REIS; OLIVEIRA NAVES, 2020). Apesar de ser possível estabelecer discussão quanto à natureza de direito da privacidade, tal seara não convém ao presente trabalho, que investiga as ferramentas e artifícios utilizados para garantir a privacidade online, no sentido de resguardar os dados pessoais e íntimos dos usuários, assim como sua violação.

Para adentrar no aspecto regulatório da privacidade, é imprescindível tratar de algumas leis no cenário nacional e internacional. De início, a regulação do tema já era existente em alguns dispositivos legais: primeiramente, o direito à privacidade se encontra presente na Carta Magna brasileira, não há explicitamente referência à privacidade, porém, refere-se indiretamente a ela no artigo 5º, inciso X, que preserva a intimidade e a vida privada, assim como o inciso LXXIX que resguarda a proteção de dados digitais (BRASIL, 1988). Em sentido diverso, em regulação mais recente, não se dispõe algo a respeito no Código Civil (BRASIL, 2002). A esse tema se deu mais ênfase em leis esparsas posteriores, como o Marco Civil da internet e a LGPD.

Tendo em vista que a expansão da internet e o uso de dados é um fenômeno global, o cenário internacional assumiu a dianteira na implementação regulatória da

privacidade. Em 2016, foi implementada a GDPR (*General Data Protection Regulation*), como instrumento para proteger os dados e a privacidade na União Europeia. Dispõe em seu primeiro artigo que visa a proteger as liberdades e direitos fundamentais de pessoas naturais e em particular seu direito à proteção de dados pessoais (EUROPEIA, 2016). O Marco Civil abordava a privacidade como um princípio a ser seguido, já a GDPR afirma que a proteção de dados pessoais é um direito. Lei homóloga foi instituída no âmbito brasileiro ao final de 2018, a LGPD (Lei Geral de Proteção de Dados), que copia até mesmo o nome da lei europeia, afirma em seu artigo inicial que possui o "objetivo de proteger os direitos fundamentais de liberdade e de privacidade"(BRASIL, 2018b).

Por conseguinte, a natureza da privacidade culminou gradativamente para um direito. Tal direito é resguardado pela Autoridade Nacional de Proteção de Dados (ANPD), predisposta no artigo 55-A, da LGPD (BRASIL, 2018b). Para fins terminológicos, a definição adotada neste trabalho dispõe que a privacidade é a capacidade de indivíduos ou grupos de isolar ou expressar eles mesmos, ou suas informações seletivamente, especialmente para indivíduos (SUN et al., 2020). É importante ressaltar, porém, que a mera instituição legal da privacidade como um direito não implica em ela se tornar uma prioridade estatal. Ainda mais em razão de a privacidade não ser um absoluto: por exemplo, uma pessoa que assassina outra, sendo o evento detectado por câmeras de vigilância, teria que ter sua privacidade resguardada? Essa pessoa teria direito à imagem produzida dela? São questões de cunho jurídico, fora do âmbito do presente trabalho, mas que demonstram a complexidade de se atribuir tal natureza jurídica à privacidade. Desse modo, a privacidade se tornou um direito no ordenamento jurídico brasileiro, diante disso, a violação deste direito clama por alguma sanção. De maneira geral, porém, essas sanções estão ou incipientes, ou de momento impraticáveis no âmbito do Brasil. Essa violação se dá na medida em que se coletam e distribuem dados de usuários digitais, em especial os de cunho sensível, bem como aqueles coletados sem o consenso do usuário.

3.1.3 Sobre a Coleta de Dados

Inicialmente, convém delimitar o escopo do presente trabalho, de modo a explicar o que se entende por dados, em especial dados pessoais. Dados são informações, sendo assim, extremamente abrangentes na vida de cada indivíduo; não é qualquer informação que é considerada um dado pessoal, mas este é interpretado de forma bem expansiva em termos legais (KUNER, 2003). Esse termo inclui todo dado a respeito de uma pessoa: econômico, profissional, jurídico e assim por diante, não somente o que concerne apenas à vida pessoal (KUNER, 2003, p. 52). A coleta de dados por parte de organizações públicas e privadas frequentemente envolve dados

pessoais, uma vez que a finalidade dessas coletas é, em geral, para compreender com maior precisão o comportamento e a pessoa detentora daquelas informações difusas, tomando certas decisões, como quais anúncios apresentar a ela, se esta pessoa representa um risco à sociedade e até mesmo como persuadi-la a mudar de opinião, como é visto adiante.

A finalidade da coleta de dados varia conforme o agente coletor. Para empresas, os dados pessoais digitais são relevantes para descobrir potenciais novos clientes, estabelecendo um público-alvo de publicidade e propaganda; o rastreamento dos usuários digitais por meio de um endereço de IP, ou outro identificador, possibilita que esses dados sejam atrelados a alguma identidade real, diante disso, a publicidade online permitiu que essas organizações rastreassem os usuários eletronicamente e guardassem esses dados, quase sem custo (GOLDFARB; TUCKER, 2011, p. 27). Nesse contexto, nota-se a substancial capacidade informacional que essas empresas possuem à disposição.

Os governos, como coletores de dados pessoais, também possuem seus próprios interesses. A ANATEL, agência regulatória brasileira de comunicações, planejava construir uma infraestrutura técnica e propor regulação para permitir se conectar diretamente nas companhias de telecomunicações e obter informação relacionada ao uso de serviços pelos consumidores (números discados, tempo, data, quantidade paga e duração das chamadas): a justificativa era de saber se os usuários estavam recebendo os serviços no nível regulatório apropriado (RUBINSTEIN; NOJEIM; LEE, 2014). Na Alemanha, informações como nome, endereço e número de telefone são transferidas à Federal Network Agency, uma agência regulatória (RUBINSTEIN; NOJEIM; LEE, 2014). Por fim, o acesso pode ser mais invasivo, como ocorre no governo da China, que mantém quase ilimitado e irrestrito acesso aos dados do setor privado: isso faz parte da estratégia de governo digital (*e-government*) que essa entidade está a implantar (RUBINSTEIN; NOJEIM; LEE, 2014). Essa última invasão não é adstrita somente ao governo chinês, trata-se de um fenômeno global que mesmo o Brasil está adotando, conforme se observa em medidas como Serviço de Identificação do Cidadão (BRASIL, 2021), que regulamenta e digitalização e centralização dos dados de identidade de brasileiros.

No que tange à atuação online dos consumidores, em pesquisa datada de 2009, é possível compreender que o público norte americano, em sua maioria, posicionava-se de maneira contrária à publicidade sob medida (*taillored advertising*) , naquela época (TUROW et al., 2009). Ao mesmo tempo em que essa publicidade é orientada para as necessidades do consumidor, um anúncio com alto grau de precisão pode revelar que quem o enviou utilizou informação sobre o consumidor (PÅHLMAN; WALDENSKIÖLD, 2013). Mesmo quando informados de que o rastreamento em websites seria anônimo, ainda assim, 68% responderam que definitivamente não permitiriam esse tracking.

Somado a isso, 90% dos jovens adultos, que responderam à pesquisa, afirmaram que rejeitariam tal medida se esta fosse oriunda de rastrear o que eles fazem offline. Por conseguinte, há indícios de que o público digital, em geral, desgosta de medidas online invasivas de sua intimidade (TUROW et al., 2009, p. 3).

Grandes empresas de tecnologia, entre as mais significantes, Google, Amazon, Microsoft, Meta e Apple são as que detém a maior capacidade de violar a privacidade de seus usuários, através de extensa coleta de dados. Isso ocorre por algumas razões, como o fato de elas terem sido pioneiras em seus serviços, possuírem tecnologia avançada e, principalmente, uma grande base de usuários. Tecnologias como análise de Big Data viabilizaram uma expansão na compreensão que essas organizações possuem a respeito de quem utiliza seus serviços. Notavelmente, a equipe do Youtube da Google possui capacidade de processar grandes quantidades de dados, na ordem de trilhões de linhas por segundo e petabytes de dados (BECKER, 2016) Em recente pesquisa realizada com 236 empresas de tecnologia da Malásia, a respeito da adoção da indústria 4.0 (HIZAM-HANAFIAH; SOOMRO, 2021), constatou-se que aproximadamente 72% das empresas utilizam em alto grau Big Data. Apesar de as empresas investirem principalmente nessa tecnologia para fins de melhorar a performance da organização, resultados indicam que a velocidade e variedade de dados possui papel vital nesse fim, enquanto que o volume em si não (GHASEMAGHAEI; CALIC, 2020). Convém, porém, ressaltar que o uso dessa tecnologia está presente em alto grau em empresas de tecnologias, como as supracitadas, haja vista que elas predispõem de quantidade significativa de dados sobre seus usuários, bem como de capacidade para processá-los.

Ocorre que com o desenvolvimento paulatino da internet e o aumento exponencial de usuários, a aglutinação de informações modificou. No início da internet, não havia propriamente um mecanismo de pesquisa capaz de procurar informações pulverizadas na rede, razão pela qual os usuários vinculavam-se a sites conhecidos, que se interligavam, formando uma verdadeira rede entre eles. Para atender a essa demanda, surgiram mecanismos de pesquisa, softwares de rede ou scripts baseados em rede que procuram palavras-chave em documentos e arquivos, retornando uma lista de resultados contendo aquelas palavras-chave procuradas (JAIN, 2013). O trabalho de um mecanismo de pesquisa é dividido em duas partes, a primeira é o rastejamento e a segunda é a indexação; na primeira fase, o rastejador, ou aranha, visita as páginas que vão ser incluídas na pesquisa, tomando os seus conteúdos. Após esse processo, o indexador processa esses dados, filtrando-os de modo a correlacionar à pesquisa, em seguida, esses dados processados são movidos para outros computadores, arquivos ou partes de memória (JAIN, 2013).

Esse processo, aparentemente complexo, resulta em milhões de resultados que podem ser filtrados de acordo com o texto inserido no mecanismo de pesquisa, a

query. O simples fato de ser viável o acesso de tamanha quantidade de informação é uma mudança substancial na transmissão e armazenamento de dados. No entanto, a privacidade dos usuários não necessariamente está resguardada com esse tipo de tecnologia, principalmente ao utilizar o mecanismo de pesquisa da Google. Essa organização classifica cada pessoa em grupos, baseada no que aprende de cada indivíduo: a tecnologia utilizada para esse fim variou com o tempo, recentemente se adotou o Aprendizado Federado de cohorts (FLoC); sendo cohorts grupos de pessoas semelhantes, federado implica fontes múltiplas e o aprendizado implica em uma inteligência artificial ativa formulando os perfis. Em março de 2021 a Google iniciou os teste com essa tecnologia em seu navegador Google Chrome, a partir do Chrome 89, substituindo cookies de terceiros. Após certa resistência por parte de outros concorrentes, bem como em relação ao compliance à GDPR, em janeiro de 2022, essa organização anunciou que havia terminado de desenvolver tal tecnologia, propondo o novo API de tópicos para substituí-la (KARLIN, 2022) (ROTH, 2022).

O FloC adicionava demasiados dados de impressão digital. Esse termo termo é utilizado para denominar dados que, apesar de não estarem diretamente relacionado à identidade digital do sujeito, como o endereço de IP e cookies , proporcionam informações consideráveis de quem está navegando, quais sejam: marca do computador e modelo, versão do sistema operacional, versão do navegador, extensões do navegador, fuso horário, configurações de linguagem, bloqueador de anúncios utilizado, tamanho da tela e resolução e especificações de hardware, como processador, placa de vídeo e disco rígido, em síntese, tratam-se de metadados (BACA, 2016). Donde, é possível rastrear os usuários digitais, não obstante o endereço de IP e cookies estarem desativados, pois cada um tende a ter um somatório de dados de impressão digital que o identifica digitalmente.

Desse modo, o mecanismo de pesquisa frequentemente utilizado pelos usuários digitais é, de fato, um instrumento de construção de perfil. Trata-se de um dos principais meios de coleta de dados no contexto de internet atual, haja vista o constante e prolongado uso. Outras vias de obtenção de dados são sistema operacional, navegador, aplicativos de mensagem, redes sociais, e-mail, *smartphones*, ondas de rádio identificação, BLE (*Bluetooth Low Energy*) (YANG et al., 2020) e outros softwares e hardwares comumente utilizados. O que viabiliza muitas vezes essa coleta é justamente a característica de software proprietário das organizações que desenvolvem determinado serviço, de modo que não se sabe propriamente os dados coletados, sua precisão e a extensão dessa coleta.

O que é notável, porém, diante de mudanças tecnológicas recentes, é a expansão da coleta de dados de modo a necessitar cada vez menos da participação ativa do usuário. Isto ocorre porque tecnologias como IoT formam entre si redes *mesh* (SICHITIU, 2005), capazes de transmitir dados sem que o usuário propriamente or-

dene. Esses dispositivos constantemente monitoram e coletam certas informações, de modo a gerarem dados de impressão digital, conforme comentado anteriormente. Diante disso, o desenvolvimento tecnológico atual tende a cada vez mais prejudicar e violar a privacidade dos indivíduos, que muitas vezes não compreendem a extensão das informações que um simples dispositivo IoT transmite sobre eles.

3.1.4 A Importância da Privacidade Digital no Contexto da Administração de Empresas

A administração de empresas envolve um conhecimento interno e externo de uma organização (DRAGNIĆ, 2014). O conhecimento interno diz respeito ao conhecimento dos processos, empregados, estrutura, metas, receitas, despesas, lucro e outros dados relevantes. Já o conhecimento gerencial externo corresponde à relação da organização com outros agentes em um mercado, e a influência que estes exercem sobre aquela. Sendo assim, a privacidade digital é cada vez mais relevante não só como requisito regulatório, mas também entre os consumidores digitais. Nesse contexto, é mister que as organizações contemporâneas compreendam a importância de adotarem medidas protetivas da privacidade digital de seus usuários, bem como limitarem os dados coletados e transmitidos.

Boa parte dos usuários digitais não possuem eles mesmos práticas de privacidade digital, condizentes aos seus dados pessoais informados. Isso se dá em razão da falta de conhecimento e da não aplicação de certas técnicas que preservam sua privacidade digital. Na mesma conjuntura, estavam pessoas que não utilizavam equipamentos de segurança no trânsito, no manejo de máquinas pesadas, em locais de construção e assim por diante; estas não possuíam práticas condizentes ao perigo que naturalmente envolvia a atividade exercida. Analogamente, o ambiente digital é em grande parte desconhecido pelos seus usuários, razão pela qual as medidas protetivas adequadas dificilmente são utilizadas, o que permite a coleta extensiva de dados pessoais e a consequente violação da privacidade. Fabricantes de carros começaram a alertar o motorista que não utilizava cinto de segurança, o que auxiliou na implementação dessa prática. Da mesma forma, as organizações devem visar à preservação da privacidade digital de seus usuários, certificando-se de que somente a informação necessária é coletada; isso força tanto os indivíduos, quanto organizações a perceberem que os dados devem ser protegidos, e que quanto menos são coletados, menor a chance de eles serem vazados (ADAMS, 2017, p. 17).

Os administradores devem se atentar para a esfera regulatória da privacidade digital. Em certos países já há litígios a respeito de violações da privacidade digital de usuários, através de coleta de dados por meio de softwares. Um exemplo é o uso de dados de saúde para publicidade sob medida; naturalmente, um dado a respeito da

saúde de uma pessoa tende a ser significativamente íntimo, de modo que o seu uso para fins publicitários é questionável. Em recente litígio judicial, os alvos da publicidade recebiam propagandas que promoviam curas e serviços médicos sem prova científica, consoante os dados médicos obtidos do público-alvo. A problemática envolve o fato de os usuários não terem consentido em compartilhar seus dados médicos sensíveis, bem como a existência de proteção legal de informação eletrônica sobre saúde, por parte da HIPAA (TOULAS, 2022). Nesse sentido, é cada vez mais imprescindível que os gestores compreendam a extensão do que podem coletar e transmitir de dados, dada a sua sensibilidade e a necessidade de privacidade do usuário digital.

O processo de uso de dados passa por algumas etapas, quais sejam: propósito, coleta de dados, análise, interpretação e ação (LAI; SCHILDKAMP, 2013, p. 16). A ação da organização é, de maneira geral, a única forma que se tem de compreender o quanto se conhece de determinado indivíduo no contexto digital, isto é, dificilmente uma pessoa vai compreender o quanto de seus dados estão em posse de uma organização, sem que esta os use para fins publicitários ou outros que tornem evidentes sua existência. Nesse contexto, é esperado que as organizações compreendam com afinco a vida pessoal de seus consumidores, no entanto, não revelam sua compreensão em totalidade, uma vez que não explicitam tudo na prática.

Por conseguinte, o uso de dados facilita a tomada de decisão por parte de uma organização, contanto que se compreenda os limites de suas ações após sua interpretação. No caso anterior, que envolve informações concernentes à saúde, o Meta pôs em ação um conhecimento a respeito de seus usários que para eles e para o aparato regulatório deveria ser privado e protegido. Nem sempre as análises preditivas, prescritivas, descritivas e diagnósticas (SARKER, 2021, p. 7) devem ser postas em prática, principalmente quando os dados envolvem a privacidade e limitações regulatórias. Ademais, práticas de dados são importantes para todas as organizações, mesmo aquelas que não tiveram algum comprometimento em seus dados podem sofrer detrimentos financeiros substanciais quando um concorrente próximo tem um vazamento de dados (MARTIN; BORAH; PALMATIER, 2017, p. 34) se as organizações almejam revelar suas práticas de dados aos consumidores (o que de fato é uma política de privacidade de dados relevante), elas também precisam provê-los com algum elemento de controle sobre a informação (MARTIN; BORAH; PALMATIER, 2017, p. 35).

Além disso, ressalta-se que a privacidade digital tem tido maior relevância entre os consumidores. Essa relevância é perceptível ao analisar o crescimento de serviços de VPNs, navegadores privados e hardwares de segurança. Surge, nessa contingência, um mercado de produtos de segurança digital, que pode ser explorado por novas organizações. Trata-se de um mercado de difícil entrada, uma vez que os usuários tendem a considerar, em maior grau, a transparência por parte das organizações e de seus serviços, o que faz com que organizações desvinculadas de grandes empresas

de tecnologia, ou empresas com histórico de vazamento de dados, se sobressaiam, mesmo que iniciem com projetos voluntários, tal qual o LineageOS (LINEAGEOS, 2022).

3.2 Violações da Privacidade Digital

A privacidade digital é violada quando há uma coleta indevida de dados a respeito do usuário, de seus dispositivos, de seus arquivos, em síntese, de suas informações pessoais (GNU, 2022e). Isso ocorre com demasiada frequência, haja vista que a utilização de diversos softwares tem, como pré-requisito, a coleta de dados pessoais. Mesmo softwares mais elementares, como um sistema operacional de um *smartphone* ou *desktop*, em sua maioria, violam a privacidade digital de seus usuários. Essa violação é potencializada pelo que se denomina de software proprietário (*proprietary software*), ou privativo.

3.2.1 Softwares Proprietário e Software Livre

Um software pode ser classificado de diversas formas, a classificação doravante adotada o diferencia, na medida em que ele é livre (FOSS), ou proprietário. Um software livre é um software dotado de 4 liberdades essenciais: a liberdade de executá-lo, estudá-lo, redistribuí-lo e distribuí-lo com modificações (GNU, 2022a). A palavra livre não significa que o software não possa ser comercializável, haja vista que ele pode possuir essas liberdades, ao mesmo tempo em que os seus usuários paguem por seu uso; o que não pode ocorrer, porém, é delimitar as liberdades a um pagamento, uma vez que equivaleria a não concedê-las, tornando-o um programa não livre. Ainda, um software pode possuir seu código aberto, o que viabiliza o seu estudo, porém, pode não ser modificável, nem distribuível, em razão de restrições de sua licença, assim, nem todo software aberto é livre, porém, todo software livre é aberto, há diferenças valorativas entre o software livre e o *open source* (STALLMAN, 2022). Somado a isso, essa modalidade está mais próxima da comunidade e dos usuários, na medida em que a maioria dos sistemas FOSS foram desenvolvidos por programadores voluntários (BOULANGER, 2005). O software livre, por conseguinte, deve ser incentivado como meio para preservar a privacidade digital dos usuários, uma vez que tais violações são ser evitadas, e quando existentes, são com frequência retiradas por outros desenvolvedores, de modo a disponibilizar o software, de acordo com a necessidade natural dos usuários.

Em contrapartida, o software proprietário pode não respeitar a liberdade do usuário, colocando o desenvolvedor ou dono em posição de detendor de informações, perante quem o utiliza (GNU, 2022d). É comum que os desenvolvedores de um software

proprietário sejam pertencentes a um aparato organizacional centralizado, de modo que a participação comunitária no seu desenvolvimento é reduzida ou limitada a certas funcionalidades (BOULANGER, 2005). Atualmente, grande parte dos softwares usados no dia a dia dos indivíduos são proprietários, alguns exemplos são Facebook, Instagram, Snapchat, WhatsApp e outros; um software proprietário pode possuir diversas funcionalidades maliciosas, GNU (2022d) apresenta mais de 550 exemplos dessas funcionalidades, no entanto, cabe ressaltar que neste trabalho somente algumas serão abordadas, tendo em vista que nem todas violam propriamente a privacidade digital. Essas violações podem se dar em variados produtos, desde carros e jogos eletrônicos, até páginas web e as técnicas são das mais variadas, desde censura, fraude e incompatibilidade até manipulação e vigilância. Desse modo, o desrespeito da liberdade do usuário culmina em adições maliciosas no software que por sua vez ocasionam violações na privacidade digital do consumidor do serviço/produto.

3.2.2 Organizações Privadas com histórico de Violação da Privacidade Digital

Notavelmente, a vigilância é uma funcionalidade comum nos softwares proprietários de grandes empresas de tecnologia, como Microsoft e a Apple (GNU, 2022e). Uma cláusula comum dessas organizações, em sua política de privacidade, dispõe que elas compartilham informações agregadas e não pessoalmente identificáveis com terceiros/parceiros. Porém, mesmo em dados anonimizados pode ser possível atribuí-los aos indivíduos, como por exemplo dados que demonstram os locais aonde uma pessoa frequenta, por exemplo, podem ser de fácil atribuição a uma identidade real, especialmente em hábitos poucos tradicionais, que quando agregados a outros dados sócio demográficos podem identificá-la. Afinal, cada um possui uma rotina diferente, um trabalho diferente, uma residência diferente e assim por diante. Desse modo, é importante se atentar ao que é coletado de dados.

O Microsoft Windows é definitivamente um sistema operacional utilizado por substancial parte da população (STATCOUNTER, 2022a). Não obstante essa constatação, há funcionalidades questionáveis quanto à manutenção da privacidade digital dos consumidores deste produto. As configurações padrão do Windows 8 e 10 coletam dados sobre o usuário e seu dispositivo, sendo que parte desses dados são carregados em servidores da Microsoft e de fabricantes do equipamento original; um usuário padrão não sabe como modificá-las, ou nem mesmo pensaria em modificá-las (LOVELESS, 2016). O Windows 10 também possui o modo de telemetria "completo", que é a configuração padrão, permitindo que engenheiros do Windows acessem chaves de registro que podem conter informações confidenciais, como a senha de login do administrador (ARS, 2017) (MICROSOFT, 2010). O uso da assistente denominada "Cortana", permite a coleta dados como localização, entrada de voz, sites visitados, telemetria,

enviando-os aos servidores da Microsoft; somado a isso, houve significativa desconsideração pela escolha do usuário em não atualizar seu sistema operacional, quando do início das atualizações (KALIA, 2016).

A vigilância privativa não está adstrita ao sistema operacional da Microsoft. O MacOS, sistema operacional de desktop da Apple, também possui esta funcionalidade. As versões modernas desse OS enviam à Apple um hash (um identificador único) de todo programa executado. Esse envio é realizado utilizando a internet, o servidor visualiza o IP do usuário e sabe quando a solicitação veio. As informações coletadas nesse processo são a data, o horário, o computador, o ISP, a cidade, o estado e o hash da aplicação (PAUL, 2020). Isso significa que a Apple sabe quando o usuário está em casa, no trabalho, quais aplicativos são abertos, quantas vezes eles são abertos, mesmo se um navegador Tor é aberto (que deveria, em teoria, ser anônimo e privado). Até 2015, (LOPES, 2015, p. 262) essa informação não era criptografada, não estando somente circunscrita à Apple mas também aos intermediários de serviços da Internet.

Em se tratando de organizações privadas, a Apple é uma das que mais se apresenta como protetora da privacidade de seus usuários. Em 2021, com a finalidade de prevenir material de abuso sexual infantil (CSAM) e vitimização de crianças por predadores sexuais, um sistema de detecção desse material foi anunciado pela Apple. Sua operação consiste em escanear a galeria de fotos carregada no iCloud para resultados compatíveis em relação a uma tabela de "valores hash", mantidas pelo NCMEC, centro nacional para crianças perdidas e exploradas, com imagens de abusos de crianças. Um valor hash é uma curta string, derivada por meio do processamento de um arquivo maior através de um algoritmo matemático e rotineiramente utilizado para rapidamente determinar se dois arquivos são idênticos ou não (SANCHEZ, 2021). Após escanear, se houver algum resultado compatível, notifica-se a Apple que é responsável por reportar o usuário para o NCMEC e, consequentemente, às autoridades. O sistema detecta somente fotos do usuário designadas para o backup do iCloud, por escolha da Apple. O sistema é adequado para o fim a que se destina, conforme justificado pela Apple. Cabe, contudo, esclarecer que o funcionamento do algoritmo é *ipso facto* um meio de vigilância pessoal: trata-se de um programa, sendo executado constantemente no dispositivo, com o fim de escanear e encontrar conteúdo proibido e, em encontrando, reportá-lo, juntamente com dados pessoais do usuário (SANCHEZ, 2021).

O Chromebook, desktop de baixo custo da Google, massivamente orientado para fins educacionais, é outro exemplo de coleta de dados. O baixo custo desses dispositivos os torna convenientes para uso educacional, porém, os dados coletados precisam muitas vezes serem trafegados via Internet para armazenamento em nuvem (GEBHART et al., 2017, p. 5). Essa coleta, ao mesmo tempo em que pode favorecer o

desenvolvimento estudantil do aluno, transforma-se em um mecanismo de vigilância, não só por parte do professor, mas também por parte da organização que controla o fluxo de dados (KUMAR et al., 2019) . Tal prática culminou no banimento de Chromebooks em escolas dinamarquesas, em razão de o acordo de processamento de dados aparentemente não permitir a transmissão de dados para outros países, com o intuito de proporcionar suporte (SAWERS, 2022) .

Pode-se perceber, nessa conjuntura, que os sistemas operacionais mais utilizados acabam comprometendo a preservação da privacidade digital, já que possuem mecanismos de vigilância e priorizam a coleta de dados.

3.2.3 Organizações Públicas com histórico de Violação da Privacidade Digital

Não obstante as violações de privacidade provenientes de companhias de tecnologia, os governos também possuem ferramentas de vigilância. A violação da privacidade dos usuários digitais realizada pelos governos era conjecturada, contudo, mediante a exposição de informações concisas a respeito do assunto, por parte de Edward Snowden, essa especulação se tornou em um fato notório. Primeiramente, programas da Agência Nacional de Segurança dos Estados Unidos da América (NSA) têm por fim coletar dados; em razão disso, há atuação conjunta de estados para essa finalidade mútua (BAUMAN et al., 2014, p. 122). A atuação dos estados para o fim de coletar dados de sua população é facilitada quando se detém o controle regulatório das telecomunicações e cabeamento.

O trabalho em si de coleta de dados não é, em geral, realizado diretamente pelos estados. Há empresas de segurança da informação contratadas e financiadas especialmente para essa finalidade, como a Palantir; essa empresa tem como clientes a NSA, FBI e CIA, agências de inteligência estadunidense. A companhia foi criada por Peter Thiel, com o problema em mente de reduzir terrorismo ao mesmo tempo em que preserva liberdades civis (GREENBERG, 2013). Naturalmente, a mesma finalidade louvável, utilizada pela Apple para implementar seu sistema de detecção de imagens ilícitas, foi explicitada pelo fundador dessa organização. A Palantir já atuou e atua em diversos projetos de organizações estatais de vigilância dos EUA, de modo que foi utilizada para conectar a base de dados entre esses departamentos governamentais (BURNS, 2015). Nesse contexto, resta claro a proximidade que essa organização possui com o governo americano, uma vez que possui e possuiu direto acesso aos dados de segurança estatal.

Muitos dos dados aos quais essas entidades estatais têm acesso são provenientes de empresas de tecnologia. As organizações previamente comentadas (Apple, Amazon, Meta e Google), juntamente com a Microsoft, consideradas gigantes da tecnologia, são fonte de dados para a NSA e diversos serviços de inteligência europeus;

a conveniência em usar serviços de armazenamento na nuvem e redes sociais permite, por intermédio de metadados (dados sobre outros dados, como o horário em que uma foto foi retirada, bem como a sua localização), aos serviços de inteligência o mapeamento de relações entre pessoas, seus endereços de IP e seu conteúdo compartilhado, localização e interesses (BAUMAN et al., 2014, p. 123). Donde, nota-se o trabalho em conjunto entre o público e privado no monitoramento dos usuários digitais, resultante da extensa coleta de dados.

3.2.4 Redes Sociais e a Coleta Massiva de Dados

Tratou-se, de início, a respeito de sistemas operacionais que podem violar a privacidade de seus usuários, tendo em vista que são softwares elementares para utilizar a tecnologia. Cabe agora abordar uma perspectiva já constantemente enfatizada (SMITH et al., 2012), segundo a qual as redes sociais são em essência coletoras de dados e potenciais violadoras da privacidade digital de seus usuários.

Desde os primórdios do Facebook, até a atualidade com aplicativos como TikTok, a coleta, venda, transmissão e exploração de dados é uma parte do que gera valor a esses softwares. É justamente por isso que, dificilmente, uma organização vai cobrar para usarem sua rede social, uma vez que os dados obtidos dos usuários, e o influxo que eles geram entre si é mais rentável do que realizar um sistema de assinatura de tais serviços. Nesse sentido, as redes sociais são potenciais violadores de privacidade.

Dentre as redes sociais mais populares, encontra-se o TikTok. Essa rede social consiste na exposição de vídeos curtos, a respeito dos mais variados assuntos. Ocorre, porém, que o seu modelo de negócio é análogo ao de outras redes sociais, ou seja, é de se esperar que esse software colete dados de seus usuários. É típico dessa rede social requisitar constantemente permissões a certos acessos e funcionalidades do *smartphone*, como contatos, calendário e localização, aplicativos instalados, e armazenamento externo. Certos dados, como a localização, são coletados periodicamente, de modo que o usuário tem sua privacidade constantemente violada (MASON, 2022).

Essa prática de redes sociais se agrava quando não há propriamente segurança de que os dados dos usuários serão preservados. O Twitter revelou que havia sofrido um vazamento de seus dados que revelava o endereço de e-mail e o número de telefone dos usuários. Essa falha no código do Twitter persistiu por 6 meses, contudo, a empresa não forneceu a quantidade de usuários afetados (ASHWIN, 2022). A vulnerabilidade, aparentemente, foi explorada por um hacker que, em seguida, anunciou na dark web dados de 5,4 milhões de usuários, incluindo celebridades e grandes empresas (ABRAMS, 2022). Nesse contexto, redes sociais que possuem grande quantidade

de dados a respeito de seus usuários não só podem violar a privacidade, como também podem ocasionar vazamento involuntário dos dados que coletaram.

O Instagram também possui práticas semelhantes, no sentido de coletar múltiplos dados de seus usuários. Em razão de as coordenadas do GPS serem armazenadas em fotos, o Instagram guarda o histórico dessas fotos postadas, de modo a saber a respeito da localização de grande parte de seus usuários, que não retiram metadados de suas fotos (BATES, 2018). Há além disso questionamentos a respeito de espionagem de conversa offline, utilizando-as para publicidade sob medida (DIEZ, 2017).

Somado a essas populares redes sociais, o Snapchat é outro software com fins análogos. Ele constantemente armazena o IP e a localização do usuário, bem como requisita permissão para os contatos, calendário do celular, receber e mandar SMS, arquivos do celular no cartão MicroSD, câmera, microfone, e identificar informações do dispositivo (SNAP, 2022). Caso o usuário recuse conceder muitas permissões, em especial acesso aos arquivos, o aplicativo o bloqueia de utilizá-lo. Uma das principais funcionalidades que violam a privacidade do usuário é o Snap Map, que compartilha em tempo real a localização precisa do usuário. Essa funcionalidade pode ser limitada de modo a não compartilhar a localização com outras contatos, no entanto, cabe ressaltar que ainda assim há coleta de dados a respeito da localização precisa do usuário, não granularizada (DEAHL, 2017).

Por fim, cabe abordar um aplicativo de mensagem denominado Discord. Esse software é viável para dispositivos móveis e desktops; esse programa coleta toda informação que passa por sua plataforma de comunicação, que é centralizada em seu servidor. De maneira geral, todo software que possui um servidor centralizado é capaz de armazenar, processar e transmitir informações de seus usuários, uma vez que elas necessariamente passam por sua posse. Essa organização explicitamente expõe que coleta informações como endereço de IP, UUID do dispositivo, endereço de e-mail do usuário, todas as mensagens, todas as imagens, dados do chat de voz (DISCORD, 2022b). Trata-se de um software que minera dados de seus usuários, o que significa que potencialmente suas informações poderão ser vendidas para companhias de publicidade (DISCORD, 2022a).

O problema fundamental das redes sociais, no que tange à privacidade digital, é que elas exigem dados que não são relevantes ao serviço que proporcionam. Isso ocorre em razão de haver um interesse comercial nessas informações, de modo que quanto maior a coleta de dados, mais precisos se tornam os anúncios sob medida que estas organizações apresentam a seus consumidores.

3.2.5 Profilamento e Mecanismos de Pesquisa

Convém, ademais, tratar do profilamento (*Profilling*) dos usuários digitais. Esse profilamento é perceptível quando se trata das organizações com as quais a Google cultiva relações. Jigsaw é uma organização que almeja uma internet "mais segura para um mundo mais seguro"; seu trabalho está centrado em desinformação, censura, toxicidade, extremismo violento, consoante dispõe seu site (JIGSAW, 2022). Em resumo, o propósito da Jigsaw é utilizar os dados para manipular comportamentos. Essa companhia desenvolve o projeto denominado método de redirecionamento.

No início, esse projeto tinha como fim identificar usuários simpatizantes de extremismo violento, e oferecer alternativas aos seus resultados de pesquisa, direcionando-os para conteúdos alternativos (GREENBERG, 2013). A classificação em grupos/cohort é realizada com base em dados de suas pesquisas no Google: se estas se enquadrarem nos termos definidos por eles, determinados previamente, então aquela pessoa é classificada em determinado grupo.

Esse método foi desenvolvido por uma parceira da Jigsaw com a Moonshot CVE. O Redirect Method é um programa de código aberto, administrado pelo Google, Moonshot CVE e outros, que usa anúncios direcionados e vídeos do YouTube com curadoria enviados por pessoas de todo o mundo para enfrentar a radicalização online. Ao se concentrar naqueles que já pesquisam conteúdo extremista na Pesquisa Google, o Redirect oferece conteúdo de indivíduos em risco que desmente as mensagens de recrutamento dos extremistas (MOONSHOT, 2022a).

Percebe-se que há uma manipulação dos resultados de pesquisa com base naão apenas nas preferências de pesquisa dos usuários, mas sim, num perfil previamente identificado, priorizando certos websites alternativos nos primeiros lugares (METAXAS; PRUKSACHATKUN, 2017).

Não obstante esse método ser inicialmente direcionado para uma causa louvável, de evitar terrorismo, ele pode ser redirecionado para outros grupos. O problema da progressão do método de redirecionamento é quem estaria encarregado de classificar grupos, mesmo os extremistas? Ora, no espectro político tais definições são relativistas, uma vez que o centrista de hoje, pode ser o extremista de amanhã, bem como tal definição é contingente a países, haja vista que o considerado normal em determinado país, pode ser considerado extremo em outro. Tratam-se de questões que vão além da violação da privacidade, que, de fato, já ocorreu, na medida em que a Google já classificou o indivíduo a determinado grupo/cohort. No próprio site da Moonshot, apresentam-se alguns tópicos em que o método de redirecionamento é utilizado: violência *incel* no Canadá, tendências de procura de supremacia branca nos Estados Unidos, antissemitismo na contingência de teorias da conspiração antivacina, Coronavírus, conspiração de 5G, gênero, discurso de ódio e assim por diante

(MOONSHOT, 2022b). São dezenas de projetos com essa finalidade de redirecionamento, que utilizam não somente Google, mas também o Facebook e o Twitter, como ferramentas para a implementação desse método.

Por conseguinte, remanesce claro o efeito que a violação de privacidade possui, no que tange a mecanismos de pesquisa. Na medida em que alguém é classificado em um grupo/cohort e utiliza essas tecnologias, não há mais como compreender se as informações apresentadas são ordenadas à verdade, ou filtradas por um fim político-ideológico. São consequências que perpassam os meios tradicionais de procura de informação (MELLOR, 2002): o historiador, após o período Romano, poderia ir a uma biblioteca e realizar uma pesquisa a respeito da história do Império Romano, ele veria os livros e escolheria qual ler, em que ordem ler e assim por diante; os mecanismos de pesquisa atuais, que utilizam o redirecionamento, omitem e alteram os dados, conforme quem pesquisa. Nesse contexto, é como se o historiador fosse à biblioteca e encontrasse espaços vazios, ou arquivos da história de outros povos, de modo a influenciá-lo a não pesquisar o tópico, por ausência de informações.

Tratou-se principalmente do mecanismo de pesquisa da Google, mas tal tecnologia de redirecionamento pode ser aplicada em diversos outros locais. Como visto, Twitter e Facebook também o utilizam; ocorre, porém, que a Google detém dominância no market share de mecanismo de pesquisas, na ordem de aproximadamente 91% do mercado, de modo que a maioria do tráfego digital em pesquisas é realizado por intermédio dessa plataforma (STATCOUNTER, 2022b). Esse índice se mantém consistente por volta dos 90% em mais de 10 anos de análise, o que demonstra o período de dominância tecnológica que essa companhia possui.

3.2.6 Violações da Privacidade Digital em Dispositivos IoT

As violações da privacidade não se limitam, no entanto, a dispositivos de alta tecnologia, com processadores, chips e outros hardwares de última geração. Com o advento da denominada Indústria 4.0 e Internet das Coisas (IoT), as violações de privacidade se tornaram ainda mais exponenciais. Os dispositivos inteligentes, qualificados como pertencentes à IoT, são unicamente identificáveis e a maioria é caracterizada por baixa energia, pequena memória e capacidade de processamento limitado (KHAN; SALAH, 2018). Exemplos notáveis de tais dispositivos são: campainhas, câmeras, tomadas, torradeiras, geladeiras, sensores de movimento, lâmpadas e tags em geral.

Cada um desses dispositivos tem uma funcionalidade adicional, que viabiliza, em geral, controle remoto de suas usabilidades. Uma câmera pode ser vista em qualquer lugar do mundo, uma tomada pode ser desligada ou ligada remotamente, uma lâmpada e assim por diante. A principal característica desses dispositivos, porém, é a sua

capacidade de se comunicarem entre si, isto é, utilizarem-se de certas frequências para receber e transmitir dados em uma rede *mesh* sem fio. Essa rede mesh sem fio (*WNM*) permite a transmissão de dados de um nodo para outro, sem a necessidade de extenso cabeamento (SHILLINGTON; TONG, 2011). O que viabiliza essa transmissão é a existência de transceptores, que são receptores e, ao mesmo tempo, transmissores de ondas de rádio; donde, há substancial diferença entre um dispositivo que simplesmente transmite o tráfego gerado por ele mesmo, e aquele que transmite o seu tráfego, bem como o de outros que lhe enviam dados. O primeiro apenas se comunica com a rede, já o segundo (IoT) interliga outros dispositivos, formando uma extensa rede de comunicação e um fluxo de dispositivos.

O dispositivo pode ler a mensagem, usando um decodificador, e a retransmitir, caso ela não seja para ele, por meio de um codificador. Assim, uma mensagem em uma frequência particular pode ser propagada a uma longa distância por aparentemente dispositivos inócuos como uma lâmpada IoT, um sensor de movimentação, uma torradeira e assim por diante. As transmissões de dados devem ser diminutas, porque a velocidade de transmissão do FSK, sistema de modulação de frequência (VODHANEL et al., 1990), é baixa. Um tempo para viver (TTL) dá à mensagem um tempo de vida, para não se propagar permanentemente. Cada mensagem identifica o dispositivo original que a enviou, geralmente com máximo de 800 metros, mas pode passar por distâncias ilimitadas se há outros dispositivos na área, uma vez que estes criam redes capazes de alcançarem longas distâncias.

Essas transmissões de dados não se limitam somente aos dispositivos IoT. A tecnologia denominada BLE (Bluetooth Smart), ou Bluetooth de baixa energia, possibilita comunicações de baixa complexidade, sem fio, de pouco gasto energético e baixa latência (YANG et al., 2020). Qualquer aparelho que possua Bluetooth pode transmitir dados a uma distância de 800 metros, com apenas uma mudança de software; tal mudança já foi realizada em Amazon Echoes e Câmeras Ring e inclusive potencialmente é feita em televisores da Samsung, tornando-os parte de uma rede *mesh* que os interliga. Por meio dessa tecnologia, é possível às televisões não somente receberem o sinal, como também enviar feedbacks às operadoras. Inicialmente, isso pode ser utilizado para medição de audiência por meio da medida Nielsen, que proporciona estimativas de audiências de diversos programas (WEBSTER, 2008), contudo, tais informações podem ser cada vez mais invasivas, tendo em vista que diversos dispositivos Bluetooth já possuem câmera integrada. Em todos os casos, porém, trata-se de uma invasão de privacidade da qual grande parte dos usuários não está consciente.

Com a crescente expansão da tecnologia Bluetooth para diversos dispositivos, as redes *mesh* tem a capacidade de se expandir e ocupam substancial parte de cidades. Carros, telefones, aplicações de áudios, aspiradores de pó, televisores, fones de ouvidos são alguns dos exemplos de dispositivos que carregam tal tecnologia e via-

bilizam a formação de uma rede mesh. Quanto à segurança do Bluetooth, notam-se três categorias de vulnerabilidade: espionagem passiva, ataque de homem no meio (man-in-the-middle, MITM) e rastreamento de identidade (YANG et al., 2020).

A primeira vulnerabilidade consiste em um terceiro dispositivo captar os dados sendo transferidos entre dois dispositivos conectados. Como solução para esse problema, o BLE criptografa os dados sendo transferidos por meio da criptografia AES-CCM. Enquanto a segunda vulnerabilidade, Man in the middle attack, ocorre quando um dispositivo malicioso se passa por outros dois dispositivos legítimos, com a finalidade de enganar aqueles se conectando. Tanto o central, quanto o periférico se conectam ao malicioso, que roteia o tráfego entre os dois outros dispositivos; transmite-se uma aparência de conexão legítima, enquanto, em realidade, a conexão entre ambos está comprometida. Esse ataque possibilita injeção ou remoção de dados antes de chegarem a seu recipiente. Na versão 4.2 do Bluetooth, introduziu-se conexões seguradas por LE, necessitando de três passos para realizar a conexão: troca por pareamento, geração de chave por meio da criptografia ECDH e autenticação. Por último, o rastreamento de identidade ocorre quando uma entidade maliciosa é capaz de associar o endereço do dispositivo BLE com um usuário específico, rastreando-o fisicamente. Para solucionar isso, o BLE modifica periodicamente o endereço do dispositivo para torná-lo não rastreável (YANG et al., 2020, p. 4).

3.2.7 Privacidade e Conveniência na Conjuntura de IoT

Tratam-se de vulnerabilidades, sendo assim, podem ser exploradas, não obstante as medidas protetivas. Isso por si só representa um risco à privacidade, porém, o que ocorre em definitivo é o envio dessas informações a bancos de dados centralizados, em certos usos, como monitoramento de saúde, vigilância e rastreamento. No que tange a certos usos de dados, faz-se necessário abordar a relação inversamente proporcional entre privacidade e conveniência ao usar a tecnologia. Por conveniência, diversos usuários digitais abdicam de sua privacidade em detrimento de facilidade de uso, na medida em que as alternativas que não violam a privacidade tendem a ser mais complexas e menos intuitivas aos usuários, como é visto na parte de soluções apresentadas no presente trabalho serem também amplamente conhecidas e utilizadas. Nesse contexto, há um preço pela conveniência, que pode ser a de ter a privacidade potencialmente violada, uma vez que as informações pessoais acabam por ser divulgadas com maior amplitude, como gostos, localidade, opiniões políticas, entre outros (NG-KRUELLE et al., 2002).

Um exemplo é que uma pessoa pode desejar ter sua saúde monitorada por um serviço médico 24 horas por dia. Para esse fim, ela utiliza a tecnologia BLE para enviar dados pessoais para um banco de dados centralizados, em troca de monitoramento

de seu estado físico. Essa pessoa está obtendo auxílio médico, em detrimento de compartilhar seus dados pessoais; pode parecer uma troca razoável, contudo, inclusive os dados mais íntimos, como os atinentes à sexualidade, são transmitidos; não somente é possível detectar tais atos por meio de frequência cardíaca, movimentação e afins, como também estes serão armazenados em um banco de dados (YANG et al., 2020, p. 8) vinculado diretamente à identidade do sujeito. O que se tinha como privado, torna-se por meio da conveniência tecnológica, um dado registrável.

Diante disso, os dispositivos mais simplórios, como torradeiras, sensores de movimentação, televisores, geladeiras e campainhas podem servir para formar essa rede de transmissão, desde que estejam equipados com transceptores. Esses transceptores, componentes dotados de receptores e transmissores, são caracterizados por seu gasto energético em relação à taxa de transmissão de dados (SCHUMACHER et al., 2017), assim, não poderiam, conforme a sua natureza em dispositivos IoT, transmitir dados mais sensíveis, como vídeos que exigem mais taxa de transmissão. No entanto, os riscos de privacidade são substanciais, pois tais dispositivos se tornam capazes de transmitir usabilidade por vias aéreas: o horário em que a torrada ficou pronta, quando que o sensor de movimentação foi ativado, quando se modifica o canal de televisão, quando se abre a geladeira, quando se toca a campainha, quando a porta foi aberta e assim por diante. Essas informações são transmitidas para outros dispositivos, que novamente os transmitem para um destino desconhecido, programado originalmente no que inicialmente transmitiu o sinal.

Outra potencial violação de privacidade se dá por intermédio de ondas de rádio de identificação (RFID), presentes nesses dispositivos. Essas ondas de rádio de identificação estão localizadas em tags, acopladas a certos dispositivos, que emitem mensagens legíveis para leitores mais especializados de RFID. O leitor recupera informação sobre o número de ID por meio de um banco de dados e age de acordo com isso. As tags também possuem memória, razão pela qual são capazes de transferir vários leitores de RFID para diferentes localizações. Essa informação pode rastrear o movimento do item catalogado, tornando a informação disponível para cada leitor (WEINSTEIN, 2005). Diante disso, a tecnologia está crescentemente sendo utilizada em documentos como passaportes, carteiras de habilitação e até mesmo em rodas de veículos. O RFID comercial padrão de segunda geração pode ser identificado por equipamentos normais; ocorre que, com apenas uma mudança de software, os dispositivos podem incluir um sinal de RFID, enviá-lo e ler a resposta, novamente, uma vez que se encontra na mesma frequência dos rádios construídos em inúmeros desses dispositivos.

Tal tecnologia representa uma forma conveniente de transmissão de dados, uma vez que a tag passiva é extremamente barata. Não somente a tag passiva é módica, como também possui um capacitor que é abastecido pelo próprio leitor, por intermédio

de um sinal eletromagnético (WEINSTEIN, 2005, p. 2). Nesse contexto, há substanciais similaridades entre a tecnologia RFID e BLE: ambas são facilmente implementáveis em dispositivos, são de baixo custo e, principalmente, proporcionam transmissão de dados como localização, com alta amplitude e conveniência para o coletor. Apesar de a RFID ser mais antiga, as duas podem ser utilizadas como instrumentos para violação de privacidade; há mais tecnologias com princípios semelhantes, como Zigbee, Thread (da Google), 802.15, LoRa. No que tange à Internet das Coisas, portanto, resta claro que não se pode mais esperar que aparelhos domésticos comuns cumpram sua finalidade primária somente. Quanto mais esses dispositivos se popularizam, maior ficam as redes *mesh* e, com isso, maior é a capacidade de vigilância, abrindo a oportunidade para ataques cibernéticos e violação de privacidade.

A Apple possui um sistema análogo aos moldes da IoT comentado anteriormente. Por intermédio de Air Tags (APPLE, 2022), é possível detectar a localização dos dispositivos, com a já tratada tecnologia BLE. Desse modo, seguindo tendência análoga de criação de redes *mesh* de suas concorrentes, Amazon por meio de seus produtos Ring Camera e Amazon Echo (LYONS, 2020) e Google por meio de produtos Google Nest e da tecnologia Open Thread (OPENTHREAD, 2022), a Apple também criou sua própria rede *mesh*, que expõe a localização de seus usuários. As Air Tags funcionam de maneira semelhante às tags previamente mencionadas, mas com a tecnologia BLE, ao invés de RFID; sendo assim, elas constantemente emitem o sinal, sem a necessidade de serem abastecidas magneticamente por um leitor. Diante disso, tais dispositivos permanecem ativos por volta de um ano, haja vista o seu baixo uso energético.

Uma Air Tag pode ser acoplada em um chaveiro, por exemplo. Esse chaveiro está próximo de outros *smartphones* da Apple, que enviam o identificador dessa Air Tag à Apple e a sua direção, juntamente com a localização desse smartphone que recebeu o sinal. Nesse contexto, não somente essa tecnologia rastreia o que a ela está acoplada, como também outros smartphones da Apple nas proximidades, revelando as suas localizações. Contanto que um sujeito que possua um iPhone esteja no alcance da Air Tag (por volta de 60 metros), este tem sua localização enviada à Apple, de modo que não há propriamente privacidade no que tange aos locais dos usuários da Apple, em especial nas cidades e locais com maior densidade demográfica. A localização do smartphone é refinada pela própria Air Tag, haja vista que seu ID e direção são enviados juntamente com a localização do smartphone, sendo assim, trata-se de um rastreamento ainda mais preciso que o GPS; tal localização e interação entre dispositivo é constantemente armazenada, o que o usuário vê é simplesmente a última localização do Air Tag (BRAXMAN, 2021).

Outra grande empresa de tecnologia que é marcante nas tecnologias IoT é a Amazon. Essa organização possui diversos dispositivos dessa natureza, quais sejam Amazon Echo, câmeras Ring, robôs e outros dispositivos. No que tange às câmeras

Ring, as funcionalidades desse dispositivo viabilizam crescente vigilância a respeito não só dos proprietários de determinada residência, mas também dos transeuntes nas proximidades, uma vez que são dotadas de potentes receptores de áudio e imagem (GUARIGLIA, 2022). A incorporação de outras companhias, das mais diversas áreas pela Amazon, torna esta empresa uma detentora de dados extremamente sensíveis sobre uma parcela significativa da população. A empresa iRobot recentemente foi adquirida, o que proporciona maior coleta de dados sobre os indivíduos, haja vista que um de seus principais produtos é um robô aspirador que mapeia a residência, onde é instalado, sendo um dado sensível e consequentemente transmitido para domínios da Amazon (GAULT, 2022).

3.2.8 Smartphones e Violações da Privacidade

O uso de *smartphones* é fenômeno de crescimento na última década. Há inúmeros estudos que abordam o uso desses dispositivos com as mais variadas perspectivas (LI et al., 2022). Para o presente trabalho, convém abordar os riscos à privacidade que esses aparelhos apresentam aos seus usuários que, imersos em um mundo virtual, muitas vezes ignoram a capacidade de vigilância e espionagem que seus dispositivos possuem.

É relevante, de início, abordar as funcionalidades que um *smartphone* possui. Esse dispositivo, externamente, é dotado de câmeras, sendo nos mais recentes, de diversas câmeras, tanto frontais, quanto traseiras. Somado a isso, um *smartphone* possui microfone, capaz de captar áudio com alcance e precisão elevados. Internamente, há diversos componentes que o conectam a redes, como antenas, adaptadores e outros transmissores. Os celulares modernos vem com dois processadores separados, um para o propósito geral dos aplicativos que roda o principal sistema operacional (Android, IoS e outros), enquanto o outro é responsável por estabelecer comunicação com a rede de telefone móvel. Esse último processador sempre roda um sistema operacional proprietário/privativo, capaz de monitorar o usuário, ao ativar o microfone, localização do GPS e acessar a câmera (KOCIALKOWSKI, 2014) Em suma, trata-se de um computador móvel, com acesso à internet e a informações pessoais do usuário. O que o diferencia, porém, é a capacidade informacional condensada que possui, adstrita a um sistema operacional. Isso viabiliza a instalação de aplicativos dos mais variados tipos, que possuem inúmeras funcionalidades, desde enviar mensagens, assistir vídeos, até monitorar atividades físicas (AGU et al., 2013).

Não obstante as conveniências que um *smartphone* possui, a imensa maioria desses dispositivos é utilizada para vigilância e coleta de dados. Pela possibilidade do usuário instalar diversos aplicativos, há a possibilidade de viabilizar uma atividade maliciosa denominada backdoor, que viabiliza que alguém, que não deveria estar no

controle do computador, no qual o programa está instalado, envie comandos para ele. Alguns termos de serviço apresentam a presença de backdoors universais em seus aplicativos.

As empresas desenvolvedoras do hardware e software desses dispositivos possuem, assim, substancial poder informacional sobre seus usuários. Há de se enfatizar, no entanto, que a grande maioria dessas organizações vinculadas a *smartphones* utilizam de software proprietário nos dispositivos que comercializam. Desse modo, é mais difícil saber com precisão que tipo de coleta de dados é realizada, apesar de diversas terem sido descobertas (GNU, 2022b) (GNU, 2022c).

Em síntese, os telefones celulares desenvolvidos na última década são potenciais dispositivos de monitoramento. Uma vez que grande parte da população utiliza *smartphones*, o potencial de vigilância se amplifica, na medida em que tais dispositivos não somente espionam seus proprietários, mas também o ambiente no qual estes se encontram inseridos. Analogamente à tecnologia IoT, os celulares também extrapolam suas funcionalidades padrão e proporcionam aos detentores dos softrwares instalados significativo poder informacional concernente aos seus consumidores.

3.2.9 Violações de Privacidade em Jogos Eletrônicos

Por fim, cabe tratar de um dos entretenimentos mais populares na atualidade, os jogos digitais. Esse tipo de entretenimento pode ser um grave violador da privacidade digital dos jogadores. Ocorre com frequência que a organização desenvolvedora do jogo almeja obter dados adicionais da sua base de jogadores e, para isso, extrapola a funcionalidade essencial de entretenimento de um jogo digital.

Dentre as possibilidades de violação de privacidade em jogos está a possibilidade de gravar imagens ou áudios dos seus jogadores. A Microsoft, por exemplo, possuía empresas associadas que eram responsáveis por ouvir áudio de usuários desses consoles, enquanto eles conversavam em suas casas, sendo a maioria vozes de crianças, com o intuito de melhorar as funcionalidades de comando de voz do console (COX, 2022).

Em razão de grande parte dos jogos serem vendidos uma única vez, ou muitos serem gratuitos para jogar, outros métodos de monetização são, por vezes, utilizados. Em diversos jogos, desde jogos *indies* até consolidados (como Civilization 6 e The Elder Scrolls Online), há um software que é executado conjuntamente ao jogo, denominado Red Shell; trata-se de um programa de rastreamento de dados do jogador, que proporciona análises de publicidade, ao mesmo tempo em que coleta dados como endereço de IP, versão do navegador, navegadores instalados, fuso horário, linguagem do sistema, fontes disponíveis, resolução da tela e outros (CHALK, 2018). O propósito dessa coleta é gerar impressão digital dos usuários; a Red Shell transmite

essa informação para terceiros, de modo a avaliar a efetividade de publicidade sobre os jogadores (REDSHELL, 2022).

A probidade nos jogos é visada pelos seus desenvolvedores. Ocorre, porém, que para este fim certas organizações abusam de seu software, como o fez a Riot Games. Seu novo sistema antitrapaça é executado na inicialização do sistema no nível kernel do Windows; apesar de a organização afirmar não coletar dados a respeito de seus usuários por essa via,essa prática intrinsecamente aumenta a superfície de ataque contra o sistema operacional (HRUSKA, 2020).

Há ainda um jogo mais invasivo, do ponto de vista da privacidade. Kerbal Space Program é um jogo com temática aeroespacial, em que o usuário constrói aparatos espaciais, em seguida propulsionando-os em órbita; o jogo coleta dados como nome e sobrenome, endereço de e-mail, número de telefone, foto, endereço postal, geolocalização, informação de pagamento, idade, gênero, data de nascimento, código postal, configuração de hardware, ID do console, compras, endereço de IP e outras informações de serviços integrados e redes sociais (TAKE-TWO, 2018). Nesse contexto, a empresa desenvolvedora comercializa essas informações para empresas de publicidade, sendo assim, não somente esse jogo está rastreando o jogador, mas também serviços de publicidade que obtém essa informação.

Por fim, uma grande companhia da indústria de jogos é a Steam. Esta organização é responsável pela comercialização de inúmeros jogos digitais; o seu acesso, porém, está circunscrito à coleta de certos dados como nome, endereço, e-mail, idade, endereço de ID, ID único do dispositivo, posts no fórum, gravações de chat de voz e outros. A Steam confirma que transmite essa informações a terceiros (STEAM, 2018). Além disso, seu sistema antitrapaça grava o histórico de navegação do usuário e o envia para um servidor da Valve; apesar de essa empresa ter negado armazenar o histórico de navegação do usuário (NEWELL, 2018).

A alternativa à coleta de dados, propulsionada por esse monólito de vigilância digital é complexa e exige comprometimento pessoal. Passa primeiramente pela compreensão de que a coleta de dados involuntária está presente em múltiplas tecnologias cotidianas e, em razão disso, o sacrifício individual a certas tecnologias se faz necessário, caso a pessoa não queira ser exposta ao monitoramento destas empresas e ao risco de violação de privacidade. Por isso, deve o usuário digital procurar alternativas em softwares que não coletam seus dados. Não obstante a necessidade de os usuários preservarem sua privacidade digital de forma autônoma, os desenvolvedores também tem de cumprir certos princípios.

3.3 Princípios de Preservação da Privacidade Digital no Desenvolvimento e Distribuição de Software

As violações de privacidade são inúmeras e se encontram presentes nos mais variados softwares. Disso resulta que a mudança não parte unicamente do usuário, mas também dos desenvolvedores de software, sendo imprescindível que sigam diretrizes adequadas à proteção da privacidade de seus clientes. Isso, no entanto, resulta em limitações significativas quanto à coleta de dados, o que pode até mesmo ser um empecilho à existência de determinados softwares.

Para preservar a privacidade, deve existir nos primórdios do desenvolvimento de software padrões de privacidade. Um possível padrão a ser adotado é o ISO/IEC 29100, que apresenta princípios e diretrizes para que um software preserve a privacidade de seus usuários (DROZD, 2015). Serão abordadas 11 diretrizes a serem seguidas por desenvolvedores, com o intuito de preservar a privacidade digital dos utilizadores do software. Em cada princípio, há diferentes técnicas a serem seguidas, sendo algumas na apresentação do sofware ao usuário e outras no seu desenvolvimento propriamente dito (COLESKY et al., 2022k). Essas diretrizes estão presentes em grande parte no Marco Civil da internet (BRASIL, 2018a).

O primeiro princípio é denominado consenso e escolha. Trata-se da obtenção de consenso do usuário do software para coletar, processar e transmitir dados. O consenso pode ser implícito ou explícito: o explícito é comumente o mecanismo usado para os usuários consentirem deve ser claro, por exemplo, um botão denominado "Eu consinto"(COLESKY et al., 2022l). O controlador dos dados deve assegurar o entendimento suficiente de cada usuário a respeito das potenciais consequências de aceitar o termo. Em se tratando de consenso implícito, como no caso de Cookie Walls em websites, deve ser dada oportunidade aos usuários de escolherem não usar o serviço e portanto não estar sujeitos ao processamento de dados requisitado (COLESKY et al., 2022m). Além disso, deve o controlador garantir que os usuários estão informados clara e concisamente, previamente ao aceite (COLESKY et al., 2022n). Corresponde a esse princípio, o previsto no artigo 7º, inciso IX, da legislação supracitada.

O segundo princípio diz respeito à legitimidade de propósito e especificação. O serviço deve oferecer um contrato para o usuário (disponibilizando uma política de privacidade) que vincula o controlador à sua palavra, e o usuário deve consentir ao processamento de seus dados para propósitos específicos. Deve o acordo vincular qualquer representante do controlador, bem como ser claro o suficiente para o usuário entender. Quando a organização necessitar de coleta adicional de dados, deve obter consenso específico, informado e explícito do usuário (COLESKY et al., 2022j). A especificação é necessária para se obter a finalidade da organização com aquele dado. Além disso, os softwares possuem, de maneira geral, uma finalidade essencial

a eles, seja esta entretenimento, transporte, finanças e outras. Naturalmente, os dados tem de ser adequados a essas finalidades, de modo que uma software de calculadora, por exemplo, não pode exigir de seu usuário que ele ative sua câmera, ou disponibilize seus contatos. Corresponde a esse princípio o previsto no artigo 7º, inciso VII.

O terceiro princípio é a limitação de coleta de dados. Esse princípio é aplicável a algumas espécies de dados, mas principalmente se relaciona com a finalidade a que se propõe o software, bem como a certas naturezas de dados. O dado mais comum de se aplicar tal limitação é a localização; a granularidade do local consiste em coletar e armazenar apenas o local necessário do usuário (ex. ao invés de compartilhar o exato local do usuário, compartilhar somente o município, estado, ou o país) (COLESKY et al., 2022h). Outra implementação possível é a divulgação seletiva, que consiste em adequar um serviço, que exige extensa coleta de dados pessoais, para funcionar com um nível de coleta com o qual o usuário se sente confortável (BERKELEY, 2022). Corresponde a esse princípio o previsto no artigo 7º, inciso VII.

O quarto princípio diz respeito à minimização de dados. Este princípio corresponde a minimizar a coleta de dados do usuário, ou até mesmo circunscrever o dado coletado somente ao usuário. Confinar parcela dos dados, principalmente os pessoais, para os dispositivos dos usuários, não os enviando para servidores centrais da empresa (COLESKY et al., 2022q), permitir que o usuário controle o dado que deseja compartilhar (COLESKY et al., 2022d),utilizar sistema de gestão de obrigações (*obligation management*), que apresenta um ciclo de vida informacional baseado nas preferências individuais e políticas organizacionais (COLESKY et al., 2022i). Se a organização perpassa esse limite, é razoável afirmar que o foco de seu negócio está mais em vigilância e coleta de dados, do que aquele proposto inicialmente. Corresponde a esse princípio o previsto no artigo 7º, inciso VII.

O quinto princípio diz respeito à limitação de uso, retenção e divulgação. É aplicável a softwares em que os usuários do serviço querem compartilhar conteúdo, mas nem todo o conteúdo que eles geram é adequado para compartilhamento, diante disso, é recomendável viabilizar exposição seletiva dos dados do usuário . Proporcionar ao usuário a possibilidade de definir a quem certo conteúdo é destinado auxilia na manutenção desse princípio (COLESKY et al., 2022c). Desse modo, é razoável que a organização os oriente de que certo compartilhamento é potencialmente invasivo, restabelecendo o consenso para prevenir vazamento acidental de dados. Corresponde a esse princípio o previsto no artigo 7º, inciso VII.

O sexto princípio consiste na precisão e qualidade do software e de sua distribuição. Deve a organização possuir um termo de acordo que disponha adequadamente a coleta de dados, bem como seja explícito e breve em afirmar o que será coletado. A introdução de ícones não excessivos, cuidadosamente agrupados e compreensíveis ao usuário é uma prática que auxilia na compreensão dos usuários, bem como abrevia

aceite ou não (COLESKY et al., 2022f). Os ícones tem de ser apropriados e consistentes ao que se quer transmitir aos clientes (COLESKY et al., 2022a). Corresponde a esse princípio o previsto no artigo 7º, inciso VI.

O sétimo princípio é a abertura, transparência e informação do software. Usuários podem entender no primeiro olhar, os potenciais riscos da coleta de dados, por meio do uso de ícones, um repositório de softwares como o F-droid faz isso para indicar se há alguma funcionalidade nociva em um software, o que auxilia na informação. Uma funcionalidade comum aos softwares é a coleta periódica de determinado dado, como o endereço de IP ou o local; isso muitas vezes passa desapercebido pelo usuário, o que demonstra falta de transparência. Para gerar mais transparência, convém aos desenvolvedores alertarem o usuário dessas coleta periódica, de modo que ele possa consentir ou não a ela (COLESKY et al., 2022b). Em adição a esse princípio a abertura do código fonte do software proporciona transparência significativa aos usuários, de modo que ele pode ser inspecionado, apontando, assim, suas funcionalidades maliciosas. Corresponde a esse princípio o previsto no artigo 7º, inciso VI.

O oitavo princípio é a participação e acesso do indivíduo. Os usuários têm diferentes preocupações quanto às informações pessoais transmitidas; alguns querem compartilhar mais, outros menos. Diante disso, os controladores que ganham com a atividade do usuário e querem incentivá-la, mas isso pode afetar outros usuários negativamente. Sendo assim, a adoção de um sistema de reciprocidade, em que o usuário que mais participa é mais recompensado gera proporcionalidade à participação e contribuição de cada cliente do software (COLESKY et al., 2022o). Assim, o usuário deve compreender que o sistema valoriza suas preferências, deve perceber valor real na sua participação, se desejar, deve ser auxiliado em uma transição suave no ecossistema de maior para menor participação ou vice-versa. Corresponde a esse princípio o previsto no artigo 7º, inciso X.

O nono princípio é concernente à responsabilização. O controlador deve ser responsabilizado quando descumpre os termos a que se obriga, bem como nas ocasiões em que há vazamento de dados, ou quando o controlador excede as atribuições a que ele se vinculava, coletando dados excessivos, espionando seus usuários e assim por diante. Corresponde a esse princípio o previsto no artigo 3º, inciso VI.

O décimo princípio diz respeito à segurança da informação. Esse princípio engloba inúmeras práticas que, ao mesmo tempo que são benéficas ao usuário final, podem tornar cansativa a utilização de determinado software. Deve o desenvolvedor instaurar práticas como armazenar dados pessoais nos dispositivos pessoais do usuário, prevenir acesso suspeito aos seus dados através de alertas e autenticação de múltiplos fatores (COLESKY et al., 2022p). Avisar os usuários quanto ao potencial de identificar o usuário, conforme a agregação de informações (COLESKY et al., 2022g). Essa agregação pode transformar dados aparentemente não invasivos em

intrusivos, de modo que o usuário desconhece. Criptografar os dados sensíveis do usuário, como senha, e-mails e outros que podem comprometer (COLESKY et al., 2022e). Corresponde a esse princípio o previsto no artigo 10, § 4º.

O décimo primeiro e último princípio consiste no *compliance* de privacidade. Deve o desenvolvedor adequar o sistema desenvolvido a um nível de privacidade minimamente exigido, de modo que, mesmo diante de um vazamento de dados internos, os dados sensíveis do usuário não sejam comprometidos. Isso envolve diversas práticas e um somatório dos princípios tratados anteriormente.

Esses princípios denotam algumas práticas capazes de preservar a privacidade digital dos usuários. Cabe aos desenvolvedores discernirem a respeito de outras práticas, em especial, condizentes ao software que desenvolvem. Não se trata, portanto, de um rol taxativo de práticas, mesmo porque as práticas de software constantemente se desenvolvem ao ponto de algumas se tornarem obsoletas. Resta, por conseguinte, abordar a percepção desses princípios por parte do consumidor final do software. Para isso uma pesquisa foi desenvolvida com questionamentos correlatos aos princípios supracitados, buscando relacioná-los com perguntas familiares aos usuários.

4 Método de Pesquisa

Adiante serão abordados os meios adotados na pesquisa realizada com intuito de aprender a compreensão prática dos usuários digitais: o enquadramento da pesquisa, a sua operacionalização assim como a coleta de dados serão tópicos do presente capítulo.

De início, cabe esclarecer que a metodologia ora adotada é um estudo exploratório, com etapa qualitativa, baseada na parte teórica abordada anteriormente e no conhecimento empírico para a confecção do questionário, posteriormente submetido à análise. Outra etapa é a quantitativa, com uma amostra não probabilística, tendo em vista que houve 116 questionários realizados.

4.1 Enquadramento da Pesquisa

Esta pesquisa foi desenvolvida por intermédio de uma abordagem quantitativa, em um questionário distribuído nas mídias digitais. A distribuição se deu através de e-mails, envios em grupos de WhatsApp e compartilhamento em redes sociais, como o Instagram. O usuário digital que se deparasse com a pesquisa de TCC poderia respondê-la, ou não, sendo assim, de caráter voluntário. As perguntas abrangem tópicos relativos à privacidade digital, sendo que cada pergunta abrange ao menos um dos princípios explicados anteriormente.

4.2 Contextualização da Pesquisa

Há que se ressaltar, além disso, que a temática da pesquisa concerne à privacidade digital da pessoa que responde. Inicialmente, parte-se de algumas noções específicas sobre o que proporciona maior ou menor privacidade digital: essas práticas estão subentendidas nas perguntas, razão pela qual a natureza quantitativa da pesquisa é explícita, pois há informação bem definida sobre o problema. Não se está, por intermédio desta pesquisa, objetivando saber quais são as melhores práticas de segurança/privacidade digital, mas sim conhecer se os usuários digitais as praticam, ou não, diante de sua percepção de privacidade digital. Diante disso, a presente pesquisa possui abordagem quantitativa que segundo Silva, Lopes e Junior (2014) só tem sentido quando há um problema muito bem definido e há informação e teoria a respeito do objeto de conhecimento, entendido aqui como o foco da pesquisa e/ou aquilo que se quer estudar. Para este fim prático, foi necessário introduzir uma pesquisa quantitativa para o público digital, de modo a questioná-lo a respeito do uso das alternativas, focadas na privacidade digital. A finalidade dessa pesquisa é explorar a prática digital dos usuários, assim como a extensão com que se preocupam com ela

e, para isso, utilizam de meios não usuais para preservá-la.

4.3 Operacionalização da Pesquisa

Tal pesquisa, assim, foi realizada por intermédio de um questionário de conhecimento e uso das tecnologias abordadas anteriormente, divulgado no meio digital, com 116 respostas. O intuito dessa pesquisa é analisar o quanto efetivamente o usuário de internet está preocupado com sua privacidade digital. Haja vista as extensas violações tratadas anteriormente, a preservação da privacidade digital, em grande parte, dá-se por intermédio das escolhas dos usuários digitais. Desse modo, para relacionar a preservação da privacidade destes com o presente trabalho, as perguntas serão correlatas aos princípios abordados no capítulo anterior.

Cada princípio tem no mínimo uma pergunta correspondente 1, de modo que o questionário abrange todos eles. As alternativas apresentam práticas congruentes e não congruentes ao princípio abordado; caso o usuário responda de forma congruente ao princípio, ele está realizando uma boa prática, contrariamente, ele está realizando uma prática ruim de preservação da privacidade digital. Adiante serão apresentadas as perguntas realizadas e suas relações com os princípios ISO/IEC 29100. As alternativas disponíveis, encontram-se em documento anexado a este trabalho.

4.3.1 Coleta de Dados

A coleta dos dados utilizados para essa pesquisa se deu por intermédio do formulário de respostas do Google. Para esclarecer aos usuários de que o questionário possui um fim acadêmico, encontrava-se uma explicação da sua finalidade, bem como de seu caráter anônimo, no início do questionário tipo survey; ao continuar, o usuário aceitava tacitamente os termos e compartilhava suas respostas para as análises realizadas. Em razão disso, não houve coleta de e-mails, nem informações demasiadamente pessoais, como nome, telefone, endereço e assim por diante.

Neste formulário, foram redigidas 33 perguntas, sendo 3 de cunho demográfico e 30 relativas ao tema abordado. Entre essas 30, uma delas era dissertativa e perguntava o que o usuário pensa sobre privacidade digital; uma boa parte dos questionados responderam a essa pergunta, mas houve quem não a respondeu. O restante das perguntas, 29 questões, eram todas objetivas, 9 destas eram de múltipla escolha, enquanto 20 eram de escolha singular. Nesta conjuntura, as respostas eram condicionadas às alternativas apresentadas e à pergunta objetiva; as que possuíam múltipla resposta, porém, possuíam também a alternativa "outro", em que o questionado poderia responder de forma mais abrangente. Naturalmente, trata-se de um questionário, em sua maioria, em que as perguntas são previamente estruturadas e se tem o cui-

Questões	**Princípios**
O que você considera mais importante em um serviço online? 3	Limitação de uso, retenção e divulgação; Segurança da Informação
Você lê os termos de uso dos serviços/aplicativos que utiliza? 4	Consenso e escolha
Você utiliza algum Software Livre (em que os usuários possuem a liberdade de executar, copiar, distribuir, estudar, mudar e melhorar o software). Exemplo: Gnu/Linux? 5	Legitimidade de propósito e especificação; Abertura, transparência e informação; Limitação de Coletas
Qual(is) destes sistemas operacionais de desktop você utiliza? 6	Limitação de Coletas; Minimização de Dados; Segurança da Informação
Qual (is) destes sistemas operacionais de *smartphone* você utiliza? 7	Limitação de Coletas; Minimização de Dados; Segurança da Informação
Qual(is) destes navegadores você utiliza? 8	Limitação de Coletas; Minimização de Dados; Segurança da Informação
Você utiliza navegadores para diferentes usos (Exemplo: um para trabalho, outro para uso pessoal)?	Limitação de Coletas; Legitimidade de propósito e especificação;
Qual(is) destas redes sociais você utiliza? 9	Participação e acesso do indivíduo, Limitação de Coletas, Minimização de Dados
Quanto às fotos que você publica em sites, redes sociais e aplicativos de mensagens: 10	Precisão e qualidade; Limitação de Coletas; Minimização da Coleta de Dados
Você se sente informado a respeito dos dados que compartilha nas redes sociais?	Participação e acesso do indivíduo; Compliance de Privacidade; Consenso e Escolha;
Qual a configuração de privacidade das suas contas de rede social ?	Abertura, transparência e informação
Qual(is) destes aplicativos de mensagem você utiliza? 11	Legitimidade de propósito e especificação; Limitação de Coletas, Minimização de dados; Segurança da Informação
Você utiliza algum serviço de VPN? Se sim, qual? 12	Limitação de uso, retenção e divulgação
Você utiliza algum serviço de armazenamento em nuvem? 13	Limitação de Coletas; Segurança da Informação; Limitação de uso, retenção e divulgação
Qual(is) destes mecanismos de pesquisa você utiliza? 14	Limitação de uso, retenção e divulgação; Limitação de Coletas; Precisão e qualidade
Quanto à localização, você prefere: 15	Limitação de Coletas; Precisão e qualidade
Quanto a cookies: 16	Limitação de Coletas; Consenso e escolha
Os discos rígidos dos seus dispositivos: 17	Segurança da Informação; Limitação de Coletas
Você armazena suas senhas no navegador/sistema operacional?	Limitação de Coletas; Minimização de Dados
Os sites ou aplicativos que você utiliza auxiliam na criação de uma senha forte (vários caracteres, letras maiúsculas e caracteres especiais)? 18	Segurança da Informação; Minimização de Dados
Com relação às suas senhas: 19	Segurança da Informação
Você utiliza autenticação de múltiplos fatores para suas contas? 20	Segurança da Informação; Limitação de uso, retenção e divulgação
Você utiliza sua conta do Google, Facebook ou Apple para entrar em sites? 21	Consenso e escolha; Limitação de uso, retenção e divulgação
Você se sente incomodado quando tem que utilizar biometria como forma de autenticação (Impressão digital, rosto, olhos, etc.)? 22	Limitação de uso, retenção e divulgação; Minimização de Dados
Você teme que seus dados biométricos possam ser vazados? 23	Responsabilização
Você utiliza sistema de segurança por câmeras? 24	Minimização de dados;
Você acredita que, diante do vazamento de seus dados pessoais, a empresa que vazou:	Responsabilização
Em geral, de que forma os sites e serviços que você utiliza apresentam as informações que coletam de você?	Consenso e escolha; Abertura, transparência e informação
Qual a configuração de privacidade das suas contas de rede social?	Abertura, transparência e informação; Limitação de uso, retenção e divulgação; Participação e acesso do indivíduo

Tabela 1: Tabela da relação entre as questões e os Princípios

dado de não fugir delas (BONI; QUARESMA, 2005, p. 75); a pergunta dissertativa, porém, possuía maior grau de subjetividade do questionado, razão pela qual era facultativa.

5 Análise de Dados

As análises adiante contemplam as práticas boas em azul (forte, a melhor prática, claro uma prática boa), as práticas ruins estão apresentadas em laranja, já as práticas que podem ser ruins ou boas para a privacidade digital estão em cinza. Tendo em vista a apresentação das perguntas e a respectiva relação com os princípios, cabe agora partir à análise dos dados.

O questionário foi compartilhado em redes sociais e grupos de WhatsApp, de diferentes conhecimentos tecnológicas, com o intuito de abranger tipos diversos de populações. Em decorrência disso, as 116 respostas demonstram preocupação significativa com a privacidade digital, porém, na prática, não se observam atitudes congruentes a essa preocupação, na medida em que grande parte deles não preservam com suas escolhas de software sua privacidade digital. Isso significa que, ou os usuários estão agindo contrariamente ao que pensam, ou eles dão relevância à privacidade, no entanto, o seu resguardo deve ser feito por outrem (empresas, regulações, governanças...).

De início, a demografia dos questionados demonstra que 52,6% das respostas partiram de mulheres, enquanto que 47,4% foram provenientes de homens. Quanto à orientação sexual, 83,5% se declararam heterossexuais e 16,5% homossexual, bissexual ou não ortodoxo. A mediana da idade foi de 26,5 anos, sendo assim, mais pessoas jovens responderam ao questionário.

A primeira pergunta redigida aos questionados é sobre o que eles pensam sobre privacidade digital. Trata-se de uma pergunta opcional, que permite a escrita, de modo que sua análise demonstra respostas esparsas, mas com algumas tendências. Muitos consideram a privacidade digital como importante, enquanto outros a consideram como inexistente. Há ainda aqueles que não se posicionam, em razão de possuírem pouco conhecimento a respeito. Aproximadamente 50%, dos 84 que responderam, disseram que a privacidade digital é importante ou essencial, por volta de 10% afirmaram que ela é inexistente, equanto apenas 6% disseram que ela é um direito. Aproximadamente 20% relacionou a privacidade digital com dados; alguns relatram que se trata de um assunto intrigante, outros a relacionaram com violação e uma parcela pontuou seu caráter limitado. Na figura 1, encontram-se as palavras mais utilizadas pelos usuários para descreverem o que pensam sobre privacidade digital:

Desse modo, percebe-se que os usuários compreendem, em parte, que a sua privacidade digital é violada. Alguns afirmam isso com base no que lhes transmitem em formas de publicidades, o que demonstra um efeito negativo, do ponto de vista da privacidade, ao utilizar dados sensíveis do usuário, como a fala offline, para certos fins publicitários. Poucos afirmaram que a privacidade é propriamente um direito, não obstante ser essa a consideração jurídica a seu respeito, consoante a LGPD. De fato,

Figura 1: Mapa de Tendências das palavras respondidas

os usuários digitais não necessariamente pensam do ponto de vista jurídico sobre a privacidade, mas sim de sua perspectiva individual com o uso em geral da internet. Uma resposta, inclusive, considerou parar de utilizar o *smartphone*, devido ao "rastro digital"que este deixa do usuário. Houve, inclusive, pessoas que afirmaram desconhecer do assunto, mas que gostariam de ter o conhecimento de como proteger seus dados. Diante disso, a preocupação por parte dos usuários a respeito da privacidade é notável.

Em seguida, esclarecendo a preocupação geral a respeito da privacidade digital, quase 85% dos questionados estar preocupados, em médio para alto grau (4 ou 5). Perto de 50% dos questionados responderam estar preocupados em alto grau (5); estratificando as respostas, percebe-se que, entre os questionados com menos de 30 anos, 40% respondeu estar preocupado em alto grau com a privacidade, enquanto que entre os questionados com mais de 30 anos, 63% afirmou se preocupar em alto grau com a privacidade digital. Nota-se, assim, uma tendência de se preocupar mais com a privacidade digital entre as pessoas com mais idade. No que tange à orientação sexual, 54,2% dos heterossexuais afirmam se preocupar alto grau com a privacidade; já entre quem não se considera heterossexual, 25% dos questionados se preocupa em alto grau. Ao classificar os níveis de preocupação, chegou-se ao nível alto, correspondente a grau 5 de preocupação (média + desvio padrão), ao nível baixo correspondente a um grau menor que 3.57 e ao nível médio (média - desvio padrão),

correspondente ao intervalo entre o baixo e o médio (de 3.58 a 4.99):

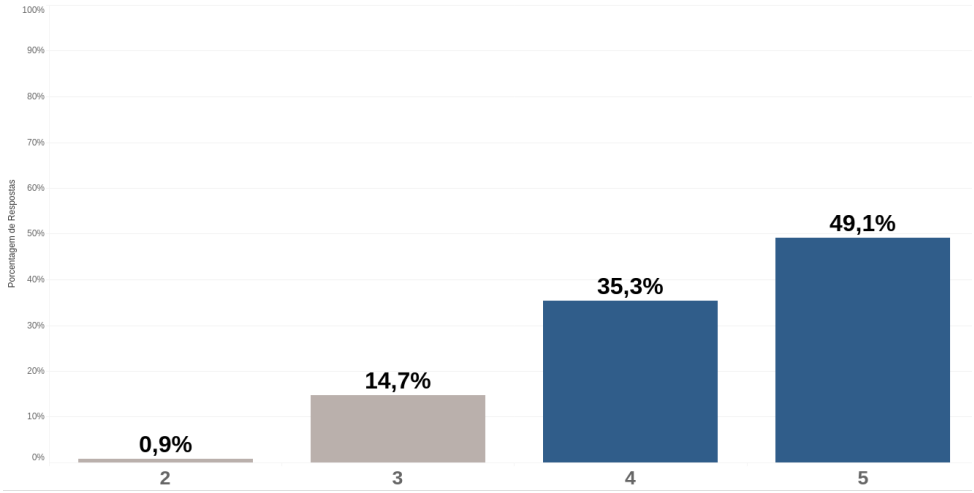

Figura 2: De 1 a 5, o quanto você se preocupa com sua privacidade digital?

A pergunta seguinte concerne à relação entre privacidade e conveniência. Como visto, quanto maior a conveniência, menor tende a ser a privacidade digital do usuário. Sendo assim, a maioria dos questionados respondeu que prefere que o serviço preserve seus dados e mantenha sua privacidade, mesmo que não seja tão conveniente de utilizá-lo. Disso se depreende que os usuários aparentemente preferem a privacidade à conveniência.

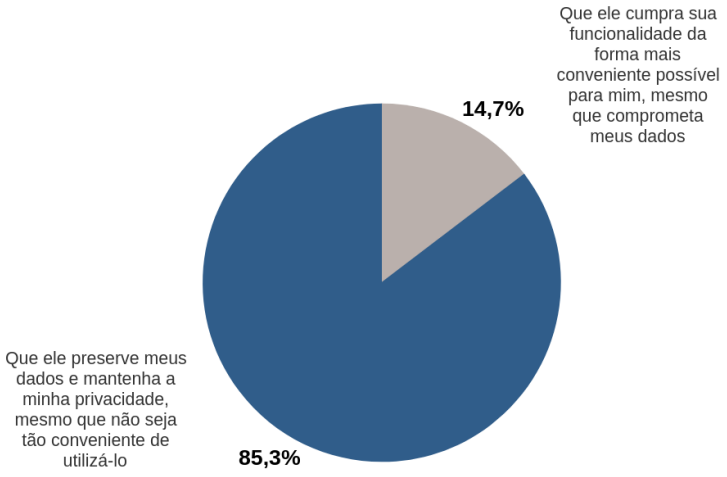

Figura 3: O que você considera mais importante em um serviço online?

Em seguida, a pergunta diz respeito aos termos de uso dos softwares utilizados. Os termos de uso correspondem ao princípio do consenso e escolha anteriormente abordado; o fato de grande parcela das pessoas nunca lerem os termos de uso significa que sua efetividade na transmissão do consenso é questionável, haja vista que não há como consentir com o que se desconhece. Há outras formas de se obter

consenso, que são pouco utilizadas pela maioria das organizações, como o uso de ícones para apresentar os dados que serão coletados e uma linguagem mais acessível, na escrita do documento. A figura 4 demonstra que há um número significativo de pessoas que não leem esses termos:

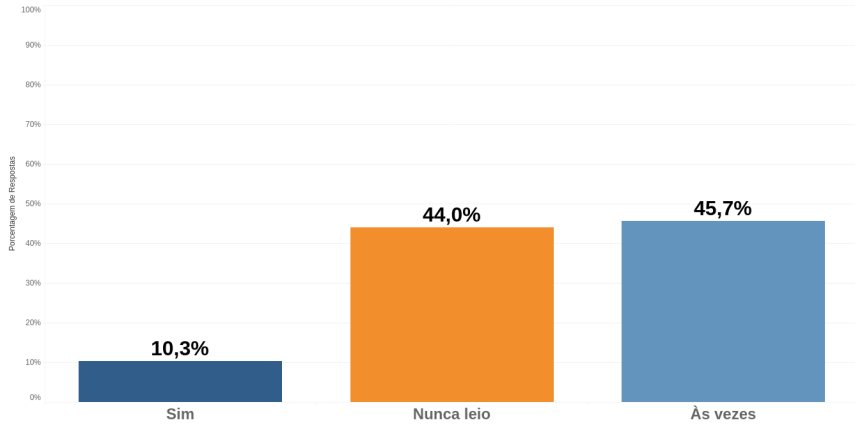

Figura 4: Você lê os termos de uso dos serviços/aplicativos que utiliza?

Na sequência, dado interessante demonstra que apenas aproximadamente 20% das pessoas utilizam software livre (ou sabem que utilizam). Isso demonstra que poucos que estão preocupado com sua privacidade digital conhecem a importância de se utilizar software livre para preservá-la; isso, em certo grau, aponta para uma falha na preservação da privacidade por parte dos usuários, parcialmente em razão do desconhecimento dessa modalidade de software. A figura 5 apresenta que mais da metade dos questionados não utiliza software livre:

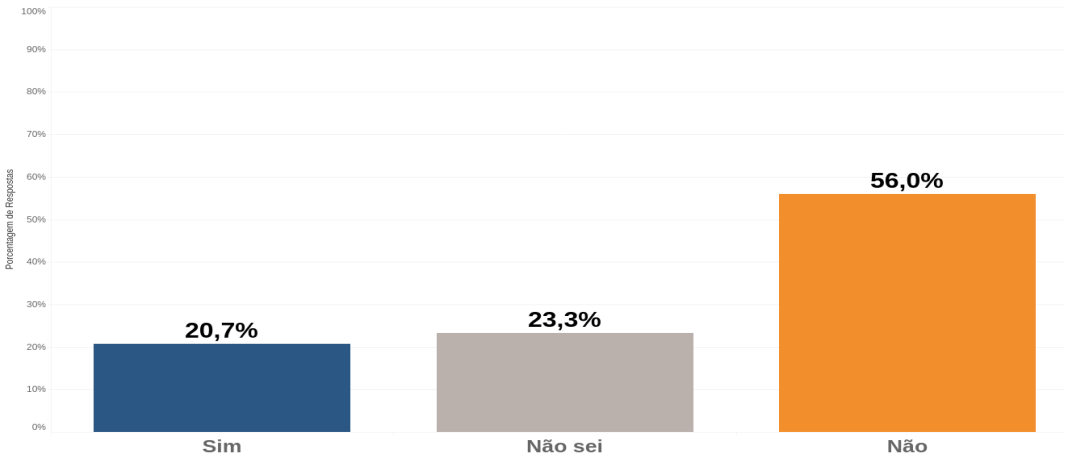

Figura 5: Você utiliza algum software livre? Exemplo: Gnu/Linux.

Para compreender melhor a utilização de softwares por parte dos questionados, a pergunta seguinte concerne ao sistema operacional utilizado. Nessa conjuntura, o esperado é que as pessoas utilizem um sistema operacional livre, como o GNU/Linux

ou Open BSD; a escolha de sistemas operacionais como MacOS, Windows e ChromeOS favorecem a coleta de dados e vigilância do usuário, de modo que seu uso representa uma escolha inadequada, do ponto de vista da privacidade. Como se depreende da figura 6, por volta de 13% dos questionados utilizam Gnu/Linux, em contrapartida, quase 90% utilizam o Windows. Trata-se de uma pergunta de múltipla escolha, razão pela qual um usuário de Windows pode utilizar outro sistema operacional também. Dos que responderam não utilizarem software livre, aproximadamente 90% utiliza Windows, seguido de Chrome OS e por fim Mac OS. Entre os preocupados em alto grau com a privacidade 14% alegaram utilizar Gnu/Linux. É perceptível que o uso de sistemas operacionais proprietários (em laranja) é mais significativo entre os questionados.

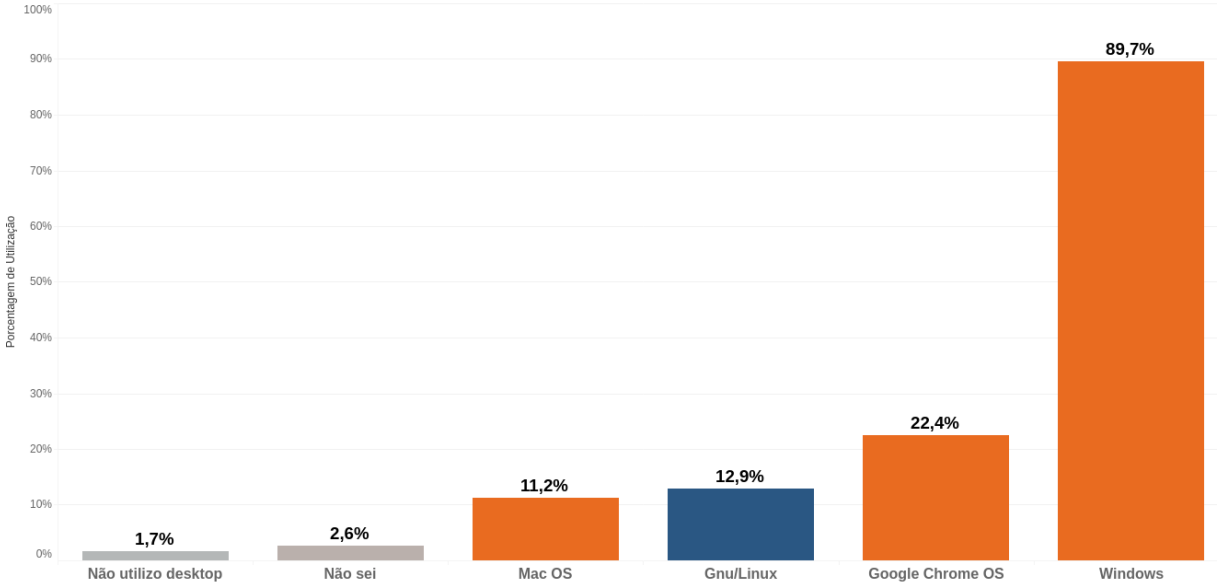

Figura 6: Qual(is) destes sistemas operacionais de desktop você utiliza?

Quanto ao sistema operacional utilizado no *smartphone* do questionado, a privacidade é ainda menos resguardada. Somente dois usuários não utilizam o IOS e Android padrão. O uso de dois sistemas operacionais tende a ser uma prática de privacidade superior, contanto que o usuário segregue os dados em cada um deles (exemplo: um para o trabalho, outro para uso pessoal). Ainda assim, o usuário que preza pela privacidade digital em realidade deve se distanciar desses dispositivos, pois todos se conectam à rede de telefonia, de modo que é possível descobrir a localização de cada usuário, com certa facilidade. O único questionado, que utiliza uma custom ROM de android não marcou estar preocupado em alto grau com a privacidade digital, mas sim em nível médio. A figura 7 demonstra a grande presença de IOS e Android entre a imensa maioria dos usuários:

A seguir, os usuários são questionados a respeito do uso de navegadores. Os navegadores na figura 8 são em sua maioria violadores da privacidade digital, os que

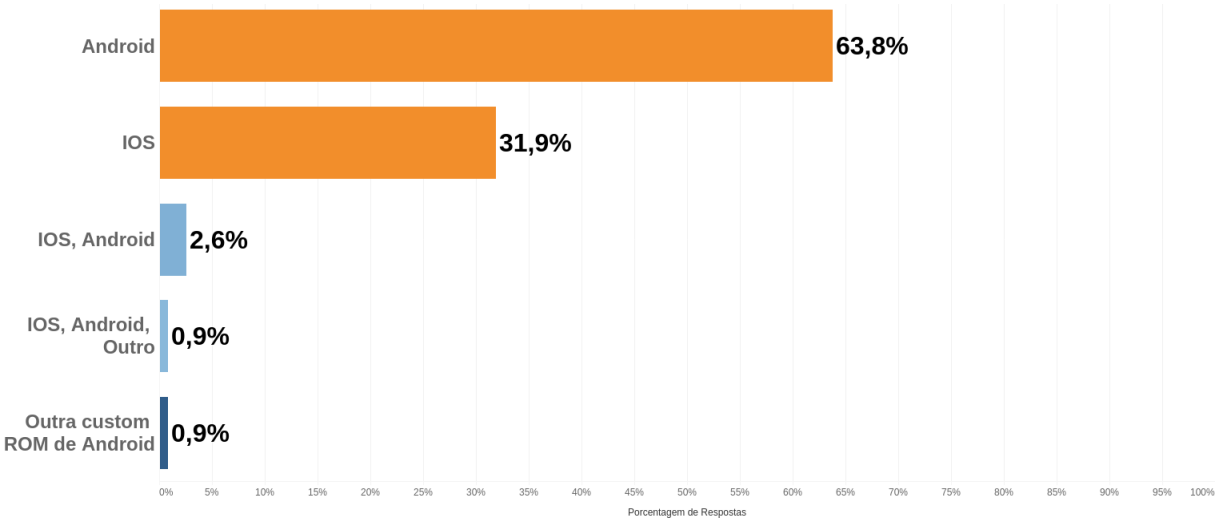

Figura 7: Qual(is) destes sistemas operacionais de *smartphone* você utiliza?

estão em laranja possuem algum grau de código fechado, Brave, em azul claro, pode ser mitigado ao ponto de se tornar pouco violador. O Tor é, em tese, o mais seguro dentre os respondidos, uma vez que mascara o IP de quem navega, por meio de sua network. Já o Firefox, em cinza na imagem, é possível de ser mitigado ao ponto de não ser um violador de privacidade, porém, por padrão, ele viola a privacidade. O navegador que mais viola a privacidade dentre os citados é o Google Chrome, na medida em que possui código parcialmente fechado, potencialmente recorda fala no ambiente, rastreia o histórico de pesquisa do usuário, profila o uso computacional, salva as senhas dos usuários em seus servidores, entre outros. Apesar disso, o Chrome é de longe o mais utilizado, na faixa dos 95% dos usuários.

Cabe aqui um adendo, uma vez que é possível múltipla resposta nessa pergunta, um usuário pode segregar o uso de navegadores, usando o Chrome para trabalho, por exemplo, e outro navegador para uso pessoal. Foi o que 44% dos que utilizam Chrome responderam, estes afirmaram diversificar seus navegadores, de modo que a violação à privacidade é mitigada. Ainda assim, as funcionalidades maliciosas deste navegador permanecem ativas, por conseguinte, muitos se preocupam com a privacidade, mas poucos efetivamente convergem a ela em seu uso digital.

A seguir há outra pergunta crítica do ponto de vista da privacidade. A pergunta concerne ao uso de redes sociais; como visto anteriormente, esses softwares estão repletos de violadores de privacidade, nesse sentido, seu uso é extremamente prejudicial para a preservação da privacidade digital. Donde, a resposta mais condizente à preservação da privacidade digital é nenhuma. Consoante as respostas, em razão da múltipla escolha, cada usuário tem média aproximadamente 4 redes sociais. Quanto mais redes sociais, maior tende a ser a exposição individual; apenas 2% dos que responderam não utilizam rede social. A figura 9 apresenta as redes sociais utilizadas

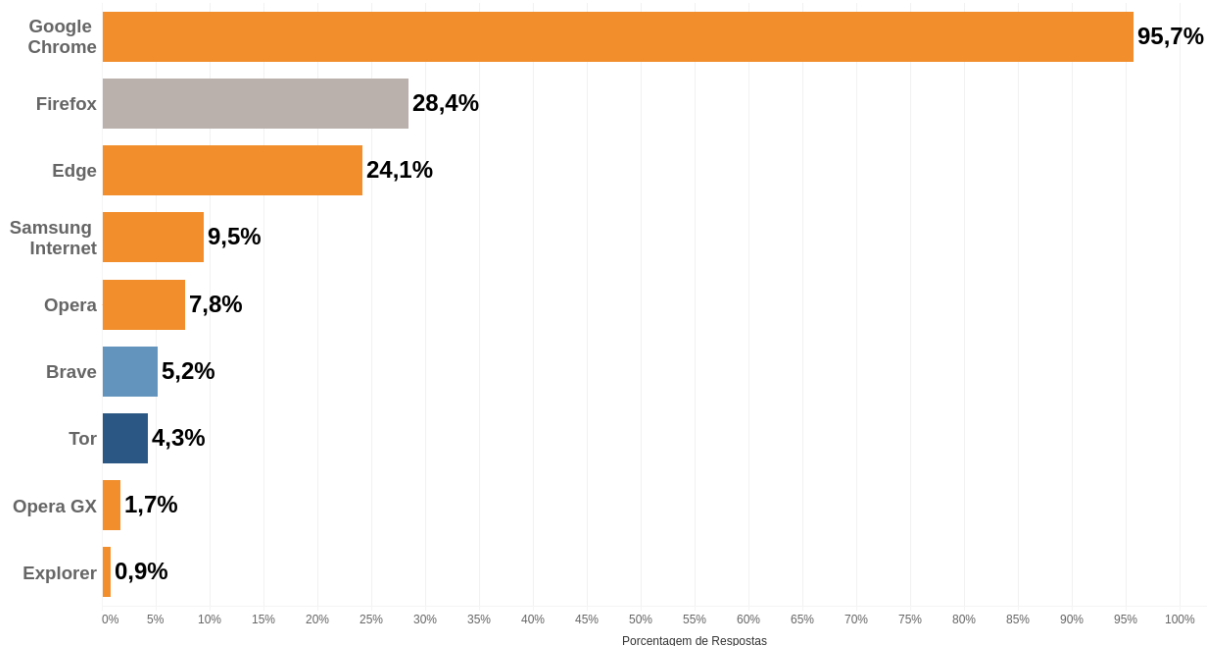

Figura 8: Qual(is) destes navegadores você utiliza?

pelos usuários, as redes sociais em azul claro, apesar de coletarem dados podem ser usadas no navegador de forma mais privada. Dos que utilizam redes sociais, a maioria (aproximadamente 66%) mantém suas contas privadas, enquanto o restante as mantém públicas.

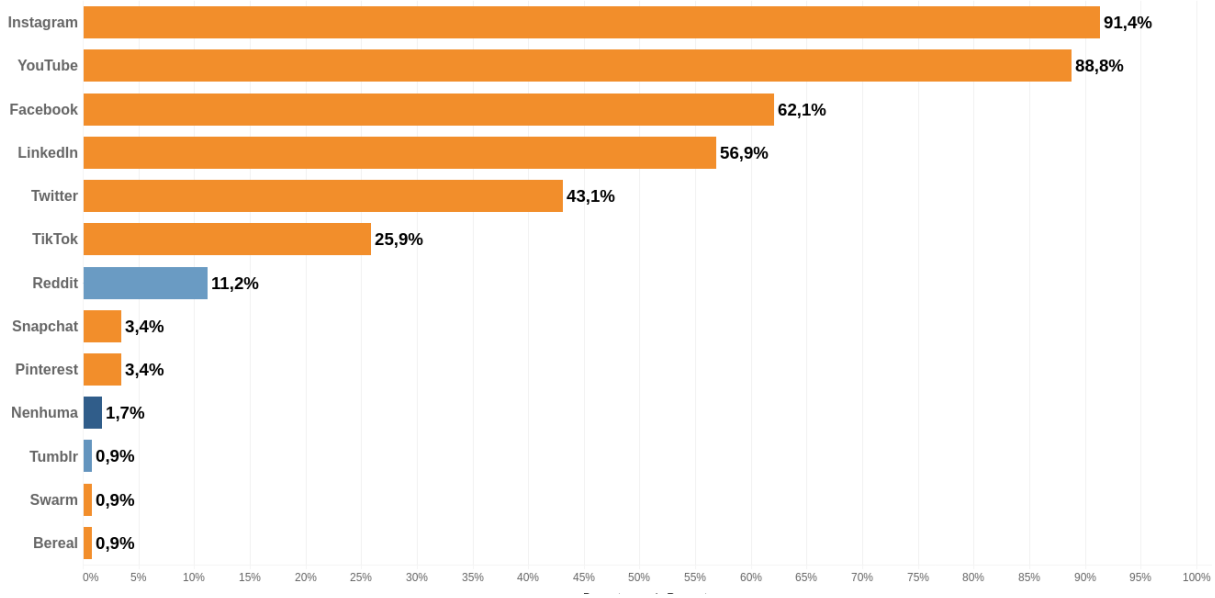

Figura 9: Qual(is) destas redes sociais você utiliza?

Não obstante o alto uso de redes sociais, apenas 11,2% retiram os metadados de suas fotos. Os metadados, ou dados provenientes do formato EXIF, são dados intrínsecos à foto retirada com câmeras mais modernas, que armazenam o local aonde

esta foi retirada, o horário dela, bem como outras informações. Esses dados, ao serem postados na rede social, podem ser sensíveis e prejudicar a privacidade digital do usuário. Aproximadamente metade dos questionados afirma que não retira tais metadados, e 1/5 não sabe a respeito, como se depreende da figura 10.

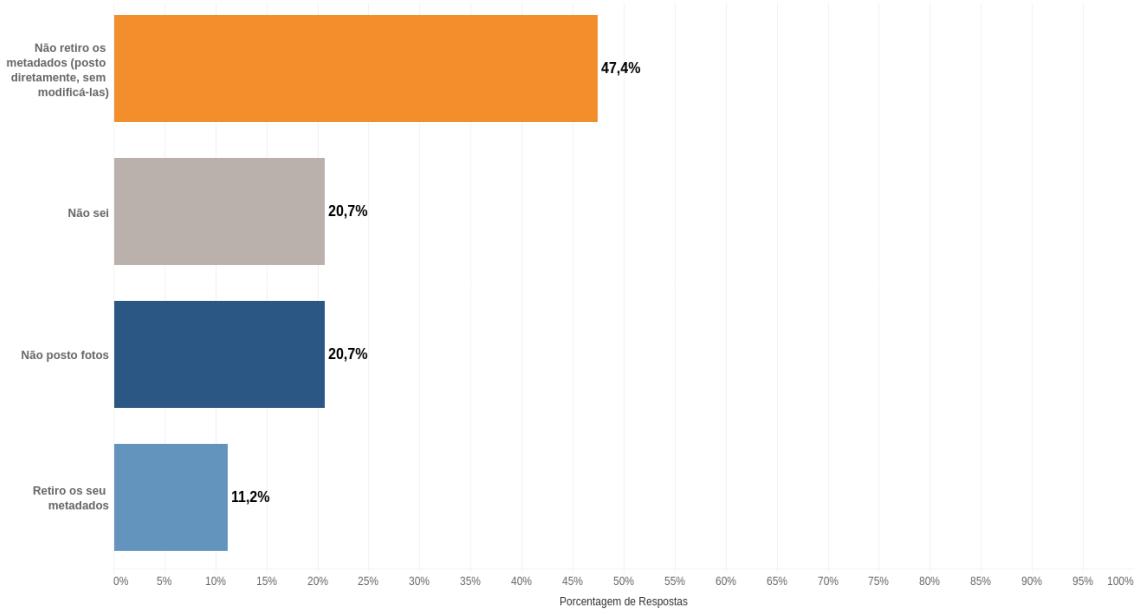

Figura 10: Quanto às fotos que você publica em sites, redes sociais e aplicativos de mensagens

Em seguida, tem-se o uso de aplicativos de mensagem por parte dos usuários. Todos os usuários questionados utilizam WhatsApp, que é um aplicativo de mensagem da Meta, uma empresa com notório histórico de coleta de dados. De fato, o uso de aplicativos de mensagem em geral está condicionado ao ambiente social da pessoa, isto é, se a maioria utiliza WhatsApp, por consequência, outros utilizam também. Apesar disso, no que tange à privacidade digital, a utilização do Telegram é benéfica, apesar de possuir um servidor centralizado. SMS pode ser conveniente, na medida em que o usuário utilize um *dumbphone*, um telefone sem as funcionalidades abrangentes de um *smartphone*, em que não há aplicativos de mensagem, somente o SMS direto. Ocorre, porém, que o SMS não é criptografado e pode ser facilmente interceptado, o que prejudica a privacidade digital em outra via. Messenger é da Meta, o que o torna análogo ao WhatsApp, em termos de coleta. Já o Signal e o Matrix são os mais seguros da 11, visto que possuem servidores descentralizados, apesar de serem menos utilizados.

Em sequência, trata-se do uso de VPN pelos usuários. Usar um VPN não implica em privacidade, uma vez que os dados do usuário perpassam o servidor da empresa de VPN, de modo que a segurança dos dados que trafegam esse servidor são correlatas à segurança que se deposita na empresa que presta o serviço de VPN. Além disso,

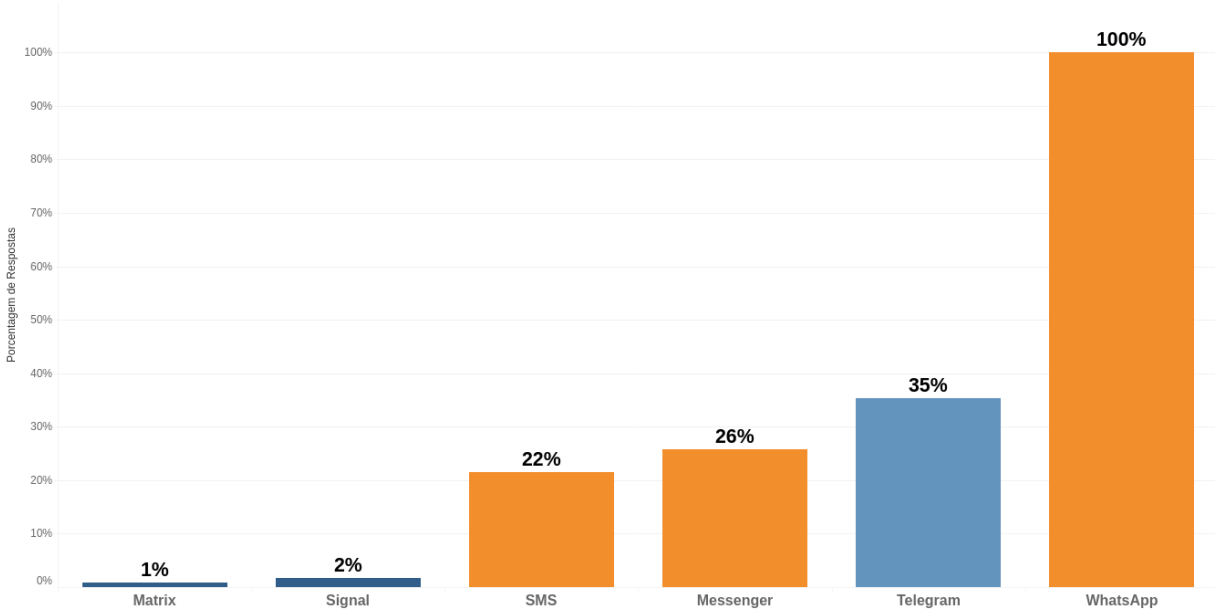

Figura 11: Qual(is) destes aplicativos de mensagem você utiliza?

muitas empresas de VPN exigem cadastro de diversos dados sensíveis, de modo que é possível que o tráfego seja redirecionado ao perfil real da pessoa que utiliza o serviço. Há uma melhora, em certa medida, da privacidade do usuário, na medida em que o servidor vai requisitar acesso aos domínios, não o usuário, sendo assim, seus *requests* estarão mesclado com os de outros usuários; além disso, o VPN criptografa a conexão do usuário, o que pode ser conveniente para redes abertas. Uma empresa que é mais segura quanto aos dados pessoais é a Mullvad VPN, que possibilita pagar seu serviço por meio de Monero, uma criptomoeda focada na privacidade do usuário, não rastreável. No entanto, nenhum dos aproximadamente 20% que utilizam VPN contrata o serviço dessa organização, como se percebe na figura 12

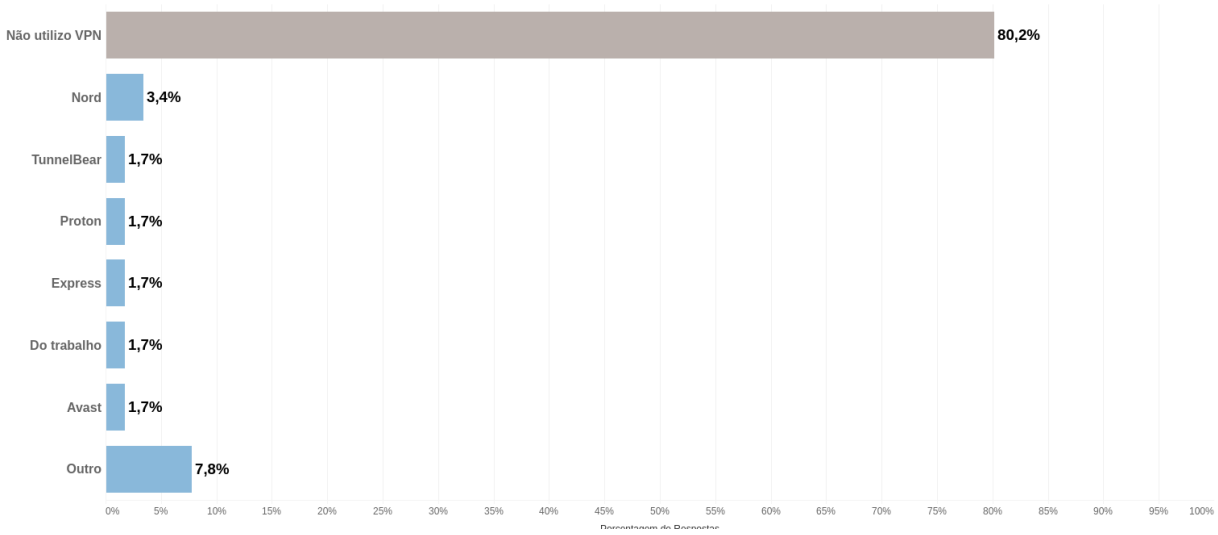

Figura 12: Você utiliza algum serviço de VPN? Se sim, qual?

O armazenamento em nuvem é uma forma conveniente de se armazenar dados. Essa conveniência vem com o preço de confiar no servidor em que eles são armazenados; quase 90% dos questionados responderam que utilizam o Google Drive e quase 30% utilizam o iCloud, enquanto por volta de 40% utiliza o One Drive. Nesse contexto, quem detém os servidores desses 3 serviços são, respectivamente, Google, Apple e Microsoft, ou seja, não necessariamente os dados ali armazenados serão resguardados, como foi abordado anteriormente no que tange às fotos carregadas no iCloud. Não utilizar armazenamento em nuvem é a melhor opção para preservar a privacidade digital, caso o usuário não consiga ter um servidor de confiança, ao ponto de estabelecer seu próprio serviço de cloud com o Nextcloud ou outro software. A figura 13 demonstra a dominância que grandes empresas de tecnologia possuem nesse segmento.

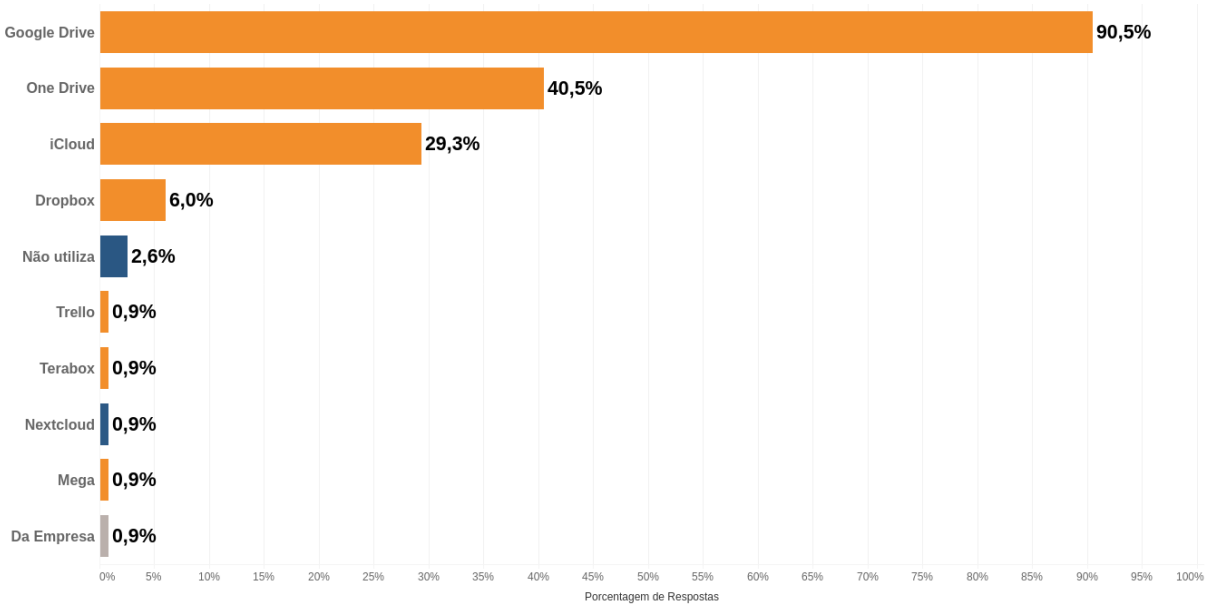

Figura 13: Você utiliza algum serviço de armazenamento em nuvem?

Em seguida, o questionados é questionado a respeito de qual mecanismo de pesquisa utiliza. Nesse segmento, 81% dos questionados utilizam apenas o Google como mecanismo de pesquisa e apenas 2% não utilizam o Google, em combinação com outro mecanismo de pesquisa. Considerando quem utiliza mais de um mecanismo de pesquisa, o Google é utilizado por 98,3% dos questionados. DuckDuckGo é um navegador mais próximo da privacidade, no entanto, assim como o Google, o CEO afirmou manipular resultados de pesquisa em favor da Ucrânia, na recente guerra entre a Rússia e a Ucrância. Yahoo e Bing são semelhantes ao Google, pois vendem informações do usuário para empresas de publicidade, rastreiam o usuário, no caso do Yahoo, o histórico de internet do usuário é enviado ao ecossistema Oath, que viola a privacidade do usuário. Brave Search é um mecanismo de pesquisa mais privado

e isento, pois não filtra ativamente as pesquisas do usuário, de modo a demonstrar apenas alguns resultados. Starpage é um mecanismo de pesquisa que apresenta os resultados do Google, porém, sem o rastreamento e violação de privacidade intrínseco. Qwant também é um mecanismo de pesquisa com foco em privacidade, no entanto, está indisponível no Brasil, sendo seu uso viável com VPN. Por fim, o SearX é possívelmente o melhor mecanismo, uma vez que agrega resultados de outros mecanismos e os servidores são descentralizados, como é possível ver na figura 14, os mecanismos de pesquisa tradicionais ainda são os mais utilizados, o que denota uma preferência, na prática, por conveniência à privacidade.

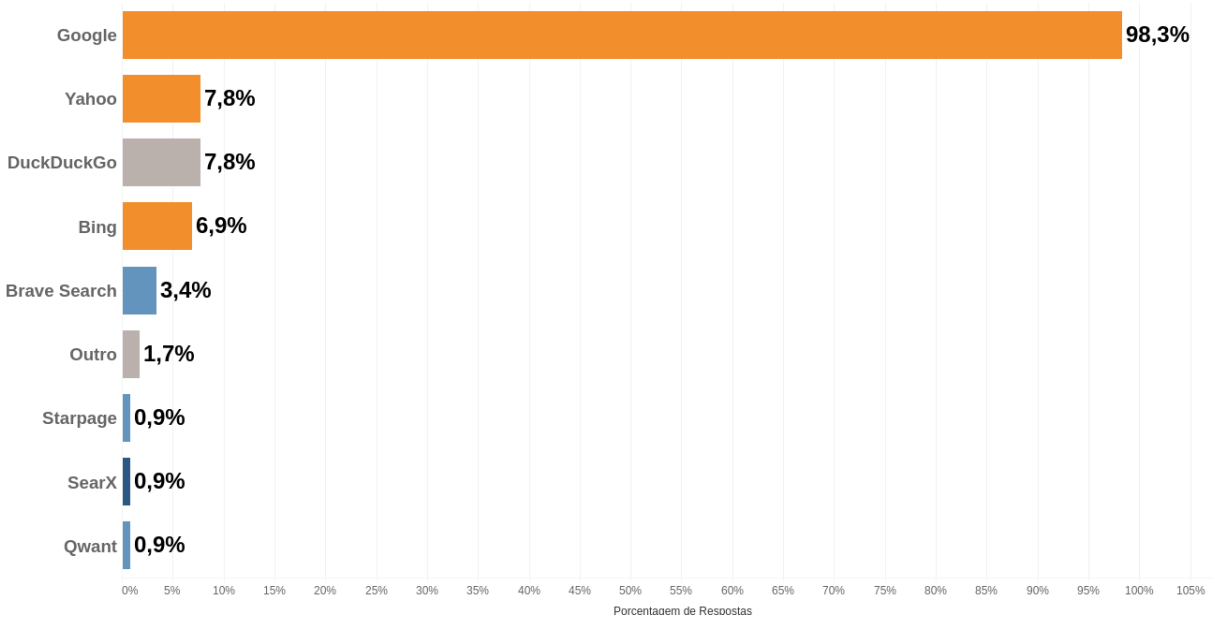

Figura 14: Qual(is) destes mecanismos de pesquisa você utiliza?

Em pergunta a respeito da preferência do uso da localização, a maioria dos questionados prefere a granularização: 68,1% das respostas foi no sentido de preferir que os aplicativos utilizem apenas o necessário (15), como país, estado e município, ao invés da localização exata. De fato, em grande parte o uso de *smartphone* dificulta essa granularização, pois é muito comum que essa localização seja coletada no local exato. A granularidade da localização minimiza a coleta de dados a somente o que é necessário pelo serviço.

Em seguida, para compreender a relevância dada à política de cookies pelos usuários, perguntou-se que medida este toma diante de um pedido de permissão para cookies. Há cookies que são úteis para o uso da web, como aqueles que guardam a senha do usuário, ou informações que facilitam a navegação em determinados sites. Porém, uma boa parte dos cookies serve para rastreamento na web, de modo que bloqueá-los ou não aceitar as políticas de cookies é uma medida que preserva a privacidade do usuário. 64,6% dos questionados aceitam a política de cookies, mas

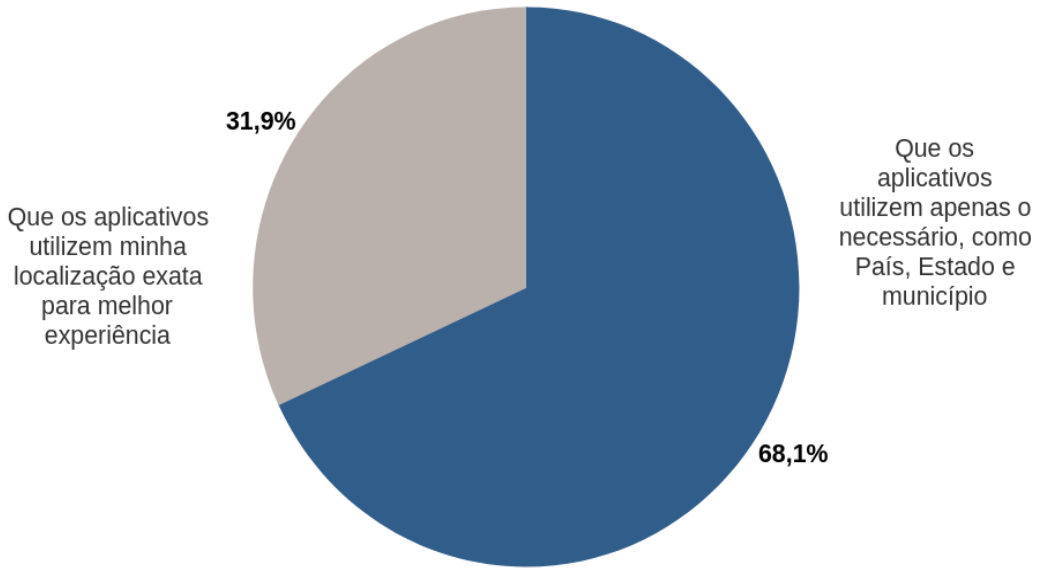

Figura 15: Quanto à localização, você prefere

apenas 15,5% dos que responderam realmente leram as políticas de cookies. Houve, inclusive, uma resposta escrita que aborda o tema considerando extremamente inconveniente de ter essa política de cookies em cada site que acessa. A figura 16 demonstra que uma parcela grande dos questionados evita cookies, na ordem dos 35%:

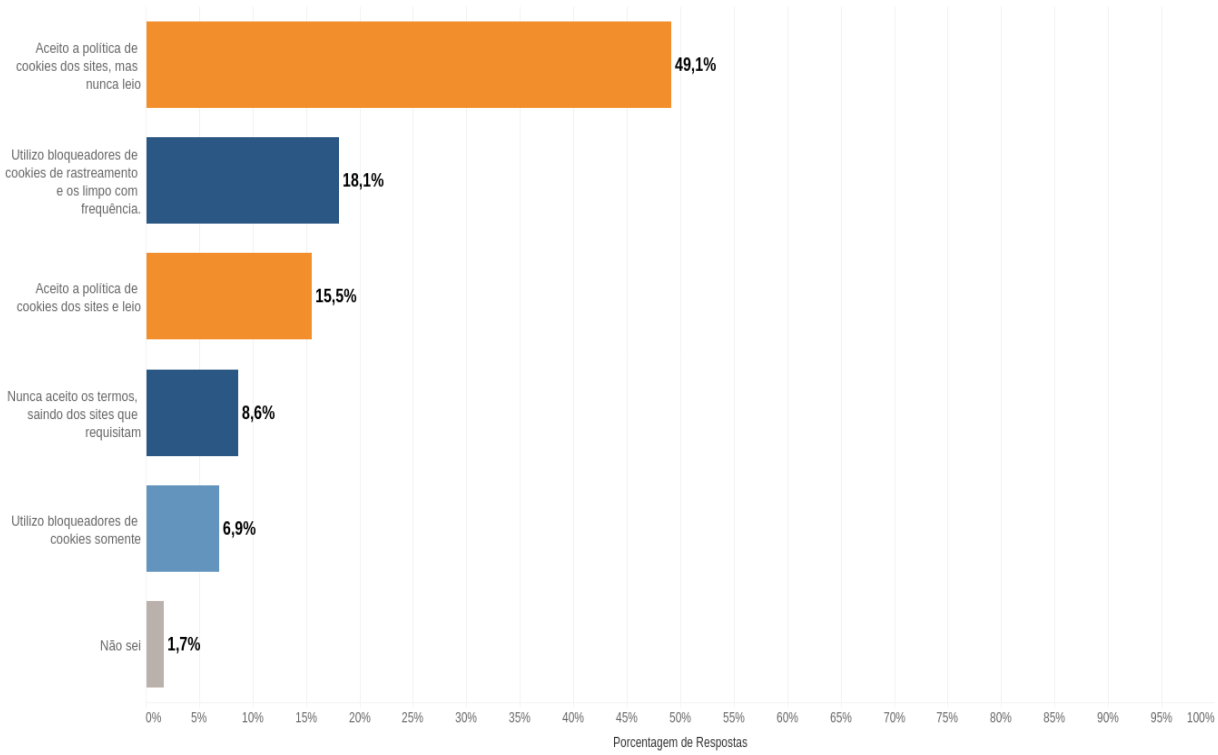

Figura 16: Quanto a cookies

A seguir, para distanciar um pouco da temática de coleta de dados, são abordadas medidas de segurança do usuário. Nessa conjuntura, apenas 25% dos questionados criptografam seus discos rígidos, que armazenam boa parte de seus dados pessoais. A não criptografia permite o acesso livre aos dados do usuário, contanto que se tenha acesso ao disco rígido. Entre os usuários que possuem preocupação alta com a privacidade digital, a maior parte deles, 35,1%, criptografam seus discos rígidos. Uma boa parte dos usuários não possuem essa prática, assim como uma boa parte dos questionados desconhece da criptografia, que é uma prática de suma importância para preservar a integridade de dados em disco rígidos, como demonstra a figura 17:

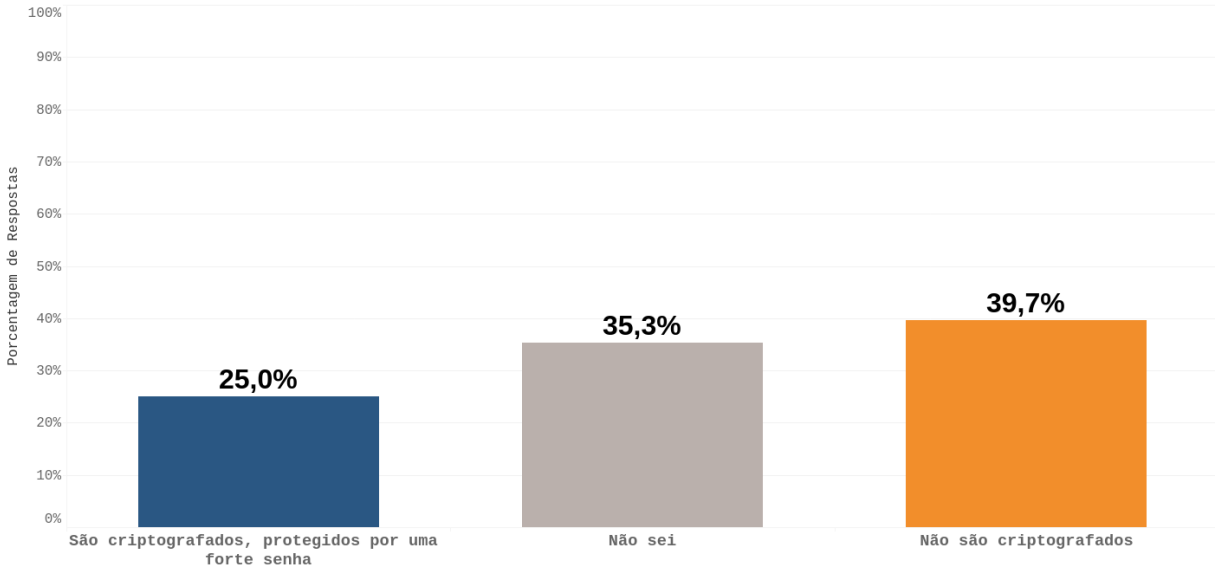

Figura 17: Os discos rígidos de seus dispositivos

Comprovando uma boa prática difundida, a maioria dos questionados relatam que os sites os orientam para a criação de uma senha forte, que contenha caracteres especiais e seja minimamente extensa. É o que se depreende da figura 18, em que 74,1% afirma que são orientados a criar uma senha forte:

Apesar disso, apenas 12,9% dos questionados afirmaram nunca usar a mesma senha. Por volta de 25%, porém, afirmaram que sempre utilizam a mesma senha, conforme a figura 19, o que pode gerar uma falha de segurança significativa, na medida em que o e-mail possui a mesma senha do que outros sites, que podem vazar essas senhas, sem o devido procedimento de segurança, devido ao armazenamento incorreto, sem hash e não *salted*, desses dados.

Um fator que auxilia na mitigação dessa prática incorreta de segurança é a utilização de autenticação de múltiplo fator. A figura 20 demonstra que quase 70% utilizam essa autenticação, de modo que não basta que um invasor saiba a senha de sua conta; deve este obter acesso geralmente ao número de telefone do alvo, ou a outro e-mail, o que dificulta uma possível invasão nas contas do questionado.

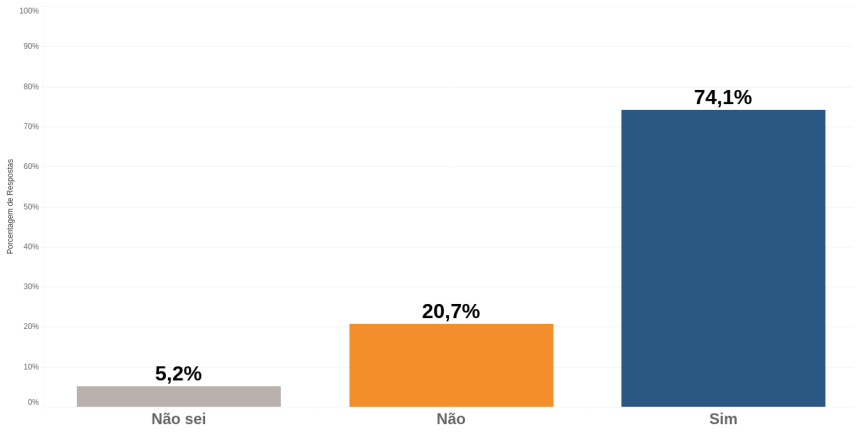

Figura 18: Os sites ou aplicativos que você utiliza auxiliam na criação de uma senha forte?

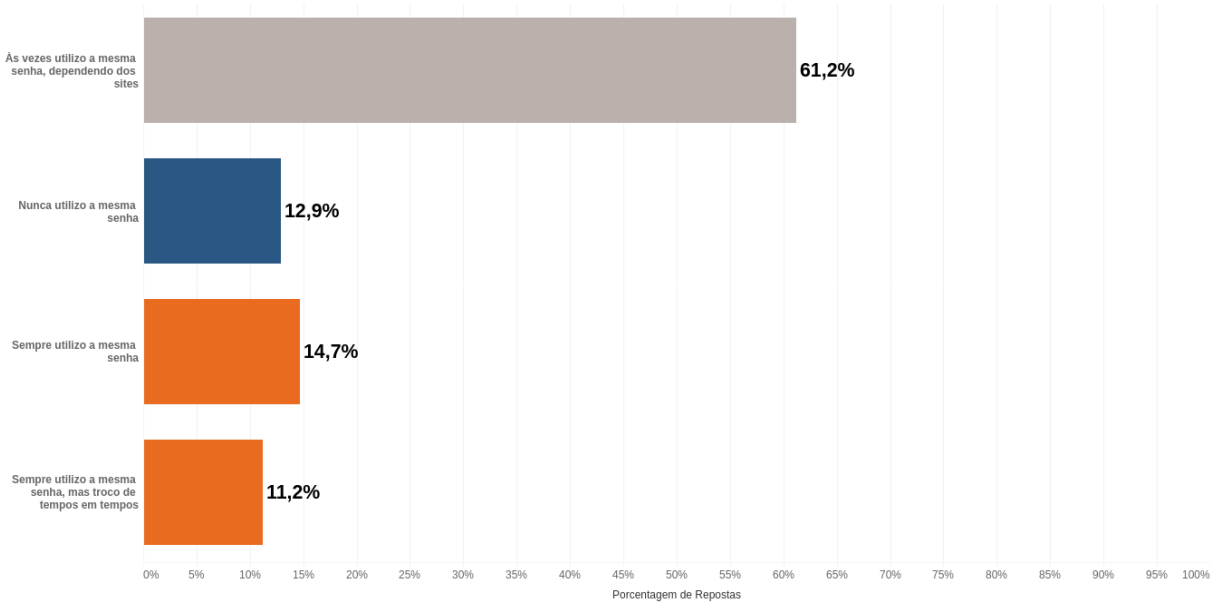

Figura 19: Com relação às suas senhas

Para minimizar a coleta de dados e o profilamento, recomenda-se que os usuários digitais utilizem a conta do Google, Facebook ou Apple para entrar em serviços. É extremamente conveniente entrar com apenas um clique, sem precisar fazer um cadastro em determinado site, por isso que a figura 21 demonstra que mais de 85% dos questionados utilizam essa forma de cadastro nos sites que acessam. Ao utilizar essa forma de cadastro sua privacidade é severamente diminuída, pois todos os dados proveniente daquele serviço cadastrado serão facilmente atrelados à identidade real do usuário. Diante disso, para preservar a privacidade digital, deve o usuário utilizar o máximo possível de e-mails, inclusive e-mails temporários como os fornecidos pelo Guerrilla Mail, isso evita spams demasiados e auxilia o usuário a manter sua identidade real preservada.

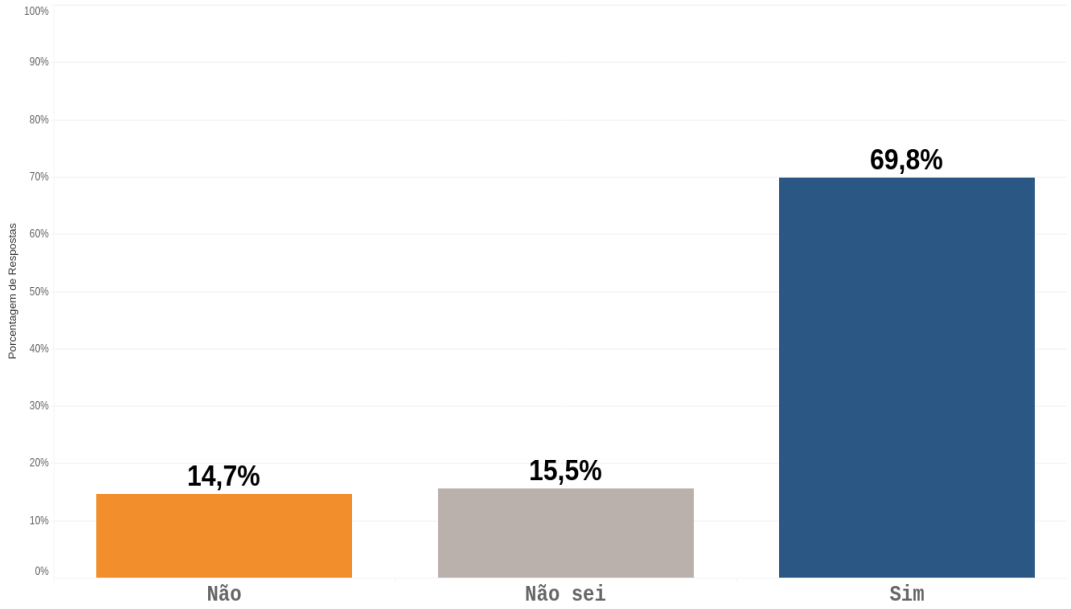

Figura 20: Você utiliza autenticação de múltiplos fatores para suas contas?

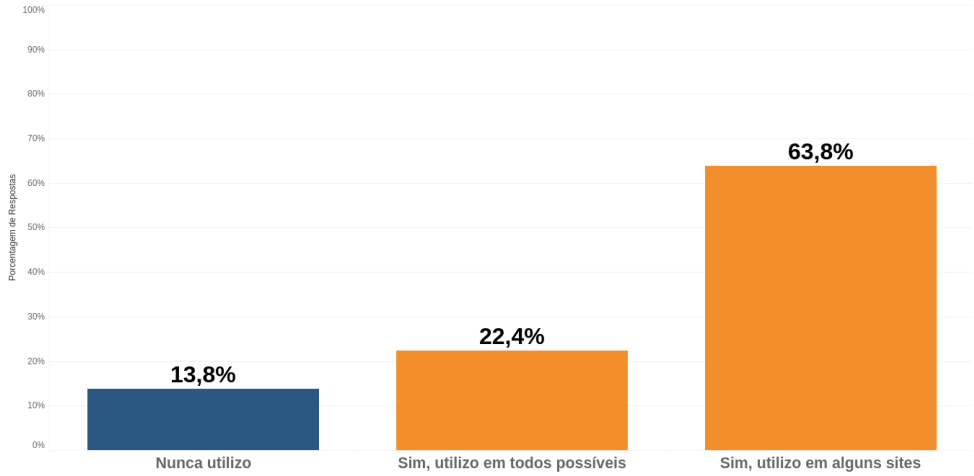

Figura 21: Você utiliza sua conta do Google, Facebook ou Apple para entrar em sites?

Uma outra autenticação conveniente é a biometria. A maioria dos usuários não se sente incomodado ao utilizar biometria como forma de autenticação, no entanto, mais de 60% destes que não se sentem incomodados temem que seus dados biométricos sejam vazados. No outro espectro, dos 21% que temem utilizar biometria como forma de autenticação, mais de 95% deles teme que seus dados biométricos sejam vazados (22). Diante de um vazamento de dados, as respostas dos questionados foram quase unânimes em afirmar que a organização deve ser responsabilizada (97,4%). No Brasil, ainda é incipiente tal responsabilização, no entanto, diversos processos nesse sentido tramitaram e tramitam em cortes como as dos Estados Unidos.

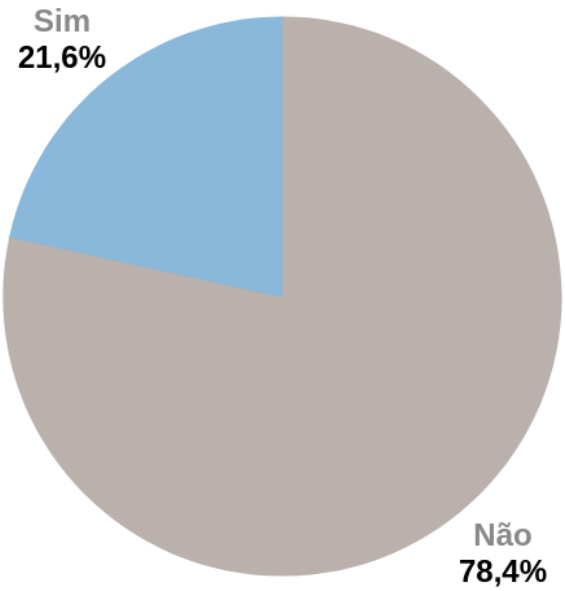

Figura 22: Você se sente incomodado quando tem que utilizar biometria como forma de autenticação (impressão digital, rosto, olhos, etc.)?

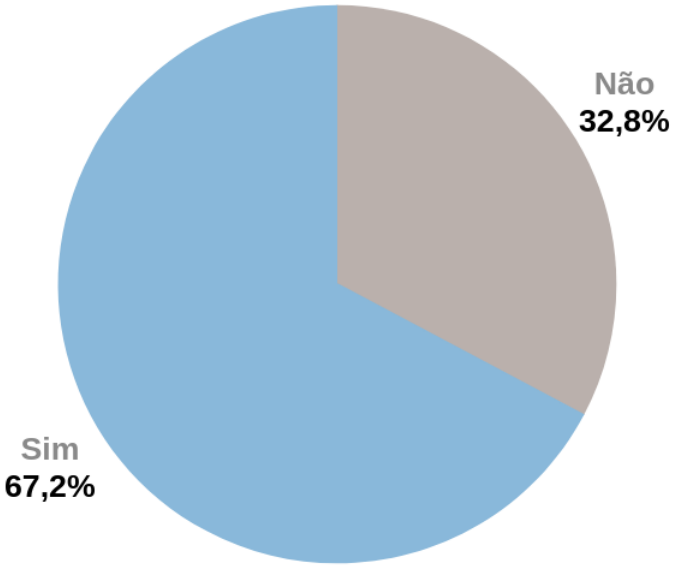

Figura 23: Você teme que seus dados biométricos possam ser vazados?

Por fim, há uma pergunta concernente ao uso de câmeras de vigilância. A utilização desses dispositivos é pouco presente entre os questionados, apenas 16,4% responderam que os utilizam (24). Quase 1/4 dos que responderam se preocupar em grau máximo com sua privacidade, porém, utilizam tais dispositivos, o que pode significar uma relação entre privacidade e valor à segurança. A câmera de vigilância por si só não é prejudicial à privacidade do indivíduo, no entanto, os servidores que muitas vezes recebem os dados de imagem podem se tornar violadores de pri-

vacidade, pois costumam coletar dados de seus usuários.Muitos deles, além disso, exigem conta para acessar a imagem das câmeras de segurança, o que circunscreve o uso da câmera de vigilância a proporcionar uma identidade ao fornecedor do serviço.

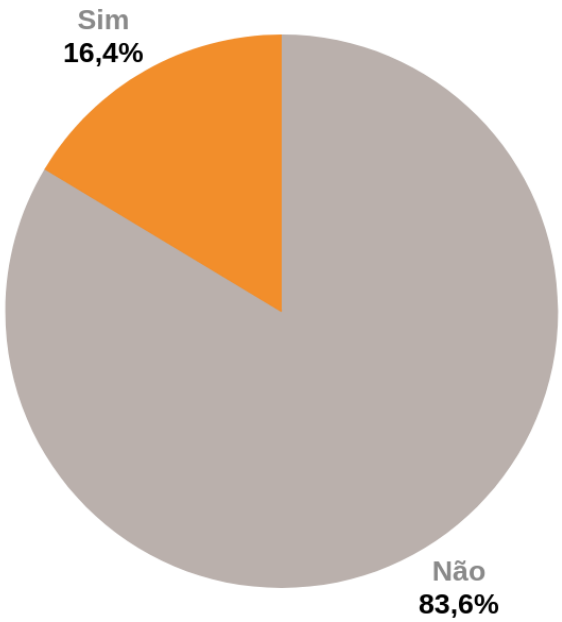

Figura 24: Você utiliza sistema de segurança por câmeras?

Através da pesquisa exploratória anteriormente abordada, muitos resultados foram apresentados. Em síntese, os dados analisados demonstram a importância que a privacidade digital possui na vida dos questionados. Nem sempre, porém, as práticas dos usuários são condizentes à importância atribuída a este direito. As razões para essa dissonância apontam para um desconhecimento generalizado das violações realizadas nos serviços utilizados pelos usuários digitais.

Frequentemente, estudos a respeito do uso da internet são veiculados, de modo a evidenciar os danos provenientes de sua utilização exacerbada (GREENFIELD, 2007). Trata-se de uma temática de estudo já abordada, razão pela qual as pessoas tendem a compreender que o uso excessivo da internet resulta em consequências negativas, como o vício e a desconexão com a realidade. A coleta de dados, via software, no entanto, é raramente conhecida pelos usuários, mesmo sendo um fato notório desde os documentos revelados por Snowden. Nesse contexto, há uma preocupação inata das pessoas no que tange a sua privacidade digital, mas estas desconhecem a que extensão as violações ocorrem.

Isso resulta em ações contraditórias no meio digital. Não há como uma pessoa valorizar em grau máximo sua privacidade digital e, ao mesmo tempo, possuir 4 redes sociais distintas, utilizar aplicativos de mensagens orientados à coleta de dados e sistemas operacionais não livres. Soma-se a essa contradição a conveniência que certos aplicativos proporcionam ao usuário, de modo que deixá-los por outro que pos-

sui menos funcionalidades pode ser uma verdadeira dificuldade. É evidente, porém, que dada a tamanha valorização da privacidade digital, um usuário estaria disposto a modificar seu ambiente digital de modo a aceitar aplicativos com menos funcionalidades em troca da preservação de seus dados: muitos responderem afirmativamente, mas, ao mesmo tempo, não se observa que estes tenham modificado suas práticas digitais 3.

Há, por conseguinte, valorização da privacidade por parte dos usuários digitais questionados. Não há, por outro lado, práticas verdadeiras de preservação da privacidade digital, provenientes de grande parte dos questionados. Nessa conjuntura, a principal mudança no cenário de coleta de dados deve partir de quem utiliza o serviço, isto é, este deve estar ciente de que está utilizando um serviço, cujas funcionalidades maliciosas comprometem sua privacidade. Disso se conclui que, para muitos, ainda é mais importante aderir a um software que constantemente coleta dados pessoais, do que preservar a privacidade digital individual. Deve-se ressaltar, no entanto, que quanto mais um indivíduo prezar pela sua privacidade, mais outras pessoas, por consequência, também desfrutarão da privacidade, uma vez que grande parte da coleta de dados se estende a outras pessoas com as quais o usuário digital interage física e virtualmente; donde, a fundamental importância de que a privacidade digital não seja apenas circunscrita a alguns, mas seja uma prática intrínseca à ação digital.

6 Conclusão

O objetivo deste trabalho foi analisar, sob o ponto de vista de usuários de serviços digitais, se suas preocupações quanto a preservação da privacidade digital condizem com seus conhecimentos e ações práticas no mundo digital. Para isso, este trabalho analisou a percepção de um conjunto de 116 pessoas a respeito da preservação e violação da privacidade digital, a partir de perspectivas como usuários de serviços digitais. Com ênfase nas práticas comumente adotadas pelos usuários digitais respondentes desta pesquisa, conclui-se que a maioria dos questionados se preocupa em alto grau com a privacidade digital, no entanto, estes demonstram ser pouco proativos para a preservarem, pois suas próprias escolhas no ambiente virtual acabam fragilizando a preservação da sua privacidade.

Através deste trabalho foi possível abordar um tema de crescente importância. Adstrito à constante digitalização da sociedade, outros problemas surgem, as barreiras físicas se rompem, e as relações se tornam mais dinâmicas e instantâneas. A privacidade que antes era somente um conceito presente em um ambiente físico e real, estendeu-se a um ambiente digital e virtual, em que os dados de cada indivíduo podem ser coletados, transformados e comercializados.

Nesse contexto inovador, diversas organizações pioneiras surgem com a finalidade de explorar um novo nicho de mercado. Esse nicho envolve o conhecimento e profilamento dos indivíduos que navegam no ambiente virtual, em seus mais variados dispositivos. Essas organizações coletoras de dados utilizam das mais variadas técnicas, que podem violar a privacidade digital dos usuários, para adquirir mais informações valiosas para diversos fins, como marketing, vigilância governamental e criação de *cohorts*.

Para preservar a privacidade que gradativamente se tornou um direito no ordenamento jurídico brasileiro diversos agentes se prontificam: entidades estatais, organizações privadas e os próprios usuários. As regulações, por parte dos governos, estão sendo aplicadas em alguns locais, enquanto em outros permanecem apenas formalidades. As medidas oriundas de organizações privadas são, em geral, frutíferas quando emergentes de uma comunidade que valoriza a privacidade digital; quanto àquelas organizações orientadas ao lucro, frequentemente, mudaram apenas os seus termos de uso e política de privacidade, enquanto a coleta remanesceu a mesma. Os usuários, por fim, devem estar preocupados com sua privacidade digital ao ponto de modificarem severamente seu uso da internet; somente com substituições e exclusões drásticas de softwares maliciosos a preservação da privacidade digital é possível da perspectiva do usuário.

As atitudes dos usuários, diante da privacidade, consoante o questionário realizado, foram de um lado positivas, de outro negativas. Por mais que estes valorizem

a privacidade digital, em alto grau, poucos deles aderem a práticas que realmente conduzem à privacidade no ambiente digital. Substancial parte em razão de desconhecimento das melhores práticas, enquanto menor parte em razão de preferir a conveniência desses serviços coletores de dados em detrimento da privacidade. Para aprimorar a privacidade digital, os usuários devem conhecer as melhores práticas para esse fim e aplicá-las em seus dispositivos e uso cotidiano da web. Analogamente ao desenvolvimento de um setor da economia, em que as práticas começam rudimentares e, aos poucos são desenvolvidas, o mesmo deve ocorrer com o uso da internet por parcela das pessoas; atualmente, a diligência ao usar a internet, no sentido de preservação de dados, é circunscrita a poucos, porém, tais práticas começam a ser difundidas, de modo a abranger e interessar outros indivíduos. Tendo em vista que a preocupação quanto à privacidade digital é geral, essas práticas tendem a se difundir organicamente com o tempo.

Os resultados obtidos são relevantes, no sentido de apreender se as regulações recentes foram eficazes ou não. Na medida em que uma regulação é implementada, espera-se algum resultado prático na vida dos indivíduos; no caso em comento, qual seja, das regulações concernentes à coleta de dados, o impacto destas nos usuários digitais em aparência é insignificante, haja vista que as práticas no ambiente digital não foram aprimoradas, em direção à maior privacidade. Resta evidente que a ação do indivíduo na internet é primordial para garantir sua privacidade, tendo em vista que nas organizações privadas a coleta de dados remanesce e as regulações adicionaram alguns requisitos legais, mas não impedem por si só que subsista tal coleta, como se vê em qualquer rede social; em essência, se o usuário quiser utilizar um aplicativo malicioso, pouco importa as regulações de coleta de dados, pois o uso destes aplicativos é voluntário. Desse modo, cabe ao usuário aprimorar seu conhecimento a respeito da internet, de modo a utilizar softwares congruentes à privacidade digital, uma vez que é leviano depositar demasiada expectativa na regulação em um ambiente de tamanha dinamicidade como o digital. Somado a isso, deve o agente digital avaliar a que extensão seus dados estão seguros em agências estatais, haja vista que organizações públicas também convergem com organizações privadas na obtenção de informações pessoais.

Em razão de este trabalho adotar uma metodologia simplificada de questionário e análise exploratória, a amostra não é significativa ao ponto de estabelecer certezas sobre o tema. Alguns dados obtidos foram congruentes com a realidade digital, como a dominância do Google como mecanismo de pesquisa, já outros precisam ser explorados com mais afinco, como certas preferências e práticas individuais. Muito se pode extrair de uma eventual pesquisa qualitativa sobre o tema, de modo a inquirir com mais profundidade os usuários digitais. Trata-se, além disso, de um tópico dinâmico que pode muito bem ter conclusões diversas em um futuro próximo. Perguntas que

poderiam ser abordadas com mais intensidade seriam aquelas referentes à Internet das Coisas (IOT): a presença crescente dessa tecnologia nas residências pode significar uma violação sistematizada de privacidade não só dos usuários que ali residem, mas também de outros adjacentes, como mencionado no capítulo 3.2.6.

O que se estima, por conseguinte, é uma mudança geral no ambiente da internet. Inicialmente as pessoas queriam ser notadas na web, razão pela qual possuíam seus próprios websites e apresentavam informações pessoais neles. Atualmente, no entanto, essa prática se tornou obsoleta, não só porque surgiram redes sociais, mas também porque há uma tendência oposta de anonimidade e privacidade no ambiente digital. Essa tendência, de fato, é uma orientação dos usuários da exposição para a preservação de dados; as razões devem ser estudadas mais a fundo, porém, é certo que softwares com base nesse fim serão mais utilizados do que antes, o que pode comprometer a hegemonia de grandes empresas de tecnologia, como a Microsoft, Apple e Google que, em grande parte, construíram-se por meio da coleta de dados.

Referências

ABRAMS, L. **Hacker selling Twitter account data of 5.4 million users for $30k**. 2022. Disponível em: <https://www.bleepingcomputer.com/news/security/hacker-selling-twitter-account-data-of-54-million-users-for-30k/>. Acesso em: 25 ago. 2022.

ADAMS, M. Big data and individual privacy in the age of the internet of things. **Technology Innovation Management Review**, v. 7, n. 4, 2017.

AGU, E. et al. The smartphone as a medical device: Assessing enablers, benefits and challenges. In: IEEE. 2013 IEEE International Workshop of Internet-of-Things Networking and Control (IoT-NC). [S.l.: s.n.], 2013. p. 48–52.

APPLE. **Air Tag**. 2022. Disponível em: <https://www.apple.com/airtag>. Acesso em: 13 abr. 2022.

ARS, S. **Dutch privacy regulator says Windows 10 breaks the law**. 2017. Disponível em: <https://arstechnica.com/gadgets/2017/10/dutch-privacy-regulator-says-that-windows-10-breaks-the-law/>. Acesso em: 21 ago. 2022.

ASHWIN. **Twitter confirms that a data breach leaked email addresses and phone numbers of users**. 2022. Disponível em: <https://www.ghacks.net/2022/08/08/twitter-confirms-that-a-data-breach-leaked-email-addresses-and-phone-numbers-of-users/>. Acesso em: 25 ago. 2022.

BACA, M. **Introduction to metadata**. [S.l.]: Getty Publications, 2016.

BATES, P. **4 Ways Instagram Is Spying on You Right Now**. 2018. Disponível em: <https://web.archive.org/web/20180131084312/https://www.makeuseof.com/tag/ways-instagram-spying-you/>. Acesso em: 25 ago. 2022.

BAUMAN, Z. et al. After Snowden: Rethinking the impact of surveillance. **International political sociology**, Oxford University Press, v. 8, n. 2, p. 121–144, 2014.

BECKER, T. Big data usage. In: NEW horizons for a data-driven economy. [S.l.]: Springer, Cham, 2016. p. 143–165.

BERKELEY, U. **[Support] Selective Disclosure**. 2022. Disponível em: <https://www.privacypatterns.org/patterns/Support-Selective-Disclosure>. Acesso em: 26 ago. 2022.

BONI, V.; QUARESMA, S. J. Aprendendo a entrevistar: como fazer entrevistas em Ciências Sociais. **Em tese**, v. 2, n. 1, p. 68–80, 2005.

BOULANGER, A. Open-source versus proprietary software: Is one more reliable and secure than the other? **IBM Systems Journal**, IBM, v. 44, n. 2, p. 239–248, 2005.

BRASIL. Decreto Número 10900, de 17 de Dezembro de 2021. Brasil, 17 dez. 2021. ISSN 1677-7042. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10900.htm>. Acesso em: 11 ago. 2022.

BRASIL. CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 5 out. 1988. ISSN 1677-7042. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm>. Acesso em: 11 ago. 2022.

BRASIL. Decreto nº 10.900, de 17 de dezembro de 2021. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 17 dez. 2021. ISSN 1677-7042. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/Decreto/D10900.htm#:~:text=1%5C%C2%5C%BA%5C%20Este%5C%20Decreto%5C%20estabelece%5C%20o,federal%5C%20direta%5C%2C%5C%20aut%5C%C3%5C%A1rquica%5C%20e%5C%20fundacional.>. Acesso em: 28 fev. 2022.

BRASIL. Lei 10.406, de 10 de Janeiro de 2002, Código Civil. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 10 jan. 2002. ISSN 1677-7042. Disponível em: <https://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406compilada.htm>. Acesso em: 11 ago. 2022.

BRASIL. Lei nº 12.965, de 23 de Abril de 2014: Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 14 ago. 2018. ISSN 1677-7042. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 7 out. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 14 ago. 2018. ISSN 1677-7042. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 28 fev. 2022.

BRAXMAN, R. **Apple Airtag and the Snitch Network!** 2021. Disponível em: <https://youtu.be/vN7_sl3qNxk>. Acesso em: 13 mai. 2021.

BURNS, M. **Leaked Palantir Doc Reveals Uses, Specif Functions and Key Clients**. 2015. Disponível em: <https://techcrunch.com/2015/01/11/leaked-palantir-doc-reveals-uses-specific-%20functions-and-key-clients>. Acesso em: 14 abr. 2022.

CHALK, A. **Red Shell analytics software causes privacy uproar, over a dozen developers vow to drop it (Updated)**. 2018. Disponível em:

<https://www.pcgamer.com/red-shell-analytics-software-causes-privacy-uproar-over-a-dozen-developers-vow-to-drop-it/>. Acesso em: 26 ago. 2022.
COLESKY, M. et al. **Appropriate Privacy Icons**. University of California. 2022. Disponível em: <https://www.privacypatterns.org/patterns/Appropriate-Privacy-Icons>. Acesso em: 26 ago. 2022.
COLESKY, M. et al. **Asynchronous notice**. University of California. 2022. Disponível em: <https://privacypatterns.org/patterns/Asynchronous-notice>. Acesso em: 26 ago. 2022.
COLESKY, M. et al. **Discouraging blanket strategies**. University of California. 2022. Disponível em: <https://www.privacypatterns.org/patterns/Discouraging-blanket-strategies>. Acesso em: 26 ago. 2022.
COLESKY, M. et al. **Enable/Disable Functions**. University of California. 2022. Disponível em: <https://www.privacypatterns.org/patterns/Enable-Disable-Functions>. Acesso em: 26 ago. 2022.
COLESKY, M. et al. **Encryption with user managed keys**. University of California. 2022. Disponível em: <https://www.privacypatterns.org/patterns/Encryption-user-managed-keys>. Acesso em: 26 ago. 2022.
COLESKY, M. et al. **Icons for Privacy Policies**. University of California. 2022. Disponível em: <https://www.privacypatterns.org/patterns/Icons-for-Privacy-Policies>. Acesso em: 26 ago. 2022.
COLESKY, M. et al. **Increasing Awareness of Information Aggregation**. University of California. 2022. Disponível em: <https://privacypatterns.org/patterns/Increasing-Awareness-of-Information-Aggregation>. Acesso em: 26 ago. 2022.
COLESKY, M. et al. **Location Granularity**. University of California. 2022. Disponível em: <https://www.privacypatterns.org/patterns/Location-granularity>. Acesso em: 26 ago. 2022.
COLESKY, M. et al. **Obligation Management**. University of California. 2022. Disponível em: <https://www.privacypatterns.org/patterns/Obligation-management>. Acesso em: 26 ago. 2022.
COLESKY, M. et al. **Outsourcing [with-consent]**. University of California. 2022. Disponível em: <https://privacypatterns.org/patterns/Outsourcing-%5Bwith-consent%5D>. Acesso em: 26 ago. 2022.

COLESKY, M. et al. **Privacy Patterns**. University of California. 2022. Disponível em: <https://www.privacypatterns.org/>. Acesso em: 26 ago. 2022.
COLESKY, M. et al. **Privacy Patterns**. University of California. 2022. Disponível em: <https://privacypatterns.org/patterns/Obtaining-Explicit-Consent>. Acesso em: 26 ago. 2022.
COLESKY, M. et al. **Privacy Patterns**. University of California. 2022. Disponível em: <https://privacypatterns.org/patterns/Informed-Implicit-Consent>. Acesso em: 26 ago. 2022.
COLESKY, M. et al. **Privacy Patterns**. University of California. 2022. Disponível em: <https://privacypatterns.org/patterns/Sign-an-Agreement-to-Solve-Lack-of-Trust-on-the-Use-of-Private-Data-Context>. Acesso em: 26 ago. 2022.
COLESKY, M. et al. **Reciprocity**. University of California. 2022. Disponível em: <https://www.privacypatterns.org/patterns/Reciprocity>. Acesso em: 26 ago. 2022.
COLESKY, M. et al. **Unusual Activities**. University of California. 2022. Disponível em: <https://www.privacypatterns.org/patterns/Unusual-activities>. Acesso em: 26 ago. 2022.
COLESKY, M. et al. **User data confinement pattern**. University of California. 2022. Disponível em: <https://www.privacypatterns.org/patterns/User-data-confinement-pattern>. Acesso em: 26 ago. 2022.
COX, J. **Microsoft Contractors Listened to Xbox Owners in Their Homes**. 2022. Disponível em: <https://www.vice.com/en/article/43kv4q/microsoft-human-contractors-listened-to-xbox-owners-homes-kinect-cortana>. Acesso em: 26 ago. 2022.
DEAHL, D. **Snapchat's newest feature is also its biggest privacy threat**. 2017. Disponível em: <https://web.archive.org/web/20190223064446/https://www.theverge.com/2017/6/23/15864552/snapchat-snap-map-privacy-threat>. Acesso em: 25 ago. 2022.
DIEZ, D. L. N. **Instagram is listening to you**. 2017. Disponível em: <https://damln.medium.com/instagram-is-listening-to-you-97e8f2c53023>. Acesso em: 25 ago. 2022.
DISCORD. **Data Privacy Controls**. 2022. Disponível em: <https://support.discord.com/hc/en-us/articles/360004109911>. Acesso em: 26 ago. 2022.
DISCORD. **Política de Privacidade do Discord**. 2022. Disponível em: <https://discord.com/privacy>. Acesso em: 26 ago. 2022.
DRAGNIĆ, D. Impact of internal and external factors on the performance of fast-growing small and medium businesses. **Management: Journal of**

contemporary management issues, Sveučilište u Splitu, Ekonomski fakultet, v. 19, n. 1, p. 119–159, 2014.
DROZD, O. Privacy pattern catalogue: A tool for integrating privacy principles of ISO/IEC 29100 into the software development process. In: SPRINGER. IFIP International Summer School on Privacy and Identity Management. [S.l.: s.n.], 2015. p. 129–140.
EUROPEIA, U. Regulation (EU) 2016/679 (General Data Protection Regulation). União Europeia, 27 abr. 2016. ISSN 1677-7042. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679%5C&from=EN>. Acesso em: 17 mar. 2022.
FAWCETT, T.; PROVOST, F. **Data Science para Negócios: O que você precisa saber sobre mineração de dados e pensamento analítico de dados**. [S.l.]: Alta Books Editora, 2016.
GAULT, M. **Amazon Buys Roomba Company, Will Now Map Inside of Your House**. 2022. Disponível em: <https://www.vice.com/en/article/y3pp8y/amazon-buys-roomba-company-will-now-map-inside-of-your-house?utm_source=reddit.com>. Acesso em: 25 ago. 2022.
GEBHART, G. et al. **Spying on Students: School-Issued Devices and Student Privacy**. 13 abr. 2017. Disponível em: <https://www.eff.org/files/2017/04/13/student-privacy-report.pdf>. Acesso em: 22 ago. 2022.
GHASEMAGHAEI, M.; CALIC, G. Assessing the impact of big data on firm innovation performance: Big data is not always better data. **Journal of Business Research**, Elsevier, v. 108, p. 147–162, 2020.
GNU. **O que é o software livre?** 2022. Disponível em: <https://www.gnu.org/philosophy/free-sw.html>. Acesso em: 20 ago. 2022.
GNU. **Sistemas operacionais da Apple são malware**. 2022. Disponível em: <https://www.gnu.org/proprietary/malware-apple.html>. Acesso em: 26 ago. 2022.
GNU. **Software do Google é malware**. 2022. Disponível em: <https://www.gnu.org/proprietary/malware-apple.html>. Acesso em: 26 ago. 2022.
GNU. **Software privativo frequentemente é malware**. 2022. Disponível em: <https://www.gnu.org/proprietary/proprietary.html>. Acesso em: 21 ago. 2022.
GNU. **Vigilância Privativa**. 2022. Disponível em: <https://www.gnu.org/proprietary/proprietary-surveillance.html>. Acesso em: 21 ago. 2022.
GOLDFARB, A.; TUCKER, C. E. Online advertising, behavioral targeting, and privacy. **Communications of the ACM**, ACM New York, NY, USA, v. 54, n. 5, p. 25–27, 2011.

GREENBERG, A. **How A 'Deviant' Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut**. 2013. Disponível em: <https://%3Cwww.forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut/?sh=9b825d177852>. Acesso em: 14 abr. 2022.

GREENFIELD, D. The addictive properties of Internet usage. **Internet addiction: A handbook and guide to evaluation and treatment**, Wiley Online Library, p. 133–153, 2007.

GUARIGLIA, M. **Senator Declares Amazon Ring's Audio Surveillance Capabilities "Threaten the Public"**. 2022. Disponível em: <https://www.eff.org/deeplinks/2022/06/senator-declares-concern-about-amazon-rings-audio-surveillance-capabilities>. Acesso em: 25 ago. 2022.

HIZAM-HANAFIAH, M.; SOOMRO, M. A. The situation of technology companies in industry 4.0 and the open innovation. **Journal of open innovation: technology, market, and complexity**, MDPI, v. 7, n. 1, p. 34, 2021.

HRUSKA, J. **Riot Games' New Anti-Cheat System Runs at System Boot, Uses Kernel Driver**. 2020. Disponível em: <https://www.extremetech.com/gaming/309320-riot-games-new-anti-cheat-system-runs-at-system-boot-uses-kernel-driver>. Acesso em: 26 ago. 2022.

JAIN, A. The role and importance of search engine and search engine optimization. **International Journal of emerging trends & technology in computer science**, v. 2, n. 3, p. 99–102, 2013.

JEAN-NICOLAS, R. Semester paper: Building railways in the XIXth century. **Institute for Transport Planning and Systems**, 2016.

JIGSAW. **Jigsaw: A safer internet means a safer world**. 2022. Disponível em: <https://web.archive.org/web/20200815071016/https://jigsaw.google.com/>. Acesso em: 13 abr. 2022.

KALIA, A. **With Windows 10, Microsoft Blatantly Disregards User Choice and Privacy: A Deep Dive**. 2016. Disponível em: <eff.org/deeplinks/2016/08/windows-10-microsoft-blatantly-disregards-user-choice-and-privacy-deep-dive>. Acesso em: 21 ago. 2022.

KARLIN, J. **Evolution from FLoC**. 2022. Disponível em: <https://github.com/patcg-individual-drafts/topics>. Acesso em: 14 abr. 2022.

KHAN, M. A.; SALAH, K. IoT security: Review, blockchain solutions, and open challenges. **Future generation computer systems**, Elsevier, v. 82, p. 395–411, 2018.

KOCIALKOWSKI, P. **Replicant developers find and close Samsung Galaxy backdoor**. 2014. Disponível em:

<https://www.fsf.org/blogs/community/replicant-developers-find-and-close-samsung-galaxy-backdoor>. Acesso em: 26 ago. 2022.
NG-KRUELLE, G. et al. The price of convenience: Privacy and mobile commerce. **Quarterly Journal of Electronic Commerce**, INFORMATION AGE PUBLISHING, v. 3, p. 273–286, 2002.
KUMAR, P. C. et al. The platformization of the classroom: Teachers as surveillant consumers. **Surveillance & Society**, v. 17, n. 1/2, p. 145–152, 2019.
KUNER, C. **European data privacy law and online business**. [S.l.]: Oxford University Press, USA, 2003.
LAI, M. K.; SCHILDKAMP, K. Data-based decision making: An overview. **Data-based decision making in education**, Springer, p. 9–21, 2013.
LI, T. et al. Smartphone App Usage Analysis: Datasets, Methods, and Applications. **IEEE Communications Surveys & Tutorials**, IEEE, 2022.
LINEAGEOS. **About**. 2022. Disponível em: <https://lineageos.org/about/>. Acesso em: 13 abr. 2022.
LOPES, G. V. Vigilância Cibernética no Brasil: O Caso Snowden sob o PRISMa de um insider. **Revista ECO-Pós**, v. 18, n. 2, p. 261–265, 2015.
LOVELESS, M. **Bring your own Dilemma: OEM Laptops and Windows 10 Security**. 2016. Disponível em: <https://duo.com/decipher/bring-your-own-dilemma-oem-laptops-and-windows-10-security>. Acesso em: 21 ago. 2022.
LYONS, K. **Amazon will launch a new location-tracking mesh network system later this year.** 2020. Disponível em: <https://www.theverge.com/2020/9/21/21448926/amazon-sidewalk-ring-echo-tile-wifi-mesh-ble-location-tracking>. Acesso em: 13 abr. 2022.
MARKOVIKJ, D. et al. Mining facebook data for predictive personality modeling. In: 2. PROCEEDINGS of the International AAAI Conference on Web and Social Media. [S.l.: s.n.], 2013. v. 7, p. 23–26.
MARTIN, K. D.; BORAH, A.; PALMATIER, R. W. Data privacy: Effects on customer and firm performance. **Journal of Marketing**, SAGE Publications Sage CA: Los Angeles, CA, v. 81, n. 1, p. 36–58, 2017.
MASON, M. **TikTok's 'alarming', 'excessive' data collection revealed**. 2022. Disponível em: <https://web.archive.org/web/20220718031155/https://www.afr.com/policy/foreign-affairs/tiktok-s-alarming-excessive-data-collection-revealed-20220714-p5b1mz>. Acesso em: 25 ago. 2022.
MELLOR, R. **The roman historians**. [S.l.]: Routledge, 2002.
METAXAS, P. T.; PRUKSACHATKUN, Y. Manipulation of search engine results during the 2016 US congressional elections, 2017.

MICROSOFT. **AutoAdminLogon**. 2010. Disponível em: <https://docs.microsoft.com/pt-br/previous-versions/windows/it-pro/windows-2000-server/cc939702(v=technet.10)>. Acesso em: 21 ago. 2022.
MOONSHOT. **Moonshot: Working to end online harms, applying evidence, ethics, and human rights**. 2022. Disponível em: <https://web.archive.org/web/20220204125227/https://moonshotteam.com/work/>. Acesso em: 13 abr. 2022.
MOONSHOT. **Resources**. 2022. Disponível em: <https://moonshotteam.com/resources/>. Acesso em: 13 abr. 2022.
NEWELL, G. **Valve, VAC, and trust**. 2018. Disponível em: <https://web.archive.org/web/20180521023711/https://www.reddit.com/r/gaming/comments/1y70ej/valve_vac_and_trust/>. Acesso em: 26 ago. 2022.
NISSENBAUM, H. Privacy in context. In: PRIVACY in Context. [S.l.]: Stanford University Press, 2010.
OPENTHREAD. **Openthread: An open foundation for the connected home**. 2022. Disponível em: <https://openthread.io/>. Acesso em: 13 abr. 2022.
PÅHLMAN, K.; WALDENSKIÖLD, E. Personalized marketing-A qualitative study on tailored marketing online from a consumer's perspective, 2013.
PAUL, J. **Your Computer Isn't Yours**. 2020. Disponível em: <https://sneak.berlin/20201112/your-computer-isnt-yours/>. Acesso em: 21 ago. 2022.
REDSHELL. **Hi there, we're Red Shell.** 2022. Disponível em: <https://web.archive.org/web/20220104195144/https://redshell.io/gamers>. Acesso em: 26 ago. 2022.
REIS, É. V. B.; OLIVEIRA NAVES, B. T. de. O meio ambiente digital e o direito à privacidade diante do Big Data. **Veredas do Direito: Direito Ambiental e Desenvolvimento Sustentável**, v. 17, n. 37, p. 145–167, 2020.
ROTH, E. **Google abandons FLoC, introduces Topics API to replace tracking cookies**. 2022. Disponível em: <https://www.theverge.com/2022/1/25/22900567/google-floc-abandon-topics-api-cookies-tracking>. Acesso em: 14 abr. 2022.
RUBINSTEIN, I. S.; NOJEIM, G. T.; LEE, R. D. Systematic government access to personal data: a comparative analysis. **International Data Privacy Law**, Oxford University Press, v. 4, n. 2, p. 96–119, 2014.
SANCHEZ, J. **Apple's iPhone: Now With Built-In Surveillance**. 2021. Disponível em: <https://policycommons.net/artifacts/1804960/apples-iphone/2537024/>. Acesso em: 13 abr. 2022.

SARKER, I. H. Data science and analytics: an overview from data-driven smart computing, decision-making and applications perspective. **SN Computer Science**, Springer, v. 2, n. 5, p. 1–22, 2021.
SAWERS, P. **Denmark bans Chromebooks and Google Workspace in schools over data transfer risks**. 2022. Disponível em: <https://techcrunch.com/2022/07/18/denmark-bans-chromebooks-and-google-workspace-in-schools-over-gdpr/?guccounter=1>. Acesso em: 25 ago. 2022.
SCHOEMAN, F. D. **Privacy and social freedom**. [S.l.]: Cambridge university press, 1992.
SCHUMACHER, T. et al. A review of ultra-low-power and low-cost transceiver design. In: IEEE. 2017 Austrochip Workshop on Microelectronics (Austrochip). [S.l.: s.n.], 2017. p. 29–34.
SHILLINGTON, L.; TONG, D. Maximizing wireless mesh network coverage. **International Regional Science Review**, SAGE Publications Sage CA: Los Angeles, CA, v. 34, n. 4, p. 419–437, 2011.
SICHITIU, M. L. Wireless mesh networks: opportunities and challenges. In: CITESEER. PROCEEDINGS of World Wireless Congress. [S.l.: s.n.], 2005. v. 2, p. 21.
SILVA, D. da; LOPES, E. L.; JUNIOR, S. S. B. Pesquisa quantitativa: elementos, paradigmas e definições. **Revista de Gestão e Secretariado**, v. 5, n. 1, p. 01–18, 2014.
SMITH, M. et al. Big data privacy issues in public social media. In: IEEE. 2012 6th IEEE international conference on digital ecosystems and technologies (DEST). [S.l.: s.n.], 2012. p. 1–6.
SNAP, I. **Privacy Policy**. 2022. Disponível em: <https://www.snap.com/en-US/privacy/privacy-policy>. Acesso em: 25 ago. 2022.
STALLMAN, R. **Por que o Código Aberto não compartilha dos objetivos do Software Livre**. 2022. Disponível em: <https://www.gnu.org/philosophy/open-source-misses-the-point.html>. Acesso em: 21 ago. 2022.
STATCOUNTER. **Statcounter: GlobalStats**. 2022. Disponível em: <https://gs.statcounter.com/os-market-share>. Acesso em: 13 abr. 2022.
STATCOUNTER. **Statcounter: GlobalStats**. 2022. Disponível em: <https://web.archive.org/web/20220406210047/https://gs.statcounter.com/search-engine-market-share>. Acesso em: 13 abr. 2022.
STEAM. **Privacy Policy**. 2018. Disponível em: <https://web.archive.org/web/20180601093517/https://store.steampowered.com/privacy_agreement/>. Acesso em: 26 ago. 2022.

SUN, Y. et al. When machine learning meets privacy in 6G: A survey. **IEEE Communications Surveys & Tutorials**, IEEE, v. 22, n. 4, p. 2694–2724, 2020.
TAKE-TWO. **Privacy Policy**. 2018. Disponível em: <https://web.archive.org/web/20180603120327/https://www.take2games.com/privacy/>. Acesso em: 26 ago. 2022.
TOULAS, B. **Meta, US hospitals sued for using healthcare data to target ads**. 2022. Disponível em: <https://www.bleepingcomputer.com/news/security/meta-us-hospitals-sued-for-using-healthcare-data-to-target-ads/>. Acesso em: 20 ago. 2022.
TUROW, J. et al. Americans reject tailored advertising and three activities that enable it. **Available at SSRN 1478214**, 2009.
VODHANEL, R. S. et al. Performance of directly modulated DFB lasers in 10-Gb/s ASK, FSK, and DPSK lightwave systems. **Journal of lightwave technology**, IEEE, v. 8, n. 9, p. 1379–1386, 1990.
WARREN, B.; BRANDEIS, L. **The Right to Privacy.: 4 HARV. L. REV. 193**. [S.l.: s.n.], 1890.
WEBSTER, J. G. Nielsen ratings. **The international encyclopedia of communication**, Wiley Online Library, 2008.
WEINSTEIN, R. RFID: a technical overview and its application to the enterprise. **IT professional**, IEEE, v. 7, n. 3, p. 27–33, 2005.
WESTIN, A. F. Social and political dimensions of privacy. **Journal of social issues**, Wiley Online Library, v. 59, n. 2, p. 431–453, 2003.
YANG, J. et al. Beyond beaconing: Emerging applications and challenges of BLE. **Ad hoc networks**, Elsevier, v. 97, p. 102015, 2020.