PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS
CENTRO DE CIÊNCIAS HUMANAS E SOCIAIS APLICADAS
FACULDADE DE DIREITO

LUCAS GABRIEL CABRAL DE CASTRO

SEGURANÇA E PRIVACIDADE DE DADOS NA UTILIZAÇÃO DE DISPOSITIVOS VESTÍVEIS – WEARABLES

Campinas
2022

LUCAS GABRIEL CABRAL DE CASTRO

SEGURANÇA E PRIVACIDADE DE DADOS NA UTILIZAÇÃO DE DISPOSITIVOS VESTÍVEIS – WEARABLES

Monografia apresentada como parte das exigências para conclusão do Curso de Bacharelado em Direito pela Pontifícia Universidade Católica de Campinas – PUCC, no ano de 2022.

Orientador: Prof. Dr. Daniel Blikstein

Campinas

2022

LUCAS GABRIEL CABRAL DE CASTRO

SEGURANÇA E PRIVACIDADE DE DADOS NA UTILIZAÇÃO DE DISPOSITIVOS VESTÍVEIS – WEARABLES

Monografia apresentada como parte das exigências para conclusão do Curso de Bacharelado em Direito pela Pontifícia Universidade Católica de Campinas – PUCC, no ano de 2022.

Campinas, ____ de _____ de ____

BANCA EXAMINADORA

_____

Prof.
Pontifícia Universidade Católica de Campinas (PUC-CAMPINAS)

Prof.
Pontifícia Universidade Católica de Campinas (PUC-CAMPINAS)

Dedico este trabalho a Deus, à minha família, aos meus professores, colegas de curso e a todos aqueles consumidoras e pessoas de bem que um dia foram lesadas, ou ainda, tiveram seus dados pessoais utilizados pelas grandes companhias.

AGRADECIMENTOS

Chegar onde chegamos, lutar como lutamos, tudo isso que enfrentamos não foi por acaso e jamais cumpriremos uma jornada de forma individual.

Dessa forma, esse trabalho resume toda uma trajetória, a qual jamais seria cumprida se não fosse os outros, ou seja, por mais que quem aqui esteja escrevendo seja o Lucas, fato é que não seria possível chegar aqui sem o coletivo.

Mas, esse coletivo tem forma, tem rosto, tem cheiro, cada pessoa tem sua identidade que jamais vou esquecer. Não só minha família, são todos aqueles cruzaram o meu caminho e de alguma forma ajudaram a construir o que chamamos destino.

Destaco a generosidade dos astros, de Deus e de tudo aquilo que existe de divino na minha vida.

Assim, Yolanda, cada palavra aqui escrita tem um pedaço de você, achei que apenas seria capaz de sentir o amor de irmão dentro da minha própria casa, com aqueles que são sangue do meu sangue, mas você me ensinou o contrário, me ensinou muitas das magias desse mundo, mostrou que existe amor verdadeiro entre opostos, mesmo que de signos iguais, mães quase homônimas e preferências similares.

De igual tom falo da Nana, Ana Júlia Furlan, é inacreditável como seis meses influenciam em uma vida toda, digo isso, porque, bastaram o transcurso de exatos seis meses para eu encontrar uma parceira de vida, com que eu posso confiar e entregar tudo que eu preciso, me aturar esse tempo foi essencial, muito obrigado, espero que seis meses se transformem em uma vida de amizade, te amo.

Nessa mesma caminhada eu encontrei a Nicole, fato é que já conhecia ela, minto, não conhecia, eu realmente conheci a pureza e sinceridade dessa mulher esse ano ... que ano transformador, e só ela para enfrentar a jornada comigo, muito mais que uma dupla, uma irmã, cada palavra, cada troca, tudo tão singular, agradeço aquele quem te colocou na minha frente, sem você tudo seria mais nebuloso, tenho certeza.

Mas isso tudo significa uma coisa, a vida é feita de escolhas, e eu escolhi me permitir, ser amado e amar, e nisso me permiti também conhecer a Carol, Carolzinha, Globinho, vários sinônimos, para a mesma pessoa, a qual me faltam palavras para descrever o que representa. Enfim, eu encontrei, parece um tesouro, daqueles que levam anos para serem descobertos. E de fato levou, foram 5, mas achei, no final da caminhada ... pum ... Caiu no meu colo de paraquedas, e sabe lá Deus o que será daqui para frente, mas que seja da forma que foi até aqui, verdadeiro e leve, fazendo o bem recíproco entre ambos os envolvidos.

Nessa altura lagrimas caíram, memórias surgiram, nomes pipocam a todo instante na minha mente, mas, ressalta aos olhos a amizade de um cara, João. Gulla, eu queria que você soubesse o diferencial de pessoa que você é, a passada pura, o coração aberto e o amor intenso, você é acolhedor, mas não como tantos outros, você ama de forma única, meu parceiro de palestra, espero que seja para sempre o meu parceiro de palestra.

Dito isso, resta falar dela, Isa, Bixete, Bixinha, minha parceira, tem coisa que tem que acontecer, independente do tempo que demore, e, você demorou, porque demorou tanto. Não importa, fato é que você alugou um condomínio no meu coração, o abraço que conecta vale mais do qualquer digito que eu coloque aqui, basta lembrar do cheiro, do conforto e do encaixe, obrigado minha pequena, você é incrível.

A última citação expressa e nominal que faço é da Raquel, cabe a ela o conforto do beijo, do carinho e do abraço, a manhã fria se torna mais quente e o passado amargo fica mais doce. Foram 5 anos, mas o último foi daqueles, a companhia que ela proporciona, a risada que ela puxa e o abraço apertado que ela tem, não tem preço, faria tudo de novo, reviveria cada momento, até porque, foram eles que me levaram até aqui me fortificaram dia após dia, parece que ela sabia que cada afeto gratuito na verdade tinha o custo altíssimo, no fundo me manter na linha, seguir em frente, motivar e pular cada obstáculo, obrigado Quelzinha, você tem meu coração.

Destino esse que não se consolidaria pela presença de duas pessoas, realmente essas duas peças são fundamentais no quebra-cabeça da vida, sem eles nada disso teria cor, cheiro e forma, sem eles não eu não me imaginaria vivo, com a energia e vitalidade que faço as coisas.

Falar dessas duas peças até se tornou clichê nessa atualidade pós-moderna que vivemos, de toda forma acredito ser fundamental falar deles, pois sem André e Cristina as coisas se tornam mais complexas, são eles minha base e alicerce, cada viga da minha vida foram eles que construíram.

Portanto, o monumento que hoje eu sou, obra inacabada, mas que ao passar dos anos cresce, é fruto de muito suor e lagrimas que constantemente eles derramam por mim, sendo egoísta da minha parte não dedicar isso a eles, meus amores e a quem eu daria minha vida.

Quem não tem nenhum tipo de medo é irresponsável. Coragem não é a ausência do medo. É o controle dele.

Augusto Cury – O Colecionador de Lagrimas**.**

RESUMO

Este trabalho de conclusão de curso, busca a análise detalhada dos impactos da legislação brasileira sobre a proteção e privacidade de dados dos consumidores, ora aderentes da utilização de dispositivos vestíveis, também popularmente conhecidos como *Wearables.* Assim, através do método hipotético-indutivo foram realizas buscas legislativas, doutrinárias e jurisprudências para verificação do atual panorama nacional, com comparativos internacionais, sobre a matéria em voga, pode, ao final, observar falhas protetivas e algumas lacunas deixadas pelo legislador pátrio, quanto a necessidade de blindagem informacional de usuários.

Palavras-chave: Lei Geral de Proteção de Dados; Wearables; Privacidade; Consumidor; União Europeia.

ABSTRACT

This course completion paper seeks a detailed analysis of the impacts of Brazilian legislation on the protection and privacy of consumer data, now adherents of the use of wearable devices, also popularly known as Wearables. Thus, through the hypothetical-inductive method, legislative, doctrinaire and jurisprudence analyses were conducted to verify the current national panorama, with international comparisons, on the matter in vogue. At the end, it is possible to observe protective flaws and some gaps left by the Brazilian legislature regarding the need for informational shielding of users.

Keywords: General Law of Data Protection; Wearables; Privacy; Consumer; European Union.

SUMÁRIO

INTRODUÇÃO

O mundo globalizado é constantemente surpreendido com novas tecnologias informativas, as quais são capazes de captar, processar, armazenar e compartilhar diversos segmentos de dados.

Dentre as inovações apontadas, surge o desenvolvimento de equipamentos destinados à adaptabilidade da vida cotidiana das pessoas, ou seja, sua finalidade precípua é serem dispositivos inteligentes que se inserem de forma natural na dia-dia dos indivíduos, agregando funcionalidade e qualidade de vida aos usuários aderentes

Essas tecnologias, para melhor desempenho e inserção no mercado, foram projetadas para serem anexadas ao próprio corpo humano, sendo usadas como verdadeiros acessórios, chamadas então de dispositivos vestíveis, no inglês *Wearables*.

Inclusive, muitas dessas tecnologias foram desenvolvidas seguindo criterioso processo de design funcional, a fim de se aparentarem com utilitários já utilizados no cotidiano popular, tais como óculos e relógios, garantindo assim que os novos dispositivos ganhassem propagação mercadologia e desejo consumerista do varejo internacional.

Fato é que os dispositivos vestíveis já se encontram amplamente difundidos ao redor do globo, sendo fabricados, operados e comercializados por potenciais industriais já consolidadas no mercado tecnológico, tal como a norte-americana Apple e a empresa concorrente japonesa Samsung, conhecidas, respectivamente, pelo lançamento mundial dos *Wearables* Apple Watch e Galaxy Watch.

Sendo assim, considerando a difusão desses dispositivos em território nacional, considerando o potencial informacional das ferramentas, capazes, como dito, de captarem e compartilharem dados pessoais dos usuários aderentes do produto, faz-se necessário o enfrentamento dos aspectos jurídicos, concernentes a privacidade de dados do contingente populacional, tal como o estudo das estruturas legais capazes de atenuar a voracidade de atuação das companhias e fabricantes dos itens vestíveis.

1. WEARABLES: ESTUDO DA TERMINOLOGIA E DO MANEJO DE DADOS DOS USUÁRIOS PELAS PLATAFORMAS

1.1. Conceito De Wearables e Popularização Das Tecnologias Vestíveis

Inicialmente, para melhor inserção e compreensão básica dos assuntos que circundam a temática dos *Wearables*, é necessária uma análise conceitual sobre a terminologia da palavra, sendo de pudor realizar tanto uma análise semântica da sentença, tanto quanto uma análise social do termo.

Nesse sentido, tratando-se de um termo transferido da língua inglesa, é importante realizar uma breve análise gramatical de *Wearables*, posto que a apresentação do sentido literal da palavra irá auxiliar na compreensão e aplicação social do tema, ou seja, o entendimento semântico da palavra esclarece e expõe as utilizações fáticas da terminologia.

Assim, através de uma busca realizada na plataforma de traduções inglês-português da *Cambridge University*, é possível se verificar que *Wearables* são resumidamente explicados como sendo: coisas que podem ser vestidas, tais como roupas e óculos, as quais contém inseridas em seu escopo tecnologia semelhante de computadores, podendo ainda serem conectados à internet[1].

Logo, como anteriormente mencionado, a análise semântica da terminologia auxilia na compreensão da utilização prática dos *Wearables*, posto que, após a exposição de seu significado, é possível idealizar e imaginar inúmeras aplicações sociais das tecnologias mencionadas.

Dessa forma, a utilização desses dispositivos cresce no imaginário popular ano após ano, ganhando espaço no mercado de consumo e se inserindo amplamente no cotidiano das pessoas.

Participam desde avanço marcas como *Apple*, *Samsung*, *Xiaomi* e a pioneira *Fitbit*, ou seja, reiteradamente, ao passar do tempo, os *Wearables* se tornaram um artigo do cotidiano, havendo participação massiva de grandes companhias para a promoção e implementação destes vestíveis.

Desde que foram realizados os lançamentos dos primeiros monitores, no ano de 2007, a Marca *Fitbit*, por exemplo, já havia concretizado a comercialização de 60 (sessenta) milhões

[1] Wearable technology consists of things that can be worn, such as clothing or glasses, that contain computer technology or can connect to the internet (CAMBRIDGE SCHOOL CLASSICS, **Cambridge Dictionary of American English for Speakers of Portuguese**, Editora WMF Martins Fontes, 2013).

de dispositivos inteligentes até o ano de 2017, ao passo que em 2019 já haviam sido registrados um total de 29.6 milhões de usuários ativos, distribuídos em 110 diferentes países, fato que resguardou para a marca o título de primeiro lugar no ramo de *social fitness* do planeta[2].

Entretanto, atualmente os *Wearables*, não se resumem a simples acessórios de embelezamento, transpassando inúmeras barreiras de utilização, sendo capazes de aferir desde o número de passos do usuário, o ritmo cardíaco, a geolocalização, o humor, sendo até mesmo capazes de aferir os ritmos gástricos, as posturas corporais, fluxos menstruais e os padrões sexuais de quem deles de utiliza[3].

Posto isso, os dispositivos vestíveis possuem tecnologia suficiente para serem utilizados de diversas formas, concentrando hoje no mercado três diferentes aplicabilidades, sendo elas, a saúde, o esporte e o *business*.

Diante dos destaques comerciais de utilização dos *Wearables*, surgem inúmeras teorias comportamentais que explicam a expansão de sua popularização, teorias essas que se preocupam em detalhar a forma pela qual esses dispositivos se inseriram no cotidiano popular e ali permaneceram.

Pelo exposto, diante das teorias que explicam a inserção dos *Wearables* no cotidiano popular, vale ser destacada a *unified theory of acceptance and use of technology 2 (UTAUT2)* (em português: teoria unificada de aceitação e utilização de tecnologia 2), a qual considera uma série de aspectos sociais e comportamentais para explicar a aceitação do indivíduo ao uso de dispositivos eletrônicos (Venkatesh, Viswanath; Morris, Michael G.; Davis, Gordon B.; Davis, Fred D. 2003. "User Acceptance of Information Technology: Toward a Unified View". MIS Quarterly, 425–478).

A teoria indicada é perfeitamente compatível com o estudo em análise, sendo, através dela, possível se verificar a intensão dos consumidores em adotar a tecnologia vestível, examinando concomitantemente os efeitos do produto em relação à segurança da informação e privacidade dos usuários.

Nesses termos, pela análise comportamental, segundo a teoria *UTAUT2,* é possível se concluir que os *Wearables*, antes exclusivamente usados no campo militar, se consolidaram no cotidiano popular, em razão de proporcionarem ao usuário um grande aumento na qualidade de vida.

---

[2] BITENCOURT CUNHA, Elias. "**Coletamos dados para o seu bem" O Truque retórico do imaginário sobre o dado digital promovido nos termos de uso, documentos de privacidade e relatórios de investidores da plataforma**. Fitbit, Florianópolis, Revista de Literatura, Linguística, e Educação e Artes, v. 16, p. 157-182, 2020.
[3] BITENCOURT CUNHA, op. cit.

Isso porque, devido aos parâmetros de monitoramento diário físico-psicológicos oferecidos pelo *smart accessory* (em português: acessório inteligente), o dispositivo proporciona a manutenção de um estilo de vida saudável, voltado ao autocuidado e bem estar social.

Mas não só, devido ao ganho de qualidade de vida, os usuários de *Wearables* passam a estar motivados de forma hedônica, tornando-se um prazer usar a tecnologia e pro do bem-estar de vida individual.

Cumulado ao fator prazer e bem-estar social, outro ponto que facilita a inserção dos vestível no cotidiano popular, é o fato de que a indústria de tecnologia coloca no mercado dispositivos extremamente acessíveis, cujo manuseio, personalização e suporte às necessidades pessoais á garantido aos usuários, sendo esses fatores a preocupação principal dos fabricantes de vestíveis.[4]

Portanto, em frente aos fatores apresentados, os dispositivos móveis tornaram-se parte fundamental de um estilo de vida saudável, enraizando-se no cotidiano de milhões de pessoas.

Atualmente os *Wearables* encontram-se difundidos na sociedade, sendo possível se concluir que os usuários priorizam a manutenção de seu bem-estar individual frente à possíveis interferências em sua vida privada, tal como a segurança de dados e a tecnologia de informação invasiva.

1.2. Definição De Usuários e Conceito de Dados

Conforme exposto no tópico anterior, a utilização cotidiana dos *Wearables* é um quadro sintomático, observado ao redor de todo o globo, sendo então necessária a realização de uma análise territorial desse fenômeno, evitando-se então uma fundamentação generalista do assunto.

Em outros termos, para melhor discussão sobre a temática, inclusive para obtenção de uma maior precisão dos impactos jurídico-sociais, é de suma importância restringir a exposição para dentro dos limites e ditames da estruturação do Direito brasileiro, possibilitando analisar-se a legislação aplicável sobre a utilização de dispositivos vestíveis inteligentes no Brasil.

---

[4] GAO, Yiwen; LI, Hi; LUO, Yan; **An Empirical Study of Wearable Technology Acceptance in Healthcare, R**egular Paper. Emerald Group Publishing Limited, v. 115, n. 9, p. 1704-1723, 2015.

Desse modo, concentrando a exposição para os limites do sistema jurídico brasileiro, a abordagem do uso de *Wearables* precisa ser realizada sob enfoque de como são classificados os usuários perante a legislação pátria, bem como, de que modo ocorre a classificação desses dados propriamente ditos dentro do ordenamento.

Sendo assim, a legislação mais completa e compatível com a temática da utilização de *Wearables* encontra respaldo na Lei Geral de Proteção de Dados, Lei nº 13.709, de 14 de agosto de 2018, a qual dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, havendo o legislador o pleno objetivo de proteção aos direitos fundamentais de liberdade e privacidade dos usuários, sejam elas pessoas naturais ou jurídica, como bem mencionado pelo Artigo 1º do referido diploma legal.[5]

Nesse sentido, diante do diploma legal em análise, é possível a extração de diversos conceitos primordiais para entendimento da temática, em especial, para entendimento dos impactos da utilização de *Wearables* na segurança e proteção de dados.

Para tanto, inicialmente, vale se destacar que a Lei Geral de Proteção de Dados não se vale do termo *usuários*, mas sim da expressão *titular*.

Logo, para estruturação da fundamentação aqui apresentada servirá de sinônimo ambas as expressões, tanto usuário, tanto quanto titular, uma vez que titular, segundo a legislação, é aquela pessoa detentora dos dados objetos de tratamento.

De tal maneira que, na hipótese de utilização de vestíveis inteligentes, usuários e titulares serão aqueles que se utilizam da tecnologia e fornecem suas informações, seu próprio corpo e dados para as plataformas desempenharem suas análises, cabendo a elas o fornecimento da apuração dos dados capitados, ou seja, mediante o fornecimento de dados dos titulares, os dispositivos revertem as informações apuradas em quesitos quantitativos almejados pelo utilizador, tais como as frequências cardíacas, avaliações de humor e contagem de passos.[6]

Dessa forma, as informações fornecidas pelos usuários aos *Wearables* são classificadas como dados pelo ordenamento jurídico brasileiro, havendo uma divisão dúplice quanto a espécie de dados, de tal forma que a Lei Geral de Proteção de Dados, classifica tais conjuntos informativos entre dados pessoais e dados pessoais sensíveis.

---

[5] Prescreve o artigo 1ª da LGPD, *in verbis: "*Art. 1º Esta Lei dispõe 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".

[6] PINHEIRO, Patrícia Peck, **Proteção de Dados Pessoais: Comentário a Lei nº 13.709/2018 (LGPD)**. 2ª. Ed., São Paulo, Editora Saraiva Educação, 2020.

A respeito da divisão, dados pessoais são classificados como um conjunto de informações capazes de identificar uma pessoa, não se resumindo tão somente as características como nome, idade e endereço residencial, mas também a informações que dizem respeito à sua localização atual, perfil e histórico de compras, dados acadêmicos e identificadores de internet, tal como o *Internet Protocol (IP)* (em português: Protocolo da Internet).

Enquanto é estabelecida a referida definição para dados pessoais, a mesma legislação classifica dados sensíveis como sendo aqueles estritamente relacionados a características atreladas à própria personalidade do indivíduo, como dados vinculados à sua saúde, vida sexual, genética, biométrica e sociais, tais como a convicção política e filiação a organizações religiosas.

Pelo exposto, os titulares de dados, sendo eles sensíveis ou não, através de um ato de vontade, compartilham dessas informações com as plataformas controladores dos *Wearables*, empresas essas já mencionadas anteriormente, como Apple e Samsung, multinacionais de grande influência e potencial econômico.

Esses dados, uma vez coletados por essas empresas, fornecidos livremente pelos usuários, através de aceite de um possível "termo de uso e serviços", contratos online sem rigor técnico específico, passam a sofre um procedimento denominado *Tratamento dos Dados*.

O Tratamento de Dados é um procedimento genérico, classificado pela Lei Geral de Proteção de Dados como sendo qualquer operação que consista no manuseio de dados do usuário, seja através da coleta, classificação, utilização, distribuição, transmissão ou avaliação das informações extraídas dos usuários.

Face o exposto, os usuários de *Wearables* estão constantemente suscetíveis ao procedimento de Tratamento de Dados, uma vez que a atuação dos dispositivos vestíveis se fundamenta essencialmente na captação de informações dos usuários e transformação desses conjuntos informacionais em análises comportamentais.

Dentre os dados coletados, as plataformas responsáveis pelos dispositivos vestíveis têm pleno acesso à dados pessoais dos usuários e dados sensíveis de tais titulares, questionando-se então se os meios de aceite fornecidos são suficientes para preservar a segurança de informação e privacidade da pessoa.

Em outras palavras, torna-se uma pauta importante a fragilidade dos instrumentos normativos pelo qual se dá o aceito do usuário, os quais muitas vezes são dotados de extrema informalidade, estando os titulares plenamente expostos ao fornecimento de seus dados, sem haver a contrapartida na garantia de proteção das informações fornecidas.

Assim, sendo o consentimento uma manifestação dotada de exteriorização inequívoca para concessão de algo, o titular se restringe ao consentimento para que seus dados sejam postos à procedimentos de tratamento, a partir de então as plataformas estão autorizadas a realizar as medidas necessárias para quantificação das informações pretendidas.

Neste cenário, as plataformas dos *Wearables*, seguindo a legislação aplicável, assumem o papel de Agentes Controladores, uma vez que, como já exposto, mediante a autorização do usuário, recepcionam dados dos titulares e operam a realização do tratamento, em especial, a conversão desse conjunto informativo em análises comportamentais que são largamente oferecidas pelos dispositivos vestíveis.

Portanto, sendo expostas as classificações que cabiam, qualificando cada qual dos papeis exercidos dentro de uma cadeia de fornecimento e transformações de dados, é necessário, na sequência, avaliar o modo pelo qual os *Wearables* realizam seus procedimentos de tratamento de dados, para que então seja possível futuramente avaliar eventual fragilidade jurídica sobre o tema.

1.3. Captação de Dados – Sistema de Extração e Disseminação dos Dados em Dispositivos Vestiveís

No tópico anterior, diante das qualificações apresentadas, ficou evidenciado o papel do usuário, dos dados, dos procedimentos de tratamento de dados e dos operadores de dados dentro das relações existentes entre consumidores de *Wearables* e as plataformas administradoras.

Dessa forma, para destacar a vulnerabilidade dos titulares de dados, bem como para evidenciar a liquidez em que as informações são dissipadas por esses *gadgets*, se mostra importante expor como os dispositivos vestíveis realizam a captura de dados e convertem as informações obtidas em outros conjuntos informativos.

Assim, em um estudo realizado pela Universidade de Columbus com parceria feita pela Universidade do Kentucky, foi possível se detalhar os instrumentos centrais, cinco características contidas dentro dos *Wearables*, os quais permitem a assimilação de dados dos usuários, armazenamento dos conjuntos obtidos e conversão dos dados auferidos.[7]

[7] PEREZ, Alfredo J.; ZEADALLY, Sherali, **Privacy Issues and Solutions for Consumer Wearables**, IEE Computer Society, IT Professional, 2018.

Nesse sentido, como primeira ferramenta, os dispositivos vestíveis contam com um conjunto de sensores, incluindo GPS, acelerômetro responsável pela aferição de velocidade, giroscópio para verificação da direção e angulação, além de câmeras para mapeamento do local.

Mas não só, ainda, alguns dispositivos, contam com sensores de contato e de áudio, capazes de interpretar e armazenar informações obtidas através da fala e do tato.

Diante das informações capitadas pelos conjuntos de sensores, os dados são transplantados para microprocessadores ou microcontroladores, responsáveis por calcular e filtrar as informações extraídas da atividade humana.

Após os procedimentos de extração, cálculo e filtração, os dados são importados para um armazém de mídia embutido, onde as informações sensitivas coletadas são armazenadas para análise posterior.

Também, os dispositivos vestíveis contam com uma série de itens de saída, os quais proporcionam ao usuário sinais vibracionais, sons, conjuntos visuais, como luzes e telas que se vinculam diretamente com as informações extraídas do comportamento humano, inclusive transformando alguns dos dados obtidos em alertas e notificações aos titulares.

Entretanto, fato é que os dados obtidos pelos *Wearables* não são mantidos com exclusividade dentro do acessório vestível utilizado pelo usuário, isso porque, esses *gadgets* contam com ferramentas internas para comunicação externa, ou seja, os *Wearables* são dotados de Redes de Área Pessoal, conhecidos mundialmente como *personal area network (PAN)* (em português: rede de área pessoal), capazes de comunicar o dispositivo com outras unidades.

Além da rede PAN, uma das mais simplórias ferramentas de comunicação, muitos dos dispositivos vestíveis contam com outros poderosas ferramentas de interface, muitas delas diretamente conectas à smartphones que diretamente se vinculam a uma nuvem de dados, tal como a *Icloud*, software da Apple que oferece aos usuários o armazenamento de inúmeros tipos de dados, como documentos, fotos e músicas.[8]

Pelo exposto, é possível se verificar uma possível fragilidade na proteção dos dados fornecidos pelos usuários, uma vez que, durante todo o tempo de uso do *Wearable* o usuário se sujeita a extração continuada de informações, o que resulta em um conjunto informativo imenso aos controladores de dados, mas, em contrapartida, os dispositivos apresentam grande fluidez no fluxo comunicativo, sendo as informações extraídas facilmente dissipadas para redes sociais,

[8] APPLE INC, **Icloud Drive – Welcome To Icloud,** Apple.com, 2022. Disponível em: https://www.apple.com/legal/internet-services/icloud/

terceiros interessados e outros usuários, o que proporciona lacunas de proteção.

1.4. Segurança dos Usuários – Impacto dos Termos de Uso e Serviços Na Privacidade Dos Usuários

A partir da problemática apresentada, torna-se questionável a confiabilidade na segurança e privacidade de dados dos usuários, de tal modo que é de suma importância a realização de uma análise dos meios pelo qual os titulares prestam o aceite para os operadores de dados, uma vez que, somente com essa análise será possível verificar se os usuários possuem plena ciência das condições à eles impostas desde o momento da aceitação.

Nesse sentido, é inegável que atualmente o maior problema da utilização de *Wearables* são voltadas a questões de privacidade dos consumidores, de tal modo que, pesquisas de mercado realizadas pela PWC[9] mostram que 43 por cento da população Americana, cerca de 141.6 milhões de pessoas[10], não se sentem confortáveis em compartilhar qualquer tipo de informação pessoal, demonstrando a preocupação do usuário sobre o tema.

Assim, segundo apontamentos realizados por Mitchell, em sua obra *Sensing Mine, Yours, Theirs and Ours: Interpersonal Ubiquitous Interactions*[11](em português: Sentir o meu, o teu, o deles e o nosso: Interacções Interpessoais Ubíquas), é possível chegar à conclusão que existem diversas esferas de violação da privacidade, as quais, por consequência, preocupam os usuários de *smart* eletrônicos.

Dentre essas esferas de problemática, destaca-se, por exemplo, as implicações sociais de uma eventual falha de privacidade, uma vez que, a referida falha pode permitir acesso de dados pessoais de um único usuário à sua gama inteira de amigos próximos, dando conhecimento à terceiros de dados que jamais podiam ser compartilhados. Mas não só, evidentemente podem surgir crimes oportunistas a partir destes erros procedimentais, causando ao titular o extremo temor que seus dados possam ser usados para a prática de crimes cibernéticos.

---

9 Health Wearables: Early Days, report, PWC Health Research Institute, May 2016; www.pwc.com/us/en/health-industries/health-research-institute/publications/healthwearables early-days.html.

10 População dos Estados Unidos, setembro de 2022 – Country Meters; https://countrymeters.info/pt/United_States_of_America_(USA)

11 MITCHELL, Robb. **Sensing mine, yours, theirs, and ours: interpersonal ubiquitous interactions.** In: Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers. 2015. p. 933-938.

Esses cenários de inseguranças possuem grande propensão de ocorrência devido às funcionalidades dos *Wearables*, destacadas no tópico anterior, pensemos, por exemplo, no reconhecimento facial oferecido por algumas dessas ferramentas, a associação e o reconhecimento do usuário pode ser irrestritamente feita ao longo do tempo, podendo ele ser identificado em lugares ou situações que essencialmente ele não desejaria de ser reconhecido por outros.

Nesse mesmo contexto, o acesso de controle das plataformas vestíveis é nebuloso, temendo os usuários pelo acesso de suas informações por terceiros que não possuem qualquer relação, mas que eventualmente possuem relação, seja ela comercial ou não, com a plataforma gerenciadora de dedos.

A referida vulnerabilidade de dados possuí diversas implicações jurídicas, desde o aceite ao fornecimento de dados, até ocorrências póstumas, tangentes ao direito de esquecimento, uma vez que os dados são coletados padecem de garantias quanto a possibilidade de cancelamento ou instrumentos de exclusão das informações coletadas, implicando diretamente no *direito de esquecimento* pertencente aos usuários, os quais podem eventualmente se depara com informações e dados cujo interesse é que de simplesmente nunca mais fossem lembrados.

Logo, o maior questionamento é se os Termos de Uso e Serviços das plataformas de *Wearables* são suficientes para afastar essas inseguranças e garantir ao usuário a plena privacidade dos dados coletados.

Sendo assim, os Termos de Uso e Serviços são basicamente documentos jurídicos, a espelho de contratos convencionais, os quais estabelecem regras e disposições de como serão estabelecidas as relações entre os usuários e a plataforma fornecedora do serviço ofertado, a partir dessas disposições são previstas, consequentemente, direitos e deveres para ambas as partes.[12]

No cenário dos *Wearables* esses documentos jurídicos possuem grande relevância, isso porque, conforme exposto anteriormente, o tratamento de dados pelos operadores apenas é autorizado mediante o consentimento do titular das informações, de tal modo que os Termos de Uso e Serviços são os meios pelo qual os usuários prestam seus aceites às plataformas iniciarem os procedimentos de extração, conversão, dissipação e armazenamento dos conjuntos informativos.

---

[12] LUGER, Ewa; MORAN, Stuart; RODDEN, Tom**. Consent for all: revealing the hidden complexity of terms and conditions.** In: Proceedings of the SIGCHI conference on Human factors in computing systems. 2013. p. 2687-2696.

De toda sorte, por se tratar de um instrumento jurídico, os Termos de Uso e Serviços padecem de qualquer padronização, de modo que, muitas vezes, a linguagem utilizada e a estruturação do documento dificultam a compreensão do usuário, dada a complexidade e falta de acessibilidade dos conteúdos ali dispostos, a exemplo disso pode se destacar que algumas plataformas, por mais que ofereçam a interface em português, apresentam ao consumidor uma política toda em sua língua nativa, como o inglês.

Mesmo diante das complexidades contidas nos Termos de Uso e Serviços, os usuários aceitam as cláusulas impostas e unilateralmente formuladas pelas empresas de tecnologia, se vinculando de forma integral as condições apresentadas mesmo não possuindo integral consciência do que realmente estão se vinculando, exatamente pelo fato de não compreenderam os termos impostos, ou ainda, por não terem sequer realizado a leitura do conteúdo.

Dessa forma, destaca-se que essencialmente os usuários deveriam possuir o pleno arbítrio de escolher quais recursos dos *Wearables* seriam utilizados pelo seu aplicativo, bem como quais dados realmente gostaria que fossem coletados ou armazenados, ao contrário disso, os titulares concedem às plataformas um aceite irrestrito, permitindo que os operadores realizem um tratamento ilimitado das informações concernentes aos usuários.

Por meio dos Termos de Uso e Serviços os operados assumem um papel quase de ditatorial, impondo aos usuários barreiras de acesso, controle informativo, vigilância e restringindo a sensação de ação e liberdade dos titulares, própria *Google* em suas políticas internas, restringe a possibilidade de recuperação e acesso de alguns dados do usuário, mesmo quando o indivíduo deixa de utilizar os serviços ofertados, existem óbices a exclusão de conjuntos informativos.[13]

Diante do cenário apresentado, os Termos de Uso e Serviços possuem grande similitude a um contrato, posto que assume a forma de negócio jurídico vinculado à um acordo de vontade entre as partes contratantes, de tal maneira que o consentimento de ambos qualifica a relação como sendo bilateral.[14]

Por isso, tratando-se de uma relação jurídica obrigacional de caráter bilateral, deve ser irrestritamente observado o princípio da autonomia da vontade, a fim de que os interesses do acordo satisfaçam o interesse de ambas as partes contratantes, cabendo as partes possuir a contratar por aquilo que desejarem, de modo que o instrumento sirva para resguardar diretos e

---

[13] PISA, Licia Frezza. **Discurso e poder em Michel Foucault: o controle do que dizemos na rede visto pela política de privacidade do Google.** Domínios de Lingu@ gem, v. 8, n. 1, p. 250-266, 2014.

[14] DA SILVA PEREIRA, Caio Mário. **Instituições de Direito Civil - vol. III - Contratos**. , Editora Forense, Rio de Janeiro, p.7, 11ª ed., 2004.

obrigações de amos os polos da relação.

> O princípio da autonomia da vontade se alicerça exatamente na ampla liberdade contratual, no poder dos contratantes de disciplinar os seus interesses mediante acordo de vontades, suscitando efeitos tutelados pela ordem jurídica. Têm as partes a faculdade de celebrar ou não contratos, sem qualquer interferência do Estado. Podem celebrar contratos nominados ou fazer combinações, dando origem a contratos inominados.[15]

Ao lado do princípio da autonomia, deveria de vigorar nos instrumentos regulamentadores das relações *Wearables-Consumidores*, o princípio da boa-fé objetiva, a fim de que, principalmente os operadores de dados, promovessem comportamentos intersubjetivos, mesmo que não contratados, direcionados ao cumprimento dos termos vinculativos e ainda, promovessem ações, sejam elas repressivas ou preventivas, contra danos aos usuários.

Entretanto, em contramão dos princípios basilares dos contratos, os Termos de Uso e Serviços são eivados de vícios, inclusive no que concerne a manifestação de vontade de usuário, posto que, em inúmeras situações, não há o cumprimento dos requisitos subjetivos da manifestação de vontade.

Isso porque, como requisitos da manifestação de vontade a parte contratante necessita, primeiramente, de plena capacidade civil, havendo em um segundo momento de exteriorizar sua aptidão de forma livre e desvencilhada de qualquer vício.

Ocorre que, é de conhecimento notório que os Termos de Uso e Serviços das plataformas de *Wearables* não possuem qualquer controle hereditário para cadastramento e utilização dos serviços, embasando o descumprimento do requisito da capacidade, posto que permite a vinculação de menor impúrbere ao tratamento de dados.

Ademais, pelo fato do consumidor não compreender e sequer realizar a leitura dos termos contratados, é questionado se de fato a manifestação de vontade não é eivada de vício, uma vez que o usuário não possuí pleno conhecimento das condições à que vinculou, aparentando ser precário o consentimento concedido à plataforma, ou seja, o que antigamente poderia ser consentido através da assinatura por meio de firma, atualmente pode ser realizado por um simples *checklist* do mouse em um *gap* eletrônico[16].

Em suma, os Termos de Uso e Serviço não oferecem a segurança necessária para os dados dos usuários, havendo, inclusive, concretas dúvidas se os requisitos de validade da

---

[15] GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro, v. 3**: Contratos e Atos Unilaterais- 9ª Ed. São Paulo: Saraiva, p. 41, 2020.

[16] BEHRENS, Fabiele. **A assinatura eletrônica como requisito de validade dos negócios jurídicos e a inclusão digital na sociedade brasileira.** Curitiba: Dissertação de Mestrado PUC/PR, 2005.

manifestação de vontade dos usuários foram cumpridos, o que, consequentemente, implica na possibilidade de tratamento dos dados ofertados. Esse cenário, aponta diretamente para necessidade de serem analisadas as consequências jurídicas e proteções legais à disposição do consumidor, quando da utilização e aceite das ofertas feitas por plataformas de dispositivos vestíveis.

1.5. Legítimo Interesse do Usuário no Tratamento de Dados

Diante da fragilidade exposta no tópico anterior, no que tangência as inconsistências dos documentos de aceite oponíveis aos usuários de *Wearables*, pelo qual é manifestada a concordância no uso e tratamento de dados pessoais, mostra-se pertinente a análise dos mecanismos jurídicos que oferecem proteção, ou ainda, atenuam a esfera protetiva dos consumidores perante a invasão massiva das corporações em seus conjuntos informativos.

Para tanto, a fim de estabelecer-se uma melhor compreensão da estrutura jurídica que circunda o legítimo interesse do usuário, é importante ser frisado que a intervenção estatal é absolutamente necessária para regulação do tema, de tal modo que a operação de companhias captadoras de dados não é livre, existindo hoje instrumentos jurídicos limitadores de sua atuação.

Dentre os mecanismos jurídicos limitadores, ora vigentes no cenário econômico mundial, destaca-se que o estabelecimento de uma política pública europeia para gerenciamento da controvérsia foi o ponto inicial, isso porque, após a modernização da gestão jurídica europeia, os países integrante do bloco, de forma conjunta, realizaram a promulgação do Regulamento 2016/679[17] do Parlamento Europeu e do Conselho, instrumento jurídico popularmente conhecido como Regulamento Geral de Proteção de Dados (RGPD), outrora aprovado em 27 de abril de 2016.

O referido conjunto normativo europeu, preocupou-se, preponderantemente, com a proteção e circulação de dados pessoais, permitindo então que houvesse um primeiro movimento de adequação econômica à padrões legalmente impostos.

Em outras palavras, renomadas empresas de tecnologia, dominantes no mercado de consumo, tiveram que adequar suas políticas internas de tratamento de dados para continuidade

[17] UNIÃO EUROPEIA. Regulamento (EU) 2016/679 do Parlamento e do Conselho Europeu de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Bruxelas, 27 de abril de 2016. Disponível em: https://eurlex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em: 29 de outubro de 2022.

de suas atividades econômicas dentro dos países integrantes da União Europeia (EU), de modo que, a partir de então, níveis de segurança de dados passarão a serem exigidos para manutenção de relações comerciais com os referidos agentes econômicos.

A legislação europeia sobre o tema possui lastro em diversos julgados anteriormente realizados em território europeu, sendo importante para a análise do legitimo interesse do usuário, manifestação de vontade para tratamento de dados pessoais, o julgamento realizado pelo Tribunal Constitucional Alemão, em 15 de dezembro de 1983.

Isso porque, a partir do julgamento do caso da Lei do Censo (Volkszählungsgesetz)[18], reconheceu-se que os titulares dos dados possuem uma carga participativa indiscutivelmente superior no que concerne à autodeterminação de seus conjuntos informativos.

Sendo assim, a sentença da corte firmou um marco para as legislações que irão surgir na sequência, tal como o Regulamento Geral de Proteção de Dados, ora firmado pela União Europeia (EU), posto que reconheceu um direito subjetivo fundamental ao indivíduo, para que esse pudesse protagonizar o processo de tratamento de seus dados.[19]

Logo, tendo em vista o surgimento de movimento global, a espelho disso o Brasil, através da regulamentação jurídica conferida pela Lei nº 13.709/2018, Lei Geral de Proteção de Dados, vigente de desde 2020, também passou a conferir preceituação jurídica para o desenvolvimento da personalidade do cidadão dentro da esfera de utilização das plataformas digitais, regulamentação essa que abarca, como dito anteriormente, a utilização e operação de dados nos dispositivos vestíveis, ora denominados mundialmente como *Wearables.*

Diante do surgimento de microssistema jurídico para regulamentação das operações realizadas dentro de plataformas digitais, surgiram também novas exigências para os operadores de dados, de modo que, a partir da leitura do Artigo 7º da Lei Geral de Proteção de dados é verificado o condicionamento do tratamento de dados pessoais a hipóteses legais pré-definidas

---

[18] A lei do recenseamento visava à coleta dos dados dos cidadãos referentes à profissão, moradia e local de trabalho, com intuito de fornecer à administração pública informações acerca do crescimento populacional, da distribuição espacial da população pelo território e das atividades econômicas realizadas no país. Os dados a serem coletados por pesquisadores estavam listados na lei, que estabelecia também uma multa para o cidadão que se recusasse a responder. Ademais, o § 9.º da norma determinava que os dados poderiam ser comparados àqueles presentes em registros públicos, com a finalidade de averiguar a veracidade das informações fornecidas, além de possibilitar a sua transmissão na forma anônima a órgãos públicos federais. Foram ajuizadas diretamente diversas reclamações constitucionais contra a lei do recenseamento, com fundamento na violação direta ao Art. 2 I GG, que protege o livre desenvolvimento da personalidade. O Tribunal conheceu da reclamação e, no mérito, confirmou a constitucionalidade da lei em geral, declarando nulos os dispositivos que determinavam a comparação dos dados coletados, bem como a sua transferência para outros órgãos da administração. MENDES, Laura Schertel. **O direito fundamental à proteção de dados pessoais. Revista de Direito do Consumidor**, São Paulo, v. 79, p. 45-82, jul./set. 2011.

[19] MENDES, op. cit, p. 45-81.

pelo legislador pátrio.

Nesse sentido, neste momento, torna-se importante destacar-se a primeira hipótese autorizativa contida no referido diploma legal, o qual determina que o tratamento de dados pessoais do usuário será possível, *ipsis litteris*, mediante o fornecimento de consentimento pelo titular, igualando-se a inicial presunção estabelecida pela suprema corte alemã.[20]

Inclusive, a regulamentação brasileira, sobre ao legítimo interesse do usuário, guarda estrita relação com o *General Data Protection Regulation (GDPR[21])* (em português: Regulamento Geral de Protecção de Dados), utilizada pela União Europeia, uma vez que o conjunto normativo europeu, em seu Artigo 06º, expõe também um rol taxativo de hipóteses permissivas para que as operadoras de dados possam realizar o tratamento de dados de seus usuários, vinculando na primeira hipótese a possibilidade de tratamento mediante o consentimento do titular.

Logo, com o estabelecimento deste permissivo, tanto no contexto europeu, tanto quanto na trajetória brasileira, determina que o detentor dos dados, ora o usuário, possuí para si o direito de autodeterminação de seus conjuntos informativos, cabendo ao indivíduo a liberdade de delimitação de sua própria esfera privada, posto, que à ele cabe o poder de legitimar que terceiros realizem em determinada medida a utilização de seus dados pessoais. Trata-se aqui do controle e gerência do usuário quanto a titularidade de seus direitos de personalidade, conferindo ao indivíduo autonomia individual para pactuar sobre a temática.[22]

Entretanto, o consentimento exigido pela legislação, nos moldes em que se verifica atualmente, é obtido de forma absolutamente precária, não oportunizando ao usuário a livre escolha de aceitação, quanto a disposição ou não de seus dados pessoais, uma vez que, grande parte das plataformas digitais, obrigam o consumidor à aceitarem seus termos de uso e serviços, já que em caso negativo, uma vez não aceitando-se pela disposição dos dados pessoais, o indivíduo estará vedado à utilizar-se dos serviços fornecidos pela corporação.

Posto isso, ao lado da fragilidade dos documentos formais de obtenção do consentimento, questiona-se essencialmente se a manifestação de vontade é suficiente para que as atividades de gerência de dados sejam realmente controladas, pois o aceite se torna uma obrigatoriedade ao usuário frente a disponibilidade dos serviços digitais outrora fornecidos.

---

[20] DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais: fundamentos da Lei Geral de Proteção de Dados.** 2ª ed. São Paulo: Thomson Reuters Brasil, p. 377-379, 2019.

[22] BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** 2ª ed. Rio de Janeiro: Forense, 2020. E-book.

1.6. Legítimo Interesse do Usuário à Luz da Teoria Voluntarista do Negócio Jurídico

Dessa forma, a fragilidade na proteção de dados possuí estrita ligação com a teoria do negócio jurídico, uma vez que, sendo a manifestação de vontade um dos requisitos autorizativos para manipulação e tratamento de dados, devem ser observadas as regras elementares constitutivas da exteriorização da vontade para constituição validada da autorização por parte do usuário.

Sendo assim, realizando a subsunção das teorias explicativas do negócio jurídico, à luz da manifestação de vontade dos agentes, o problema aqui enfrentado deve ser analisado sobre a ótica dos requisitos constitutivos e validadores desse fenômeno jurídico.

Vale mencionar que o sistema jurídico pátrio adotada a corrente voluntarista, pontificada por Orlando Gomes.

A teoria voluntarias, ora predominante no Direito brasileiro, conforme orientação contida no Artigo 112 do Código Civil de 2002, com redação semelhante no Artigo 85 do Código Civil de 1916, determina que o negócio jurídico nada mais é que a declaração de vontade dirigida para provocação de determinados efeitos jurídico, uma ação de vontade, dirigida para consecução de determinado fim, o qual pode constituir, modificar ou extinguir uma relação jurídica.[23]

Logo, o aceite do usuário é plenamente configurado como um negócio jurídico, tratando-se de uma manifestação de vontade capaz de estabelecer uma relação jurídica, uma vez que a partir da ação do indivíduo a plataforma encontra-se autorizada a manejar seus dados pessoais, permisso outrora contido na Lei Geral de Proteção de Dados, consequentemente, os efeitos e circunstâncias do ato encontram pleno respaldo legal.

Consequentemente, uma vez a manifestação de vontade do usuário se enquadrando no conceito de negócio jurídico, fato é que o referido ato formal está sobre plena influência dos requisitos de existência, validade e eficácia ora vinculados a todo negócio jurídico.

Posto isso, para análise de cada um dos planos, deve-se tem em mente a existência de um nivelamento entre os planos do negócio jurídico, partindo-se primordialmente do plano da existência, para em sequência ser alcançado o plano da validade e, assim, para que apenas ao

---

[23] GAGLIANO**,** Pablo Stolze e FILHO, Rodolfo Pamplona, **Novo Curso de Direito Civil, Parte Geral**, 1, 16ª Edição, Editora Saraiva, janeiro de 2014, Revista e Atualizada, São Paulo/SP, Capítulo X.

final o negócio jurídico possa produzir os efeitos à que lhe foram inicialmente admitidos pelo permissivo legal.

Em outras palavras, primeiramente analisa-se o surgimento do negócio jurídico, o aceite ou não do usuário, para posteriormente serem verificados os requisitos para que este seja considerado perfeito, estando apto ou não para produzir seus efeitos, consistindo na possibilidade de mesmo havendo o aceite, serem analisadas a presença dos requisitos que autorizam os operadores a manejarem os dados pessoais dos usuários.

Assim, para enfretamento da temática aqui abordada e limitação da discussão, faz-se necessário que o enfoque da problematização seja concentrado no plano de validade dos negócios jurídicos, uma vez que, no que concerne ao aceite do usuário para tratamento de seus dados pessoais é nesse plano que serão encontradas barreiras suficientes para que seja questionada se a medida concessiva eximida pelo indivíduo atinge a perfeição e consequentemente poderá produzir seus efeitos.

Como primeiro requisito de validade do aceite é importante se ressaltar que a manifestação de vontade deverá ser livre e dotada de boa-fé, nesse sentido, a autonomia privada torna-se um princípio regulador dos negócios jurídicos, traduzindo que os indivíduos hão de ter liberdade negocial para atuação no mercado.

Entretanto, a liberdade de atuação não é irrestrita, havendo limites balizadores para que certos princípios sejam também tutelados em comunhão, de tal modo que a própria constituição federal consagra mecanismos limitadores da autonomia da vontade (Artigos 05º, XII e XIII e 170, III da Carta Magna), verificando-se então que o individualismo, com o surgimento de constituições sociais, foi atenuado pelo solidarismo.

Diante dessas circunstâncias limitadoras, a validade da manifestação de vontade direcionada para a vinculação permissiva do usuário às plataformas operadoras de dados torna-se questionável.

Isso porque, como já dito anteriormente, o aceite está estritamente ligado à possibilidade ou não do indivíduo habilitar-se para utilização dos serviços oferecidos pela plataforma.

Sendo assim, usando-se o exemplo do *Apple Watch (*dispositivo vestível em forma de relógio digital[24]*)*, quando o usuário nega a concessão e tratamento dos dados de saúde, tais

[24] Dentro da política de termos de uso e serviços do IWatch, verifica-se que a plataforma realiza quase que um processamento irrestrito de dados, inclusive, utilizando-se das informações obtidas para finalidades comerciais, como anúncio de produtos, como observa-se na integra do documento: Segmentos - Criamos segmentos, que são grupos de pessoas que compartilham características similares e usamos esses grupos para direcionar os anúncios. Informações sobre você podem ser usadas para determinar a quais segmentos você é atribuído e, portanto, quais anúncios você recebe. Para proteger sua privacidade, anúncios direcionados são exibidos apenas se mais de 5.000 pessoas atenderem aos critérios de direcionamento. Podemos usar informações como as seguintes para atribuir

como contagem de passos, aferição de batimentos e geolocalização, o dispositivo eletrônico torna-se inoperante, não exercendo determinadas funções originalmente garantidas pela ferramenta.

Logo, nesse ponto, evidentemente a manifestação de vontade do usuário não é livre, as operadoras de dados se utilizam de artifícios ardilosos para convencimentos dos usuários, de tal modo que vinculam a manifestação de vontade ao estrito interesse da plataforma, de tal modo que o aceite nada mais é que uma sujeição da pessoa humana aos termos impostos pela companhia, sem qualquer possibilidade de autodeterminação, tampouco gerenciamento do processo de tratamento que será realizado sobre os conjuntos informativos ora extraídos pelos dispositivos vestíveis.

Dos pontos apresentados, muito se remete também a necessidade de cumprimento dos requisitos de boa-fé objetiva dentro dos negócios jurídicos, tratando-se aqui de evidente relação bilateral, onde de um lado tem-se o usuário e do outro o operador de dados, sendo certo que as partes deverão de obedecer a um critério ético de confiança recíproca.

Dessa forma, tratam-se de regras éticas mínimas, o que, evidentemente é amplamente violado pelas corporações em análise, já que os interesses comercias que circundam a obtenção de conjuntos informativos superam qualquer valoração, de tal modo que, mesmo sem o pleno conhecimento do usuário, acerca do meio pelo qual os dados serão explorados, tem-se o aceite do consumidor, razão pela qual, em certa medida, há ausência de boa-fé por parte da operadora, a qual, evidentemente, não comunica de forma clara e objetiva a destinação final das informações outrora capitadas.

No sentido dos termos aqui expostos, para verificação de uma possível má fé objetiva no ato volitivo exercido pelo manifestante, expressa Bruno Lewick, em um de seus magistrais artigos, “investigação eivada de dificuldade e incertezas, faz-se necessária a consideração de um patamar geral de atuação, atribuível ao homem médio, que pode ser resumido no seguinte questionamento: de que maneira agiria o *bônus pater familiae*, ao deparar-se com a situação em apreço? Quais seriam as suas expectativas e as suas atitudes, tendo em vista a valoração jurídica, história e cultura do seu tempo e de sua comunidade?”.[25]

Não sendo suficiente para conclusão de que o aceite emitido pelo usuário se mostra como um negócio jurídico invalido, vale mencionar o desrespeito a mais um requisito de

---

você a segmentos: Informações da Conta: seu nome, endereço, idade, sexo e dispositivos registrados na conta do seu ID Apple. Informações como seu nome na página de registro do seu ID Apple ou saudação na sua conta do ID Apple podem ser usadas para definir seu gênero. Você pode atualizar as informações da sua conta no site do ID Apple. https://support.apple.com/pt-br/guide/watch/welcome/watchos, acesso em 29 de outubro de 2022.

[25] LEWICK, Bruno. **Panorama da Boa-fé Objetiva**, in Gustavo Tepedino, p. 56.

validade, sendo certo que, em inúmeras vezes, não se tem a presença de um agente emissor e vontade capaz para o negócio mencionado, nos termos do Artigo 104 do Código Civil.

A ausência de capacidade remete a figura da pessoa natural, oportunidade em que lhe faltando plena capacidade para prática de atos jurídicos, deverá de ser devidamente representada ou assistida para concessão de plena validade à ação perpetrada.

Ocorre que, em se tratando de autorização para manejo de dados pessoas, especialmente na análise da utilização de *Wearables*, tem-se que grade parte dos consumidores de dispositivos vestíveis são absolutamente incapazes, ou seja, são indivíduos que ainda não alcançaram 16 (anos) completos e que em regra não poderiam conceder referido aceite às plataformas operadoras, como explicitamente abordado no Artigo 3º do Código Civil.[26]

Mas não só, as plataformas de que se aproveitam dos dados fornecidos pelos usuários, quando do fornecimento dos termos de uso e serviços, documentos por meio do qual o ato permissivo é consolidado, não possuem qualquer controle sobre as condições pessoais do agente, ou seja, trata-se de documento genérico que não é capaz de verificar as peculiaridades de cada caso, deixando de ser um instrumento que permita a identificação de eventual incapacidade do usuário emissor do ato volitivo.

Deste modo, poderá haver desrespeito a qualquer uma das hipóteses de incapacidade, seja concernente aos critérios etários, seja nos casso de ébrios eventuais, viciados em tóxicos e os pródigos, sendo certo que, do modo que hoje são disponibilizados os instrumentos de aceite, qualquer um desses indivíduos poderá prestar seu ato volitivo, sem que haja o estabelecimento de qualquer barreira para impedimento.

Logo, por mais que exista, no plano jurídico e fático, a manifestação de vontade do usuário, a qual em regra autorizaria os controladores ao processamento de tratamento de conjuntos informativos, fato é que a incapacidade do agente vicia o negócio jurídico, deixando este de produzir seus e feitos e consequentemente impedindo que as corporações prossigam com o tratamento dos dados pessoais extraídos através de dispositivos vestíveis.

Assim, em conformidade com os critérios estabelecidos pela doutrina voluntaria, acerca dos requisitos de validade do negócio jurídico, torna-se compreensível que o aceite realizado

---

[26] Verifica-se, nesse ponto, a existência de uma estrita semelhança com a redação do art. 6º, alínea "f", do GDPR: "O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: (...) f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança". UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Disponível em: Acesso em: 20 outubro de 2022.

pelo usuário, muitas vezes, não é acompanhado do atendimento integral de tais preceitos.

Por consequência, descumpridos os requisitos de validade exigidos, o ato permissivo concedido às plataformas operadoras de dados pessoais torna-se um ato jurídico invalido, estando impossibilitado de produzir seus efeitos legalmente delimitados.

O ponto abordado, foi brilhantemente trabalhado por Pablo Stolze Gagliano, em sua obra Novo Curso de Direito Civil, Parte Geral, preceituando a seguinte afirmativa "Nota-se que, em todas estas situações, as partes gozam de plena capacidade, posto estejam impedidas circunstancialmente de praticar ato específico, por relevantes razões de ordem social e pública. A consequência da violação de um desses impedimentos é a nulidade do negócio que se realizou, por violação a expressa disposição de lei".[27]

Logo, sendo o processamento de dados pessoais um efeito jurídico imediato do aceite, as operadoras de dados estariam impossibilitadas de realizar as diligências que lhe foram inicialmente atribuídas pela Lei Geral de Proteção de Dados, uma vez que o ato jurídico é considerado invalido, concluindo-se que a legislação especial, por mais que preveja instrumento protetivo, deixou de realizar disposições especificas para os casos de vício ao negócio jurídico, devendo então serem aplicadas aos casos concretos, aqui verificados, as disposições contidas no Código Civil.

Portando, diante de todo o exposto, verifica-se nesse primeiro momento, a insuficiência da legislação pátria para proteção de dados dos usuários, uma vez que o consentimento não é suficiente para autodeterminação dos dados, tornando-se mera formalidade, cujo caráter de eficácia e validade tornam-se comprometidos, ante a ocorrência de hipóteses jurídicas limitadoras, sem que haja, até o momento, consequências ao tratamento de dados, originado de aceite viciado.

1.7. Wearables Como Um Dispositivo Global: Perspectiva Internacional da Legislação Protetiva de Dados

1.7.1. Globalização Dos Dados No Mercado De Consumo

Diante de todo o cenário apresentado até o momento, é claro que os problemas de

[27] GAGLIANO, Pablo Stolze e FILHO, Rodolfo Pamplona. **Novo Curso de Direito Civil, Parte Geral**, 1, 16ª Edição, Editora Saraiva, Revista e Atualizada, São Paulo, Capítulo X, p. 391, 2014.

privacidade de dados envolvendo a utilização de dispositivos vestíveis supera as barreiras nacionais, tratando-se de um problema global que implica na análise e diferentes organizações jurídicas para compreensão integral da problemática.

A globalidade do assunto está estritamente ligada à fluidez da informação, isso porque, no atual cenário mundial a captação da informação, em especial o tratamento e processamento de dados, não se restringe às quatro linhas das fronteiras brasileiras.

Pelo contrário, em virtude da internacionalização do mercado, o que se ilustra pela multinacionalidade de marcas e corporações, os dados eventualmente extraídos por um *Wearable* são difundidos irrestritamente para diferentes pontos do mundo, ao passo que, o usuário não possuí o poder, tampouco o controle, para direcionamento das informações capitadas.

Pois, além da existência de multinacionalidade das empresas receptoras de dados, o que por si só garante que os dados captados em território nacional de difundam ao redor do globo, existe hoje o estabelecimento de relações comerciais entre diferentes marcas e empresas.

Essas relações comerciais também influenciam diretamente no modo pelo qual o processamento de dados é realizado, tornando-se outra ferramenta de ramificação da cadeia informativa, comprometendo de uma vez por todas a nacionalização do dado extraído.

Para ilustração do tema, os termos de uso e serviços do aplicativo *WhatsApp*, ferramenta de comunicação amplamente difundida ao redor do mundo, disponível tanto em como celulares, tanto quanto em dispositivos vestíveis como o *Apple Watch* e *Galaxy Watch BT*, garante a utilização dos dados extraídos pelo serviço comunicativo com todas as empresas integrantes do *Grupo Meta*.

O *Grupo Meta*[28], por sua vez, é um conjunto de empresas capitaneadas pela *Meta Platforms INC,* originalmente identificada como *Facebook*, mas que, logo após a ascensão da marca e do rápido desenvolvimento econômico da companhia, consolidou sua renomeação para evitar conflitos de interesses inerentes a patentes e produtos, ora ofertados pela desenvolvedora.

Dentre as empresas integrantes do grupo econômico, vale o destaca para as sociedades empresariais: *Facebook Payments Inc, Facebook Technologies, WhatsApp LLC, WhatsApp Ireland Limites e Novi Financial Inc*.

---

[28] Termos de uso e serviços da Whatsapp e constituição do *Grupo Meta* "Além dos serviços oferecidos pela Meta Platforms Inc. e Facebook Ireland Ltd, a Meta é proprietária e opera todas as empresas listadas abaixo, que operam de acordo com seus respectivos termos de serviço e políticas de privacidade. Para saber mais sobre nossas práticas de privacidade, visite a página de privacidade do WhatsApp. Para saber mais sobre as práticas de privacidade das Empresas da Meta e como elas tratam os dados dos usuários ao oferecer serviços a você.", disponível em https://faq.whatsapp.com/3328550797183840/?locale=pt_BR,. Acesso em 30 de out. de 2022.

Ocorre que, em virtude da globalização e organização de mercado de cada uma das marcas listadas acima, a sede empresarial de cada uma dessas empresas não se encontra disposta na mesma unidade da federação, pelo contrário, cada qual dessas sociedades possuí sede uma um país do globo, tal como, Porto Rico, Estado Unidos da América, Ilhas Marianas do Norte e Guatemala.[29]

Assim, todos os dados captados através da utilização do aplicativo *WhatsApp* poderão ser distribuídos dentro do processamento informativo de qualquer uma das empresas integrantes do grupo meta, como explicitamente indicado nos termos de uso e serviço da ferramenta[30], o que reflete na disponibilização de dados pessoais dos usuários para diferentes países e regiões continentais.

Logo, as indicações e disposições inerentes ao tratamento de dados dos usuários, encontram-se expostas a conhecimento do consumidor, o qual, como dito anteriormente, sob pena de impossibilidade de utilização dos serviços comunicativos ofertados pela plataforma, manifesta concordância com a manipulação dos dados nos termos impostos pela companhia.

Portanto, demonstrado que o atual modelo de processamento de dados não limita a utilização territorial de conjuntos informativos, havendo a comercialização, difusão e troca de conteúdos entre diferentes empresas, sejam elas pertencentes do mesmo grupo econômico ou não, se mostra necessária a análise de diferentes modelos jurídicos para compreensão da problemática de privacidade na utilização de *Wearables.*

2. MODELO EUROPEU NO CONTROLE DE PRIVACIDADE

Como já simploriamente abordado nos capítulos anteriores, o sistema protetivo consolidado no Brasil, considerando a somatória das disposições contidas na Lei Geral de Proteção de Dados e no Marco Civil da Internet, inspirou-se fundamentalmente na estrutura

---

[29] Listagem de países em que o Grupo Meta possuí sede, bem como algumas regiões em que atuam "Meta Platforms Technologies, LLC, or if you reside in the U.S. Territories (American Samoa, Guam, Northern Mariana Islands, Puerto Rico, U.S. Virgin Islands)", disponível em https://www.meta.com/legal/quest/store-terms-of-sale/?utm_source=faq.whatsapp.com&utm_medium=oculusredirect#data-protection. Acesso em: 30 de out de 2022.

[30] Disposição contida nos **termos de uso e serviços da ferramenta** "Empresas afiliadas. Fazemos parte das Empresas da Meta. Como parte das Empresas da Meta, o WhatsApp troca informações com elas, conforme descrito na Política de Privacidade do WhatsApp, inclusive para disponibilizar integrações que possibilitem que você conecte a experiência do WhatsApp a outros Produtos das Empresas da Meta; para garantir a segurança, a proteção e a integridade dos Produtos das Empresas da Meta; e para aprimorar sua experiência com anúncios e produtos nos Produtos das Empresas da Meta. Saiba mais sobre as Empresas da Meta e seus respectivos termos e políticas aqui." Disponível em https://www.whatsapp.com/legal/terms-of-service. Acesso em: 30 de set. de 2022.

jurídica consolidada na União Europeia, fazendo ser imprescindível a análise dessa sistemática, incluindo-se o panorama histórico envolvido na estruturação do sistema europeu.

Nesse sentido, o primeiro marco temporal relevante para entendimento da trajetória adotada no velho continente é a segunda guerra mundial, pois, nessa oportunidade, com a finalidade precípua de garantir a paz, criou-se o Conselho da Europa (CdE), organização responsável pela promoção conjunta da Convenção Europeia dos Direitos Humanos em 1953.

A legislação em comento foi importe marco para o Estado do Direito, pois a partir dela surgiram importantes considerações sobre a democracia e sobre os direitos humanos, bem como as primeiras disposições sobre a direito à privacidade.

Isso porque, no Artigo 08º da Convenção Europeia dos Direitos Humanos encontra-se disposição expressa para que toda pessoa humana tenha o direito de ter sua vida privada respeitada, inclusive no que tangencia a inviolabilidade de correspondência e a inviolabilidade de domicílio.

Dessa forma, evidentemente a Convenção Europeia de Direito Humanos[31] serviu de paradigma para todas as demais estruturas jurídicas que futuramente viessem a ser criadas, posto que, uma vez garantindo inviolabilidade à vida privada, garante a intervenção mínima do Estado na autonomia privada, mas, em comunhão, garante a participação do agente estatal para garantia destes interesses, a fim de que eventuais atos lesivos sejam afastados da esfera privada do indivíduo.

Posteriormente, com o avanço dos sistemas legislativos, cumulado ao desenvolvimento dos meios digitais-informativos, formulou-se a Convenção da Eslováquia, convenção nº 108 de 1981, por meio da qual expandiu-se a proteção da vida privada para o ambiente digital, ora chamado pela própria convenção de *"sistemas automatizados"*, garantindo a qualquer usuário a proteção de suas liberdades fundamentais.

Sendo assim, considerando os efeitos vinculantes da Convenção da Eslováquia, todos os países signatários do documento passaram a regular a transferência de dados, seja na esfera do setor público, seja na esfera do setor privado, passando a serem estabelecidas as primeiras políticas procedimentais para aplicabilidade e garantia de efetividade da medida.

---

[31] Conforme exposto, o Artigo 08º da legislação garante proteção a Vida Privada "ARTIGO 8° Direito ao respeito pela vida privada e familiar 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros. UNIÃO EUROPÉIA. Convenção Europeia de Direitos do Homem de 1953. Disponível em <echr.coe.int>. Acesso em: 30 de out. de 2022.

Entretanto, a União Europeia ainda entendia ser necessário que fossem esculpidos novos sistemas jurídicos protetivos, capazes de atender os interesses populacionais, os interesses do mercado e o desenvolvimento tecnológico que estava sendo difundido no continente.

Para tanto, o bloco econômico desenvolveu a Diretiva nº 46 de 1995, considerada como primeiro instrumento jurídico que pautou com exclusividade as temáticas atinentes à proteção de dados.

De toda sorte, a diretiva outrora promulgada não possuía caráter impositivo, tratando-se de uma orientação do bloco para todos os países integrantes da organização, de modo que, ao invés de estabelecer-se uma organização sobre o tema, a diretiva passou a gerar uma série de discussões entre os países membros, os quais divergiam em uma série de questões contidas no documento, tal como os critérios qualitativos e quantitativos para aplicação de multas nos casos de vazamento de dados.

Diante da dissonância verifica, a mesa diretiva da União Europeia elaborou e propôs ao bloco a instituição do Regulamento Geral de Proteção de Dados, ao passo que, após a aprovação e certificação de todos os países membros, em 2016, houve a promulgação do documento, atingindo a sua eficácia plena em 25 de maio de 2018.

Convém ser reforçado que, o instrumento jurídico promulgado pela União Europeia, *Regulamento Geral de Proteção de Dados*, possuí eficácia de lei, cuja aplicabilidade dos efeitos erradia para todos os países integrantes do bloco econômico, *European Economic Area* (em português: Espaço Económico Europeu), independentemente do ordenamento jurídico internos destes países.

Surge então, o primeiro instrumento jurídico de eficácia imediata no território europeu, documento este que viria a ser utilizado como paradigma para estruturação da Lei Geral de Proteção de Dados, cuja aplicabilidade erradia efeitos em território nacional.

Mas, por mais que existam mecanismo formais de proteção da privacidade, fato é que a União Europeia também criou estruturas para efetividade das medidas criadas, isto é, o bloco econômico europeu, através da criação de *Supervisory Authorites* (em português: Autores Supervisores), criou entidades para controle e fiscalização da atividade concernente ao processamento de dados pessoais.

Nesse sentido, as Autoridade de Proteção de Dados possuem suas primeiras concepções na Convenção de Estrasburgo, convenção de 1981, por meio do qual delimitou-se as primeiras funções da entidade, garantindo a ela, precipuamente, os poderes de fiscalização e regulamentação, lastreado na legislação outrora desenvolvida.

Posteriormente, com a elaboração do Regulamento Geral de Proteção de Dados, efetivo

desde 2018 em todo o bloco econômico europeu, aprimorou-se as competências das autoridades públicas, conferindo a elas o poder de independência, para que assim fosse possível conferir maior eficácia na fiscalização da aplicação das normas contidas no regulamento.

A partir do poder fiscalizatório, realizo pelas autoridades de supervisão, é possível o sancionamento daqueles que cometem violações ao Regulamento Geral de Proteção de Dados, sejam elas pessoas jurídicas de direito privado, tal como empresas e *hackers* (compreendidos como aqueles terceiros que acessam indevidamente dados pessoais de usuários), tanto quanto pessoas jurídicas de direito público.

Neste cenário, pensando-se na possibilidade de aplicação de sanções em pessoas jurídicas de direito público, é possível rememorar-se o caso brasileiro de circulação de Fake News e direcionamento de propagandas nas campanhas eleitorais de 2018.

Nessa oportunidade, em que no campo de amostragem foi de análise sobre 346 *fake news* sobre as eleições, delimitou-se a amostra para análise aprofundada de somente 57 dessas *fake news*, mesmo assim, chegou-se expressivo resultado de que 1.073 contas foram alcançadas e mais de quase 4 milhões de compartilhamentos nos últimos meses das eleições, caso que, se ocorrido em território europeu, poderia ter sido evitado pela plena atuação das autoridades controladoras.[32]

Posto isso, demonstra-se a grande importância a existência de autoridade fiscalizadoras, dada a relevância de sua atuação, a própria União Europeia garante para essas entidades o poder de autogestão, tratando-se de autoridade independente, imparciais e desinteressas em qualquer movimento político ou econômico dos países membros.

Dessa forma, verifica-se um verdadeiro distanciamento da autoridade com os estados participantes do bloco econômico, garantindo-se então que as entidades não estabeleçam relações de dependência ou submissão, posto que, mediante a subordinação restaria prejudicada a garantia de segurança e neutralidade nas ações realizadas em benefício da proteção de dados.

Logo, o Regulamento Geral de Proteção de Dados, regulamento nº 2016/679, leciona em seu Artigo 51 que as autoridades controladoras deverão atuar de forma autônoma, com total independência para aplicação das normas dispostas no instrumento normativo, defendendo

[32] A pesquisa realizada sobre o tema foi elaborada por Tatiana Maria Silva Galvão Dourado "A livre circulação de ideias passou a ser exercida sem contrapeso editorial e mensagens políticas antidemocráticas ganham visibilidade pública online se populares elas forem. A metodologia da pesquisa foi construída a partir de métodos mistos e métodos digitais. Em uma primeira etapa, foi realizada análise exploratória da natureza política de 346 fake news sobre as eleições. Em seguida, delimitou-se amostra para análise aprofundada composta por 57 dessas fake news, que foram propagadas principalmente por 1.073 contas e alcançaram quase 4 milhões de compartilhamentos nos últimos meses das eleições, e analisadas a partir de quatro dimensões: clima de opinião hostil, dos meios e modos de propagação, da mimetização do formato jornalístico e conteúdo político. DOURADO, Tatiana Maria Silva Galvão. **Fake News na eleição presidencial de 2018 no Brasil**. 2020.

somente os interesses dos usuários para garantia das liberdades individuais e da privacidade, ocasionando, por consequência, a circulação de conjuntos informativos por todo o território do velho continente.

Essa autonomia garantida às autoridades controladoras é garantida de três formas distintas, de forma que todo o bloco garante para essas instituições absoluta autonomia financeira, estrutura e funcional, como garantia à observância do Artigo 52 do Regulamento Geral de Proteção de Dados

Assim, para garantia de efetividade da medida, todos os países integrantes do bloco econômico têm o dever de separação orçamentária, destinando reiteradamente verbas públicas para as Autoridade de Proteção de Dados, inclusive, garantindo que o controle orçamentário dos estados deverá ser justificado, sendo proibido a intrusão injustificada nas políticas de gestão financeira.

Ademais, as Autoridade de Proteção de Dados possuí uma organização funcional própria, contando com corpo de funcionário e cargos eletivos, de tal modo que a instituição de uma tirania é absolutamente vedada, já que cada cargo eletivo conta com tempo máximo de permanência de 04 anos, sendo vedada a exoneração sem justo motivo.

Diante de toda a estruturação apresentada, as Autoridades de Proteção de dados, contam com atribuições de investigação, correção e tarefas consultivas, podendo exercer tais poderes, seja na forma de auditorias, notificações de responsáveis, advertências, aplicações de sanções, bem como emissão de pareceres destinados a organizações estatais e entidades privadas.

Por todo o exposto, mostra-se essencial a instituição de uma autoridade com caráter autônomo para fiscalização e organização dos modelos jurídicos de proteção de dados, sendo certo que a instituição de um modelo jurídico está estreitamente vinculada, para bom funcionamento, a uma entidade capaz de garantir efetividade aos formalismos contidos no documento, sob pena de criação de uma legislação morta, cuja efetividade beira o inutilíssimo.

Portanto, o modelo europeu de proteção de dados, além de possuir grande histórico formal-protetivo, estatuindo normas legais de proteção aos usuários e regimentos procedimentos de processamento de dados, também possuí a organização ampla de um sistema efetivo, ou seja, o formalismo legal e sua eficácia estão subordinados à atuação da Autoridades de Proteção de Dados, as quais através de uma política estatal, uma cultura orçamentaria e social-política podem dar garantimos aos indivíduos.

2.1. Jurisprudência – Casos No Âmbito da Corte de Justiça da União Europeia

2.1.1. Caso Rigas

Popularmente conhecido como *Caso Rigas*, numerado como C-13/16[33], a corte de justiça da União Europeia deparou-se com o pleito da empresa Rigas, responsável pela administração de bondes na Letônia, a qual pretendia obter acesso, por intermédio do banco de dados da polícia, informações pessoais para identificar e obter contato de um indivíduo que danificou um dos bondes da companhia, oportunidade em que ele abriu a porta do taxi e arranhou a lataria do veículo.

Nesse sentido, após a solicitação da empresa administradora, a polícia local negou o fornecimento das informações de endereço e número telefônico do indivíduo, apenas expondo para a companhia o nome do passageiro, sob fundamento de que estava restringida de fornecer os dados solicitados em respeito à lei que rege o tratamento de casos administrativos no país, ordenamento interno da Letônia.

Diante do empasse apresentado, a Autoridade de Proteção de Dados da Letônia foi intimada para emitir um parecer sobre o assunto, concluindo então que a polícia estava estritamente ligada à legislação pátria, de modo que as regras de processamento de dados tratam-se de normas permissivas e não se vinculam para a obrigatoriedade no fornecimento de dados, ou seja, mesmo a empresa Rigas possuindo interesse legítimo para obtenção do conjunto informativo, fato é que a autoridade policial não tem a obrigação de divulgar os dados.

Dessa forma, para solução do litígio a controvérsia foi levada para conhecimento da Corte de Justiça da União Europeia, sob fundamento de aplicabilidade do Artigo 07º, f da diretiva 95/46/CE (“ f - O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do artigo 1º)[34].

Assim, diante do postulado, a Corte de Justiça da União Europeia determinou que o tribunal da Letônia caberia a decisão final sobre o casos, desde que três fases de apreciação fosses respeitadas para resolução da controvérsia, em outras palavras, a aplicabilidade do artigo acima exposto deveria de ser feita sob ótica da (I) viabilidade de existência de um interesse legítimo pelo terceiro, a quem os dados serão oportunamente divulgados (II) se o processamento

---

[33] CJUE. Case C-13/16 **Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA ‘Rīgas satiks**, julgamento de 4 de maio de 2017.

[34] Redação integral do Artigo 07º, f do Regulamento Geral de Proteção de Dados da União Europeia, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 30.out. 2022.

dos dados atenderá os interesses defendidos pelo terceiro (III) ao final, através do sistemática da ponderação, verificar se as liberdades e direitos fundamentais do titular dos dados apresentam conformidade com o interesse legítimo do terceiro.

Portanto, a partir do julgamento do *Caso Rigas*, três parâmetros foram estabelecidos para justificarem o vazamento de dados do usuário para terceiros interessados, de modo que, inexistindo o cumprimento de todos os fatores indicados a operadora estará desautorizada a realizar a transferência dos conjuntos informativos, julgamento esse que também destacou importante papel consultivo das Autoridade de Proteção de Dados.

2.1.2. Caso Mani

Neste caso, classificado com C-398/15[35], o que estava em pauta era a solicitação de um cidadão italiano para que seus dados pessoais fossem excluídos do Registro Público de Empresas, conjunto informativo controlado pela Câmara de Comércio Regional.

O pedido formulado pelo indivíduo, estava consubstanciado na necessidade de manutenção das suas atividades comerciais, uma vez que os registros públicos ligados à sua pessoa natural estavam ligados à uma antiga empresa falida, razão pela qual, qualquer um que realizasse o acesso aos registros se deparada com uma avaliação de riscos (*rating)* do usuário, fato que evidentemente vinha prejudicando o solicitando na concretização de novos negócios.

Diante da controvérsia apresentada, a Corte determinou que o requerente não poderia determinar a exclusão dos seus dados pessoais da plataforma, tampouco solicitar que os conjuntos informativos não pudessem ser acessados pelo público geral.

Isso porque, foi firmado o entendimento de que os interesses de terceiro, bem como do comércio em geral, não poderiam de ser atenuados pelo interesse privado, de modo que houve a sobreposição dos direitos coletivos sobre a solicitação de exclusão de dados formulados por pessoa individualizada.

Portanto, analisando o caso, bem como a postura adotada pela Corte de Justiça da União Europeia, pode-se verificar que em algumas situações fáticas específicas, tratando-se aqui de direito ao esquecimento, verifica-se a possibilidade de restrição das garantias individuais conferidas aos sujeitos de direito, de tal modo que, por mais que o ordenamento europeu realizasse a previsão protetiva, esta foi afastada em atendimento da coletividade

---

[35] CORTE DE JUSTIÇA DA UNIÃO EUROPEIA. Caso C-398/15 **Camera di Commercio, Industria, Aritigianato e Agricoltura di Lecce v. Salvatore Manni**, julgamento de 9 de março de 2017.

2.1.3. Caso Ryneš

Mais adiante, em análise caso Ryneš, registrado sob C-212/13[36], verificasse o pleito de Frantisek Ryneš, em que instalou um sistema de câmeras de segurança na entrada de sua casa, objetivando, exclusivamente garantir a proteção de sua casa, vida privada e família, após inúmeros ataques realizados por desconhecidos.

Nesse sentido, em breve síntese, o Sr. Ryneš, na cidade de Praga, capital da República Tcheca, havia recebendo inúmeros ataques de desconhecidos, consistentes em vidros quebrados e tentativas de assalto, sendo, até o momento, extremamente dificultoso identificar o autor dos delitos.

De toda sorte, após a instalação do sistema de segurança, novos ataques foram registrados na residência do indivíduo, de tal modo que, foi possível identificar dois indivíduos quebrando a janela da casa na noite do dia 6 para 7 de outubro de 207, filmagem essa que serviu como prova para instauração de processo penal contra os vândalos.

Ocorre que, os acusados impugnaram a prova apresentada, afirmando que se tratava de um tratamento ilegal dos dados pessoais, pois, em tese, não havia consentido para o processamento de suas imagens.

Em contraposição ao defendido pelo agressor, sustentou-se pela legalidade na instalação do sistema de segurança residencial, bem como pela captação de imagens dos indivíduos que transitavam na rua, tal como os dois agentes responsáveis pelo ataque.

Isso porque, o artigo 03º, nº2, da Diretiva 95/46, dispõe que o Regulamento Geral de Proteção de Dados pessoais não se aplica às atividades realizadas pelo indivíduo no exercício de atividades exclusivamente pessoais ou domésticas.[37]

Assim, diante dos dois argumentos apresentado, a Corte decidiu que os sistemas de vigilância por vídeo, destinados à captura de imagens de vias públicas não se encontram na hipótese de exclusão conferida pelo Regulamento Geral, de tal modo que que a atividade de

---

[36] CORTE DE JUSTIÇA DA UNIÃO EUROPEIA. Caso C-212/13 **Frantisek Ryneš v. Urad pro ochranu osobnich udaju**, Julgamento em 11 de dezembro de 2014.

[37] A integralidade do artigo mencionado encontra-se no próprio Regulamento Geral de Proteção " 2. A presente directiva não se aplica ao tratamento de dados pessoais:- efectuado no exercício de actividades não sujeitas à aplicação do direito comunitário, tais como as previstas nos títulos V e VI do Tratado da União Europeia, e, em qualquer caso, ao tratamento de dados que tenha como objecto a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando esse tratamento disser respeito a questões de segurança do Estado), e as actividades do Estado no domínio do direito penal,- efectuado por uma pessoa singular no exercício de actividades exclusivamente pessoais ou domésticas." Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 30 de out. de 2022.

tratamento estaria condicionada à autorização do usuário para processamento da imagem, mas que, neste caso em partículas, poderia haver o tratamento das imagens obtidas em detrimento da proteção da propriedade privada, saúde, e vida dos familiares, bem como da própria integridade física do Sr. Ryneš.

2.1.4. Caso Fashion ID

Ademais, neste caso, caso C-40/17[38], a empresa Fashion ID GmbH &CO. KG é uma loja, com plataforma online, destinada a comercialização de artigos de moda, inserindo em seu *website* um *plug-in* (botão de redirecionamento) de curtida, vinculada ao aplicativo *Facebook*.

Consequentemente, no momento em que quaisquer usuários acessasse a página da loja *Fashion ID* as suas informações pessoais de endereço e IP (*Internet Protocol* – conjunto de dados virtuais do usuário) eram automaticamente transferidas para o *Facebook*, independentemente se o usuário realizasse qualquer interação com o botão de *plug-in*, inclusive, tendo ele conta ou não na mídia social ora relatada.

Sendo assim, a Verbraucherzentrale NRW e.V, uma associação alemã destinada para proteção dos consumidores, ajuizou uma ação inibitória contra a empresa, fundamentando que a utilização do *plug-in* no site violaria preponderantemente os direitos dos usuários perante a legislação protetiva de dados.

Diante do ajuizamento da ação, o Tribunal Regional Superior de Dusseldorf, Alemanha, solicitou a interpretação de diversos dispositivos legais do Regulamento Geral de Proteção de Dados, Diretiva 95/46/CE, questionando preliminarmente a legitimidade da associação em pleitear sob o interesse de terceiros, e, no mérito, colocou a prova a responsabilidade de tratamento de dados pelo *Fashion ID*, bem como sua obrigatoriedade em comunicar os usuários sobre o processamento de tais conjuntos informativos, sob ótica do dever de recolher o consentimento informado dessas pessoas.

Nesse sentido, para melhor julgamento do caso e solução do litígio, o tribunal local solicitou que a Corte de Justiça da União Europeia formulasse um parecer, a fim de que fossem respondidos os questionamentos e dúvidas do Tribunal de Dusseldorf sobre a aplicabilidade das normas contidas no Regulamento Geral de Proteção de dados.

Portanto, à luz do exposto, a Corte determinou que o Tribunal Regional Superior de

[38] CORTE DE JUSTIÇA DA UNIÃO EUROPEIA, Caso C-40/17, **Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e V**, julgado em 29 de julho de 2019.

Dusseldorf, Alemanha, analisasse a questão considerando que associações sem fins lucrativos possuem legitimidade ativa para instaurarem procedimento judiciais, sob fundamento na legislação protetiva e proteção dos interesses de consumidores, ainda, sustentou que é uma obrigatoriedade a coleta do consentimento dos usuários, sendo ainda um dever da plataforma informar o navegante que seus dados estão sendo coletados.[39]

2.1.5. Caso Keylogger Software – Justiça Federal do Trabalho na Alemanha

A ferramenta *Keylogger Software* foi instalada nos computadores e todo os funcionários de uma empresa alemã, consistindo em um aplicativo extremamente invasivo, capaz de armazenar todas as informações de digitação dos funcionários, ou seja, o aplicativo não só registrava o trabalho final do empregado, mas toda a atividade por eles realizada, cada palavra e ação registrada ao longo da persecução das funções laborais.

Sendo assim, diante da evidente atividade violadora de direitos informacionais, em 07 de julho e 2017, um ex-empregado da empresa entrou cum um processo judicial em face da ex-empregadora, BAG 2 AZR 681/16[40], de tal modo que obteve integral procedência do pedido na instância primária, fazendo com que empresa recorresse ao tribunal, por intermédio de apelação, alegando legítimo interesse de rastrear as atividades de seus funcionários.

Ocorre que, em julgamento ao recurso, o tribunal local determinou que a atividade de monitoramento realizada pela empresa não era razoável, tratando-se de medida que não poderia sustentar-se no legítimo interesse da companhia, posto que a funcionalidade do aplicativo violava a autodeterminação do usuário sobre os dados capturados.

Portanto, a corte entendeu que diversos fatores levavam a conclusão que o monitoramento era excessivo, inclusive, porque eram capturadas informações bancárias,

---

[39] Nesse sentido, o parecer formulado pela Corte de Justiça da União Europeia respondeu todos os questionamentos formulados pelo tribunal local, elencando dentro da resposta o seguinte direcionamento "O consentimento da pessoa em causa obtido nos termos do artigo 7.o, alínea a), da Diretiva 95/46 tem de ser dado a um administrador de uma página Web que integrou o conteúdo de um terceiro. O artigo 10.o da Diretiva 95/46 deve ser interpretado no sentido de que a obrigação de informação prevista nesta disposição também é aplicável a esse administrador da página Web. O consentimento da pessoa em causa nos termos do artigo 7.o, alínea a), da Diretiva 95/46 tem de ser dado e a informação na acepção do artigo 10.o da mesma diretiva tem de ser prestada antes de os dados serem recolhidos e transferidos. No entanto, o alcance destas obrigações deve corresponder à responsabilidade conjunta do administrador pela recolha e pela transmissão dos dados pessoais." Disponível em https://curia.europa.eu/juris/document/document.jsf?text=&docid=209357&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=30349. Acesso em: 30 de out. de 2022.

[40] BUNDESARBEITSGERICHT. **Caso BAG 2 AZR 681/16**, julgado em 27 de julho de 2017. Disponível em: http://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=pm&nr=19403. Acesso em: 30 out. de 2022.

números de PIN e senhas, sem que fosse oportunizado ao funcionário consentimento de fornecimento, sendo então a medida necessária restringir a atividade do empregador, em respeito a todos os sistemas protetivos da União Europeia, no que concerne o tratamento de dados.

3. PANORÂMA NACIONAL DA SEGURANÇA DE DADOS NA UTILIZAÇÃO DE DISPOSITIVOS VESTÍVEIS

Evidentemente, a discussão acerca do tratamento de dados digitais não pode se restringir aos métodos e estruturas jurídicas fundamentadas ao redor do mundo, assim como exposto no tópico anterior no tocante a estruturação europeia de proteção de dados, sendo certo que se faz necessária a análise dos preceitos e fundamentos jurídicos consolidados em território nacional para aferição do nível protetivo conferido pela legislação pátria aos dados processados em dispositivos vestíveis.

Isso porque, assim como todo o restante do globo, no Brasil também se difundiu a tecnologia portátil, sendo possível observar-se a utilização de dispositivos vestíveis por inúmeros indivíduos circulantes em território nacional.

Segundo dados coletados pelo IBGE (Instituto Brasileiro de Geografia e Estatística)[41], mais de 80% (oitenta por cento) dos domicílios brasileiros possuem internet, dados estes que evidenciam a importância do tratamento de dados em território nacional, visto que o alcance de internet para esse contingente populacional significa o processamento de mais de 80 (oitenta) milhões de usuários, conjuntos informacionais encontram-se disponíveis para operadores de dados, conforme estatísticas apresentadas pelo Governo Nacional[42].

Assim, torna-se indiscutível a necessidade de análise do ordenamento jurídico pátrio para verificação dos mecanismos que resguardam os dados dos usuários de dispositivos vestíveis, assim como, se existente, verificar eventuais lacunas legislativas no tocante a matéria,

---

[41] Os dados de utilização de internet, requisito intrinsicamente vinculado com a utilização de *Wearables*, se encontram disponíveis na plataforma online do IBEG, no seguinte endereço eletrônico https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular-no-brasil.html. Acesso em: 06 de nov. de 2022.

[42] Os dados demográficos em análise foram obtidos através da pesquisa Censo 2022, realizada pelo Governo Federal. Disponível em: www.gov.br/pt-br/noticias/educacao-e-pesquisa/2022/10/censo-2022-ja-alcancou-quase-metade-da-populacao-estimada-do-pais#:~:text=Quase%20metade%20da%20popula%C3%A7%C3%A3o%20brasileira,da%20popula%C3%A7%C3%A3o%20estimada%20do%20pa%C3%ADs. Acesso em 06 de nov. de 2022.

posto que, assim como no ordenamento jurídico europeu, a existência de preceitos vagos gera a propensão de uma atuação mais efetiva da esfera judiciária para criação de padrões e preceitos normativos para cumprimento dos já existentes.

Nesse sentido, cumpre informar em um primeiro momento, que o Brasil é considerado um país retardatário no que concerne a proteção de dados pessoais na esfera digital, uma vez que, considerando toda a perspectiva global sobre o assunto, tanto quanto movimentações políticas, quanto movimentações jurídicas sobre o tema, o ordenamento jurídico pátrio apenas realizou previsões protetivas muito após a estruturação global da temática.

Esse descompasso temporal deve-se muito a perspectiva econômica e cultural da nação, muito embora o Brasil seja hoje uma país consolidado no que abrange a utilização de meios tecnológicos, fato é que não é um polo industrial, reconhecido mundialmente por avanços e criações industriais.

Pelo contrário, a manufatura nunca foi o principal objeto comercial brasileiro, sendo ao longo do tempo uma nação que preocupou-se estritamente com a produção agrária e o desenvolvimento do setor mercadológico propiciado pela agricultura e pecuária, o que consequentemente implica diretamente da fundamentação jurídica consubstanciada ao longo do tempo, à luz disso, pode-se notar que o *Estatuto da Terra – Lei nº 4.504*, legislação concernente às obrigações relacionadas a imóveis rurais e política agrícola entrou em vigor em 30 de novembro de 1964, cerca de 56 (cinquenta e seis) anos atrás.

Em outras palavras, a existência precípua de uma legislação exclusivamente voltada para proteção da terra e voltada para tratar das relações jurídicas decorrentes de imóveis rurais demonstra a preocupação do legislador pátrio com a organização mercantil agrícola, bem como ilustra que o Brasil não é o país da manufatura, o que consequentemente implicou no retardamento da estruturação de uma política nacional de proteção de dados.

Logo, o primeiro regime jurídico, responsável pelo tratamento específico da proteção de dados foi a Política Nacional de Informática, a qual, de forma genérica e sem maiores complicações, trouxe disposições sobre a possibilidade de sigilo informacional, bem como organizou procedimentos de retificação e de dados pessoais.

Ao lado da Política Nacional de dados, a Constituição Federal de 1988, foi responsável pelas disposições iniciais sobre o Habeas Data, conforme estruturação contida no Artigo º, LXXII, da Magna Carta, com complementação fundada pelo regulamento interno da Lei nª 9.507 de 1997, os quais criaram os preceitos fundamentais deste importante remédio constitucional utilizado para retificação de informações pessoais, essencialmente restringidas por determinada instituição privada ou pública.

Desta forma, o legislador pátrio realizou os primeiros passos necessários para estruturação de uma política protetiva de dados pessoais na utilização da internet, aplicável também na utilização de *Wearables*, uma vez que trouxe conceitos e fundamentações jurídicas iniciais sobre dados e suas relevâncias na esfera pública e privada, sendo ainda possível observar a preocupação para garantir ao proprietário do dado a autonomia de seus conjuntos informativos, protegendo-o quanto a insegurança e a violação desses conjuntos informativos.

Posto isso, estruturada a importância dos dados e da titularidade da informação, o progresso nacional foi marcado pela regulamentação do Marco Civil da Internet – Lei nº 12.962 de 23 de abril de 2014, por meio da qual, conforme Artigo 1º, caput, do referido diploma, preceitua normas garantidoras dos direitos e deveres inerentes ao uso de internet no Brasil.

Para tanto, proteção e determinação do processamento de dados em ambiente digital, está contido no Marco Civil da Internet um capítulo exclusivo para fundamentação da temática, estruturação essa contida na *Sessão II- Da Proteção aos Registros, aos Dados Pessoais e as Comunicações Privadas.*

No referida sessão, é possível se observar a existência de um artigo propriamente designado para a reafirmação de princípios básicos ineres aos usuários, isso porque, pela breve leitura do Artigo 10, verifica-se que o legislador preocupou-se veementemente em destacar a necessidade de proteção à intimidade, a vida privada, honra e imagem das pessoas envolvidas em relações jurídicas desenvolvidas em ambiente virtual, medida protetiva a qual aplica-se indistintamente na utilização na utilização de dispositivos vestíveis.

Mas não só, em continuidade da leitura do diploma legal em análise, nota-se que no Artigo 11 existe preceituação afirmativa que reforça a necessidade dos receptores de dados em garantir ao usuários a proteção dos dados pessoais, zelando pelos direitos inerentes a privacidade e ao sigilo informativo, sendo certo que a dinâmica estabelecida vinculada empresas e corporações atuantes em território nacional o que significa que, ao espelho do noticiado em território europeu, o mercado restou-se obrigado à cumprir com as novas diretrizes protetivas estabelecida pelo legislador brasileiro, cabendo à eles realizar a conformação de suas políticas internas com o ordenamento jurídico estruturado.

Somando-se ao apresentado, posteriormente, com o advento da Lei Geral de Proteção de Dados – Lei nº 13.709 de 14 de agosto de 2018, surgiram as disposições finais sobre a temática, sendo construído um mecanismo jurídico consolidado sobre o tratamento e proteção e dados pessoais em território nacional no país, cujos dispositivos que melhor atendem ao tema aqui abordado já foram analisados em tópicos anteriores.

Sendo assim, mesmo diante da existência de uma legislação protetiva, ainda existem

diversos problemas que não possuem solução, principalmente quando em pauta tecnologias, cujo desenvolvimento e surgimento são recentes, de tal forma que, o ordenamento jurídico passa a apresentar certas lacunas para o tratamento de dados dos usuários, tal como, como anteriormente exposto, problemáticas como o consentimento e a inviolabilidade do dado privado.

Ocorre que, à luz dos precedentes desenvolvidos pela Suprema Corte da União Europeia, diante de um cenário desenvolvimentista, em que o Direito se torna uma feramente inócua, incapaz de alcançar o progresso mercadológico, surge margem para o ativismo judicial[43].

Entende-se como ativismo judicial, como a intervenção do poder judiciário para garantismo da justiça, em outras palavras, havendo um contexto de absência do poder legislativo, caberá, nos limites dos três poderes, ao demais garantirem o equilíbrio, a fim de efetivação de princípios individuais, inclusive direitos humanos, inerentes aos indivíduos de determinado círculo social.

Entretanto, dado o nascimento recente da matéria em análise, cujas problemática ainda não foi amplamente enfrentada pelos tribunais pátrios, o ativismo judicial, desacompanhado de uma efetivação uniforme de precedentes, pode ocasionar um descompasso decisório, em outras palavras, o ativismo judicial no tocante a proteção de dados de usuários pode estar estritamente vinculada a efetivação de uma insegurança jurídica, propiciando diferentes soluções para o mesmo contexto fático-jurídico.

Portanto, evidentemente o ordenamento jurídico não é capaz de acompanhar o desenvolvimento tecnológico e o avanço da ciência de dados, apresentando, consequentemente, uma série de problemáticas cujo escopo jurídico não apresenta soluções, seja pelo desenvolvimento tardio da legislação protetiva, seja pela falha ao estabelecer critérios claros na abordagem informativa, cabendo, em último caso a atuação do poder judiciário para efetivação desses direitos perante ao processamento latente de dados pelas plataformas e operadoras de dispositivos vestíveis.

---

[43] CAMARGO, Daniel Marques de; DOMINGOS, Fernanda Cristina Rosseto**. Ativismo Judicial: Limites, Possibilidades e Reflexos na Efetivação de Direitos Humanos Fundamentais.** In: SIQUEIRA, Dirceu Pereira; SANTOS, Murilo Angeli Dias dos. Estudos contemporâneos de hermenêutica constitucional. Birigui: Boreal, p. 67, 2017.

CONCLUSÃO

Diante de todo o quanto apresentado, fica evidente que os dispositivos vestíveis já se encontram difundidos na sociedade brasileira, sendo considerados dispositivos usualmente utilizados no cotidiano popular, seja para a prática de esportes, seja para o aferimento de níveis clínicos, vinculados a saúde do usuário, seja por interesse no mercado de consumo, despertado pela moda e pressão popular, ou ainda, necessidades do mundo corporativo.

Entretanto, por serem dispositivos atrelados ao próprio corpo humano, o tempo de permanência de suas funcionalidades é maximizado, garantindo que as operadoras dos produtos consigam extrair uma quantidade exorbitante de dados dos usuários aderentes da ferramenta, dados esses que são captados, armazenados e posteriormente compartilhados pelas operadoras de dados.

Ocorre que, a utilização de dispositivos vestíveis e o tratamento de dados captados proporcionam ampla discussão jurídica sobre a qualidade de preservação da privacidade e individualidade do indivíduo protegido pela legislação pátria, colocando-se à prova a efetividade das medidas protetivas estabelecidas pela constituição federal e pela própria legislação supraconstitucional.

Dessa forma, através dos apontamentos apresentados, tanto quanto pela revisão bibliográfica consubstanciada, fica evidente as falhas na coleta de consentimento do usuário, o retardamento na instauração de políticas públicas protetivas, tanto quanto a consolidação tardia de uma legislação atinente à problemática da privacidade e proteção de dados.

Portanto, dentre todas as divergências e questionamentos levantados, fica evidente a insuficiência do sistema legislativo átrio para solução dos conflitos decorrentes das relações instauradas entre usuários de dispositivos vestíveis e as plataformas operadoras de dados, fato que permite a flexibilização de decisões judiciais, a luz dos acontecimentos evidenciados no continente europeu, replicando-se na propagação de ativismo judicial por parte do judiciário.

BIBLIOGRAFIA

ALMEIDA, Juliana Evangelista de; ALMEIDA, Daniel Evangelista Vasconcelos**. Os Provedores de Aplicação de internet e a mitigação do princípio da finalidade em vista da cooperação com agências de inteligência**. Revista de Direito, Governança e Novas Tecnologias, Curitiba, V. 2, n. 2, p. 53-74, jul/dez. 2016. Disponível em: https://indexlaw.org/index.php/revista dgnt/article/view/1487. Acesso em: 08 de junho de 2022.

APPLE INC, **Icloud Drive – Welcome To Icloud,** Apple.com, 2022. Disponível em: https://www.apple.com/legal/internet-services/icloud/.

BAGGIO, Andreza Cristina. O direito do consumidor brasileiro e a teoria da confiança. São Paulo: Editora Revista dos Tribunais, 2012.

BARBOSA, Murilo Oliveira. A importância do direito à privacidade digital, redes sociais e extensão universitária. Fragmentos de Cultura, Goiânia, v. 24, n. 8, p. 89-97, dez. 2014. Disponível em: http://dx.doi.org/10.18224/frag.v24i0.3757. Acesso em 08 de junho de 2022.

BEHRENS, Fabiele. **A assinatura eletrônica como requisito de validade dos negócios jurídicos e a inclusão digital na sociedade brasileira.** Curitiba: Dissertação de Mestrado PUC/PR, 2005.

BUCHER, T. *If... Then Algorithimic Power And Politics*. New Tork: Oxford University Pressa, 2018.

BUNDESARBEITSGERICHT. **Caso BAG 2 AZR 681/16**, julgado em 27 de julho de 2017. Disponível em: http://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=pm&nr=19403. Acesso em: 30 out. de 2022.

CAMARGO, Daniel Marques de; DOMINGOS, Fernanda Cristina Rosseto**. Ativismo Judicial: Limites, Possibilidades e Reflexos na Efetivação de Direitos Humanos Fundamentais.** In: SIQUEIRA, Dirceu Pereira; SANTOS, Murilo Angeli Dias dos. Estudos contemporâneos de hermenêutica constitucional. Birigui: Boreal, p. 67, 2017.

CAMBRIDGE SCHOOL CLASSICS, **Cambridge Dictionary of American English for Speakers of Portuguese**, Editora WMF Martins Fontes, 2013.

CJUE. Case C-13/16 **Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiks**, julgamento de 4 de maio de 2017.

CORTE DE JUSTIÇA DA UNIÃO EUROPEIA. Caso C-212/13 **Frantisek Ryneš v. Urad pro ochranu osobnich udaju**, Julgamento em 11 de dezembro de 2014.

CORTE DE JUSTIÇA DA UNIÃO EUROPEIA. Caso C-398/15 **Camera di Commercio, Industria, Aritigianato e Agricoltura di Lecce v. Salvatore Manni**, julgamento de 9 de março de 2017.

DA SILVA PEREIRA, Caio Mário. **Instituições de Direito Civil - vol. III - Contratos**. Editora Forense, Rio de Janeiro, p.7, 11ª ed., 2004.

DOURADO, Tatiana Maria Silva Galvão. **Fake News na eleição presidencial de 2018 no Brasil**. 2020.
EL CLARÍN. Para cuidales la salud, exigen a estudiantes que usen pulsera inteligente. *El Clarín,* p. 1-3, 2016.
FITBIT INC. *FITBIT Terms Of Service*. Disponível em: https://www.fitbit.com/legal/terms-of-service. Acesso em 088 de junho de 2022.

GAGLIANO, Pablo Stolze e FILHO, Rodolfo Pamplona. **Novo Curso de Direito Civil, Parte Geral**, 1, 16ª Edição, Editora Saraiva, Revista e Atualizada, São Paulo, Capítulo X, p. 391, 2014.

GAO, Yiwen; LI, Hi; LUO, Yan; **An Empirical Study of Wearable Technology Acceptance in Healthcare, R**egular Paper. Emerald Group Publishing Limited, v. 115, n. 9, p. 1704-1723, 2015.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro, v. 3**: Contratos e Atos Unilaterais-9ª Ed. São Paulo: Saraiva, p. 41, 2020.

GOULD, H. Form app doctors to big data: five ways tech will shape healthcare. *The Guardian,* p. 17-19, 10 out. 2016.

LUGER, Ewa; MORAN, Stuart; RODDEN, Tom. Consent for all: revealing the hidden complexity of terms and conditions. In: Proceedings of the SIGCHI conference on Human factors in computing systems. 2013. p. 2687-2696.

MENDES, Laura Schertel. **O direito fundamental à proteção de dados pessoais. Revista de Direito do Consumidor**, São Paulo, v. 79, p. 45-82, jul./set. 2011.

MITCHELL, Robb. **Sensing mine, yours, theirs, and ours: interpersonal ubiquitous interactions.** In: Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers. 2015. p. 933-938.

PEREZ, Alfredo J.; ZEADALLY, Sherali, **Privacy Issues and Solutions for Consumer Wearables**, IEE Computer Society, IT Professional, 2018.

PINHEIRO, Patrícia Peck, **Proteção de Dados Pessoais: Comentário a Lei nº 13.709/2018 (LGPD)**. 2ª. Ed., São Paulo, Editora Saraiva Educação, 2020.
PISA, Licia Frezza. **Discurso e poder em Michel Foucault: o controle do que dizemos na rede visto pela política de privacidade do Google.** Domínios de Lingu@ gem, v. 8, n. 1, p. 250-266, 2014.

UNIÃO EUROPÉIA. **Convenção Europeia de Direitos do Homem de 1953**. Disponível em <echr.coe.int>. Acesso em: 30 de out. de 2022.