U.PORTO

2.° CICLO DE ESTUDOS

CIÊNCIAS JURÍDICO-CIVILÍSTICAS

Internet das coisas (*IoT*) e a Proteção dos Dados: uma análise da aplicabilidade do RGPD aos dispositivos inteligentes

Ellis Bezerra de Mendonça Oliveira

M
2021

Ellis Bezerra de Mendonça Oliveira

Internet das Coisas (*IoT*) e a Proteção dos Dados: uma análise da aplicabilidade do RGPD aos dispositivos inteligentes

Dissertação conducente à obtenção do grau de Mestre em Ciências Jurídico-Civilísticas, realizada sob a orientação da Professora Doutora Maria Raquel Guimarães.

Setembro de 2021

Resumo

Nos primórdios, a internet foi concebida como uma rede entre computadores com o objectivo de criar um mundo virtual paralelo ao mundo real. A Internet das Coisas (*IoT*) surgiu nesse cenário para romper a fronteira entre esses dois mundos, por meio da conexão entre os diversos objetos do quotidiano a computadores e sensores, em um sistema ubíquo, que possibilita uma coleta massiva de dados do mundo real, o tratamento automatizado dessas informações e a tomada de decisões sem qualquer intervenção humana.
Os benefícios trazidos por essa nova realidade às mais diversas áreas, vêm acompanhados de um impacto no conceito de privacidade e de uma série de questionamentos éticos acerca dos limites da penetrabilidade da inteligência artificial nas vidas humanas e dos riscos decorrentes da concentração de poder nas mãos dos controladores dos bancos de dados, sejam eles públicos ou privados.
O presente trabalho visa a analisar como as regras do Regulamento Geral de Proteção de Dados da União Europeia respondem às demandas originadas nesse novo cenário e em que medida são eficientes na consecução do propósito de proteger a privacidade dos titulares de dados sem impor pesados óbices ao desenvolvimento tecnológico.

Palavras-chave: Internet das Coisas, *IoT*, Privacidade, Proteção de Dados, Direitos da Personalidade, Regulamento Geral de Proteção de Dados, RGPD, Inteligência Artificial, Decisões automatizadas.

Abstract

In the beginning, the internet was created to function as a network between computers, emerging the virtual world in parallel to the real world. Then, the Internet of Things (*IoT*) was designed to break the boundary between these two worlds by interconnecting daily objects with computers and sensors, in a ubiquitous system, enabling a massive data collection, automated process of these information and decision-making without human interference.
This new reality brings benefits in many areas, but at the same time raises ethical questions about the limits of artificial intelligence penetration in human lives and about the risks concentration of power in the hands of data controllers, whether public or private.
This paper aims to assess how the rules of EU General Data Protection Regulation respond to the issues arising in this new scenario and how efficient they are achieving the purpose of protecting the privacy of data subjects without imposing obstacles to the improvement of technology.
Keywords: Internet of Things, *IoT*, Privacy, Informational Privacy, Data Protection, Personality Rights, General Data Protection Regulation, GDPR, Artificial Intelligence, Automated Decision-making.

Sumário

Introdução

O progresso tecnológico experimentado nas últimas décadas tem impactado substancialmente na vida das pessoas, fazendo surgir novas formas de comunicação, de produção, de transporte, de interação social. Desde o surgimento da internet, contudo, a importância da tecnologia na vida do homem comum tomou proporções inéditas e, a partir da Internet das Coisas, ganhou concretude a realidade futurista das máquinas a "conviverem" com seres humanos em um mundo em que real e virtual são quase indissociáveis. Menos de três décadas desde a criação da World Wide Web (www), que popularizou o acesso à rede mundial de computadores, e hoje já não precisamos acessar a internet, pois vivemos a internet. Tamanha revolução social não viria sem nos impor consequências negativas ou diversos desafios éticos e jurídicos.

Neste trabalho, nos debruçamos sobre um pequeno recorte desse desafio, analisando o impacto da Internet das Coisas no que concerne ao direito à privacidade e, mais especificamente, à proteção dos dados pessoais.

Iniciamos, assim, na primeira parte, pelo estudo do elástico conceito de privacidade e sua evolução histórica, sempre a sofrer ajustes necessários a responder aos anseios sociais dominantes. Desse conceito, extraímos a noção de proteção dos dados pessoais, que embora originada nesse direito da personalidade à privacidade, nele não se esgota. Por fim, descrevemos o histórico da proteção jurídica garantida aos dados pessoais, definindo o contexto jurídico no qual surgiu o atual Regulamento Geral de Proteção dos Dados (RGPD) vigente na União Europeia, mas com inquestionável impacto em todo o mundo digital.

Na segunda parte, cuidamos de conceituar brevemente a Internet da Coisas (*IoT*) e os elementos tecnológicos que a fizeram possível e/ou a potencializaram, como a inteligência artificial, o *machine learning* e o *Big data*. A partir daí, analisamos a aplicabilidade do RGPD aos dispositivos *IoT*, apresentando o enquadramento jurídico dessa realidade.

Já na terceira parte, voltamos os olhos ao RGPD e a apresentamos uma leitura dos seus objetivos, princípios e conceitos sob a óptica tecnológica da Internet das Coisas. Destacamos, outrossim, as peculiaridades dessa realidade tecnológica e como suas características impactam na interpretação e aplicação do Regulamento.

Por fim, apresentamos alguns dos principais desafios a serem enfrentados para aplicação prática das regras do RGPD aos dispositivos inteligentes e às tecnologias a ele associadas,

descrevendo os pontos de aparente incompatibilidade entre os avanços tecnológicos e as regras e princípios do Regulamento.

1. A proteção jurídica dos dados pessoais: o contexto histórico do RGPD

1.1 A evolução do conceito de privacidade e sua proteção como direito da personalidade

O conceito de privacidade, significando algo de acesso restrito em contraponto ao que é de domínio público, remonta à antiguidade clássica. Embora na Grécia antiga Aristóteles já falasse na existência da *esfera privada* ("oikos") e da *esfera pública* ("polis"), foi dos romanos que herdamos o vocábulo *privatus*, raiz etimológica de *privacidade*[1]. Para os antigos, o âmbito privado, para além da família, abarcava igualmente questões económicas, diferentemente do âmbito público, relativo às relações comunitárias e à vida do cidadão na *polis*.

Note-se que desde então o conceito de "privado" nasce de um critério negativo em relação ao que é público. Representa, assim, um conjunto de coisas agregadas por terem em comum o fato de não serem identificadas como algo de interesse ou domínio público. Essa dicotomia público-privada foi, com o tempo, sendo associada a outra: vida pessoal (homem singular ou família) *versus* vida social ou comunitária[2]. Por isso, ao poucos, o termo *privacidade* passou a abarcar tudo aquilo que se afastava da vida comunitária e estava relacionado com a individualidade do homem ou com o seu núcleo social mais íntimo: a família.

Segundo Bioni[3], a habitação representaria o ambiente privado (o homem em seu castelo). A casa, assim, seria um ambiente reservado à reflexão e ao pensamento crítico, antecessores necessários às discussões que teriam lugar no espaço público. Esse refúgio, segundo o autor, protege o indivíduo contra a instalação de visões totalitárias, sendo o direito à privacidade basilar à democracia e condição essencial ao livre desenvolvimento da personalidade[4].

Tal distinção ostentava uma consequência decisória, por caber ao *homem* e não à *polis* decidir sobre sua esfera privada e determinar os rumos de suas vidas naquilo que não dissesse respeito à vida comunitária. Com o tempo, a *privacidade* foi estreitando os laços de conteúdo com

---

[1] CORREIA, Victor. *Sobre a Privacidade*. Editora Sinapsis. 2016. p. 63.
[2] Paulo Mota Pinto fala que a privacidade se baseia em uma *tensão entre o social e o individual*. PINTO, Paulo Mota. *Direitos de Personalidade e Direitos Fundamentais: estudos*. Coimbra. Gestlegal, 2018. p. 509.
[3] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento.* Rio de Janeiro, Forense, 2019.p. 93.
[4] BIONI, Bruno Ricardo. *Op. Cit*. p. 93.

o conceito de liberdade, já que, na esfera privada, cabia ao indivíduo escolher livremente seu modo de agir. Esse pensamento encontra seu apogeu no Iluminismo, notadamente com ascensão do pensamento liberal, como ensina Correia[5].

Os limites do conceito de *privacidade*, contudo, ganham contornos diferentes a depender do momento histórico e cultural considerado. Ora, sendo privado tudo o que não é público, é de se concluir que o conteúdo da esfera privada variará ao longo da história e estará relacionado aos diversos arranjos políticos adotados e ao grau de transferência de poder da esfera individual para o Estado, em benefício da coletividade e do interesse público. Por esse motivo, o vocábulo *privacidade* tem como característica intrínseca certa elasticidade e imprecisão, não sendo possível extrair dele um significado estanque sem ter em consideração o momento histórico e a forma de abordagem do tema (se sob a perspectiva jurídica, filosófica, política)[6]. Dessa elasticidade decorre a impossibilidade de definir os contornos de um bem jurídico: por um lado, reflete sua amplitude, por outro pode resultar em uma nebulosidade, como as ideias de "felicidade" e "segurança"[7], que impede ou dificulta sobremaneira a proteção legal.

Como tentativa de segmentar os vários extratos da privacidade, para fins de estabelecer o grau de sigilo e a proteção merecida, foi elaborada a teoria das esferas, creditada a Heinrich Hubmann, na obra "Das Persomlichkeitrecht", de 1953. O autor propõe em termos de profundidade do grau de privacidade a ilustração representada por três círculos concêntricos, caracterizando, do mais restrito para o mais abrangente, a "esfera individual", a "esfera privada" e a "esfera secreta"[8].

Em linhas gerais, o que é "individual" corresponde ao homem integrado ao meio social, como seu "carácter", sua "personalidade", dando ensejo ao "direito a ser socialmente respeitado na sua individualidade" e a uma resistência contra a "massificação" do indivíduo. Já as esferas "privada" e "secreta" representam a necessidade de proteção de certos aspetos da vida contra a invasão pública e a "curiosidade". Segue Pinheiro a defender ser na "área secreta" que se

---

[5] CORREIA, Victor. *Op. Cit.*. p. 64.
[6] PINTO, Paulo Mota. *Op. Cit.*. p. 503.
[7] PINTO, Paulo Mota. *Op. Cit.*. p. 504.
[8] PINHEIRO, Alexandre Sousa. *Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*. AAFDL. Lisboa, 2015. p. 447.

desenvolvem os pensamentos, opiniões, descrição de sensações e tudo aquilo que as pessoas desejam manter em reserva e possuem interesse no seu segredo[9].

Já Paulo Mota Pinto esclarece que a definição de privacidade pressupõe, em um primeiro momento, a sua distinção em relação a outros interesses com os quais por vezes é confundida. Por isso, o autor cuida de excluir do conceito de privacidade noções relativas à liberdade de condução da própria vida, assim como a reputação, o bom nome e a livre fruição de atributos pessoais[10]. Por outro lado, numa perspectiva positiva, Mota Pinto enumera três interesses abrangidos pelo conceito de privacidade: o controlo sobre as informações pessoais, a subtracção da atenção dos outros (anonimato) e a solitude[11]. Para além disso, a privacidade é a estrutura que garante o desenvolvimento da individualidade e das relações humanas de confiança. Por isso, é comumente associada com um aspecto da dignidade humana[12].

Em terras norte-americanas, é considerado marco da proteção jurídica da privacidade o artigo *The Right of Privacy*, de autoria de Warren e Brandeis e publicado em 1890 na *Havard Law Review*[13]. Na época, nos Estados Unidos da América, experimentava-se o avanço da imprensa, popularizada, massificada e incrementada pela possibilidade de ilustração com fotografias. Conforme descreve Pinheiro[14], a partir de 1860, os jornais passaram a publicar entrevistas que se revelavam no mais das vezes uma devassa à intimidade da pessoa, embora de forma consentida, pois o entrevistado anuía com as perguntas. Outro elemento citado pelo autor consiste na invenção de George Eastman, responsável pelo lançamento das máquinas de fotografar *hand-handle Kodak*. Sob o *slogan* "You press the button, we do the rest", os dispositivos se popularizaram e o ato de fotografar passou a significar mais um novo meio de invasão da privacidade, notadamente mediante especulação e exposição da vida de pessoas socialmente relevantes[15].

---

[9] PINHEIRO, Alexandre Sousa. *Op. Cit.* p. 448.
[10] PINTO, Paulo Mota. *Op. Cit.* p. 505.
[11] PINTO, Paulo Mota. *Op. Cit.* p. 507.
[12] PINTO, Paulo Mota. *Op. Cit.* p. 508.
[13] WARREN, Samuel D. e BRANDEIS, Louis D. *The Right To Privacy*. Harvard Law Review, Vol. IV, N. 5, 1890, p. 193-220.
[14] PINHEIRO, Alexandre Sousa. *Op. Cit.* Pp. 276-278.
[15] Paulo Mota Pinto descreve as razões pelas quais os problemas relacionados à privacidade foram objeto de preocupação na sociedade americana: a agressividade da imprensa, o abismo tecnológico entre a realidade americana e a dos demais países e, ainda, os valores fundamentais daquela sociedade, mormente a especial relevância da defesa do indivíduo. PINTO, Paulo Mota. *Op. Cit.* p. 512

É nesse contexto que Warren e Brandeis traçam uma interpretação de precedentes da *common law* com o objetivo de apresentar como ilícito civil (*tort)* a conduta de entidade privadas (imprensa) ao expor fatos da vida privada de alguém ou fotografias não autorizadas. Assim, a *privacy* americana, como um direito, foi construída pelos autores a partir do *right to be let alone*, extraindo dele uma interpretação condizente com o novo contexto social e estendendo seu conteúdo de modo a permitir a proteção dos indivíduos frente às invasões da imprensa. A partir daí, o *right to privacy* passou a ser reconhecido pela jurisprudência e consagrado nas leis, com contornos conceituais amplos, inclusive fundamentando decisão da Suprema Corte, em 1965, sobre a possibilidade de proibir o uso de contraceptivos (caso *Griswold* contra *Connecticut*)[16].

A ampla abrangência da *privacy* americana permitiu, portanto, que o direito à privacidade servisse de fundamento tanto para a restringir as formas de tornar pública uma informação pessoal (*informational privacy*), quanto para garantir a liberdade do indivíduo de conduzir sua própria vida, por meio de atos autodeterminados de conteúdo social, cultural, ético ou moral (*decisional privacy*)[17]. Por isso, o *right to privacy* nos Estados Unidos inspirou ao mesmo tempo o *Privacy Act* (lei federal com o fim de proteger o controlo da informação contra atos de entidades públicas) e decisões judiciais sobre os mais variados assuntos, como a inconstitucionalidade de leis que proíbem o aborto, a permissão do "direito a morrer" e a permissão do uso de cabelos compridos por certos profissionais[18].

Já na Europa, o direito à privacidade se desenvolveu a partir do reconhecimento dos direitos da personalidade, cuja proteção jurídica autônoma remonta ao século XIX[19]. Partiu-se, portanto, da premissa de conceber a pessoa humana como titular de uma série de direitos protetores dos bens da personalidade. A origem dessa proteção, todavia, é, como dissemos, atribuída ao Direito Romano, que já previa salvaguardas à honra, à reputação e à dignidade, bens que permaneceram sob proteção em boa parte dos países europeus durante os séculos XVIII e XIX[20]. Tais bens, inerentes a toda pessoa e essenciais ao livre desenvolvimento da

[16] PINTO, Paulo Mota. *Op. Cit*. p. 513.
[17] PINHEIRO, Alexandre Sousa. *Op. Cit.* pp. 365/366.
[18] PINTO, Paulo Mota. *Op. Cit*. p. 514.
[19] PINTO, Paulo Mota. *Op. Cit*. p. 478.
[20] ONDREASOVA, Eva. *Personality Rights in Different European Legal Systems: Privacy, Dignity, Honour and Reputation*. Em OLIPHANT, Ken; PINGHUA, Zhang; e LEI, Chen. The Legal Protection of ersonality Rights: Chinese and European perspectives. Leiden. Brill, 2018. p. 27

personalidade, comporiam uma espécie de patrimônio imaterial e dentre eles estariam, por exemplo, o direito à imagem e o direito à vida privada[21].

Com marco jurisprudencial europeu, Pinheiro[22] cita as decisões francesas do "Tribunal Civil de la Seine", ambas em proteção ao *droit à la vie privée*, uma que "*proibiu a exibição pública de uma quadro que representava a Madre Superior das Irmãs de Providência*", em 1855, e a outra que tratou da "*publicação de imagens (desenhos e pinturas) ilustrando a atriz Rachel Félix no seu leito de morte"*, em 1858.

Mas foi principalmente após a Segunda Guerra Mundial, com o fenômeno da "despatrimonialização do Direito Civil[23], que as demandas impostas pelas circunstâncias fáticas[24] impulsionaram a proteção legal aos direitos da personalidade, sobretudo na Alemanha, onde, em 1954, a jurisprudência construiu o "direito geral de personalidade", a partir da interpretação conjunta do §823, n.º 1.º do BGB e da dignidade da pessoa humana (art. 2.º, n.º 1.º, da Lei Fundamental da República da Alemanha de 1949) (caso *Lesebrief*)[25], para concluir pela impossibilidade de publicação de notas pessoais sem o consentimento de autor vivo.

A proteção da personalidade por meio de um direito geral a englobar todos os aspectos da personalidade constituiu um sistema adotado não só pela Alemanha, mas também por outros países europeus com Itália e Áustria. A vantagem apontada para o sistema reside na sua abrangência, que permite o desenvolvimento do direito de acordo com as mudanças tecnológicas e sociais. Todavia, há críticas ao modelo, notadamente ante à dificuldade de se estabelecer os contornos do instituto e à insegurança jurídica daí decorrente[26].

Por outro lado, países com a França optaram pela proteção aos diversos direitos da personalidade separadamente, inclusive o direito à privacidade, ambos expressamente incluídos no Código Civil francês em 17 de Julho de 1970[27]. O modelo, também adotado por países com Suécia e Reino Unido, embora permita uma melhor diferenciação entre as diferentes facetas

---

[21] PINHEIRO, Alexandre Sousa. *Op. Cit.* pp. 432 e ss.
[22] PINHEIRO, Alexandre Sousa. *Op. Cit.* p. 436.
[23] BIONI, Bruno Ricardo. *Op. Cit.* p. 55.
[24] Nesse tocante, não apenas o cenário pós-guerra e derrota nazista, mas o desenvolvimento tecnológico, com a invenção do computador e a democratização da fotografia e da imprensa, tudo contribuindo para a transformação da pensonalidade como um bem economicamento valioso, conforme descrição de PINHEIRO, Alexandre Sousa. *Op. Cit.* p. 435.
[25] PINHEIRO, Alexandre Sousa. *Op. Cit.* p. 438.
[26] ONDREASOVA, Eva. *Op. Cit*. p. 49.
[27] ONDREASOVA, Eva. *Op. Cit*. p. 34.

dos direitos da personalidade, na prática pode resultar na existência de lacunas e contradição entre valores[28].

Em Portugal, o artigo 70.º, n. 1.º, do Código Civil de 1966 representa salvaguarda aos direitos da personalidade, através de uma cláusula geral, a fim de proteger os indivíduos *contra qualquer ofensa ilícita ou ameaça de ofensa à sua personalidade física ou moral*. O dispositivo serve como espécie de "direito-quadro" a abranger bens da personalidade não tipificados, do modo "aberto" sincrónica e diacronicamente[29]. Além disso, o Código Civil português também prevê a proteção de direitos da personalidade específicos, como o direito sobre o conteúdo de cartas-missivas e outros escritos (artigos 75.º a 78.º), o direito à imagem (artigo 79.º) e o direito à reserva sobre a intimidade da vida privada (artigo 80.º)[30].

Alerta Orlando de Carvalho, contudo, que o direito geral da personalidade não deve ser confundido com uma mera ferramenta para superação das lacunas deixadas pela previsão dos direitos de personalidades especiais, tampouco como a condensação desses direitos em um único dispositivo. Deve servir, assim, o direito geral da personalidade como fundamento axiológico para as demais disposições legais, como referencial interpretativo portanto[31].

Em relação ao direito à privacidade propriamente dito, importa destacar sua proteção específica prevista na Convenção Europeia dos Direitos do Homem (artigo 8.º), de 1950, bem como nos Códigos Civis de França e de Portugal[32]. Em Portugal, como também em Espanha, há ainda proteção constitucional ao direito à privacidade, nomeadamente no artigo 26.º[33].

Em geral, a proteção à privacidade abrange a defesa da esfera privada e da intimidade, principalmente em assuntos relacionados à saúde, sexualidade e vida familiar. Em alguns casos também incluída nesse rol a proteção ao anonimato[34]. Em Portugal, especificamente, o Código Civil preferiu o uso da expressão "intimidade da vida privada", representando, por si, um recorte ao amplo direito à privacidade[35]. Para Mota Pinto, a dicção legal resulta na exclusão

---

[28] ONDREASOVA, Eva. *Op. Cit*. p. 50.
[29] PINTO, Paulo Mota. *Op. Cit*. p. 493/494.
[30] PINTO, Paulo Mota. *Op. Cit*. p. 498.
[31] CARVALHO, Orlando de. *Teoria Geral do Direito Civil.* 3ª ed.Coimbra. Coimbra Editora, 2012. p. 263.
[32] ONDREASOVA, Eva. *Op. Cit*. p. 57.
[33] PINTO, Paulo Mota. *Op. Cit*. p. 521.
[34] ONDREASOVA, Eva. *Op. Cit*. p. 61/62.
[35] GUIMARÃES, Maria Raquel e REDINHA, Maria Regina. *Through the Keyhole: Privacy in COVID-19 Times - A Portuguese Approach*. Intersentia Online. 2020. Disponível em https://www.intersentiaonline.com/publication/coronavirus-and-the-law-in-europe/2 [Consulta em Agosto de 2021]

não só dos eventos próprios da "vida pública" de alguém, mas também de aspectos da vida privada não íntimos, por exemplo, os segredos dos negócios[36].

Para estabelecer a fronteira entre a vida pública e a privada do indivíduo, deve-se recorrer a critérios que se tornarão mais ou menos eficientes a depender do contexto em que são aplicados[37]. Por exemplo, o critério espacial pode-se mostrar eficiente para garantir a proteção de informações próprias do ambiente doméstico, sendo certo, contudo, que alguns eventos privados poderão ter lugar em ambientes públicos. Por outro lado, a tecnologia permitiu um maior acesso a esses ambientes íntimos objeto de reserva, seja pela variabilidade de novas ferramentas a permitirem a intrusão de terceiros, seja pela possibilidade de o próprio indivíduo divulgar publicamente informações íntimas.

Assim, vê-se que apesar de a proteção da privacidade não estar necessariamente ligada à tecnologia, o desenvolvimento tecnológico tornou ainda mais premente a necessidade de proteção legal da privacidade, pois hoje existem meios consideravelmente mais eficazes de violação da intimidade, sobretudo quando consideramos a penetrabilidade de sensores, microfones e câmeras, objetos atualmente omnipresentes[38]. Logo, hoje o contexto tecnológico é preponderante para definir os contornos do conceito de privacidade, de modo que, sem considerá-lo, a proteção legal não conseguirá responder às demandas atuais nem adaptar-se às novas ameaças.

1.2 O direito à proteção dos dados pessoais

Apesar de os contornos conceituais e doutrinários da proteção de dados já estarem fixados desde antes – com a evolução do conceito de privacidade e o reconhecimento da necessidade de se proteger a individualidade e controlar o acesso e a divulgação de informações pessoais – foram os avanços tecnológicos da segunda metade do século passado e a capacidade de tratamento de dados em escala inédita, com possibilidade de cruzamento de informações de origens diversas, que elevaram a importância do tema[39] a ponto de ser considerado urgente algum tipo de regulamentação específica, desmembrada da genérica proteção da privacidade.

---

[36] PINTO, Paulo Mota. *Op. Cit*. p. 532.
[37] O contexto nesse caso deve ser avaliado não só considerando cada indivúduo caso a caso, mas também em função das valorações de cada formação social, conforme ensina PINTO, Paulo Mota. *Op. Cit*. p. 528.
[38] PINTO, Paulo Mota. *Op. Cit.* p. 511.
[39] TOMÉ, Herminia Campuzano. *Vida Privada y Datos Personales: Su Protección Jurídica Frente a La Sociedad de la Información.* Tecnos. Madrid, 2000. p. 71.

Para Mafalda Barbosa, a popularização do uso da informática resultou na democratização do risco antes existente em relação aos poderes públicos, em razão da concentração de informações em poder do Estado. Hoje, a utilização de modernos sistemas de informação e a possibilidade de compartilhamento de dados entre eles permite a qualquer particular a articulação de diversas informações acerca de um mesmo indivíduo, o que aprofundou a necessidade de regulação específica do acesso, tratamento e transmissão dos dados pessoais[40].

Sobre o assunto, destaca-se a categorização das normas de proteção de dados em *quatro gerações,* a depender do seu escopo: proteção do indivíduo contra o processamento massivo de dados pelos Estado (*primeira geração)*, ampliação da proteção também em relação a bancos de dados não estatais (*segunda geração*), deslocamento do papel de protagonismo do Estado para o indivíduo através do consentimento (*terceira geração*) e a articulação entre o protagonismo do consentimento do titular com a aplicação das leis por autoridades independentes[41].

Nos Estados Unidos, o termo *privacy* já foi concebido, com vimos, com amplo escopo. Extraído a partir do *right to be let alone*, a proteção da privacidade serviu de fundamento para decisões jurisprudenciais tanto relacionadas à *informacional privacy*, quanto à *decisional privacy*, de modo que o direito da proteção dos dados se confunde com a própria tutela da privacidade.

Na Europa, por outro lado, conforme descreve Bioni, o conceito de privacidade teria se alargado de modo a abarcar, para além de sua faceta estática, uma feição dinâmica correspondente à proteção dos dados pessoais e sua prerrogativa de controlo das informações pelo titular (autodeterminação informativa)[42]. Porém, o autor defende que isso não significa dizer que o direito à proteção de dados pessoais deve ser reduzido a uma mera evolução do direito à privacidade, pois ele possui autonomia própria. Prova disso é que o direito à proteção de dados rompe com a dicotomia entre o público e o privado, passando o bem jurídico a estar associado ao conceito de dado pessoal[43]. Para o autor, o direito à proteção de dados pode ser

---

[40] BARBOSA, Mafalda Miranda. P*roteção de dados e direitos de personalidade: uma relação de interioridade constitutiva. Os beneficiários da proteção e a responsabilidade civil*. Estudos de Direito do consumidor, N.º 12, Coimbra, Centro de Direito do Consumo/FDUC, 2017. p. 77.

[41] BIONI, Bruno Ricardo. *Op. Cit.* pp. 115-117.

[42] BIONI, Bruno Ricardo. *Op. Cit.* pp. 93 e ss. Para o autor, o conceito tradicional de privacidade possui característica estática, pois define *a priori* quais fatos estão ou não incluídos na esfera privada do indivíduo. Por outro lado, a proteção de dados representaria uma perspectiva dinâmica de privacidade ao passo que entrega ao indivíduo a liberdade positiva de controlar suas próprias informações.

[43] BIONI, Bruno Ricardo. *Op. Cit.* pp. 97/98.

inserido no rol dos direitos à personalidade, pois os dados pessoais constituem uma projeção da pessoa humana[44].

Já Barreto Menezes Cordeiro, sem negar importância dos direitos da personalidade como fundamento para o direito da proteção de dados, ensina que esse novo direito vai além de simplesmente proteger os interesses dos titulares, estabelecendo os critérios essenciais para garantir a livre circulação dos dados pessoais[45].

Em termos de regulamentação própria, o marco inicial do Direito da proteção de dados é considerado a criação, pelo Congresso dos Estados Unidos da América, do *Special Subcommittee on Ivasion of Privacy*, em 1965[46]. O *Special Subcommittee* realizou uma série de audiências tendo, primeiramente, o foco de investigar supostas prática violadoras da *privacy* por agências federais. Mas a partir de 1968, os trabalhos voltaram-se também a entidades privadas, notadamente agências de crédito, responsáveis à época pela elaboração de verdadeiros dossiês que descreviam o perfil de cada cliente.

Sobre o assunto, ensina Barreto Menezes Cordeiro ter a preocupação, na época, emergido do fato de esses relatórios individuais conterem, muitas vezes, informações incorretas, irrelevantes e viciadas ou, ainda, invadirem desarrazoadamente a esfera pessoal e secreta. Além disso, os dossiês elaborados pelas agências de crédito impactavam de modo substancial a vida dos titulares dos dados por determinarem o seu acesso ao crédito, por exemplo, e até mesmo influenciarem na contratação de um seguro ou na seleção para ocupar um posto de trabalho. A desenvolvimento da Sociedade de Consumo, com a procura maciça por crédito, levou a uma generalização dessa prática e tornou ainda mais urgente a necessidade de regulamentação específica[47]. Os resultados legislativos do *Special Subcommittee* vieram mais tarde com a aprovação do *Fair Credit Reporting Act* (1970)[48] e o *Privacy Act* (1974)[49].

---

[44] BIONI, Bruno Ricardo. *Op. Cit.* pp. 63-65.

[45] CORDEIRO, António Barreto Menezes. *Op. Cit.* p. 33.

[46] CORDEIRO, António Barreto Menezes. *Op. Cit.* p. 53.

[47] Para ilustrar esse cenário, o Professor faz referência às palavras de Hillel Black, escritas em 1961: "*If your name is not in the records of at least one credit bureau, it doesn´t mean you don´t rate. What means is that you are either twenty-one or dead*". CORDEIRO, António Barreto Menezes. *Op. Cit.* pp. 56/57.

[48] Tinha por escopo proteger o particular contra a coleta de informações incorretas, estabelecer poderes de fiscalização ao *Federal Trade Commission (FTC)* e impor responsabilidades a quem desenvolve esta atividade. Em resumo, "*para assegurar que agências exerçam suas sérias responsabilidades com justiça, imparcialidade, e respeito pelo direito do consumidor à sua privacidade*", conform dicção do §602 do *Fair Credit Reporting Act* em tradução livre.

[49] Regula o tratamento de dados no âmbito dos órgãos governamentais, tendo o intuito de estabelecer salvaguardas ao cidadão contra a invasão de privacidade por agências federais.

Para Barreto Menezes Cordeiro, o *Privacy Act* estabelece um conjunto de princípios que hoje representam o núcleo do Direito da proteção de dados[50]. De fato, do documento é possível extrair o protagonismo do titular de dados em relação à atividade de tratamento, sobretudo por estabelecer seu direito de acesso a quais dados seus estão sendo tratados e com quais finalidades, bem como deveres das agências federais como o de restringir a atividade de tratamento de dados pessoais a propósitos necessários e legais, respeitada a finalidade, garantida a atualidade da informação e evitado o seu mau uso (em tradução livre do texto normativo "*misuse"*).

No que toca ao Direito estado-unidense é o que importa aos propósitos do presente trabalho destacar, sendo digno de menção entretanto que diversos outros diplomas foram aprovados desde então com impacto na temática de proteção dos dados com aplicações limitadas a certo estado daquela Federação ou a certos setores tais como *Family Educational Rights and Privacy Act* (1978), *Right to Finantioal Privacy* (1978)*, Privacy Protection Act* (1980), *The Electronic Communications Privacy Act* (1986).

Já na Europa, os primeiros traços partem da jurisprudência alemã, onde cunhou-se pela primeira vez o termo *Datenschutz* (proteção dos dados em tradução livre para o português). Note-se que dadas as diferenças de evolução do conceito nos diferentes ordenamentos jurídicos, a proteção de dados europeia não corresponde exatamente à *privacy* americana, embora sejam comumente tratadas como sinônimo. Conforme ensinamentos de Pinheiro, a *Datenschutz* pode ser correlacionada, em linha gerais, com a *informational privacy*, mas essa correlação não exacta, até pelo fato de a proteção de dados europeia abranger certos interesses não resguardados pelo direito estado-unidense, razão pela qual a Europa não reconhece como *adequada* a proteção garantida pelos americanos[51].

A decisão partiu da análise da constitucionalidade da Lei dos Censos de 1983. Segundo a lei alemã, todos os cidadãos consentiriam na coleta de dados pessoais para fins estatísticos, sendo previsto também, de forma genérica e sem especificar a finalidade, o cruzamento desses dados com outros contidos em bancos de dados públicos na execução de atividades administrativas. A partir do art. 2.º, n.º 1, (livre desenvolvimento da personalidade) e o art. 1.º, n.º 1 (dignidade da pessoa humana), ambos da Constituição Alemã, e decidiu-se pela existência

[50] CORDEIRO, António Barreto Menezes. *Op. Cit.* p. 59.
[51]PINHEIRO, Alexandre Sousa. *Op. Cit*. pp. 428/429.

do direito do indivíduo de ser protegido contra "*a recolha, armazenamento, uso e transmissão ilimitados de dados pessoais"*[52].

Para Pinheiro, a fundamentação do julgado alemão, que ainda não tratava expressamente de autodeterminação informativa, é paradigmática justamente por dissociar o direito à privacidade e o direito à proteção de dados e não resumir esse último a uma mera evolução do primeiro, justificando a importância em não confundir esse conceito com o da *privacy* no contexto americano[53]. Ademais, a importância da Decisão dos Censos vai além da construção do princípio da especificação dos propósitos, pois também rompe com a ideia do protagonismo do consentimento com meio de legitimação do tratamento de dados, mormente a posição de assimetria do cidadão frente ao Estado[54].

Essa independência do direito à proteção de dados em relação ao direito à privacidade tem uma relevância indiscutível para o desenvolvimento do tema até os patamares regulatórios atuais. Primeiro por servir de base à conclusão de que o simples consentimento não pode ter o condão de justificar todo e qualquer tratamento, sob pena de transformar a pessoa em "*objeto a ser ilimitadamente explorado*"[55]. Segundo por ampliar o alcance dessa proteção[56].

1.3 A proteção jurídica dos dados pessoais

Os mais variados meios de produção adotados pelas sociedades ao longo da história sempre impactaram no valor de determinados bens e, por consequência, no grau de proteção jurídica direcionadas aos bens considerados pilares da estrutura econômico-social. Foi assim com as terras, no período eminentemente agrícola; com os parques industriais (seja de fabricação de bens, seja de produção de energia), no período da primeira revolução industrial; com os estabelecimentos comerciais, na sociedade pós-industrial.

Por sua vez, o aprofundamento da complexidade da teia social, atrelado ao desenvolvimento de novas tecnologias – de modo veloz e irreversível – trouxe-nos até o momento presente: o da era da informação, na qual tem mais poder quem detém "os dados".

---

[52] PINHEIRO, Alexandre Sousa. *Op. Cit.* p. 479.
[53] PINHEIRO, Alexandre Sousa. *Op. Cit.* p. 487.
[54] BIONI, Bruno Ricardo. *Op. Cit.* pp. 104/106.
[55] BIONI, Bruno Ricardo. *Op. Cit.* p. 106.
[56] A título de comparação, Bioni remete a uma decisão anterior do mesmo tribunal alemão em relação à Lei do Microcenso de 1957 a qual centrou-se na fundamentação de que, em aplicação ao direito à privacidade, a coleta de dados para ser considerada ilegítima deveria violar a esfera íntima do cidadão. BIONI, Bruno Ricardo. *Op. Cit*. p. 106.

Nesse contexto, houve um aumento exponencial da atividade de coleta de dados e, para o mercado, os bancos de dados passaram a ser considerados ativos cada vez mais valiosos[57]. Assim como nos períodos históricos anteriores em relação aos respectivos "bens-pilares", o arcabouço normativo referente aos dados assume especial significado, pois, para além de regular o acesso a um bem jurídico economicamente relevante, passa a representar a proteção mesma do indivíduo, da sua vida e da sua liberdade[58].

No que toca especificamente aos dados pessoais, a sua proteção no direito português remonta ao legislador constitucional de 1976, que já lhe garantiu proteção (art. 35.º), ainda que remetendo a definição de "dados pessoais" à legislação ordinária[59]. A previsão representa a autonomia do direito da proteção de dados em relação à proteção da intimidade da vida privada, consagrada no art. 26.º da Constituição Portuguesa. Ainda, do texto legal extrai-se que proteção dos dados pessoais vai além daquelas informações relativas à vida privada, em relação às quais há especiais exigências (art. 35.º/3)[60]. Ainda que de forma embrionária, se comparada com a sistematização positivada mais tarde pelo RGPD, o art. 35.º da Constituição foi pioneiro ao estabelecer os direitos dos titulares de dados como o *direito de acesso*, o *direito ao não tratamento de dados sensíveis* e o *direito ao sigilo dos dados*[61].

A definição de "dados pessoais" pela legislação infraconstitucional viria apenas em 1991 com a Lei da Protecção de Dados Pessoais face à Informática (Lei n.º 10/91, de 27 de Abril), cujas disposições se aplicavam "*À constituição e manutenção de ficheiros automatizados, de bases de dados e de bancos de dados pessoais*" e "*Aos suportes informáticos relativos a pessoas*

---

[57] Seja por exploração direta por meio da publicidade direcionada, seja por constituir importante fonte de informação sobre o consumidor, conforme conclui CORÔA, Marília de Mello e Silva. *O Mercado De Dados: Estrutura, Funcionamento e o Reflexo do RGPD no Novo Mercado à Base De Dados Pessoais.* Dissertação (Mestrado em Ciências Jurídico-civilísticas) Faculdade de Direito da Universidade do Porto. Porto, 2020. p. 51.

[58] A importância que os dados representam para Era Digital é retratada na expressão "os dados são o novo petróleo", conforme ensina CORDEIRO, António de Menezes. *Op. Cit.* p. 29.

[59] A redação original do Artigo 35.º contava com apenas três números, um referente ao direito do cidadão de "*de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a rectificação dos dados e a sua actualização"* (n.º 1) e os outros dois referentes às proibições de tratamento de dados relativos à convicções políticas, fé religiosa ou vida privada (n.º 2) e de atriubuição de número nacional único aos cidadãos (n.º 3). Apenas após as revisões constitucionais de 1982, 1989 e 1997 o texto constitucional alcança a atual redação, conforme detalha SARMENTO E CASTRO, Catarina. *40 anos de "Utilização da Informática" - O artigo 35.º da Constituição da República Portuguesa*. Revista e-Pública, Vol. 3, N.º 3, 2016. pp 46/49 Disponível em https://www.e-publica.pt/volumes/v3n3a04.html [Consulta em Agosto de 2021]

[60] SARMENTO E CASTRO, Catarina. *Op. Cit.* pp. 50.

[61] DIAS, Carlos André Ferreira. *A Privacidade na era da Internet das Coisas: direiros de personalidades e proteção de dados.* Dissertação (Mestrado em Ciências Jurídico-civilísticas) Faculdade de Direito da Universidade do Porto. Porto, 2019. p. 12.

colectivas e entidades equiparadas, sempre que contiverem dados pessoais"[62]. Essa primeira legislação teve vigência até 1998, quando foi revogada pela Lei n.º 67/98, de 26 de Outubro, responsável pela transposição da Diretiva 95/46/CE[63].

Já no direito europeu, o marco legislativo relativo a proteção dos dados pessoais é associado à Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares, de 28 de janeiro de 1981, primeiro instrumento internacional juridicamente vinculativo[64] adotado sobre a matéria, "*(...) resultado do movimento promovido pela OCDE para facilitar a harmonização das legislações de proteção dados pessoais.*"[65]. A importância do tema consagrou-se, posteriormente, com sua inclusão na Carta dos Direitos Fundamentais da União Europeia (artigo 8.º)[66] e no Tratado sobre o Funcionamento da União Europeia (artigo 16.º)[67].

De forma sistematizada, outrossim, a matéria foi tratada pela primeira vez pela Diretiva 95/46/CE, transposta em Portugal pela Lei n.º 67/98, em vigor até ser revogada pelo Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, ou Regulamento Geral de Proteção de Dados (RGPD), que representa a concretização da relevância reconhecida à proteção dos dados, não só em uma perspectiva econômica (reforço da confiança para o consumo digital e da competitividade das empresas com postura responsável em relação às políticas de privacidade), mas também de proteção dos direitos de personalidade, sobretudo à privacidade.

---

[62] Art. 3.º, n.º 1, da Lei n.º 10/91.

[63] BARBOSA, Mafalda Miranda. *Op. Cit.* pp. 75-131..

[64]Fichas técnicas sobre a União Europeia – 2021. Disponível emhttps://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf . [Consulta em Fevereiro de 2021].

[65] BIONI, Bruno Ricardo. *Op. Cit.* p. 122.

[66] Artigo 8.º

Proteção de dados pessoais

1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.

3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

[67] Artigo 16.º (ex-artigo 286.o TCE)

1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes. As normas adotadas com base no presente artigo não prejudicam as normas específicas previstas no artigo 39.o do Tratado da União Europeia.

Sobre o assunto, Barreto Menezes Cordeiro ressalta o impacto do Direito da proteção de dados na vida quotidiana provocado pelos avanços tecnológicos significativo das últimas décadas e a posição de fragilidade do indivíduo frente aos mais variados responsáveis pelo tratamento, público ou privados. Essas entidades, impulsionadas pelas necessidades atreladas ao tratamento automatizado de dados, vêm acumulando uma grande quantidade de informações a ponto de superar o conhecimento que o próprio indivíduo detém sobre ele mesmo. O RGPD surge, assim, em resposta a essa realidade já existente, colocando os dados pessoais e seu tratamento no centro do debate jurídico e empresarial[68].

No contexto do RGPD, a proteção de dados pessoais ostenta *dupla função* por garantir a privacidade e os direitos fundamentais do titular e ao mesmo tempo impor a regras de modo a não obstar ao desenvolvimento econômico[69], o que fica evidenciado já nos primeiros considerando do Regulamento como os de número 1 (proteção de dados como direito fundamental), número 2 (introduz o mister económico do Regulamento não desconectado do foco no bem-estar das pessoas) e número 6 (referência ao impacto tecnológico).

2. *IoT*: noção e enquadramento jurídico

2.1 O que é *IoT*?

O termo *Internet of Things* (ou, em português, Internet das Coisas), doravante *IoT*, é utilizado hoje para referenciar dispositivos com a característica de serem interconectáveis de modo a tornar possível a criação de uma rede formada por "coisas" de naturezas diversas.

Nos primórdios, a internet foi concebida como uma rede entre computadores, fazendo emergir uma nova realidade em que conviviam, paralelamente, dois mundos: o mundo real, onde viviam as pessoas a manipular os mais diversos objetos e equipamentos, e o mundo virtual, formado por computadores ligados entre si. A internet, assim, para "interagir" ou "espelhar" o mundo real, dependia da intervenção humana para coletar dados do mundo real e processá-los com uma finalidade específica.

Já nessa época inicial do desenvolvimento da *internet* se falava da possibilidade da conexão *device-to-device* (D2D), mas foi apenas em 1999 que o termo *Internet of Things* foi criado por

[68] CORDEIRO, António de Menezes. *Op. Cit.* p. 29.
[69] BIONI, Bruno Ricardo. *Op. Cit.* p. 108.

Kekin Ashton por ocasião de uma palestra para a Procter & Gamble[70]. Como precursores desse tipo de tecnologia, são citados diversos autores cujo trabalho consistia em estudar a possibilidade de se interconectar dispositivos capazes de interagir entre si sem intervenção humana. Dentre todos, destacamos Mark Wiser, autor do artigo intitulado "*The computer for the 21ts Century*"[71], no qual cunhou o termo "computação ubíqua" para designar a conexão entre dispositivos de forma "invisível" às pessoas[72]; e Neil Greenfield, ante a publicação, em Janeiro de 1999, do seu livro "*When the Things Start to Think"*.

Já a criação do primeiro dispositivo considerado como *IoT device* é creditado a John Romkey, responsável pela criação de uma torradeira ligada à internet (rede TCP-IP) e controlável através de um computador[73].

Não há, no âmbito europeu uma definição legal para Internet das Coisas, mas há na literatura especializada diversos conceitos propostos[74], sempre mencionando a conectividade entre objetos dos mais variados, por meio de protocolos de comunicação[75]. Para além da característica de interconectividade (D2D), o desenvolvimento tecnológico acrescentou ao mundo da *IoT* outras funcionalidades que potencializaram sua eficiência tais como a conectividade *wireless* (*Bluethooth, wi-fi,* identificação por radiofrequência RFID), a

---

[70] ASHTON, Kevin. *That 'Internet of Things' Thing*. RFID Journal. 22 de Junho.2009. Disponível em https://www.rfidjournal.com/that-internet-of-things-thing [Consulta em Fevereiro de 2021]

[71] WISER, Mark. *The computer for the 21ts Century*. Scientific American, Vol. 265, N.º 3, 1991.

[72] PEPPET. Scott R. *Freedom of Contract in Augmented Reality*. Em Research Handbook on the Law of Virtual and Augmented Reality. Edward Elgar. Chelteham, 2020. p. 609.

[73] O dispositivo, depois melhorado para incorporar um robô responsável por introduzir o pão, foi apresentado na Interop 89' Conference com a inovação de ser 100% automatizado por funcionar sem qualquer interação humana.

[74] Por exemplo, para Ken Goldstein , "*IoT is the concept for connecting a device to the Internet and other connected devices*." GOLDSTEIN, Ken. *Cyber Beware: Iot Technology Growing Explosively*. International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel, 2019, Vol. 3, Nº 6. p. 8. Disponível em https://heinonline.org/HOL/P?h=hein.journals/idpp3&i=131 [Consulta em Agosto de 2021]. Já para Noto La Diega, *IoT* "*entails any physical entity capable of connectivity that directly interfaces the physical world, such as embeddes devices, sensors and actuators*". LA DIEGA, Guido Noto. *Internet of things and patents: Towards the iot patent wars.* Journal of Commercial and Intellectual Property Law, 2017, Vol. 3, nº. 2. p. 48. Disponível em https://heinonline.org/HOL/Page?handle=hein.journals/tfm2017&id=223&collection=journals&index= [Consulta em Agosto de 2021]. Elvy, vai além da conectivividade e menciona *"a network of products, systems and platforms connected through enable devices that collect, store and communicate with other devices, cloud software, on-site infrastructure, and individuals to maximize efficiency*". ELVY, Stacy-Ann. *Contracting in the age of the internet of things: article of the ucc and beyond.* Hofstra Law Review, 2016, Vol. 44, nº 3. p. 840. Disponível em https://heinonline.org/HOL/Page?public=true&handle=hein.journals/hoflr44&div=40&start_page=839&collection=journals&set_as_cursor=0&men_tab=srchresults [Consulta em Agosto de 2021]

[75] CAPISIZU, Larisa-Antonia. *Legal Perspectives on the Internet of Things*. Conferinta Internationala de Drept, Studii Europene si Relatii Internationale. Maio de 2018. p.524. Disponível em https://heinonline.org/HOL/Page?public=true&handle=hein.journals/cidstue2018&div=55&start_page=523&collection=journals&set_as_cursor=0&men_tab=srchresults [Consulta em Agosto de 2021]

inteligência artificial (sobretudo com a introdução do *machine learning)* e a coleta de dados sem intervenção humana (através da associação dos dispositivos a sensores)[76].A coleta e tratamento desses dados possibilitam ao dispositivo mapear o comportamento do utilizador de modo a proporcionar uma experiência inteiramente personalizada.

Tais características da tecnologia *IoT* torna-a penetrável em todos os ambientes e aspetos da vida cotidiana, já que os chamados dispositivos inteligentes (*smart device*) tomam as mais diversas formas, desde automação doméstica (domótica), passando por roupas e acessórios (*wearables),* brinquedos (*smart toys*), até grandes máquinas industriais, cidades inteligentes (*smart cities*) e equipamentos de mobilidade (*smart cars*). Concretizado, assim, o caráter da ubiquidade computacional previsto Mark Wiser no início da década de 1990.

A partir de então, a realidade do mundo assume um formato no qual o ambiente físico se confunde com o digital[77]. Agora, não é mais necessária a intervenção humana para fornecer dados da realidade física para os computadores, pois os diversos dispositivos do nosso dia-a-dia são dotados de sensores e coletam esses dados automaticamente, bem como compartilham esses dados com outros dispositivos, possibilitando o cruzamento de informação e a confecção de perfis comportamentais cada vez mais precisos.

Por esse motivo, não teria sido possível o desenvolvimento da *IoT* não fosse a realidade do *Big Data*[78]. A revolução do *Big Data* tornou-se possível em razão, dentre outros fatores, da redução do preço do silicone, do barateamento das tecnologias de conectividade e do *Cloud Computing*, essencial para ao aumento da capacidade de armazenamento. Conforme ensina Ugo Pagallo, Massimo Durante, e Shara Monteleone[79] a *computação em nuvem* condensou em si as

---

[76] Nos dias atuais, a torradeira de Romkey, para além de ser acionável por um comando de computador ou *smartphone* a ela conectados através de rede sem fio, poderia ser interligada aos dados da agenda eletrônica de seu usuário e iniciar a operação de modo sincronizado ao horário do alarme que o desperta. Ainda, a torradeira seria capaz de guardar informações acerca do comportamento do utilizador, como a hora em que ele efetivamente recolhe a torrada para consumo e em que situações ele precisa reaquecer o alimento por ter, por exemplo, sido preparado demasiado cedo.

[77] Ilustra essa nova realidade o *slogan* difundido por executivos da Google segundo o qual agora "*We don´t go online. We live online*" em referência ao contraste entre o mundo cibernético atual, no qual vivemos hiperconectados, e aquele experimentado outrora, quando selecionávamos momentos do dia para "acessar" a internet.

[78] A definição primeira de *Big Data* é atribuído a Doug Laney que inaugurou a famosa referência aos 3V's relativos ao volume de dados, velocidade de processamento e variedade de análises. Mais tarde foram acrescentados mais dois V´s referentes a veracidade e valor, conforme narra PAGALLO, Ugo. *The legal challenges of big data: Putting secondary rules first in the field of eu data protection.* European Data Protection Law Review (EDPL), 2017. Vol. 3. N.º. 1. p. 36.

[79] PAGALLO, Ugo; MASSIMO, Durante; e MONTELEONE, Shara. *Whats is New with the Internet of Things in Privacy and Data Protection? For Legal Chalenges on Sharing and Control in IoT*. Em LEENES, Ronald, *et al*.

vantagens do fácil acesso com o armazenamento extenso e barato, características potencializadas pela conexão 5G, as interconexões via radio e outras redes invisíveis e a ubiquidade da telefonia móvel

Tamanha facilidade não viria sem ônus. Hoje, é crescente o debate acerca da banalização dos dispositivos hiperconectados com benefícios questionáveis, fazendo surgir o termo *internet das coisas inúteis.* Sobre isso, ensina Magrani[80] que o barateamento e popularização dessa tecnologia permitiu a associação da avançada tecnologia a objetos triviais, sem utilidade proporcional. Assim, sob a promessa de facilitar a vida, a tecnologia pode influir apenas para complicar o uso e encarecer o produto sem contrapartida significativa[81].

A ameaça potencial da *IoT* que mais interessa ao presente trabalho, todavia, relaciona-se com os perigos envolvendo a segurança da informação e a proteção de dados. Isso porque, cada dispositivo, por mais simples ou pouco útil, representa uma porta de coleta dados, dados esses que serão somados às inúmeras informações coletadas pelos diversos dispositivos conectados a uma mesma rede. Esse volumoso conjunto de dados (*big data*) permitem traçar um perfil cada vez mais preciso do indivíduo, mapeando e prevendo seus hábitos, preferência e escolhas e dando às máquinas – e consequentemente às empresas e pessoas que as controlam – o poder de conhecer o usuário mais do que ele mesmo[82].

A grande preocupação, nesse contexto, é o poder garantido pelas empresas detentoras dos dados e terceiros que compram seus produtos, pois as estratégias de *marketing* crescem exponencialmente em efetividade e tornam-se capazes de manipular silenciosamente as mentes e induzir escolhas de consumo[83]. A propaganda detalhadamente personalizada e com alvo minunciosamente definido deixa de exercer o tradicional efeito meramente persuasivo e passa a funcionar como um controlo da própria vontade individual, dando ensejo a verdadeira

---

Data Protection and Privacy: (In)visibilities and Infrastructures. Cham: Springer, 2017. (Law, governance and technology series). p. 60.

[80] MAGRANI, Eduardo. *A Internet das Coisas.* Rio de janeiro, FGV Editora, 2018. p. 47.

[81] Como exemplo, Magrani cita o produto *egg minder* consistente em uma bandeja com sensor para contabilizar o número de ovos em determinado frigorífico, destacando a preocupação com a sustentabilidade ambiental, pois os dispositivos inúteis possuem a tendência de tornarem-se rapidamente ultrapassados e serem descartados, gerando grande volume de lixo tóxico para o qual não há destinação (*e-waste*). MAGRANI, Eduardo. *Op. Cit.* p. 48.

[82] FRIAS, Hélder. *A Internet de Coisas (IoT) e o Mercado Segurador.* Em FinTech: desafios da tecnologia financeira. coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte. Vol. 1. Almedina. Coimbra, 2017. p. 222.

[83] OLIVEIRA, Madalena Perestrelo de. *Definição de Perfis e Decisões Automatizadas no Regulamento Geral sobre a Proteção de Dados*. Em Em FinTech: desafios da tecnologia financeira. coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte. Vol. 2. Almedina. Coimbra, 2017. pp. 64/65.

"ditadura dos dados"[84]. Para além disso, a rapidez com que esses dispositivos penetraram nossa vida cotidiana e o baixo grau de informação disponível aos usuários resulta em um consumo irrefletido desses produtos, pois os usuários pouco se preocupam com o local e grau de segurança do armazenamento desses dados, ou com a destinação e uso desses dados pela entidade deles detentora.

Sobre o assunto, explica Siegel[85] que a maioria dos consumidores utilizam os dispositivos inteligentes com o objetivo de facilitar e simplificar suas rotinas quotidianas, sem considerarem ou sequer terem conhecimento do grau de segurança desses aparelhos em relação aos seus dados. Para além do risco de invasões de privacidade por meio de *hackers* com o objetivo de controlar o próprio dispositivo (que pode ser desde um simples sensor de presença a um brinquedo inteligente dotado de câmera e poder de interação com a criança), falhas de segurança também podem permitir um ataque *hacker* atraído pela volumosa quantidade de dados coletados. Alerta ainda o autor que, mesmo sendo cada vez mais regulares e frequentes as invasões e os vazamentos de informações, as pessoas parecem não levar a sério os riscos ou, quando os consideram, não sabem como se proteger deles.

Essas preocupações embora se refiram à toda gama de inovações tecnológicas, apresenta-se mais acentuada no caso dos dispositivos *IoT* ante penetrabilidade desse tipo de tecnologia nos aspetos mais íntimos da vida humana. Por exemplo, mesmo se tomarmos como parâmetro o impacto das redes sociais da esfera da privacidade – tendo em conta que o arranjo social estimula que os indivíduos compartilhem com o grande público toda sorte de informações pessoais que obviamente os expõem – esse impacto ainda é consideravelmente menor do que o proveniente da Internet das Coisas.

Em sua maioria, os dados coletados no âmbito das redes sociais são controlados pelos seus usuários ao selecionarem que fotos compartilham, quais dados introduzem em seus perfis e quais pessoas têm acesso àquelas informações. Já no campo da *IoT*, os dispositivos, por exemplo, componentes de uma rede doméstica, estão silenciosamente absorvendo todos os dados daquele núcleo familiar (ubiquidade), desde o número de pessoas, seus hábitos,

---

[84] BIONI, Bruno Ricardo. *Op. Cit.* p. 89-92, para quem "no contexto do *Big Data*, são os algoritmos que passam a orquestrar as dessas pessoas, decidindo a respeito das suas oportunidades."

[85] SIEGEL, Jeremy. *When the Internet of Things Flounders: Looking into GDPR-Esque Security Standards for IoT Devices in the United States from the Consumers' Perspective.* Journal of High Technology Law. 2020, Vol. 20, n.º 1, pp. 190/191. 189-229. Disponível em https://heinonline.org/HOL/Page?handle=hein.journals/jhtl20&id=189&collection=journals&index= [Consulta em Abril de 2020].

conversas, perfil de consumo, preferências musicais e outros aspetos de comportamento dos mais triviais aos mais íntimos.

Um exemplo desse comparativo, envolvendo uma espécie de dados especialmente sensíveis e íntimos, são os casos envolvendo redes sociais de relacionamento. Vazamento de informações coletadas por aplicações como o *Tinder*[86] ou no famoso caso *Ashley Madison*[87] têm o potencial, como é óbvio, de expor os usuários à humilhação pública e à devassa da intimidade. Mas é de se admitir que o grau de detalhe das informações lançadas à plataforma é controlado pelos participantes (escolha de fotos e informações pessoais publicadas ou conteúdo das conversas estabelecidas).

Por outro lado, é inegavelmente mais agressiva a exposição sofrida pelos consumidores no caso, também amplamente divulgado[88], envolvendo o *smart sex toy* manufaturado pela empresa canadiana *We-Vibe*. Nesse caso, consumidores americanos acionaram judicialmente a fabricante de um vibrador, cujo diferencial era o de ser controlável por meio de aplicação no telemóvel. Descobriu-se, entretanto, que o dispositivo coletava, sem consentimento específico, dados pessoais sensíveis dos utilizadores tais como data, duração e configuração de cada utilização, reportando, em tempo real, ao fabricante.

Note-se que, nesses casos, até mesmo as tentativas de anonimização dos dados são por vezes mal sucedidas, pois o volume e qualidade dos dados, mesmo que dissociados de uma identificação nominal, possibilitam a individualização do titular e garantem a reversibilidade do processo de anonimização. Segundo analisa Brasher, a avançada tecnologia da Internet das Coisas permite análises impossíveis em um cenário com quantidade reduzida de dados; a esse fator soma-se a ampla possibilidade de compartilhamento desses dados, de cruzamento de informações colhidas por dispositivos distintos e a coleta de dados sensíveis indistintamente. Tudo isso, resulta não só numa coleta de dados mais intrusiva, mas no aumento do risco de reversão do processo anonimização[89].

---

[86] A aplicação de relacionamento mais famosa do mundo.

[87] *Site* destinado às pessoas que procuram relacionamentos extraconjugais, cujos dados foram vazados em 2015, expondo estimados 33 milhões de usuários, conforme amplamente noticiado pela mídia. Notícia Disponível em https://www.publico.pt/2015/08/21/tecnologia/noticia/portugueses-estao-no-ashley-madison-a-maioria-no-norte-do-pais-1705602, [Consulta em Junho de 2021].

[88] Conforme notícia do *The Guardian* disponível em https://www.theguardian.com/technology/2017/mar/14/we-vibe-vibrator-tracking-users-sexual-habits e no portal português "Sábado", disponível em https://www.sabado.pt/ciencia---saude/detalhe/fabricante-de-vibradores-condenado-por-espiar-utilizadoras [Consulta em Junho de 2020].

[89] BRASHER, Elizabeth A. *Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation*. Columbia Business Law Review, 2018, n.º 1, p. 237. Disponível em

A violação da privacidade dos consumidores, nesse caso, alcançava potencialmente dados de que os titulares sequer tinham controlo ou conhecimento. Mais ainda, mesmo que ao comprar o dispositivo *smart* o indivíduo médio antecipe a ocorrência da coleta e tratamento de dados pessoais, não tem como prever exatamente quais são esses dados e nem o tipo ou finalidade do tratamento, realizado em sua quase totalidade sem interferência humana. Essa é, notadamente, a circunstância que justifica a acentuada preocupação quando se trata de proteção de dados e da privacidade do usuário de dispositivos *IoT* quando comparado a outras modalidades de coleta.

Outro ponto essencial para estabelecermos os contornos do problema, é a penetrabilidade da coleta de dados decorrente do crescimento exponencial, quase generalizado, do uso de *smartphones*. Isso porque, ao contrário dos objetos inteligentes – ao alcance apenas de uma parcela da população –, os *smartphones* representam a evolução dos telemóveis comuns e, por sua vez, dos telefones domésticos, cuja utilização já se encontra há anos sedimentada nos costumes. Por isso, é reduzido o público alheio à revolução do *Big Data*, dando ensejo a um fenômeno nomeado *datificação das vidas*[90].

O fenômeno representa a transformação da vida do indivíduo em um apanhado de dados contendo todas as *nuances* de sua existência, significando não só o seu rastreio virtual (histórico de navegação na internet, por exemplo) mas a sua localização física constante também no mundo *offline* (sociedade da vigilância). A base disso, segundo Solove, está na elaboração de verdadeiros *dossiês digitais* utilizados pelas empresas para descobrir novas formas de fazer negócios, pelo mercado financeiro para determinar a quem aprovará crédito, pelos empregadores para analisar o passado de candidatos a empregos, pelos órgãos governamentais para investigar cidadãos e descobrir roubos e fraudes e outros usos ainda não conhecidos [91].

Esses dossiês electrónicos funcionam, assim, como um prolongamento digital do indivíduo e, para além de sua representação em formato de *bits*, há a classificação e segmentação das pessoas com base em tais informações, em uma atividade denominada *profiling*[92]: prática que agrupa os dados pessoais de um indivíduo de modo a elaborar um relatório a seu respeito a fim de basear a tomada de inúmeras decisões. Tais perfis permitirão a

---

https://heinonline.org/HOL/Page?handle=hein.journals/colb2018&id=215&collection=journals&index=# [Consulta em Agosto de 2021]

[90] BIONI, Bruno Ricardo. *Op. Cit.* pp. 87/88.

[91] SOLOVE, Daniel J. The Digital Person. New York and London. New York University Press, 2004. p.3.

[92] BIONI, Bruno Ricardo. *Op. Cit.* pp. 89 e ss.

classificação da pessoa de acordo com determinados estereótipos e servirão de filtro invisível para o direcionamento de conteúdos disponíveis na rede.

A técnica da definição de perfis (*profiling*), no caso da Internet das Coisas, pode, então, ser desmembrada em três elementos: a coleta dos dados (efetuada diretamente pelo dispositivo por meio de sensores, fornecida por terceiros ou disponíveis na *nuvem*); o tratamento automatizado por meio de um algoritmo (*machine learning*); e a decisão automatizada (*decision making*)[93]. Os dados coletados, frise-se, são utilizados não só para compor o perfil do titular a ele correspondente, mas também servem como substrato para a definição de padrões de comportamento (necessários categorização dos demais perfis) e como espécie de guia para checagem das decisões automatizadas a cada processamento, de modo que o ciclo se retroalimenta[94].

A preocupação surge da potencialidade de doutrinar-se a pessoa com um conteúdo e uma informação ditados pelos interesses inferidos por intermédio dos seus dados, isolando-a da interação com conteúdos diferentes que fogem ao perfil enquadrado, com influência nos mais variados aspetos da vida desde a celebração de contratos até o acesso à informação[95].

Todas essas características e peculiaridades têm preponderante impacto na análise do direito à proteção de dados pessoais e da aplicação do RGPD em relação aos dispositivos de Internet da Coisas por suscitarem problemas e discussões não existentes em relação a outros universos abrangidos pela proteção de dados.

2.2 Aplicabilidade do RGPD aos dispositivos *IoT*

Sob a perspectiva da aplicabilidade material do RGPD, o artigo 2.º do Regulamento estabelece ser aplicável as suas regras "*ao tratamento de dados pessoais por meios total ou parcialmente automatizados*", com excepção das hipóteses elencadas no próprio artigo. Não há dúvidas que, nesse aspeto, as operações desempenhadas pelos dispositivos do *IoT* estão abarcadas pela aplicação material do Regulamento sempre que se referirem a dados pessoais, sobretudo em razão da amplitude desse conceito trazido pelo RGPD no artigo 4.º.

---

[93] KAMARINOU, Dimitra; MILLARD, Christopher; e SINGH, Jatinder. *Machine Learning with Personal Data*. Em LEENES, Ronald. Et al. Data Protection and Privacy: The Age pf Intelligent Machines. Oxford, Hart, 2017. p. 94.
[94] KAMARINOU, Dimitra; MILLARD, Christopher; e SINGH, Jatinder. *Op. Cit.* p. 95.
[95] BIONI, Bruno Ricardo. *Op. Cit.* p. 91.

Em relação à aplicação territorial, o artigo 3.º do RGPD estabelece dois critérios de aferição, quais sejam o critério do *estabelecimento* (n.º 1) e o do *direcionamento* (n.º 2).

De acordo com o primeiro critério, incidirá o RGPD sempre que o tratamento de dados pessoais for efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento. Nesse quesito, uma primeira observação acerca dos dispositivos de *IoT* é a de que a atividade de tratamento será total ou parcialmente desenvolvida pelo próprio dispositivo, sem que esse tratamento se vincule a nenhum estabelecimento comercial, seja do fabricante/desenvolvedor do aparelho, seja do vendedor. Logo, a aplicabilidade do Regulamento pode ser questionada, sob o critério do estabelecimento (artigo 3.º, n.º 1), nas hipóteses em que o dispositivo é comprado em estabelecimento estrangeiro e também foi fabricado por empresa sem estabelecimento na União Europeia.

Também é importante sopesar o contexto atual de desenvolvimento tecnológico e a realidade de já existirem empresas sem estabelecimentos físicos e com atuação global. Não raras são as empresas não localizadas em lugar nenhum a não ser no meio virtual. Nesse aspecto, é indiferente, nos termos do próprio regulamento, o local onde estão armazenados os dados coletados (servidor) ou onde ocorre a atividade de tratamento em si, se dentro ou fora dos limites da União. Além disso, a localização dos titulares dos dados, por esse critério, não é tomada em consideração para fins de aplicação do RGPD. Ou seja, na hipótese de tratamento realizado no contexto de um estabelecimento situado em qualquer dos Estados-Membros[96], o Regulamento será aplicável mesmo que se refiram a pessoas singulares localizadas fora do território da União[97].

Igualmente irrelevante, para fins de avaliar o local do estabelecimento, é o critério formal de registo empresarial, pois o considerando 22 do RGPD expressamente dispõe que "*estabelecimento pressupõe o exercício efetivo e real de uma atividade com base numa*

---

[96] COMITÉ EUROPEU DE PROTEÇÃO DE DADOS (CEPD) Diretrizes 3/2018 sobre o âmbito de aplicação territorial do RGPD (artigo 3.º), versão 2.0, de 12/11/2019. Disponível em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_pt.pdf [Consulta em Agosto de 2021] No documento, o CEPD apresenta o seguinte exemplo: uma empresa francesa desenvolveu uma aplicação de partilha de automóveis exclusivamente destinada a clientes de Marrocos, da Argélia e da Tunísia. O serviço apenas está disponível nesses três países, mas todas as atividades de tratamento de dados pessoais são efetuadas em França pelo responsável pelo tratamento de dados. Nesse caso, é aplicável o RGPD, nos termos do artigo 3.º, nº 1.

[97] Nesse sentido, destaca-se o teor do considerando 14: A proteção conferida pelo presente regulamento deverá aplicar-se às pessoas singulares, independentemente da sua nacionalidade ou do seu local de residência, relativamente ao tratamento dos seus dados pessoais.

instalação estável.", não sendo fator determinante a sua forma jurídica. O texto do considerando vai, outrossim, ao encontro da disposição já existente na revogada Diretiva 95/46/CE e também do teor da jurisprudência do TJUE[98] nos casos *Google Spain* contra AEPD[99], *Weltimmo* contra a NAIH[100] e VKI (Associação de proteção dos consumidores austríaca) contra *Amazon EU Sàrl*[101].

Para o Comité Europeu de Proteção de Dados, a interpretação, a ser realizada caso a caso, não pode ser restritiva, sob pena de não se alcançar o objetivo de garantir uma proteção eficaz e completa. Por outro lado, não se pode exceder na amplitude interpretativa de modo a permitir a conclusão de que qualquer presença na UE é suficiente para atrair a incidência da legislação da UE em matéria de proteção de dados[102].

Já o artigo 3.º, n.º 2 do RGPD, estabelece o critério do *direcionamento* para fins de análise da aplicação territorial do Regulamento, de modo que a ausência de estabelecimento empresarial do responsável pelo tratamento em um dos Estados-Membros não é suficiente de *per si* para afastar a incidência do Regulamento. Do texto do dispositivo legal extrai-se duas novas hipóteses de aplicação territorial, sendo irrelevante o facto de existir ou não estabelecimento do responsável pelo tratamento na União Europeia, desde que, em qualquer dos dois casos, se refira ao tratamento de dados pertencentes a titulares que se encontrem na União Europeia, não sendo necessário que se trate de nacional de algum Estado-membro, sequer residente. Todavia, para o CEPD, o dispositivo deve ser interpretado no sentido de se considerar as atividades dirigidas intencionalmente, e não de modo inadvertido ou acidental, a indivíduos situados na UE[103].

Para além de se encontrar o titular na União Europeia, para ser aplicável o RGPD , é preciso ainda que se configure umas das hipóteses descritas nas alíneas *a)* e *b)* do dispositivo, ou seja,

---

[98] Embora todos esses precedentes remetam à época anterior à vigência do RGPD, entendemos, no mesmo sentido de CEPD, que são relevantes a para fins de interepretação da regra do artigo 3.º, n.º 1, notadamente da expressão "tratamento no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou subcontratante". COMITÉ EUROPEU DE PROTEÇÃO DE DADOS (CEPD). *Op. Cit.* p. 8.

[99] Caso *Google Spain* contra AEPD (C‑230/14, EU:C:2014:317). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62012CJ0131&from=PT [Consulta em Julho de 2021]

[100] Caso *Weltimmo* contra NAIH (C‑230/14, EU:C:2015:639). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62014CJ0230&qid=1625334800153&from=PT [Consulta em Julho de 2021]

[101] Caso VKI (*Verein für Konsumenteninformation*) contra *Amazon EU Sàrl* (C-191/15, EU:C:2016:612).

[102] COMITÉ EUROPEU DE PROTEÇÃO DE DADOS (CEPD). *Op. Cit.* p. 8.

[103] COMITÉ EUROPEU DE PROTEÇÃO DE DADOS (CEPD). Op. Cit. p. 17.

oferta de bens ou serviços na União Europeia[104] ou *controlo de comportamento de pessoas* localizadas na União Europeia.

Na primeira hipótese, o aplicador do direito deverá considerar todos os elementos fáticos (moeda utilizada na transação, língua, área de entrega de mercadoria, menção a especificidades voltadas ao público europeu, etc.) a fim de definir se, em conjunto, demonstram *evidente intenção* do responsável de ofertar produto ou serviço ao público europeu, mesmo não estando estabelecido em nenhum dos Estados-membros. Saliente-se, ainda, que a análise não tem por objetivo definir, de modo estanque, se o RGPD se aplica ou não a uma empresa, na condição de responsável pelo tratamento de dados, mas se se aplica a uma determinada operação. Assim, um mesmo responsável pelo tratamento (ou subcontratante) pode, ao mesmo tempo, estar vinculado às regras do RGPD em relação a parte de suas atividades, e não estar em relação a outra parte[105].

Na segunda hipótese (artigo 3.º, n.º 2, *b)*), há uma infinidade de situações possíveis relacionada a tratamento de dados por meio de dispositivos *IoT*, pois tais aparelhos têm como principal atividade justamente a coleta de dados relacionados com comportamento, com definição de perfis e tomada de decisões automatizadas e personalizadas[106]. O CEPD, inclusive, faz menção a essa particularidade nas Diretrizes 3/2018[107] ao se referir ao considerando 24[108] do RGPD e esclarecer considerar aplicável a mesma regra a outros tipos de controlo de comportamento por meio de aparelhos usáveis (*wearable*) e outros dispositivos inteligentes. Por fim, o Comité elenca exemplificativamente atividades que considera configurar controlo,

---

[104] O considerando 23 do RGPD esclarece ter que ser "*evidente a sua intenção de oferecer serviços a titulares de dados num ou mais Estados-Membros da União*."

[105] COMITÉ EUROPEU DE PROTEÇÃO DE DADOS (CEPD). *Op. Cit.* pp. 21/22, onde consta o exemplo de uma universidade que oferece vagas em cursos voltados ora para público nacional e ora para a comunidade académica internacional. Apenas em relação a esse último caso será aplicável o Regulamento, especificamente em relação aos dados por ventura sejam coletados no processo seletivo cujo público-alvo envolvia intencionalmente pessoas localizadas na UE.

[106] OLIVEIRA, Madalena Perestrelo de. *Definição de Perfis e Decisões Automatizadas no Regulamento Geral sobre a Proteção de Dados*. Em Em FinTech: desafios da tecnologia financeira. coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte. Vol. 2. Almedina. Coimbra, 2017. p. 62.

[107] COMITÉ EUROPEU DE PROTEÇÃO DE DADOS (CEPD). *Op. Cit*. p. 22.

[108] Considerando 24: O tratamento de dados pessoais de titulares de dados que se encontrem na União por um responsável ou subcontratante que não esteja estabelecido na União deverá ser também abrangido pelo presente regulamento quando esteja relacionado com o controlo do comportamento dos referidos titulares de dados, na medida em que o seu comportamento tenha lugar na União. A fim de determinar se uma atividade de tratamento pode ser considerada «controlo do comportamento» de titulares de dados, deverá determinar-se se essas pessoas são seguidas na Internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes.

entre as quais, publicidade comportamental, atividades de geolocalização e controlo do estado de saúde de uma pessoa[109].

Também é importante salientar que o responsável pela atividade de tratamento pode subcontratar empresas para executar operações em seu nome e sob suas instruções, sem que isso afaste a aplicação do Regulamento, independentemente de o subcontratante possuir ou não estabelecimento na União Europeia. Ademais, nos termos do artigo 27.º, nas hipóteses de aplicação do RGPD, por força do artigo 3.º, n.º 2, deverá o responsável pelo tratamento ou o subcontratante designar por escrito um representante, sem que isso configure "estabelecimento"[110].

Pelo exposto, extrai-se dos termos do RGPD que suas regras serão aplicáveis a operações de tratamento realizadas através de dispositivos de *IoT* tanto quanto a qualquer outra operação de tratamento, desde que observadas as hipóteses legais. Porém, não se pode negar que algumas particularidades da *IoT* trazem específicos desafios quando da avaliação da incidência do Regulamento, notadamente em razão do fato de a atividade de tratamento ser, em boa parte, executada por máquinas, sem qualquer intervenção humana, bem como de haver interligação, com compartilhamento de dados, entre os mais variados sistemas e dispositivos, dificultando muitas vezes a identificação do "responsável" pelo tratamento[111]. Por isso, ressalta-se ainda mais a importância do atendimento, pelas empresas componentes da cadeia de produção e distribuição dos dispositivos, ao princípio da transparência e a informação as entidades direta ou indiretamente envolvidas no processo de tratamento[112].

---

[109] COMITÉ EUROPEU DE PROTEÇÃO DE DADOS (CEPD). *Op. Cit.* p. 23.
[110] COMITÉ EUROPEU DE PROTEÇÃO DE DADOS (CEPD). *Op. Cit*. p. 27.
[111] Essa dificuldade já foi destacada pelo Comité Europeu, mas no âmbito da responsabilidade civil: COMITÉ ECONÓMICO E SOCIAL EUROPEU Parecer sobre «Confiança, privacidade e segurança para os consumidores e as empresas na Internet das coisas (IdC)» Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018IE1038&qid=1625339548895&from=PT [Consulta em Julho de 2021] itens 3.1 e 3.4.
[112] A maior atenção ao princípio da transparência em relação aos dispositivos de *IoT* foi destacada pelo GT29 desde a Opinião n.º 8/2014. GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Opinion 8/2014 on the on Recent Developments on the Internet of Things.* Setembro, 2014. Disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf [Consulta em Julho de 2021].

3. Principais desafios do RGPD frente às inovações tecnológicas da IoT

3.1 Objetivos e Princípios do RGPD

O desenvolvimento da chamada "Era da informação" somado aos objetivos da União Europeia, notadamente ante a livre circulação de produtos e pessoas resultou na idealização do Mercado Único Digital, com a construção de uma ambiente digital livre e seguro no âmbito da União Europeia. É nesse contexto que o RGPD surge, em substituição da Diretiva 95/46/CE, mormente da necessidade de um complexo normativo que garanta a proteção adequada e idêntica dos dados pessoais nos Estados da UE e a circulação da informação no âmbito europeu[113].

Assim, pode-se dizer que a espinha dorsal do RGPD é constituída de dois grandes objetivos: para além de proteger direitos fundamentais das pessoas singulares, notadamente o direito à proteção de dados, o Regulamento tem por objetivo promover a livre circulação dos dados pessoais. O RGPD, portanto, não se propõe a impedir o tratamento de dados pessoais. Ao contrário, o mister o Regulamento ratifica a licitude desse tratamento e estabelece as bases legais para que a atividade se dê em benefício do desenvolvimento econômico e tecnológico, sem pôr em xeque, todavia, a privacidade e demais direitos dos titulares[114].

Digno de realce é a abrangência material do RGPD. Apesar da associação imediata do Regulamento ao desenvolvimento tecnológico e ao mundo digital, suas regras se aplicam igualmente aos dados constantes de documentos físicos e tratados de modo não digital. Esse grande alcance do RGPD exige do intérprete e do aplicador do direito uma leitura dos princípios e conceitos da lei sob diferentes perspectivas, tendo sempre em consideração a natureza do tratamento de dados. Do contrário, uma leitura anacrónica dos dispositivos legais pode servir de equivocado entrave aos avanços tecnológicos.

Em relação aos princípios do tratamento de dados, são listados no artigo 5.º do RGPD: *licitude, lealdade e transparência* (n.º 1, *a)*); *limitação das finalidades* (n.º 1, *b)*); *minimização dos dados* (n.º 1, *c)*); *exatidão* (n.º 1, *d)*); *limitação da conservação* (n.º 1, *e)*); *integridade e confidencialidade* (n.º 1, *f)*) e *responsabilidade* (n.º 2).

---

[113] PINHEIRO, Alexandre Sousa, et al. *Comentário ao regulamento geral de proteção de dados*. Almedina, 2018. p. 97.

[114] CORDEIRO, António de Menezes. *Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019.* Coimbra. Almedina, 2020. p. 33.

A licitude deve ser entendida na sua acessão estrita, ou seja, não apenas deve estar de acordo com as leis, de uma forma geral, mas o princípio indica uma necessidade de o tratamento de dados corresponder a uma das hipóteses enumeradas no artigo 6.º do Regulamento[115]. Tal interpretação é extraída da própria redação legal, pois o artigo 6.º estabelece ser apenas lícito o tratamento enquadrado em alguma daquelas situações.

Por sua vez, o princípio da lealdade reforça a proteção do titular de dados ao impedir que o tratamento ocorra em seu prejuízo mesmo em situações potencialmente consideradas como lícitas. O termo, contudo, trata de um conceito aberto e, portanto, pouco preciso, sobretudo consideradas as lacunas vocabulares entre as diferentes línguas[116]. Assim, o atendimento do princípio da lealdade deverá ser observado em concreto, caso a caso, considerada a relação entre o responsável pelo tratamento e o titular, bem como suas legítimas expectativas.

O princípio da transparência representa importante pilar do RGPD, não só por constituir uma das novidades do diploma em relação à Diretiva 95/46/CE[117], mas também por ser relevante tê-lo em consideração, para fins de legitimidade do tratamento, durante todo o processo de tratamento. Isso porque, além das informações a serem prestadas no momento da recolha (artigo 13.º, ns.º 1 e 2), o dever de transparência determina que o titular continue a ser informado, por exemplo, em relação ao tratamento posterior dos dados pessoais (artigo 13.º, n.º, 3). É esse princípio, também, a base para o direito de acesso aos dados (artigo 15.º, n.º 1).

Ademais, não basta apenas prestar as informações, sendo imprescindível que elas sejam prestadas de forma concisa e acessível, com linguagem clara e simples. Ou seja, o responsável pelo tratamento deve envidar todos os esforços para estabelecer uma efetiva comunicação com o titular e deixá-lo ciente de todo o processo de tratamento, de seus direitos e das medidas de segurança adotadas.

Já o artigo 5.º, n.º 1, *b)* condiciona a recolha de dados à existência de uma finalidade *determinada*, *explícita* e *legítima*, em congruência com o artigo 8.º, n.º 2 da Carta Dos Direitos Fundamentais da União Europeia. Para o Grupo de Trabalho do Artigo 29.º para a Proteção de

---

[115] CORDEIRO, António Barreto Menezes. *Op. Cit.* p. 152.
[116] CORDEIRO, António de Menezes. *Op. Cit,* p. 153. Conforme descreve o autor, o princípio aparece na versão italiana do Regulamento como *correttézza,* na inglesa, como *fairness* e, na alemã, como *Treu und Glauben*, as quais não correspondem propriamente à tradução de lealdade, presente nas versões em português, espanhol e francês.
[117] CORDEIRO, António de Menezes. *Op. Cit,* p. 154.

Dados (GT29)[118] a exigência dos fins específicos é essencial para a análise do grau de interferência razoável na esfera privada do titular[119] e também representa uma salvaguarda à autodeterminação informacional a medida que é essencial para a garantia do controlo dos dados pelo titular[120]. Note-se que não há impedimento à existência de múltiplas finalidades, porém elas devem ser previamente conhecidas pelo responsável pelo tratamento e informadas ao titular (explícitas), além de respeitar, cada uma delas, as exigências legais (legítimas).

A segunda parte do dispositivo também permite que seja estabelecida uma nova finalidade no curso do processo de tratamento, desde que "não incompatíveis" com a finalidade originária. Nesse quesito, ensina Barreto Menezes Cordeiro[121] que, na análise dessa "não incompatibilidade" devem ser observados os fatores enumerados no artigo 6.º, n.º 4 do RGPD, devendo o responsável, também, certificar-se do respeito pelos princípios em relação às novas finalidades, bem como informar o titular dessa decisão (artigos 13.º, n.º 3 e 14.º, n.º 4).

Também como forma de reduzir a coleta dos dados apenas ao necessário, o RGPD estabelece o princípio da minimização (artigo 5.º, n.º 1, *c)*). Pelo princípio, não basta a mera apresentação de uma finalidade legítima, sendo essencial também que essa coleta se resuma ao mínimo necessário. Ficam excluídos, assim, os dados não relacionados com a finalidade, os inapropriados e os dispensáveis, sobretudo quando é possível atingir o fim almejado com o suporte de técnicas menos invasivas, com a anonimização e a pseudonomização.

O princípio da exatidão é autoexplicativo e exige que os dados mantidos sejam corretos e, além disso, atualizados sempre que necessário. Consequentemente, é dever do responsável pelo tratamento apagar ou retificar dados incorretos ou desatualizados.

Já o artigo 5.º, n.º 1, *e)* estabelece uma limitação temporal, ao determinar caber ao responsável pelo tratamento definir e informar ao titular a periodicidade para apagamento e atualização dos dados. O princípio visa obstar à manutenção das informações por tempo excessivo, expondo seus titulares desnecessária e/ou permanentemente.

---

[118] O GT29 é o grupo de trabalho europeu independente que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018, quando teve seus documentos ratificados na primeira seção plenária do Comé Europeu para a proteção de Dados, conforme informação disponível em https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en [Consulta em Setembro de 2021]

[119] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Opinion 3/2013 on purpose limitation.* Abril, 2013. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [Consulta em Julho de 2021].

[120] CORDEIRO, António de Menezes. *Op. Cit*, p. 155.

[121] CORDEIRO, António de Menezes. Op. Cit, p. 157.

A última alínea do artigo 5.º, n.º 1 estabelece os princípios da integridade e confidencialidade com o fim de reforçar a responsabilidade do detentor dos dados em relação à segurança da informação propriamente dita.

Por fim, o princípio de responsabilização, trazido pelo artigo 5.º, n.º 2 funciona como norma de efetivação das anteriores ao definir não apenas o dever do responsável pelo tratamento de agir em conformidade com os princípios, mas também a responsabilidade de comprovar essa conformidade.

3.2 Os conceitos do RGPD sob a perspectiva tecnológica da IoT

Como dito, o RGPD se propõe a normatizar as diversas modalidades de tratamento de dados, equilibrando a tensão aparentemente existente entre o valor dos dados pessoais na sociedade da informação e a imprescindível proteção dos direitos fundamentais e da esfera privada do indivíduo. Por isso, cabe ao intérprete da lei analisar os conceitos gerais e as diversas regras impostas no Regulamento considerando as particularidades e características de cada espécie de tratamento.

A realidade da *IoT* representa uma ruptura da estrutura de mundo tal qual o conhecíamos e introduz tecnologias, operações e, consequentemente, desafios inexistentes no tratamento de dados seja por meios analógicos, seja por meios digitais "tradicionais". Assim, parece recomendável uma análise dos conceitos introduzidos no RGPD sob a perspectiva dos avanços tecnológicos da Internet das Coisas para permitir uma interpretação da lei condizente com essa nova realidade.

O artigo 4.º do RGPD elenca diversos conceitos, definindo-os com o objetivo de emprestar a esses termos a precisão necessária à interpretação da lei. De partida, cabe-nos à análise do próprio conceito de "dados pessoais", pois a qualificação como "pessoal" dos diversos dados coletados pelos dispositivos de *IoT* é o que definirá a aplicabilidade ou não da proteção do Regulamento.

A norma, neste aspecto, estabelece ser dado pessoal toda "*informação relativa a uma pessoa singular identificada ou identificável (...)*". Note-se que, partindo-se desse conceito, nem todos os dados coletados pelos sensores da Internet das Coisas ou compartilhado entre os diversos aparelhos interconectados estão abrangidos pelo conceito de "dados pessoais"; por exemplo, quando estivermos diante de dados ambientais como a temperatura de uma dada localidade ou o índice de umidade do ar. Isoladamente, os dados ambientais não se referem a

nenhuma pessoa e, portanto, podem ser coletados e tratados sem as amarras do RGPD. Porém, associados a outros dados coletados, esses sim qualificados como pessoais, certos dados "não pessoais" podem integrar um feixe de informações, consideradas como "pessoais" em seu conjunto.

O GT29, na Opinião 4/2007[122], estabeleceu, ainda na vigência da Diretiva 95/46/CE, as balizas para interpretação do conceito de "dados pessoais". Embora a redação do RGPD não coincida integralmente com o texto da Diretiva revogada, o núcleo da definição legal permaneceu inalterado, pois concentrado nos termos *qualquer informação*, *relativa*, *pessoa singular*, *identificada ou identificável*.

Ao usar o termo *qualquer informação*, o Regulamento demonstra seu claro objetivo de fincar definição de abrangência ampla. Disso se extrai que se considera "dado pessoal" informações de qualquer natureza, seja objetiva ou subjetiva, como as opiniões e os sentimentos. Também, para configurar "dado pessoal" não é necessário que a informação seja verídica ou esteja provada, tanto que o próprio RGPD garante ao titular o direito de solicitar retificação, atualização ou apagamento de dados incorretos ou falsos. A amplitude do termo também permite concluir que os dados pessoais podem apresentar formatos (ter conteúdos dos mais diversos e vão desde informações estritamente sigilosas e sensíveis, como histórico médico, passando por conversas e informações relativas ao seio doméstico e familiar, até comportamentos em ambientes de trabalho e social[123].

O termo *relativa*, embora de significado evidente, permite igualmente algumas colocações relevantes. Certamente, qualquer informação sobre alguém, é facilmente classificada como "dado pessoal", inexistindo, portanto, dificuldades em reconhecer a pessoalidade de informações como nome, data de nascimento, tipo sanguíneo, perfil em uma rede social ou histórico de navegação em dispositivo pessoal. Porém, conforme destaca o GT29, algumas informações podem constituir dados pessoais, mesmo que, de modo imediato, se

---

[122] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Opinion 4/2007 on the Concept of Personal Data*. Disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf [Consuta em Julho de 2021]

[123] Interessantes exemplos são trazidos pelo GT29 a demonstrar a diversidade dos dados pessoais: a gravação da voz de alguém em uma chamada de *telemarketing*, as imagens de alguém capturadas por câmeras de vigilância (desde que seja reconhecível a pessoa) e, ainda, o desenho de um criança colhido em um teste psiquiátrico realizado no contexto de uma lide judicial. GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Op. Cit.* p. 8.

refiram a coisas[124]. No caso dos dispositivos de *IoT*, pode-se imaginar o exemplo relativo aos frigoríficos inteligentes que mantêm uma lista de compras com alimentos em falta ou de produtos próximos de atingir o prazo de validade. Esses dados podem ser analisados unicamente com o fim de avaliar a periodicidade de reposição de dado produto, ou sua durabilidade média, mas se associados ao perfil do residente podem configurar dados de comportamento.

Para sistematizar a qualificação de uma informação como relativa ou não a uma pessoa, o GT29 afirma que, além do conteúdo dos dados, objetivamente considerado, deve-se analisar também as circunstâncias do tratamento desses dados, pois o caráter pessoal pode decorrer igualmente da finalidade do tratamento ou, ainda, do seu resultado prático. Exemplo disso são os mecanismos de rastreamento de veículos utilizados pelas empresas gestoras de táxis, no exemplo citado na Opinião 4/2007[125], ou atualmente pelas plataformas eletrônicas de transporte tipo TVDE[126]. O sistema de localização se refere, numa perspectiva imediata, ao veículo e não ao motorista (conteúdo) e a finalidade não é a de rastrear a pessoa, mas de possibilitar a ligação entre o passageiro e o carro mais próximo, bem como de fornecer uma estimativa de tempo ao cliente. Contudo, esses mesmos dados podem basear certas conclusões acerca do comportamento dos motoristas, como excesso de velocidade ou condução imprudente, tendo como resultado sua penalização.

Sob a perspectiva da Internet das Coisas, mostra-se relevante ponderar a facilidade com a qual uma informação de conteúdo objetivamente impessoal pode ser associada a outros elementos de modo a impactar na esfera pessoal de alguém. Tal circunstância decorre da ubiquidade dessa tecnologia, notadamente potencializada por sensores, gravadores e câmeras associadas aos dispositivos, somada ao volume de dados coletados (*Big Data*), compartilhados entre dispositivos e cruzados com o objetivo de extrair as mais diversas conclusões a respeito das pessoas.

A análise da pessoalidade do dado sob a perspectiva do resultado, nas hipóteses em que conteúdo e finalidade sejam impessoais, também se apresenta especialmente relevante em um

---

[124] Os exemplos colacionados na Opinião 4/2007[124] se referem ao valor de um certo imóvel e ao histórico de manutenção de um carro. Em ambos os casos, os dados tanto podem ser analisados de modo impessoal (e. g. aferição do valor do metro quadrado em determinada zona), quanto pessoal (e. g. avaliar o tamanho do patrimônio do proprietário para fins fiscais, no caso do imóvel, ou mensurar a produtividade do mecânico, no caso do veículo). GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Op. Cit.* pp. 9/10.

[125] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Op. Cit*. p. 11.

[126] Transporte em veículos descaracterizados a partir de plataforma electrónica, modalidade de transporte passageiros regulamentada em Portugal pela Lei n.º 45/2018 de 10 de agosto.

meio tecnológico baseado em *machine learning*, à medida em que os resultados obtidos pelas máquinas nem sempre podem ser antecipados ou controlados em sua totalidade. Ou seja, até mesmo dados a princípio impessoais podem influir nos processos de decisão realizados exclusivamente por algoritmos e causarem impacto na vida de uma pessoa[127].

Quanto ao termo *pessoa singular*, não parece merecer grandes digressões. Isso porque, como visto, o direito à proteção de dados no contexto europeu derivou da proteção dos direitos de personalidade e, portanto, são titulares os seres humanos vivos e não, por exemplo, uma pessoa coletiva.

Por fim, cabe a análise da relevância da expressão *identificada ou identificável*. É certo que a forma mais simples de identificar um dado pessoal parte da correlação dessa informação com o nome da pessoa. Mas, como é óbvio, essa não é a única maneira de identificar o titular de determinado dado. Sobretudo nas modalidade de tratamento em que são elaborados perfis, para análise estatística ou tomada de decisões, o titular de uma informação pode ser identificado mesmo sem menção ao seu nome e quanto mais preciso for o perfil e maior o volume de dados, mais fácil será essa identificação.

Nesse tocante, o considerando 26 do RGPD estabelece que para aferir se o titular de determinado dado é identificável deve-se considerar "*todos os meios suscetíveis de ser razoavelmente utilizados*". Por isso, é possível concluir que na era do *machine learning* e do tratamento de dados por algoritmos, o espectro do que se considera *identificável* é ampliado. Isso porque, buscas, análises e cruzamentos de dados considerados impossíveis ou absurdamente custosos à ação humana podem ser rapidamente operados pelas máquinas. Soma-se, então, de um lado a velocidade operacional dos computadores e dispositivos e, de outro, a imensa capacidade de armazenamento de dados e o resultado é a potencialização da capacidade de identificação de uma pessoa a partir de um registro aparentemente impessoal ou anonimizado.

No caso dos dispositivos *IoT*, é importante mencionar duas características que também permitem uma maior facilidade na identificação do titular de um dado coletado.

---

[127] Para Bioni trata-se de uma leitura consequencialista da lei, que parte da distinção não entre dados pessoais e dado não pessoais, objetivamente considerados, mas da análise da relação de causa e efeito gerada pela atividade de tratamento na vida de determinado titular. O autor defende, outrossim, que tal leitura da norma só se justifica a partir da proteção dos direitos da personalidade. BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento.* Rio de Janeiro, Forense, 2019. p. 78/81.

Primeiro, pela sua pretensão de personalizar a experiência do usuário, boa parte desses dispositivos são de utilização individual (como é o caso dos relógios *smartwatch* e da maioria dos dispositivos tipo *wearable*, além de outros já utilizados na área da saúde como *intimate contact sensors*, *ingestible sensors* e *implantable sensors*[128]) ou restrita a um ambiente com um número limitado de pessoas, como o ambiente doméstico (caso dos assistentes eletrônicos, cuja utilização é restrita, regra geral, aos moradores de uma casa ou aos ocupantes de um escritório). Portanto, qualquer informação coletada, seja por seus próprios sensores, seja pela transferência de dados a partir de outro dispositivo a ele conectado, é facilmente associada ao seu dono ou relacionada a um dos poucos usuários.

Segundo, a coleta desses dados é realizada comumente por meio de câmeras e sensores biométricos, através do tratamento de dados personalíssimos como impressões digitais, voz e reconhecimento facial. Logo, quanto mais dispositivos interconectados e mais eficientes os sensores, mais precisa é a identificação do titular de cada informação.

Outro conceito elencado no artigo 4.º do RGPD com especial relevância para o campo da Internet das Coisas é o de "definição de perfis". O GT29 já direcionou seus estudos à análise das definição de perfis como suporte das decisões automatizadas, elaborando uma série de orientações[129]. Já de início, o documento destaca os aspetos positivos e negativos desse tipo de funcionalidade, que, ao mesmo tempo, garante aumento de eficiência e economia de recursos, trazendo ganhos nos campos da saúde, educação, transportes, mas também representando um risco significativo para os direitos e as liberdades das pessoas[130]. A norma estabelece que "definição de perfis" constitui qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados para avaliar certos aspetos pessoais de uma pessoa singular, tais como situação económica, saúde, preferências e comportamentos de uma maneira geral[131].

Ou seja, a definição de perfis envolve desde a recolha de dados pessoais para essas finalidades, passando por uma análise automatizada para identificar correlações (total ou

---

[128] PEPPET, Scott R., *Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent.* Texas Law Review, 2014. p. 98.

[129] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679*. Outubro, 2017. Rev. Fevereiro, 2018. Disponível em file:///C:/Users/User/Downloads/guideline%20decis%C3%B5es%20automatizadas%20e%20profilling.pdf [Consulta em Agosto de 2021].

[130] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Op. Cit.* p. 5.

[131] OLIVEIRA, Madalena Perestrelo de. *Op. Cit.*. p. 63.

parcialmente sem intervenção humana), até resultar na aplicação dessas conclusões a uma pessoa, identificando padrões comportamentais e classificando o indivíduo de acordo, por exemplo, com sua capacidade para executar uma tarefa, seus interesses ou comportamentos futuros presumíveis[132].

Note-se que o conceito legal estabelece que o tratamento é automatizado, porém a tomada de decisão (terceira fase do processo) pode ou o não o ser. Ou seja, a definição de perfis nem sempre está atrelada a decisões automatizadas. Ao analisar um pedido de empréstimo, a instituição financeira muitas vezes recorre à avaliação do perfil do solicitante, que pode ter a forma, por exemplo, de um sistema de *score* proporcional ao risco de inadimplemento baseado em uma série de dados comportamentais. A decisão acerca da concessão ou não do empréstimo pode ser realizada tanto por um ser humano (definição de perfil sem decisão automatizada), quanto por uma máquina através de algoritmo e com base em dados coletados por diversos outros dispositivos a ela conectados (definição de perfil usada para basear uma decisão automatizada). Igualmente, pode haver decisão automatizada sem definição de perfil, notadamente na hipótese de dispositivos acoplados a sensores, como nos casos das coimas de trânsito aplicadas automaticamente quando um radar deteta o excesso de velocidade de um veículo ou uma câmera o avanço ao sinal vermelho[133].

Como já mencionado, um dos atributos do objetos inteligentes é a personalização da experiência, pois à medida em que o usuário utiliza o dispositivo e este acumula dados acerca do seu comportamento, funcionamento do seu corpo e particularidades individuais, a máquina, através de seus algoritmos, adquire a capacidade de antecipar a vontade do usuário, tomando decisões por ele. Ou seja, a partir dos dados coletados, o dispositivo elabora conclusões acerca da personalidade do indivíduo, o que gera especial preocupação com a possibilidade de decisões automatizadas discriminatórias[134] ou de tratamento de dados de forma a expor a reputação do titular ou causar-lhe prejuízo financeiro, como destacado no considerando 75 do RGPD. O mesmo considerando também destaca a preocupação com a definição de perfis relativos a pessoas vulneráveis. Nesse ponto, mister ressaltar a problemática acerca da incapacidade de a máquina distinguir um vulnerável de um não vulnerável ou mesmo dados comuns dos dados sensíveis.

---

[132] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Op. Cit.* p. 7/8.
[133] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Op. Cit*. p. 8.
[134] OLIVEIRA, Madalena Perestrelo de. *Op. Cit*. p. 63.

Tudo isso justifica um tratamento específico pelo RGPD em relação à definição dos perfis e decisões automatizadas, conforme disciplinam os artigos 21.º e 22.º. Por sua vez, o considerando 71 impõe limitações à prática, ressaltando o direito de o titular de não ficar sujeito a ela e também o resguardo das crianças em relação a esse tipo de tratamento. Contudo, no caso da Internet das Coisas os dispositivos devem ser interpretados com a cautela devida, pois sua interpretação restritiva pode inviabilizar a própria tecnologia base dos dispositivos. A seguir, detalharemos a regulamentação específica do RGPD acerca das definições de perfis e decisões automatizadas e os desafios dela decorrentes em relação à Internet das Coisas.

O artigo 4.º também traz o conceito de "responsável pelo tratamento" como sendo a pessoa singular ou coletiva que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais. No âmbito da Internet das Coisas, identificar esse(s) responsável(eis) pode se apresentar como tarefa especialmente difícil. Isso porque, uma fabricante de frigorífico, por exemplo, que lança ao mercado um produto *smart*, provavelmente, não será a responsável direta pelo desenvolvimento da inteligência artificial a ele associada, componente comumente contratado de uma empresa de tecnologia. Ademais, esse dispositivo pode ser conectado, pelo usuários, a outros dispositivos, desenvolvidos por outras empresas, formando uma rede de compartilhamento dados. Note-se, por isso, que não raras são as hipóteses em que nenhuma das empresas está integralmente no controlo das finalidades e dos meios de tratamento, pois a operação se dá sem qualquer intervenção humana.

Nesse tocante, o artigo 26.º do RGPD introduz as figuras dos "responsáveis conjuntos", para as hipóteses em que dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento. Ao passo que os artigos 27.º e 28.º estabelecem regras específicas para essa hipótese, definindo as responsabilidades de cada um desses corresponsáveis. A questão posta em relação aos dispositivos de *IoT* diz respeito a essa posição de controlo em relação à atividade de tratamento, que na prática é integralmente realizada pelo dispositivo. Além disso, quanto às configurações e aos limites do tratamento, muitas vezes, são definições que cabem não às empresas desenvolvedoras, mas ao próprio usuário do dispositivo, sendo ele não raro quem decide inclusive acerca do tratamento de dados de terceiros coletados pelo seu dispositivo. Assim, já há teses defensoras da possibilidade de inclusão do proprietário do dispositivo entre o rol de "responsáveis pelo tratamento"[135], em aplicação análoga às

[135] Acerca do tema: DE CONCA, Silvia. *Between a Rock and a Hard Place: Owners of smart speakers and joint control*, SCRIPTed, 2020. Vol. 17, n. 2. Pp. 238-268.

decisões do TJUE nos casos *Wirtschaftsakademie*[136] e *Jehovah's Witness*[137], ambos os julgamentos ainda sob a vigência da Diretiva Diretiva 95/46/CE.

Por fim, cabe uma análise específica do conceito de "consentimento" trazido pelo Regulamento e suas implicações no âmbito da *IoT*, pois, embora o consentimento não seja a única base legal para legitimar o tratamento de dados, é uníssono que ele compõe núcleo central da norma, tamanha a sua evidência.

O RGPD, no artigo 4.º, n.º 11, assim define consentimento: *manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.*

Quanto à manifestação de vontade, essa é constituída por dois elementos: primeiro, a vontade humana e, depois, sua exteriorização[138]. Note-se que essa exteriorização não pressupõe obrigatoriamente uma declaração, seja oral ou escrita. Há diversas formas de exteriorizar uma vontade, exigindo a lei apenas que, se não declarada, seja resultado de um ato positivo inequívoco. No caso de uma dispositivo de Internet das Coisas a simples aquisição do equipamento pode ser interpretada como uma manifestação de vontade. Ora, se alguém resolve comprar determinado dispositivo, manifesta com aquele ato a vontade de utilizá-lo, assumindo as consequências naturais decorrentes daquele uso.

Quanto ao caráter da liberdade, a princípio toda vontade manifestada, por exemplo, por meio da compra de um dispositivo é livre, mas em casos excepcionais essa liberdade pode ser questionada, como nas hipóteses de coação, de uma compra imposta como condição para outro negócio jurídico, como uma exigência do empregador no curso de uma relação de trabalho ou eivada de quaisquer dos vícios de vontade elencadas no Direito Civil[139]. Em resumo, não poderá ser considerada de livre vontade a manifestação se ela não decorrer de uma escolha verdadeira

---

[136] Em que o TJUE entendeu que configuram responsáveis conjuntos o *Facebook* e o administrador de uma páginas de fãs criada na rede social. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62016CJ0210&from=PT [Consulta em Agosto de 2021]

[137] Em que o TJUE entendeu que configuram responsáveis conjuntos a comunidade religiosa e cada um de seus membros em relação ao tratamento de dados realizados no contexto da pregação porta a porta. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62017CJ0025&from=PT [Consulta em Agosto de 2021]

[138] CORDEIRO, António Barreto Menezes. *O consentimento do titular dos dados no RGPD*. Em FinTech: desafios da tecnologia financeira. coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte. Vol. 2. Almedina. Coimbra, 2017. p. 42.

[139] Em defesa da aplicação do Direito Comum na seara das proteção de dados quando com ela não seja incompatível: CORDEIRO, António Barreto Menezes. *Op. Cit.* p. 42.

ou, ainda, quando não puder recusada ou revogada sem que o titular dos dados seja prejudicado, conforme estabelece o considerando 42, *in fini*.

Ademais essa manifestação deve ser específica. Logo, será inválido o consentimento dado de forma genérica, sob pena de se transformar o consentimento em uma autorização ilimitada para o responsável pelo tratamento tratar todo e qualquer dado de determinado titular. Dessa especificidade necessária, surge a exigência da granularidade. O consentimento deve ser granular à medida em que, sendo mais de uma as finalidades de tratamento, deve ser garantido ao titular consentir com cada uma isoladamente[140].

A ausência de granularidade no consentimento representa um dos grandes desafios para o tratamento dos dados por dispositivos de *IoT*, pois na hipótese de o tratamento basear-se no consentimento, caso o titular não esteja de acordo com todas as finalidades de tratamento, a única opção que lhe resta é a não aquisição do dispositivo ou sua não utilização, pois não pode ele opor-se a uma ou mais finalidades de tratamento. Assim, não raras são as críticas ao protagonismo pelo RGPD ao consentimento como meio de legitimação do tratamento de dados apesar da evidente falta de opção do titular, que na maioria das vezes tem que exercer sua escolha com base no "tudo-ou-nada": permitir o tratamento dos seus dados beneficiando-se do mundo digital ou ficar alheio ao desenvolvimento tecnológico para proteger-se da vigilância exercidas pelas corporações detentoras de dados[141].

Ainda, essa manifestação de vontade deve ser informada. A exigência aparece como corolário do princípio da transparência e intimamente ligado ao objetivo do RGPD de garantir efetivo controlo dos seus dados pelos titulares. Até porque, sequer é possível falar propriamente em vontade livre e manifestação específica sem atrelar esses elementos ao conhecimento do titular em relação as circunstâncias relevantes para sua decisão. Entre as informações mínimas que devem ser prestadas, para o GT29[142], estão: i) identidade do responsável pelo tratamento; ii) finalidade de cada uma das operações de tratamento; iii) quais dados são recolhidos; iv) o direito do titular de retirar o consentimento; v) informações acerca da utilização dos dados para

---

[140] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679*. Novembro, 2017. Disponível em file:///C:/Users/User/Downloads/20180416_article_29_wp_guidelines_on_consent_publish_09A6854F-F638-8898-7A0543CE0857250F_51030.pdf [Consulta em Agosto de 2021]. p. 11.

[141] BETKIER, Marcin. *Privacy Online, Law and the Effective Regulation of Online Services*. Cambridge, Intersentia, 2019. p. 1.

[142] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Op. Cit.* pp. 14/15.

decisões automatizadas em conformidade com o artigo 22.º, n.º 2, *c)*; vi) possíveis riscos de transferências de dados (artigo 46.º).

No caso da Internet das Coisas, essa informação também se apresenta como um importante desafio. Primeiro, porque o caráter da novidade intrínseco a esses avanços tecnológicos vem acompanhado de um desconhecimento acerca de todas consequências e impactos dessa tecnologia na vida das pessoas. No caso da *IoT* há, inclusive, muito desconhecimento de seus limites pela própria comunidade científica e, por consequência, desconfiança dos usuários. Segundo, porque boa parte dos dispositivos não dispõe de ecrã ou possui um de pequenas dimensões de modo que não são compatíveis com o objetivo de comunicar ao seu utilizador um grande número de informações, de maneira clara e em linguagem acessível[143]. Essas dificuldades já foram evidenciadas pelo GT29, no Parecer 8/2014, quando a entidade ponderou que os mecanismos clássicos utilizados para obter o consentimento dos indivíduos comumente não se mostram compatíveis com os dispositivos inteligentes, o que pode resultar num consentimento de baixa qualidade[144].

Por fim, o RGPD exige que a manifestação de vontade seja explícita. Importante mencionar que o vocábulo *explícita*, apesar de constar da Proposta de RGPD apresentada incialmente pela Comissão Europeia[145], foi suprimido da versão final do texto normativo nas demais versões, mas não na portuguesa[146]. A supressão foi resultado da consagração da posição defendida pelo Conselho da União Europeia para evitar a interpretação segundo à qual o consentimento haveria de ser escrito.

Embora a versão em português não tenha acompanhado as demais, certamente o conhecimento do desfecho das negociações quando da aprovação do texto direcionam a interpretação do termo "explícita", que deve ser encarado como antônimo de "implícita" no

---

[143] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Orientações relativas à transparência na aceção do Regulamento 2016/679*. Novembro, 2017. Disponível em https://www.uc.pt/protecao-de-dados/suporte/20180411_orientacoes_relativas_a_transparencia_wp260_rev01 [Consulta em Agosto de 2021].
[144] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Opinion 8/2014 on the on Recent Developments on the Internet of Things.* Setembro, 2014. Disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf [Consulta em Julho de 2021].
[145] COMISSÃO EUROPEIA. *Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados)*. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52012PC0011&from=sl [Consulta em Agosto de 2021] p. 45.
[146] CORDEIRO, António Barreto Menezes. *O consentimento do titular dos dados no RGPD. Op. Cit. p.40.*

sentido de que o consentimento não pode ser presumido ou resultar de atos negativos, como o silêncio ou a inércia.

4. A (aparente) incompatibilidade entre o RGPD e o tratamento de dados realizado pelos dispositivos de *IoT*

Enquanto a implementação da Internet das Coisas com suas caraterísticas de ubiquidade, hiperconectividade e omnipresença inaugurou uma nova era tecnológica marcada por um volume inédito de dados tratados, o Regulamento Europeu de Proteção de Dados surge como resultado da evolução histórica da legislação de proteção de dados pessoais, assentado, portanto, em conceitos e premissas que remontam a períodos em que o progresso tecnológico alcançava níveis consideravelmente inferiores de automação.

É esse o cenário que serve de pano de fundo para o debate acerca de uma aparente incompatibilidade entre o RGPD e a realidade da *Internet of things* e que permite as não raras críticas aos Regulamento no sentido de ele já ter nascido obsoleto ou de representar entrave inconveniente ao desenvolvimento tecnológico.

Acerca do assunto, Zarsky[147] publicou já em 2017, antes portanto da entrada em vigor do Regulamento mas depois da sua aprovação, um estudo crítico do RGPD apontando incompatibilidades na norma em relação aos atuais avanços tecnológicos. Embora não tenha tratado especificamente da *IoT*, Zarsky elencou quatro aparentes conflitos entre RGPD e a "Era do *Big Data*": o princípio da limitação das finalidades (artigo 5.º, 1, *b)*), o princípio da minimização dos dados (artigo 5.º, 1, *c)*), as categorias especiais de dados (artigo 9.º) e a regulação específica das decisões automatizadas (artigo 22.º).

Também outros questionamentos surgem a partir das restrições legais às decisões automatizadas e os entraves que elas podem implicar no desenvolvimento da inteligência artificial e no funcionamento dos algoritmos. Analisaremos esses questionamentos sob duas perspectivas: o conflito entre o princípio da transparência e a opacidade da inteligência artificial (efeito *black-box*); e a incompatibilidade entre o *machine learning* e o direito ao esquecimento.

---

[147] ZARSKY, Tal Z. *Incompatible: The GDPR in the Age of Big Data.* Seton Hall Law Review. Vol. 47, n.º 4, 2017. pp. 995-1020. Disponível em https://heinonline.org/HOL/P?h=hein.journals/shlr47&i=1019 [Consulta em Julho de 2021]

4.1 O impacto do princípio da limitação das finalidades (Artigo 5.º, n.º 1, *b)* do RGPD)) no tratamento de dados pelos dispositivos de IoT

Conforme já introduzimos no item 3.1, o princípio da finalidade estabelecido no artigo 5.º, n.º 1, *b)*, do RGPD exige que os dados sejam recolhidos para finalidades, além de legítimas, determinadas e explícitas. Além disso, há uma vedação ao tratamento posterior para finalidades incompatíveis com as primeiras (aquelas que justificaram a recolha). Nesse quesito, a própria norma cuida de elencar três exceções muito específicas: interesse público, investigação científica ou histórica e fins estatísticos.

Ou seja, o Regulamento parte da premissa de que a finalidade precede à coleta dos dados, sendo esta última uma ação necessária à consecução daqueles fins primeiros.

Por outro lado, a realidade do Big Data – e, por consequência, da Internet das Coisas – parte de premissa inversa, segundo a qual o devem ser recolhidos os dados para, posteriormente, trata-los para finalidades cuja possibilidade sequer era antecipada. Isso porque o ponto central do desenvolvimento da inteligência artificial é o de superar os limites da inteligência humana, não só por meio da obtenção de uma maior velocidade de processamento de informações e capacidade de armazenamento, mas realizando atividade tidas por impossíveis ou inimagináveis em uma realidade sem máquinas inteligentes.

Nesse cenário, é mister ressaltar que embora a inteligência artificial seja programada, em alguns aspectos, para espelhar o modo de pensar humano e potencializar seus resultados, em outros aspectos, a máquina supera os limites da mente humana rompendo com o padrão por ela seguido e adotando um novo padrão, invisível aos nossos olhos, dada a nossa limitada capacidade de armazenamento de informações . Para descobrir esses novos padrões, é indispensável a coleta massiva de dados para uma finalidade que só vai ser evidenciada a posteriori.

Por isso, Zarsky[148] destaca que, o cumprimento do RGPD no tocante à limitação das finalidades, as entidades engajadas em qualquer atividade que envolva análise de *Big Data* estariam obrigadas a monitorar de modo ininterrupto suas operações de modo a fiscalizar se estariam sendo excedidas as finalidades antecipadas ao titular quando da recolha dos dados, exigência impossível de ser cumprida ou, ao menos, extremamente difícil e custosa. Em

[148] ZARSKY, Tal Z. *Op. Cit.* p. 1006.

alternativa, caberia a essas entidades tentar driblar o entrave legal, informando os titulares das finalidades abrangentes, correndo, todavia, o risco de ter sua finalidade considerada inespecífica e, portanto, ilegítima sob a perspectiva do Regulamento.

Para além desse obstáculo que o princípio da limitação das finalidades impõe à Internet das Coisas, impondo restrições diretas aos seus meios de funcionamento, há também os entraves indiretos. Por exemplo, as restrições decorrente do princípio acabam por dificultar o acesso de pequenas empresas e *startups* ao mercado de dados e concentram o poder nas mãos das chamadas "gigantes da tecnologia" (*Big Techs*). Por isso, para Zarsky, o princípio também é conflitante com a era do *Big Data* na medida em que diminui o ambiente de competição necessário à inovação[149].

Contudo, a realidade é que a limitação da finalidade não é apenas mais uma regra – a qual poderia ter sua aplicação flexibilizada a depender do tipo de tecnologia utilizado no tratamento de dados pessoais[150]– mas representa uma das pedras angulares do Regulamento. Então, eventual conclusão no sentido de ser impossível a compatibilização entre o princípio e o Big Data e, por consequência, a Internet das Coisas, resultaria na defesa da inaplicabilidade de todo o diploma a essa seara.

Zarsky[151], nesse tocante, apresenta algumas soluções. A primeira, de ordem prática, sugere um monitoramento rigoroso do uso dos dados com o fim de promover a confiança e conter abusos por partes dos responsáveis pelo tratamento. Assim, o controlo pretendido pelo Regulamento seria efetivado não por meio de uma proibição impeditiva ao tratamento (ex ante), mas por meio de limitação posterior sempre que o uso dos dados se revele abusivo[152].

A segunda solução se relaciona com o seguinte trecho do dispositivo regulamentar: "não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades". Segundo o autor, a compatibilização entre o RGPD perpassa pela interpretação do termo

---

[149] ZARSKY, Tal Z. *Op. Cit.* p. 1007.

[150] Até porque isso violaria a neutralidade expressa no considerando 15. Sobre o assunto: PAGALLO, Ugo. *The legal challenges of Big Data: putting secondary rules first in the field of EU Data Protection.* European Data Protection Law Review (EDPL), 2017. Vol. 3. N.º. 1. pp.36-46.

[151] ZARSKY, Tal Z. *Op. Cit.* p. 1007.

[152] Zarsky, T. Z., *Desperately Seeking Solutions: Using implementation-based solutions for the troubles of information privacy in the age of data mining and the internet society*. Maine Law Review, 2004. Vol. 56. N.º 1. p. 33. Disponível em: https://heinonline.org/HOL/Page?public=true&handle=hein.journals/maine56&div=7&start_page=13&collection=journals&set_as_cursor=0&men_tab=srchresults [Consulta em Agosto de 2021].

"incompatível", ao passo que o tratamento de dados posterior, para finalidades diversas da inicialmente informada ao titular seria admissível desde que não fossem incompatíveis entre si. Ou seja, o vocábulo incompatível não pode ser interpretado de forma restritiva de modo a concluirmos que as finalidades de tratamento devam ser as exatas finalidades pretendidas quando da recolha dos dados; elas podem ser diferentes, desde que não incompatíveis.

Nesse quesito, é importante analisar o teor do artigo 6.º, n.º 4, do RGPD que determina que o responsável pelo tratamento, para fins de verificação da compatibilidade entre as finalidades, primeira e posterior, deve ter em conta: a) qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior; b) o contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento; c) a natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9.º, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.º; d) as eventuais consequências do tratamento posterior pretendido para os titulares dos dados; e e) a existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização.

Apesar das dificuldades práticas de aplicação desses parâmetros na seara do Big Data e da inteligência artificial, certo é que a compatibilização entre o princípio da limitação das finalidades e o funcionamento da IoT perpassa obrigatoriamente por uma interpretação do texto normativo que flexibilize a rigidez da suas restrições.

4.2 O paradoxo entre o princípio da minimização dos dados e o volume de dados envolvidos nas análises *Big Data*

O princípio da minimização dos dados (artigo 5.º, n.º1, *c)* do RGPD) constitui outra pedra angular do Direito da Proteção dos Dados, mas, diferentemente do princípio da limitação das finalidades[153], não tem origem *constitucional*. Para Zarsky, essa particularidade permite uma maior margem de flexibilização ao legislador europeu quanto à abrangência do princípio [154].

Do princípio da minimização é possível deduzir restrições ao tratamento de dados em várias perspectivas como, por exemplo, no momento da recolha, com a limitação do escopo e

[153] Extraído da expressão "*para fins específicos*" constante do Artigo 8.º, n. 2, da Carta dos Direitos Fundamentais da União Europeia.
[154] ZARSKY, Tal Z. *Op. Cit.* p. 1009.

categoria dos dados coletados, mas também em relação ao período de tempo que os dados permanecem armazenados[155]. A lógica por trás do princípio é simples: quanto menos dados à disposição do responsável pelo tratamento – seja porque já deletados, seja porque sequer coletados – menores as chances de haver utilização abusiva de dados, para além do consentimento do titular, por exemplo, e também menores os riscos de segurança ou menor o impacto de eventual vazamento.

Na contramão dessa lógica, a realidade do *Big Data* parte da premissa segundo a qual quanto maior for o volume de dados recolhido e armazenado, mais precisas serão as análises possíveis, mais útil será o tratamento desses dados e melhor decisões poderão ser tomadas pelas máquinas sem a intervenção humana.

Ou seja, salta aos olhos o paradoxo emergente da aplicação de uma legislação que determina a restrição da coleta e armazenamento de dados "ao mínimo necessário" a tecnologias baseadas em análises por meio de algoritmos e máquinas inteligentes, cujo funcionamento pressupõe um volume considerável de dados, para deles extrair padrões de comportamento e daí conseguir prever escolhas do usuário e se amoldar às suas preferências. Ademais, a exclusão dos dados ou a coleta restritiva causa lacunas capazes de impedir o bom funcionamento dos algoritmos, provocando distorções, diminuindo a qualidade sua performance e, consequentemente, sua utilidade[156].

Nesse tocante, Zarsky sugere que uma solução para essa incongruência entre a análise de *Big Data* e o RGPD emerge da exceção legal em relação ao tratamento de dados para fins estatísticos (artigo 5.º, n.º 1, *b), in fine*), bem como a pseudonomização (artigo 6.º, n.º 4, *e)*), sem deixar de ressaltar entretanto que nem sempre essa estratégia será possível e, em alguns casos, a pseudonomização pode restringir consideravelmente os benefícios decorrentes do tratamento[157].

Já Peter K. Yu, defende o compartilhamento de dados entre os controladores, notadamente as grandes plataformas e os controladores de dispositivos inteligentes por meio de uma maior *interoperatividade* entre as bases de dados e esforços no sentido de garantir a portabilidade dos

---

[155] Daí decorre a obrigação do responsável pelo tratamento de estabelecer prazos para apagamento dos dados pessoais, conforme texto do considerando 39: "(...) A fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica. (...)"

[156] YU, Peter K., *Beyond Transparency and Accountability: Three additional features algorithm designers should build into intelligent platforms*. Northeastern University Law Review. 2021. Vol. 13, n.º 1. pp. 290.

[157] ZARSKY, Tal Z. *Op. Cit.* p. 1011.

dados. Para o autor, essa *interoperatividade* não só potencializa a utilidade dos dispositivos para seus usuários, como contribui para uma maior competitividade no setor da inteligência artificial e induz a avanços tecnológicos, inclusive em relação à segurança da informação[158].

4.3 A proibição ao tratamento de categorias especiais de dados (dados sensíveis) e a impossibilidade prática de máquinas inteligentes distinguirem a natureza dos dados

O artigo 9.º do RGPD, assim como já fazia a Diretiva 95/46/CE, cria categorias especiais de dados pessoais a partir da sua potencialidade em revelar informações sensíveis acerca do indivíduo, notadamente as que podem lhe expor a tratamento discriminatório ou as que dizem respeito às esferas mais íntimas. Por isso, a norma proíbe, em linhas gerais, o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical e, ainda, dados genéticos, biométricos ou os relativos à saúde, à vida e a orientação sexual.

O próprio disposto cuida de estabelecer uma série de situações em que o tratamento de dados dessa natureza será considerado legítimo, por exemplo, na hipótese de ser dado o consentimento explícito pelo titular em relação a finalidades específicas (artigo 9.º, n.º 2, *a)*) ou quando o tratamento disser respeito à proteção de interesses vitais do titular ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento (artigo 9.º, n.º 2, c*)*).

O maior desafio, no que toca à Internet das Coisas, emerge do fato de não ser possível a princípio o controlo e seleção por dispositivos inteligente da natureza dos dados em tratamento. A primeira dificuldade surge da própria elasticidade do conceito. Por exemplo, em relação aos dados relativos à saúde, incluído nas categorias especiais, o considerando n.º 35 estabelece que "*deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. (...)"*.

Ou seja, um dado aparentemente sem qualquer relação com a saúde de uma pessoa singular poderá, dentro de certo contexto, revelar informações relacionadas à saúde, fazendo incidir as restrições legais em relação ao seu tratamento. No contexto atual da pandemia de Covid-19, por exemplo, isso pode ser bem observado em relação aos dados que indicam a procedência

[158] YU, Peter K. *Op. Cit.* p. 291.

geográfica de passageiros. A princípio, origem e destino de um viajante ou informações constantes de uma passagem de avião, em nada se relacionam à saúde do titular dos dados. Contudo, no cenário pandêmico o local de origem de alguém permite inferir sua exposição potencial ao vírus, bem como a alguma cepa variante característica de determinada localidade.

Portanto, todo dado não estritamente relacionado diretamente com as categorias especiais pode potencialmente revelar, a depender do contexto, informações consideradas sensíveis e atrair um conjunto de regras e proibições distintas das regulares. Não se trata, assim, de um apanhado de dados de natureza objetivamente determinados, mas envolve uma acurada avaliação caso a caso acerca da natureza daquelas informações, o que pode se mostrar impossível de ser realizado por um dispositivo inteligente ou, no mínimo, exigiria um grau de sofisticação de inteligência artificial que inviabiliza o desenvolvimento de novos dispositivos[159].

Além disso, Zarsky pondera que se todo dado pode em teoria revelar informações sensíveis, então não existiriam razões para manter a distinção. A manutenção dessas categorias especiais, nesse sentido, teria tão somente um condão simbólico de destacar uma especial atenção à informações potencialmente causadora de tratamento discriminatório. Contudo, prossegue o autor, a sustentar que na era do *Big Data* o tratamento discriminatório mais comum decorre não de conduta intencional a partir de certa informação sensível, mas principalmente é gerado sem intenção, em consequência do mal funcionamento de algoritmo[160]. Ou seja, nesse tocante a divisão dos dados em categorias geral e especial não atingiria a finalidade almejada a medida em que não teria impacto na ocorrência de tratamento discriminatórios.

Por fim, cita-se outras consequências negativas advindas da criação das categorias especiais: a) a flexibilidade do conceito gera custos regulatórios e judiciais para preencher as lacunas desse conceito aberto; b) essa imprecisão conceitual resulta em insegurança jurídica, provocando desestímulo de investimento e onerando, sobretudo, pequenas empresas com a necessária consultoria jurídica; c) simbolicamente, se todos os dados são qualificáveis potencialmente como pertencentes à categoria especial, na prática, nenhuma informação será

[159] ZARSKY, Tal Z. *Op. Cit.* p. 1013.
[160] ZARSKY, Tal Z. *Op. Cit.* p. 1014.

considerada especialmente sensível e, ao fim, todos os dados receberão tratamento uniforme e almejado alto nível de proteção a certos dados será diluído[161].

4.4 As restrições legais às decisões automatizadas e a opacidade da Inteligência Artificial em contraponto ao dever de transparência

O artigo 22.º do RGPD se refere especificamente a normas especiais aplicáveis às decisões automatizadas, sejam ela associadas ou à definição de perfis, conforme tratamos *supra*. A primeira distinção legal imposta para esse tipo de tratamento de dados, que é a base do funcionamento dos dispositivos de *IoT*, é o direito do titular de dados de não ficar sujeito a nenhuma decisão totalmente automatizada (artigo 22.º, n.º 1). Já o artigo 22.º, n.º 2 prevê algumas exceções para a regra geral: a) nas hipóteses necessárias à celebração ou execução de um contrato; b) em hipóteses específicas admitidas pelo Direito Europeu ou de qualquer Estado-Membro, desde que com as necessárias salvaguardas aos direitos e interesses dos titulares; c) por fim, na hipótese de consentimento explícito do titular. Essas exceções, de acordo com o número 4 do mesmo artigo, não se aplicam quanto se tratar de dado qualificado nas categorias especiais, o que suscita os desafios descritos acima.

Ainda, o artigo 22.º, n.º 3 estabelece dois direitos aos titulares de dados, nomeadamente o de poder solicitar intervenção humana e o de manifestar oposição à decisão conforme seu ponto de vista.

Zarsky apresenta, em sua visão, os dois principais motivos para o especial tratamento dedicado às decisões automatizadas, sendo o primeiro relacionado com o dever de honra e respeito por partir do pressuposto que o titular, notadamente nas hipóteses de tomadas de decisão que impactam significativamente sua vida, prefere que sua situação seja avaliada por um ser humano. Já o segundo motivo se apresenta como consequência de uma generalizada falta de confiança nas máquinas e sistema tecnológicos, razão que vem pouco a pouco perdendo sua força conforme avança o progresso da tecnologia[162].

Portanto, a tensão entre o RGPD e o universo da Internet das Coisas – que envolve naturalmente a inteligência artificial e o *Big Data* – mostra-se das mais evidentes incompatibilidades. Enquanto o Regulamento se preocupa em determinar que o tratamento

[161] ZARSKY, Tal Z. *Op. Cit.* p. 1015.
[162] ZARSKY, Tal Z. *Op. Cit.* p. 1017.

integralmente automatizado e a submissão dos titulares às decisões daí advindas seja excecional, no mundo *IoT* esse tipo de tratamento é a regra e quanto mais desenvolvida a tecnologia, menor será a necessidade de intervenção humana.

Nesse aspeto, o RGPD atua como freio à inovação e ao progresso tecnológico. Primeiro, por impor entraves ao funcionamento do *Big Data* e minimizar, por consequência, sua eficiência e utilidade; segundo, ainda nos casos excecionais em que é permitido o tratamento pelo RGPD, a operação deve ser realizada de tal maneira que seja "interpretável" ao ser humano, exigindo, muitas vezes, algum tipo de intervenção humana, comprometendo, mais uma vez, a eficiência dos sistemas; terceiro, tudo isso onera consideravelmente a operação e apresenta-se como desestímulo aos investimentos[163].

Outra obrigação imposta pelo Regulamento ao responsável pelo tratamento decorre dos artigos 13.º, n.º 2, *f)* e 14.º, n.º 2, *g)* segundo os quais o titular de dados deve ser informado da existência de decisões automatizadas, bem como acerca da lógica subjacente a elas e as consequências do tratamento. Esse "direito à explicação", na prática, pode se revelar extremamente custoso, quando não impossível, pois não raros são os sistemas em relação aos quais se conhece os dados coletados (*inputs*) e o resultado do tratamento (*outputs*), mas não o procedimento realizado pela máquina para transformar um em outro[164]. Em relação a essa obscuridade da lógica por trás de alguns sistemas inteligentes, os especialistas cunharam o nome de efeito *black-box*.

O termo tem sido utilizado como referência ao caráter da opacidade da Inteligência Artificial, que torna o padrão de procedimento do algoritmo indetectável, em alguns casos, mesmo se submetida à intensa observação humana, pois o acesso ao *output* por si nem sempre permite perceber e reproduzir o sequencial lógico realizado pela máquina sobretudo porque ele não é constante. A mudança dos padrões utilizados para realizar as operações pemite às máquinas inteligentes um contínuo aprimoramento de sua performance, ao mesmo tempo em que torna sua operação icognoscível. Para Forti, as obrigações impostas pelo Regulamento demonstram que remete a uma época em que os algoritmos da Inteligência Artificial não

[163] ZARSKY, Tal Z. *Op. Cit.* p. 1017.
[164] YU, Peter K. *Op. Cit.* p. 268.

exerciam importante papel na vida cotidiana e, por isso, resultam numa incompatibilidade entre o funcionamento da IA e o grau de transparência legalmente exigido[165].

A essa problemática acerca da dificuldade de os próprios desenvolvedores e operadores conhecerem as lógicas subjacentes aos procedimentos realizados pelas máquinas inteligentes, soma-se o questionamento acerca da capacidade de os titulares perceberem essa lógica na hipótese desse lhes ser informada. Nesse aspecto, o dever de explicação se mostra pouco útil sob a perspectiva do titular que, mesmo nas situações nas quais é possível compreender a lógica informada, a análise da pertinência e adequação desses procedimentos exige dedicação de tempo, esforços e energia consideráveis[166].

Estabelece-se daí um círculo vicioso: a opacidade dos dispositivos inteligente não permite atingir o grau de transparência esperado pelos usuários, que adquirem e operam os dispositivos sem completo entendimento de como eles funcionam e decidem. Consequentemente, crescem as preocupações com a confiabilidade dessas máquinas e a segurança de seus processos e aumenta a demanda por mais transparência. Esse estado de desconfiança é ainda mais facilmente observado em relação aos dispositivos utilizados na área da saúde (e-*Health*), pois o efeito *black-box* impede médicos e pesquisadores de apreender a lógica dos procedimentos automatizados, trazendo incertezas em relação a soluções e diagnósticos a não ser que confiem no bom funcionamento do algoritmo. Ilustrativo exemplo é trazido por Nahmias e Perel[167] quando mencionam a implementação do mecanismo de *machine learning* no Mount Sinai Hospital, em Nova York. O sistema se provou mais tarde ser extremamente eficiente no tratamento dos dados coletados pelo hospital, sendo capaz de detetar várias doenças, inclusive distúrbios psíquicos como esquizofrenia. Todavia, nem os médicos pesquisadores nem os desenvolvedores não conseguiram alcançar como o algoritmo conseguiu tal feito, tornando impossível a concretização do direito à explicação.

Também em relação à utilização da IA no campo médico, Forti[168] apresenta outros entraves decorrentes dos princípios do RGPD, notadamente o da transparência, tais como a exposição do funcionamento dos dispositivos como desestímulo à inovação por dificultar a

---

[165] FORTI, Mirko. *The Deployment of Artificial Intelligence Tools in the Health Sector: Privacy Concerns and Regulatory Answers within the GDPR*. European Journal of Legal Studies, 2021. Vol. 13, n.º 1. p. 31
[166] YU, Peter K. Op. Cit. p. 277.
[167] NAHMIAS, Yifat. e PEREL, Maayan. *The Oversight of Content Moderation by AI: impact assessments and their limitations*. Harvard Journal on Legislation, 2021. Vil. 58, n.º 1. p. 155.
[168] FORTI, Mirko. *Op. Cit.* pp. 32/34.

proteção da propriedade intelectual e as restrições ao tratamento de certas categorias de dados (além dos estritamente da saúde, os relativos a gênero, raça e outros fatores que influenciam nos diagnósticos, mas podem também resultar em tratamento descriminatórios).

Nesse sentido, Taylor apontou a insuficiência das regras do Regulamento para fins de proteção do titular de dados notadamente no tocante a imprecisões ocorridas no curso do do processo decisório automatizado[169]. Para o autor, seja o direito a explicação (artigos 13.º a 15.º), seja o direito a não ser submetido a decisões automatizadas (artigo 22.º) asseguram um bom nível de qualidade de tratamento de dados, pois, no primeiro caso o dever é de o responsável pelo tratamento genericamente informar as consequências da decisão, mas isso não abrange descrever potenciais imprecisões, muitas vezes sequer conhecidas[170]. No segundo caso, igualmente, pois o titular pode querer consentir com a decisão automatizada, desde que ela esteja atrelada a uma garantia da precisão do algoritmo e da ausência danos em potencial daí decorrentes. O autor faz, ainda, um paralelo entre o dever de transparência do RGPD e o consentimento informado exigido no caso de submissão do paciente a um procedimento médico, em que não basta a informação acerca da natureza e fases do procedimento, tampouco alerta acerca da possibilidade de o tratamento vir a não ser eficaz, mas indispensável a enumeração dos riscos inerentes ao procedimento, mesmo que ele acontença exactamente da forma como programada[171].

Por todas essas peculiaridades da AI e, consequentemente, dos dispositivo de Internet das coisas, sobretudo a amplitude de sua penetrabilidade e as múltiplas áreas em que sua implementação é possível, Nahmias e Perel concluem no sentido de ser impossível a imposição de um único sistema regulatório flexível o suficiente para satisfazer as demandas próprias de cada setor, razão pela qual defendem criação de regras específicas a cada domínio[172].

---

[169] TAYLOR, Roger. *Op. Cit.* pp. 72/73.

[170] O exemplo apresentado pelo autor se refere às análises automatizadas de crédito. Cabe ao responsável, pelo direito à informação o dever de informar ao titular a existência da decisão automatizada e possibilidade de aquele crédito ser ou nao negado, sem necessidade de mencionar imprecisões do algoritmo que podem levar a uma decisão injusta.

[171] TAYLOR, Roger. *Op. Cit.* pp. 72/73.

[172] NAHMIAS, Yifat. e PEREL, Maayan.. *Op. Cit.* p. 163.

4.5 Os algoritmos e o direito a ser esquecido

O artigo 17.º do RGPD apresenta uma prerrogativa do titular de dados que constitui uma das principais inovações do diploma: o direito ao apagamento de dados, também chamado de direito a ser esquecido. Esse direito pode ser exercido por qualquer dos motivos elencados pela lei, entre os quais a retirada do seu consentimento às decisões automatizadas e sua oposição a elas (artigo 17.º, n.º 1, *c)*).

Tal prerrogativa legal tem impacto significativo no funcionamento da Inteligência Artificial, pois o sistema alcança maior eficiência quanto maior seja a base de dados da qual extrai suas decisões. Ou seja, o apagamento de qualquer dado, mesmo que o tratamento não mais interesse ao seu titular individualmente, interfere no estabelecimento dos padrões pelo dispositivo e na sistemática de funcionamento do algoritmo a ele associado[173].

Outra dificuldade, de ordem eminentemente prática, refere-se à dificuldade de implementação do direito ao apagamento e/ou custos envolvidos no processo[174]. Isso porque, é próprio desse tipo de tecnologia a implementação de mecanismos e medidas contra falhas no sistema suficientes para causar perdas significativas e corrupção dos processos, como por exemplo os *backups* automáticos e a capacidade de acessar versões anteriores do banco de dados. Isso não só é essencial ao bom funcionamento e segurança do sistema, mas também constitui uma obrigação legal decorrente do artigo 32.º do RGPD, principalmente em relação ao n.º 1, *c)*.

Nesse tocante, é mister mencionar já ter o TJUE decidido acerca do direito ao esquecimento – com base em construção jurisprudencial antes mesmo da entrada em vigor do RGPD – no famoso caso, aqui já referido, envolvendo *Google Spain* e a Agência Espanhola de Proteção de dados e Mario Costeja González[175]. Na ocasião o Tribunal já se manifestou sobre o conflito entre direitos fundamentais evidenciado entre o direito do titular à sua vida privada e à proteção de seus dados e o interesse económico do motor de busca, bem como o dos internautas em aceder a informações pessoais através do motor de busca. Ainda, o acórdão, do ponto de vista material, afirma expressamente que o dever de apagamento não induz à necessidade de suprimir totalmente a página dos índices do motor de busca, mas tão somente à

---

[173] FORTI, Mirko. *Op. Cit.* pp. 39.
[174] CABRAL, Tiago Sérgio. *Op. Cit.* p. 383.
[175] Caso *Google Spain* contra AEPD (C‑230/14, EU:C:2014:317). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN

desindexação desse resultado à busca pelo nome da pessoa[176]. Por esse motivo, Cabral[177] defende não coincidirem o "direito à não indexação", reconhecido no acórdão, e o "direito a ser esquecido", tal qual expressamente previsto no RGPD, para o autor de modo significativamente mais desenvolvido.De qualquer forma, é oportuno ressaltar que o TJUE traçou limites desse direito ao esquecimento (ou à não indexação) que, longe de absoluto, deve ser exercido em consideração aos demais interesses envolvidos, e em harmonia com os direitos fundamentais de terceiros, sobretudo se pensarmos nas hipóteses em que da confiabilidade do sistema depende a proteção à saúde e, consequentemente, o direito à vida, como nos casos envolvendo dispositivos *e-Health*.

Para Cabral[178], todavia, essa não é um incompatibilidade incontornável, pois embora os padrões estabelecidos pelo *machine learning* demandem a maior quantidade possível de dados pessoais acumulados, os padrões em si não se referem a nenhuma pessoa em específico, de modo que essas "regras" resultantes dos processamentos dos dados, não podem ser considerados dados pessoais e, por isso, não estão sujeitos ao apagamento. Para ilustrar, o autor apresenta o exemplo de uma aplicação que identifica quando as pessoas que estão posando para uma fotografia se encontram a sorrir e de olhos abertos. Para que o dispositivo "aprenda" a identificar essas circunstâncias são fornecidas milhares de fotografias de pessoas com variados tipos de sorrisos e cores dos olhos. Da análise de todas essas fotografias (dados pessoais), o algoritmo define padrões que irá utilizar para aferir se as pessoas estão ou não a sorrir. Esses padrões não remetem a nenhuma pessoa e é impossível estabelecer de qual fotografia o sistema extraiu determinada informação, pois o modelo corresponderia à representação de todos os dados pessoais agregados.

Por isso, o autor conclui que a realidade da inteligência artificial pode ser conciliada com as regras do RGPD, cabendo aos desenvolvedores desse tipo de tecnologia ter em conta: a) a necessidade de implementar algoritmos resistentes ao apagamento dos dados, utilizando as estratégia de *privacy by design* e *privacy by defalt*; b) garantir uma volumosa quantidade de

---

[176] A esse respeito, destaca-se a análise do GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. *Diretrizes para a Execução do Acórdão do Tribunal de Justiça da União Europeia no Processo c-131/12, Google Spain sl e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Novembro, 2014. Disponível em https://ec.europa.eu/newsroom/article29/items/667236/en [Consulta em Agosto de 2021].

[177] CABRAL, Tiago Sérgio. *Forgetful AI: AI and the Right to Erasure under the GDPR*. European Data Protection Law Review, 2020. Vol. 9, nº 3. pp. 381.

[178] CABRAL, Tiago Sérgio. *Op. Cit.* p. 385.

dados para diminuir o impacto do apagamento, se possível mediante anonimização; c) evitar tanto quanto possível o tratamento de dados com base no consentimento ou no interesse legítimo, dando preferência para o estabelecimento de uma relação contratual[179].

Conclusão

A noção de privacidade apresenta contornos fluidos que se contraem e se dilatam a depender do contexto histórico e social. Nesse aspeto, a tecnologia sempre exerceu relevante influência no conceito e impulsionou a proteção jurídica do bem. É da evolução da noção de privacidade e do desenvolvimento tecnológico relativo ao processamento de dados que surge o direito à proteção de dados.

Por sua vez, a Internet das Coisas representa a evolução da internet e concretiza realidade antes restrita às obras de ficção científica, inaugurando uma nova era tecnológica e ensejando a demanda por regulamentação dessa atividade.

Já o Regulamento Europeu de Proteção de Dados, embora recentemente aprovado, surge como resultado da evolução histórica da legislação de proteção de dados pessoais ao logo de décadas e assenta-se, portanto, em conceitos e premissas que remontam a períodos em que o progresso tecnológico alcançava níveis consideravelmente inferiores de automação e dependia quase integralmente da intervenção humana para realização dos processos.

Estabelece-se, então, um aparente paradoxo em que o avanço tecnológico é ao mesmo tempo causa da necessidade por regulamentação do tratamento de dados pelo Estado, mas também sua velocidade pode representar uma obsolescência dessas regras.

Contudo, por todo o exposto neste trabalho, conclui-se que essa contradição é meramente aparente e, se acompanhado de uma intepretação sistemática e atenta ao contexto tecnológico, o RGPD representa um avançado sistema de regras suficiente a garantir a proteção de dados e a privacidade dos titulares, sem se impor óbices desproporcionais ao desenvolvimento tecnológico. Mais do que nunca, faz-se necessário dos operadores do direito um olhar para o texto normativo nunca desassociado das peculiaridades de cada realidade tecnológica e sempre mediante a ponderação dos vários interesses e direitos envolvidos. O verdadeiro desafio está exatamente nessa compatibilização entre a estabilidade das regras postas e a ebulição do mundo tecnológico com suas constantes e velozes mudanças.

---

[179] CABRAL, Tiago Sérgio. *Op. Cit.* p. 388.

A eventual defesa da inaplicabilidade do RGPD ao mundo da Internet das Coisas pode resultar em uma total e danosa desproteção dos direitos da personalidade, bem como na construção de um ambiente tecnológico inseguro e lesivo até mesmo ao desenvolvimento enconómico. Igualmente, não nos parece o melhor caminho a defesa de uma mudança constante da lei a reboque das evoluções tecnológicas, sob pena, mais uma vez, de se sacrificar a necessária segurança jurídica.

Assim, entendemos que o Regulamento Geral de Proteção de Dados quando bem interpretado constitui importante ferramenta para a pacificação dos conflitos em relação aos dispositivos de *IoT*, não só por possibilitar o desenvolvimento e aprimoramento da tecnologia, mas por direcioná-los ao fim de garantir o bem-estar das pessoas, tendo como norte os direitos da personalidade atrelados aos interesses económicos.

Referências Bibliográficas.

ASHTON, Kevin. *That 'Internet of Things' Thing*. RFID Journal. Junho/2009. Disponível em https://www.rfidjournal.com/that-internet-of-things-thing [Consulta em Fevereiro de 2021]

BARBOSA, Mafalda Miranda. *Proteção de dados e direitos de personalidade: uma relação de interioridade constitutiva. Os beneficiários da proteção e a responsabilidade civil*. Estudos de Direito do consumidor, N.º 12, Coimbra, Centro de Direito do Consumo/FDUC, 2017. Pp. 75-131.

BETKIER, Marcin. *Privacy Online, Law and the Effective Regulation of Online Services*. Cambridge, Intersentia, 2019.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento.* Rio de Janeiro, Forense, 2019.

BRASHER, Elizabeth A. *Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation*. Columbia Business Law Review, 2018, nº 1, pp. 209-253. Disponível em < https://heinonline.org/HOL/Page?handle=hein.journals/colb2018&id=215&collection=journals&index=# > , [Consulta em Agosto de 2021]

CARVALHO, Orlando de - *Teoria Geral do Direito Civil.* 3ª ed.. Coimbra. Coimbra Editora, 2012.

CABRAL, Tiago Sérgio. *Forgetful AI: AI and the Right to Erasure under the GDPR*. European Data Protection Law Review, 2020. Vol. 9, nº 3. pp. 378-389.

CAPISIZU, Larisa-Antonia. *Legal Perspectives on the Internet of Things*. Conferinta Internationala de Drept, Studii Europene si Relatii Internationale. Maio de 2018. pp.523-532. Disponível em https://heinonline.org/HOL/Page?public=true&handle=hein.journals/cidstue2018&div=55&start_page=523&collection=journals&set_as_cursor=0&men_tab=srchresults [Consulta em Agosto de 2021]

COMITÉ ECONÓMICO E SOCIAL EUROPEU. *Parecer sobre "Confiança, privacidade e segurança para os consumidores e as empresas na Internet das coisas (IdC)*" Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018IE1038&qid=1625339548895&from=PT [Consulta em Julho de 2021]

COMITÉ EUROPEU DE PROTEÇÃO DE DADOS (CEPD). *Diretrizes 3/2018 sobre o âmbito de aplicação territorial do RGPD (artigo 3.º)*, versão 2.0, de 12/11/2019. Disponível em

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_pt.pdf [Consulta em Agosto de 2021]

CORDEIRO, António Barreto Menezes. *Direito da Proteção de Dados*: *à luz do RGPD e da Lei nº 58/2019.* Coimbra, Almedina. 2020.

CORDEIRO, António Barreto Menezes. *O consentimento do titular dos dados no RGPD*. Em FinTech: desafios da tecnologia financeira. coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte. Vol. 2. Almedina. Coimbra, 2017. Pp. 33-56.

CORREIA, Victor. *Sobre a Privacidade*. Sinapsis Editores, 2016.

CORÔA, Marília de Mello e Silva. *O Mercado De Dados: Estrutura, Funcionamento e o Reflexo do RGPD no Novo Mercado à Base De Dados Pessoais*. Dissertação (Mestrado em Ciências Jurídico-civilísticas) Faculdade de Direito da Universidade do Porto. Porto, 2020.

CREMONA, Marise. *New Technologies and EU Law*. Oxford, Oxford University Press, 2017.

DE CONCA, Silvia. *Between a rock and a hard place: Owners of smart speakers and joint control*, SCRIPTed, 2020. Vol. 17, n. 2. Pp. 238-268.

DIAS, Carlos André Ferreira. *A Privacidade na era da Internet das Coisas: direiros de personalidades e proteção de dados*. Dissertação (Mestrado em Ciências Jurídico-civilísticas) Faculdade de Direito da Universidade do Porto. Porto, 2019.

ELVY, Stacy-Ann. *Contracting in the age of the internet of things: article of the ucc and beyond.* Hofstra Law Review, 2016, Vol. 44, nº 3. p. pp. 839-932. Disponível em https://heinonline.org/HOL/Page?public=true&handle=hein.journals/hoflr44&div=40&start_page=839&collection=journals&set_as_cursor=0&men_tab=srchresults [Consulta em Agosto de 2021]

FABIANO, Nicola. *Internet of Things and the Legal Issues Related to the Data Protection Law according to the New European General Data Protection Regulation*. Athens Journal of Law, 2017. Volume 3. pp. 201-214.

FORTI, Mirko. *The Deployment of Artificial Intelligence Tools in the Health Sector: Privacy Concerns and Regulatory Answers within the GDPR. European Journal of Legal*

Studies, 2021. Vol. 13, nº 1. pp. 29-44.

GOLDSTEIN, K. (2019). *Cyber beware: Iot technology growing explosively*. International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel, 2019, Vol. 3, nº 6. pp. 7-13. Disponível em https://heinonline.org/HOL/P?h=hein.journals/idpp3&i=131. [Consulta em Agosto de 2021]

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS.

-*Diretrizes para a Execução do Acórdão do TJUE no Processo c-131/12, Google Spain sl e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Novembro, 2014. Disponível em https://ec.europa.eu/newsroom/article29/items/667236/en [Consulta em Agosto de 2021].

-*Opinion 3/2013 on purpose limitation.* Abril, 2013. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [Consulta em Julho de 2021].

-*Opinion 8/2014 on the on Recent Developments on the Internet of Things*. Setembro, 2014. Disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf [Consulta em Julho de 2021].

-*Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679*. Outubro, 2017. Rev. Fevereiro, 2018. Disponível em file:///C:/Users/User/Downloads/guideline%20decis%C3%B5es%20automatizadas%20e%20profilling.pdf [Consulta em Agosto de 2021].

-*Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679*. Novembro, 2017. Disponível em file:///C:/Users/User/Downloads/20180416_article_29_wp_guidelines_on_consent_publish_09A6854F-F638-8898-7A0543CE0857250F_51030.pdf [Consulta em Agosto de 2021].

-*Orientações relativas à transparência na aceção do Regulamento 2016/679*. Novembro, 2017. Disponível em https://www.uc.pt/protecao-de-dados/suporte/20180411_orientacoes_relativas_a_transparencia_wp260_rev01 [Consulta em Agosto de 2021].

GUIMARÃES, Maria Raquel e REDINHA, Maria Regina. *Through the Keyhole: Privacy in COVID-19 Times - A Portuguese Approach*. Intersentia Online. 2020. Disponível em https://www.intersentiaonline.com/publication/coronavirus-and-the-law-in-europe/2. [Consulta em Agosto de 2021]

FRIAS, Hélder. *A Internet de Coisas (IoT) e o Mercado Segurador*. Em FinTech: desafios da tecnologia financeira. coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte. Vol. 1. Almedina. Coimbra, 2017. pp. 219-233.

KAMARINOU, Dimitra; MILLARD, Christopher; e SINGH, Jatinder. *Machine Learning with Personal Data*. Em LEENES, Ronald. *et al*. Data Protection and Privacy: The Age of Intelligent Machines. Oxford, Hart, 2017. pp. 89-112.

LA DIEGA, Guido Noto. *Internet of things and patents: Towards the iot patent wars*. Journal of Commercial and Intellectual Property Law, 2017, Vol. 3, nº. 2. pp. 47-66. [Consulta em Agosto de 2021] Disponível em https://heinonline.org/HOL/Page?handle=hein.journals/tfm2017&id=223&collection=journals&index=

LUGER, Ewa e ROSNER, Gilad. *Considering the Privacy Design Issues Arising from Conversation as a Platform*. Em LEENES, Ronald. Et al. Data Protection and Privacy: The Age pf Intelligent Machines. Oxford, Hart, 2017. pp. 193-211.

MAGRANI, Eduardo. *A Internet das Coisas*. Rio de janeiro, FGV Editora, 2018.

NAHMIAS, Yifat. e PEREL, Maayan.. *The Oversight of Content Moderation by AI: impact assessments and their limitations*. Harvard Journal on Legislation, 2021. Vil. 58, nº 1. pp. 145-194.

ODREASOVA, Eva. *Personality Rights in Different European Legal Systems: Privacy, Dignity, Honour and Reputation.* Em OLIPHANT, Ken; PINGHUA, Zhang; e LEI, Chen. The Legal Protection of ersonality Rights: Chinese and European perspectives. Leiden. Brill, 2018. Pp. 24-70.

OLIVEIRA, Madalena Perestrelo de. *Definição de Perfis e Decisões Automatizadas no Regulamento Geral sobre a Proteção de Dados*. Em Em FinTech: desafios da tecnologia financeira. coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte. Vol. 2. Almedina. Coimbra, 2017. pp. 61-88.

PAGALLO, Ugo. *The legal challenges of Big Data: putting secondary rules first in the field of EU Data Protection.* European Data Protection Law Review (EDPL), 2017. Vol. 3. Nº. 1. pp.36-46.

PAGALLO, Ugo, MASSIMO, Durante, e MONTELEONE, Shara. *Whats is New with the Internet of Things in Privacy and Data Protection? For Legal Chalenges on Sharing and Control in IoT*. Em LEENES, Ronald, et al. Data Protection and Privacy: (In)visibilities and Infrastructures. Cham: Springer, 2017. (Law, governance and technology series). pp. 59-78.

PEPPET. Scott R. *Freedom of Contract in Augmented Reality*. Em Research Handbook on the Law of Virtual and Augmented Reality. Edward Elgar. Chelteham, 2020. p. 609/635.

PEPPET, Scott R., *Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent.* Texas Law Review, 2014.

PINHEIRO, Alexandre Sousa. *Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*. AAFDL. Lisboa, 2015.

PINHEIRO, Alexandre Sousa, *et al. Comentário ao regulamento geral de proteção de dados*. Almedina, 2018.

PINTO, Paulo Mota. *Direitos de Personalidade e Direitos Fundamentais: estudos*. Coimbra. Gestlegal, 2018. p. 478.

ROUVROY, Antoinette. "*Of Data and Men": Fundamental Rights and Freedoms in a World of Big Data*. Council of Europe, Directorate General of Human Rights and Rule of Law, 2016. Disponível em https://rm.coe.int/16806a6020 [Consulta em Agosto de 2021]

SARMENTO E CASTRO, Catarina. *40 anos de "Utilização da Informática" - O artigo 35.º da Constituição da República Portuguesa*. Revista e-Pública, Vol. 3, N.º 3, 2016. pp. 42/66. Disponível em https://www.e-publica.pt/volumes/v3n3a04.html [Consulta em Agosto de 2021]

SIEGEL, Jeremy. *When the Internet of Things Flounders: Looking into GDPR-Esque Security Standards for IoT Devices in the United States from the Consumers' Perspective.* Journal of High Technology Law, 2020, Vol. 20, n.º 1. pp. 189-229. Disponível em https://heinonline.org/HOL/Page?handle=hein.journals/jhtl20&id=189&collection=journals&index= [Consulta em Agosto de 2021]

SOLOVE, Daniel J. *The Digital Person.* New York and London. New York University Press, 2004.

TAYLOR, Roger. *No privacy without Transparency*. Em LEENES, Ronald. et al. Data Protection and Privacy: The Age of Intelligent Machines. Oxford, Hart, 2017. pp. 63-85.

TOMÉ, Herminia Campuzano. *Vida Privada y Datos Personales: Su Protección Jurídica Frente a La Sociedad de la Información.* Tecnos. Madrid, 2000.

TSCHIDER, Charlotte A. *Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age*. Denver Law Review, 2018-2019, Vol. 3, Nº. 3. pp. 87-144.

WARREN, Samuel D. e BRANDEIS, Louis D. *The Right to Privacy*. Harvard Law Review, 1890, Vol. IV, Nº. 5. pp. 193-220.

YU, Peter K., *Beyond Transparency and Accountability: Three additional features algorithm designers should build into intelligent platforms*. Northeastern University Law Review, 2021, Vol. 13, Nº. 1. pp. 263-296.

ZARSKY, Tal Z. *Incompatible: The GDPR in the Age of Big Data.* Seton Hall Law Review. Vol. 47, nº 4, 2017. pp. 995-1020. *Disponível em* https://heinonline.org/HOL/P?h=hein.journals/shlr47&i=1019 [Consulta em Julho de 2021]

ZARSKY, T. Z., *Desperately Seeking Solutions: Using implementation-based solutions for the troubles of information privacy in the age of data mining and the internet society*. Maine Law Review, 2004, Vol. 56, Nº 1. pp. 13-60. Disponível em: https://heinonline.org/HOL/Page?public=true&handle=hein.journals/maine56&div=7&start_page=13&collection=journals&set_as_cursor=0&men_tab=srchresults [Consulta em Agosto de 2021].

Índice