INTRODUÇÃO

Diante das constantes e cada vez mais rápidas transformações da informação e consequentemente, da sociedade causada pelos avanços tecnológicos, a privacidade torna-se um dos temas mais relevantes da atualidade. Nesse contexto, é notória a preocupação social, nacional e internacional, da proteção à privacidade.

A importância do direito à privacidade é tamanha que nem a própria pessoa pode dela renunciar, abdicar ou alienar, pois é inviolável.

Temos vivido o auge da era da publicidade na internet e, consequentemente, a era da falta da privacidade do indivíduo, posto que a internet proporciona uma sociedade desenfreadamente vigiada, tanto pelo Estado, como pelas grandes empresas, o que gera uma invasão da privacidade, além do uso imoderado dos dados pessoais.

Falar de privacidade é falar de dados, é falar de informação e é sobre isso que este artigo abordará. Como afirma o Doneda (2021, p.15) em sua Obra "Da privacidade à proteção de dados pessoais": "Sem privacidade não haveria um espaço no qual o indivíduo estivesse livre para pensar, desenvolver as suas próprias ideias, experimentar e seguir o seu próprio caminho de vida como lhe aprouver e parecer adequado" (Doneda, 2021, p.15).

1. EVOLUÇÃO E CONSOLIDAÇÃO DA PRIVACIDADE NOS ESTADOS UNIDOS

A origem da privacidade se deu no mundo antigo, precisamente em Roma e Grécia. Ao pensar em privacidade, podemos considerá-la como um conceito evolutivo, pois há uma atualização dela para o mundo moderno.

Na medida que as cidades foram crescendo, houve a necessidade de separação do que era público e do que era privado. Essa separação é algo muito antigo na história da humanidade, porém, quando comparamos a noção de privacidade romana com a noção moderna, em especial nas revoluções liberais do século XVIII, temos uma significativa mudança.

Na Idade Antiga, a ideia da privacidade era muito mais ligada à família, ou seja, quem controlava o que era privado, era quem detinha o poder familiar, o pai da família, que decidia sobre as questões privadas. Ele era uma autoridade não regulamentada e tinha poder, quase que absoluto, do seu núcleo familiar.

A mudança do conceito de privacidade acontece a partir da Idade Moderna, quando a forma antiga de ordenação social e aristocrática começa a ser modificada, e o indivíduo torna-se a sua grande preocupação. Tal transformação deixou o problema mais complexo.

Nessa nova fase, dois caminhos sobre a privacidade são criados: o clássico artigo *The Right to Privacy* de 1890[1], escrito por Warren e Brandeis e na outra linha, uma ideia que derivou da jurisprudência do Tribunal Constitucional alemão, que é a defesa ao direito à privacidade de dados, direito esse que é entendido como parte do direito à autodeterminação informativa, é um princípio derivado da combinação dos Artigos 1 (1) e 2 (1) da GG[2].

Esses conceitos históricos são de fundamental importância para a compreensão da origem da privacidade no mundo, da proteção de dados pessoais e toda a sua evolução e necessidade.

A evolução do conceito de privacidade, como mencionado acima, se dividiu no mundo através dos sistemas dos Estados Unidos e da Europa, que eventualmente, comunicam-se, mesmo sendo culturalmente diferentes entre si.

Na cultura americana, a privacidade é derivada do *Common law*, tendo por base o texto da 4ª emenda da Constituição dos Estados Unidos, pois estava muito mais direcionada para a proteção da propriedade. Segundo o disposto na referida emenda:

> O direito das pessoas de estarem seguras em suas pessoas, casas, papéis e pertences, contra buscas e apreensões não razoáveis, não deve ser violado e nenhum mandado deve ser emitido, mas por causa provável, apoiado por juramento ou afirmação, e particularmente descrevendo o local a ser revistado e as pessoas ou coisas a serem apreendidas[3].

Em 1890, no entanto, através de artigo intitulado *The Right to Privacy* publicado na *Harvard Law Review*, Warren e Brandeis, efetivamente marcaram a discussão sobre a privacidade. O referido artigo surge como a primeira tentativa de levar a ideia de proteção da propriedade privada para algum fundamento para além da propriedade, ou seja, que alcançasse o indivíduo. Eis que a ideia central encontra-se no propósito declarado pelos autores de "considerar o direito existente, que oferece um princípio que pode ser devidamente invocado para proteger a privacidade do indivíduo em caso afirmativo, identificar a natureza e a extensão de tal proteção.[4]".

---

[1] https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html,
[2] Constituição alemã: https://jus.com.br/artigos/98042/constituicao-da-alemanha-de-1949-revisada-em-2014.
[3] 4ª Emenda da Constituição americana, Disponível em: https://constitution.congress.gov/constitution/amendment-4/. Acesso em: 15 maio 2023. (Tradução nossa).
The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
[4]Privacidade: Disponível em: https://plato.stanford.edu/entries/privacy/ Acesso em: 15 maio 2023. – (Tradução nossa).

Tal artigo, portanto, é criado com a ideia centrada no indivíduo e não na propriedade do indivíduo, ou seja, uma releitura da 4ª emenda à Constituição Americana, no sentido da proteção da pessoa em si.

Após a publicação desse artigo, alguns casos na jurisdição americana foram fundamentados com base na expectativa de utilizar a 4ª emenda, como o direito à privacidade do indivíduo, dentre os quais, dois merecem destaque devido as repercussões obtidas.

O primeiro aconteceu em 1928, um caso de interceptação telefônica. A discussão se dava pelo fato de se admitir ou não a 4ª emenda, já que o entendimento dominante era de que ela protegia a invasão em domicílio, sendo que essa interceptação foi feita sem invasão. Então, em uma votação acirrada, por 5x4, entenderam que, nesse caso, não se aplicava a 4ª emenda, ou seja, não haveria a proteção constitucional para o direito à privacidade. Eles ainda se baseavam na ideia de que a 4ª emenda protegia somente a propriedade.

Vale ressaltar que no caso em questão, dentre os quatro juízes que votaram a favor de se utilizar a 4ª emenda, um deles foi Louis Brandeis, o mesmo que escreveu o primeiro artigo sobre privacidade em 1890, e passou a fazer parte da Suprema Corte. Sua participação gerou uma visão mais ampla para assuntos que envolviam a privacidade.

Cada vez mais, por influência de Brandeis, a Suprema Corte entendia que a 4ª emenda deveria ser interpretada não como uma proteção apenas da propriedade, mas como a proteção efetiva contra a intrusão na vida privada.

Desde então, os operadores do direito ampliaram a discussão acerca do limite da coleta e a utilização de dados pessoais, os quais estão muito atrelados ao desenvolvimento tecnológico, havendo clara tentativa de normatizar e estabelecer limites equilibrados entre a vida privada e o direito à informação.

A análise de Brandeis só foi efetivamente aceita pela Suprema Corte americana em 1967, em outro caso sobre escuta telefônica, bastante semelhante àquele julgado em 1928, porém, dessa vez, a orientação foi diferente. Nesse processo, começou a entender que a 4ª emenda se destinava a proteger pessoas e não necessariamente coisas.

Essa ação se tornou um divisor de águas sobre privacidade na Constituição Americana. Por ela, foi aceita pela primeira vez, o *Right to privacy* ou o Direito à privacidade, como matéria constitucional.

Construído pela jurisprudência norte-americana, o *Right to Privacy* (Direito à Privacidade), como concebido na jurisprudência dos Estados Unidos, engloba várias proteções

individuais. Embora não esteja explicitamente mencionado na Constituição dos Estados Unidos, foi interpretado pelos tribunais como sendo implícito nos vários direitos constitucionais. Em geral, o direito à privacidade pode incluir:

1. O direito de ficar sozinho (direito à solidão): Isso se refere à proteção contra interferências indevidas de terceiros em sua vida privada.

2. Proteção contra divulgação pública de fatos embaraçosos privados: Este direito protege os indivíduos contra a divulgação não autorizada de informações pessoais que poderiam ser humilhantes ou embaraçosas.

3. Proteção contra a divulgação de informações falsas: Este direito protege os indivíduos contra danos decorrentes da publicação de informações falsas que possam prejudicar sua reputação ou imagem pública.

4. Proteção contra apropriação de nome ou imagem: Este direito protege os indivíduos contra o uso não autorizado de seu nome ou imagem para fins comerciais.

Estes são os componentes centrais do direito à privacidade, embora a definição exata possa variar de acordo com a jurisdição e as circunstâncias específicas das várias decisões da Suprema Corte dos EUA que abordam a privacidade. Algumas decisões notáveis incluem Griswold v. Connecticut (1965)[5], que concedeu um direito à privacidade nas "penumbras" e "emanações" de outras garantias constitucionais, e Roe v. Wade (1973)[6], que afirmou o direito à privacidade em relação às decisões pessoais sobre a reprodução. Cumpre destacar, porém, que mais recentemente (2022) a suprema corte dos Estados Unidos da América, revogou a decisão Roe v. Wade (1973), trazendo para o cenário norte americano, uma nova compreensão sobre o princípio a privacidade, no qual o aborto não se enquadra como uma decisão pessoal sore a reprodução (REDAÇÃO OESTE, 2022).

2. ORIGEM DA PRIVACIDADE NA ALEMANHA

[5] https://supreme.justia.com/cases/federal/us/381/479/ Acesso em: 16 maio 2023.
[6] https://www.bbc.com/portuguese/internacional-61929519 Acesso em: 16 maio 2023.

Diferentemente da ideia americana de que o direito à privacidade está muito ligado ao trinômio: pessoa, informação e segredo, na Alemanha, o contexto se deu pela necessidade de controle.

O Estado Alemão é muito preocupado com a questão do controle, afinal, eles passaram por um regime totalitário excessivo.

Através de censos realizados pelo Estado, na primeira metade do século XX, o governo alemão tinha acesso a dados da população. Esses censos eram feitos em cartões perfurados, através de uma tecnologia utilizada pela IBM, e em cada perfuração, havia informações que o sistema da IBM conseguia extrair. Através disso, houve uma facilidade para que os nazistas encontrassem os judeus, acelerando assim o holocausto na Segunda Guerra Mundial[7].

A denominada Lei do Censo de 1983, obrigava a população a responder um questionário extenso de informações. Essas perguntas seriam submetidas a tratamentos informatizados, permitindo que o processamento e a capacidade de cruzar esses dados fossem cada vez maiores. Havia muitos pontos polêmicos, foi uma lei altamente controversa e provocou um amplo debate sobre a proteção de dados. A lei propunha uma pesquisa abrangente que incluiria muitos detalhes pessoais dos cidadãos, o que suscitou preocupações significativas de privacidade, tais como: i) confrontação de dados: A lei permitia que os dados coletados pelo censo fossem confrontados com os dados do registro público para retificação. Isso gerou temores de que os dados do censo pudessem ser usados para outros propósitos, violando a privacidade dos indivíduos; ii) compartilhamento de dados: Outra questão polêmica era a possibilidade de compartilhamento de dados com outras autoridades federais e estaduais sem limites claros. Isso levantou questões sobre a segurança dos dados e a possibilidade de uso indevido e iii) multa por não responder: A lei estabelecia multas para quem não respondesse ao questionário do censo, o que foi visto como uma invasão do direito de privacidade dos indivíduos[8].

Em resumo, essa lei previa que os dados, coletados por uma finalidade estatística, poderiam ser utilizados sem qualquer tipo de controle para qualquer outra atividade governamental e o indivíduo não tinha nenhum conhecimento de como esses dados seriam utilizados.

---

[7] "IBM and the Holocaust" por Edwin Black: O website do autor fornece uma visão geral de suas alegações e um arquivo de documentos de suporte. Link: https://www.ibmandtheholocaust.com/ - Acesso em: 16 maio 2023.
[8] file:///C:/Users/ester/Downloads/44826-137939-1-PB.pdf. Acesso em: 16 maio 2023.

Várias reclamações constitucionais foram ajuizadas diretamente contra a lei, sob a alegação de que ela violaria diretamente alguns direitos fundamentais dos reclamantes, sobretudo o direito ao livre desenvolvimento da personalidade, conforme discorre o Artigo (Art. 2 (1) GG):

> Artigo 2º Livre Desenvolvimento da Personalidade, direito à vida e à incolumidade física, liberdade da pessoa humana
> I Todos têm o direito ao livre desenvolvimento de sua personalidade, desde que não violem direitos de outrem e não se choquem contra a ordem constitucional ou a lei moral. (tradução nossa)[9].

No início da década de 80, a Suprema Corte alemã viu a necessidade de levar a democracia adiante. Nesse período ela reconhece que, com ajuda do processamento de dados, informações detalhadas podem ser armazenadas, consultadas, combinadas e formar um quadro da personalidade completa do indivíduo, sem que essa pessoa tenha como controlar, com exatidão, como a informação será usada, ampliando, significativamente, de maneira até então desconhecida, as possibilidades sobre a influência no comportamento das pessoas. A Suprema Corte começa a entender que esse tipo de legislação gerava um controle, então ela usa esse controle como exemplo para a democracia. Os dados pessoais devem ser elementos constitutivos da personalidade humana de modo que qualquer decisão sobre o seu tratamento deve competir ao seu titular.

Desse modo, não há como falar em privacidade como ideia de proteção de segredo, mas como ideia de proteção de controle, que é exatamente o conceito da democracia, ou seja, o Estado não pode controlar o povo e sim, o povo controlar a democracia.

A Suprema Corte alemã vem atuando nessa linha ativista, porém, de uma forma diferente da utilizada nas décadas de 50, 60 e 70, que antes era uma pauta extremamente positivista. Agora ela usa o ativismo como atuação de defesa à construção e à estrutura da democracia, fazendo com que surja a ideia da autodeterminação informacional, que é o direito que todo indivíduo tem de controlar os seus próprios dados pessoais.

---

[9] No original: https://www.bundestag.de/gg/grundrechteConstituição alemã: https://jus.com.br/artigos/98042/constituicao-da-alemanha-de-1949-revisada-em-2014 Artikel 2
(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.
(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

O Tribunal Constitucional Alemão, por meio de consistentes e bem fundamentadas decisões, tem inspirado vários outros países, como Portugal, Espanha e o próprio Brasil na elaboração de normas constitucionais, bem como para pautar suas decisões jurídico-constitucionais mais importantes.

Percebe-se que com o avanço tecnológico, direitos universalmente consagrados como a intimidade e a vida privada passam a exigir um sistema de proteção mais específico quando relacionados à informação, pois atualmente as informações na internet, além do seu alcance global, são eternizadas.

Ao discutir a questão do direito à intimidade e à privacidade, José Adércio Leite Sampaio de maneira perspicaz enfatiza que, em sua essência, a evolução do direito fundamental à intimidade e à vida privada reflete a jornada humana em busca de dignidade. Essa trajetória é delineada pelas lutas enfrentadas contra a opressão e o arbítrio, em prol da afirmação da liberdade. Nesse contexto, os direitos fundamentais se entrelaçam com essa busca incessante.

3. DIREITO À PRIVACIDADE NO BRASIL: UM TEMA DE RELEVÂNCIA CRESCENTE

Antes da Constituição de 1988, a legislação brasileira tratava de forma fragmentada e insuficiente as questões relacionadas à privacidade. Havia uma lacuna normativa que não garantia a proteção adequada dos indivíduos em suas esferas pessoais e íntimas. O Código Civil de 1916, por exemplo, não previa expressamente o direito à privacidade, o que limitava a atuação do Judiciário na proteção desses direitos.

A evolução do direito à privacidade no Brasil tem sido um tema de relevância crescente ao longo das últimas décadas. A noção de privacidade como um direito fundamental começou a ser reconhecida e protegida de forma mais efetiva a partir da promulgação da Constituição Federal de 1988, que consagrou a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

O Artigo 5º, inciso X, da Constituição estabelece que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação". Esse dispositivo constitucional conferiu uma base sólida para a proteção da privacidade no ordenamento jurídico brasileiro.

No entanto, a consagração do direito à privacidade na Constituição não foi suficiente para garantir sua efetividade na prática. Era necessário desenvolver leis específicas e mecanismos de proteção que regulamentassem e assegurassem a aplicação desse direito. Assim,

ao longo das décadas seguintes, foram criadas diversas leis e regulamentações que buscaram complementar a proteção à privacidade no Brasil.

Em 1990, foi promulgada a Lei nº 8.078, conhecida como Código de Defesa do Consumidor, que trouxe importantes dispositivos relacionados à proteção de dados pessoais. O Código estabeleceu, por exemplo, que o consumidor tem direito à proteção contra a publicidade enganosa e abusiva, que possa violar sua privacidade ou causar qualquer forma de constrangimento ou intimidação.

Outro marco importante na evolução do direito à privacidade no Brasil foi a promulgação da Lei nº 9.296/1996, conhecida como Lei de Interceptação Telefônica. Essa lei estabeleceu regras claras para a realização de interceptações telefônicas, assegurando que essa prática só pudesse ser realizada com autorização judicial, em situações específicas e mediante a observância de garantias fundamentais. Ela contribuiu para restringir abusos e proteger a privacidade das comunicações.

No final da década de 1990, o avanço da tecnologia e a popularização da internet trouxeram novos desafios para a proteção da privacidade. Com o aumento do uso da internet, surgiram questões relacionadas à privacidade *on-line*, como a coleta e o uso de dados pessoais pelos sites e serviços digitais. Nesse contexto, foi necessário estabelecer uma legislação específica para regulamentar essa área.

Foi somente em 2018 que o Brasil aprovou sua primeira lei geral de proteção de dados pessoais, a Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados (LGPD). Inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD estabelece regras claras para a coleta, uso, armazenamento e compartilhamento de dados pessoais por parte de empresas e órgãos públicos.

A LGPD atribui aos titulares dos dados o controle sobre suas informações pessoais, estabelecendo a necessidade de consentimento para o tratamento de dados, a transparência sobre as práticas de coleta e uso de informações, além de prever a obrigação das empresas de adotarem medidas de segurança adequadas para proteger os dados pessoais.

A LGPD também estabelece sanções administrativas para o descumprimento da lei, como advertências, multas e até mesmo a suspensão das atividades relacionadas ao tratamento de dados. Essa lei representa um avanço significativo na proteção da privacidade no Brasil e coloca o país em linha com as melhores práticas internacionais nesta área.

Além da LGPD, outras leis foram promulgadas nos últimos anos para proteger a privacidade e os dados pessoais dos brasileiros. É o caso, por exemplo, da Lei nº 13.853/2019,

que criou a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por zelar pela aplicação da LGPD e fiscalizar o cumprimento das normas de proteção de dados.

A evolução do direito à privacidade no Brasil reflete uma maior conscientização sobre a importância desse direito fundamental na sociedade contemporânea. O reconhecimento da privacidade como um direito humano fundamental e a criação de leis específicas para sua proteção são passos importantes para garantir que as pessoas possam exercer sua liberdade e autonomia na esfera pessoal, sem interferências indevidas.

No entanto, apesar dos avanços legislativos, ainda há desafios a serem enfrentados na proteção da privacidade no Brasil. A aplicação efetiva das leis, a conscientização da população sobre seus direitos e a promoção de uma cultura de respeito à privacidade são aspectos fundamentais para garantir que as pessoas possam desfrutar plenamente deste direito.

Em um contexto de constante avanço tecnológico, é necessário estar atento às novas demandas e ameaças à privacidade, como o uso indevido de informações pessoais por meio de aplicativos, redes sociais e outras plataformas digitais. Nesse sentido, a educação digital e a conscientização sobre boas práticas de proteção de dados são essenciais para que as pessoas possam navegar no ambiente digital de forma segura e consciente.

Em suma, a evolução do direito à privacidade no Brasil tem sido marcada por avanços significativos ao longo das últimas décadas, desde a consagração desse direito na Constituição de 1988 até a promulgação da LGPD em 2018. No entanto, é fundamental continuar aprimorando a legislação e as práticas de proteção da privacidade, garantindo que os direitos individuais sejam preservados no contexto digital e em todas as esferas da vida.

A privacidade está intimamente ligada à proteção de dados. Ela é o resultado da soma da pessoa com a informação e o segredo. Já a proteção de dados é a soma da pessoa, com a informação e o controle. Sendo assim, com a proteção de dados, houve um aumento do conceito de privacidade. Por isso é tão importante saber a evolução histórica do tema de Direito à privacidade pelo mundo, em especial, nos Estados Unidos e na Alemanha, pois se de um lado, os americanos tratam a privacidade pela ótica do indivíduo, por outro lado, a legislação alemã entende que a privacidade se dá à proteção dos dados desse indivíduo.

O Brasil foi altamente influenciado pelas duas legislações, inclusive, o nosso Supremo Tribunal Federal baseou-se no conceito de autodeterminação de informação, utilizado na Alemanha, para criar a Medida Provisória 954, reconhecendo que a proteção de dados é um elemento sinérgico à privacidade, ou seja, com a proteção de dados, houve um aumento do conceito de privacidade.

4. CONFLITO ENTRE ACESSO À INFORMAÇÃO E PRIVACIDADE

Acesso à informação e privacidade são dois princípios fundamentais na era da informação. Embora ambos tenham um papel crucial no desenvolvimento social e tecnológico, frequentemente entram em conflito. A tensão entre esses dois valores reflete um paradoxo da modernidade: o desejo de saber mais (acesso à informação) contra o desejo de proteger a intimidade e os dados pessoais (privacidade).

A era da informação trouxe uma explosão de dados, disponibilizando ao público uma quantidade sem precedentes de informação. A ideia de "conhecimento livre" defende que, para o bem comum, a informação deve ser acessível a todos. Essa concepção valoriza a transparência, a responsabilização e a democracia, todas fundamentadas no acesso livre e aberto à informação.

No entanto, essa abertura traz consigo riscos significativos para a privacidade. Informações pessoais, dados confidenciais e conteúdos sensíveis, quando mal geridos ou mal utilizados, podem prejudicar indivíduos e organizações. Isso tem levado a um interesse crescente na proteção da privacidade, com leis de proteção de dados sendo implementadas ao redor do mundo.

Há uma tensão intrínseca entre acesso à informação e privacidade. Uma maior divulgação de informações pode levar a uma erosão da privacidade. Inversamente, a proteção estrita da privacidade pode limitar o acesso à informação. As fronteiras entre o público e o privado estão constantemente sendo redefinidas e negociadas nesta dinâmica.

Vamos considerar, por exemplo, as redes sociais. Elas dependem da partilha de informações para funcionar. Os usuários compartilham informações pessoais, ideias e experiências, promovendo a comunicação e a interação. No entanto, essas plataformas também coletam, armazenam e utilizam essas informações para diversos fins, muitas vezes sem o consentimento explícito dos usuários.

Essa coleta massiva de dados levanta sérias preocupações com a privacidade. Os usuários podem não estar cientes da extensão da coleta de dados, nem de como eles são utilizados. Além disso, a falta de segurança adequada pode levar a vazamentos de dados, expondo informações privadas.

A transparência é outro ponto de tensão. O acesso à informação requer transparência. No entanto, muitas vezes, as organizações preferem manter suas operações e decisões em segredo para obter a vantagem competitiva ou por motivos de segurança. Isso pode impedir a responsabilização e prejudicar a confiança do público.

Por outro lado, a transparência excessiva pode ser prejudicial. A divulgação de informações sensíveis pode colocar indivíduos ou organizações em risco. Portanto, é necessário um equilíbrio entre transparência e proteção da privacidade.

Também há a questão do consentimento. O acesso à informação muitas vezes depende do consentimento dos indivíduos para coletar e usar seus dados. No entanto, o consentimento nem sempre é informado. Os termos de serviço e as políticas de privacidade podem ser longos e confusos, levando os usuários a concordar sem entender completamente as implicações.

Em uma sociedade democrática, o acesso à informação é essencial. No entanto, este acesso deve ser equilibrado com o direito à privacidade. A questão é como garantir esse equilíbrio. Leis de proteção de dados, como o Regulamento Geral de Proteção de Dados da União Europeia, estão ajudando a definir esse equilíbrio, mas a aplicação ainda é um desafio.

Além disso, a tecnologia está sempre avançando, criando novos desafios. Por exemplo, a inteligência artificial pode processar grandes quantidades de dados para revelar padrões e tendências. Isso pode ser útil, mas também pode ser usado para analisar indivíduos ou grupos, potencialmente invadindo a privacidade.

O conflito entre acesso à informação e privacidade é uma questão complexa que não pode ser resolvida com uma solução única. Exige um equilíbrio cuidadoso, com leis de proteção de dados, educação digital e melhores práticas de gestão de dados. À medida que avançamos na era da informação, essa questão continuará a ser relevante e desafiadora.

A proteção da privacidade e a liberdade de informação (informar e ser informado), como condições à dignidade da pessoa humana, não podem ser violadas ou anuladas uma pela outra, ainda que se admita uma limitação.

Mesmo as pessoas expostas, por sua própria vontade, possuem direito a controlar a coleta e a transmissão de seus dados privados, ainda que sua esfera de privacidade seja reduzida.

Deve-se considerar a exposição individual de cada um na ponderação da existência ou não de invasão da sua vida privada, considerando e diferenciando o tratamento individual das personalidades públicas e pessoas comuns. Fica resguardado, de forma mais ampla, para as pessoas comuns.

A informação é uma ferramenta essencial para proteção de um país, para a inserção de um indivíduo na sociedade e para a formação de sua própria personalidade, tornando-se fundamental para a economia. O dado da informação é a riqueza da atualidade e moldará o futuro. Castells (1999), em sua obra intitulada *A sociedade em rede*, afirma que “a fonte de produtividade acha-se na tecnologia da geração de conhecimentos, de processamento da informação e de comunicação de símbolos”.

Se não controlado e mensurado de forma equitativa e igualitária, o tratamento de dados poderá possuir um condão devastador na vida privada de um indivíduo.

O professor Vicenzo Ferrari (2000), explica a palavra informação com o olhar tecnológico: compreende um dado "in-formação", pois a coleta, seu armazenamento e seu tratamento, na realidade formam conhecimentos, opiniões e podem ser capazes de demonstrar a própria personalidade do indivíduo, ainda que parcial.

É importante ter em mente que, por um lado, a informação utilizada de forma exacerbada e com desvio de finalidade é uma afronta a privacidade, que deve ser garantida, bem como empodera demasiadamente os detentores dessas informações. Já a sonegação de informação de uma pessoa para a sociedade poderá causar uma verdadeira exclusão social, sendo-lhe negado acesso a bens básicos para a vida, como programas sociais, saúde, educação ou mesmo o acesso ao crédito.

Atualmente, a denominada sociedade da informação, tem como principal característica a valorização do conhecimento e da informação, em especial daqueles adquiridos com a coleta e tratamento de dados. O dado e sua interpretação tem demasiado poder para direcionar e manipular a formação da pessoa, impedindo seu livre desenvolvimento e interferindo na sua capacidade de escolhas e senso crítico.

Nossa privacidade é minimizada diariamente, através de aplicativos diversos de coleta e armazenamento de dados, como saúde, localização, trânsito, compras, cartões de créditos, dentre outros.

Esses dados devem receber a verdadeira tutela jurídica, pois, se de um lado, a falta de acesso a dados mínimos, se dá uma efetiva exclusão do homem, sua vulnerabilidade, por outro lado, poderá levar a lesão de direitos.

A verdadeira função dos bancos de dados é o fornecimento de dados para fortalecimento da economia, sociedade e o desenvolvimento individual da plena personalidade, que somente é possível por meio de liberdade de escolha.

Vale ressaltar que a abrangência demasiada das exceções ao direito à informação poderá causar o fator reverso e prejuízos aos indivíduos, pois algumas informações, ainda que econômicas, são de interesse social.

A própria ONU – Organização das Nações Unidas, já se manifestou acerca das necessidades de ponderação entre os direitos à informação e à privacidade. Restrições devem ser proporcionais e claras, definidas em lei que seja acessível, concreta, clara e sem qualquer ambiguidade.

O direito à informação serve como base à vida individual de cada pessoa, possibilitando suas escolhas e a formação do seu livre convencimento.

Quando se fala de informações, logo falamos de proteção de dados e cadastros. Não se trata apenas de cadastros de consumo, mas sim, que a proteção de dados abarca todo e qualquer dado inerente às pessoas, e aqui se encontram os dados políticos, genéticos, mercantis, sociais, religiosos, biométricos, bancários, dentre outros objetivos, sem excluir os cadastros de consumo.

5. COMO TER PRIVACIDADE COM A DISTRIBUIÇÃO DE DADOS?

O advento da tecnologia digital e da internet transformou a maneira como nos comunicamos e fazemos negócios, trazendo diversos benefícios. No entanto, isso também levou a um aumento substancial na quantidade e na frequência com que os dados são coletados, armazenados e distribuídos. Isso gerou preocupações sobre privacidade e segurança dos dados.

A primeira etapa para proteger a privacidade na distribuição de dados é entender o que é realmente necessário para coletar e compartilhar. Em muitos casos, os dados são coletados e distribuídos sem que o indivíduo entenda o que está sendo coletado e para qual finalidade. Portanto, é fundamental que as organizações sejam transparentes sobre suas práticas de coleta e compartilhamento de dados. Além disso, elas devem oferecer aos indivíduos a capacidade de optar por não compartilhar seus dados.

A criptografia é uma ferramenta poderosa que pode ser usada para proteger os dados durante a coleta, o armazenamento e a distribuição. Ela funciona convertendo os dados em um formato que só pode ser lido por aqueles que possuem uma chave de descriptografia especial. Isso torna muito mais difícil uma pessoa não autorizada acessar os dados.

A minimização de dados também é uma estratégia importante para proteger a privacidade. Isso envolve coletar apenas os dados gerados para uma determinada finalidade. Ao limitar a quantidade de dados coletados e compartilhados, reduz-se o risco de violação de privacidade.

Uma abordagem mais recente à privacidade dos dados é o uso de técnicas de aprendizado de máquina federada. Isso permite que os modelos de aprendizado de máquina sejam treinados em dados distribuídos, sem a necessidade de transferir os dados brutos para uma central local. Isso pode fornecer um alto nível de privacidade, pois os dados individuais nunca precisam sair do dispositivo ou da rede onde são armazenados.

As leis e regulamentos de proteção de dados têm um papel importante a cumprir na proteção da privacidade na distribuição de dados. Leis como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia e a Lei de Proteção de Privacidade do Consumidor da Califórnia (CCPA) estão estabelecendo novos padrões para a coleta, o armazenamento e a distribuição de dados.

Garantir a privacidade na distribuição de dados é um desafio complexo que requer uma combinação de práticas de gerenciamento de dados, técnicas de proteção de dados e regulamentações legais. No entanto, ao priorizar a privacidade desde o início, as organizações podem não apenas proteger os direitos dos indivíduos, mas também ganhar sua confiança e lealdade a longo prazo.

A privacidade dos dados é uma questão que se tornou ainda mais proeminente na era digital, em que informações valiosas são flexíveis a um ritmo impressionante. A distribuição de dados, seja para fins de análise de negócios, para aprimorar a experiência do usuário ou para facilitar as operações, é uma prática comum. No entanto, como garantir a privacidade durante essa distribuição é uma pergunta que deve ser abordada com muita seriedade.

I. Entendendo a Privacidade dos Dados:

A privacidade dos dados refere-se ao direito de que um indivíduo tem de manter suas informações pessoais longe de acesso não autorizado, uso indevido, divulgação ou destruição. Esse conceito estende-se a todos os formatos de dados, incluindo digital e físico. A privacidade dos dados está profundamente enraizada em leis e regulamentos de privacidade, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e a Lei de Proteção de Dados Pessoais (LGPD) no Brasil.

II. Riscos à Privacidade dos Dados na Distribuição de Dados

A distribuição de dados, se não for feita corretamente, pode levar a vários riscos à privacidade dos dados. Isso inclui a possibilidade de vazamentos de dados, em que as informações são acidentalmente expostas a partes não autorizadas. Os dados também podem ser interceptados durante a transferência, dando a atores mal-intencionados a chance de acessar, alterar ou destruir informações. Além disso, se os dados não forem devidamente anonimizados ou pseudonimizados antes da distribuição, pode haver riscos à privacidade do indivíduo a quem os dados se referem.

III. Estratégias para a Privacidade dos Dados na Distribuição de Dados

Existem várias estratégias que podem ser integradas para garantir a privacidade dos dados durante a distribuição de dados. Elas incluem:

Criptografia: A criptografia é uma técnica essencial para proteger a privacidade dos dados durante a distribuição. A criptografia transforma dados legíveis em um formato codificado que só pode ser lido ou processado após a descriptografia. Ao distribuir dados, a criptografia pode ajudar a prevenir a interceptação e o acesso não autorizado aos dados.

Anonimização e Pseudonimização: O gerenciamento de consentimento é um aspecto importante da privacidade dos dados. As organizações devem obter o consentimento explícito dos indivíduos antes de receber, processar ou distribuir seus dados. Além disso, os indivíduos devem ter a capacidade de retirar seu consentimento a qualquer momento.

Gerenciamento de consentimento: O gerenciamento de consentimento é um aspecto importante da privacidade dos dados. As organizações devem obter o consentimento explícito dos indivíduos.

Segurança de Dados: A segurança dos dados envolve a implementação de medidas para proteger os dados contra acessos não autorizados, alterações, destruição ou continuidade. Isso inclui o uso de firewalls, sistemas de detecção de intrusões, autenticação de dois fatores, entre outros.

A privacidade na distribuição de dados é uma questão complexa que exige uma abordagem multifacetada. Ao implementar estratégias como criptografia, anonimização, gerenciamento de consentimento e segurança dos dados, as organizações podem garantir que a privacidade seja mantida durante a distribuição de dados. É importante lembrar, no entanto, que a privacidade dos dados é um esforço contínuo que exige monitoramento constante e adaptação à medida que novas ameaças e desafios surgem.

CONCLUSÃO

Na era digital em que vivemos, a privacidade parece estar em um terreno cada vez mais frágil. Com o avanço da tecnologia, das redes sociais e da informatização, somos constantemente questionados: o homem ainda tem privacidade?

A tecnologia, em muitos aspectos, tornou-se uma espada de dois gumes. Por um lado, facilitou a comunicação, o acesso à informação e instrumentos, um mundo de possibilidades

que facilitam a vida de muitos. Por outro lado, a digitalização de nossas vidas colocou em xeque a ideia de privacidade. Cada interação online, cada "clique", deixa um rastro digital, que pode ser coletado, analisado e usado para diferentes fins.

As redes sociais, por exemplo, são plataformas onde compartilhamos aspectos pessoais de nossas vidas. As informações que fornecemos, como fotos, localização, interesses, estão disponíveis para quem quiser ver, e, muitas vezes, são usadas por empresas para fins de publicidade.

Além disso, nossos smartphones e outros dispositivos inteligentes são constantemente alimentados com nossos dados, desde nossos hábitos de navegação até nossos padrões de sono. Esses dados, embora sejam inofensivos, podem revelar informações sensíveis sobre nós, quando analisados em conjunto.

Outro ponto de preocupação é a vigilância governamental. Em nome da segurança nacional, muitos governos ao redor do mundo aumentaram sua capacidade de vigilância digital. Isso levanta questões sobre o direito à privacidade e o risco de abuso de poder.

Mas então, o homem ainda tem privacidade? A resposta não é tão simples. Embora existam ameaças à nossa privacidade, ainda existem opções de proteção em vigor.

Em primeiro lugar, existem as leis de proteção de dados que procuram proteger a privacidade dos indivíduos. Essas leis exigem que as empresas tratem os dados pessoais de forma responsável e transparente, e forneçam aos indivíduos o direito de acessar, corrigir e apagar seus dados.

Em segundo lugar, existem tecnologias disponíveis para ajudar a proteger nossa privacidade online. Criptografia, VPNs, navegadores privados e outros softwares de segurança podem ajudar a proteger nossos dados e atividades online de olhos curiosos.

Finalmente, cada indivíduo tem o poder de proteger sua própria privacidade. Isso envolve fazer escolhas ecológicas sobre o que compartilhamos *on-line*, ler e entender as políticas de privacidade das plataformas que usamos, e tomar medidas para proteger nossos dados pessoais.

Em conclusão, a privacidade na era digital é uma questão complexa que envolve uma mistura de legislação, tecnologia e comportamento individual. Embora existam ameaças reais à nossa privacidade, também existem meios de protegê-la. A chave é a conscientização e a educação sobre nossos direitos.

REFERÊNCIAS BIBLIOGRÁFICAS

CASO KATZ V. ESTADOS UNIDOS, (1967), Disponível em https://supreme.justia.com/cases/federal/us/389/347/. Acesso em: 15 maio 2023.

CASTELLS, Manuel. **A Sociedade em Rede**: a era da informação, economia, sociedade e cultura), São Paulo: Paz e Terra, 1999, v1.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: Editora Revistas dos Tribunais, 2021.

FERRARI, Vicenzo. Mídia e Direito à informação. *In*: GERMAN, Christiano *et al*. **Informação e democracia**. Rio de Janeiro: Ed. da UERJ, 2000, p. 165.

MARTINS, Leonardo. (org.) **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal alemão**. [Coletânea original: Jürgen Schwabe. Tradução de Beatriz Hennig; Leonardo Martins; Mariana Bigelli de Carvalho; Tereza Maria de Castro; Vivianne Geraldes Ferreira]. Montevidéu: Konrad-Adenauer-Stiftung, 2005.

MIRANDA, Leandro Alvarenga. **A proteção de dados pessoais e o paradigma da privacidade**. 1. ed. São Paulo: All Print Editora, 2018.

NATIONAL CONSTITUCION CENTER. **Caso Olmstead V. Estados Unidos** (1928). Disponível em: https://constitutioncenter.org/the-constitution/supreme-court-case-library/olmstead-v-united-states . Acesso em: 15 maio 2023.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada.** Belo Horizonte: Del Rey, 1998.

UNITED STATES OF AMERICA [Constituição (1791)]. **Constitution of the United States - Fourth Amendmen**, Disponível em: https://constitution.congress.gov/constitution/amendment-4/. Acesso em: 15 maio 2023.

WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privac**y. Harvord Law Review. Disponível em: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acesso em: 15 maio 2023.

REDAÇÃO OESTE. **SUPREMA CORTE DOS EUA DERRUBA DIREITO CONSTITUCIONAL AO ABORTO**. **Revista Oeste**, São Paulo, v. 1, n. 1, p. 1-1, jun. 2022. Disponível em: https://revistaoeste.com/mundo/suprema-corte-dos-eua-derruba-direito-constitucional-ao-aborto/. Acesso em: 28 ago. 2023.