# XI ENCONTRO INTERNACIONAL DO CONPEDI CHILE - SANTIAGO

# DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

ZULMAR ANTONIO FACHIN
FABIANO HARTMANN PEIXOTO

### Copyright © 2022 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos. Nenhuma parte deste anal poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

### Diretoria - CONPEDI

Presidente - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Diretora Executiva - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - UNIVEM/FMU - São Paulo

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Representante Discente: Prof. Dra. Sinara Lacerda Andrade - UNIMAR/FEPODI - São Paulo

### Conselho Fiscal:

Prof. Dr. Caio Augusto Souza Lara - ESDHC - Minas Gerais

Prof. Dr. João Marcelo de Lima Assafim - UCAM - Rio de Janeiro

Prof. Dr. José Filomeno de Moraes Filho - Ceará

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Prof. Dr. Valter Moura do Carmo - UNIMAR - São Paulo

#### **Secretarias**

### Relações Institucionais:

Prof. Dra. Daniela Marques De Moraes - UNB - Distrito Federal

Prof. Dr. Horácio Wanderlei Rodrigues - UNIVEM - São Paulo

Prof. Dr. Yuri Nathan da Costa Lannes - Mackenzie - São Paulo

### Comunicação:

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - Paraíba

Prof. Dr. Matheus Felipe de Castro - UNOESC - Santa Catarina

### Relações Internacionais para o Continente Americano:

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Prof. Dr. Jerônimo Sigueira Tybusch - UFSM - Rio Grande do Sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

### Relações Internacionais para os demais Continentes:

Prof. Dr. José Barroso Filho - ENAJUM

Prof. Dr. Rubens Beçak - USP - São Paulo

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - Paraná

### **Eventos:**

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - Minas Gerais

Profa. Dra. Cinthia Obladen de Almendra Freitas - PUC - Paraná

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - Mato Grosso do Sul

Membro Nato - Presidência anterior Prof. Dr. Raymundo Juliano Feitosa - UMICAP - Pernambuco

### D597

Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Fabiano Hartmann Peixoto; Zulmar Antonio Fachin – Florianópolis: CONPEDI, 2022.

Inclui bibliografia

ISBN: 978-65-5648-567-6

Modo de acesso: www.conpedi.org.br em publicações

Tema: Saúde: Direitos Sociais, Constituição e Democracia na América Latina

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Internacionais. 2. Governança. 3. Novas tecnologias. XI Encontro Internacional do CONPEDI Chile - Santiago (2: 2022: Florianópolis, Brasil).

CDU: 34



# XI ENCONTRO INTERNACIONAL DO CONPEDI CHILE -SANTIAGO

### DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

### Apresentação

O XI ENCONTRO INTERNACIONAL DO CONPEDI, com temática "Direitos sociais, Constituição e Democracia na América Latina", ocorrido entre os dias 13 e 30 de outubro de 2022, reuniu centenas de pesquisadores de diversos países. Com submissão extremamente substantiva, a linha de pesquisa Direito, Governança e Novas Tecnologias necessitou de subdivisão. A presente apresentação, então, refere-se aos trabalhos submetidos, selecionados e efetivamente apresentados e discutidos no GT Direito, Governança e Novas Tecnologias II.

Foi traço marcante a discussão sobre os impactos e as interfaces da tecnologia com temas tradicionais do Direito. Percebeu-se nela um papel extremamente relevante para o desenvolvimento do conhecimento e ensino jurídicos.

Fenômeno intensificado na última década, a tecnologia vem provocando análises e/ou avaliações no campo constitucional, processo e especialidades jurídicas. O cenário digital e cibernético teve abordagens multidisciplinares em trabalhos aprofundados. Assim, destacamse as grande temáticas do GT:

- Inteligência Artificial
- Algoritmos
- Metaverso
- Lei Geral de Proteção de Dados
- Economia disruptiva
- Autodeterminação informacional
- Provas digitais
- Regulação internacional de dados

- Regulação de ciberespaço
- Compliance
- Inclusão digital

Centralmente, os trabalhos sobre Inteligência Artificial buscaram demonstrar a íntima relação entre compromissos éticos no uso ou desenvolvimento de sistemas com referenciais de direitos fundamentais. Discutiu-se, da mesma forma, os impactos dos novos sistemas de IA nos conceitos e alcances de institutos tradicionais do Direito, tais como a responsabilidade civil.

Igualmente presente, as análises de estratégias regulatórias também ocuparam relevante espaço no GT, especialmente no sentido dos desafios internacionais sobre a temática. Manifestações mais recentes da tecnologia no campo jurídico também foram apresentadas, destacando-se a interface dos direitos da personalidade no metaverso e a ampliação dos chamados "cookies" como ferramentas de potenciais fragilizações no sistema de proteção de dados.

Apresentado por pesquisadores do país anfitrião (Chile), aspectos da economia disruptiva em interface com a tecnologia promoveram debates sobre possíveis leituras chilenas das influências econômicas sobre o Direito e uma comparação com o panorama brasileiro.

Como não poderia ser diferente, os desafios da gestão e proteção de dados e os desdobramentos da Lei Geral brasileira também foram objeto de apresentação de pesquisas e demonstraram quantos novos desafios são postos à comunidade jurídica internacional.

Destacam-se, nesta breve apresentação, a análise e discussões sobre o incremento dos sistemas de certificação digital - tão intensificados em tempos de pandemia -, notadamente pelas inevitáveis dúvidas em razão do debate público-privado e das necessárias cautelas impostas pelos riscos de aumento na desigualdade entre cidadãos.

De uma maneira geral, as discussões do GT se encaminharam para a percepção de profundas alterações no modo tradicional de se observar o fenômeno jurídico, das inúmeras oportunidades apresentadas pela tecnologia e da proporcional necessidade de se observar riscos que as acompanham, especialmente sob a ótica de direitos fundamentais.

Dentro desta variedade interessante de relatos de pesquisa, os coordenadores desse grupo de trabalho convidam a todas e todos para a leitura na íntegra dos artigos.

Zulmar Antonio Fachin - Unicesumar e Faculdades Londrina - zulmarfachin@uol.com.br

Fabiano Hartmann Peixoto - Universidade de Brasília - fabiano\_unb@unb.br

# COOKIES INDIGESTOS: AS FERRAMENTAS DE SPYWARE SOB À LUZ DA LEI DE PROTEÇÃO DE DADOS

# INDIGESTIBLE COOKIES: THE TOOLS OF SPYWARE UNDER THE LIGHT OF DATA PROTECTION LAW

Adriana Rossini <sup>1</sup> Natalia Maria Ventura da Silva Alfaya <sup>2</sup> Anabela Cristina Hirata <sup>3</sup>

### Resumo

O trabalho traz uma reflexão sobre o uso dos cookies como ferramentas de spyware para a coleta de dados pessoais e de consentimento dos usuários à luz da Lei de Proteção de Dados. O problema que orienta a pesquisa pode ser sintetizado na seguinte pergunta: A política de cookies atual alcança a proteção dos dados pessoais dos usuários? A regulação que a nova legislação trouxe mudanças quanto ao trato das informações coletadas dos cidadãos brasileiros, como o direito para o titular acessar, editar ou solicitar a exclusão de seus dados, maior cuidado com dados sensíveis, portabilidade de dados e sanções administrativas se houver descumprimento mas, especialmente, quanto a coleta de dados autorizada, com destaque para as ferramentas que visam obter o consentimento do usuário quanto ao uso de suas informações. Tem por objetivo demonstrar como essas ferramentas personificam seus usuários, revestindo o usuário de uma falsa sensação de confiança e transparência quanto a política de privacidade, quando, na verdade, o simples consentimento não é suficiente para assegurá-los quanto ao bom uso de seus dados. Adota o método hipotético-dedutivo, utilizando-se de livros e artigos científicos produzidos no Brasil e no exterior. Questiona a eficácia da proteção à intimidade através do uso de cookies e a dificuldade da aplicação do Direito diante das inovações tecnológicas. Conclui que a utilização desses dados sem o conhecimento dos usuários caracteriza violação à privacidade e aponta para necessidade de um novo modelo de transparência em sua utilização.

**Palavras-chave:** Cookies, Dados pessoais, Consentimento, Privacidade e transparência, Lei de proteção de dados

<sup>&</sup>lt;sup>1</sup> Mestranda no Programa de Mestrado Profissional em Direito, Sociedade e Tecnologias das Faculdades Londrina. E-mail: adrianarossini.adv@gmail.com

<sup>&</sup>lt;sup>2</sup> Doutora em Ciências Sociais e Jurídicas pela UFF. Professora no Programa de Mestrado Profissional em Direito, Sociedade e Tecnologias da Escola de Direito das Faculdades Londrina. E-mail: naty.alfaya@gmail.com

<sup>&</sup>lt;sup>3</sup> Mestre em Direito, Sociedade e Tecnologias (Faculdades Londrina). Aluna Especial na disciplina de "Direito e Inteligência Artificial" (UnB). Bacharel em Direito (PUCPR). Advogada. ORCID – 0000-0002-8729-523X. Email: anabelahirata@hotmail.com.

### Abstract/Resumen/Résumé

The work brings a reflection on the use of cookies as spyware tools for the collection of personal data consent of users in the light of the Data Protection Act. The problem that guides the search can be synthesized in the following question: Does the current cookie policy achieve the protection of users' personal data? The regulation that the new legislation presentes brought changes in the treatment of information collected from Brazilian citizens, as the right for the holder to access, edit or request the deletion of his/her data, greater care for sensitive data, data portability and administrative sanctions if there is non-compliance but, especially, regarding the authorized data collection, with emphasis on the tools aimed at obtain the user's consent to the use of their information. It aims to demonstrate how these tools embody their users, the user with a false sense of trust and transparency regarding the privacy policy, when, in fact, simple consent is not enough to assure them of the proper use of their data. It adopts the hypothetical-deductive method, using books and scientific articles produced in Brazil and abroad. It questions the effectiveness of protection of intimacy through the use of cookies and the difficulty of applying the law in the face of technological innovations. It concludes that the use of this data without the knowledge of users caracterizes a violation of privacy and points to the need for a new model of transparency in its use.

**Keywords/Palabras-claves/Mots-clés:** Cookies, Personal data, Agreement, Privacy and transparency, Data protection law

# 1 INTRODUÇÃO

A crescente evolução das novas tecnologias de informação tem proporcionado às empresas avanços significativos nos mecanismos de coleta de dados pessoais de seus usuários. Embora o uso dessas ferramentas proporcione uma melhoria significativa nas relações com seus consumidores, o uso abusivo e o compartilhamento irrestrito dessas informações violam os princípios norteadores do uso da internet no Brasil, pontuados pela Lei de Proteção de Dados.

Assim, por meio de revisão bibliográfica e legislativa, questiona-se a eficácia da proteção à intimidade em face do uso dos *cookies* como ferramentas de *spyware* e a dificuldade da aplicação do Direito diante das constantes inovações tecnológicas.

Através da análise dos principais aspectos que a tecnologia traz para a sociedade atualmente, pretende-se verificar o uso dos cookies para o consentimento dos termos de uso conforme determina a Lei de Proteção de dados e seu alcance e efetividade. Como objeto principal, pretende verificar os reflexos produzidos pelos *cookies* e *spams* como verdadeiras ferramentas de *spyware*.

Conclui-se que a obtenção e utilização de dados pessoais sem o consentimento dos usuários caracteriza violação a privacidade, ferindo a dignidade da pessoa humana, motivo pelo qual propõe-se um modelo de transparência desde a coleta até a utilização dos dados pessoais, de forma a estar ao alcance dos usuários tanto a autorização para a coleta e uso quanto a desistência e exclusão total dos dados pessoais pelo titular da aplicação de Internet.

### 2 INTERNET DAS COISAS

A internet tem proporcionado uma enorme mudança na vida das pessoas. A conectividade revolucionou o cotidiano do mundo e causou reflexos nas inter-relações sociais, culturais, econômicas e políticas do ser humano.

Neste contexto, as inovações voltaram-se para a Internet das Coisas ou, Tecnologia das Coisas, onde a ideia por trás deste conceito teve origem em novas possibilidades originadas através de dispositivos inteligentes conectados a internet, que possibilitassem desta forma, a comunicação a partir de qualquer lugar, a qualquer momento, por um dispositivo (DINIZ, 2006).

A Internet das coisas, em inglês, *Internet of Things* (IoT) foi uma expressão criada por Kevin Ashton, pesquisador britânico do *Massachusetts Institute of Technology* (MIT), desde 1999, em referência a habilidade de diversos tipos de objetos conseguirem estabelecer conexão com a internet (ZAMBARDA, 2014).

Atualmente, é possível encontrar dispositivos IoT sendo utilizados tanto em situações comuns da vida diária como no âmbito profissional. Desse modo, essas ferramentas tecnológicas estão contribuindo para o acontecimento da transformação digital no mundo.

Esta revolução tecnológica trouxe consigo importantes inovações e possibilidade relacionadas a área de negócios, pesquisas, nichos de mercado assim como novos desafios (LEMOS; MARQUES, 2018).

Podemos citar vários exemplos de uso dessas tecnologias no dia a dia e dentre as suas diversas aplicações, podemos observar a utilização da IoT em: aplicativos de celular, que permitem indicar o melhor percurso no trânsito, evitando que pessoas cheguem atrasadas ao trabalho ou a outros lugares; etiquetas com sensores de rádio frequência coladas em uniformes escolares, permitindo fazer o monitoramento da presença dos alunos em sala de aula; geladeiras que informam os produtos que estão faltando nas suas prateleiras, enviando a lista de compras diretamente para o supermercado; além de outras aplicações que facilitam a rotina e o cotidiano das pessoas (SINGER, 2012).

Um grande exemplo: A casa inteligente. Cada vez mais presentes nas residências, inúmeros aparelhos baseados na IoT, como *Smart* Tvs, Termostatos, Geladeiras, Máquinas de lavar, Cafeteiras, fechaduras inteligentes, sem mencionarmos os assistentes virtuais Google Home (Google), Alexa (Amazon), Siri (Apple), entre outros, como Bixby (Samsung) e Cortana (Windows). Apenas para ilustrar, o assistente virtual é uma secretária digital ou um ajudante online, acionado por comando de voz ou texto, que interage com os usuários e tem a capacidade de interpretar conteúdos e entender os comandos recebidos, sem dificuldades. Com este assistente você pode fazer simples buscas na internet e até garantir o controle da sua casa inteligente. Foi considerado o equipamento com tecnologia de IoT mais procurado em 2021<sup>1</sup>.

\_

Conforme relatório de pesquisa "2021 Global IoT Trends" in https://embarcados.com.br/relatorio-da-pesquisa-2021-global-iot-trends/

Outro exemplo bastante procurado são os *Wearables*, que são os equipamentos vestíveis de tecnologia IoT, ou seja, acessórios que utilizamos no corpo, como *smartwatches* e fones de ouvidos *wireless* (sem fio).

A IoT invadiu o seguimento da saúde e hoje a tecnologia ajuda na integração com o prontuário do paciente, atualizando e informando a cada instante qualquer alteração no estado clínico, como pressão sanguínea e frequência cardíaca, otimizando o atendimento e o tratamento médico.

Outro grande seguimento que se rendeu a tecnologia IoT é o da agricultura, pois sensores de acesso a internet monitoram a todo o tempo a temperatura, umidade do solo e do ar, ativando automaticamente os sistemas de irrigação, sempre que necessário e conectando todos os integrantes daquele manejo, tornando-o cada vez mais eficaz e lucrativo.

Na verdade, quando pensamos em avanço tecnológico, a noção de Internet das coisas é um dos assuntos que primeiro se destacam. Afinal, esse fenômeno vem moldando e desenhando nosso futuro de forma completamente inédita. E, para os céticos e avessos à tecnologia, que se perguntam, de que "coisas" estamos falando? A resposta é: qualquer coisa!

Coisas do cotidiano se tornam mais inteligentes e têm suas funções ampliadas por cruzamentos de dados. Isso é o que acontece quando um assistente virtual cruza dados dos seus dispositivos conectados para te informar, mesmo que você não tenha solicitado, o tempo que você levará para chegar ao trabalho quando você senta no seu carro para sair de casa.

Sem dúvidas, a tecnologia de IoT que mais se popularizou, foram os chamados gadgets, que são dispositivos eletrônicos portáteis como smartphones, smartwatches, e-readers, vídeo games. Mas sua difusão rápida, também trouxe grande preocupação. Tais dispositivos não sabem onde você vai por magia, mas sim pela interconectividade dos dispositivos inteligentes a sua volta. Assim, tais dispositivos conectados a rede de internet das coisas, estão todo o tempo emitindo, recebendo, trocando e cruzando dados. Na verdade, o ser humano produz mais dados do que pode imaginar.

A IoT não se restringe apenas à conexão de dispositivos eletrônicos à internet, mas também ao compartilhamento de informações realizado entre eles, permitindo dessa forma que diversas informações possam ser acessadas de forma rápida e eficiente.

Surge dessa nova inter-relação do ser humano com a internet, o fenômeno BIG DATA: grandes e massivos conjuntos de dados, gerados pelos usuários da rede mundial

de computadores<sup>2</sup> – internet - que precisam ser processados e armazenados. Com esse "novo" fenômeno, um dos maiores problemas que as empresas enfrentarão, é com a grande quantidade de informações que esses dispositivos passam a produzir.

A Internet das Coisas (IoT) é o "filho mais promissor" da chamada Industria 4.0 e tem sido apontada como a tecnologia mais transformadora da atualidade, proporcionando às empresas maior eficiência, flexibilidade e oportunidades de crescimento. Entretanto, conforme os sistemas se tornam cada vez mais complexos, suas vulnerabilidades aumentam e a segurança continua a ser a maior preocupação na implementação de IoT.

A nova revolução industrial é também chamada de Indústria 4.0 e possui como característica a integração de sensores e elementos da produção conectados na rede, unindo mundo real e virtual. Portanto, sendo a Indústria 4.0 o princípio de uma nova revolução industrial, pode-se afirmar que a automação vem mudando o modo de como os bens são produzidos através de novas tecnologias.

A Indústria 4.0 pode assumir outros nomes, como por exemplo "Indústria Inteligente" e "Fábrica Inteligente". Independentemente de sua nomenclatura, ela está diretamente relacionada com a IoT, sendo uma evolução que vem trazendo melhoria aos processos industriais, conectando não apenas máquinas, mas criando um *network* em toda a cadeia de produção de um produto. A Indústria 4.0 tem como objetivo tornar as informações mais acessíveis e em tempo real, além de reduzir ainda mais a interferência humana (GONÇALVES, 2016).

Podemos assim afirmar que, o maior desafio para o crescimento da Internet das Coisas apontada pela Indústria 4.0<sup>3</sup>, são preocupações relacionadas com confiança, segurança e privacidade (SILVEIRA, 2015).

# 3 INTIMIDADE E PRIVACIDADE: A PROTEÇÃO DE DADOS NA INTERNET

funcionava como editor, criado por Berners-Lee. https://tecmasters.com.br/historia-do-world-wide-web-famoso-www/

A World Wide Web foi criada por Tim Berners-Lee, físico e cientista da computação britânico, em 12 de março de 1989. Quando trabalhava na Organização Europeia para a Pesquisa Nuclear (CERN), ainda em 1980, Tim Berners-Lee propôs um projeto baseado em hipertexto (informações interligadas de forma não-linear), para facilitar o compartilhamento de informações entre os pesquisadores. Mais adiante, em 1989, percebeu a oportunidade de unir o projeto em hipertexto e a internet, o que deu origem à World Wide Web. O primeiro site do CERN foi criado em 1990, por meio de um navegador que também

<sup>&</sup>lt;sup>3</sup> Silveira (2015) afirma que a indústria 4.0 tem o conceito básico da conexão entre máquinas em tempo real, que possibilita que as empresas criem redes inteligentes que controlam todos os módulos de produção de forma autônoma, podendo assim prever falhas e agendar manutenções.

Embora o tema pareça novo, assuntos relativos à proteção de nossos dados e a privacidade no uso da internet são discutidos há anos.

Frise-se que a preocupação com o "right of privacy" (ZANINI, 2015, p. 3) foi uma das principais teses do direito estadunidense e já estava presente no seu sistema jurídico desde o século XIX. Em textos e decisões da Suprema Corte (in casu, Wheaton v. Peters), é possível identificar a expressão "ser deixado só", surgindo as primeiras ideias e conceitos de direito à privacidade, como inerentes a personalidade jurídica, não se limitando somente a terminologia da palavra privacidade, mas ampliando seu conceito. Destacam-se também, os casos Schuyler v. Curtis (1891) e Marks v. Jaffa (1893) como aqueles que teriam iniciado as discussões a respeito do right of privacy nos tribunais dos Estados Unidos (ZANINI, 2015, p. 4 e 5).

O tema - proteção de dados pessoais - se entrelaça de diversas formas com o inerente direito fundamental a privacidade e, embora a segurança de nossas informações não seja novidade na legislação mundial, as primeiras leis especificas para a proteção desses dados surgiram em meados dos anos 70.

No Brasil, o direito à privacidade é assegurado constitucionalmente como direito humano fundamental. A Constituição Federal de 1988, não se restringiu ao direito à privacidade e abrangeu à preservação da vida privada e da intimidade da pessoa, a inviolabilidade da correspondência, do domicílio e das comunicações. Correlato, mencionava de forma extensiva alguns pontos sobre a proteção de dados de seus cidadãos. No artigo 5°, inciso X: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" e no inciso XII: "É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal" (BRASIL, 1988).

No início dos anos 90 o Brasil desenvolveu um manual específico para as relações entre empresas e clientes editando o Código de Defesa do Consumidor, evoluindo ainda mais a busca pela defesa de informações discriminando ainda, uma seção

\_

<sup>&</sup>lt;sup>4</sup> Antes do artigo de Warren e Brandeis, vamos encontrar na obra do Juiz Thomas Cooley, publicada em 1880, sob o título *A Treatise on the Law of Torts*, a primeira utilização da expressão "right to be let alone". Apesar de ter cunhado a expressão, Cooley não a relacionou com a noção de privacy (RIGAUX, 1990, p. 272), mencionando-a em seu trabalho sobre responsabilidade civil (torts) como parte do seguinte trecho: "The right to one's person may be said to be a right of complete immunity: to be let alone" (COOLEY, 1880, p. 29).

específica sobre cadastros e banco de dados. No texto, a legislação defende o direito do consumidor acessar os dados que uma empresa tem sobre ele e solicitar sua correção, caso alguma informação esteja errada. O artigo 13º ainda deixa claro que dificultar o acesso às suas próprias informações ou deixar de comunicar ao titular sobre o registro de seus dados são consideradas infrações.

Há ainda artigos que garantem a privacidade e responsabilizam as empresas sobre a segurança dos dados, como o artigo 11º, capítulo 3: "Os dados pessoais do consumidor serão preservados, mantidos em sigilo e utilizados exclusivamente para os fins do atendimento" (BRASIL, 1990).

Mas alguns anos depois, com a Lei nº 9.296 de 1996, a legislação viria a acrescentar ser "inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

O ano de 2013 foi de extrema importância para a regulação das normas sobre privacidade online no Brasil, pois foi implementada a primeira lei sobre uso responsável da internet no país. Pela primeira vez foram vistos na legislação conceitos como a neutralidade de rede e a liberdade de expressão e definidas quais são as obrigações dos órgãos públicos no fornecimento de internet.

Em março de 2013, o decreto nº 7.962 ainda acrescentou orientações que complementam o Código de Defesa do Consumidor. O artigo 2º define que são diretrizes do Plano Nacional de Consumo e Cidadania a "autodeterminação, privacidade, confidencialidade e segurança das informações e dados pessoais prestados ou coletados, inclusive por meio eletrônico" (BRASIL, 2013).

O Marco Civil da Internet, assim chamada a Lei nº 12.965/2014, preocupou-se em regulamentar a forma como os direitos seriam protegidos no ambiente virtual. Tal marco foi o primeiro no Brasil a estabelecer de forma direta os "princípios, garantias, direitos e deveres para o uso da Internet no Brasil" (BRASIL, 2014).

Mas com os acontecimentos internacionais de 2018, observados casos de grandes vazamentos de dados, a má utilização de informações pessoais, e com o acinte da União Europeia decidindo revisitar suas regras de proteção de dados, culminando no Regulamento Geral de Proteção de Dados (GDPR), os legisladores brasileiros também viram a necessidade de compilar essas normas em um código específico, favorecendo o acesso normativo de todos.

Surgem, então, os primeiros esboços para uma lei brasileira específica à proteção dos dados pessoais, como uma alternativa ao Marco Civil da Internet.

Em 2020 entrou em vigor a Lei Geral de Proteção de Dados (LGPD), sendo a resposta dos legisladores brasileiros a esta crescente necessidade de normatizar o uso dos dados pessoais no mundo todo.

Claramente influenciada pelos princípios da diretiva europeia, a LGPD vale para todas as empresas que recolhem ou tratam dados no território nacional ou de cidadãos brasileiros.

Assim como o GDPR, alguns dos principais pontos da LGPD são: o direito para o titular acessar, editar ou solicitar a exclusão de seus dados, recolhimento autorizado (com exceção em casos específicos), maior cuidado com dados sensíveis, portabilidade de dados e sanções administrativas se houver descumprimento.

Vejam que, a União Europeia e seu Regulamento Geral de Proteção de Dados (GDPR), obrigou empresas do mundo todo – incluindo-se as gigantes Facebook e Google – a mudarem a forma como coletavam e usavam os dados de seus usuários, sendo responsável pelo fomento de uma onda de novas leis sobre o tema no mundo todo, inclusive no Brasil.

A sua aprovação, realça a importância dos direitos à privacidade e à proteção de dados, principalmente no que diz respeito aos ambientes digitais. Consequentemente, espera-se um fortalecimento das liberdades individuais e uma garantia jurídica maior à aplicação da Lei Geral de Proteção de Dados (LGPD), reforçando o compromisso e a preocupação do legislador em proteger os interesses e liberdades dos cidadãos.

Além disso, o engajamento em torno da proteção de dados e da privacidade, estimula os investimentos em tecnologia no país. Elevar o status de proteção de dados classificando-os como direitos e garantias fundamentais dos cidadãos, também fortalece as leis que regulam as relações interpessoais do cidadão brasileiro com a internet, conferindo uma estrutura pronta, sólida e segura para coletar, tratar, armazenar e empregar as informações dos usuários de forma adequada.

### 4 FERRAMENTAS TECNOLÓGICAS DE COLETA DE DADOS

Com o crescimento da tecnologia IoT, a indústria passou por grandes mudanças para assimilar o impacto dessas inovações. A IoT já é uma realidade e vem fortalecendo ainda mais a relação entre o homem e as máquinas. Sendo assim, ela pode ser aplicada

tanto no meio industrial, quanto em qualquer outro meio, desde que exista uma conexão com a internet.

Com o tempo, a quantidade de dados gerados foi crescendo de forma exponencial. De acordo com Junior (2012), as estimativas variam, mas todas concordam que existe um aumento na geração de dados, obrigando a indústria e suas plataformas a lidarem com essas informações despejadas na internet o tempo todo. Estima-se que a sociedade guarda mais de 13 *exabytes* em novos dados, a cada ano, e é devido a esta enorme quantidade de informações geradas que surge o conceito de Big Data.

Ainda segundo Junior (2012), o Big Data "[...] refere-se a o conjunto de dados cujo tamanho está além da habilidade de ferramentas típicas de banco de dados em capturar, gerenciar e analisar."

Na verdade, a captação cada vez mais acentuada de dados pessoais marca a sociedade atual. Seja para o fim de identificação dos usuários ou para classificação ou individualização de suas navegações, essas informações tornam-se cada vez mais obrigatórias para que o sujeito possa articular-se no ambiente digital.

Na sociedade da informação (CASTELLS, 2005) os dados tornam-se o aspecto central das inter-relações homem máquina e na modulação da realidade, sendo que se vislumbra uma dataficação das coisas e das pessoas. O armazenamento de dados em nuvem é um condicionador chave para a nova forma de organização social, pelo fato de salvaguardar um volume enorme de dados e seu acesso em diferentes partes do espaço físico e também através do possível e rápido compartilhamento dessas informações.

Para Castells, a sociedade, motivada pelo rearranjo das tecnologias da informação, muda suas bases materiais, tonando-se cada vez mais descentralizada, conectada e interdependente, sendo que uma revolução tecnológica concentrada nas tecnologias de informação passou a remodelar as bases da sociedade em ritmo acelerado.

A respeito da utilização desses dados pessoais para fins negociais e outros mais diversos e de aplicações infindáveis, configuram-se em verdadeiras "ferramentas digitais de coleta, tratamento e transferência de dados pessoais que potencializaram essas operações em quantidade, qualidade e velocidade, conferindo cada vez mais destaque a esse tema no contexto da tutela do consumidor" (ALIMONTI, 2010).

### 4.1 O CONSENTIMENTO DO USUÁRIO NO TRATAMENTO DE DADOS

O tratamento de dados carrega consigo a possibilidade de exposição e utilização indevida ou abusiva das informações privadas. E é nesse sentido que a Lei Geral de Proteção de Dados (LGPD) pautou seus mecanismos de proteção, tornando relevante o desenvolvimento de instrumentos que proporcionem ao sujeito o controle sobre as informações que compartilha. Ao mesmo tempo que surgem o valor de mercado e o valor social na manipulação de dados pessoais, surge também a necessidade de se regular este tratamento.

Em 2018, a promulgação da Lei Geral de Proteção de Dados partiu da premissa que o tratamento informatizado dos dados pessoais se relacionava diretamente com os direitos fundamentais de personalidade e privacidade, já amplamente discutidos em códigos e compilações legais. Com relação a essas proteções de direitos dos usuários, a LGPD detém como objeto a regulação sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Em sintonia com o que dispõe o Regulamento Europeu (GDPR) sobre o tema, propõe a proteção do indivíduo, através de duas premissas: controle exercido por cada titular e também pelo agente de tratamento de dados, o qual deve respeitar os institutos para a proteção do sujeito inclusive fornecer elementos para a plena qualificação do instituto do consentimento.

Verifica-se que a Lei Geral de Proteção de Dados define o consentimento como a "manifestação livre, informada, e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (artigo 5°, XII), neste sentido trata o consentimento como essa manifestação de vontade que autoriza a outrem o tratamento de dados pessoais.

Na LGPD, vontade e consentimento estão associados de forma prática na lei, condicionando o tratamento de dados, dentre outras possibilidades, pela concessão de consentimento do seu titular (inciso I, artigo 7°), sendo que no caput de seu artigo 8° resta consignado que o consentimento deverá ser fornecido por um "meio que demonstre a manifestação de vontade do titular".

Verifica-se, portanto, um vínculo entre os institutos da "vontade" e do "consentimento", que se configuram numa verdadeira preocupação do legislador quanto a segurança do consentimento como forma plena de autonomia privada.

Cabe registrar que, a LGPD veda o tratamento de dados pessoais se verificados vícios de consentimento (artigo 8°, § 3°). Assim, verifica-se a relação direta entre manifestação de vontade livre e espontânea e o consentimento escorreito – aquele que não é maculado por vícios de formação da vontade ou da sua exteriorização.

# 4.2 CONTRATOS DE ADESÃO NA ERA DA INFORMAÇÃO

A sociedade na era da informação pode ser melhor descrita por Zigmunt Bauman através da sua definição de sociedade líquida. Para o autor, a contemporaneidade é notadamente marcada pela "fluidez". Se verifica, portanto, a sociedade contemporânea em colapso do planejamento e da ação a longo prazo, assim como o desaparecimento das estruturas sociais conforme conhecíamos (BAUMAN, 2013). Uma nova mentalidade de "curto prazo", que substitui a de "longo prazo". A "flexibilidade" e a "rapidez" tornamse o eficaz para essa sociedade.

Castells ainda exemplifica que essa sociedade, surgida nesse paradigma ignora aspectos tradicionais assentados, dando gênese a novos conceitos e modernizando os que, todavia, persistem – como é o caso de certos modelos de negócios. O que vemos é que a velocidade com que as novas tecnologias são incorporadas na realidade do ser humano, impacta de forma significativa suas relações negociais, de forma prática, a maneira e as formas de consentimento de uso de dados pessoais pela forma manifesta da sua vontade nos contratos de adesão e uso.

Certo é que, atualmente, com a dataficação dos contratos firmados, prevalece a maioria por meio de adesão, onde as normas já estão pré-estabelecidas e padronizadas. A forma simplista coaduna com uma realidade mais dinâmica e imediatista, onde os termos de uso e contratos de adesão possuem características próprias, dispondo de cláusulas prontas e que, de forma geral, não admitem alterações, cabendo ao usuário apenas aceitalas ou não. Adere-se a termos já pré-determinados e seu caráter incontestável, faz com que muitas vezes, sejam sequer lidas suas cláusulas.

De forma prática, verifica-se um descompasso entre a previsão normativa e a forma como o consentimento vem sendo obtido.

91

<sup>&</sup>lt;sup>5</sup> O estudioso compara a modernidade às características dos estados da matéria, sendo que o sólido possui dimensões claras e precisas, contudo o líquido não se atém às formas, sofrendo mudanças quando submetido à pressão, e, nesse contexto, associa o presente contexto a essa exacerbada maleabilidade.

As políticas de privacidade são contratos de adesão, tratados de forma massificada quanto ao tratamento de dados dos usuários e os agentes de tratamento. Embora as políticas de privacidade estejam presentes como uma forma de cumprir os requisitos legais para o consentimento e garantir a informação ao usuário, não são suficientes para dar a autonomia e empoderamento ao usuário sobre a gestão dos seus dados pessoais.

Com todo o respeito ao doutrinador, é imperativo que seja resguardado um equilíbrio as previsões da Lei Geral de Proteção de Dados, diante do consentimento do usuário e o tratamento de seus dados pessoais. Nesse sentido, impera-se inclusive trazer maior transparência e relevância quanto ao uso constante pela autorização de *Cookies*.

### 4.3 COOKIES

Cookies são arquivos de caráter temporário, criados por sites que compilam informações obtidas do usuário e os armazenam no computador do mesmo, por meio do navegador. A princípio, cookies possuem a finalidade facilitadora de redução de tráfego, assim como, personalização a navegação no intuito de melhor adequar os gostos do usuário, tornando mais atrativo o site.

Os *cookies*, de maneira simples, são arquivos de textos, enviados pelo site ao navegador, na oportunidade em que é realizado um acesso. Assim, em uma nova oportunidade de entrada, o navegador reenvia os dados ao site para que suas informações sejam configuradas de forma automática.

Usualmente são interligados a violação de privacidade por armazenamento das mesmas informações para usos indevidos como comercialização dos dados.

Em sua gênese, foram criados com a função de saciar a demanda de lojas *onlines*, isso em meados de 1990, mas somente nos últimos anos tiveram a atenção voltada ao seu uso. Em maio de 2018, com a entrada em vigor da lei GDPR (*General Data Protection Regulation*) ou Regulamento Geral de Proteção de Dados, o qual obrigou a exibição de um aviso claro sobre a política de *cookies* do site em questão, assim como, passou a regulamentar a transparência no que concerne ao fim destinado as informações obtidas dos usuários.

Cookies, embora categorizados como "arquivos temporários" dentro do sistema Windows, não possuem um prazo padrão convencionado para deleção, podendo estar programados para serem excluídos no momento que o usuário fecha o navegador, ou, por

outro lado, é possível também que permaneça como identificador de determinado usuário até que seja realizada a remoção manual do *cookie* (CASTELLUCCIA, 2012, p. 23-24).

Os principais tipos de cookies seriam: os do próprio domínio (primários ou *first party cookies*); os definidos por terceiros (denominados *third party cookies*), os que somente funcionam enquanto estiver aberta determinada página (cookies de sessão ou *session cookies*) e os que atuam mesmo depois que o site ou página for fechada (*cookies* permanentes) (ALDEIAS, 2012 apud FRANÇA, 2015, p. 98)

Desse modo, qualifica-se como *cookie*, um arquivo rotulado como "temporário" que armazena informações de um usuário, por período indeterminado, da mesma forma que em grande parte dos casos, possui finalidade indeterminada para tais informações.

No contexto da aplicabilidade de LGPD, houve um aumento exponencial da utilização dessa ferramenta com a finalidade de obtenção da autorização do navegante para a coleta de dados, sendo que a maioria dos sites adotou os *cookies* como uma solução ao consentimento para tratamento de dados. O problema generalizou-se em razão das políticas de privacidade adotadas pelo padrão dos contratos de adesão, com termos padronizados e que não podem ser alterados, resumindo-se em aceitar ou não os *cookies de uso* para a navegação. Muitas vezes a própria *interface* do site o leva a aceitar os *cookies*, sem poder sequer recusá-los.

Na teoria, qualquer usuário pode bloquear o uso de *cookies*. Em termos práticos, não é o que ocorre. Castelluccia (2012, p. 23-24) observa a existência de cookies muito mais complexos, como os *supercookies* e os *evercookies*. Os *supercookies* atuam com os elementos fornecidos pelos navegadores, gerenciando todos os dados do usuário. De forma prática ele contorna qualquer controle exercido pelo usuário, acerca do que é ou não coletado e deletado. Já os chamados *evercookies* podem ser ainda mais difíceis, pois manipulam o armazenamento temporário de informações (cachê) e permanecem no computador mesmo que aparentemente deletados. Esses cookies indesejáveis, funcionam praticamente como um *spywares*, podendo trazer inúmeros prejuízos aos usuários.

Conforme Oliveira e Silva (2018, p. 313) atualmente, os dados pessoais adquiriram *status* "de ativos intangíveis, tornando-se estratégicos para os negócios no setor. Empresas como Google, Amazon, Uber e Netflix possuem os dados de seus clientes como o principal ativo de sua atividade empresarial."

A utilização de *cookies* e de *spams* não é considerada ilegal, uma vez que trazem inúmeros benefícios de navegabilidade aos usuários no ambiente virtual. Todavia, tal uso tem se dado de forma "desenfreada e desregulada", acarretando prejuízos de tempo,

dinheiro e invasão de privacidade para o usuário" (PRATES, 2014, p. 42). Embora tenham havido mudanças de entendimento, são constantes os abusos em relação ao envio de *spams* e à utilização de *cookies*, contexto que muitas vezes passa despercebido pelas pessoas que utilizam a Internet e que, na maioria das vezes, não possuem conhecimento técnico para verificar se estão sendo monitoradas ou afetadas por essas ferramentas. Neste cenário, a falsa ideia de anonimato no ambiente virtual favorece tais políticas, principalmente como ferramentas de envio de vírus e práticas de cibercrimes (PRATES, 2014, p. 42).

### 4.3.1 *SPAMS*

O termo "spam", da sigla em inglês, significa Sending and Posting in Mass - Enviando e postando propaganda em massa. Tratam-se de mensagens eletrônicas enviadas pelo remetente sem o consentimento do destinatário, geralmente com caráter apelativo voltado a publicidade, entretanto, também podem envolver táticas de phishing<sup>6</sup> que por sua vez, são considerados crimes cibernéticos.

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, os principais tipos de ações envolvendo *phishing* utilizados pelos autores destes crimes são: mensagens que contêm links para programas maliciosos; páginas de comércio eletrônico ou internet banking falsificadas; e mensagens contendo formulários para o fornecimento de informações importantes.

Outra importante marca dessa classe de mensagem é o seu volume de tráfego massivo dentro do ciberespaço, de acordo com o projeto *SpamLaws*, iniciativa que dá visibilidade a assuntos como privacidade e segurança dentro da internet, afirma que por dia, aproximadamente 45% de todos e-mails enviados em todo o mundo podem ser classificados como *spam*, o que equivale a 112 bilhões de e-mails, de um total de 250 bilhões de e-mails.

O primeiro relato histórico de *spam* registrado ocorreu em 1994, em um caso envolvendo 2 advogados em um fórum de discussões e submissões de artigos, os mesmos

O termo phishing é originado da palavra inglesa fishing, que significa pescar, ou seja, é a conduta daquele que pesca informações sobre o usuário de computador. É um tipo de fraude eletrônica, onde o golpista busca obter informações pessoais do usuário como senhas, dados financeiros, números de cartões de crédito e outros dados pessoais.

enviaram repetidas mensagens relacionadas a loteria para todos os usuários da rede, chegando a comprometer o tráfego, logo irritando e tipificando a prática como "spam".

Conclui-se então de modo substanciado que *spam*, nada mais é do que um conteúdo não solicitado, enviado através de um meio de comunicação eletrônico.

### 4.3.2 SPYWARE

Há diversas formas com as quais os atacantes cibernéticos podem buscar seus objetivos. Caldas (2016) afirma que parte considerável das ações criminosas em redes computacionais são praticadas com uso de *softwares* maliciosos, conhecidos por *malwares* e os define como programas criados com a intenção de se infiltrar em um sistema de computador alheio de forma ilícita, para causar danos, alterações ou roubo de informações.

Somando-se aos *malwares*, Gaspar (2007) destaca a existência de outro tipo de ameaça, os *spywares*. Estes foram criados, inicialmente, com fins comerciais, para monitorar o comportamento de usuários da internet, sem seus consentimentos, permitindo a venda dessas informações. Atualmente, os *spywares* têm sido utilizados para subtrair informações financeiras e alterar as configurações do computador, instalando outros tipos de *softwares* ou redirecionando o tráfego *web* para sites com propagandas. Segundo Pais, Moreira e Varajão (2013), os *spywares* podem ser instalados em um computador por meio de *trojans*<sup>7</sup>, ao acessar sites com aplicações capazes de explorar vulnerabilidades de navegadores de internet. Podem, ainda, ser instalados por meio de *shareware* e *freeware*<sup>8</sup>, em que o *spyware* está incluído na aplicação de instalação do *software*. E, ainda, segundo os autores, os *spywares* podem ser instalados com ou sem consentimento do usuário, podem disponibilizar ou não o tipo de informação que coletam, bem como a sua finalidade.

Para Gaspar (2007), o *spyware* era, à época, a ameaça mais preeminente da internet e representava uma grande fatia dos crimes cibernéticos, sendo utilizado por

Expressão em língua inglesa para o termo Cavalo de Tróia. Programa malicioso que entra em sistemas simulando ser outro.

<sup>&</sup>lt;sup>8</sup> Leister e Christophersen (2012) indicam que os *sharewares* são desenvolvidos por entusiastas que comercializam seus programas. Tais programas podem ser usados gratuitamente por um período de avaliação, mas estão sujeitos ao pagamento posterior de uma taxa, caso o usuário ainda deseje utilizálos. Já os *freewares* são *softwares* que podem ser usados sem custos.

crackers<sup>9</sup>, em conjunto com *malwares*, para invadir computadores, roubar dados financeiros e pessoais dos usuários, obter informações sensíveis das empresas, entre outros.

Atualmente, alguns *supercookies* tem se personificado como *spywares*, uma vez que se introduzem no computador com a finalidade de captação e compartilhamento de informações dos usuários, sendo difíceis de serem detectados ou mesmo deletados.

# **5 CONSIDERAÇÕES FINAIS**

A sociedade contemporânea é caracterizada pela "fluidez" e agilidade nas suas relações culturais, sociais e políticas. Essa característica imediatista das relações humanas, trouxe um reflexo ainda mais sério para suas relações consumeristas, apoiadas pela agilidade e pelo avanço tecnológico que estão presentes na sua vida cotidiana.

O ser humano está inserido em um ambiente digital, onde as interações entre homem e máquina passaram a ser comuns e frequentes. Seus aparelhos celulares, seus objetos, *smart tvs*, seus carros e até mesmo suas casas, conectam-se através da internet e agora conversam entre si, trocando dados e fazendo conexões, tornando a vida mais prática e fácil. A informação torna-se mais rápida, agilizando a vida e o tempo do ser humano. Em contrapartida, a Internet das Coisas traz ao ser humano uma profunda sensação de insegurança. O compartilhamento excessivo de dados pessoais fragiliza as relações do homem no espaço virtual.

Na sociedade da hiperconectividade, a utilização massiva de dados pessoais por organismos estatais e privados, através das tecnologias da informação, apresenta novos desafios ao direito à privacidade. As políticas de tratamentos de dados é uma constante preocupação dos legisladores. Sob essa ótica e para trazer uma resposta adequada aos desafios advindos dessa revolução tecnológica, a Lei de Proteção de Dados foi promulgada em 2018.

A finalidade da Lei Geral de proteção de dados é a de regular todo o tratamento de dados pessoais realizado na sociedade, tanto pelo setor público, quanto pelo setor

segurança cibernética. Já os *crackers* são os verdadeiros criminosos, pois utilizam seus potenciais cognitivos para cometerem atos ilícitos.

O termo hacker, bastante utilizado cotidianamente como uma generalização de usuários criminosos, não significa exatamente isso. Ramalho Terceiro (2002) aponta hacker, genericamente, como alguém possuidor de grande habilidade em computação. Já os crackers, black-hats ou scrit kiddies são hackers que utilizam seus conhecimentos para atacar computadores. Dessa forma, hackers podem utilizar seus conhecimentos para análise de vulnerabilidades e, inclusive, trabalhar em parcerias com empresas de

privado. Busca, dessa forma, preservar a coletividade e os direitos fundamentais dos cidadãos.

Entretanto, no afă de regular a transparência das relações contratuais no ciberespaço, a lei deu ensejo a massificação do uso de *cookies* e termos de adesão, no intuito de cumprir a determinação legal, pela necessidade de consentimento do usuário. Embora não exista regulamentação que desaprove o uso de *cookies* e *spams*, o trabalho aponta para os malefícios que o uso indiscriminado dessas ferramentas podem causar.

Deste modo, verifica-se que a política de *cookies* pode ser tanto benéfica como maléfica para o usuário em rede e que, por mais que tais estratégias de monitoramento online e direcionamento de conteúdo sejam baseadas na navegabilidade e no comportamento *online* do usuário, em tese, *cookies* podem ser controlados e bloqueados.

O estudo alerta para existência de certos tipos de *cookies* cuja regulação e abrangência são mais complexos, bem como menos acessíveis ao cidadão que desconhece os ditames do mercado tecnológico fundamentado no capitalismo de vigilância, fundado na vigilância excessiva do cidadão para fins de consumo e controle social. Esses *supercookies* são advertidos como *spyware*, por terem a função única de compartilhar dados pessoais de seus usuários, não podendo sequer ser detectados ou deletados.

Numa análise incisiva quanto ao consentimento regulado pela Lei de Proteção de Dados, o estudo concluiu que o legislador se preocupou com os conceitos dos institutos de "vontade" e do "consentimento", buscando alcançar a segurança do consentimento como forma plena de autonomia privada. Trazendo ao cidadão uma certa liberdade para gerir o uso de seus dados pessoais.

Em que pese a intenção do legislador, muito ainda há por se alcançar nas interrelações do homem dentro do universo virtual. O internauta, deixa um rastro economicamente viável. Em virtude das políticas adotadas atualmente, nas rotinas dentro da internet, através de *cookies* e históricos de navegação, rastreamento de Ips (sigla em inglês para protocolo de internet), o usuário gera um perfil que possui valor de mercado. Através da conectividade com a rede, os usuários geram em tempo integral, quantidades massivas de informação, o *big data*. Nunca foi tão fundamental a privacidade do ser humano.

No que se refere ao compartilhamento de dados com terceiros para finalidades omerciais, técnicas ou de processamento, a maioria das plataformas permite o compartilhamento como opção padrão, cabendo ao usuário procurar a opção para

desativar o compartilhamento, quando existente. Este é o chamado sistema *opt-out*<sup>10</sup>. Isto confronta diametralmente com a opção adotada pelo legislador brasileiro, que exige a adoção de um sistema *opt-in*<sup>11</sup>, no qual a opção oferecida por padrão deve ser aquela que não permite o compartilhamento de dados, até que o próprio usuário modifique esta opção. Esta foi a opção adotada pela Lei Geral de Proteção de Dados. Segundo a norma, é necessária a obtenção de consentimento explícito pelo titular dos dados, ou seja, este deve ser informado e dado livremente para que os consumidores optem ativamente por se engajar ou não em atividades que envolvam exposição de dados.

Assim, é necessário analisar a transparência como se dá o consentimento acerca da utilização de políticas de *cookies* pelo usuário, principalmente à luz da Lei Geral de Proteção de Dados, de modo a assegurar a liberdade e autonomia ao usuário para o gerenciamento de seus dados, bem como para a proteção de seus direitos à privacidade, à informação e a preservação de suas inter-relações no espaço digital.

### REFERÊNCIAS

ANDRE CUNHA SAUER; JOÃO PADILHA MOREIRA. **LGPD - Lei Geral de Proteção de Dados.** SEMINÁRIO DE TECNOLOGIA GESTÃO E EDUCAÇÃO, v. 3, n. 2, 20 nov. 2021. Disponível em:

http://raam.alcidesmaya.edu.br/index.php/SGTE/article/view/354/344. Acesso em: 25 Ago. 2022.

BOFF, Salete Oro; FORTES, Vinícius Borges. A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil. Sequência (Florianópolis), p. 109-127, 2014. Disponível em:

https://www.scielo.br/j/seq/a/LqY93YW8FMSNPgkVBg75nbH/?format=pdf&lang=pt. Acesso em: 25 Ago. 2022.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil\_03/leis/l8078compilado.htm. Acesso em: 25 Ago. 2022.

BRASIL. **Lei nº 9.296 de 24 de Julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil 03/leis/l9296.htm. Acesso em: 25 Ago. 2022.

Também conhecido como "descadastro", uma vez dado o opt-in, é preciso garantir que o usuário tenha maneiras de revogá-lo.

De maneira geral, o *opt-in* é uma autorização formalizada que o usuário ou cliente dá para que uma empresa esteja apta a enviar comunicações, conteúdos e notificações. Ele é importante para garantir que a pessoa tem interesse genuíno em receber mensagens e e-mails, por exemplo.

BRASIL. Lei nº 12.527/2011, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 50, no inciso II do § 30 do art. 37 e no § 20 do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil\_03/\_ato2011-2014/2011/lei/l12527.htm. Acesso em: 25 Ago. 2022.

BRASIL. Lei nº 12.737/2012, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil\_03/\_ato2011-2014/2012/lei/l12737.htm. Acesso em: 25 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. Disponível em: http://www.planalto.gov.br/ccivil\_03/\_ato2011-2014/2014/lei/l12965.htm. Acesso em: 25 Ago. 2022.

CANCELIER, Mikhail Vieira de Lorenzi. **O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro.** SciELO Brasil – Scientific Electronic Library Online, Universidade Federal de Santa Catarina, 2019. Disponível em: https://www.scielo.br/j/seq/a/ZNmgSYVR8kfvZGYWW7g6nJD/?format=pdf&lang=pt; Acesso em: 25 Ago. 2022.

CARVALHO, Cristiano. Internet das coisas: entenda o que é e como funciona. Publicado em Tecmundo. 2020. Disponível em: https://www.tecmundo.com.br/internet/230884-internet-coisas-entenda-funciona.htm#:~:text=Casa%3A%20existem%20in%C3%BAmeros,irriga%C3%A7%C3%A3o%2C%20quando%20necess%C3%A1rio. Acesso em: 25 Ago. 2022.

GONÇALVES, M. P. **Proposta de implementação da Indústria 4.0 na área da logística**. Trabalho de conclusão de curso apresentado com requisito parcial para obtenção do título de bacharel em Engenharia de Transportes e Logística da Universidade Federal de Santa Catarina, Centro Tecnológico de Joinville, Joinville – SC. 2016. Disponível em:

file:///C:/MEUS%20DADOS%20NAO%20APAGAR/Downloads/Tcc\_Final.pdf Acesso em: 25 Ago. 2022.

JAMIL, George Leal; NEVEZ, Jorge Tadeu Ramos. **A era da informação:** considerações sobre o desenvolvimento das tecnologias da informação. Perspectivas em ciência da informação, v. 5, n. 1, 2000. Disponível em: https://periodicos.ufmg.br/index.php/pci/article/view/23309. Acesso em: 25 Ago. 2022.

JUNIOR, Walter Teixeira Lima. **Big Data, Jornalismo Computacional e Data Journalism: estrutura, pensamento e prática profissional na Web de dados**. Universidade Federal de São Paulo. Estudos em comunicação nº 12, p.207-222 - 2012. Disponível em: chrome-

extension://efaidnbmnnnibpcajpcglclefindmkaj/http://www.ec.ubi.pt/ec/12/pdf/EC12-2012Dez-11.pdf. Acesso em: 25 Ago. 2022.

LEMOS, André; MARQUES, Daniel. OLIVEIRA, N. D.; GOMES, M.; LOPES, R.; NOBRE, J. Segurança da Informação para Internet das Coisas (IoT): uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD). **Revista Eletrônica de Iniciação Científica em Computação**, [S. l.], v. 17, n. 4, 2019. DOI: 10.5753/reic.2019.1704. Disponível em: https://sol.sbc.org.br/journals/index.php/reic/article/view/1704. Acesso em: 25 Ago. 2022.

LIMA, Luciano de Almeida. **O direito à privacidade nas redes sociais na internet.** Universidade Regional do Noroeste do Estado do Rio Grande do Sul – UNIJUÍ – Mestrado em Direitos Humanos. Ijuí-RS. 2016. Disponível em: https://bibliodigital.unijui.edu.br:8443/xmlui/handle/123456789/4204. Acesso em: 25 Ago. 2022.

LORENZON, Laila Neves. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD E GDPR) e seus respectivos instrumentos de *enforcement*. **Revista do Programa de Direito da União Europeia**, v. 1, p. 39-52, 2021. Disponível em:

file:///C:/MEUS%20DADOS%20NAO%20APAGAR/Downloads/document%20(1).pdf Acesso em: 25 Ago. 2022.

MAIA, Luciano Soares. **A privacidade e os princípios de proteção do indivíduo perante os bancos de dados pessoais.** Publica Direito. Jurídica. Faculdade de Direito de Campos – FDC. Brasília-DF. 2011.

Disponível em:

file:///C:/MEUS%20DADOS%20NAO%20APAGAR/Downloads/luciano\_soares\_maia.pdf. Acesso em: 25 Ago. 2022.

MORGENSTERN, Grasiele Giusti; TISSOT, Tania Regina gottardo. Crimes cibernéticos: phishing – privacidade ameaçada. Relatório técnico-científico. **XXIII Seminário de Iniciação Científica**. Salão de Conhecimento. 2015. Disponível em: file:///C:/MEUS%20DADOS%20NAO%20APAGAR/Downloads/5174-Texto%20do%20artigo-22388-1-10-20150827%20(1).pdf. Acesso em: 25 Ago. 2022.

NEVES, Rebeca de Aguilar Pereira. **GDPR e LGPD:** Estudo comparativo. CEUB – educação Superior. Repositório UNICEUB. Brasília – DF. 2021. Disponível em: chrome-

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.uniceub.br/jspui/bitstream/prefix/15239/1/Rebeca%20Neves%2021750900.pdf. Acesso em: 25 Ago. 2022.

PINHEIRO, D. S.; MACEDO, F. L. S.; JUNIOR, J. N. V.; SILVA, M. T, Século XXI, as mudanças tecnológicas propostas pela Internet das Coisas. Universidade Paulista – UNIP - Instituto de Ciências Exatas e Tecnologia - Bacharelado em Ciência da Computação. Iniciação - Revista de Iniciação Científica, Tecnológica e Artística - Edição Temática em Tecnologia Aplicada. vol. 7. n. 4. 2018, São Paulo: Centro Universitário Senac. Disponível em:

file:///C:/MEUS%20DADOS%20NAO%20APAGAR/Downloads/3-IC.pdf. Acesso em: 25 Ago. 2022.

SANTOS, Pedro Miguel Pereira. MENDES, Ana. **Internet das coisas: o desafio da privacidade.** Repositório Comum - Comunidades & Colecções IPS - Instituto Politécnico de Setúbal IPS - ESCE - Escola Superior de Ciências Empresariais - Dissertações de mestrado. 2016. Disponível em: http://hdl.handle.net/10400.26/17545 Acesso em: 25 Ago. 2022.

SILVEIRA, Cristiano Bertulucci; LOPES, Guilherme Cano. **O que é Indústria 4.0 e como ela vai Impactar o mundo.** 2016 - Republicado 2018. Disponível em: https://www.citisystems.com.br/industria-4-0/. Acesso em: 25 Ago. 2022.

TOBBIN, Raissa Arantes; CARDIN, Valéria Silva Galdino. Política de *cookies* e a "crise do consentimento": Lei Geral de Proteção de Dados e a autodeterminação informativa. **Revista da Faculdade de Direito da UFRGS**, Porto Alegre, n. 47, p. 241-262, dez. 2021. Disponível em: https://doi.org/10.22456/0104-6594.113663. Acesso em: 25 Ago. 2022.

ZAMBARDA, Pedro. **Internet das Coisas:** entenda o conceito e o que muda com a tecnologia. Publicado em www.techtudo.com.br. 2017. Disponível em: https://www.techtudo.com.br/noticias/2014/08/internet-das-coisas-entenda-o-conceito-e-o-que-muda-com-tecnologia.ghtml. Acesso em: 25 Ago. 2022.

ZANINI, Leonardo Estevam de Assis. **O Surgimento e o Desenvolvimento do** *Right of Privacy* **nos Estados Unidos.** Justitia, São Paulo, 70-71-72 (204/205/206), jan./dez. 2013-2014-2015. Disponível em:

http://www.mpsp.mp.br/portal/page/portal/documentacao\_e\_divulgacao/doc\_biblioteca/bibli\_servicos\_produtos/bibli\_informativo/bibli\_inf\_2006/Justitia%20n.204-206.21.pdf; Acesso em: 25 Ago. 2022.

FACHIN, Zulmar. O direito fundamental à proteção de dados pessoais: análise da decisão paradigmática do STF na ADI 6.387-DF. **Revista Videre**, v. 14, n. 19, p. 298-313, 2022. Disponível em: https://ojs.ufgd.edu.br/index.php/videre/article/view/15629. Acesso em: 25 Ago. 2022.