UNIVERSIDADE DE BRASÍLIA

FACULDADE DE DIREITO

GRADUAÇÃO EM DIREITO

AMANDA BRAGA FERREIRA

UE *VS*. EUA: UMA ANÁLISE COMPARATIVA DO CAMPO JURÍDICO DA REGULAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS E DA INTELIGÊNCIA ARTIFICIAL NO OCIDENTE

Brasília/DF

2023

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE DIREITO

GRADUAÇÃO EM DIREITO

AMANDA BRAGA FERREIRA

UE *VS.* EUA:

uma análise comparativa do campo jurídico da regulação da proteção de dados pessoais e da inteligência artificial no Ocidente

Monografia apresentada à Banca Examinadora da Faculdade de Direito da Universidade de Brasília, campus Darcy Ribeiro, como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador: Professor Doutor Alexandre Kehrig Veronese Aguiar

Brasília/DF

2023

AGRADECIMENTOS

Antes de qualquer um, agradeço aos meus pais, Sara e Luciano. Além da própria vida e das condições materiais para chegar até aqui, vocês me agraciaram com cuidado, sabedoria, força e amor, incondicionalmente. A história de vocês serviu como inspiração a cada dia e eu guardo no coração cada um dos seus conselhos, mesmo quando insisto em seguir o meu caminho. Filhos são filhos e pais são pais, e a minha gratidão não pode ser devidamente expressa em algumas palavras, mas espero que saibam que eu não teria chegado até aqui sem vocês. E irei muito além, por e com vocês.

Agradeço à minha avó Dorca, de sabedoria e determinação infinitas. A senhora abriu o Mar Vermelho para a nossa família, com sua mente ousada e seu espírito inabalável, que lutou pelas e para as gerações que te seguiram e vão te seguir. Para mim, a senhora é uma eterna saudade e a maior fonte de inspiração. Espero, algum dia, levar o seu legado adiante, ensinando e mudando a vida de muitos.

Agradeço aos meus avós Sirlene e Francisco. Sou grata pelo amor e pelo carinho de vocês. Os senhores, também, são raízes da nossa família e eu só tenho a aprender com os seus corações tão doces e fortes.

Agradeço ao meu avô, Paulo, um dos maiores contadores de “estórias” e “histórias” que já conheci.

Agradeço ao meu irmão, Daniel, que, com todas as nossas diferenças, me incentiva e me inspira a ser melhor.

Agradeço ao meu amor, Mateus, que aposta em mim em todas as situações, de olhos fechados. Obrigada por confiar em mim, mesmo quando eu mesma não fui capaz disso. Obrigada por torcer por mim, de forma tão verbal e tão amorosa, tanto nos meus momentos de força quanto nos de fragilidade. Você me inspira a ser uma pessoa melhor.

Agradeço às minhas amigas, Alice, Ana e Júlia. Há mais de uma década vocês me acompanham, testemunhando do meu pior e do meu melhor, e ainda estão aqui. Quando as vejo, sinto como se suas conquistas também fossem minhas, por isso, não posso deixar de dizer: esta vitória também é de vocês.

Agradeço ao grande amigo – e professor – José Péricles. A experiência de estagiar é naturalmente enriquecedora, mas ter o senhor como supervisor, sem dúvidas, foi um catalisador no meu crescimento, não só profissional, mas acadêmico e pessoal.

Agradeço ao meu orientador, o professor Alexandre Kehrig Veronese Aguiar. O meu primeiro contato com o senhor foi no terceiro semestre, na disciplina de Sociologia Jurídica. Ali, conheci uma visão diferente do Direito, não só pelo conteúdo apresentado, mas também pela proposta didática diferente e comprometida com os alunos. O senhor ajudou a instigar, em mim, o interesse pela pesquisa acadêmica, o qual vigorou com as oportunidades e a honra de tê-lo como orientador nos projetos de iniciação científica. O senhor serviu como um exemplo do *ser* cientista no Brasil. Apesar de lamentar pelas dificuldades que a comunidade científica enfrenta, me motivo por figuras como o senhor, que tiram o melhor de cada oportunidade para aperfeiçoar o ensino universitário e a academia brasileiros.

Agradeço aos examinadores da banca: Alexandre Araújo Costa, Ana de Olivera Frazão e Amanda Nunes Lopes Espiñeira Lemos. Os senhores foram escolhidos não só por serem especialistas na área, mas também com base na minha profunda admiração por cada um. Tenho nos senhores um referencial acadêmico que marcará a minha trajetória definitivamente.

Agradeço à Universidade de Brasília e aos meus professores ao longo do curso na Faculdade de Direito: meus agradecimentos por me mostrarem como o ensino público tem, não só salvação, mas muito potencial.

Eu não cheguei aqui apenas por sorte, ou coincidência, mas por uma conjunção de bençãos que me sustentaram, todos os dias, e eu não posso deixar de reconhecer o meu privilégio. Apesar de ser apenas o encerramento da graduação, espero, como futura jurista, contribuir para a sociedade – para que o Direito não seja apenas campo de disputa pelo poder ou instrumento da argumentação, mas uma ferramenta para a Justiça. Este é o início do meu pequeno-grande legado e eu espero fazer jus à Faculdade de Direito que me formou.

RESUMO

No cenário internacional do desenvolvimento das tecnologias digitais e, consequentemente, da sua regulação, a União Europeia e os Estados Unidos da América são dois dos agentes mais relevantes. Esses gigantes geopolíticos são sujeitos historicamente conhecidos pelos seus projetos de dominação, notavelmente por meio das políticas colonialistas e imperialistas, as quais teriam sido, em tese, abandonadas na contemporaneidade. Sem embargo, em princípio, os modelos regulatórios da proteção de dados e da inteligência artificial, no âmbito europeu e no estadunidense, parecem encontrar-se em constante conflito pelo exercício de maior influência sobre o ordenamento de outros países, sendo possível notar, em nome da globalização ou da internacionalização, nuances de poder simbólico que estende-se até mesmo para as políticas regulatórias. Dessa forma, este trabalho pretende analisar comparativamente essas duas matrizes regulatórias, a partir da teoria de Pierre Bourdieu, em especial por meio do emprego dos conceitos de campo e poder simbólico, com o propósito de explorar suas similitudes e diferenças jurídico-políticas e compreender o possível uso do discurso da internacionalização como uma forma de retomar a influência para além de suas fronteiras.

Palavras-chave: regulação**;** proteção de dados; inteligência artificial; União Europeia; Estados Unidos da América; Pierre Bourdieu.

ABSTRACT

In the international landscape of digital technology development and, consequently, its regulation, the European Union and the United States of America are two of the most important players. These geopolitical giants are subjects historically known for their domination projects, notably through colonialist and imperialist policies, which have supposedly been abandoned in the contemporary age. However, in principle the regulatory models for data protection and artificial intelligence, in both Europe and the United States, seem to be in constant conflict over the influence they have on countries' legal systems, and it is possible to see nuances of a symbolic power that extends even to regulatory policies in the name of globalization or internationalization. In this way, this paper aims to analyze comparatively these two regulatory matrices, based on Pierre Bourdieu's theory, especially through the concepts of field and symbolic power, with the purpose of exploring their legal-political similarities and differences and understanding the possible use of the discourse of internationalization as a way of regaining influence beyond their borders.

Keywords: regulation; data protection; artificial intelligence; European Union; United States of America; Pierre Bourdieu.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

Carta dos Direitos Fundamentais da União Europeia – CDFUE

Departamento de Comércio – DoC

Departamento de Transporte – DoT

Diretiva 95/46/CE – Diretiva

Federal Trade Commission – FTC

Inteligência Artificial – IA

Lei Federal de Gestão da Segurança da Informação de 2002 – FISMA

Lei Gramm-Leach-Bliley ou Lei de Modernização dos Serviços Financeiros de 1999 – GLBA

Lei de Portabilidade e Responsabilidade de Seguros de Saúde de 1996 – HIPAA

Lei de Privacidade de Comunicação Eletrônica de 1986 – ECPA

Lei de Proteção e Privacidade Online Infantil de 1998 – COPPA

Lei de Vigilância de Inteligência Estrangeira de 1978 – FISA

Ordem Executiva – OE

Organização das Nações Unidas – ONU

Organização para a Cooperação e Desenvolvimento Econômico – Regulamento Geral de Proteção de Dados – RGPD

Quadro de Privacidade de Dados UE-EUA – QPD UE-EUA

Tratado sobre o Funcionamento da União Europeia – TFUE

Tribunal de Justiça da União Europeia – TJUE

Grupo de Alto Nível em IA – AI HLG

SUMÁRIO

INTRODUÇÃO

No estudo das ciências sociais, muito se fala em *poder*. As lentes de estudo desse conceito são diversas, cabendo citar, a título de exemplo, a econômica, a racial, a de gênero, a religiosa, a linguística, entre outras – uma lista, talvez, infinita, comparando-se as variadas nuances que pode assumir.

No Direito, como ciência social aplicada, o poder assume um papel também central. Na sua base científica, tem-se teorias como o *juspositivismo* e o *jusnaturalismo*, que buscam explicar os fundamentos de existência da norma e do ordenamento jurídico – no primeiro caso, a norma como o direito *posto*, reduzido ao enunciado da lei e determinado pela vontade dos homens; no segundo, como a tradução de um direito *natural*, a partir de uma racionalidade superior e independente da vontade humana.

Empregando as lentes da teoria Pierre Bourdieu, é possível notar que a determinação do Direito se dá a partir de uma perspectiva *internalista*, na qual busca legitimar-se a si mesmo a partir de sua lógica intrínseca, notada nas próprias normas e na interação entre os juristas; e uma perspectiva *externalista*, que indica que o poder jurídico é um reflexo de outras relações de força existentes, tal qual a econômica e a política (Bourdieu, 2022). Nesse contexto, cabe apresentar o conceito do autor de *campo jurídico*, que entende como:

> (...) o lugar de concorrência pelo monopólio do direito de dizer o direito, quer dizer, a boa distribuição (nomos) ou a boa ordem, na qual se defrontam agentes investidos de competência ao mesmo tempo social e técnica que consiste essencialmente na capacidade reconhecida de interpretar (de maneira mais ou menos livre ou autorizada) um corpus de textos que consagram a visão legítima, justa (*), do mundo social (Bourdieu, 2022, pp. 220-221).

De toda forma, para que uma norma seja transposta ao ordenamento jurídico, é necessária alguma intervenção de poder. Na Modernidade, diante do paradigma do Estado Democrático de Direito e da ascendência do neoconstitucionalismo, essa função é exercida pela constituição, legitimadora de todas as outras normas, inclusive daquelas de natureza regulatória.

Marcio Iorio Aranha, em Manual de Direito Regulatório, trata da relação entre a norma constitucional e a função do Estado:

> O Estado, enquanto produto constitucional, encarna as medidas de poder – competências – delegadas pelo documento constitucional nos limites das finalidades para quais foram criadas – funções. Desse batimento entre suas competências e funções, têm-se sua identidade jurídica: o Estado é um centro de atributos jurídicos qualificado pela intensa incidência do direito público via manifestação de aspectos sobreviventes da soberania, tais como a possibilidade jurídica do uso da força física e sua exclusividade, e a não-oponibilidade interna e externa para afirmação do ordenamento jurídico vigente (Aranha, 2021, p. 3).

Portanto, o Estado (Regulador) é um dos agentes que promove a regulação, sendo responsável pela "garantia de preservação das prestações materiais essenciais à fruição de direitos fundamentais" (Aranha, 2021, p. 11), de maneira que "a especificação de dito conteúdo exige a análise do dispositivo normativo, como cristalização cultural que é, associado aos influxos de transformações das ideias legislativas, jurisprudenciais, sociais, enfim, da realidade cultural circundante" (Aranha, 2021, p. 11).

Dessa forma, os Poderes Legislativo e Judiciário, essencialmente relacionados à ideia de lei, são acompanhados pelo aparato administrativo do Estado, com vistas à persecução dos objetivos constitucionalmente consagrados.

Nesse contexto, ganham relevância a regulação, no seu sentido amplo, e as políticas públicas, estas sendo, em essência, as opções políticas feitas frente às "restrições e condições" (Martins, 2022, p. 18) da atuação governamental, ou mesmo o "instrumento capital da atividade governativa" (Berenguer, 2020, p. 35). De fato, a própria legitimidade democrática do Estado Regulador é fundada na sua natureza de "partícipe necessário da decisão política" (Aranha, 2021, p. 19).

A regulação da proteção de dados pessoais e da inteligência artificial, objeto de estudo deste trabalho, também parte desses pressupostos gerais sobre poder e regulação, com o diferencial de que o ambiente regulatório tecnológico é inerentemente rápido, volátil e relativamente inexplorado. Falar em tecnologia implica em falar em inovação, com todos as suas benesses e riscos, e, sem dúvida, com a apresentação de novos desafios à sociedade.

A proteção de dados pessoais tem origem no direito à vida privada e passou a ser tratada como um direito específico já nos anos 1970. Na década seguinte, alguns instrumentos internacionais foram criados, com destaque para as *Diretrizes* da *Organização para Cooperação e Desenvolvimento do Econômico* de 1980 (OCDE) e a *Convenção 108 do Conselho da Europa,* de 1981, sobre as quais Alexandre Veronese disserta:

> O ponto central para a OCDE, portanto, era formar diretrizes que pudessem dotar os países de leis nacionais que fossem compatíveis entre si e, assim, oferecer a possibilidade de se construir um regime internacional de proteção à privacidade e aos dados pessoais. O documento da OCDE, de 1980, interpretava já haver prescrições jurídicas internacionais relacionadas à garantia da liberdade de informação e à proteção da privacidade, tais como a Convenção Europeia de Direitos do Homem (1950) e o Pacto Internacional sobre os Direitos Civis e Políticos (1966). (...) Os oito princípios das Diretrizes da OCDE formam um conjunto útil de elementos para proteção dos dados pessoais e da privacidade. As Diretrizes vigoraram de 1980 até 2013, em sua formulação original.
>
> (...)
>
> O segundo documento internacional sobre o tema da proteção à privacidade e aos dados pessoais é a Convenção 108, do Conselho da Europa. Preliminarmente, contudo, é necessário explicar o que é o Conselho da Europa e que o mesmo não deve ser confundido com a União Europeia ou com algum dos seus órgãos.
>
> Pela exposição anterior – sobre as Diretrizes da OCDE – deve ter ficado claro que o Conselho da Europa estava a discutir uma convenção sobre proteção de dados pessoais para ser aprovada naquele final da década de 80 do século passado. Isso veio a ocorrer em janeiro de 1981. O documento é conhecido como a Convenção 108 do Conselho da Europa. Como é comum em relação aos tratados internacionais, a Convenção foi sendo assinada e ratificada paulatinamente pelos quarenta e sete países que compõem o Conselho da Europa. Cabe notar que nove países externos ao Conselho assinaram e ratificaram o tratado. Entre eles, é possível citar o México, a Argentina e o Uruguai. A diferença mais relevante entre a Convenção 108 e as Diretrizes da OCDE é que a primeira constitui normas jurídicas cogentes para os Estados que a firmaram ou aderiram (Veronese, 2021, pp. 694-695).

A partir dos anos 1990, portanto, ocorreu a verdadeira ascensão do debate sobre a proteção de dados pessoais, com o aumento da produção de leis nacionais, instrumentos multilaterais e outros marcos regulatórios sobre o assunto.

Inicialmente, esse debate assumiu uma perspectiva limitada à proteção de dados como um desdobramento da privacidade. Contudo, o lapso temporal permitiu o desenvolvimento e a consolidação não somente da produção científica, mas também legislativa sobre proteção de dados, de sorte que, cada vez mais, esse direito é associado "à autodeterminação informativa e a direitos fundamentais da mais alta importância, como a liberdade, a igualdade e a própria cidadania" (Frazão, 2021, p. 34).

Ademais, a comunidade científica já possui consensos acerca de certos conceitos e práticas ideais, como é o caso das noções de *privacy by design* e *privacy by default*:

> A primeira diz respeito ao fato de que, quando algum agente decide realizar qualquer tipo de tratamento de dados pessoais, deve pensar na privacidade em cada passo, o que inclui projeto, desenvolvimento de produtos e softwares, sistemas de informática, dentre outros, a fim de assegurar que a privacidade será garantida durante todo o ciclo do tratamento. Já a segunda diz respeito ao fato de que, ao lançar qualquer produto ou serviço ao público, as regras mais protetivas de tutela da privacidade devem ser

> aplicadas, sem que se exija do usuário qualquer iniciativa para tal propósito (Frazão, 2021, p. 48).

Igualmente, diversos países – ou agrupamentos de países – possuem alguma produção normativa no sentido da regulação de proteção de dados, muitos deles possuindo sistemas próprios e complexos, "ora mais severos, ora mais flexíveis" (Veronese, Mendonça; 2022; p. 95).

Nesse contexto, Alexandre Veronese e Luiza Mendonça destacam o fato de que as variações entre modelos regulatórios podem "ocasionar distorções regulatórias, já que o regime de proteção em determinados países poderia ser mais flexível justamente com o intuito de atrair diferentes empresas e negócios para o seu território" (Veronese, Mendonça; 2021; p. 95). Tal comentário não é apenas uma possibilidade, mas demonstra uma verdadeira propensão percebida no eixo Ásia-Pacífico.

Por outro lado, a inteligência artificial (IA), apesar de ter o seu desenvolvimento iniciado entre os anos de 1943 e 1955 (Russell, Norvig; 2022; p. 35), somente passou a se tornar objeto de interesse pelos legisladores a partir dos anos 2010.

Isso porque, apesar de ter se tornado uma indústria já no final dos anos 1980, passou posteriormente por um período de estagnação, muito relacionado às dificuldades estruturais e de base, atualmente superadas por um amplo desenvolvimento de tecnologias de armazenamento e processamento e auxiliadas pela alta disponibilidade de dados, associada ao fenômeno do *bigdata*[1].

Em face da prosperidade do desenvolvimento científico tardio da IA, Ryan Calo aponta que muito recentemente os legisladores passaram a se atentar para um mundo tecnológico que já existia há anos. A partir de 2016, nos EUA, começaram a ser feitos estudos pelo Comitê de Energia e Comércio, pelo Comitê Econômico Conjunto e pela Casa Branca de Barack Obama; enquanto Japão e União Europeia (UE) também podem ser citados como pioneiros na iniciativa de estabelecer comissões para o debate acerca da Inteligência Artificial (Calo, 2017, p. 2).

A regulação dessa tecnologia, sem embargo, continua um tanto incerta, na medida em que a criação de comissões e a realização de estudos por si só não são suficientes para

[1] Na contemporaneidade, a disponibilidade de dados é enorme, o que é essencial para o desenvolvimento da IA, que se baseia no desenvolvimento de algoritmos. Os algoritmos funcionam com base nos *inputs*, ou seja, com a inserção de dados e informações, e geram, a depender da forma como são estruturados, diferentes *outputs*, ou seja, resultados. Conforme retratado na metodologia, é esse fenômeno que permite uma aproximação e uma comparação, neste trabalho, da regulação da proteção de dados pessoais e da IA.

estabelecer uma política regulatória confiável, o que gera grandes preocupações em relação ao impacto que a implementação de tais tecnologias pode ter na sociedade.

De fato, desde o final do século XX, tem-se registros de receios em relação ao impacto das novas tecnologias, motivo pelo qual a Organização das Nações Unidas (ONU), pela sua Assembleia Geral, editou a Resolução 3384/1975 (XXX), denominada *Declaração sobre o Uso do Progresso Científico e Tecnológico no Interesse da Paz e em Benefício da Humanidade*[2], na qual enuncia alguns valores segundo os quais deveria dar-se o desenvolvimento científico-tecnológico:

> 1. Todos os estados deverão promover a cooperação internacional para garantir que os resultados do progresso científico e tecnológico sejam usados no interesse de fortalecer a paz e a segurança internacionais, a liberdade e a independência, tendo também como objetivo o desenvolvimento econômico e social dos povos e a efetivação dos direitos e liberdades humanos de acordo com a Carta das Nações Unidas.
> 2. Todos os Estados deverão tomar medidas apropriadas para prevenir o uso dos progressos científicos e tecnológicos, particularmente pelos órgãos estatais, para limitar ou dificultar o gozo dos direitos humanos e das liberdades fundamentais da pessoa consagrados na Declaração Universal dos Direitos Humanos, nos Pactos Internacionais de Direitos Humanos e em outros instrumentos internacionais relevantes.
> 3. Todos os estados deverão adotar medidas para garantir que os avanços científicos e tecnológicos satisfaçam as necessidades materiais e espirituais de todos os setores da população.
> 4. Todos os Estados deverão se abster quaisquer atos que utilizem os avanços científicos e tecnológicos com o propósito de violar a soberania e a integridade territorial de outros Estados, de intervir em seus assuntos internos, de fazer guerras de agressão, de sufocar movimentos de libertação nacional ou de seguir políticas de discriminação racial. Tais atos não somente representam flagrante violação da Carta das Nações Unidas e dos princípios do direito internacional, como também representam uma distorção inadmissível dos propósitos que devem orientar o progresso científico e tecnológico em benefício da humanidade.
> 5. Todos os estados deverão cooperar para o estabelecimento, fortalecimento e desenvolvimento da capacidade científica e tecnológica dos países em desenvolvimento com o objetivo de acelerar a realização dos direitos sociais e econômicos dos povos desses países.
> 6. Todos os Estados deverão adotar medidas próprias para ampliar os benefícios da ciência e da tecnologia a todas as camadas da população e a protegê-los, social e materialmente, das possíveis consequências negativas do uso indevido do progresso científico e tecnológico, inclusive sua utilização indevida para violar os direitos do indivíduo ou do grupo, em particular no que diz respeito à vida privada e à proteção da pessoa humana e sua integridade física e intelectual.
> 7. Todos os Estados deverão adotar as medidas necessárias, inclusive de ordem legislativa, a fim de assegurar que a utilização dos avanços da ciência e da tecnologia contribua para a maior realização possível dos direitos humanos e das liberdades fundamentais sem qualquer discriminação de raça, sexo, idioma ou crenças religiosa.

[2] No inglês, *Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Mankind*.

> 8. Todos os Estados deverão adotar medidas eficientes, inclusive de ordem legislativa, para prevenir e evitar a utilização dos avanços científicos em detrimento dos direitos humanos e das liberdades fundamentais da pessoa humana.
> 9. Todos os Estados deverão, sempre que necessário, agir a fim de garantir a conformidade com a legislação que garante os direitos e as liberdades humanas nas condições de progresso científico e tecnológico (Assembleia Geral da ONU, 1975, p. 86, tradução livre)[3].

Apesar das várias mudanças ocorridas desde 1975, muitas das preocupações expressas no passado são as mesmas, ou ao menos são muito próximas daquelas debatidas na atualidade, principalmente no que diz respeito à noção de que deve-se proteger, além dos direitos humanos e fundamentais de forma ampla, a privacidade e a própria personalidade humanas.

Outro ponto interessante é que, apesar de tais declarações terem sido feitas por um organismo internacional, desde então já se tinha consciência da possibilidade de um Estado tentar, por meio do desenvolvimento científico -tecnológico, se sobrepor a outros Estados, em especial aqueles considerados "em desenvolvimento". Por esse motivo, a Assembleia Geral

---

[3] No original, "*1. All States shall promote international co-operation to ensure that the results of scientific and technological developments are used in the interests of strengthening international peace and security, freedom and independence, and also for the purpose of the economic and social development of peoples and the realization of human rights and freedoms in accordance with the Charter of the United Nations.*
2. All States shall take appropriate measures to prevent the use of scientific and technological developments, particularly by the State organs, to limit or interfere with the enjoyment of the human rights and fundamental freedoms of the individual as enshrined in the Universal Declaration of Human Rights, the International Covenants on Human Rights and other relevant international instruments.
3. All States shall take measures to ensure that scientific and technological achievements satisfy the material and spiritual needs for all sectors of the population.
4. All States shall refrain from any acts involving the use of scientific and technological achievements for the purposes of violating the sovereignty and territorial integrity of other States, interfering in their internal affairs, waging aggressive wars, suppressing national liberation movements or pursuing a policy of racial discrimination. Such acts are not only a flagrant violation of the Charter of the United Nations and principles of international law, but constitute an inadmissible distortion of the purposes that should guide scientific and technological developments for the benefit of mankind.
5. All States shall co-operate in the establishment, strengthening and development of the scientific and technological capacity of developing countries with a view to accelerating the realization of the social and economic rights of the peoples of those countries.
6. All States shall take measures to extend the benefits of science and technology to all strata of the population and to protect them, both socially and materially, from possible harmful effects of the misuse of scientific and technological developments, including their misuse to infringe upon the rights of the individual or of the group, particularly with regard to respect for privacy and the protection of the human personality and its physical and intellectual integrity.
7. All States shall take the necessary measures, including legislative measures, to ensure that the utilization of scientific and technological achievements promotes the fullest realization of human rights and fundamental freedoms without any discrimination whatsoever on grounds of race, sex, language or religious beliefs.
8. All States shall take effective measures, including legislative measures, to prevent and preclude the utilization of scientific and technological achievements to the detriment of human rights and fundamental freedoms and the dignity of the human person.
9. All States shall, whenever necessary, take action to ensure compliance with legislation guaranteeing human rights and freedoms in the conditions of scientific and technological developments".

consagrou, há quase 50 anos, a imprescindibilidade do respeito à soberania nacional para que as inovações tecnológicas sirvam adequadamente à humanidade.

O fato é que, ao longo da história, diversos atores internacionais, sujeitos ou não de direito internacional público, têm promovido, dentro e fora de suas fronteiras, uma atuação em prol do que entendem ser a melhor forma de limitar tal desenvolvimento apenas na medida necessária para que não representem um perigo aos indivíduos, sem prejudicar, contudo, as iniciativas de inovação.

A OCDE é um importante ator internacional nesse contexto. Um exemplo disso é o seu relatório *Reguladores da Comunicação para o Futuro*[4], em que anuncia que "a transformação digital está impondo novos desafios às funções e mandatos atuais dos reguladores de comunicação, aos quais os reguladores precisam se adaptar" e que "a principal questão para os formuladores de políticas da OCDE não é mais *se* as estruturas regulatórias precisam mudar, mas sim *como*"[5] (OCDE, 2022, p. 3, tradução livre, destacou-se).

No relatório, além de reforçar as vantagens da implementação de tecnologias no setor de comunicações, a OCDE afirma a necessidade de regular a inovação sem prejudicar seus avanços, sugerindo, inclusive, que não é necessário renunciar às regulações existentes, mas sim adaptá-las para que possam proteger a igualdade de acesso, os direitos dos consumidores, a segurança das comunicações e outros objetivos importantes da regulação.

Nesse ínterim, afirma que cada país possui sua própria "jornada regulatória" (OCDE, 2022, p. 8, tradução livre), mas que será indispensável a adaptação da regulação e dos reguladores, destacando-se o papel da regulação multisetorial e da cooperação entre agentes nacionais e internacionais.

Outro exemplo relevante é a adoção, pela OCDE, da *Recomendação do Conselho para uma Governança Regulatória Ágil para Potencializar a Inovação*[6] (OCDE, 2023b).

Nesse documento, a OCDE define a regulação como um conjunto de instrumentos, estabelecidos pelos governos, aos quais empresas e cidadãos estão sujeitos (OCDE, 2023b). Conceitua, ainda, as políticas regulatórias como um conjunto de "princípios, regras

[4] No inglês. *Communication Regulator for the Future*.
[5] No original, "*The digital transformation is posing new challenges to current roles and mandates of communication regulators to which regulators need to adapt*" e "*The key question for OECD policymakers is no longer whether regulatory structures need to change, but rather how*".
[6] No inglês, *Recommendation of the Council for Agile Regulatory Governance to Harness Innovation*.

procedimentos, e instituições introduzidas pelo governo para expressar o propósito de desenvolvimento, administração e revisão da regulação" (OCDE, 2023b, p. 3, tradução livre).

Por sua vez, as ferramentas de gerenciamento regulatório são consagradas como aquelas disponíveis para implementar essas políticas, podendo ser de natureza legal; infralegal; administrativa; e até autorregulatória.

Dentre outras recomendações, a OCDE sugere que os Estados-aderentes adaptem suas ferramentas de forma a garantir que a abordagem regulatória se paute em ciclos adaptativos e flexíveis, empregue soluções tecnológicas, promova a cooperação entre agentes – ou *stakeholders*– públicos e privados, nacionais e internacionais, construa um ambiente de confiança e transparência (OCDE, 2023b).

Essas orientações são melhor desenvolvidas ao longo da própria Recomendação, mas também são objeto de aprofundamento em outro texto, intitulado pela *Orientação Prática sobre Governança Regulatória Ágil para a Potencializar a Inovação*[7] (OCDE, 2023a).

De forma geral, a OCDE demonstra a preocupação em adaptar as políticas e ferramentas regulatórias tradicionalmente empregadas pelos Estados para formas mais flexíveis ou, utilizando o termo amplamente mencionado, *imunes ao futuro*. Com isso, propõe uma mudança da abordagem para evitar que a excessiva dependência em normas prescritivas limite a regulação sobre tecnologias que estão em constante desenvolvimento ou se tornem obsoletas ou desconexas do objeto regulado, incapazes de disciplinar adequadamente o cenário tecnológico.

Para isso, entende como ideal a limitação das regras prescritivas aos casos em que absolutamente necessário para garantir a segurança jurídica, favorecendo, sempre que possível, uma abordagem orientada aos resultados e baseada em instrumentos não vinculativos juridicamente.

Esses são apenas alguns exemplos de como as inovações tecnológicas impactam as abordagens regulatórias implementadas por agentes estatais. Como todo posicionamento, parte de um viés político e econômico, especialmente por serem documentos de autoria de uma organização internacional que tem como objetivo primordial o progresso econômico e comercial mundial.

[7] No inglês, *Practical Guidance on Agile Regulatory Governance to Harness Innovation*.

No presente trabalho, tem-se como recorte espacial a UE e os EUA, dois grandes agentes na regulação da proteção de dados e da inteligência artificial.

Diante disso o primeiro capítulo se concentra no modelo europeu, primeiramente sobre proteção de dados e, em seguida, sobre a inteligência artificial.

O sistema de proteção de dados pessoais da UE, hoje regido primordialmente pelo Regulamento Geral de Proteção de Dados (RGPD), notavelmente possui uma natureza abrangente e tem como prioridade os direitos fundamentais – e os *princípios europeus*. Exatamente por isso, é considerado avançado e assume protagonismo no cenário internacional.

A influência para além de suas fronteiras se intensifica pela sua exigência de que outros países sejam considerados adequados para que possam tratar dados dos cidadãos europeus e, portanto, para que haja qualquer tipo de fluxo transfronteiriço de dados pessoais, essencial em um mundo globalizado.

Contudo, o caráter de defensor dos direitos fundamentais pode ser considerado restritivo ao desenvolvimento da inteligência artificial. Talvez por isso, a UE por enquanto parece estar trilhando um caminho menos incisivo na regulação da inteligência artificial, optando por uma abordagem baseada na fixação de princípios éticos e na análise de riscos.

Em seguida, no segundo capítulo, direciona-se o olhar para os EUA, que adotam, na proteção de dados pessoais, uma abordagem setorial, há muito tempo vendo na regulação excessiva pelo Estado um empecilho ao desenvolvimento econômico e tecnológico.

Os EUA parecem aplicar a mesma lógica à inteligência artificial – ou talvez até uma versão ainda mais extrema e libertária do que a notada na proteção de dados, no sentido de ter aversão à edição de leis federais e à fiscalização por órgãos públicos, preferindo abordagens relacionadas à autorregulação[8].

No terceiro capítulo, além de comparar as abordagens apresentadas, questiona-se a possível aplicação dos conceitos de Pierre Bourdieu, como campo, poder simbólico, visões internalistas e externalistas, entre outros, para colaborar com o processo de compreensão da

[8] Segundo Marcio Iorio, aquela consiste em "um conjunto de formas regulatórias decorrentes da atribuição de certo nível de autonomia ao sistema regulado para produzir suas próprias regras, contribuir no processo de elaboração de regras próprias ou situadas no regulador e/ou cooperar na aplicação ou fiscalização da regulação." (Aranha, 2021, p. 86). Apesar de possuir diversas formas de manifestação, sendo um termo guarda-chuva, todas partiriam do entendimento de que as próprias forças internas, ou seja, as forças dos regulados seriam no mínimo relevantes e talvez até suficientes para garantir a ordem do sistema regulatório.

realidade europeia e estadunidense da regulação de proteção de dados e IA e da influência que ela representa no cenário internacional globalizado.

Por fim, as conclusões finais servem como uma retomada de todo o exposto, analisando também os limites das deduções a que se pode chegar num trabalho desta dimensão, deixando outras perguntas pertinentes à comunidade científica.

METODOLOGIA

Sinteticamente, esta monografia tem como finalidade analisar as características da regulação da proteção de dados e da inteligência artificial na UE e nos EUA; comparar as suas diferenças e as semelhanças; e, analisar a aplicabilidade de conceitos de Pierre Bourdieu – em especial, os conceitos de campo e poder simbólico – para descrever os possíveis embates entre UE e EUA pela influência transnacional.

Não se trata de um ambiente desconhecido, e muito menos árido, já que diversas pesquisas atuais tratam do mesmo objeto de estudo, mas , aqui, procurou-se realizar uma análise das tecnicidades dos sistemas *e* das estruturas de poder ocultas pela máscara da globalização e da internacionalização de normas e modelos regulatórios.

O interesse inicial era, na verdade, pela regulação de tecnologias emergentes de uma forma mais abrangente – computação em nuvem, *blockchain*, inteligência artificial, internet das coisas – e considerando a atuação dos principais protagonistas do campo das inovações tecnológicas – UE, EUA e China.

Contudo, contemplar outras áreas além da inteligência artificial, assim como estudar o contexto chinês, levaria ao risco de fugir do escopo de uma monografia, principalmente porque exigiria não só uma contextualização sobre as nuances e tecnicidades das diferentes tecnologias e abordagens regulatórias, mas também um grande aprofundamento sobre a realidade chinesa, que em muito se distingue da ocidental.

Destaca-se, ainda, que a noção de Ocidente que se aborda neste trabalho desenvolve-se apenas como um recorte dentre aqueles países que são, geograficamente, considerados ocidentais. Na verdade, além de um recorte espacial, trata-se de um direcionamento do olhar para o *norte global*, ou seja, ao que se entende por *primeiro mundo* ou por *países desenvolvidos* e que, frequentemente, são reconhecidos como os únicos atores ocidentais mais relevantes, o

que não necessariamente reflete a realidade. A proposta é de observar, com olhos críticos, UE e EUA como atores importantes no cenário geopolítico, entendo as suas contribuições sem deixar de perceber a problemática do discurso globalizador que neutraliza a autonomia, a relevância e mesmo as particularidades de outros países e outros autores por não serem hegemônicos – ou, conforme a linguagem que aqui se toda, os detentores do poder simbólico.

Com isso, objetiva-se trazer à luz as nuances existentes por trás de um primeiro olhar direcionado apenas à descrição da abordagem regulatória e, dessarte, evidenciar a existência de um potencial de exercer poder sobre outras regiões geográficas, por meio de influência econômica, política e jurídica, ainda que isso não de se dê de forma impositiva ou óbvia, mas *simbólica*.

Destaca-se que, apesar de entender que um embate entre diferentes modelos regulatórios é também um embate entre diferentes histórias, valores e culturas (Baumer, Earp & Poindexter, 2004), pela limitação do escopo da monografia, esses tópicos não puderam se tornar o foco do trabalho, concentrando-se a pesquisa nas questões regulatórias e políticas.

Outrossim, a escolha especificamente pelos casos da proteção de dados e da IA se deu com base em dois critérios. Primeiramente, pelo fato de que a utilização de dados, inclusive daqueles de caráter pessoal, tem estreita relação com o *bigdata* e, portanto, com o desenvolvimento de algoritmos e da IA.

Dessa forma, a regulação da forma como dados pessoais são tratados tem implicância na forma como empresas podem desenvolver IA, tanto que modelos protetivos demais são muitas vezes entendidos como prejudiciais ao desenvolvimento dessa (e de outras) tecnologias. Também considerando a limitação de tempo e espaço de um trabalho de conclusão de curso, optou-se por tratar apenas da proteção de dados *pessoais*, e não de dados em gerais.

O segundo critério possui um caráter menos relacionado à realidade da regulação e mais conexo à forma como se poderia desenvolver a pesquisa. A regulação de proteção de dados se iniciou ainda no século passado, de maneira que os ordenamentos jurídicos já tiveram tempo de se adaptar a essa disciplina e a doutrina sobre o assunto é extensa.

O mesmo não ocorre com a IA, que tem sido abordada pelos legisladores apenas na última década, aproximadamente. Por esse motivo, comparar um caso mais consolidado e outro menos, tornaria o estudo mais produtivo e completo, além de oferecer mais benefícios à compreensão da realidade atual.

A adoção de Pierre Bourdieu como marco teórico serviu como uma luva, colaborando para concretizar a percepção de que o estudo da regulação pode – e deve – ser feito a partir de um ponto de vista pragmático, orientado a estudar como o Direito deve portar-se a fim de lidar com disfuncionalidades do sistema social.

Cuidando-se de um autor mais conhecido pela sua contribuição às ciências sociais, é pertinente fazer algumas observações sobre sua teoria e, mais especificamente, retomar alguns de seus conceitos mais conhecidos e explicar os pontos de intersecção do seu pensamento sociológico com as ciências jurídicas.

É necessário reconhecer neste espaço a pertinência de sua crítica à linguagem jurídica, que considera caracterizada pela *apriorização*, ou seja, por um processo de combinação de elementos da língua comum e de elementos estranhos a ela, com vistas a dois principais efeitos: a *neutralização* e a *universalização*. Sobre isso, o autor explica:

> Esta retórica da autonomia, da neutralidade e da universalidade, que pode ser o princípio de uma autonomia real dos pensamentos e das práticas, está longe de ser uma simples máscara. Ela é a própria expressão de todo o funcionamento do campo jurídico e, em especial, do trabalho de racionalização, no duplo sentido de Freud e de Weber, a que o sistema das normas jurídicas está continuamente sujeito, e isto desde séculos. Com efeito, aquilo a que se chama "o espírito jurídico" ou "o sentido jurídico e que constitui o verdadeiro direito de entrada no campo (...) consiste precisamente nesta *postura universalizante*. Esta pretensão estatutária a uma forma específica de juízo, irredutível às instituições frequentemente inconstantes do sentido da equidade (...) é um dos fundamentos da cumplicidade, geradora de convergência e de cumulatividade, que une, na concorrência pelas coisas em jogo e por meio dessa concorrência, o conjunto, todavia muito diferenciado, dos agentes que vivem da produção e da venda de bens e serviços jurídicos (Bourdieu, 2022, pp. 224-226).

É essa linguagem que permite que o Direito seja utilizado como instrumento na divisão do trabalho de dominação, realizada por agentes com interesses distintos e por representantes de diferentes formas de poder – tal qual a econômica, a política, a cultural. Essas agências, contudo, são complementares, na medida em que participam conjuntamente de um campo que é construído e se constrói (Bourdieu, 2022).

A ciência do direito, assim, tende a se tornar uma massa maleável, que serve aos teóricos e aos práticos, assim como às diferentes tradições jurídicas, a exemplo da romano-germânica e da anglo-americana – aquela, mais focada na exegese pura da lei; esta, na construção histórica a partir de precedentes (Bourdieu, 2022, p. 227) – sempre voltada, contudo, à formação de um corpo de normas e à regulação das esferas cotidianas.

O autor defende fortemente o “falar em vez de ser falado por palavras emprestadas, carregadas de significado social” (Bourdieu, 2019, p. 19), de maneira que o processo de pesquisa não se pautou em qualquer intenção de produzir um saber neutro ou universal, mas sim demonstrar uma visão possível dentre várias.

Além disso, compreende-se que a linguagem empregada também por outros autores necessariamente demonstra um viés normalmente relacionado às suas próprias individualidades acadêmicas e profissionais.

De toda forma, esta iniciativa, sendo um trabalho de conclusão de curso de graduação em Direito, não deixa de ser uma “inclinação a agir que se engendra na relação entre um espaço de jogo propondo certas apostas (...) e um sistema de disposições ajustado a esse jogo (...), senso do jogo e dos desafios que implicam tanto a inclinação quanto a aptidão a jogar o jogo, a se interessar pelo jogo, de se envolver no jogo” (Bourdieu, 2019, pp. 36-37).

Além do esclarecimento sobre o papel da linguagem para Bordieu, cabe destacar que um dos principais conceitos desenvolvidos pelo autor francês, *campo*, foi construído a partir da retomada da pesquisa de outros pensadores, sempre observando “a particularidade de um caso particular” (Bourdieu, 2022, p. 65), até encontrar “propriedades gerais, válidas nos diferentes campos” (Bourdieu, 2022, p. 66).

A partir de tais ideias, mergulhou-se nas particularidades do contexto europeu e estadunidense e nas, ainda mais particulares, formas de cada agente regular a proteção de dados e a inteligência artificial.

Tratando-se de uma pesquisa explicativa e qualitativa, buscou-se o aprofundamento para além dos conhecimentos gerais sobre as práticas regulatórias, a partir do contato com as críticas elaboradas pelos acadêmicos da área, promovendo um confronto entre diferentes opiniões até que fosse possível, a partir desses conhecimentos, construir uma opinião a ser externada neste trabalho.

O principal procedimento, para isso, foi a pesquisa bibliográfica e documental, analisando-se textos de diversas naturezas: artigos, capítulos de livros, relatórios, regulamentos, pareceres oficiais, entre outros.

Todos os textos foram fichados e classificados quanto à sua pertinência em relação ao objeto da pesquisa até que, num momento de maior amadurecimento sobre o tema, passou-se à escrita do trabalho, buscando retratar detalhadamente todas as informações essenciais, para que

mesmo leitores não tão familiarizados com o assunto fossem capazes de compreender a problemática.

1. No "Velho Continente", a União Europeia

1.1. A Proteção De Dados Como Direito Fundamental

1.1.1. A Diretiva 95/46/CE

Segundo Baumer, Earp e Poindexter, "entender essas diferenças entre as abordagens regulatórias é fundamental para atender com sucesso aos requisitos de privacidade das informações em um mercado global que depende de fluxos de informações transfronteiriços"[9] (Baumer, Earp, Poindexter; 2004; p. 401, tradução livre).

É nesse sentido que esses autores argumentam que, para compreender determinado sistema de proteção de dados, é preciso entender, ainda a sua história e a sua cultura. No caso da Europa ressaltam que sua atuação e seus valores sociais e jurídicos são continuamente influenciados pela Segunda Guerra Mundial e pelos horrores dos regimes autoritários (Baumer, Earp, Poindexter; 2004).

No caso da proteção de dados, esse seria um dos fatores que tornariam a população da UE, de forma geral, mais preocupada com a proteção da privacidade e dos dados pessoais (Baumer, Earp, Poindexter; 2004; p. 401).

Segundo Veronese e Mendonça, em uma dimensão constitucional, na UE, a proteção de dados pessoais compreende a disciplina dos direitos fundamentais, ancorada na dignidade da pessoa humana, nos direitos da personalidade, na privacidade e na autodeterminação; além de avançar com o foco na relação entre particulares" (Veronese, Mendonça; 2021; p. 112).

De fato, é o que se percebe pela Carta dos Direitos Fundamentais da União Europeia (CDFUE), "que passou a ser juridicamente vinculante para os seus Estados-membros em 2009 com a assinatura do Tratado de Lisboa" (Veronese, Mendonça; 2021; p. 112), e pelo Tratado

[9] No original, "*understanding these differences in regulatory approaches is a key to successfully meeting information privacy requirements in a global marketplace that is dependent on transborder information flows*".

sobre o Funcionamento da União Europeia (TFUE), uma vez que ambos consagram a proteção de dados como um direito fundamental europeu (artigos 8º e 16, respectivamente).

A CDFUE, ainda, consagra expressamente o direito à dignidade (artigo 1°) e à integridade (artigo 3º) do ser humano, ressaltando até mesmo que, no domínio da medicina e da biologia, devem ser respeitados o consentimento livre e esclarecido da pessoa, assim como a proibição de práticas eugênicas, de transformar o corpo ou suas partes numa fonte de lucro e a proibição de clonagem reprodutiva.

Ademais, a CDFUE protege expressamente a liberdade (artigo 6º) e a vida privada e familiar (artigo 7º), além de diversos outros direitos amplamente relacionados a um Estado Democrático de Direito.

Para além dessa dimensão constitucional, há ainda uma dimensão regulatória relevante, que notavelmente foi inaugurada com a *Diretiva 95/46/CE*.

A Diretiva foi editada nos anos 90 como uma tentativa de padronizar a tutela da proteção de dados entre os Estados-membros, que estavam criando suas próprias leis e gerando, com as diferenças entre os diplomas, óbices à integração europeia.

Propôs-se, no seu artigo 1º, a dois objetivos primordiais – proteger o direito fundamental à proteção de dados e assegurar a livre circulação de dados pessoais entre os Estados-Membros.

Apesar de não possuir caráter vinculante, nos termos do artigo 288 do TFUE, a Diretiva 95/46/CE dispôs expressamente, ainda no artigo 1º, que cada Estado-membro deveria garantir a proteção das liberdades e proteções individuais em relação ao tratamento de dados pessoais e que, nesse sentido, não poderia restringir ou proibir a livre circulação desses dados.

Com esse objetivo, conceituou definições relevantes como “dados pessoais”, “tratamento de dados pessoais”, “ficheiro[10] de dados pessoais”, “responsável pelo tratamento”, “subcontratante” “terceiro”, o que facilita o entendimento das disposições desenvolvidas ao longo do texto, em especial para aqueles que precisariam estar em conformidade com ele.

Ainda, estabeleceu condições gerais de licitude, criando princípios relativos à qualidade dos dados e à legitimidade do seu tratamento; categorias específicas de tratamento; direitos de informação e de acesso ao titular dos dados; restrições aos direitos dos titulares;

[10] *Arquivo*, no português brasileiro.

direito de oposição da pessoa em causa; parâmetros de confidencialidade e segurança do tratamento de dados; obrigação de notificação às autoridades de controle; recursos judiciais cabíveis, assim como previsões de responsabilização e sanções.

De fato, a Diretiva 95/46/CE criou um ordenamento próprio, demonstrando uma preocupação não só com o que ocorreria dos dados dos cidadãos da UE dentro de suas fronteiras, mas também criando, no seu artigo 25, condições para a transferência de dados pessoais para países terceiros.

Suscitou, dessa forma, a necessidade de que um país tivesse um nível de proteção de dados adequado, o que seria apreciado a partir de vários fatores:

> (...) 2. A adequação do nível de protecção oferecido por um país terceiro será apreciada em função todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, serão tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projectados, os países de origem e de destino final, as regras de direito, gerais ou sectoriais, em vigor no país terceiro em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse país (União Europeia, 1995).

Ao tratar do fluxo transfronteiriço de dados e impor obrigações aos interessados em lidar com dados pessoais dos cidadãos de uma das principais figuras do cenário geopolítico e comercial internacional, essa disposição foi responsável por um grande impacto na regulação da proteção de dados em diversos países.

De fato, Pablo Palazzi, em *La transmisión internacional de datos personales y la protección de la privacidad*, disserta sobre como a Diretiva, ainda que não tivesse precipuamente a intenção de exportar as ideias regulatórias da UE, acabou fazendo-o, exercendo influência sobre a América Latina (Palazzi, 2002). Argentina e Uruguai são exemplos disso, tendo sido alguns dos poucos países considerados adequados sob a égide da Diretiva, em 2003 e 2012, respectivamente.

Tal comentário não se restringe, contudo, ao contexto latino-americano, vez que outros os países e regiões também foram contemplados com uma decisão positiva de adequação sob a égide da Diretiva: Suíça (2000); Canadá, apenas para organizações comerciais (2002); Guernsey (2003); Ilha de Man (2004); Jersey (2008); Andorra (2010); Ilhas Faroé (2010); Israel (2011); e Nova Zelândia (2013).

A essa lista acrescentou-se os EUA, que, todavia, são um caso particular, uma vez que o seu modelo de proteção diverge muitíssimo do modelo europeu, como se verá adiante.

De toda forma, tem-se que, desde a Diretiva, já era possível perceber que o modelo europeu de proteção de dados pessoais adquiria um caráter abrangente, baseado em normas positivadas sobre o assunto, gerais e específicas, aplicadas tanto ao setor público quanto ao privado (Hoofnagle, 2016, p. 766).

1.1.2. O Regulamento Geral sobre a Proteção de dados

Esse caráter se consolidou mais ainda com a substituição da Diretiva pelo Regulamento Geral sobre a Proteção de Dados (*RGPD*), aprovado em 2016 e em vigor desde 2018, momento em que tornou-se "imediatamente aplicável à ordem jurídica interna dos países da UE" (Veronese, Mendonça; 2021; p. 114).

Apesar de tratar-se de um novo instrumento legal da União, não se notou uma ruptura em relação à Diretiva, mas sim uma continuidade, com o diferencial de tornar o modelo europeu ainda mais abrangente. Nesse sentido, Alexandre Veronese e Luiza Mendonça explicam:

> Em semelhança ao que já ocorria com a Diretiva 95/46/CE, o RGPD tem o objetivo duplo de proteger os dados pessoais e de assegurar a livre circulação de dados. Contudo, ao ser aplicado a todos os Estados-membros, sem uma maior margem de adaptação que a transposição de diretivas permite, o RGPD poderá, provavelmente, propiciar um ambiente regulatório mais uniforme e, assim, fortalecer a salvaguarda dos direitos fundamentais com melhor equilíbrio entre a proteção de dados pessoais e a livre circulação de dados (Veronese, Mendonça; 2021; p. 114).

Por sua vez, Potvin-Solis defende que o RGPD "contribui para reforçar os direitos dos indivíduos e as obrigações dos controladores e processadores de dados, bem como as condições relacionadas à independência das autoridades de supervisão, à cooperação e à coerência"[11] (Potvin-Solis, 2018, p. 19, tradução livre).

[11] No original, "*(...) contribue à renforcer les droits des personnes et les obrigations qui prèsent sur les responsables du traitement des données et sur les sous-traitants ainsi que les conditions tenant à la indépendance des autorités de contrôles, la coopération et la cohérence*".

A tabela 1, em anexo, foi formulada com o objetivo de demonstrar algumas das mudanças de um texto em relação ao outro, no que diz respeito aos princípios e direitos dos titulares consagrados.

Percebe-se que, de forma geral, os princípios e direitos elencados pela Diretiva 95/46/CE e pelo Regulamento são praticamente os mesmos, com a diferença de que o RGPD revelou um maior detalhamento ao cuidar das hipóteses de incidência e de exceção, assim como de outros detalhes voltados ao cumprimento de cada uma das previsões.

Além disso, o RGPD inovou ao prever expressamente quatro novos direitos aos titulares: direito de retificação (artigo 16º), direito ao apagamento dos dados ou direito ao esquecimento (artigo 17º), direito à limitação do tratamento (artigo 18º), direito de portabilidade de dados (artigo 20º).

Outro parâmetro de comparação é o número de considerandos que acompanha os seus artigos: na Diretiva, foram propostos 72 enunciados, enquanto, no RGPD, 173 – mais de 100 cláusulas introdutórias a mais.

Nesse contexto, importante ressaltar que os considerandos, apesar de não possuírem a força normativa de artigos, são recursos importantíssimos para lidar com as "áreas cinzentas da incerteza normativa"[12] (Floridi, 2018, p. 6, tradução livre).

Ademais, prestam à realização de uma hermenêutica baseada nas intenções e nos diálogos entre os agentes que criaram a própria norma – no caso, o Parlamento Europeu, o Conselho Europeu, a Comissão Europeia, o Comitê Econômico e Social Europeu e o Comitê das Regiões (União Europeia, 2016c). Tal importância é notada mais claramente no contexto jurisdicional, mas não deixa de ser presente em outros âmbitos de aplicação.

Luciano Floridi defende que os considerandos seriam, inclusive, um resultado da ética, como recurso de criação, o que ele designa como *hard ethics*, e de interpretação, ou *soft ethics* (Floridi, 2018). Nesse sentido, o autor explica:

> A *ética rígida* (veja A + B + C na figura 1) é o que geralmente temos em mente quando discutimos valores, direitos, deveres e responsabilidades - ou, de forma mais ampla, o que é moralmente certo ou errado e o que o que deve ou não deve ser feito - durante a formulação de novas regulamentações ou ou contestar as existentes. Resumidamente, na medida em que (e pode não ser muito) a ética contribui para criar, moldar ou alterar a lei, podemos chamar isso de ética dura. Por exemplo. Fazer lobby

[12] No original, "*grey areas of normative uncertainty*".

> em favor de uma boa legislação ou para melhorar a que já existe pode ser um caso de ética rígida.
>
> (...)
>
> A *ética branda* abrange o mesmo campo normativo que a *ética rígida* (novamente, veja A + B + C na figura 1), mas faz isso considerando o que deve e o que não deve ser feito além da regulamentação existente, não contra ela, ou apesar de seu escopo, ou para alterá-la, ou para contorná-la, por exemplo, em termos de autorregulação. Em outras palavras, a ética branda é uma ética pós-conformidade porque, nesse caso, 'dever implica poder' (Floridi, 2018, pp. 4-5, tradução livre)[13].

Dessa forma, o RGPD teria, no mínimo, elementos de *soft ethics* muito mais extensos e complexos do que a Diretiva, demonstrando, mais uma vez, o amadurecimento da discussão no âmbito da UE.

Outro ponto que chama a atenção é que o RGPD emprega com frequência o termo "titular de dados", ao passo que a Diretiva, redigida em um momento de menor consolidação do tema, recorria apenas ao termo "pessoa em causa", o que revela o recrudescimento da robustez dos conceitos orientadores da disciplina da proteção de dados pessoais.

No que diz respeito à transferência de dados para além das fronteiras da UE, o artigo 44° do RGPD estabelece seu princípio geral:

> Artigo 44.o
>
> Princípio geral das transferências
>
> Qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional. Todas as disposições do presente capítulo são aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento. (União Europeia, 2016d).

---

[13] No original, "*Hard ethics (see A + B + C in figure 1) is what we usually have in mind when discussing values, rights, duties and responsibilities—or, more broadly, what is morally right or wrong, and what ought or ought not to be done—in the course of formulating new regulations or challenging existing ones. In short, insofar (and it may not be very far) as ethics contributes to making, shaping or changing the law, we can call that hard ethics. For example. Lobbying in favour of some good legislation or to improve that which already exists can be a case of hard ethics.*
(...)
Soft ethics covers the same normative ground as hard ethics (again, see A + B + C in figure 1),but it does so by considering what ought and ought not to be done over and above the existing regulation, not against it, or despite its scope, or to change it, or to by-pass it, e.g. in terms of self-regulation. In other words, soft ethics is post-compliance ethics because, in this case, 'ought implies may'".

Nesse ponto, igualmente, o RGPD demonstrou um aumento da complexidade em comparação ao marco legislativo anterior. Além das decisões de adequação, já previstas na Diretiva 95/46/CE como um mecanismo geral de autorização das transferências, prevê os mecanismos das garantidas adequadas (artigo 46º), as regras vinculativas aplicáveis às empresas (artigo 47º), das derrogações para situações específicas (artigo 49º) e da cooperação internacional por meio de regras, acordos e tratados internacionais (artigo 50º).

Apesar da inexistência de hierarquia entre tais mecanismos, Miguel Gayo explica que "as decisões de adequação da Comissão Europeia representariam o padrão mais alto (Kuner, 2017, p. 904), ao requerer que o sistema legal do terceiro países seja substancialmente equivalente"[14] (Gayo, 2019, p. 216, tradução livre).

De fato, isso é perceptível diante do detalhamento dos critérios estabelecidos como parte do processo de tomada dessas decisões. Nesse sentido, a compatibilidade entre os níveis de proteção é aferida com base na existência de uma lei específica e, de maneira geral, na completude do sistema regulatório. Nos termos do artigo 45, n° 2:

> 2. Ao avaliar a adequação do nível de proteção, a Comissão tem nomeadamente em conta os seguintes elementos:
>
> a) O primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação dessa legislação e das regras de proteção de dados, das regras profissionais e das medidas de segurança, incluindo as regras para a transferência ulterior de dados pessoais para outro país terceiro ou organização internacional, que são cumpridas nesse país ou por essa organização internacional, e a jurisprudência, bem como os direitos dos titulares dos dados efetivos e oponíveis, e vias de recurso administrativo e judicial para os titulares de dados cujos dados pessoais sejam objeto de transferência;
>
> b) A existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros; e
>
> c) Os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em

[14] No original, "*las decisiones de adecuación de la Comisión Europea supondrían el estándar más alto (Kuner, 2017, p. 904), al requerir que el sistema legal del tercer país sea substancialmente equivalente*".

> sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais (União Europeia, 2016d).

A Diretiva, previa, como único instrumento, as decisões de adequação, sem, contudo, especificar com base em que critérios elas seriam tomadas, tendo sido necessária a elaboração de parecer pelo Grupo de Trabalho do Artigo 29°.

Desde então, alguns países foram considerados adequados segundo o padrão do RGPD: Japão (2021), que inclusive já passou pela primeira revisão periódica (2023); Reino Unido (2021), Coréia do Sul (2021) e, novamente, EUA (2023).

Complementarmente a essas normas gerais, ao longo dos anos foram produzidos outros marcos regulatórios, de caráter específico, importantes para uma proteção mais abrangente dos dados pessoais, dentre os quais é possível citar: a Diretiva 2000/31/CE, sobre o comércio eletrônico; a Diretiva 2016/680/UE proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados e a Diretiva 2016/681/UE, sobre a utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, detecção, investigação e repressão das infrações terroristas e da criminalidade grave.

1.2. A Inteligência Artificial a Partir de Padrões Éticos

1.2.1. Uma Introdução à Inteligência Artificial

Por outro lado, a regulação da IA pela UE ainda está em processo de consolidação. Contudo, antes de partir para uma descrição do estado da arte do modelo europeu para a IA, é preciso perpassar por tópicos gerais da ciência que estuda esse ramo da tecnologia. Isso porque, apesar de muito se falar sobre os impactos da IA na sociedade, os seus principais conceitos e ideias são pouco difundidos.

A IA começou a ser desenvolvida no período que Stuart Russel e Peter Norvig chamam de gestação da inteligência artificial, ocorrido entre os anos de 1943 e 1955 (Russell, Norvig; 2022; p. 35).

Desde então, o estudo da IA passou por momentos de intensas descobertas e alto entusiasmo, tais como os desencadeados pela contribuição de nomes como Alan Turing e John McCarthy, e pela criação de tecnologias importantíssimas, como *machine learning*[15] e *deep learning*[16].

Passou, também, por momentos de estagnação, frente a limitações relacionadas à capacidade computacional e ao número de dados disponíveis, de maneira que muitos projetos eram abstratamente idealizados, mas não podiam ser executados por uma impossibilidade prática.

A partir dos anos 1980, ainda, percebe-se uma tentativa de consolidação do estudo da IA, a partir do momento em que ela começa a se tornar uma indústria, não apenas nos Estados Unidos da América (EUA), mas também no Japão e no Reino Unido. Todavia, as empresas então engajadas no desenvolvimento da IA, recém criadas e objetos de tanta esperança e investimento, falharam em corresponder às expectativas criadas e entraram na crise que Russel e Norvig chamam de *Inverno da IA* (Russell, Norvig; 2022).

Apesar de tais dificuldades, a IA não se tornou um projeto abandonado, preso a um período específico e passado da história humana. Na contemporaneidade, porém, esta crise já foi resolvida e a IA é considerada uma promessa para o futuro, principalmente no que diz respeito ao aumento da eficiência de determinadas atividades e, consequentemente, ao crescimento econômico.

São diversos os aspectos que poderiam ser explorados para ilustrar o cenário de desenvolvimento atual da IA. O primeiro desses é exatamente a imprecisão sobre o que se entende como IA. Segundo Stuart Russell e Peter Norvig, ao longo da história, diferentes

---

[15] Segundo Joanna J. Bryson, "*machine learning (ML), which is one means of developing AI wherein computation is used to discover useful regularities in data. Systems can then be built to exploit these regularities, whether to categorize them, make predictions, or select actions directly*" (Bryson, 2020, p. 6) e, ainda, "*Machine learning is actually a statistical process we use for programming some aspects of AI*" (Bryson, 2020, p. 17)

[16] "*Deep learning networks typically deploy multilayered cascades of nonlinear processing units alongside (supervised or unsupervised) machine learning algorithms to perform pattern analysis and classification tasks, by deriving higher level features from lower level features to build hierarchical representations spanning different levels of abstraction. As Metz reports, such systems are "already pushing their way into real world applications. Some help drive services inside Google and other Internet giants, helping to identify faces in photos, recognize commands spoken into smartphones, and so much more."28 They have famously learned to play challenging intellectual games to high levels of proficiency, culminating in Google's AlphaGo, a deep-learning-based system for playing the game Go that, in March 2016, recorded a 4–1 victory over Lee Sedol, one of the highest ranked human players in the world. In addition, they are being used to complete life-critical assignments such as detecting earthquakes and predicting heart disease. And, crucially for the present discussion, deep learning networks are central to the control mechanisms that the autonomous AI industries see as pivotal to the eventual success of their products, especially when combined with huge data sets that may be analyzed and navigated by the networks in question to track and reveal task-useful distinctions, patterns, and trends*" (Wheeler, 2020, p. 350).

pesquisadores procuraram conceituar essa ciência a partir de dois pares de lentes: “humano vs. racional e pensamento vs. comportamento”[17] (Russell, Norvig; 2022, p. 19; tradução livre). A partir da combinação dessas lentes, surgem quatro caminhos para a conceituação de IA.

A ideia de *agir humanamente* é derivada do Teste de Alan Turing, em que um interrogador humano fazia determinadas perguntas e, então, recebia as respectivas respostas, devendo identificar se a autoria delas seria de uma pessoa ou de um computador. Caso o interrogador não conseguisse discernir quais formulações tinham sido elaboradas pela máquina, esta seria considerada aprovada pelo teste.

Inicialmente, essa avaliação tinha interesse em entender processo de ação humano por uma perspectiva abstrata, mas outros pesquisadores recorreram a versões mais complexas dele, buscando explorar a interação física entre computador e objetos e pessoas no mundo material (Russell, Norvig; 2022, p. 20).

A versão completa do Teste de Turing[18] permite a análise de seis técnicas que, hoje, são centrais no estudo da IA e que evidenciam a capacidade de uma máquina de simular o agir humano: processamento da linguagem natural; representação de conhecimento; raciocínio automatizado; *machine learning* – ou seja, capacidade de adaptação; visão computacional; e robótica (Russell, Norvig; 2022; p. 20).

O *pensar humanamente* se concentra na compreensão e no estudo sistemático de como acontece o pensamento humano, guardando uma forte relação com a ciência cognitiva, que “junta modelos computacionais de IA e técnicas experimentais da psicologia para elaborar teorias precisas e testáveis acerca da mente humana”[19] (Russell, Norvig; 2022, p. 21; tradução livre).

Essa perspectiva também se aproveita da técnica computacional para simular o processo neurológico de formação de imagens mentais “para determinar o conteúdo semântico dos pensamentos internos de uma pessoa”[20] (Russell, Norvig; 2022; p. 21; tradução livre).

---

[17] No original, “*human vs. rational and thought vs. behavior*”.
[18] Peter e Norvig afirmam que, apesar da previsão de Turing de que, até o ano de 2000, haveria computadores capazes de serem aprovados pelo seu teste, “nós estamos do outro lado dos 2000 e ainda não conseguimos concordar se algum programa de fato foi aprovado” (2022, p. 1035). Contudo, ao consultar mecanismos de pesquisa, o ChatGPT começa a aparecer de forma mais frequente em diversas notícias como a primeira IA ser aprovada pelo Teste de Turing, embora ainda não exista um consenso sobre sua aprovação (Blakemore, 2023) (Biever, 2023).
[19] No original, “*brings together computer models from AI and experimental techniques from psychology to construct precise and testable theories of the human mind*”.
[20] No original, “*to ascertain the semantic content of a person’s inner thoughts*”.

Por sua vez, a ideia de *pensar racionalmente* recorre à lógica, principalmente por meio de silogismos, para criar programas e sistemas inteligentes. Permitindo a "representação de enunciados sobre objetos de todos os tipos no mundo e a relação entre eles"[21] e recorrendo às ideias extraídas das teorias da probabilidade, a IA pode ser estruturada para, a partir de informações brutas, interpretar o funcionamento do mundo e até mesmo fazer inferências sobre ele (Russell, Norvig; 2022; p. 21; tradução livre).

Por fim, a quarta lente, *agir racionalmente*, se relaciona à noção de *agência*, de forma que um agente computacional pode ser desenvolvido para atingir o melhor resultado possível. Uma vez que os computadores podem "agir autonomamente, perceber o ambiente, persistir por um longo período de tempo, adaptar-se às mudanças, e criar e buscar efetuar metas"[22] (Russell, Norvig; 2022; pp. 21-22; tradução livre), a eficiência esperada da máquina é muito maior, comparada àquela que um humano pode atingir.

Tal contextualização demonstra claramente que a IA não se restringe ao campo da ciência da computação, recorrendo, na verdade, a diversas outras áreas do conhecimento, tal qual a filosofia, a matemática, a economia, a neurociência, a psicologia, entre outras (Russell, Norvig; 2022).

Essa multidisciplinariedade, reforçada pelo *bigdata* e pelo aumento da capacidade computacional, permitiu que os cientistas contornassem, um a um, os obstáculos ao desenvolvimento da IA, e alcançassem a capacidade de idealizar não só IAs "fracas", mas também com as "fortes". Nesse sentido, Russell e Norvig explicam:

> Em 1980, o filósofo John Searle introduziu uma distinção entre IA fraca – a ideia de que as máquinas poderiam agir como se fossem inteligentes – e IA forte – a afirmação de que as máquinas que fazem isso estão realmente pensando conscientemente (não apenas simulando o pensamento). Com o passar do tempo, a definição de IA forte mudou para se referir ao que também é chamado de "IA de nível humano" ou "IA geral" – programas que podem resolver arbitrariamente uma ampla variedade de tarefas, inclusive novas, e fazê-lo tão bem quanto os humanos.
>
> Os críticos da IA fraca, que se opunham à própria possibilidade de comportamento inteligente das máquinas, agora parecem tão cegos quanto Simon Newcomb, que, em outubro de 1903, escreveu que "o voo aéreo é um dos grandes problemas com os quais o homem pode lidar com veneração", apenas dois meses antes do voo dos irmãos Wright em Kitty Hawk. O rápido progresso dos últimos anos não prova, entretanto, que não haja limites para o que a IA pode alcançar. Alan Turing (1950), a primeira pessoa a definir a IA, também foi o primeiro a levantar possíveis objeções à IA,

[21] No original, "*notations for statements about objects in the world and the relations among them*".
[22] No original, "*operate autonomously, perceive their environment, persist over a prolonged time period, adapt to change, and create and pursue goals*".

> prevendo quase todas as que foram levantadas posteriormente por outros (Russell, Norvig; 2022; p. 1032; tradução livre)[23].

A noção de IA geral é exatamente aquela que costuma gerar um sentimento de aversão na sociedade, principalmente diante da vasta produção literária e midiática interessada pela retratação de cenários distópicos, em que a raça humana é ameaça por robôs capazes de pensamento próprio, ou "uma espécie de inteligência super-humana" (Engelke, 2020, p. 1).

Nesse sentido, Peter Engelke explica que "a pesquisa sobre IA geral continua na sua primeira infância. Pesquisadores da área estimam que a IA geral poderia ser desenvolvida até a metade do século ou até demorar ainda mais"[24] (Engelke, 2020, p. 3, tradução livre). Com efeito, é difícil ter certeza se algum dia, ou quando, os avanços tecnológicos realmente chegarão a esse nível de desenvolvimento.

A discussão sobre *o que* uma IA conseguirá ou não fazer é demasiado ampla para ser abordada neste trabalho, cabendo, pois, restringir-se ao fato de que "em geral, os programas superam o desempenho humano em algumas tarefas e ficam para trás em outras. A única coisa que está claro que eles não conseguem fazer é ser exatamente humanos*"*[25] (Russel, Norvig; 2022; p. 1034, tradução livre).

Dessa forma, apesar de não ser um horizonte impossível, o desenvolvimento de IAs quase-humanas é, no mínimo, um sonho (ou pesadelo) distante, o que não muda o fato de que a IA já produz seus efeitos sobre a sociedade, ainda que na sua forma "fraca", modificando a realidade social, econômica e até mesmo cultural (Engelke, 2020).

As promessas sobre os benefícios da IA são inúmeras: melhoramento da produção de alimentos, com a possibilidade de melhor "alimentar" o mundo; aumento da produtividade de

---

[23] No original, "*In 1980, philosopher John Searle introduced a distinction between weak AI – the idea that machines could act as if they were intelligent – and strong AI – the assertion that machines that do so are actually consciously thinking (not just simulating thinking). Over time the definition of strong AI shifted to refer to what is also called "human-level AI" or "general AI" – programs that can solve arbitrarily wide variety of tasks, including novel ones, and do so as well as humans.*
Critics of weak AI who objected to the very possibility of intelligent behavior in machines now appear as shortsighted as Simon Newcomb, who in October 1903 wrote "aerial flight is one of the great class of problems with which man can vener cope" – just two months before the Wright brothers' flight at Kitty Hawk. The rapid progress of recent years does not, however, prove that there can be no limits do what AI can achieve. Alan Turing (1950), the first person to define AI, was also the first to raise possible objections to AI, foreseeing almost all of the ones subsequently raised by others".

[24] No original, "*research into general AI remains in its infancy. Researchers in the field estimate that general AI could be developed by the middle of this century or take far longer*".

[25] No original, "*Overall, programs exceed human performance in some tasks and lag behind in others. The one thing that it is clear they can't do is be exactly human".*

empresas; aumento do número de empregos; substituição das "tarefas tediosas e perigosas que muitos trabalhadores realizam" e libertação "para concentrarem-se em aspectos mais interessantes"[26] (Russell, Norvig; 2022; pp. 1037-1038, tradução livre); auxílio de pessoas com deficiência na realização de suas tarefas; facilitação da comunicação entre pessoas de países diferentes, com o emprego de máquinas de tradução; democratização do acesso à tecnologia, posto que IAs baseadas em softwares praticamente não representariam aumento dos custos de produção (Russell, Norvig; 2022).

Sem embargo, Russell e Norvig ressalvam que a IA, como toda inovação tecnológica, possui seus efeitos colaterais negativos (2022, p. 1038). Diante disso, destacam o perigo dos usos relacionados à criação de armas autônomas letais; à vigilância excessiva, implicando danos à privacidade e à segurança digital; aos riscos de replicação e intensificação de vieses algorítmicos[27]; à vulneração da confiança e da transparência; à criação de problemas éticos e jurídicos quanto a robôs e a formas de aprimoramento humano; e à falta de segurança garantida pelas IAs de forma geral.

Engelke demonstra uma visão interessante ao destacar, ao mesmo tempo, como a IA acrescenta a certas áreas de estudo e a certas tecnologias, ao mesmo tempo em que cria problemas novos para elas.

No caso da cibersegurança, a IA "acelera todos os problemas e oportunidades encontrados no ciberespaço" (Engelke, 2020, p. 15), uma vez que representa uma oportunidade tanto para o combate quanto para o aumento do cibercrime e das práticas de *hacking*. Essa dualidade ocorre também no mundo material, em que a aplicação da lei e o crime são simultaneamente incrementados por ferramentas de IA. Outrossim, ressalta:

> Embora as autoridades de cumprimento com a lei estejam entusiasmadas com o uso de ferramentas de IA para combater o crime, o uso de tais ferramentas para combater a atividade criminosa também cria as mesmas preocupações sobre justiça, equidade,

[26] No original, "*can replace the tedious and dangerous tasks that many workers face, and free them to concentrate on more interesting aspects*".

[27] A literatura sobre o assunto, na língua inglesa, frequentemente emprega a palavra "*bias*", que, traduzida literalmente, significa "viés". Importante ressaltar, contudo, que, tratando-se de temas relacionados à IA, os vieses são, normalmente, algorítmicos. Por isso, neste texto, buscou-se especificar essa característica, utilizando o termo "viés(esses) algorítmico(s)", retomando a explicação de Peter Engelke sobre o termo: "*bias refers to how AI tools can sistematically err in their predicitions, in particular for certains categories of people. Such Ai bias can occur at the framing, data collection, and data preparation stages. During these stages, AI system's designers can introduce biases into the algorithm and/or the training data, either deliberately or (most often) via blinders that prevent the designers from seeing how their effort will bias the resulting analyses*" (Engelke, 2020, p. 6).

> privacidade de dados, direitos individuais e viés algorítmico, conforme discutido detalhadamente acima (Engelke, 2020, p. 16, tradução livre)[28].

Além disso, assim como Russell e Norvig, Engelke cuida da criação de armas autônomas letais. Ao fazê-lo, trata de seus problemas éticos e humanitários, que têm sido levantados pela comunidade científica, por organizações como a ONU e pela sociedade civil. Contudo, destaca que, enquanto a maior parte do mundo se preocupa com as implicações de tais armas para o bem-estar comum, os países considerados potências apressam-se numa espécie de corrida armamentista:

> No caso dos aparatos de segurança nacional das principais potências mundiais, a mais alta prioridade em termos de políticas públicas é simples: na ausência de limites globais vinculantes para os sistemas de armas autônomas (tratados de controle de armas), a prioridade mais importante é ter acesso a recursos suficientes para desenvolver, testar e implantar sistemas integrados de IA para garantir a superioridade sobre seus rivais geoestratégicos e militares. Com relação aos usos da IA, suas preocupações dominantes envolvem a cadeia de comando militar: quem (ou o quê) emite uma ordem de morte no campo de batalha ou, no mínimo, quem na cadeia de comando toma "decisões sobre como, quando, onde e por que a arma será empregada"?
>
> Para todas as outras pessoas no mundo, há uma gama maior de questões políticas relevantes, inclusive se alguém em qualquer lugar deve possuir tal arma.
>
> Notavelmente, as maiores potências militares do mundo (supondo que sejam os Estados Unidos, a China e a Rússia) parecem estar indo na direção oposta ao sistema da ONU. Enquanto a conversa dentro do sistema da ONU é sobre as ameaças representadas por qualquer pessoa que possua e use LEIS, as grandes potências militares do mundo estão concentradas exclusivamente no desenvolvimento dessas tecnologias, dado o desejo de seus rivais de fazer o mesmo (Engelke, 2020, pp. 18-19, tradução livre)[29].

---

[28] No original, "*Although law enforcement agencies are enthusiastic about using AI tools to combat crime, the use of such tools to counter criminal activity also creates the same concerns about justice, equity, data privacy, individual rights, and algorithmic bias as discussed at length above*".

[29] No original, "*For the major world powers' national security apparatuses, the highest policy priority is simple: in the absence of binding global limits on autonomous weapons systems (arms control treaties), the most important priority is having access to sufficient resources to develop, test, and deploy AI-integrated systems so as to ensure superiority over one's geostrategic and military rivals. Regarding the uses of AI, their dominant concerns involve the military chain of command: who (or what) issues a kill order on the battlefield, or at the very least who in the chain of command makes "decisions about how, when, where, and why the weapon will be employed"?*
For everyone else in the world, there is a greater range of relevant policy questions, up to and including whether anyone anywhere ought to possess such weapon.
Notably, the world's greatest military powers (assuming these are the United States , China , and Russia) appear to be heading in the opposite direction as the UN system. Whereas the conversation within the UN system is about the threats posed by anyone possessing and using LAWS, the world's great military powers are singularly focused on developing these technologies, given their rivals' desires to do the same".

Considerando essa "faca de dois gumes" que é a IA, Russell e Norvig sugerem que todos os cientistas envolvidos com o desenvolvimento da IA devem promover reflexões sobre a ética de seus projetos, a fim de viabilizar a sua continuidade apenas quando seja possível executá-los de forma segura e benéfica (Russell, Norvig; 2022; p. 1038).

Os autores apresentam um apanhado de princípios que perceberam ao estudar propostas de agências governamentais, organizações sem fins lucrativos e empresas, para o desenvolvimento de sistemas de IA. Ressalvam, porém, que muitos deles possuem uma linguagem vaga e, não se aplicam somente à IA, mas a todos os sistemas de *hardware* e *software*. Esses princípios seriam:

Garantir a privacidade	Estabelecer *accountability*
Garantir a imparcialidade	Defender os direitos e valores humanos
Respeitar a privacidade	Refletir diversidade/inclusão
Promover colaboração	Evitar a concentração de poder
Proporcionar transparência	Reconhecer as implicações legais/políticas

(Russell, Norvig; 2022; p. 1038 ; tradução livre)[30].

Seguindo linha semelhante, Engelke explica que as maiores empresas de tecnologias do mundo têm sido alguns dos agentes mais engajados na produção de orientações sobre a eticidade das IAs – seria o caso, inclusive, da Google e da Microsoft (Engelke, 2020, p. 3).

A Google inclui, na sua lista, sete princípios éticos sobre IA: 1) ser socialmente benéfica; 2) evitar a criação ou o reforço de vieses algorítmicos; 3) ser construída e testada visando a segurança; 4) ser responsabilizável perante as pessoas; 5) incorporar princípios de *privacy by design*; 6) manter altos padrões de excelência científica; 7) ser disponibilizada para usos que estejam de acordo com esses princípios (Google AI, tradução livre).

A Microsoft, por sua vez, entende que uma IA responsável é conduzida a partir dos princípios de 1) equidade, ou justiça; 2) confiabilidade e segurança; 3) privacidade e segurança; 4) inclusividade; 5) transparência; e 6) *accountability* (Microsoft AI, tradução livre).

[30] No original, "*Ensure Privacy, Establish accountability, Ensure fairness, Uphold human rights and values, Respect privacy, Reflect diversity/inclusion, Promote collaboration, Avoid concentration of power, Provide transparency, Acknowledge legal/policy implications*".

Peter Engelke, por sua vez, apresenta uma abordagem para além dos princípios essenciais à regulação da IA. O autor, na verdade, fala sobre elementos indispensáveis à criação, pelos governos, de "ecossistemas de inovação" (Engelke, 2020).

Nesse ínterim, sugere como imprescindível a concentração de esforços para desenvolver ciência de base, no sentido de investir na atividade acadêmico-científica como um todo, a fim de melhorar mesmo as ferramentas que, apesar de simples, são necessárias para que as inovações em relação à IA se concretizem. Um exemplo disso seria o investimento no desenvolvimento de *hardwares* (Engelke, 2020, p. 11).

Semelhantemente, o fomento da criação e do crescimento de *startups* e a atração de pesquisadores talentosos, tanto no âmbito nacional quanto no internacional, são indicadores do potencial de um ecossistema fértil para o progresso da IA (Engelke, 2020, pp. 11-13).

Outro fator que, desta vez, assume um caráter relacionado à regulação como atividade jurídica, é a existência de um regime que proteja a propriedade intelectual. Nesse sentido, Engelke assevera que "a inovação ocorre mais em locais que protegem as novas ideias e as invenções que surgem a partir delas"[31] (Engelke, 2020, p. 14, tradução livre).

Kelly Carman, por sua vez, afirma que cada país escolhe, com base nas suas forças e fraquezas, uma abordagem diferente para a regulação da IA. Apesar dessas diferenças e da necessidade de adaptação ao cenário nacional, a autora entende como possível observar cinco categorias dentro das políticas públicas relacionadas à IA que deveriam ser consideradas em qualquer abordagem regulatória: 1) investimento em pesquisa básica e aplicada; 2) atração de talentos, ou seja, treinamento e retenção de mão-de-obra qualificada para pesquisa e desenvolvimento de IA; 3) investimento na educação dos cidadãos, para que não se tornem obsoletos diante da alteração das oportunidade e relações de trabalho atuais; 4) desenvolvimento de padrões e códigos de ética para IA, principalmente em consideração aos vieses algorítmicos e dos problemas de privacidade e segurança; e 5) regulação (Carman, 2020, p. 198-199, tradução livre).

A autora ressalta, ainda, a necessidade de que a regulação e, mais especificamente, as leis adotadas sejam "versáteis, mas direcionadas para a área específica de IA a que se destinam"[32] (Carman, 2020, p. 200, tradução livre).

---

[31] No original, "*innovation occurs most in places that protect new ideas and the inventions that flow from them*".
[32] No original, "*versatile, yet unique to the specific area of AI they are intended for*".

1.2.2. Os Princípios Éticos e a Onipotência dos Valores Europeus

De fato, como se passará a expor, a própria UE está alinhada com vários desses princípios, uma vez que tem adotado uma abordagem focada, sobretudo, na fixação padrões éticos e na análise de risco, como uma forma de fomentar a produção tecnológica e alcançar um protagonismo na regulação e na produção de IA, sem abandonar os direitos fundamentais que consagra e os seus *valores europeus*.

O histórico da regulação da IA pela UE tem como primeiro marco, no ano de 2018, a criação do *Grupo Europeu em Ética, Ciência e Novas Tecnologias*[33], formado por especialistas selecionados por meio de uma chamada pública (União Europeia, 2021d).

Em 2018, o Grupo apresentou um relatório em que sintetizava alguns princípios relevantes para o desenvolvimento tecnológico, todos baseados nos direitos fundamentais da CDFUE: 1) respeito à autonomia humana; 2) prevenção de dano e proteção da integridade física ou mental; 3) justiça, direito à não-incriminação, solidariedade e justiça; 4) explicabilidade e responsabilidade.

No mesmo ano, a Comissão Europeia emitiu a Comunicação Inteligência Artificial para a Europa[34]. Nela, definiu IA como um conceito que "(...) aplica-se a sistemas que apresentam um comportamento inteligente, analisando o seu ambiente e tomando medidas — com um determinado nível de autonomia — para atingir objetivos específicos (União Europeia, 2018). Essa iniciativa revela que a Comunicação tinha como propósito apresentar, pela primeira vez, num registro oficial, o que seria a IA e quais seriam as suas utilidades, mencionando inclusive iniciativas nacionais que já empregavam essa forma de tecnologia.

Uma das estratégias apontadas pelo documento indica que a UE "deve adotar uma abordagem coordenada, a fim de tirar o máximo partido das oportunidades oferecidas pela IA e fazer face aos novos desafios que esta acarreta" (União Europeia, 2018).

Cuidava-se de iniciativa semelhante ao que propôs a Diretiva 95/46/CE, sobre proteção de dados. A fragmentação da regulação prejudica o mercado comum europeu e enfraquece até

[33] No inglês, *European Group on Ethics in Science and New Technologies*.
[34] No inglês, *Communication Artificial Intelligence for Europe*.

mesmo politicamente a UE, motivo pelo qual a Comunicação direciona o caminho que os Estados-Membros devem seguir conjuntamente.

Propôs, portanto, a criação não só de um *Mercado Único Digital*, mas também de iniciativas conjuntas de investimento e de centros de fomento à pesquisa, além de outras medidas com as quais os 27 (vinte e sete) Estados-Membros (e a Noruega) se comprometeram:

> Com base neste forte apoio político, chegou o momento de envidar esforços significativos para garantir que:
>
> — a Europa é competitiva no panorama da IA, realizando investimentos avultados que correspondam ao seu peso económico. Trata-se de apoiar a investigação e a inovação com vista ao desenvolvimento da próxima geração de tecnologias de IA, bem como a sua implantação, a fim de garantir que as empresas, em especial as pequenas e médias empresas, que representam 99 % do tecido empresarial da UE, são capazes de adotar a IA;
>
> — ninguém fica para trás no processo de transformação digital. A IA está a alterar a natureza do trabalho: serão criados postos de trabalho, enquanto outros desaparecerão e a maioria sofrerá transformações. A modernização dos sistemas de educação, a todos os níveis, deve constituir uma prioridade para os governos. Todos os cidadãos europeus devem dispor de oportunidades para adquirirem as qualificações de que necessitam. Os talentos devem ser fomentados e a diversidade e o equilíbrio entre géneros devem ser encorajados;
>
> — as novas tecnologias se baseiam em valores. O Regulamento Geral sobre a Proteção de Dados tornar-se-á uma realidade em 25 de maio de 2018. Trata-se de um passo importante para gerar confiança, elemento essencial a longo prazo, tanto para as pessoas, como para as empresas. É aqui que a abordagem sustentável da UE às tecnologias cria uma vantagem competitiva, ao adotar a mudança com base nos valores da União. Como qualquer tecnologia transformativa, algumas aplicações de IA podem suscitar novas questões éticas e jurídicas ligadas, por exemplo, à responsabilidade ou a decisões potencialmente tendenciosas. A UE deve, portanto, assegurar que a IA é desenvolvida e aplicada num quadro adequado, que favoreça a inovação e respeite os valores da União e os direitos fundamentais, bem como princípios éticos tais como a responsabilização e a transparência. A UE encontra-se bem posicionada para liderar este debate a nível mundial (União Europeia, 2018).

Enunciados esses objetivos, a Comissão reconheceu seu atraso em relação à China e aos EUA, principalmente no que diz respeito aos investimentos financeiros, mas afirmou a sua intenção de não ficar para trás. Mais precisamente, anunciou que "a UE deve estar na vanguarda das evoluções tecnológicas no domínio da IA e garantir que estas são rapidamente implementadas na economia" (União Europeia, 2018, tradução livre).

Com esse fim, comprometeu-se a: 1) reforçar a capacidade industrial e tecnológica da UE e a adoção da IA na economia, por meio de diversas medidas de planejamento e investimento; 2) preparar as mudanças socioeconômicas, estimulando o talento e treinando os cidadãos europeus; 3) garantir um quadro ético e jurídico apropriado, para garantir a confiança

nas tecnologias desenvolvidas; 4) unir forças entre os Estados-Membros e dentro das fronteiras da UE, mas também para além delas[35] (União Europeia, 2018, tradução livre).

Os Estados-Membros, ainda em 2018, adotaram o *Plano Coordenado sobre IA*[3637], voltado ao financiamento do projeto que começava a ser traçado, com a esperança de que "aumentaria a cooperação para impulsionar a regulamentação uniforme de IA na Europa"[38], colaborando para que a UE consiga assumir o papel de líder mundial em IA (Carman, 2020, p. 204-205, tradução livre).

Nesse mesmo ano, foi criado também o *Grupo de Alto Nível em IA*[39] (AI HLG), composto por especialistas indicados pela Comissão Europeia[40].

Desde então, o AI HLG gerou quatro produtos relevantes: *as Orientações éticas para uma IA confiável*[41], as *Recomendações de políticas e investimentos para uma IA confiável*[42], a *Lista de avaliação final para uma IA confiável*[43] e as *Considerações setoriais sobre as recomendações de políticas e investimentos*[44] (União Europeia, 2018).

O mais relevante dentre esses documentos, o *Orientações éticas para uma IA confiável*, após ter seu rascunho submetido a comentário público (Shaping Europe's digital future, 2022), foi publicado em 2019.

A principal contribuição desse documento são os sete requisitos para uma IA de confiança, que passariam a modelar as políticas regulatórias europeias. Esses são: 1) ação e supervisão humanas; 2) solidez técnica e segurança; 3) privacidade e governança de dados; 4) transparência; 5) diversidade, não discriminação e equidade; 6) bem-estar social e ambiental; 7) responsabilização (União Europeia, 2019b).

---

[35] A Comunicação menciona como uma das iniciativas internacionais referenciais, nesse aspecto, o debate do G7/G20, da ONU e da OCDE sobre o papel da IA no domínio militar.
[36] No inglês, *Coordinated Plan on AI*.
[37] Esse Plano teve a sua atualização mais recente no ano de 2021, como uma forma de responder as exigências de uma realidade então marcada pela pandemia da COVID-19.
[38] No original, "*would increase cooperation to boost uniform AI regulation within Europe*".
[39] No inglês, *High-Level Expert Group on AI*.
[40] Importante destacar que não foi possível identificar de que forma esses especialistas são selecionados, nem se há algum conjunto de critérios avaliados no processo de escolha.
[41] No inglês, *Ethics Guidelines for Trustworthy Artificial Intelligence*.
[42] No inglês, Policy and Investment Recommendations for Trustworthy AI.
[43] No inglês, *The final Assessment List for Trustworthy AI*.
[44] No inglês, *Sectoral Considerations on the Policy and Investment Recommendations*.

Segundo Kelly Carman, as opções feitas nesses requisitos indicam que a UE passava, então, a adotar uma abordagem baseada na proteção do consumidor e no bem-estar social, não somente no desenvolvimento tecnológico (Carman, 2020, p. 204).

Ademais, nas Orientações o AI HLG consagrou quatro princípios éticos: 1) respeito da autonomia humana; 2) prevenção de danos, 3) equidade, 4) explicabilidade (União Europeia, 2019b). Ademais, afirmou que a UE deveria seguir uma abordagem orientada pelos direitos fundamentais consagrados nos seus tratados internacionais e na CDFUE, assim como na teoria geral sobre direitos humanos.

Todos esses seriam enunciados vinculativos para os Estados-Membros, e, portanto, oponíveis judicialmente, configurando o componente legislativo, ou a "primeira componente", do modelo europeu em formação (União Europeia, 2019b).

Outrossim, os direitos fundamentais, no seu aspecto universal e moral, também estariam relacionados ao lado ético do modelo europeu e, de tal maneira, fariam parte da sua "segunda componente", a qual seria o objeto principal das Orientações. Diga-se: as Orientações não poderiam ser consideradas vinculativas, mas apenas parâmetros para uma atuação ideal.

No mesmo dia em que o AI HLG publicou as Orientações, a Comissão Europeia emitiu mais uma Comunicação, chamada *Criando Confiança na Inteligência Artificial Centrada no Ser Humano*[45].

Retomou, neste documento, vários dos valores anteriormente enunciados, ressaltando que a confiança precisa ocupar um papel central na inserção da IA na sociedade. Tendo em vista essa finalidade, o desenvolvimento das tecnologias deveria dar-se com base nos princípios éticos europeus, tendo como centro o ser humano e se dando a partir da participação de múltiplos *stakeholders* (União Europeia, 2019a).

Ademais, afirmou que "a UE tem uma estrutura regulatória sólida que definirá o padrão global para a IA centrada no ser humano"[46] (União Europeia, 2019a). Sem dúvidas, uma enunciação tão clara não é meramente um *slogan*. Na realidade, com isso e com tantos outros posicionamentos revelados pelos documentos expostos, os órgãos e grupos europeus foram verdadeiramente enfáticos em demonstrar a sua intenção em liderar, protagonizar e, até mesmo, competir com outros países no cenário internacional.

---

[45] No inglês, *Building Trust in Human Centric Artificial Intelligence*.
[46] No inglês, "*the EU has a strong regulatory framework that will set the global standard for human-centric AI*."

Apesar de alguma competição seja natural, em especial na dimensão econômica, deve-se reconhecer que a linguagem empregada deve ser encarada como um critério relevante para compreender o desempenho da UE no desenvolvimento do jogo regulatório internacional. Mais ainda, deve-se ter cautela com tal linguagem, principalmente no caso de ela ser combinada com alegações de neutralidade ou universalidade, como se verá nos próximos tópicos.

1.2.3. Uma Abordagem Baseada em Riscos

Posteriormente, em 2020, a Comissão Europeia, inspirada pelos produtos do AI HLG, publicou o principal documento que se tem sobre a suas opções regulatórias em IA: *o Livro-Branco sobre IA*[47].

De forma geral, o Livro foi uma continuação do caminho que a UE começou a traçar anos antes, afirmando a necessidade de união dos Estados-Membros em prol de uma iniciativa comum, que não prejudicasse o mercado único e fosse fundamentada nos *valores europeus* e nos direitos fundamentais consagrados na CDFUE. Em tal contexto, estabeleceu como propósito a aceitação da IA pela sociedade e o combate aos riscos que ela pode implicar (União Europeia, 2020, p. 1).

Sugeriu, novamente, iniciativas voltadas ao aumento da "soberania tecnológica da Europa em tecnologias facilitadoras e infraestruturas essenciais para a economia de dados"[48] (União Europeia, 2020, p. 3, tradução livre), ou seja, voltadas ao desenvolvimento tecnológico de forma geral, como proposto nos anos anteriores.

Ademais, mencionou algumas áreas específicas que deveriam se tornar prioridade em termos de pesquisa e inovação. Uma delas estaria relacionada à próxima onda de dados e à demanda por novas formas de armazenamento.

Essa seria uma oportunidade a ser aproveitada pela Europa, por meio do incentivo ao desenvolvimento de novas tecnologias de armazenamento de dados, como a computação quântica, com vistas a assumir, nos próximos anos, a liderança do mercado.

---

[47] No inglês, *White Paper on Artificial Intelligence – A European approach to excellence and trust*.
[48] No inglês, "*Europe's technological sovereignty in key enabling technologies and infrastructures for the data economy*".

> Cada nova onda de dados traz oportunidades para a Europa se posicionar na economia ágil de dados e se tornar líder mundial nessa área. Além disso, a forma como os dados são armazenados e processados mudará radicalmente nos próximos cinco anos. Atualmente, 80% do processamento e da análise de dados na nuvem ocorrem em data centers e instalações de computação centralizadas, e 20% em objetos inteligentes conectados, como carros, eletrodomésticos ou robôs de fabricação, e em instalações de computação próximas ao usuário ("edge computing"). Até 2025, essas proporções deverão mudar significativamente (União Europeia, 2020, p. 4, tradução livre)[49].

Nesse ínterim, destacou que o investimento da UE em pesquisa e inovação aumentou 70% em relação ao período anterior[50], mas que ainda seria inferior àqueles feitos na América do Norte e na Ásia. Dessarte, seria imprescindível a continuidade dos esforços para o aumento do capital investido, representado principalmente pelo Plano Coordenado entre os Estados-Membros, com vistas ao plano de tornar a Europa, mais uma vez, protagonista na regulação e na determinação das *regras do jogo*.

Diga-se: para que a UE tivesse autoridade para influenciar, mais do que ser influenciada, no que diz respeito às normas limitadores e fomentadoras da IA, ela não poderia *não* ser uma potência no desenvolvimento dessas (e de outras) tecnologias emergentes, como vinha ocorrendo. Apesar do mercado e da população exponenciais e das facilidades decorrentes da integração econômica e política, a UE estava sendo deixada para trás por países que não faziam parte do projeto comum europeu e não replicavam, dessa forma, seus valores europeus.

Tendo em vista o desenvolvimento tecnológico, recomendou algumas ações: 1) a realização de consultas públicas sobre o Livro, a serem levadas em consideração no Plano Coordenado dos Estados-Membros; 2) a criação de centros de excelência que concentrassem investimentos da UE, dos Estados e do setor privado; 3) o estabelecimento de redes de pesquisadores e de universidades para atrair talentos; 4) a criação de novas parcerias público-privadas em programas de fomento, tal qual o *Horizon Europe*; 6) a promoção de diálogos transparentes para a criação de programas específicos sobre o uso da IA em determinados setores; e 7) a promoção de práticas de manejo responsável de dados.

---

[49] No original, "*Each new wave of data brings opportunities for Europe to position itself in the data-agile economy and to become a world leader in this area. Furthermore, the way in which data are stored and processed will change dramatically over the coming five years. Today 80% of data processing and analysis that takes place in the cloud occurs in data centres and centralised computing facilities, and 20% in smart connected objects, such as cars, home appliances or manufacturing robots, and in computing facilities close to the user ("edge computing"). By 2025 these proportions are set to change markedly".*

[50] Não especifica o ano, mas, pelo contexto, possível entender que é uma comparação aos números mencionados pela Comunicação de 2018.

Quanto ao âmbito internacional, verbalizou a intenção de se tornar líder na criação de alianças em torno de valores conjuntos e éticos. Reconheceu o trabalho realizado fora das suas fronteiras, citando expressamente o realizado pelo Conselho da Europa, pela Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), pela OCDE, pela Organização Mundial do Comércio (OMC) e pela União Internacional de Telecomunicações (ITU).

O Livro partiu do pressuposto de que um ecossistema de excelência em IA deveria garantir que os benefícios das tecnologias sirvam aos interesses particulares dos cidadãos e das empresas, mas também ao interesse público, como uma forma de otimizar os serviços dos Estados e auxiliar o cumprimento de objetivos socialmente relevantes, como aqueles assumidos em relação ao meio ambiente.

Para atingir tal excelência em um ambiente regulatório, seria imprescindível o respeito às normas da UE, em especial no que diz respeito aos direitos fundamentais. Isso porque seriam evidentes os riscos a direitos fundamentais, tais quais à liberdade de expressão, à liberdade de associação, à dignidade humana, à não-discriminação, à proteção de dados pessoais e da vida privada, à proteção ao consumidor e à prestação jurisdicional efetiva.

Recomendou, pois, que as legislações existentes fossem ajustadas para se tornarem mais adequadas à disciplina da IA, tratando especificamente de problemas como a opacidade gerada pelo efeito de *blackbox* e dos problemas quanto à responsabilização em casos de produtos defeituosos e possivelmente danosos ao consumidor[51] Outrossim, o Livro, ao cuidar da questão de legislação para regulação, dispôs:

> Por uma questão de princípio, a nova estrutura regulatória para IA deve ser eficaz para atingir seus objetivos, sem ser excessivamente prescritiva, de modo que possa criar uma carga desproporcional, especialmente para as PMEs. Para atingir esse equilíbrio, a Comissão é da opinião de que deve seguir uma abordagem baseada em riscos (União Europeia, p. 17, 2020)[52].

Um ponto relevante para entender de que forma o Livro Branco serviu para complementar as normas que a UE, até agora, emitiu sobre o tema, é a proposta de avaliar o

[51] Nesse sentido, seria necessário não só realocar a responsabilidade de diferentes participantes da cadeia de produção e fornecimento de produtos, mas também adaptar o conceito de segurança.
[52] No original, "*As a matter of principle, the new regulatory framework for AI should be effective to achieve its objectives while not being excessively prescriptive so that it could create a disproportionate burden, especially for SMEs. To strike this balance, the Commission is of the view that it should follow a risk-based approach".*

nível de criticidade de uma IA e, de acordo com isso, empregar ferramentas regulatórias apropriadas.

Apesar de não determinar claramente o conceito de “alto risco”, apenas associando-o a determinados setores e a certos usos, sugeriu-se que apenas as IAs consideradas potencialmente mais gravosas, independentemente do local de estabelecimento de seus operadores, deveriam ser submetidas a critérios rígidos de regulação, devendo passar por um processo de *avaliação prévia de conformidade* antes de entrarem no mercado europeu.

Esse processo avaliaria fatores da elaboração dos sistemas de IA, relacionados 1) aos dados de treinamento, 2) aos registros de uso de dados; 3) à informação e transparência; 3) à robustez e precisão; 4) à supervisão humana; e, em alguns casos específicos, 5) a requisitos especiais voltados a especialidade das funções desempenhadas pela IA, como no caso de identificação biométrica.

No caso das IAs de baixo risco, o processo de avaliação desses critérios não seria obrigatório. Entretanto, elas poderiam ser voluntariamente submetidas à avaliação a fim de receberem uma espécie de *selo de qualidade*, ou *selo de aprovação*, emitido pela UE, potencialmente tornando-se produtos percebidos como mais confiáveis pelos consumidores.

Essas avaliações de conformidade, na proposta do Livro Branco, seriam realizadas conjuntamente por autoridades de supervisão de diversos setores de diferentes Estados-Membros, a fim de complementar a expertise necessária ao processo e favorecer o monitoramento do ecossistema regulatório.

Previu-se que centros de testes independentes poderiam conduzir auditorias e avaliações dos sistemas de IA, segundo os requisitos do Livro Branco, a fim de aumentar a confiança dos consumidores e facilitar o trabalho das autoridades de supervisão competentes.

No caso de operadores de países terceiros, a entrada dos sistemas de IA no mercado europeu poderia acontecer mediante a aprovação dos órgãos da UE ou, existindo acordo de reconhecimento mútuo, mediante a aprovação dos órgãos dos próprios países terceiros responsáveis por essa avaliação.

Paralelamente, ao longo do tempo, o Parlamento Europeu adotou diversas resoluções sobre a incidência da IA em campos como ética, responsabilidade, direitos do autor, direito penal, educação, cultura e setor audiovisual. Entretanto, ainda demandava, na forma do artigo 225º do TFUE, que a Comissão adotasse uma norma abrangente sobre o tema.

Dessa forma, em 2021, após consulta pública, a UE começou a debater a *Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de Inteligência Artificial (Regulamento de Inteligência Artificial) e altera determinados atos legislativos da União* (União Europeia, 2021a). Atualmente, o projeto está em fase de negociação com os Estados-Membros e espera-se que até o final de 2023 esse novo marco legal seja aprovado (Parlamento Europeu, 2023).

O projeto foi situado como uma iniciativa da UE para alcançar o segundo objetivo enunciado pelo Livro Branco, qual seja, cuidar dos riscos associados a determinadas utilizações da IA por meio do desenvolvimento de um ecossistema de confiança.

Considerando a necessidade de avaliar o impacto da intervenção, primeiramente foram pensadas quatro opções de políticas regulatórias: 1) um instrumento legislativo da UE que criasse um regime de rotulagem voluntária; 2) uma abordagem ad hoc a nível setorial; 3) um instrumento legislativo horizontal da UE que seguisse uma abordagem baseada no risco proporcionada e possivelmente completada por códigos de conduta para os sistemas de IA que não são de risco elevado; e 4) um instrumento legislativo horizontal da UE que estabelecesse requisitos obrigatórios para todos os sistemas de IA, independentemente do risco que representam (União Europeia, 2021a).

Depois de diversos debates, a opção considerada ideal foi a terceira: uma combinação entre análise de risco e códigos de conduta. Nesse quadro, surgiu a proposta, consistente numa abordagem horizontal e flexível, direcionada a quatro objetivos específicos:

> - garantir que os sistemas de IA colocados no mercado da União e utilizados sejam seguros e respeitem a legislação em vigor em matéria de direitos fundamentais e valores da União,
> - garantir a segurança jurídica para facilitar os investimentos e a inovação no domínio da IA,
> - melhorar a governação e a aplicação efetiva da legislação em vigor em matéria de direitos fundamentais e dos requisitos de segurança aplicáveis aos sistemas de IA,
> - facilitar o desenvolvimento de um mercado único para as aplicações de IA legítimas, seguras e de confiança e evitar a fragmentação do mercado (União Europeia, 2021a)

O projeto para o Regulamento de IA tem a pretensão de estabelecer um quadro sólido de regulação, respeitando os direitos fundamentais, mantendo as normas já existentes e criando uma metodologia de análise de riscos, para garantir que apenas as IA com grande potencial

ofensivo à saúde, à segurança e aos direitos fundamentais dos indivíduos sejam sujeitas a um sistema rígido de regulação, construído a partir de "requisitos obrigatórios horizontais para uma IA de confiança" e "procedimentos de avaliação da conformidade antes de poderem ser colocados no mercado da União" (União Europeia, 2021a).

A escolha de um regulamento como o instrumento legislativo a ser implementado deu-se com base no propósito de evitar uma atuação fragmentada ou singularizada pelos Estados-Membros. A Comissão entendeu que o ideal seria que esse novo marco fosse aplicável diretamente, com base no artigo 288º do TFUE, com vistas à promoção de um mercado único para sistemas de IA, garantindo simultaneamente a confiança e a segurança jurídica.

A nova legislação visará garantir que os produtos finais integrados a algum tipo de IA sejam seguros, mas somente será aplicada aos casos ainda não regulados por outras legislações específicas, como a direcionada a automóveis autônomos[53].

No caso das IAs de baixo risco, "apenas são impostas obrigações de transparência bastante limitadas, por exemplo, no que diz respeito à prestação de informações para sinalizar a utilização de um sistema de IA quando este interage com seres humanos" (União Europeia, 2021a).

Assim como pensado no Livro Branco, a estrutura necessária terá como base a adaptação das construções regulatórias já existentes, não somente sobre IA, mas também sobre proteção de dados, defesa dos consumidores e prestação de serviços digitais. Dessa forma, criar-se-á um sistema de governança comunitário, centrado na criação do *Comitê Europeu para a Inteligência Artificial*.

Esse ecossistema também contará com centros de testes responsáveis por apoiar a inovação, com o objetivo de reduzir cargos regulamentares que obstaculizem o desenvolvimento tecnológico.

O projeto prevê que a Comissão Europeia será encarregada de acompanhar os efeitos da opção regulatória implementada e de criar um sistema de registro público de aplicações de risco elevado, alimentada pelas informações obrigatoriamente fornecidas pelos operadores e fornecedores de sistemas de IA.

---

[53] No caso, a "*COMMISSION IMPLEMENTING REGULATION (EU) 2022/1426 of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles*".

Ademais, “fornecedores de IA serão obrigados a informar as autoridades nacionais competentes sobre incidentes graves ou anomalias que constituam infrações às obrigações em matéria de direitos fundamentais assim que tomarem conhecimento das mesmas, bem como sobre eventuais recolhas ou retiradas de sistemas de IA do mercado” (União Europeia, 2021a).

As autoridades, nesse contexto, serão responsáveis por investigar tais incidentes e colaborar com o dever da Comissão de realizar, futuramente, um relatório sobre o mercado global da IA.

A proposta detalha o âmbito de aplicação das novas regras e definições relevantes, os quais serão descritos por uma perspectiva “tecnologicamente neutra”. Veja-se algumas das definições propostas:

> 1) «Sistema de inteligência artificial» (sistema de IA), um programa informático desenvolvido com uma ou várias das técnicas e abordagens enumeradas no anexo I, capaz de, tendo em vista um determinado conjunto de objetivos definidos por seres humanos, criar resultados, tais como conteúdos, previsões, recomendações ou decisões, que influenciam os ambientes com os quais interage;
>
> 2)«Fornecedor», uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que desenvolva um sistema de IA ou que tenha um sistema de IA desenvolvido com vista à sua colocação no mercado ou colocação em serviço sob o seu próprio nome ou marca, a título oneroso ou gratuito;
>
> 3)«Fornecedor de pequena dimensão», um fornecedor que seja uma micro ou pequena empresa na aceção da Recomendação 2003/361/CE da Comissão 61 ;
>
> 4)«Utilizador», uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que utilize, sob a sua autoridade, um sistema de IA, salvo se o sistema de IA for utilizado no âmbito de uma atividade pessoal de caráter não profissional;
>
> (...)
>
> 29)«Dados de treino», os dados usados para treinar um sistema de IA mediante o ajustamento dos seus parâmetros passíveis de serem aprendidos, incluindo os pesos de uma rede neuronal;
>
> 30)«Dados de validação», os dados utilizados para realizar uma avaliação do sistema de IA treinado e para ajustar os seus parâmetros não passíveis de serem aprendidos e o seu processo de aprendizagem, a fim de, entre outros objetivos, evitar um sobreajustamento; sendo que o conjunto de dados de validação pode ser um conjunto de dados separado ou parte de um conjunto de dados de treino, quer como divisão fixa ou variável;
>
> 31)«Dados de teste», os dados utilizados para realizar uma avaliação independente do sistema de IA treinado e validado, a fim de confirmar o desempenho esperado desse sistema antes de ser colocado no mercado ou em serviço;
>
> 32)«Dados de entrada», os dados fornecidos a um sistema de IA, ou por ele obtidos diretamente, com base nos quais o sistema produz um resultado;
>
> 33)«Dados biométricos», dados pessoais resultantes de um tratamento técnico específico das características físicas, fisiológicas ou comportamentais de uma pessoa singular, os quais permitem obter ou confirmar a identificação única dessa pessoa

> singular, nomeadamente imagens faciais ou dados dactiloscópicos; (União Europeia, 2021a).

Aprovado o Regulamento, serão elaboradas uma lista de abordagens e técnicas de desenvolvimento de IA e uma lista de práticas proibidas por violarem os valores da União, como aquelas com potencial de manipular as pessoas por meio de técnicas subliminares que lhes passam despercebidas, explorar as vulnerabilidades de grupos específicos e promover uma classificação social pelas autoridades públicas.

Um ponto importante do projeto é aquele que esclarece o que seriam sistemas de risco elevado, criando um sistema de classificação quanto ao risco, baseado em duas categorias:

> - sistemas de IA concebidos para serem utilizados como componentes de segurança de produtos que estão sujeitos a uma avaliação da conformidade ex ante por terceiros,
> - ·outros sistemas de IA autónomos com implicações em matéria de direitos fundamentais que são explicitamente mencionados no anexo III (União Europeia, 2021a)

Além disso, a proposta trata da fixação requisitos legais aplicáveis aos sistemas de IA de risco elevado relativamente aos dados e à governação de dados, à documentação e à manutenção de registos, à transparência e à prestação de informações aos utilizadores, à supervisão humana, à solidez, à exatidão e à segurança.

Esses requisitos seriam, na verdade, o mínimo esperado de um operador diligente e guardariam relação com normas e outras especificações técnicas desenvolvidas com conhecimentos gerais da engenharia e da ciência.

Serão determinadas, no Regulamento, as obrigações horizontais aos fornecedores de IA de risco elevado e os procedimentos de avaliação da conformidade que devem ser seguidos para cada tipo de sistema de IA de risco elevado.

Outrossim, regular-se-ão as obrigações de transparência aplicáveis a determinados sistemas, medidas de apoio à inovação, opções de governança comunitária e nacional e quadro de criação de códigos de conduta.

Apesar de não ser possível, neste trabalho, adentrar todas as especificidades do Regulamento proposto, é possível identificar, não somente nele, mas em todos os documentos

analisados, uma abordagem regulatória muito diferente daquela notada no âmbito da proteção de dados pessoais.

De fato, a UE continua adotando como base o direito constitucional comunitário, na forma dos seus direitos fundamentais. Contudo, na regulação da IA, passa a emprega-los por meio de instrumentos menos rígidos e menos abrangentes.

Interessante, nesse ponto, retomar o comentário do AI HLG nas Orientações, sobre como os direitos fundamentais fazem parte tanto da primeira componente do modelo para IA, de natureza legislativa, quanto da segunda, de natureza ética. Essa diferenciação guarda notável relação com os ensinamentos de Luciano Floridi sobre a diferença entre *soft ethics* e *hard ethics*.

Dessa maneira, pode-se dizer que a forma como os direitos fundamentais foram apresentados no *modelo para a proteção de dados* emprega-os exclusivamente na forma de *hard ethics*. Com isso, quer-se dizer que os direitos fundamentais, além de regras vinculantes *per si*, serviram como princípios para a criação de um marco regulatório abrangente e rígido, no sentido de se comprometer primordialmente com os direitos fundamentais da CDFUE.

Diferentemente, o modelo regulatório para IA parece dividir-se em dois braços: um regulatório no sentido tradicional e legislativo, relacionado à *hard ethics*, e outro aliado ao sentido do *soft law* e, ainda, à *soft ethics*, estas sendo, evidentemente, muito mais propensas a se tornarem instrumentos de influência no âmbito internacional, uma vez que vistas não como ferramentas prescritivas, mas sim sugestivas, como conselhos derivados de algo acima da moralidade, da cultura e das pluralidade humanas, existindo num plano quase metafísico.

Apesar de ser uma proposta bem mais centrada na proteção aos consumidores, quando comparada, por exemplo, à estadunidense, apresentada no capítulo seguinte, a visão europeia sobre regulação da IA parece optar por um método menos tradicional de regulação.

Em parte, isso pode dar-se à necessidade de adoção de ferramentas regulatórias mais flexíveis, como indicado pelo relatório *Reguladores da Comunicação para o Futuro* (OCDE, 2022), pela *Recomendação do Conselho para uma Governança Regulatória Ágil para Potencializar a Inovação* (OCDE, 2023b) e pela *Orientação Prática sobre Governança Regulatória Ágil para a Potencializar a Inovação* (OCDE, 2023a).

De fato, propõe a adaptação das políticas e ferramentas regulatórias tradicionalmente empregadas, quais sejam, os direitos da CDFUE e as normas específicas do direito comunitário europeu, incrementando-as com a proposta de análise de risco e de supervisão rígida apenas

nos casos de sistemas de IAs de alto risco. Restringe, portanto, suas regras prescritivas aos casos em que absolutamente necessário para garantir a segurança jurídica.

Ao centrar-se no conceito de risco, a UE consegue, justamente, favorecer uma abordagem orientada aos resultados e tornar seu ecossistema regulatório *imune ao futuro*, uma vez que será condicionado menos ao quadro legal e mais a avaliações caso a caso, tendo como objetivo garantir que os produtos finais dos sistemas de IA sejam confiáveis.

Inclusive, o caminho que a UE está escolhendo para regular a IA tem o potencial de assemelhar-se à forma como a Diretiva 95/46/CE e o RGPD lidaram com o fluxo internacional de dados, na medida que sistemas de IA só poderão ser implementados no território europeu mediante a aprovação dos órgãos da UE ou, existindo acordo de reconhecimento mútuo, mediante a aprovação dos órgãos de países terceiros.

Entretanto, outra parte da responsabilidade por essa mudança provavelmente tem a ver com o modelo europeu de proteção de dados ser considerado, por alguns, demasiado rígido e prejudicial ao desenvolvimento tecnológico.

> Os críticos argumentam que as disposições de privacidade e transparência de dados do GDPR estão afetando as empresas de tecnologia europeias, principalmente no que diz respeito aos investimentos relacionados à IA. Por exemplo, o GDPR exige que as empresas ofereçam aos indivíduos o direito a uma revisão humana de uma decisão tomada por um sistema automatizado (IA), o que aumenta os custos. Os críticos argumentam que, sem uma reforma, o GDPR reduzirá os investimentos relacionados à IA na Europa e transferirá ainda mais esses investimentos para a China e os Estados Unidos (Engelke, 2020, p. 4, tradução livre)[54].

De toda forma, é preciso esperar para que o tempo revele como será implementada tal política regulatória e se a UE conseguirá estabelecer um ecossistema regulatório bem sucedido em proteger tanto os interesses dos cidadãos quanto os empresariais e os governamentais.

[54] No original, "*Critics argue that the GDPR's data privacy and transparency provisions are having an impact on European tech firms, specifically AI-related investment. For example, the GDPR requires firms to give individuals the right to a human review of a decision made by an automated (AI) system, which raises costs. Critics argue that, without reform, the GDPR will depress AI-related investment within Europe and shift even more of it to China and the United States*".

2. No "Novo Mundo", Os Estados Unidos Da América

2.1. A Proteção De Dados Como Desdobramento Da Privacidade

2.1.1. As Características Principais do Sistema Americano

Ainda conforme a proposta de Baumer, Earp e Poindexter (2004, p. 401), para entender o modelo regulatório dos EUA para a proteção de dados pessoais, é preciso ter em mente suas particularidades históricas e culturais.

Nesse sentido, primeiramente se observa um contexto caracterizado pelo federalismo e pela influência da tradição do *common law*, de forma que o direito estadunidense assume traços específicos em cada um dos Estados federados, que possuem evidente autonomia para decidir e legislar sobre os mais diversos assuntos.

A dimensão constitucional do modelo regulatório estadunidense, diferentemente da europeia, não tem como base a previsão da proteção de dados, mas da privacidade. Sem nunca mencionar expressamente a palavra *privacy*, as Emendas Primeira, Quarta e Quinta são consideradas o corolário da proteção à vida privada nos EUA.

É diante dessa realidade que Daniel Solove, em *The Digital Person*, explica como o direito à privacidade teve os seus fundamentos influenciados pelo artigo *The Right to Privacy*, de Warren e Brandeis.

Os autores, no artigo supracitado, propõem que, apesar de uma preocupação inicial, o *common law* da época poderia se adaptar às invasões à privacidade promovidas pelo jornalismo sensacionalista, que havia se intensificado no século XIX, com o aumento da circulação de jornais e com a popularização das fotografias (Solove, 2006, p. 57).

Foi o que aconteceu, uma vez que as cortes da época reagiram por meio da criação de quatro *privacy torts*[55]: invasão de privacidade, divulgação pública de fatos privados, luz falsa e apropriação (Solove, 2006, pp. 59-62)[56]. Como explica Solove, embora essas ações tenham sido

[55] O *Tort Law*, nos EUA, é o ramo do direito privado que, a partir das normas criadas pelo *common law* e das leis estaduais, lida com a compensação das vítimas de ilícitos cíveis. Parte da ideia de que toda pessoa deve ser responsabilizada pela lesão ao direito alheio, assim como pelos danos sofridos em decorrência dessa lesão. Os *torts* são, nesse contexto, remédios ou instituições do direito civil para lidar com diferentes tipos de ilícitos civis, sendo categorizados em três grandes grupos: intencionais, negligentes e responsabilidade objetiva. Portanto, percebe-se que o *Tort Law* seria comparável ao ramo da Responsabilidade Civil no *civil law*.

[56] No inglês, "*intrusion upon seclusion, public disclosure of private facts, false light e appropriation*".

relevantíssimas para a proteção à privacidade e até hoje sejam utilizadas, elas não são úteis para a proteção de dados pessoais. Esta é, de fato, uma nova dimensão desencadeada pelas novas tecnologias, tendo como ponto de origem a privacidade.

Dessarte, o autor defende que o sistema americano possui fragilidades que prejudicam a efetiva proteção de dados pessoais, o que levaria, como será demonstrado, às exaustivas tentativas de adequação ao modelo europeu, muito mais abrangente. Veja-se, ainda, que essas fragilidades também representam os motivos pelos quais parece haver, nos EUA, uma obsolescência da disciplina legal em relação às tecnologias reguladas, a qual só parece ter sido percebida nos últimos 5 (cinco) anos, como se verá nos próximos tópicos.

Primeiramente, a proteção constitucional estaria sujeita às vontades dos governos, possuindo um alcance limitado, em especial nos casos de violações de direitos individuais pelos próprios particulares (Solove, 2006, pp. 62-64).

Em segundo lugar, as decisões da Suprema Corte, embora reconheçam costumeiramente a proteção constitucional à privacidade, falhariam em compreender o problema para além dos *torts* já consagrados (Solove, 2006, pp. 64-80).

Em terceiro lugar, o distanciamento do direito contratual em relação à proteção à privacidade criaria deformidades no sistema, impedindo a interação ideal entre diferentes direitos e liberdades consagrados pela Constituição americana (Solove, 2006, pp. 64-80).

Por fim, a produção legislativa estadunidense seria demasiado esparsa, com algumas poucas leis federais sobre privacidade, sempre direcionadas a temas muito específicos, como nos casos da *Lei de Privacidade de 1974*[57], da *Lei de Privacidade de Comunicação Eletrônica de 1986* (ECPA)[58], da *Lei de Portabilidade e Responsabilidade de Seguros de Saúde de 1996* (HIPAA)[59], da *Lei de Proteção e Privacidade Online Infantil de 1998* (COPPA)[60], da *Lei Gramm-Leach-Bliley* ou (GLBA)[61], e da *Lei Federal de Gestão da Segurança da Informação de 2002* (FISMA)[62].

Anualmente, diversos projetos de lei relacionados à proteção de dados são submetidos à avaliação do Congresso, mas muitos deles não chegam a sair do seu comitê de origem.

---

[57] No inglês, *the Privacy Act of 1974*.
[58] No inglês, t*he Electronic Communications Privacy Act of 1986*.
[59] No inglês, *the Health Insurance Portability and Accountability Act of 1996*.
[60] No inglês, *the Children's Online Privacy Protection Act of 1998*.
[61] No inglês, *the Gramm-Leach-Bliley Act* ou *Financial Services Modernization Act of 1999*.
[62] No inglês, *the Federal Information Security Management Act of 2002*.

Um dos projetos de lei que ainda aguarda votação e pode ser promissor do ponto de vista da abrangência do seu conteúdo, é o que prevê a criação da *Lei de Privacidade de Dados de 2023*[63]. Apresentado em fevereiro de 2023 pelo republicano Patrick McHenry, o projeto já foi aprovado pelo comitê. Em seguida, foi encaminhado o relatório de recomendação às casas do Congresso, para aguardar sua votação.

Segundo o GovTrack, *website* não oficial que abastecido pelos dados fornecidos pelo Congresso, o projeto possui 41% de chance de ser aprovado, com base nos critérios:

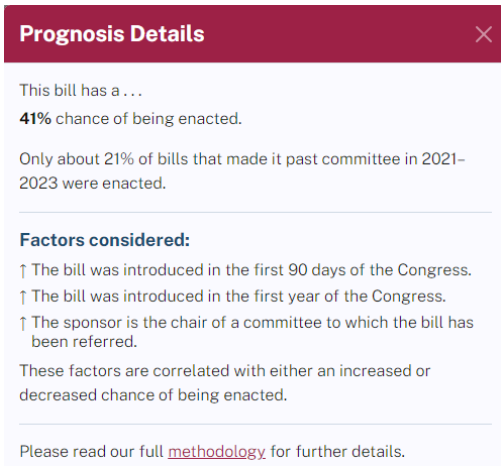

Imagem 1 – Colação da página do GovTrack sobre o projeto da Lei de Privacidade de Dados de 2023

Fonte: GovTrack. **H.R. 1165: Data Privacy Act of 2023**. GovTrack. Disponível em: https://www.govtrack.us/congress/bills/118/hr1165. Acesso em: 05 nov. 2023.

Tramita também a *Lei de Privacidade Online de 2023*[64]. O projeto foi apresentado ao Congresso em abril de 2023 pela democrata Anna Eshoo e aguarda ser considerada pelo Comitê próprio, antes de ser direcionada a uma das Casas do Congresso Americano. Sem embargo, o *website* GovTrack, indica a chance de 1% de ser promulgada, conforme a imagem:

[63] No inglês, *Data Privacy Act of 2023*.
[64] No inglês, *Online Privacy Act of 2023*.

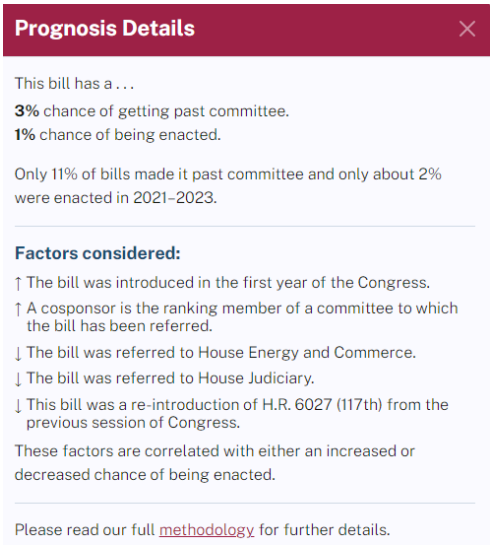

Imagem 2 – Colação da página do GovTrack sobre o projeto da Lei de Privacidade Online de 2023

Fonte: GovTrack. **H.R. 2701: Online Privacy Act of 2023**. GovTrack. Disponível em: https://www.govtrack.us/congress/bills/118/hr2701. Acesso em: 05 nov. 2023.

Outros projetos de lei que estão em trâmite legislativo possuem um escopo evidentemente especializado, como é o caso *da Lei de Pesquisa Tecnológica para Aprimoramento da Privacidade*[65], da *Lei de Proteção à Privacidade dos Americanos em Movimento*[66], da *Lei de Privacidade Financeira de 2023*[67], entre outras.

Tal ponto demonstra, na prática, o posicionamento de Solove sobre as leis estadunidenses de proteção de dados, que "frequentemente não abordam adequadamente as relações de poder subjacentes e contêm amplas exceções e brechas que limitam sua efetividade" [68] (SOLOVE, 2006, p. 71, tradução livre).

Complementarmente, Chris Hoofnagle afirma que, nos EUA, há legislações sobre tipos de dados específicos, que normalmente focam, separadamente, ou no setor privado ou no setor público:

> A abordagem americana trata o tratamento de dados como lícito, a menos que uma regra específica o proíba (...) Em um nível elevado, ele deve atender às diretrizes de qualidade de dados: deve ser justo, legal, necessário e não excessivo. A justiça se traduz, grosso modo, em transparência, uma norma adotada nos Estados Unidos. Mas

[65] No inglês, *Privacy Enhancing Technology Research Act*.
[66] No inglês, *Moving Americans Privacy Protection Act*.
[67] No inglês, *Financial Privacy Act of 2023*.
[68] No original, "*they often fail to adequately address the underlying power relationships and contain broad exceptions and loopholes that limit their effectiveness*".

> as regras sobre necessidade e processamento excessivo estão presentes apenas em alguns códigos estatutários (Hoofnagle, 2016, p. 767, tradução livre)[69].

Aliás, essa dispersão temática das normas de proteção aos dados pessoais é um dos principais elementos do modelo estadunidense e é o ponto utilizado frequentemente como parâmetro de comparação com o modelo abrangente, exemplificado neste trabalho pela abordagem da UE.

Além dessa característica de especificidade, típica do aspecto legislativo da proteção de dados nos EUA, uma outra característica definidora do modelo estadunidense é a preferência pela autorregulação, presente em todos os acordos firmados com a UE, como se passa a demonstrar.

2.1.2. *Strike one*! O Acordo de Porto Seguro

O *Acordo de Porto Seguro*[70] foi desenvolvido em um cenário pós-Diretiva 95/46/CE, com o fim de facilitar as transferências dos dados advindos da UE para tratamento por empresas estadunidenses e dar fim às limitações que prejudicavam a relação UE-EUA, em especial no aspecto comercial (Veronese, 2021).

Assim, a Comissão Europeia, auxiliada pelo Grupo de Trabalho do Artigo 29° (Veronese, 2021) e por meio da Decisão 2000/520/CE, considerou o regime do Acordo de Porto Seguro adequado ao nível de proteção da UE (União Europeia, 2000). O acordo baseava-se num modelo autorregulatório implementado a partir de sete princípios: 1) aviso/informação; 2) escolha/opção; 3) retransmissão de dados; 4) segurança; 5) integridade; 6) acesso; e, 7) aplicação/proteção.

As empresas interessadas deveriam aderir a esses princípios e às orientações do Departamento de Comércio dos Estados Unidos (DoC), prevendo que as únicas exceções ao Acordo ocorreriam à extensão necessária para atender requisitos de segurança nacional, interesse público, ou cumprimento da lei (Terpan, 2018).

---

[69] No original, "*The American approach treats data handling as legal unless a specific rule prohibits (...) On a high level, it must meet data quality guidelines: it must be fair, lawful, necessary, and not excessive. Fairness translates roughly to transparency, a norm embraced in America. But the rules on necessity and excessive processing are only present in a few statutory codes*".

[70] No inglês, *Safe Harbor Agreement*.

Tratava-se de um processo de autocertificação, que implicava na assunção, pelas empresas, dos compromissos de fornecer avisos acerca da coleta de dados, de dar a oportunidade de recusar a divulgação de informações a terceiros ou o seu uso para fins inesperados, de garantir que quaisquer terceiros proporcionem a proteção adequada, de tomar precauções razoáveis para proteger os dados retidos, de usar os dados somente para os fins pretendidos, de garantir a precisão dos dados retidos, de fornecer acesso às informações relevantes aos titulares e de estabelecer mecanismos de reclamação e fiscalização (Carlson, 2021, pp. 203-204).

De fato, o Acordo de Porto Seguro deu grande autonomia para as empresas e colocava um grande peso nas suas políticas de privacidade, havendo apenas a fiscalização pela *Federal Trade Commission* (FTC).

Entretanto, segundo Alexandre Veronese, "a aplicação dos princípios nunca foi pacífica e tranquila" (2021, p. 703), de forma que:

> O "acordo de porto seguro", contudo, não conseguiu ser mantido. Já havia um movimento de cidadãos na Europa que estava incomodado com a prevalência das empresas gigantes da Internet e com o aparecimento de um enorme mercado de coleta de meta-dados. Não obstante, o ponto final no processo de derrocada do *Safe Harbor Agreement* ocorreu com as revelações jornalísticas do caso PRISM – nome do programa de computador e do sistema eletrônico de coleta – ou de Edward Snowden, em 2013. Todavia, há uma questão jurídica que estava no centro do debate: o estatuto jurídico aplicável aos metadados dos usuários, seja nos Estados Unidos da América, seja na União Europeia. O direito federal dos Estados Unidos da América determina a retenção dos conteúdos e dos metadados pelas empresas, em razão da possibilidade de que eles sejam demandados por órgãos de segurança. A obrigação deriva da subseção (a) da Seção 2.703 do Título 18 do United States Code ("Crimes and Criminal Procedure; and Appendix"). Essa Seção é uma parte do Stored Communications Act, de 1986, que, por conseguinte, era uma parte do Electronic Communications Privacy Act. O objetivo dessa lei federal era atualizar, ao mundo eletrônico, as regras de intercepção de comunicações no direito federal estatutário dos Estados Unidos. A subseção (a) da Seção 2.703 determina que uma entidade governamental – seguindo diversos ritos legais específicos – pode demandar os conteúdos armazenados por até cento e oitenta dias. Cabe frisar que, salvo em casos excepcionais e previstos na própria Seção 2.703 do Título 18, a obtenção desses dados pessoais, sem a ciência do interessado, exige a concessão de um Warrant, que é uma ordem judicial qualificada em consonância com os termos da Quarta Emenda da Constituição dos Estados Unidos da América. No tocante aos registros de serviços de conexão e de sessões de telefonia ou computação – metadados –, eles são regulados pela subseção (c) da Seção 2.703 e podem ser obtidos pelos órgãos governamentais por uma pluralidade de meios (Veronese, 2021, p. 703).

Foi nesse contexto que o Tribunal de Justiça da União Europeia (TJUE), no caso *Shrems I*, entendeu que Decisão 2000/520/CE, que aprovou o Acordo de Porto Seguro, não

estava alinhada com a Diretiva, posto que não incluía qualquer avaliação das regras estadunidenses e não comprovava a existência de um nível de proteção adequado (TJUE, 2015).

Na ocasião, também decidiu que as autoridades nacionais de proteção de dados teriam autoridade para exercer controle sobre determinadas situações referentes às decisões de adequação, desde que não as declarassem inválidas[71].

2.1.2. *Strike two*! O Escudo de Privacidade

Diante da anulação do acordo anterior, ainda durante o governo Obama, o *Escudo de Privacidade*[72] começou a ser negociado, tendo sido concluído em 2016, durante o governo Trump, e considerado adequado pela Decisão de Execução UE 2016/1250 da Comissão Europeia (União Europeia, 2016a).

O Escudo de Privacidade, semelhantemente ao Acordo de Porto Seguro, tinha como fundamento um sistema de autocertificação, através do qual organizações dos EUA assumiam o compromisso de seguir um conjunto de princípios – *aviso; integridade dos dados e limitação dos fins; escolha; segurança; aceso; recurso, aplicação e responsabilidade*. Esse regime era complementado por princípios suplementares determinados pelo DoC, pelo qual também seria fiscalizado, juntamente à FTC e ao Departamento de Transporte (DoT).

Veronese explica que a forma como "o governo Obama produziu um conjunto de políticas públicas" levou a uma "aproximação maior com o marco jurídico e político da União Europeia" e serviu como "tentativa de institucionalizar figuras para proteção da privacidade que não existiam nos Estados Unidos da América" (Veronese, 2021, p. 711).

O Escudo teria como diferencial as figuras do *Privacy Shield ombudsperson*; *Privacy and Civil Liberties Oversight Board*; a revisão do *Patriot Act* e de outras leis relativas ao sistema de inteligência estadunidense. Dessa forma, o novo acordo não seria apenas uma renovação do Acordo de Porto Seguro. De fato, dentro dos limites da tradição jurídica estadunidense, teria

[71] Esse foi um ponto relevante na decisão, uma vez que Max Shrems, o ativista que inicou a ação, havia requisitado à *Irish Data Protection Commissioner* a proibição da transferência de dados pelo Facebook Ireland, considerando a proteção insuficiente dos dados. A autoridade, todavia, rejeitou a demanda, apresentando como fundamento a existência da decisão de adequação relativa ao *Safe Harbor*.
[72] No inglês, *Privacy Shield*.

havido uma tentativa de fortalecer a proteção de dados pessoais a nível institucional (Veronese, 2021, p. 711).

Partindo de uma perspectiva um pouco diferente, Marc Rotenberg, no artigo *Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection*¸ disserta sobre os principais problemas do acordo de 2016.

Nesse ínterim, chama atenção para *a Lei de Esclarecimento do Uso Legal de Dados no Exterior* (CLOUD)[73], que fixou o alcance extraterritorial das agências reguladoras para vigiar os dados armazenados em outras jurisdições (Rotenberg, 2020).

Outrossim, salienta a falha da FTC no caso *Facebook-Cambridge Analytica*, uma vez que ambas organizações eram certificadas sob o Escudo de Privacidade, e a falha na tentativa de reforma das práticas de vigilância em massa fundamentadas na Seção 702 da *Lei de Vigilância de Inteligência Estrangeira de 1978* (FISA)[74]; entre outros problemas coexistentes ao Escudo de Privacidade (Rotenberg, 2020, pp. 5-7).

Por sua vez, Fabien Terpan observa que, em comparação ao Acordo de Porto Seguro, no Escudo de Privacidade, as organizações privadas estariam sujeitas a "maiores compromissos com relação a notificações, limites de retenção de dados, direitos de acesso, publicidade de políticas de privacidade"[75] (Terpan, 2018, p. 1051, tradução livre).

Outra evolução em relação ao acordo anterior seriam os compromissos escritos assumidos pelo Departamento de Justiça e pelo Diretor de Inteligência Nacional, no sentido de garantir que "o acesso das agências de segurança aos dados europeus serão claramente limitados e controlados"[76] (Terpan, 2018, p. 1051, tradução livre).

Apesar das melhoras, o autor ainda entende que o *Privacy Shield* seria um caso de conformidade parcial em relação à proteção de dados pessoais promovida pela UE:

> O Privacy Shield também gera preocupações tanto na dimensão comercial quanto na de segurança. Pelo menos três tipos de deficiências afetam a parte comercial do Privacy Shield. (...) Com relação à dimensão da segurança, já mencionamos que o mecanismo ainda se baseia em cartas de autoridades públicas dos EUA, mais do que em compromissos legais reais. Embora o Office of the Director of National Intelligence declare que se absterá de coletar quantidades maciças e indiscriminadas

[73] No inglês, *Clarifying Lawful Overseas Use of Data Act of 2018.*
[74] No inglês, *Foreign Intelligence Surveillance Act* of 1978.
[75] No original, "*greater commitments with regard to notifications, limits to data retention, rights of access, publicity of privacy policies*".
[76] No original, "*security agencies' access to European data will be clearly limited and controlled*".

> de dados, não há meios legais para garantir que eles respeitarão essa declaração de intenção. Até mesmo a independência da ombudsperson continua sendo um problema, pois ela trabalha sob o comando do vice-secretário do Departamento de Estado dos EUA. O fato de a Comissão, em sua decisão de adequação, ter mencionado a independência do Ombudsman não é exatamente uma garantia de que essa independência será efetiva. (...) Embora os procedimentos de reclamações tenham melhorado, a eficácia do Privacy Shield dependerá, como foi o caso de seu antecessor, da disposição da Federal Trade Commission. Quanto às autoridades públicas, elas fizeram uso, em grande parte e indiscriminadamente, da exceção relativa à segurança nacional. Se as mesmas causas produzem os mesmos efeitos, há motivos suficientes para acreditar que as práticas que não respeitam a vida privada e a proteção de dados persistirão. Assim, o Privacy Shield parece ter cumprido apenas parcialmente a decisão de Schrems. Embora talvez não tenha retornado totalmente à estaca zero, já que algumas melhorias foram feitas, ele claramente não avançou muito mais, levando a dúvidas sobre a legalidade do novo regime (Terpan, 2018, pp. 1052-1053, tradução livre)[77].

De fato, em 2020, no caso *Schrems II*, o TJUE declarou inválida a Decisão que teria considerado os EUA um país terceiro assegurador de um nível de proteção adequado.

Foi um resultado que o próprio Max Schrems, ativista que levou tanto o Acordo de Porto Seguro quanto o Escuro de Privacidade ao TJUE, havia previsto em um artigo de 2016, em que afirmou que a continuidade da vigilância em massa pelo governo estadunidense levaria a um novo caso "*Schrems*" (Carlson, 2021, p. 203 *apud* Schrems, 2016).

No entender da corte, o sistema existente, apesar de limitar a forma como as empresas lidavam com os dados dos titulares, não limitava a liberdade às autoridades públicas estadunidenses de acessar de modo generalizado todo esse conteúdo.

De fato, mesmo a supervisão exercida pela FTC, estaria limitada aos litígios comerciais, permanecendo o Estado intocado no que diz respeito à oponibilidade do direito à privacidade.

---

[77] No original, "*Privacy Shield also raises concerns on both the commercial and security dimension. At least three types of shortcomings affect the commercial part of Privacy Shield. (…) Regarding the security dimension, we have already mentioned that the mechanism still relies on letters from US public authorities, more than actual legal commitments. While the Office of the Director of National Intelligence declare that they will refrain from collecting massive and indiscriminate amounts of data, there is no legal means to ensure that they will respect this declaration of intent. Even the independence of the Ombudsperson re-mains an issue, as she works under the vice-secretary of the US State Department. The fact that the Commission, in its adequacy decision, has mentioned the independence of the Ombudsperson, is not exactly a guarantee that this independence will be effective. (…) Although complaints procedures have improved, the effectiveness of Privacy Shield will depend, as was the case with its predecessor, on the willingness of the Federal Trade Commission. As for Public authorities, they have largely and indiscriminately made use of the exception concerning national security. If the same causes produce the same effects, there is enough reason to believe that practices that do not respect private life and data protection will persist. Thus, Privacy Shield appears to have only partially complied with the Schrems ruling. While it perhaps did not fully return to square one, as a few improvements have been made, it clearly did not really progress much further, leading to doubts about the legality of the new regime*".

O Tribunal apontou, ainda, a falta de regras sobre essas comunicações de dados a terceiros; a inexistência de previsão de medidas jurídicas corretivas eficazes para ter acesso aos dados pessoais que lhe dizem respeito, ou para obter a retificação ou a supressão de tais dados; entre diversas outras conclusões consagradas na decisão.

Nesse ínterim, percebe-se que nem o Acordo de Porto Seguro nem o Escudo de Privacidade impediram a incidência da Seção 702 do FISA e da *Ordem Executiva 12333*, do presidente Ronald Reagan (OE 12333), que permitem que o governo obrigue qualquer provedor de serviços de comunicações eletrônicas – conceituado de forma bem ampla pela OE – a entregar os dados em seu poder (Carlson, 2021, p. 205).

2.1.3. *Three strikes... and are you out*? O Quadro de Privacidade de Dados UE-EUA

Após a invalidação do Escudo de Privacidade, dois conjuntos de cláusulas contratuais padrão foram editadas e aprovadas pela Comissão, por meio das Decisões (UE) 2021/914 (União Europeia, 2021b) e 2021/915 (União Europeia, 2021c). Sem embargo, tratando-se de um mecanismo alternativo às decisões de adequação, tais decisões não foram suficientes para estabilizar a situação.

Em 3 de julho de 2023, o presidente Joe Biden emitiu a *Ordem Executiva 14086, sobre o aprimoramento das salvaguardas das atividades de inteligência nacional dos Estados Unidos* (OE 14086).

O impacto dessa ordem foi notável, na medida em que introduziu um "mecanismo independente e vinculativo que permite que indivíduos em estados qualificados (definidos como países e organizações de integração econômica regional) (...) busquem reparação por meio da apresentação de uma reclamação qualificada se acreditarem que seus dados pessoais foram coletados por meio da inteligência de sinais dos EUA de uma maneira que violou a lei aplicável dos EUA"[78] (EUA, 2023a, tradução livre).

Nesse âmbito, a OE 14086 criaria de uma nova entidade, o Tribunal de Revisão da Proteção de Dados (DPRC), voltado exatamente para a investigação e solução das reclamações.

[78] No original, "*mechanism enabling individuals in qualifying states (defined as countries and regional economic integration organizations), as designated under the E.O., to seek redress through the submission of a qualifying complaint if they believe their personal data was collected through U.S. signals intelligence in a manner that violated applicable U.S. law*".

Não somente isso, mas seriam adotados como fundamentos a minimização dos dados; a segurança dos dados; a qualidade dos dados; a supervisão das políticas e dos procedimentos; a assistência ao mecanismo de reparação; o treinamento de pessoal; e a necessidade de aprovação para abrir-se exceções a esses procedimentos.

Finalmente, em 10 de julho de 2023, um novo acordo foi firmado e aprovado por decisão de adequação da Comissão Europeia. O *Quadro de Privacidade de Dados UE-EUA* (QPD) passou a permitir, novamente, o livre fluxo de dados entre as duas potências mundiais.

O escopo do acordo é definido no seu item 2.12, segundo o qual "A proteção conferida no âmbito do QPD UE-EUA é aplicável a quaisquer dados pessoais transferidos da União para organizações localizadas nos EUA que tenham certificado a sua adesão aos princípios junto do DoC, com exceção dos dados recolhidos para efeitos de publicação, difusão ou outras formas de comunicação pública de material jornalístico e informação constante de material já publicado e arquivado" (União Europeia, 2023).

O QPD UE-EUA expressamente consagra os mesmos conceitos de "dados/informações pessoais" e "processamento" apresentados pelo RGPD. Por sua vez, define os conceitos de "controladores" e "processadores" de forma semelhante à do RGPD, optando, contudo, por uma redação mais restrita, que não incluir as autoridades públicas. Veja-se a tabela, com destaque aos trechos do texto da UE que foram replicados na decisão UE-EUA:

RGPD	QPD UE-EUA
Artigo 4º (7): «Responsável pelo tratamento», **a pessoa singular ou coletiva**, a autoridade pública, a agência ou outro organismo que, **individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais**; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro	2.1.2 (12) O QPD UE-EUA se aplica a organizações nos EUA que se qualificam como controladoras (ou seja como **uma pessoa ou organização que, individualmente ou em conjunto com outras, determina as finalidades e os meios de processamento de dados pessoais**) (...)
Artigo 4º (8): «Subcontratante», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais **por conta do responsável pelo tratamento destes**;	2.1.2 (12) O QPD UE-EUA se aplica a organizações nos EUA que se qualificam como (...) ou processadoras (ou seja, agentes atuando **em nome de um controlador**).

Tabela 2 – Comparação RGPD e QPD EU-EUA – responsável pelo tratamento e subcontratante – elaboração própria

Novamente, o acordo é baseado num sistema de certificações, por meio dos quais as organizações estadunidenses se comprometem pública e imediatamente a respeitar um conjunto de 7 (sete) princípios: 1) limitação da finalidade e escolha, segundo o qual os dados somente podem ser processados de forma legal e justa, conforme as finalidades específicas para que foram coletados, apenas na medida necessária para cumprir com elas; 2) processamento de categorias especiais de dados pessoais, que prevê que os dados considerados "sensíveis" segundo o RGPD devem ser resguardadas de forma específica sob o regime estadunidense; 3) exatidão, minimização e segurança dos dados, que determina que os dados devem ser armazenados de forma exata, atualizada e segura, sem exceder as finalidades para as quais foram coletadas; 4) transparência, conforme o qual os titulares devem ser informados da natureza do processamento de seus dados; 5) direitos individuais, que garante aos titulares direitos que podem ser opostos aos controladores ou processadores, especialmente no que diz respeito ao acesso, à objeção ao processamento, à retificação e ao apagamento de dados; 6) restrição às transferências posteriores, que só poderão acontecer para propósitos limitados e especificados, com base em um contrato com o terceiro e apenas se este garantir um regime de proteção equivalente; 7) *accountability*[79], que determina que as entidades processadoras de dados devem estabelecer e cumprir com medidas técnicas e organizacionais apropriadas para garantir com suas obrigações de proteção de dados, assim como devem ser capazes de demonstrar tais questões perante às autoridades supervisoras.

Cada um desses princípios é objeto de maior detalhamento no documento oficial, e são complementados por outros princípios de natureza suplementar propostos pelo DoC, quais sejam: 1) dados sensíveis; 2) exceções jornalísticas; 3) responsabilidade secundária; 4) realização de *due deligence*[80] e de auditorias; 5) papel das autoridades de proteção de dados; 6) autocertificação; 7) verificação; 8) acesso; 9) dados de recursos humanos; 10) contratos obrigatórios para transferências posteriores; 11) resolução de conflitos e fiscalização; 12) escolha e tempo do *opt out*; 13) informações de viagem; 14) produtos farmacêuticos e médicos; 15) registros públicos e informações disponíveis publicamente; 16) requerimentos de acesso por autoridades públicas (União Europeia, 2023).

[79] Não se traduziu esse conceito por não haver, na língua portuguesa, uma palavra que transmita o sentido exato.
[80] Não se traduziu esse conceito por não haver, na língua portuguesa, uma palavra que transmita o sentido exato. De forma geral, *due diligence* é uma análise acerca de diversos aspectos de uma empresa. Esse procedimento é relevante para o *compliance*, que, segundo Ana Frazão é "em uma definição simplificada, o *compliance* pode ser visto como um conjunto de ações a serem adotadas no ambiente corporativo para que se reforce a anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade" (2021, p. 36).

Embora não seja possível especificar, neste trabalho, cada um desses "princípios", impera explicar que apesar de serem assim nomeados, os enunciados do DoC, na verdade, aparentam ser orientações práticas.

Cuidam, dessa forma, de procedimentos e tipos de dados específicos, possivelmente servindo como elementos para a interpretação dos demais princípios e procedimentos determinados no Quadro.

Ademais, as organizações certificadas devem publicar e cumprir com suas políticas de privacidade, bem como se sujeitar aos poderes investigatórios e fiscalizatórios da FTC ou do DoT.

O DoC compromete-se a verificar o cumprimento, pelas organizações, dos requisitos de autocertificação; a facilitar a cooperação por meio de órgãos de resolução alternativa de conflitos do setor privado; a acompanhar as organizações que queiram ser ou tenham sido removidas da Lista do QPD; a buscar e corrigir situações de falsas alegações de participação.

Ainda, o DoC deve conduzir, de ofício e periodicamente, revisões e avaliações de conformidade; adaptar o *website* do QPD UE-EUA para o público-alvo; facilitar a cooperação com as autoridades de proteção de dados; cumprir com os seus compromissos do Anexo I; conduzir avaliações conjuntas do funcionamento do QPD UE-EUA com a Comissão; fazer esforços pela atualização das leis; e acompanhar eventuais reclamações diante da OE 14086.

A FTC, por sua vez, faz o compromisso de atuar no contexto da proteção ao consumidor e da proteção de dados, como fez desde os acordos anteriores, a exemplo das suas diligências nos casos contra o *Twitter*, o *CafePress* e o *Flo*.

Nesse contexto, garante que irá priorizar as notificações de violação dos princípios do QPD UE-EUA pelas autoridades europeias, assim como aquelas notificações de organizações de autorregulação e outros órgãos de solução independente de disputas.

Com essa finalidade, criou-se um processo-padrão para apurar irregularidades, estabelecendo-se uma cooperação com os Estados-Membros da UE, que foram orientados a passar à FTC informações que ajudem a coordenar sua atuação.

A FTC também compromete-se a continuar sua atuação independente e proativa na fiscalização de problemas de privacidade e segurança envolvendo organizações comerciais; a fiscalizar sistematicamente o *compliance* com o QPD UE-EUA.

O DoT, por sua vez, obriga-se a priorizar as notificações de violação dos princípios do QPD UE-EUA pelas autoridades europeias, a tratar de alegações de participação falsas ou enganosas e a monitorar as ordens executivas sobre violações ao QPD UE-EUA.

Merece destaque o item 3 do QPD UE-EUA, que trata do acesso dos dados pessoais transferidos da UE pelo governo estadunidense, especialmente para fins de aplicação da lei penal e de segurança nacional.

Em síntese, a Decisão que aprovou o novo acordo, nesse ponto, afirma que a Comissão levou em conta que quaisquer limitações ao direito à proteção de dados devem ocorrer por meio legais e de forma proporcional, ou seja, apenas na medida necessária para atender a objetivos específicos de interesse coletivo de uma sociedade democrática[81].

Nesse contexto, a lei deve estabelecer regras claras, precisas e juridicamente vinculantes, além de proteções mínimas, para que as pessoas cujos dados foram transferidos tenham garantias suficientes para proteger efetivamente seus dados pessoais contra o risco de abuso. Apenas nesses termos e em um número limitado de vezes, poderia ocorrer o acesso dos dados transferidos.

Os itens seguintes do tópico 3 fornecem informações complementares acerca das bases legais e dos procedimentos pelos quais dar-se-á o acesso a dados pessoais de cidadãos europeus, tanto pelo judiciário quanto por agências de inteligência nacional e agentes do sistema criminal, como promotores públicos e agentes de investigação federais, os quais precisam, na maior parte dos casos, obter autorização judicial prévia para tratar dados pessoais (3.1.3 [112]).

Dessarte, a estrutura geral do QPD UE-EUA permanece, de forma, a mesma dos acordos anteriores – um sistema de autocertificação baseado em princípios e na fiscalização por órgãos como o DoC, a FTC e o DoT. De fato, são percebidas apenas algumas alterações no que diz respeito ao acesso dos dados pelo governo americano.

Sem embargo, por enquanto é difícil prever se será suficiente reconhecer que as exceções ao direito à proteção de dados só poderão ocorrer mediante autorização legal – até porque, mesmo as ocorridas anteriormente, que levaram à anulação do Escudo de Privacidade, também eram objeto de autorização legal.

[81] Observa-se, nesse ponto, uma grande influência a OE 14086.

É necessário, sem dúvidas, observar como serão executadas algumas das previsões, principalmente sobre o sistema de reclamações e de funcionamento do DPRC, assim como acompanhar as leis americanas, que provavelmente precisarão ser adaptadas para comportar todas as promessas feitas no QPD UE-EUA. Essas são as modificações que parecem ter, de fato, o potencial alterar a realidade estadunidense em termos de proteção de dados.

O tempo revelará, dessa forma, se o novo QPD UE-EUA demonstrará uma mudança da lógica estadunidense, que reflete uma visão da proteção de dados distante da sua dimensão de direito fundamental, e próxima de um pensamento econômico, no sentido de ver os dados pessoais como um recurso, não só para as empresas, mas também para o próprio governo.

O próprio Max Schrems, contudo, se posicionou sobre, revelando ter poucas esperanças sobre o novo marco regulatório:

> Dizem que a definição de insanidade é fazer a mesma coisa várias vezes e esperar um resultado diferente. Assim como o "Privacy Shield", o último acordo não se baseia em mudanças materiais, mas em interesses políticos. Mais uma vez, a Comissão atual parece pensar que a bagunça será problema da próxima Comissão. A FISA 702 precisa ser prorrogada pelos EUA este ano, mas com o anúncio do novo acordo, a UE perdeu qualquer poder para conseguir uma reforma da FISA 702.
>
> (...) Agora temos "Portos", "Guarda-Chuvas", "Escudos" e "Quadros", mas nenhuma mudança substancial na lei de vigilância dos EUA. As declarações à imprensa de hoje são quase uma cópia literal das declarações dos últimos 23 anos. Apenas anunciar que algo é "novo", "robusto" ou "eficaz" não é suficiente perante a Corte de Justiça. Precisaríamos de mudanças na lei de vigilância dos EUA para que isso funcionasse - e simplesmente não as temos.
>
> (...)
>
> Temos várias opções de contestação já na gaveta, embora estejamos cansados desse pingue-pongue jurídico. Atualmente, esperamos que o caso volte ao Tribunal de Justiça no início do próximo ano. O Tribunal de Justiça poderia até mesmo suspender o novo acordo enquanto estiver analisando sua essência. Em nome da segurança jurídica e do Estado de Direito, teremos então uma resposta se as pequenas melhorias da Comissão foram suficientes ou não. Nos últimos 23 anos, todos os acordos entre a UE e os EUA foram declarados inválidos retroativamente, tornando ilegais todas as transferências de dados realizadas no passado pelas empresas - parece que agora vamos acrescentar mais dois anos a esse pingue-pongue.
>
> (...)
>
> A Comissão deve ser a "guardiã dos tratados" e a defensora do "Estado de Direito". Ela adora esse papel quando se trata de Estados-Membros que violam a legislação da UE. Agora, a própria Comissão simplesmente ignora o Tribunal de Justiça pela terceira vez (Noyb, 2023, tradução livre)[82].

[82] No original, "*They say the definition of insanity is doing the same thing over and over again and expecting a different result. Just like 'Privacy Shield' the latest deal is not based on material changes, but by political interests. Once again the current Commission seems to think that the mess will be the next Commission's problem. FISA 702*

2.2. A Inteligência Artificial Como Promessa De Desenvolvimento

2.2.1. A Regulação Deixada ao Livre Mercado

A Universidade de Stanford, em relatório de 2023, aponta que, entre 2010 e 2021, os EUA e a China apresentaram um incremento de quatro vezes no número de pesquisas entre os dois países, se tornando a maior dupla em termos de colaboração entre diferentes países.

Ao contrapor a produção científica dos dois países, contudo, percebe-se uma disputa pela liderança: a China apresenta um maior número de publicações em revistas e repositórios de IA, assim como de conferências sobre o assunto; os EUA, por sua vez, apesar de apresentar menos publicações, continua sendo mais citado – "a maioria dos grandes modelos linguísticos e multimodais do mundo (54% em 2022) é produzida por instituições americanas"[83] (Stanford, 2023, p. 23).

Sem embargo, os EUA parecem ter sido superados pela China e pela UE em termos de passos dados em direção à regulação da IA, possuindo apenas alguns poucos e restritos regulamentos sobre o tema (Carman, 2020, p. 210).

A jornada estadunidense em direção à regulação da IA começou durante o governo Obama, que organizou diversos workshops e criou um subcomitê sobre *Machine Learning* e IA (Schackleford et al., 2022, p. 40). Essas ações, futuramente, foram a fonte de criação de três relatórios: o *Plano Estratégico Nacional de Pesquisa e Desenvolvimento de Inteligência*

---

needs to be prolonged by the US this year, but with the announcement of the new deal the EU has lost any power to get a reform of FISA 702.
(...)
We now had 'Harbors', 'Umbrellas', 'Shields' and 'Frameworks' - but no substantial change in US surveillance law. The press statements of today are almost a literal copy of the ones from the past 23 years. Just announcing that something is 'new', 'robust' or 'effective' does not cut it before the Court of Justice. We would need changes in US surveillance law to make this work - and we simply don't have it.
(...)
We have various options for a challenge already in the drawer, although we are sick and tired of this legal ping-pong. We currently expect this to be back at the Court of Justice by the beginning of next year. The Court of Justice could then even suspend the new deal while it is reviewing the substance of it. For the sake of legal certainty and the rule of law we will then get an answer if the Commission's tiny improvements were enough or not. For the past 23 years all EU-US deals were declared invalid retroactively, making all past data transfers by business illegal - we seem to just add another two years of this ping-pong now.
(...)
The Commission is meant to be the 'guardian of the treaties' and the defender or the 'rule of law'. It loves that role when it comes to Member States violating EU law. Now the Commission itself simply ignores the Court of Justice for the third time".

[83] No original, "*the majority of the world's large language and multimodal models (54% in 2022) are produced by American institutions*".

Artificial, de outubro de 2016[84]; o *Inteligência Artificial, Automação e a Economia*[85], de dezembro de 2016; o *Preparando-Se Para o Futuro da Inteligência Artificial*[86], de dezembro de 2016.

O primeiro desses relatórios, considerado o mais relevante dos três (Schackleford et al., 2022, p. 41) criou estratégias nacionais de incentivo à IA, sugerindo o aumento de investimentos; a criação de métodos de cooperação entre IA e ser humano; a realização de pesquisas sobre implicações éticas, sociais, legais da IA, assim como de métodos de garantir sua segurança e transparência; a criação de bases de dados públicas, a avaliação do desenvolvimento da IA a partir de *benchmarks*, ou seja, parâmetros referências.

Nesse âmbito, o governo federal seria o principal ator:

> O plano estabeleceu sete áreas prioritárias amplas para o governo dos Estados Unidos em relação à pesquisa e ao desenvolvimento da Al. Ele enfatizou o papel que o governo federal desempenha no avanço das atividades de pesquisa, desenvolvimento e educação em Al por meio da promoção da coordenação e colaboração entre as partes interessadas para alavancar recursos intelectuais, físicos e digitais (Schackleford et al., 2022, p. 41, tradução livre)[87].

O segundo, por sua vez, apresentou um caráter essencialmente informativo, na medida em que trazia informações gerais sobre IA: histórico, definições, possíveis usos e principais riscos. Delineava, portanto, o estado da arte até então.

As observações feitas sobre os potenciais negativos demonstravam que a prática estadunidense, já começava a ser direcionada a algumas áreas de implementação da IA, por exemplo, aos carros automatizados, ao uso de algoritmos no sistema criminal e às armas automatizadas.

O terceiro tinha como principal foco o impacto da IA sobre a força de trabalho estadunidense, recomendando brevemente algumas políticas regulatórias para IA: investir no desenvolvimento da IA; educar e treinar os estadunidenses para o futuro, ajudar os trabalhadores na transição para garantir o crescimento geral.

---

[84] No inglês, *The National Artificial Intelligence Research And Development Strategic Plan*.
[85] No inglês, *Artificial Intelligence, Automation, and the Economy*.
[86] No inglês, *Preparing For The Future Of Artificial Intelligence*.
[87] No original, "*The plan established seven broad priority areas for the United States government in relation to Al research and development. It emphasized the role that the federal government plays in advancing research, development, and education activities in Al through fostering coordination and collaboration between stakeholders to leverage intellectual, physical, and digital resources*".

No ano de 2018, o governo Trump sediou a *Conferência de Cúpula da Casa Branca sobre Inteligência Artificial para a Indústria Americana*[88], durante a qual o então assistente do presidente para as políticas tecnológicas, Michael Kratsios, afirmou que a proposta americana seria uma fundamentada no *livre mercado*, o que favoreceria o avanço científico-tecnológico e combinaria os pontos fortes do governo, da indústria e da academia (Carman, 2020, p. 2010 *apud* White House Office of Sciente and Technology Policy, 2018).

Por meio da Conferência, a Casa Branca enfatizou o seu apoio ao desenvolvimento de tecnologias de IA pelo setor privado e afirmou que, como uma forma de incentivo, tinha a intenção de criar de bancos de dados abertos (Schackelford et al., 2022, p. 42).

Em seguida à Conferência, foi publicado o relatório *Inteligência Artificial para Povo Americano*[89], em que foram anunciadas as prioridades da administração da época: "(1) priorizar o financiamento de pesquisas sobre Al, (2) remover barreiras regulatórias para a implantação de tecnologias de Al, (3) treinar a força de trabalho futura, (4) obter vantagens militares estratégicas, (5) aproveitar os serviços governamentais de Al e (6) liderar negociações internacionais de Al"[90] (Schackelford et al., 2022, p. 42, tradução livre).

Segundo Kelly Carman:

> A abordagem de Kratsio é um pouco diferente das apresentadas na UE e na China. Uma economia de livre mercado "promove a produção e a venda de bens e serviços, com pouco ou nenhum controle ou envolvimento de qualquer agência governamental central", que é exatamente o que a UE e a China têm tentado evitar. Em vez de dar importância à manutenção da segurança do Al para uso do consumidor ou à regulamentação dos padrões de desenvolvimento do Al, os EUA estão se concentrando em remover todos os obstáculos que possam estar no caminho do avanço do Al (Carman, 2020, p. 211, tradução livre)[91].

[88] No inglês, *White House Summit on Artificial Intelligence for American Industry*.
[89] No inglês, *Executive Order 13859: Artificial Intelligence for American People*.
[90] No original, "*(1) prioritizing funding for Al research,(2) removing regulatory barriers to the deployment of Al technologies,(3) training the future workforce, (4) achieving strategic military advantage, (5) leveraging Al government services, and (6) leading international Al negotiations*".
[91] No original, "*Kratsio's approach differs slightly from those that have been presented in the EU and China. A free market economy 'promote sthe production and sale of goods and services, with little to no control or involvement from any central government agency',which is precisely what the EU and China have been trying to prevent. Rather than placing importance on keeping Al safe for consumer use or regulating the standards of Al development, the US is focusing on removing all obstacles 196 that may be in the way of Al advancement*".

Essa afirmação, partindo do conselheiro político de um ex-presidente, revela a abordagem que os EUA adotaram, majoritariamente, ao longo de muitos anos: o não regular, apenas incentivando e estabelecendo metas para o desenvolvimento tecnológico.

Apenas algumas exceções eram percebidas a esse não regular, ou melhor, não interferir na atuação privada, como foi o caso com os veículos autônomos e os sistemas de IA para propósitos militares (Carman, 2020, p. 212).

2.2.2. Um Pequeno Passo do Governo Federal, um Salto Gigantesco para a Regulação?

A partir de fevereiro de 2019, contudo, a abordagem estadunidense passou a se transformar, com a emissão, pelo então presidente Donald Trump, da *Ordem Executiva 13859: Mantendo a liderança americana em inteligência artificial* [92], afirmando a liderança global dos EUA no desenvolvimento da IA e a necessidade de continuidade desse papel.

Reconhecia, nesse contexto, a relevância da atuação do Governo Federal na facilitação da pesquisa e do desenvolvimento, assim como na criação de um ambiente de confiança dos cidadãos nas tecnologias relacionadas à IA e na adaptação dos trabalhadores ao novo cenário empregatício (EUA, 2019b).

Para isso, a OE 13859 afirmava que, enquanto se incentivasse a inovação e se busca a colaboração com aliados internacionais, dever-se-ia também proteger a economia, a segurança nacional, as liberdades individuais, a privacidade e os valores americanos.

Ademais, asseverava ser imperioso defender a tecnologia estadunidense em IA das "tentativas de aquisição por concorrentes estratégicos e nações adversárias"[93] (EUA, 2019b). Diante disso, seriam cinco os princípios a reger o regime estadunidense para a IA:

> (a) Os Estados Unidos devem impulsionar os avanços tecnológicos em IA no governo federal, no setor e na academia para promover a descoberta científica, a competitividade econômica e a segurança nacional.
>
> (b) Os Estados Unidos devem impulsionar o desenvolvimento de padrões técnicos apropriados e reduzir as barreiras ao teste e à implantação seguros de tecnologias de IA para possibilitar a criação de novos setores relacionados à IA e a adoção da IA pelos setores atuais.

[92] No inglês, *Maintaining American Leadership in Artificial Intelligence*.
[93] No original, "*attempted acquisition by strategic competitors and adversarial nations*".

> (c) Os Estados Unidos devem treinar as gerações atuais e futuras de trabalhadores americanos com as habilidades necessárias para desenvolver e aplicar tecnologias de IA, preparando-os para a economia atual e para os empregos do futuro.
>
> (d) Os Estados Unidos devem fomentar a confiança do público nas tecnologias de IA e proteger as liberdades civis, a privacidade e os valores americanos em sua aplicação, a fim de realizar plenamente o potencial das tecnologias de IA para o povo americano.
>
> (e) Os Estados Unidos devem promover um ambiente internacional que apoie a pesquisa e a inovação da IA americana e abra mercados para os setores de IA americanos, ao mesmo tempo em que protege nossa vantagem tecnológica em IA e protege nossas tecnologias críticas de IA contra a aquisição por concorrentes estratégicos e nações adversárias. (EUA, 2019a, tradução livre)[94].

Além disso, a OE 13859 estabelecia como objetivos da investida mútua pela promoção e proteção dos avanços estadunidenses na IA: 1) a promoção do investimento no desenvolvimento da IA, em colaboração com a indústria, a academia, aliados internacionais e entes não-federais; 2) o aprimoramento do acesso a dados e recursos computacionais federais, com o objetivo de aumentar o valor desses instrumentos, mantendo a proteção à segurança e à privacidade de forma consistente com as leis e políticas sobre o assunto; 3) a redução de barreiras às inovações tecnológicas simultânea à proteção de valores americanos; 4) a garantia de criação de padrões técnicos que minimizem potenciais riscos quanto à segurança, refletindo a prioridade dada pelo Governo Federal à confiança pública na IA; 5) o treinamento de pesquisadores e usuários estadunidenses, com ênfase na educação em áreas do conhecimento relacionadas à IA; 6) o desenvolvimento de um plano de ação para proteger a vantagem dos EUA em IA e tecnologias relevantes do ponto de vista da economia e de segurança nacional, contra concorrentes estratégicos e adversários estrangeiros (EUA, 2019b).

Segundo Carman, a combinação entre os cinco princípios e seis objetivos inaugurou um primeiro plano de ação dos EUA para a regulação da IA, refletindo "uma mudança na perspectiva dos EUA. Os EUA deixaram de querer remover toda a intervenção governamental

---

[94] No original, *"(a) The United States must drive technological breakthroughs in AI across the Federal Government, industry, and academia in order to promote scientific discovery, economic competitiveness, and national security.*
(b) The United States must drive development of appropriate technical standards and reduce barriers to the safe testing and deployment of AI technologies in order to enable the creation of new AI-related industries and the adoption of AI by today's industries.
(c) The United States must train current and future generations of American workers with the skills to develop and apply AI technologies to prepare them for today's economy and jobs of the future.
(d) The United States must foster public trust and confidence in AI technologies and protect civil liberties, privacy, and American values in their application in order to fully realize the potential of AI technologies for the American people.
(e) The United States must promote an international environment that supports American AI research and innovation and opens markets for American AI industries, while protecting our technological advantage in AI and protecting our critical AI technologies from acquisition by strategic competitors and adversarial nations".

do ‘mercado livre’ do avanço da IA e passaram a fornecer diretrizes federais para o Al”[95] (Carman, 2020, p. 213).

No mês de junho de 2019, a Casa Branca propôs uma adaptação do *Plano Estratégico Nacional de Pesquisa e Desenvolvimento de Inteligência de 2016*, praticamente mantendo intactas as sete estratégias delineadas pelo governo anterior.

O diferencial desse relatório, na verdade, foi a adição de uma oitava estratégia: o fortalecimento de parcerias público-privadas, numa continuidade “da tendência da administração de apoiar fortemente o desenvolvimento da IA liderado pelo setor privado” (Schackelford et al., 2022, p. 42).

Em setembro do mesmo ano, a Casa Branca promoveu mais uma *Conferência, sobre o uso governamental da IA*. Na ocasião, ressaltou-se, mais uma vez, a necessidade de atuação conjunta com a indústria e a academia, anunciando a intenção governamental de capacitar os servidores públicos federais e de criar um Centro de Excelência para que agências pudessem colaborar entre si, trocando conhecimento e fomentando boas práticas (EUA, 2019a).

Nesse contexto, algumas agências federais começaram a criar documentos relacionados para o desenvolvimento da IA no setor militar, ou de segurança nacional, restringindo-se, contudo, a afirmar seus objetivos quanto às inovações tecnológicas que almejam desenvolver:

> Alguns exemplos são (1) o programa *Explainable Al da Defense Advanced Research Projects Agency* ("DARPA"), que "tem como objetivo criar técnicas de aprendizado de máquina que produzam soluções mais explicáveis, mantendo alto desempenho e níveis adequados de confiança no sistema"; 219 (2) o Programa da *National Science Foundation* ("NSF") sobre Equidade em Inteligência Artificial em Colaboração com a Amazon, que se concentra no financiamento de pesquisas sobre equidade em IA210 ; e (3) a *AI Next Campaign* da DARPA, que criará soluções para a defesa contra possíveis ataques às tecnologias Al, para que os cidadãos tenham maior probabilidade de confiar nos sistemas Al. Embora todos esses objetivos sejam válidos e deem a impressão de que os EUA estão muito avançados no processo de regulamentação da Al, eles simplesmente destacam marcos teóricos que essas agências esperam alcançar (Carman, 2020, p. 213, tradução livre)[96].

---

[95] No original, “*reflect a change in theUS's perspective. The US has moved away from wanting to remove all government intervention from the "free market" of Advancement to providing federal guidelines for Al*”.

[96] No original, “*A few examples are (1) the Defense Advanced Research Projects Agency's("DARPA") Explainable Al program, which "aims to create machine learning techniques that produce more explainable solutions while maintaining high performance and appropriate levels of trust in thesystem";219 (2) the National Science Foundation's ("NSF") Program on Fairness in Artificial Intelligence in Collaboration with Amazon, which focuses on funding research on fairness in AI210 ; and (3)DARPA's Al Next Campaign, which will create solutions for*

Em 2020, a FTC publicou um *business blog* sobre a utilização de inteligência artificial e algoritmos, tratando dos usos da IA e, especialmente, do *machine learning*.

Afirmou a sua experiência em lidar com outras tecnologias de tomada de decisão, uma vez que, ao longo dos anos, já havia lidado com casos de violação no âmbito da utilização dessas tecnologias por serviços financeiros. De fato, a FTC já havia até mesmo utilizado das suas atribuições para proibir práticas desleais e enganosas decorrentes do uso de IA e da tomada de decisões automatizada (Smith, 2020).

Nesse contexto, a agência recomendou, como princípios necessários ao desenvolvimento de sistemas de IA compatíveis com o *FTC Act*: a transparência, principalmente quando da coleta de dados sensíveis; a explicabilidade das decisões geradas pelos algoritmos e dos critérios por ele analisados, em especial no caso de atribuição de pontuações de risco; a justiça das decisões, devendo haver um distanciamento de práticas discriminatórias e uma preocupação dos resultados, ou seja, dos *outputs*; a precisão e robustez dos dados, devendo haver possibilidade de retificação de dados incorretos; a *acconutability*, no sentido de que os operadores devem garantir a possibilidade de auditoria dos seus sistemas (FTC, 2020).

Em novo *blog*, de 2021, a FTC fez sugestões mais específicas sobre como garantir que o desenvolvimento de uma IA se dê de forma justa. Os desenvolvedores de IA deveriam, portanto, partir de uma base de dados sólida, preocupando-se com a possibilidade de que determinados dados (ou a falta deles), gere *outputs* discriminatórios.

Ademais, a FTC incentivou a pesquisa independente e transparente, bem como a publicação dos resultados das empresas e a divulgação dos seus dados ou do seu código como uma forma de *accountability* voluntária. Os desenvolvedores de dados deveriam, dessarte, ser honestos sobre a forma como os dados são utilizados e sobre o que as IAs desenvolvidas são capazes de fazer e com que precisão.

Somente em 2023, o Governo Federal, sob a presidência de Joe Biden, passou a produzir normativas preocupadas não somente com o incentivo ao desenvolvimento da IA.

---

defending against potential attacks 21 1 on Al technologies so that citizens are more likely to place their trust in Al systems. While all of these are worthwhile goals and give off the impression that the US is far along in the process of regulating Al, they simply highlight theoretical milestones that these agencies hope to reach".

Em maio desse ano, o *Plano Estratégico Nacional de Pesquisa e Desenvolvimento de Inteligência* passou por uma segunda adaptação, adicionando uma nova estratégia à lista anterior: o estabelecimento de uma abordagem coordenada e baseada em princípios para colaboração internacional em pesquisa de IA.

Em julho de 2023, o Governo Federal, depois de promover um diálogo com as sete maiores empresas desenvolvedoras de IA nos UEA – *Amazon, Google, Inflection, Meta, Microsoft* e *OpenAI* – divulgou alguns *compromissos voluntários* assumidos por elas, em concordância com as leis e regulações aplicáveis.

Dessa forma, sete *bigtechs* se comprometeram a garantir a segurança dos sistemas, que passariam ser testados a partir do *red teaming* [97] interno e externo; a compartilhar informações sobre problemas de segurança com outras empresas e agentes governamentais, visando ao aumento da proteção; a investir em cibersegurança; a procurar ativamente problemas de vulnerabilidade, inclusive por meio da participação de "terceiros"; a desenvolver uma espécie de marca d'água, para facilitar a identificação de audiovisuais fidedignos e a distinção em relação aos *deepfakes*[98]; a tornar públicos as limitações dos resultados de seus sistemas de IA, conscientizando os usuários sobre os riscos de vieses algoritmos; a priorizar a pesquisa sobre os riscos sociais da IA, tendo em vista à não-discriminação e a proteção à privacidade; a desenvolver sistemas de IA que auxiliem a sociedade a resolver seus maiores desafios (White House, 2023b)

Em outubro de 2023, o presidente Biden emitiu a *Ordem Executiva 14110, sobre o Desenvolvimento e Uso Seguro, Protegido e Confiável da Inteligência Artificial*[99] (EUA, 2023b), a qual já tem sido considerada o maior e mais abrangente marco regulatório estadunidense para a regulação dessa tecnologia.

---

[97] "*Red teaming can be defined as the process of testing your cybersecurity effectiveness through the removal of defender bias by applying an adversarial lens to your organization.*
Red teaming occurs when ethical hackers are authorized by your organization to emulate real attackers' tactics, techniques and procedures (TTPs) against your own systems.
It is a security risk assessment service that your organization can use to proactively identify and remediate IT security gaps and weaknesses.
A red team leverages attack simulation methodology. They simulate the actions of sophisticated attackers (or advanced persistent threats) to determine how well your organization's people, processes and technologies could resist an attack that aims to achieve a specific objective" (Anderson, 2023).

[98] Vídeos criados por IA, que aparentam serem reais, mas na verdade replicam a aparência e a voz humana e são criados com o objetivo de enganar o espectador e, normalmente, disseminar informações falsas.

[99] No inglês, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*.

O objetivo dessa OE demonstra uma mudança clara da postura até então adotada, na medida em que passa a atribuir uma atenção mais equilibrada para os potenciais *e* para os riscos da IA.

Enuncia, assim, a necessidade de desenvolvimento e incentivo a uma IA responsável, destacando (novamente) a colaboração entre governo, setor privado e academia, incluindo, dessa vez, a menção à sociedade civil.

No seu artigo segundo, a OE fixa os princípios da política regulatória que passará a ser adotada, quais sejam: uma IA segura, que cumpra com requisitos de robustez e confiabilidade; promoção da inovação e da comunicação, visando atribuir aos EUA um papel de liderança no campo da IA e permitir a solução de diversos desafios globais; o comprometimento com os trabalhadores americanos, garantindo que as transformações do mercado, a partir da introdução da IA, afetem positivamente o trabalho humano; o compromisso com a igualdade e com os direitos civis; a proteção ao consumidor; a proteção à privacidade, em respeito à Primeira Emenda; o compromisso do Governo Federal com promover, ele mesmo, um uso responsável da IA para regular e governar.

Quanto ao último objetivo, o presidente afirma a finalidade de estabelecer a liderança estadunidense no âmbito global, no social, econômica e tecnologicamente, o que revela, mais uma vez, a intenção de ocupar o protagonismo, se não para determinar ou obrigar, para se tornar um jogador mais expressivo no campo da regulação da IA.

> Essa liderança não é medida apenas pelos avanços tecnológicos que nosso país faz. Uma liderança eficaz também significa ser pioneiro nos sistemas e nas salvaguardas necessárias para implantar a tecnologia de forma responsável, além de criar e promover essas salvaguardas com o resto do mundo. Meu governo se envolverá com aliados e parceiros internacionais no desenvolvimento de uma estrutura para gerenciar os riscos da IA, liberar o potencial da IA para o bem e promover abordagens comuns para desafios compartilhados. O governo federal buscará promover princípios e ações responsáveis de segurança e proteção da IA com outras nações, inclusive nossos concorrentes, enquanto lidera conversas e colaborações globais importantes para garantir que a IA beneficie o mundo inteiro, em vez de exacerbar as desigualdades, ameaçar os direitos humanos e causar outros danos (EUA, 2023b, tradução livre)[100].

[100] No original, "*This leadership is not measured solely by the technological advancements our country makes. Effective leadership also means pioneering those systems and safeguards needed to deploy technology responsibly — and building and promoting those safeguards with the rest of the world. My Administration will engage with international allies and partners in developing a framework to manage AI's risks, unlock AI's potential for good, and promote common approaches to shared challenges. The Federal Government will seek to promote responsible AI safety and security principles and actions with other nations, including our competitors, while leading key global conversations and collaborations to ensure that AI benefits the whole world, rather than exacerbating inequities, threatening human rights, and causing other harms*".

A OE 14110 segue linha semelhante à dos compromissos voluntários das *bigtechs*¸ estabelecendo como uma de suas principais ferramentas o *red teaming*, que é definido como:

> (d) O termo "red-teaming de IA" significa um trabalho de teste estruturado para encontrar falhas e vulnerabilidades em um sistema de IA, geralmente em um ambiente controlado e em colaboração com desenvolvedores de IA. O red-teaming de Inteligência Artificial é, na maioria das vezes, realizado por "equipes vermelhas" dedicadas que adotam métodos adversários para identificar falhas e vulnerabilidades, como resultados prejudiciais ou discriminatórios de um sistema de IA, comportamentos imprevistos ou indesejáveis do sistema, limitações ou riscos potenciais associados ao uso indevido do sistema (EUA, 2023b, tradução livre)[101].

Além desse termo, a OE 14110 trata de esclarecer e definir diversos outros conceitos, tais quais "modelo" e "sistema de IA", "tecnologias emergentes e essenciais", "garantia de privacidade diferencial", entre outros.

A definição de tais conceitos pela primeira vez nos EUA, serve à segurança jurídica, pois o governo passa a se posicionar sobre o que entende como IA e define, uma a uma, as obrigações que passará a impor.

Um ponto interessante sobre esse novo marco regulatório é o fato de que passa a engajar novos agentes na estrutura regulatória: a *Secretaria de Comércio*[102], a *Secretaria de Comércio para Propriedade Intelectual*[103], o *Instituto Nacional de Padrões e Tecnologia* (NIST)[104], a *Fundação Nacional de Ciência*[105] a *Secretaria de Energia*[106], a *Secretaria de Tesouro, o Departamento de Segurança Interna e o Departamento de Defesa*[107], entre outros, passam a participar da regulação da IA e de *clusters*[108] informáticos.

---

[101] No original, "*(d) The term "AI red-teaming" means a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI. Artificial Intelligence red-teaming is most often performed by dedicated "red teams" that adopt adversarial methods to identify flaws and vulnerabilities, such as harmful or discriminatory outputs from an AI system, unforeseen or undesirable system behaviors, limitations, or potential risks associated with the misuse of the system*".
[102] No inglês, *Secretary of Commerce*.
[103] No inglês, *Secretary of Commerce for Intellectual Property*.
[104] No inglês, *National Institute of Standards and Technology*.
[105] No inglês, *National Science Foundation*.
[106] No inglês, *Secretary of Energy*.
[107] No inglês, *Secretary of the Treasury*.
[108] "*A computer cluster is a set of computers that work together so that they can be viewed as a single system*" (Wikipedia contributors, 2023).

Mais especificamente, a OE 14110 prevê que esses órgãos serão responsáveis por criar e executar diretrizes, normas, boas práticas, modelos de avaliação de riscos e bancos de ensaio de sistemas de IA, sempre nos limites da legislação vigente e empregando ferramentas já existentes e criando outras novas. Ademais, em alguns casos, serão responsáveis por iniciativas de capacitação e treinamento em IA para formar novos talentos, mas também para capacitá-los.

De forma geral, a finalidade dessas agências é avaliar os sistemas de IA de forma a aferir potenciais riscos nucleares, biológicos ou químicos, assim como ameaças à infraestrutura essencial e à segurança energética.

Nesse quadro, a OE 14110 recorre à *Lei de Produção para Defesa de 1950*[109] para atribuir à Secretaria de Comércio a competência de receber e encaminhar ao governo notificações das empresas, nos casos em que o treinamento de determinada IA represente um risco grave para a segurança nacional e pública ou para a saúde. Por essa Lei, as empresas também ficam obrigadas os resultados de suas avaliações de riscos e do *red teaming*.

Também é prevista a criação de um *Conselho de Segurança e Proteção da IA*[110], nos termos da Seção 871 da *Lei de Segurança Nacional de 2002*[111]. O Conselho será formado por especialistas da academia e dos setores privado e público, que serão responsáveis por aconselhar o governo no uso de IA no âmbito da infraestrutura crítica/essencial.

Ademais, em cada agência governamental deverá ser criada uma função de Diretor de Inteligência Artificial, que será responsável, conjuntamente com outros servidores, por coordenar o uso da IA no âmbito da agência.

Em alguns casos, serão conduzidas consultas públicas e da participação de vários *stakeholders* para avaliar as políticas regulatórias adequadas para lidar com os riscos detectados.

Até agora, a OE 14110 tem sido considerada a medida mais abrangente dos EUA para regular tecnologia até a atualizada. Algumas críticas surgem, por ser uma legislação, em certa medida, prescritiva, elaborada pelo Executivo. Nesse sentido, Ryan Calo falou ao Washington Post:

---

[109] No inglês. *Defense Production Act of 1950*.
[110] No inglês, *AI Safety and Security Board*.
[111] No inglês, *Homeland Security Act of 2002*.

> "Posso ver a frustração nessa [ordem executiva] de que muito disso deveria ser feito pelo Congresso, mas eles não estão fazendo nada", disse Ryan Calo, professor de direito especializado em tecnologia e IA na Universidade de Washington.
>
> Não está claro até que ponto a ordem afetará profundamente o setor privado, dado seu foco em órgãos federais e "circunstâncias restritas" relativas a questões de segurança nacional, acrescentou Calo (Washington Post, 2023, tradução livre)[112].

O setor privado ainda se posiciona sobre o assunto, mas alguns presidentes de *bigtechs* posicionaram-se sobre o tema prontamente:

> Brad Smith, Presidente da Microsoft: "A ordem executiva de hoje é outro passo fundamental para a governança da tecnologia de IA. Essa ordem se baseia nos Compromissos Voluntários da Casa Branca para uma IA segura, protegida e confiável e complementa os esforços internacionais por meio do Processo de Hiroshima do G7. A IA promete reduzir os custos e melhorar os serviços para o governo federal, e estamos ansiosos para trabalhar com as autoridades dos EUA para concretizar plenamente o poder e a promessa dessa tecnologia emergente." [Tweet, 30/10/23]
>
> Kent Walker, presidente de assuntos globais e diretor jurídico da Alphabet: "A IA deve beneficiar todos nos Estados Unidos. Estamos analisando a Ordem Executiva de hoje e estamos confiantes de que nossas práticas de responsabilidade de IA de longa data se alinharão com seus princípios. Continuaremos trabalhando juntos para maximizar o potencial da IA para o bem." [Tweet, 30/10/23] (White House, 2023b, tradução livre)[113].

De fato, trata-se de um marco muito recente, mas é possível perceber uma adaptação dos EUA ao cenário mundial.

2.3 A centralidade da Federal Trade Commission

Tanto durante a vigência do Acordo de Porto Seguro, quanto do Escudo de Privacidade, a FTC ocupou um papel central na tutela do direito à proteção de dados pessoais.

---

[112] No original, "'*I can see the frustration in this [executive order] that a lot of this should be done by Congress but they're not doing anything', said Ryan Calo, a law professor specializing in technology and AI at the University of Washington.*
It's unclear how deeply the order will affect the private sector, given its focus on federal agencies and 'narrow circumstances' pertaining to national security matters, Calo added".

[113] No original, "*Brad Smith, President, Microsoft: "Today's executive order is another critical step forward in the governance of AI technology. This order builds on the White House Voluntary Commitments for safe, secure, and trustworthy AI and complements international efforts through the G7 Hiroshima Process. AI promises to lower costs and improve services for the Federal government, and we look forward to working with U.S. officials to fully realize the power and promise of this emerging technology." [Tweet, 10/30/23]*
Kent Walker, President of Global Affairs & Chief Legal Officer, Alphabet: "AI should benefit everyone in America. We're reviewing today's Executive Order, and we are confident that our long-standing AI responsibility practices will align with its principles. We'll continue working together to maximize AI's potential for good." [Tweet, 10/30/23]".

Aparentemente, esse também será o caso perante o QPD UE-EUA e, possivelmente, perante a regulação da inteligência artificial nos EUA, embora a FTC não tenha sido amplamente mencionada pela OE 14110.

Dessarte, é extremamente pertinente compreender o seu histórico, o seu âmbito de atuação e o seu potencial como um dos elementos principais do modelo americano para a proteção de dados.

A FTC foi criada em 1914, inicialmente como uma pequena e independente agência do governo voltada para uma atuação antitruste. Em 1938, passou por alterações estruturais que aumentaram seus poderes, dando-lhe também a atribuição de adereçar problemas de natureza consumerista (Hoofnagle, 2016).

Inicialmente, a proteção do direito ao consumidor, nesse âmbito limitava-se à proibição de publicidade enganosa. Contudo, com o desenvolvimento da sociedade e dos direitos e com a contínua atuação da FTC, essa agência se consolidou como umas das principais fiscalizadoras e executoras da lei nos Estados Unidos da América (Hoofnagle, 2016, p. 194).

Chrish Jay Hoonagle explica que, entre as décadas de 1980 e 1990, a FTC passou a preencher os vácuos da edição de algumas das mais importantes leis federais sobre privacidade.

Mesmo hoje, a atuação da agência no âmbito da privacidade ainda é fundamental, ainda que limitada pela Seção 5 da Lei da *Federal Trade Commision*, relativa às práticas injustas e enganosas[114], prendendo-se também aos compromissos assumidos pelas empresas, fixados nas suas políticas de privacidade. A proposição de ações civis e outros remédios, portanto, acaba se tornando insuficiente na tutela do direito à privacidade, pois:

> No final, porém, o alcance da FTC é limitado. Ela apenas garante que as empresas cumpram suas promessas. Como observa Paul Schwartz, se um site não fizer uma promessa sobre privacidade, ele "ficará fora da jurisdição da FTC".78 Infelizmente, a FTC tem tempo e recursos limitados, e suas "atividades de proteção à privacidade já são ofuscadas por suas investigações mais agressivas de fraude e práticas de marketing enganosas na Internet (Solove, Hartzog; 2014; pp. 592-594; tradução livre)[115].

[114] No inglês, *unfair* e *deceptive practices*.

[115] No inglês, "*In the end, however, the FTC is limited in its reach. It only ensures that companies keep their promises. As Paul Schwartz notes, if a website doesn't make a promise about privacy, then it will "fall outside of the FTC's jurisdiction."78 Unfortunately, the FTC has only limited time and resources, and its "privacy protection activities already are dwarfed by its more aggressive investigations of fraud and deceptive marketing practices on the Internet*".

As políticas de privacidade passaram a ser mais utilizadas na década de 1990, consolidando-se como uma forma de despertar a confiança do consumidor, ainda que tenham sido inicialmente rejeitadas pelo setor empresarial. Esses compromissos ocupam, desde um então, um papel central no modelo estadunidense de proteção de dados.

Nesse ínterim, múltiplos *stakeholders* expressam uma preferência pelo modelo autorregulatório, pautado nessas políticas. A autorregulação seria, então, ideal e necessária para o desenvolvimento da Internet e demais tecnologias. A própria adoção das políticas de privacidade era vista como uma forma de evitar uma maior intervenção do direito, numa tentativa de convencer o legislador de que esse era um método suficiente e efetivo (Solove, Hartzog; 2014; pp. 592-594).

Solove e Hartzog explicam que a FTC é vista, na prática, como uma autoridade federal de proteção de dados, em contraposição à tendência de outros países de criarem uma agência específica para exercer esse papel (Solove, Hartzog; 2014; p. 600).

Os autores acrescentam que, embora o número de reclamações da FTC seja relativamente pouco significante – desde 1997, haveria pouco mais de 170 relacionadas à privacidade (Solove, Hartzog; 2014; p. 600) – esse número tem crescido proporcionalmente à expansão da jurisdição e à similaridade da forma de desempenho da agência com o modelo auto regulatório adotado pelos legisladores (Solove, Hartzog; 2014; p. 602).

Ademais, os casos por ela iniciados, são conduzidos de forma muito estratégica, de forma a construir uma espécie de "jurisprudência" positiva, investindo apenas naqueles casos que estejam bem planejados e haja uma chance maior de sucesso (Hoofnagle, 2016, p. 268).

Outros limites à maior abrangência da Agência seriam relacionados à sua estrutura escassa, com orçamento (Hoofnagle, 2016, p. 819) e funcionários insuficientes (Solove, Hartzog; 2014; p. 600), e à impossibilidade de impor multas civis e outras penalidades mais significativas (Solove, Hartzog; 2014; p. 605).

Mesmo assim, a agência é percebida como uma importante fonte de *common law*:

> Embora os casos de privacidade da FTC consistam quase todos em reclamações e acordos, eles são, em muitos aspectos, o equivalente funcional da lei comum. Embora a analogia com o direito consuetudinário tradicional tenha seus limites, ela é, no entanto, uma estrutura útil para entender a jurisprudência de privacidade da FTC. A

> common law é uma forma de lei anglo-americana que se caracteriza pelo desenvolvimento gradual por meio de decisões judiciais em uma série de casos concretos. As decisões servem como precedentes - os juízes buscam decidir os casos de forma consistente com as decisões anteriores. Na forma mais tradicional de common law, os juízes desenvolvem as regras jurídicas. Grande parte do direito civil anglo-americano, do direito contratual, do direito de propriedade e do direito penal surgiu por meio desse processo. Muitas partes desses corpos de leis foram posteriormente codificadas em estatutos, especialmente o direito penal, que hoje, nos Estados Unidos, é quase totalmente estatutário. (...) Os acordos de privacidade da FTC tecnicamente não têm força de precedente para outras empresas. Não é estritamente exigido que a FTC seja consistente, mas a FTC tem demonstrado um compromisso de permanecer consistente na prática. Como será discutido, as novas queixas e ordens de acordo não se afastam muito das anteriores. Em vez disso, a FTC desenvolve gradualmente esse conjunto de leis de forma estável. Os profissionais olham para os acordos da FTC como se tivessem peso de precedente.173 O resultado é que os advogados consultam e analisam esses acordos da mesma forma que fazem com as decisões judiciais (Solove, Hartzog; 2014; pp. 619-620; tradução livre)[116].

Diante disso, fica claro que a FTC tem o potencial de, mesmo diante de circunstâncias pouco favoráveis, se tornar um órgão mais eficaz na proteção de dados pessoais e talvez até de se tornar um dos principais atores para regulação da IA, embora não tenha sido contemplada como um dos atores principais da OE 14110.

Para isso, deve ganhar liberdade para além das políticas de privacidade e da própria estrutura na qual está inserida, de maneira a permitir-se fiscalizar práticas que explorem a ignorância do consumidor, alterando a concepção de "prática enganosa".

Necessário, ainda o desenvolvimento de algum tipo de regime regulatório – e não autorregulatório – com base em regras e padrões claros e definidos com base nas boas práticas do mercado, entre outras possíveis mudanças (Solove, Hartzog; 2014; pp. 672-676).

---

[116] No original, "*Although the FTC's privacy cases nearly all consist of complaints and settlements, they are in many respects the functional equivalent of common law. While the analogy to traditional common law has its limits, it is nonetheless a useful frame to understand the FTC's privacy jurisprudence. Common law is a form of Anglo-American law that is characterized by incremental development through judicial decisions in a series of concrete cases. The decisions serve as precedent—judges aim to decide cases consistently with previous decisions. In the most traditional form of common law, judges develop the legal rules. Much of Anglo-American tort law, contract law, property law, and criminal law emerged through this process. Many parts of these bodies of law were later codified into statutes, especially criminal law, which today in the United States is almost entirely statutory. (…) FTC privacy settlements technically lack precedential force for other companies. The FTC is not strictly required to be consistent, but the FTC has demonstrated a commitment to remaining consistent in practice. As will be discussed, new complaints and settlement orders do not stray far from previous ones. Instead, the FTC incrementally develops this body of law in a stable way. Practitioners look to FTC settlements as though they have precedential weight.173 The result is that lawyers consult and analyze these settlements in much the same way as they do judicial decisions*".

3. Da Disputa Pelo Poder Simbólico

Nos capítulos anteriores, desenvolveu-se o panorama geral sobre a regulação de diferentes áreas, em duas delimitações espaciais distintas. A partir das informações trazidas sobre o desenvolver das políticas regulatórias em proteção de dados e inteligência artificial na UE e nos EUA, o leitor pôde vislumbrar algumas dinâmicas existentes na construção desses modelos.

Compreende-se, a partir do quadro narrado, que a relação UE-EUA tem sido, há anos, conturbada. Não se trata de um conflito evidente, ou mesmo de uma inimizade. Na verdade, o *Velho Continente*, representado pela UE, e o *Novo Mundo*, associado aos EUA, possuem uma importante relação comercial e política, sendo frequentemente percebidos como os líderes da daquilo que muitas vezes se descreve *Ocidente*[117].

Dessa forma, a dualidade entre eles desenvolve-se na como uma luta silenciosa "pela imposição de formas distintas de definição do mundo" (Curto, Domingos, Jerónimo, 2022, p. XXXVII). Nesse sentido:

> As relações de interação e comunicação, longe de se constituírem como uma realidade autónoma, dependem de um estado determinado de um jogo de forças, envolvendo o "poder material ou simbólico acumulado pelos agentes (ou pelas instituições) envolvidos nessas relações". Esta é, aliás, a base da crítica de Bourdieu ao "erro interaccionista", frequente em tradições fenomenológicas e semióticas, que se traduz de modo particular nos autores que autonomizam a esfera do simbólico, enquanto esfera de comunicação independente das relações de poder. "O poder simbólico, poder subordinado, é uma forma transformada, quer dizer, irreconhecível, transfigurada e legitimada, das outras formas de poder" (Curto, Domingos, Jerónimo, 2022, p. XXXVII).

Tal trecho corresponde a uma explicação das palavras que o próprio Bourdieu utiliza para conceituar o poder simbólico, como um "poder invisível o qual só pode ser exercido com a cumplicidade daqueles que não querem saber que lhe estão sujeitos ou mesmo que o exercem" (Bourdieu, 2022, p. 4).

---

[117] Como explicitado no capítulo dedicado à metodologia, a escolha do termo Ocidente serve como uma indicação de que os próprios agentes se identificam como protagonistas nessa região, atuando de forma distanciada do Oriente e do Sul Global, que não é tratado propriamente como um *player* ocidental relevante. Tanto que os esforços de compatibilização entre os regimes da UE e EUA ocorreram diversas vezes ao longo dos anos, com concessões da parte dos dois jogadores. Essa flexibilidade, sem embargo, não é evidente ao observar as relações entre UE/EUA e América Latina/África/Ásia, de forma que estes jogadores acabam se adaptando ao ritmo daqueles *ou* jogando o próprio jogo de maneira relativamente isolada.

De fato, interessa, a partir desse marco teórico, compreender de que maneira as forças internacionais, típicas de um mundo globalizado, incidem sobre ordenamentos e práticas jurídicas nacionais, moldando-os e reinterpretando-os.

Em *Global Restructuring and the Law: Studies of the Internalization of Legal Fields and the Creation of Transnational Arenas*, David Trubek, Yves Dezalay, Ruth Buchanan e John Davis realizam, exatamente nessa linha, uma análise sobre como as interações entre as dimensões europeia e estadunidense, no final dos anos 1990, influenciaram as tradições jurídicas e a prática da advocacia uma da outra, em especial diante do cenário da integração europeia[118].

Os autores, ao longo da obra, exploram o conceito bourdieusiano de *campo*, entendendo-o como "o conjunto de instituições e práticas por meio do qual o direito é produzido, interpretado, e incorporado na tomada de decisões de caráter social" (Trubek et al., 1994, p. 411). A partir disso, estruturam uma metodologia de análise que tenta ser suficientemente complexa para compreender a realidade da forma mais precisa possível, sem perder, contudo, o caráter analítico e descritivo das diferentes tradições e processos internos e externos de produção do direito.

Para isso, entende-se que o direito não é uma construção pura, vez que não possui fim em si mesmo, mas sim na regulação da sociedade. O campo jurídico é, com efeito, uma unidade de análise, um microcosmo (Trubek et al., 1994), ou mesmo, uma imagem dentre as diversas produzidas pelo caleidoscópio que é a realidade social.

Tanto o nacional quanto o internacional são objetos de escrutínio, cada um considerado na medida da sua relevância para o processo de construção do "jurídico" numa ordem globalizada e internacionalizada. Essa perspectiva é aproveitada, neste trabalho, como uma inspiração para descrever um campo regulatório, que guarda relações com o campo jurídico, embora não se limite a ele, na medida em que possui uma conexão mais óbvia com os campos econômico e político.

---

[118] Os autores, nessa obra, afirmam: "*our purpose is to look at law and legal practice to see how the legal field itself is becoming more internationalized and how transnational arenas for legal practice are being created. Such a study, we think, will contribute to the understanding of global processes by uncovering in one field the microprocesses and concrete practices that, taken as a whole, are creating global change. Forces and logics that can be observed in the economy, the state, and the international order are at work within the legal field as well, so that the logic of the legal field constitutes a "homologous microcosm" of larger social phenomena. To understand the particular logic of the legal field is to know something meaningful about the constitution of the society of which it is a part*" (Trubek et al., 1994, p. 410)

Dessa forma, após colocar o holofote não sobre o aspecto propriamente regulatório[119] dos modelos europeu e estadunidense, este capítulo coloca luz sobre o silencioso "cabo de guerra" que ao longo dos anos tem sido realizado entre UE e EUA, primeiro pela regulação da proteção de dados pessoais e, mais recentemente, pela regulação da IA.

Nesse contexto, é preciso compreender que o campo não é formado apenas pelos seus agentes internos, mas também por influências econômicas, políticas e culturais externas:

> Os campos sociais são formados por atores com posições diferentes que lutam pelos interesses que o campo oferece: os interesses podem ser monetários, mas também podem ser status e poder. Um campo é um sistema aberto cujos limites estão sempre em questão (e constituem uma das questões sobre as quais ocorre a luta). "Os jogadores no jogo do campo empregam várias formas de capital (econômico, social ou cultural) em suas lutas com outros jogadores. O conflito dentro do campo lhe dá dinamismo, mas também o mantém como um campo: Os jogadores em disputa desafiam uns aos outros, mas não o próprio campo, de modo que as lutas reafirmam e até fortalecem os campos (Trubek et al., 1994, p. 414, tradução livre)[120].

Da mesma forma como Bourdieu descreve que as classes (e frações delas) encontram-se em uma luta simbólica na vida cotidiana, buscando impor suas próprias definições de mundo, no contexto regulatório, essa luta é conduzida pelos diferentes agentes, ou *stakeholders* – nomenclatura empregada por diversas das normas e documentos produzidos tanto pela UE quanto pelos EUA nos últimos anos.

Portanto, no âmbito regulatório essa contenda ocorre entre regulador, ou seja, "a instituição regulatória, como ambiente de manifestação dos poderes regulatórios de administração das leis" (Aranha, 2021, p. 20), e regulado, entendido como "todo player do ambiente regulatório, independentemente das fronteiras nacionais" (Aranha, 2021, p. 20).

Para analisar diferentes configurações desse, a doutrina descreve duas estratégias de definição das ferramentas e políticas a serem empregadas em nome regulação:

---

[119] Seria possível, e, sem dúvidas, relevante, compreender os instrumentos regulatórios, autorregulatórios, corregulatórios, etc. Sem embargo, deixa-se essa atribuição para outras iniciativas de pesquisa.

[120] No original, "*Social fields are made-up of actors with different positions who struggle for the stakes the field offers: the stakes may be monetary, but hey may also be status and power. A field is an open system whose boundaries are always in questions (and constitute one of the issue over which struggle occurs). "Players in the game of the field deploy various forms of capital (economic, social or cultural) in their struggles with other players. Conflict within the field gives it dynamism, but also maintains it as a field: The contending players challenge each other, but no the field itself, so the struggles reafirms and even strenghens the fieds*".

A primeira delas, chamada *top-down*, costuma ser "executado por um só autor, assentado no pressuposto de que o processo de implementação é impulsionado por uma decisão proveniente do órgão executivo do Estado, o Governo" (Berenguer, 2020, p. 36). Dessarte, tal abordagem é marcada pela burocratização e pelo protagonismo das leis e dos regulamentos.

Na contemporaneidade, entretanto, a estratégia *bottom-up* tem ganhado destaque, em especial diante do aumento da complexidade estrutural gerada pela maior participação das tecnologias nas relações sociais:

> (...) a verdade é que as sociedades capitalistas avançadas, cada vez mais globais, têm sido marcadas por uma crescente diferenciação funcional das suas instituições, o que implica diretamente no alargamento da constelação de atores envolvidos no ciclo da política pública e no aprofundamento das interdependências sistêmicas entre eles (Monteiro, Moreira; 2018; pp. 77-78).

Sendo assim, o método *bottom-up* é caracterizado pela descentralização da execução das políticas regulatórias. Ele é, em síntese, o processo de execução da política pública por meio de uma rede de diversos atores distintos que contribuem mutuamente para os objetivos almejados e as soluções pensadas (Berenguer, 2020). A regulação pela UE e pelos EUA não escapa dessa conformação.

No caso do modelo europeu para a proteção de dados, ainda percebia-se alguma proximidade do modelo *top-down*, uma vez que regido pelo RGPD, norma geral emitida pelas autoridades europeias.

Apesar de ter sido um regulamento construído por diversas "mãos", no contexto de uma união de múltiplos Estados-membros, o RGPD, como corolário do modelo europeu, possui como finalidade uma atuação conjunta, uniforme e centrada em regras prescritivas, legitimadas por uma natureza análoga à de um Estado.

Ademais, as opções regulatórias da UE para a proteção de dados fundamentam-se numa dimensão constitucional e legal, tipicamente jurídica e, portanto, universalizante:

> A norma jurídica, quando consagra em forma de um conjunto formalmente coerente regras oficias e, por definição, sociais, "universais", os princípios práticos do estilo de vida simbolicamente dominante, tende a *informar* realmente as práticas do conjunto de agentes, para além das diferenças de condição e estilo de vida: o *efeito de universalização*, a que se poderia também chamar efeito de normalização, vem aumentar o efeito autoridade social que a cultura legítima e os seus detentores já

> exercem para dar toda a sua eficácia prática à coerção jurídica (Bourdieu, 2022, p. 258).

A universalização é, de fato, o que ocorreu não só dentro das fronteiras da UE, ou seja, não somente os Estados-Membros se submeteram a esse conjunto de normas. Estas, na verdade, passaram a ser transpostas por países terceiros para seus ordenamentos nacionais, na tentativa de se tornarem parte de um grupo seleto de regimes considerados adequados pela UE, que assumiu, assim, um verdadeiro protagonismo no cenário internacional.

Não se afirma, aqui, que o modelo europeu é inadequado ou prejudicial a direitos fundamentais típicos do paradigma do Estado Democrático de Direito. Na verdade, a influência europeia serviu tanto para acelerar a regulação da proteção de dados em alguns países, quanto para impedir que essa disciplina permanecesse completamente desregulada, como ocorreu com os EUA.

Também não se contesta o fato de que, num mundo globalizado, é necessário estabelecer algum tipo de relação entre a ordem jurídica de países que pretendem manter relações comerciais e/ou políticas. No caso, era necessário determinar de que forma aconteceria o fluxo transfronteiriço de dados de maneira que o regime europeu não se tornasse inútil no momento em que os dados dos seus cidadãos fosse transferido para outros países.

Contudo, não se pode ignorar que essa tendência universalizante, na teoria de Bourdieu, "é um dos efeitos do etnocentrismo dos dominantes, fundamentador da crença na universalidade do direito" (Bourdieu, 2022, p. 260).

Nesse âmbito, também é possível extrair da teoria bourdieusiana que "o imperialismo cultural assenta no poder de universalizar os particularismos ligados a uma tradição histórica singular, fazendo com que não sejam reconhecidos como tais" (Bourdieu, 2020, p. 409).

A globalização, assim, serve como legitimação para a prática de transpor conceitos e regras para realidades distintas daquela onde tiveram origem, desparticularizando-os e desenraizando-os da sua origem teórica e prática:

> (...) podemos ver de passagem que, entre os produtos culturais hoje difundidos à escala planetária, as mais insidiosas não são as teorias aparentemente sistemáticas (como o "fim da história" ou a "globalização") e as visões filosóficas do mundo (ou que isso pretendem ser, como o "pós-modernismo"), que são fáceis de identificar. São sobretudo os termos isolados com uma aparência técnica, tais como "flexibilidade" (ou na sua versão britância, a "empregabilidade"), que, pelo facto de condensarem e

> veicularem toda uma filosofia do indivíduo e da organização social, são adequadas para funcionar como autênticas palavras de ordem políticas (...) (Bourdieu, 2022, p. 412).

Essa tentativa de universalização foi um tanto sucedida, na medida em que diversos países, hoje, possuem legislações e modelos regulatórios inteiros inspirados pelo RGPD.

Não é o caso, contudo, dos EUA, como demonstrado pelo histórico de idas e vindas de acordos e "casos Schrems".

O Acordo de Porto Seguro, o Escudo de Privacidade e, talvez até o QPD UE-EUA, os três possuem uma grande característica em comum: não refletem por completo a lógica estadunidense; e não refletem por completo a lógica europeia.

O sistema de autocertificação definido diversas vezes pelo eixo UE-EUA, combina, ao mesmo tempo, diferentes lógicas de intervenção do público e de autonomia do privado. É um tipo de autorregulação, no seu sentido de termo "guarda-chuva" (Aranha, 2021, p. 87), que, entretanto, não corresponde à verdadeira pretensão de nenhum dos seus autores.

Por isso mesmo, Acordo de Porto Seguro e Escudo de Privacidade não foram bem aceitos por diversos dos players estadunidenses, que o consideravam restritivo às empresas e às inovações tecnológicas por elas conduzidas, e nem mesmo pelos cidadãos e pelas instituições europeias, que enxergavam, nos EUA, uma prática contrária aos direitos fundamentais e valores europeus, principalmente no que diz respeito à vigilância estatal exercida sucessivamente pelos governos americanos como uma forma de manutenção da segurança nacional e da soberania.

Importante, nesse ponto, destacar que essa vigilância é enraizada na própria experiência estadunidense, intensamente marcada pelo episódio de 11 de setembro de 2001 e pela luta constante contra o "terrorismo" (Baumer, Earp & Poindexter, 2004), que a essa altura deixou de representar determinado(s) grupo(s) terrorista(s), para assumir uma natureza quase metafísico, ou seja, não acessado pelos sentidos, mas pela revelação de um mundo imaterial acessado por meio da razão.

Entretanto, apesar de o sistema da UE para a proteção de dados ter aparentemente sucedido quanto à sua influência jurídica internacional, não se pode dizer o mesmo de uma perspectiva de incentivo à inovação, ao menos não nos termos em que os doutrinadores costumam descrever um ecossistema favorável ao desenvolvimento científico e tecnológico.

Isso porque a Europa continental, nos últimos anos, parece ter ficado atrás de países como EUA, China e até Reino Unido, ex-membro da UE, no que diz respeito a números quantificadores do investimento em IA, assim como do número de startups e de atração de grandes talentos.

> Quando se trata do ecossistema global de startups de IA, um estudo de 2018 observou que os três principais participantes (medidos em termos de número de startups de IA) são os Estados Unidos, com 1.393 startups (40%), a China, com 383 startups (11%), e Israel, com 362 startups (11%).10 Quatro países europeus estão entre os dez primeiros (o Reino Unido está em quarto lugar, a França em sétimo, a Alemanha em oitavo e a Suécia em décimo). Coletivamente, porém, a Europa fica atrás apenas dos Estados Unidos, com 769 startups de IA (22% do total global). Isso mostra que, embora os países europeus isolados possam não ser competitivos globalmente, a Europa tem o potencial de ser um importante participante em IA se puder fortalecer seu mercado único digital, embora o Brexit tenha consequências de longo prazo para esses esforços.
>
> (...)
>
> Quando se trata de investimento, os Estados Unidos e a China também estão à frente da Europa. Os Estados Unidos são, de longe, os líderes em investimentos e capital de risco relacionados à IA. Enquanto suas instituições acadêmicas conduzem a maior parte da pesquisa básica, o setor privado é muito ativo na aplicação de pesquisas realizadas no país e em outros lugares. Esses atores acadêmicos e do setor privado também são excepcionalmente bons em atrair os melhores talentos globais.33 Enquanto isso, as startups chinesas de IA se beneficiam de laços estreitos com o governo, o que lhes dá acesso a grandes quantidades de financiamento do setor público e a instituições pioneiras. Por exemplo, no domínio do reconhecimento facial, a empresa CloudWalk recebeu uma doação de US$ 301 milhões do governo municipal de Guangzhou em 2017,34 enquanto a Megvii levantou US$ 460 milhões em uma rodada de financiamento liderada pelo fundo de capital de risco do governo central (Brattberg, Csernatoni, Rugova; 2020; pp. 5-7; tradução livre)[121].

A preocupação com a sua posição no "pódio" do desenvolvimento tecnológico foi externada em diversos dos documentos oficiais da UE, de maneira que a proposta de

---

[121] No original, "*When it comes to the global AI startup ecosystem, a study from 2018 noted that the top three players (measured in terms of number of AI startups) are the United States with 1,393 startups (40 percent), China with 383 startups (11 percent), and Israel with 362 startups (11 percent).10 Four European countries are among the top ten (the UK is in fourth place, France is in seventh, Germany is in eighth, and Sweden is in tenth). Collectively, though, Europe is second only to the United States, with 769 AI startups (22 percent of the global total). This shows that, while single European countries may not be globally competitive, Europe has the potential to be a major player in AI if it can strengthen its digital single market, though Brexit will have long-term consequences on such efforts.*
(...)
When it comes to investment, the United States and China are also ahead of Europe. The United States is by far the leader in AI-related investment and venture capital. Whereas its academic institutions conduct the majority of basic research, the private sector is very active in applying research done across the country and elsewhere. These academic and private-sector players are also exceptionally good at attracting top global talent.33 Meanwhile, Chinese AI startups benefit from close ties with the government, which give them access to huge amounts of public-sector funding and early-adopter institutions. For example, in the domain of facial recognition, the company CloudWalk received a $301 million grant from the Guangzhou Municipal Government in 2017,34 while Megvii raised $460 million in a funding round led by the central government's venture capital fund".

Regulamento para IA faz parte das orientações políticas do período 2019-2024, intituladas "Uma União mais ambiciosa" (União Europeia, 2021a).

Nesse âmbito, é possível distinguir claramente os modelos europeus para a proteção de dados e para a IA, ainda que este esteja em processo de consolidação.

De fato, as opções regulatórias que têm sido feitas denotam a ampla participação de outros stakeholders, vez que os direitos fundamentais não são mais a prioridade, passando a ser ponderados frente ao incentivo à inovação tecnológica.

A inovação é um elemento socialmente relevante, possuindo um potencial benéfico evidente para os cidadãos. Contudo, simplesmente afirmar que inovação e proteção aos direitos fundamentais são valores equivalentes, em termos de relevância, não implica necessariamente numa decisão orientada ao bem ou ao interesse público. Na prática, podem ocorrer diversas situações em que o incentivo à inovação seja simplesmente incompatível com o bem-estar social, de maneira que interesses distintos deverão ser objetos de ponderação.

Esse discurso, na verdade, serve possivelmente como uma forma de neutralização, em que a inovação é retratada como uma resposta a diversos problemas sociais, fazendo valer a pena a flexibilização ou até o sacrifício de determinados direitos. Ou seja, serve para a promoção "'da des-realização' e da distanciação implicadas na transformação da defrontação direta dos interessados em diálogo entre mediadores" (Bourdieu, 2022, p. 235).

Dessarte, "a revelação do justo na letra da lei" (Bourdieu, 2022, p. 231) deixa de reinar sobre o ambiente regulatório, que passa a obedecer a lógica da "flexibilidade", da "ética" e da "confiança". Tais noções não deixam de seguir um "jogo de definições prévias" (Bourdieu, 2022, p. 411), mas revela um jogo liderado por outros agentes e por outros interesses.

Importante ressaltar que a noção de ética, no modelo europeu em construção, não guarda relação com o estudo filosófico da palavra, mas sim com a elaboração de princípios e objetivos por grupos de especialista, tal qual o AI HLG e o Grupo Europeu em Ética, Ciência e Novas Tecnologias.

Ao longo da pesquisa, não se pode identificar exatamente os critérios de seleção dos integrantes do AI HLG. O Grupo Europeu em Ética, Ciência e Novas Tecnologias, por sua vez, segue uma normativa específica, sendo elaborado a partir de um chamado público de profissionais da área, considerados detentores de expertise suficiente sobre o assunto.

Apesar de ser interessante, como orienta a ideia de regulação *bottom-up*¸ a participação de diferentes agentes no processo de regulação, uma vez que determinados indivíduos podem colaborar com experiências distintas e com conhecimento técnico e profissional sobre certos assuntos, é necessário questionar: como a "ética", elemento central desse sistema, pode ser determinada por especialistas cuja seleção é, em parte, obscura e que não necessariamente representam a neutralidade científica e tecnológica que se almeja afirmar?

Nesse contexto, cabe retomar o posicionamento de Bourdieu sobre o papel dos magistrados na construção do campo jurídico:

> Em resumo, a transformação dos conflitos inconciliáveis de interesses em permutas reguladas de argumentos racionais entre sujeitos iguais está inscrita na própria existência de um pessoal especializado, independente dos grupos sociais em conflito e encarregado de organizar, segundo formas codificadas, a manifestação pública dos conflitos sociais e de lhes dar soluções socialmente reconhecidas como imparciais, pois que são definias segundo as regras formais e logicamente coerentes de uma doutrina percebida como independentes dos antagonismos imediatos (Bourdieu, 2022, p. 239).

Tal reflexão aplica-se, também, ao caso das diretrizes éticas que atualmente conduzem a política regulatória da UE, com a diferença de que não se trata, mais, de uma construção do Judiciário, como no caso comentado por Bourdieu. Também não se trata de uma construção elaborada segundo o processo legislativo comunitário, mas sim opções feitas por terceiros á ordem político-jurídica da UE, legitimados por uma expertise que, ainda, não possui limitações ou critérios evidentes.

Dessa forma, uma espécie de "corpo sistemático de regras assente em princípios racionais e destinado a ter uma aplicação universal" (Bourdieu, 2022, p. 231) ainda será aplicada para lidar com questões de proteção de dados, consumeristas e de direitos fundamentais relacionados à IA, mas a regulação, em si, se dará de forma particularizada, por meio da incidência dos princípios éticos definidos e da análise do nível de risco de cada sistema, caso a caso, e com a participação constante de diversas autoridades de supervisão estatais, assim como de agentes privados especializados na realização de auditorias.

Em consequência disso, a regulação torna-se ainda mais múltipla, seguindo a lógica de *bottom-up*, e assume uma face menos normativa.

Embora ainda se trate de uma realidade em construção, parece incidir sobre a realidade europeia continental o que Bourdieu entende como uma "remodelação das relações sociais e

das práticas culturais nas sociedades avançadas conforme o padrão norte-americano – fundado na pauperização do Estado, na mercantilização dos bens públicos e na generalização da insegurança social" (Bourdieu, 2022, p. 413).

Por esse motivo, questiona-se a UE perdeu a sua dominância pela regulação de campos relacionados à tecnologia, deixando espaço para o protagonismo almejado pelos EUA.

Em tal âmbito, percebe-se que, durante o governo Trump, os documentos oficiais utilizavam uma linguagem combativa, falando em "proteger" os avanços tecnológicos, em face de ameaças de "competidores estratégicos" e "nações adversárias".

Sob a liderança de Biden, o posicionamento em relação à esfera internacional passou a ser expresso a partir de termos mais neutros, representados pela ideia de uma liderança comprometida com os desafios mundiais e com a "cooperação" (ou "conversa") com "aliados e parceiros internacionais". Sem embargo, tal mudança de linguagem não significa necessariamente uma mudança de conduta.

Ao longo da história a opção estadunidense tem sido a de não regular, ou regular minimamente, deixando ao "livre mercado" a disciplina da economia, do desenvolvimento tecnológico e, em certo nível, até mesmo do social, como se percebe pela preferência pela autorregulação e pela falta de iniciativa estatal em determinar até mesmo a abrangência de direitos como a proteção de dados.

Claro, há uma diferença em relação ao modelo europeu, considerando que os EUA são regidos pelo sistema de *common law*. Entretanto, mesmo esse sistema possui a sua lógica de construção normativa pela via jurisprudencial (Bourdieu, 2022, p. 228), a qual tem operado minimamente ao longo do processo histórico de construção da regulação da proteção de dados e da IA, tanto considerado o Judiciário quanto considerada a fiscalização da FTC e de outras agências do governo federal.

Ambos QPD UE-EUA e OE 14110 são iniciativas do Executivo, na pessoa do presidente, que criam um regime orientado por princípios gerais e pela obrigação de prestação de contas das empresas tratadoras de dados e operadoras de sistemas de IA.

Expressamente, tais iniciativas visam ao equilíbrio de interesses distintos: governo, empresas, academia e cidadãos.

Pelo curto lapso temporal desde a sua entrada na ordem social, contudo, é difícil dizer se todos esses interesses serão efetivamente respeitados ou se, na verdade, trata-se de um

discurso legitimador do poder invisível de um dos grupos dominantes – possivelmente, o Estado e/ou o setor empresarial.

Diante desse panorama, é possível notar a contínua interação entre forças nacionais e internacionais, jurídicas, econômicas e culturais, sobre o cenário de produção jurídica e regulatória local.

O estudo das arenas locais de construção do poder simbólico é relevantíssimo para a compreensão não só dos ecossistemas regulatórios, mas das dinâmicas internacionais, como apontam precisamente Trubek, Dezalay, Buchanan e Davis:

> Um segundo motivo para manter o foco nacional é que as arenas transnacionais e supranacionais envolvem a concorrência entre os campos nacionais que buscam o domínio e os novos regimes "extranacionais" (públicos e privados) com diferentes graus de autoridade e eficácia. O processo de construção transnacional é parcial e hierarquicamente ordenado (Trubek et al., 1994, p. 411, tradução livre)[122].

Essa análise se torna relevante não por mera curiosidade de entender as relações entre UE e EUA, mas por ter o potencial de afetar países terceiros.

Isso porque ambos modelos para a regulação da IA analisados apontam para o interesse dos dois agentes internacionais de liderar e influenciar o cenário internacional, sendo que, no caso europeu, há previsão para que operadores de sistemas de IA de outros países sejam submetidos à análise de risco pelas autoridades europeias ou, em caso de acordos, pelas autoridades dos países de origem.

Dessa forma, nota-se uma nuance no modelo europeu que, assim como ocorreu com as decisões de adequação, pode vir a influenciar a regulação da IA para além de suas fronteiras.

Nesse âmbito, deve-se lembrar que a tecnologia, apesar de ser um importante vetor de inovação, não é neutra. Como ressalta Frazão, "se ficar a cargo apenas dos agentes dominantes, certamente que serão adotadas apenas as tecnologias que se ajustem aos seus interesses, independentemente das repercussões sobre a sociedade e sobre os titulares de dados" (Frazão,

[122] No original, "*A second reason for keeping a national focus is that transnational and supranational arenas involve competition between national fields seeking dominance and fledging "extra-national" regimes (both public and private) with varying degrees of authority and effectiveness. The process of transnational construction is both partial and hierarchically ordered*".

2021, p. 48). O Estado não pode, portanto, se ausentar da regulação de processos e tecnologias que utilizam dados pessoais e dados pessoais sensíveis.

Diante de todo o exposto, interessa à academia, de forma geral, estudar as relações de poder ocultas pelas práticas regulatórias que, embora não deixem de ser legítimas e necessárias para o ordenamento jurídico e para o funcionamento da sociedade, merecem ser conhecidas profunda e sistematicamente, como forma de valorização da soberania nacional e da independência de cada país, assim como proposto na Declaração sobre o Uso do Progresso Científico e Tecnológico no Interesse da Paz e em Benefício da Humanidade de 1975.

CONCLUSÃO

O presente trabalho teve como pretensão ilustrar o estado da arte da regulação da proteção de dados e da IA na UE e nos EUA e analisar o jogo de poder por trás dos modelos regulatórios, que, além de uma questão jurídica, representam uma verdadeira disputa pelo protagonismo de ditar as regras que influenciarão, cada vez mais, o funcionamento da sociedade e a sua interação com a esfera tecnológica.

Para isso, primeiro se perpassou pelo histórico da UE em direção ao RGPD, contextualizando a sua natureza fortemente ligada à dimensão constitucional e explicando de que forma o seu modelo abrangente demonstrou um evidente potencial de exportar, para além de suas fronteiras, suas concepções de direitos fundamentais e *valores europeus*.

Diversos países, desde a década de 1990, passaram a seguir dedicadamente os passos da UE na regulação da proteção de dados, de maneira que os padrões europeus passaram a ser, pelo menos parcialmente, reproduzidos em outros ordenamentos jurídicos.

Isso não necessariamente representa um retrocesso ou uma forma de dominação explícita, uma vez que em nenhum momento houve uma imposição clara, violenta ou obrigatória desses valores. Ademais, o RGPD possui uma essência muito coerente com a disciplina de direitos humanos e fundamentais na contemporaneidade, em especial no paradigma do Estado Democrático de Direito, e a sua forma de regular a proteção de dados tem sido, ao longo dos anos, celebrada e valorizada por boa parte da academia e da sociedade civil.

Sem embargo, esse poder simbólico, ou seja, essa forma de influenciar que se desenvolve sutil e silenciosamente, pode se tornar causa de preocupação caso se expanda para

outras dimensões regulatórias e jurídicas. Por isso, passou-se a observar como tem-se desenvolvido o modelo europeu para a regulação da IA, que tem um potencial ainda maior de determinar a esfera social, não somente no que diz respeito à privacidade de dados, mas muitos outros direitos e valores humanos e fundamentais relacionados à justiça, à equidade, à paz, à valorização do trabalho humano, entre outros.

Assim, o primeiro passo para compreender a regulação da IA foi contextualizar o leitor quanto ao histórico de desenvolvimento dessa ciência, ou tecnologia; fixar noções fundamentais para a compreensão da abrangência e da indefinição desse termo; demonstrar as soluções e problemas que, simultaneamente, representa; e apontar as tendências de tentar, de alguma forma, pautar ou mesmo regular a IA a partir de princípios gerais. Diante dessas noções e da compreensão do seu potencial ambivalente, passou-se a explorar os atuais documentos emitidos pela UE para a regulação da IA.

Como se demonstrou, diversos deles assumem um caráter de recomendação ou de orientação, o que faz sentido dentro da nova lógica consagrada pela doutrina e até mesmos por organismos internacionais como a OCDE, de evitar normas prescritivas e valorizar sugestões éticas, em nome do incentivo ao desenvolvimento tecnológico.

De 2018 a 2020, a UE, recorreu a esse tipo de posicionamento para enunciar seus principais objetivos, muito voltados a uma mudança de papel no cenário internacional do desenvolvimento e da regulação da IA. Inicialmente, portanto, os principais avanços do bloco foram no sentido da consagração de princípios *éticos* especificamente orientados à IA e de um planejamento de atuação conjunta dos Estados-Membros para investir economicamente e cientificamente do desenvolvimento de novas tecnologias. Essas duas novas abordagens, combinadas à estrutura jurídica existente, foram os primeiros pilares erguidos pela UE na sua política regulatória para a IA.

Contudo, os documentos mais recentes, quais sejam, o Livro-Branco e a proposta de Regulamento da IA, passaram a delinear novas ferramentas para a política europeia para a IA: a criação de um sistema de análise prévia de riscos de sistemas de IA que sejam considerados de alto risco, até agora, contudo, sem definir exatamente quais seriam esses riscos e como identificá-los; o desenvolvimento de selos de qualidade para os sistemas de baixo risco, os quais seriam guiados pelos princípios e objetivos da UE, mas não de forma vinculativa; o incentivo aos centros de teste independentes para a condução de auditorias e avaliações.

Todas essas ferramentas, conjuntamente aos princípios éticos, aos direitos fundamentais, ao direito do consumidor e ao direito da proteção de dados, se direcionariam a um fim comum: aumentar a confiança dos consumidores e facilitar o trabalho das autoridades de supervisão competentes apenas na medida necessária para evitar riscos evidentes e graves à sociedade.

O modelo da UE para IA está em pleno desenvolvimento e, por enquanto, é possível apenas observá-lo. A comparação com o caminho traçado na proteção de dados pessoais, contudo, permite algumas especulações e, sem dúvidas, a proposição de alguns questionamentos e preocupações, concentrados sobretudo na possibilidade de continuidade da influência e, portanto, do exercício de um grande poder simbólico, pela UE, na regulação da IA por outros países.

Apesar de a UE falar no desenvolvimento de uma abordagem tecnologicamente neutra, mais especificamente na sua proposta de Regulamento para a IA, ela ainda fala em liderar e protagonizar o cenário internacional. Além de, certa forma, indicar algum tipo de contradição, juntando uma linguagem neutra com uma competitiva, destaca o potencial que a UE tem de "liderar" países terceiros a adotarem um modelo regulatório menos interventivo e prescritivo, voltado à uma regulação *imune ao futuro* e ao rápido desenvolvimento tecnológico, mas possivelmente menos protetivo aos cidadãos e à própria natureza humana.

Continuando a análise, no segundo capítulo, observou-se o sistema estadunidense: primeiramente, no que diz respeito à proteção de dados e, em seguida, à IA, demonstrando como, nesses dois casos, a abordagem americana tem se pautado pela mínima intervenção, deixando ao livre mercado muitas das decisões regulatórias.

A política regulatória da proteção de dados nos EUA se pauta num modelo de *common law* em que a proteção de dados não é um direito constitucional em si e em que não se há decisões significativas da Suprema Corte sobre o tema. Ademais, esse modelo é indissociável dos acordos feitos com a UE ao longo das últimas duas décadas, quais sejam, o Acordo de Porto Seguro, o Escudo de privacidade, e, agora, com o muito recente QPD UE-EUA.

Todos esses acordos se pautaram em práticas autorregulatórias, sendo que os dois primeiros foram derrubados por decisões do TJUE que os considerados inadequados ao modelo europeu. Nesse âmbito, destacou-se a escassa proteção abusos do governo estadunidense, historicamente associado às práticas de vigilância não só aos seus cidadãos, como aos de outros países, sempre em nome da segurança nacional.

O caminho que os EUA têm traçado, sem dúvidas, não é incoerente com a sua imagem ou com a atuação no cenário econômico e geopolítico internacional e as quedas dos acordos anteriores, de certa forma, demonstram o resultado de uma tentativa de conciliação de dois modelos pautados em contextos históricos, culturais e políticos completamente distintos. Sem embargo, as novidades do governo Biden, que trazem algumas limitações às intervenções do governo federal aos dados pessoais, são recentes demais para que se possa confirmar a possibilidade evidenciada por Max Shrems de que o novo acordo será "mais do mesmo".

A segunda parte do capítulo dedicou-se a explicar as iniciativas do governo federal americano na regulação, da IA, composta, desde 2016, por relatórios e por ordem executivas presidenciais derivadas de três gestões diferentes: Obama, Trump e Biden.

Explicitou-se, nesse quadro, a diferença de abordagem de diferentes governos ao longo do tempo, principalmente na linguagem empregada para descrever a intenção de se opor a países competidores, como se o desenvolvimento da IA fosse uma questão de poder material e militar, ou para retratá-la como uma oportunidade para cooperação internacional em que os EUA seriam um *player* importante e interessado na ajuda mútua. Além disso, demonstrou-se a tendência de todos esses governos de garantir que o setor privado estivesse sempre presente na tomada de decisões sobre a IA. Em alguma medida, a academia ainda teria parte nesse processo, mas pouco se falou, nos documentos analisados, sobre como seria a sua participação.

Nesse contexto, a opção da OE 14110 pela regulação a partir de princípios e não de normas vinculativas também foi central para sua iniciativa estadunidense de começar a delinear, de fato, um modelo regulatório. Também, orientou-se pela atribuição, a alguns órgãos públicos, da responsabilidade de emitir e organizar diretrizes, boas práticas e até mesmo um modelo de análise de riscos.

Tudo isso, entretanto, são previsões, todas muito recentes, tendo sido publicas no final da pesquisa, em outubro de 2023, o que, mais uma vez, representou uma dificuldade de analisar como serão incrementadas, na prática, essas ferramentas regulatórias.

No terceiro capítulo, levando-se em conta a análise de cada um dos casos, retomou-se diversos conceitos da teoria de Pierre Bourdieu, com foco nas ideias de *campo* e de *poder simbólico*, para contemplar as semelhanças e as diferenças entre as iniciativas europeias e estadunidense ao longo do tempo e destacar que a forma como interagem e se constroem, interna e externamente indica a existência de um jogo silencioso em que disputa o poder de

pautar tanto as regras da proteção de dados pessoais, agora já mais consolidades, quanto da IA, ainda em desenvolvimento.

Diante disso, foi possível explorar a maneira como as forças nacionais e internacionais fazem parte de um campo que, ao longo do tempo, constrói a si mesmo e é construído por campos externos, como o econômico e político.

Ou seja, mesmo posicionamentos historicamente consolidados e fortalecidos podem vir a ser alterados futuramente por uma diferença de predominância entre determinados interesses, como é caso da abordagem da UE, muito protetiva em relação à proteção de dados pessoais, mas, por enquanto, mais flexível e frágil na proteção dos futuros usuários da IA. O próprio discurso da UE permite entender que essa mudança ocorreu, pelo menos em parte, pelo fato de ter sido ultrapassada no desenvolvimento tecnológico da IA, por países que não eram referência internacional na proteção de dados pessoais e não se pautavam em valores semelhantes aos valores europeus, o que coloca o bloco europeu numa posição menos favorecida nos aspectos econômico e político.

No caso dos EUA, com uma produção regulatória menos consolidada e clara no que diz respeito à proteção de dados e ainda mais recente no que diz respeito à IA, foi difícil tirar conclusões ou apresentar ideias claras sobre as implicações das opções regulatórias tomadas sobre a IA e a sua diferença entre aquelas tomadas em relação à proteção de dados, que foram, à época, muito influenciadas pela relação com a UE.

Diante disso, foram feitas reflexões acerca do que significa a mudança de postura entre diferentes governos e se alterações aparentes realmente significam uma nova conformação, ou um novo balanço de interesses e de poderes no jogo, ou *campo*, regulatório.

Sem dúvidas, a importância do trabalho teve como principal fundamento a possibilidade de alguma política regulatória vir a ser, de certa forma, exportada para outros países, por meio de um discurso neutro que, de forma obscura, desenvolve-se como um poder simbólico de determinar como se escreve a regulação e, até mesmo, a história da sociedade. Foi, de certa forma, o que ocorreu com a exportação do modelo de proteção de dados da UE, ainda que isso tenha tido diversas consequências protetivas para os direitos humanos e fundamentais em outros países, e pode ser o que esteja acontecendo com a flexibilização das tendências europeias para a regulação da IA, possivelmente influenciadas pelo pouco intervencionismo do Estado estadunidense, muito bem aceito pelas empresas que desenvolvem tecnologia e pelo “livre mercado”, mas não necessariamente favorável aos interesses coletivos.

Por fim, ressaltou-se a necessidade de valorização da soberania nacional sobre a regulação de áreas associadas ao desenvolvimento tecnológico, noção que, em 1975, já era apresentada pela Declaração sobre o Uso do Progresso Científico e Tecnológico no Interesse da Paz e em Benefício da Humanidade.

Todas essas respostas são, como destacado na metodologia, resultado não só de uma simples pesquisa bibliográfica e documental, mas resultado de um estudo que, apesar de sem dúvidas aprofundado e enraizado na ciência do direito, reflete

REFERÊNCIAS

ANDERSON, Evan. **Red teaming 101: What is red teaming**? IBM, 19. jul. 2023. Disponível em: https://www.ibm.com/blog/red-teaming-101-what-is-red-teaming/. Acesso em: 18 nov. 2023.

ASSEMBLEIA GERAL DA ONU (1975). **Resolution 3384/1975 (XXX): Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Mankind**. Nova Iorque: ONU, 1975. Disponível em: < https://www.ohchr.org/en/instruments-mechanisms/instruments/declaration-use-scientific-and-technological-progress-interests >. Acesso em: 31 out. 2023.

ARANHA, Marcio Iorio. **Manual de Direito Regulatório: Fundamentos de Direito Regulatório**. 6ª ed., ver. ampl. London: Laccademia Publishing, 2021

BAUMER, David.; EARP, Julia; POINDEXTER, J. C. Internet privacy law: a comparison between the United States and the European Union. **Computers and Security**, v. 23, n. 5, pp. 400-412, 2004.

BERENGUER, Leandro. A Pandemia Covid-19 e o Estado de Emergência em Portugal: Breves Considerações sobre Políticas Públicas. **Revista Portuguesa de Ciência Política**, Lisboa, n. 14, 2020, pp. 33-45.

BIEVER, Celeste. ChatGPT broke the Turing test – the race is on for new ways to assess AI. **Nature**, 25 jul. 2023. Disponível em: https://www.nature.com/articles/d41586-023-02361-7. Acesso em: 06 nov. 2023.

BLAKEMORE, Erin. New AI may pass the famed Turing Test. This is the man who created it. **National Geographic UK**, 28 fev. 2023. Disponível em:

https://www.nationalgeographic.co.uk/science-and-technology/2023/02/new-ai-may-pass-the-famed-turing-test-this-is-the-man-who-created-it. Acesso em: 06 nov. 2023.

BOURDIEU, Pierre. **O poder simbólico**. Lisboa: Edições 70, 2022.

BRATTBERG, Erik; CSERNATONI, Raluca; RUGOVA, Venesa. **Europe and AI: Leading, Lagging Behind, or Carving Its Own Way?** Washington D.C.: Carnegie Endowment for International Peace, 2020. Disponível em: https://carnegieendowment.org/2020/07/09/europe-and-ai-leading-lagging-behind-or-carving-its-own-way-pub-82236. Acesso em: 09 nov. 2023.

BRYSON, Joanna. The Artificial Intelligence of the Ethics of Artificial Intelligence: An Introductory Overview for Law and Regulation. *In*: DUBBER, Markus; PASQUALE, Frank; DAS, Sunit. **The Oxford Handbook of Ethics of AI**. Nova Iorque: Oxford University Press, 2020, pp. 3-25.

CARLSON, Micah. Behind the Curve: Schrems II and the Need for Increased U.S. Data Protection in a Global Economy. **Journal of Corporation Law**, vol. 47, n. 1, 2021, pp. 197-214.

CARMAN, Kelly. The genie is out of the bottle: what do we wish for the future of AI? **Penn State Journal of Law & International Affairs**, v. 9, n. 1, 2020, pp. 180-215.

CURTO, Diogo; DOMINGOS, Nuno; JERÓNIMO, Miguel. O poder simbólico e o projecto simbólico de Pierre Bourdieu. *In*: BOURDIEU, Pierre. **O poder simbólico**. Lisboa: Edições 70, 2022, pp. XV-LII.

ENGELKE, Peter. AI, Society and Governance: An Introduction. **Atlantic Council**, 2020, pp. 1-26. Disponível em: https://www.atlanticcouncil.org/in-depth-research-reports/ai-society-and-governance-an-introduction/. Acesso em: 05 nov. 2023.

EUA. **Executive Order 13859 -- Maintaining American Leadership in Artificial Intelligence**. Washington D.C., 11 fev. 2019. Disponível em: https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence. Acesso em: 09 nov. 2023.

EUA. **Summary Of The 2019 White House Summit On Artificial Intelligence In Government**. Washington D.C., 9 set. 2019. Disponível em: https://trumpwhitehouse.archives.gov/wp-content/uploads/2019/09/Summary-of-White-House-Summit-on-AI-in-Government-September-2019.pdf. Acesso em: 09 nov. 2023.

EUA. **Executive Order 14086 – Policy and Procedures**. Washington D.C., 03 jul. 2023. Disponível em: https://www.state.gov/executive-order-14086-policy-and-procedures/. Acesso em: 04 nov. 2023.

EUA. **Executive Order 14110 – Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence**. Washington D.C., 30 out. 2023. Disponível em: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/. Acesso em: 10 nov. 2023.

FLORIDI, Luciano. Soft ethics, the governance of the digital and the General Data Protection Regulation. **Philosophical Transactions - Royal Society. Mathematical, Physical and Engineering Sciences**, vol 376, n. 2133, nov. 2018, pp. 1-11. Disponível em: https://www.jstor.org/stable/10.2307/26601839. Acesso em: 03 nov. 2023.

FRAZÃO, Ana. Propósitos, Desafios e Parâmetros Gerais dos Programas de Compliance e das Políticas de Proteção de Dados. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (org). **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021. p. 34-63.

GAYO, Miguel Recio. Nivel adecuado para transferencias internacionales de datos. **Derecho PUCP**, n. 83, pp. 207-240, 2019. Disponível em: https://revistas.pucp.edu.pe/index.php/derechopucp/article/view/21472. Acesso em: 31 out. 2023.

GOOGLE AI. **Responsibility: Our Principles**. Disponível em: https://ai.google/responsibility/principles/. Acesso em: 08 nov. 2023.

HOOFNAGLE, Chris Jay. **Federal Trade Commission: Privacy law and Policy**. New York: Cambridge University Press, 2016.

JILSON, Elisa. Aiming for truth, fairness, and equity in your company's use of AI. FTC, 10 abr. 2021. Disponível em: https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai. Acesso em: 10 nov. 2023.

MARTINS, Guilherme. **Manual de Políticas Públicas: as opções econômicas do Estado**. 1ª ed. Lisboa, Editora d'Ideias, 2022.

MASLEJ, Nestor et al. **Artificial Intelligence Index Report 2023**. Stanford: Institute for Human-Centered AI -Stanford University, abr. 2023. Disponível em: https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf. Acesso em: 06 nov. 2023.

MICROSOFT AI. **Responsible AI: Principles and approach**. Disponível em: https://www.microsoft.com/en-us/ai/principles-and-approach/. Acesso em: 08 nov. 2023.

MIHAI, Claudiu. Using and Exporting Digital Authoritarianism. Challengin both Cyberspace and Democracies. **Europolity: Continuity and Change in European Governance**, v. 16, n. 2022, pp. 39-66.

MONTEIRO, Susana; MOREIRA, Amílcar. O ciclo da política pública: da formulação à avaliação Ex Post. Pp. 71-86. In FERRÃO, João; FERRÃO, J. M. Pinto Paixão (Eds.), **Metodologias de Avaliação de Políticas Públicas**. Imprensa da Universidade de Lisboa, 2018. Disponível em: https://repositorio.ul.pt/handle/10451/34438. Acesso em: 13 nov. 2023.

NOYB. European Commission giver EU-US data transfers third round at CJEU. **Noyb - European Center for Digital Rights**, Vienna, 10 jul. 2023. Disponível em: https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu. Acesso em: 05 nov. 2023.

OCDE. Communication Regulators of the Future. Paris: OCDE, out. 2022. Disponível em: https://www.oecd.org/publications/communication-regulators-of-the-future-f02209e6-en.htm. Acesso em: 31 out. 2023.

OCDE. **Practical Guidance on Agile Regulatory Governance to Harness Innovation**. Paris: OCDE, 2021a. Disponível em: https://legalinstruments.oecd.org/public/doc/669/9110a3d9-3bab-48ca-9f1f-4ab6f2201ad9.pdf. Acesso em 31 out. 2023.

OCDE. **Recommendation of the Council for Agile Regulatory Governance to Harness Innovation**. Paris: OCDE, 2021b. Disponível em: < h https://www.oecd.org/mcm/Recommendation-for-Agile-Regulatory-Governance-to-Harness-Innovation.pdf. Acesso em: 31 out. 2023.

PALAZZI, Pablo. **La transmisión internacional de datos personales y la protección de la privacidad: Argentina, América Latina, Estados Unidos y la Unión Europea**. Ciudad Autónoma de Buenos Aires: AdHoc, 2002.

PARLAMENTO EUROPEU. **EU AI Act: first regulation on artificial intelligence**. Estrasburgo, 08 jun. 2023. Disponível em: https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence. Acesso em: 09 nov. 2023.

POTVIN-SOLIS, Laurence. Objectif de sécurité et protection des données personnelles: projection dans l'ordre international d'un système constitutionnel propre à l'Union européenne. *In*: NEFRAMI, Eleftheria.; GATTI, Mauro (ed). **Constitutional Issues of EU External Relations Law**. 1. ed, v. 16. Luxemburgo: Luxembourg Legal Studies, University of Luxembourg, 2018, pp. 343-384. Disponível em: https://doi.org/10.5771/9783845277134-343. Acesso em: 05 nov. 2023.

RUSSEL, Stuartigo; NORVIG, Peter. **Artificial Intelligence: A modern approach**. 4 ed. Londres: Pearson Education, 2022.

ROTENBERG, Marc. Schrems II , from Snowden to China: Toward a new alignment on transatlantic data protection. **European Law Journal**, v. 26, n. 1-2, mar. 2020, pp. 141-152.

SHACKELFORD, Scott; ASARE, Isak; DOCKERY, Rachel; RAYMOND, Anjanette; SEGUEEVA, Alexandra. Should We Trust a Black Box to Safeguard Human Rights? A Comparative Analysis of AI Governance. **UCLA Journal of International Law and Foreign Affairs**, v. 26, n. 1, pp. 35-88.

SHAPING EUROPE'S DIGITAL FUTURE. **High-level expert group on artificial intelligence**. 7 jun. 2022. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai. Acesso em: 09 nov. 2023.

SHAPING EUROPE'S DIGITAL FUTURE. **Ethics guidelines for trustworthy AI**. Luxemburgo, 17 nov. 2022. Disponível em: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. Acesso em: 09 nov. 2023.

SMITH, Andrew. Using Artificial Intelligence and Algorithms. FTC, 8 abr. 2020. Disponível em: https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms. Acesso em: 10 nov. 2023.

SOLOVE, Daniel. Chapter 4: The Problems of Information Privacy Law. *In*: SOLOVE, D. J. **The Digital Person: Technology and Privacy in the Information Age**. Nova Iorque: New York University Press, 2004, pp. 56-74.

SOLOVE, Daniel; HARTZOG, Woodrow. The FTC and the new common law of Privacy. **Columbia Law Review**, Columbia, v. 114:583, pp. 583-676, 2014.

TERPAN, Fabien. EU-US Transfer from *Safe Harbor* to *Privacy Shield*: Back to Square One?. **European Papers**, v. 3, n. 3, pp. 1045-1059, 2018. Disponível em: https://www.europeanpapers.eu/fr/system/files/pdf_version/EP_eJ_2018_3_3_Articles_Fabien_Terpan_00261.pdf. Acesso em: 31 out. 2023.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Acórdão do Tribunal de Justiça (Grande Secção) no processo C-311/18**. Luxemburgo, 16 jul. 2020. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62018CJ0311. Acesso em: 02 nov. 2023.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Acórdão do Tribunal de Justiça (Grande Secção) no processo C-362/14**. Luxemburgo, 6 out. 2015. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62014CJ0362. Acesso em: 02 nov. 2023.

UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. Bruxelas, 24. Out. 1975. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046 . Acesso em: 31 out. 2023.

UNIÃO EUROPEIA. **Directiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de Junho de 2000 relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno («Directiva sobre o comércio electrónico»)**. Bruxelas, 17 jul. 2000. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32000L0031. Acesso em: 31 out. 2023.

UNIÃO EUROPEIA. **Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho [notificada com o número C(2016) 4176]**. Bruxelas, 12 jul. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016D1250. Acesso em: 02 nov. 2023.

UNIÃO EUROPEIA. **Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho.**

Bruxelas, 27 abr. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32016L0680. Acesso em: 31 out. 2023.

UNIÃO EUROPEIA. **Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave.** Bruxelas, 27 abr. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0681. Acesso em: 31 out. 2023.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Bruxelas, 27 abr. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679 . Acesso em: 31 out. 2023.

UNIÃO EUROPEIA. **Comunicação da Comissão: Inteligência artificial para a Europa**. Bruxelas, 24 abr. 2018. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018DC0237. Acesso em: 04 nov. 2023.

UNIÃO EUROPEIA. **Comunicação da comissão ao parlamento europeu ao parlamento europeu, ao conselho, ao comitê econômico e social europeu e o comitê das regiões: Criando confiança na inteligência artificial centrada no ser humano**. Bruxelas, 08 abr. 2019. Disponível em: https://digital-strategy.ec.europa.eu/en/library/communication-building-trust-human-centric-artificial-intelligence. Acesso em: 09 nov. 2023.

UNIÃO EUROPEIA. **Orientações éticas para uma IA confiável**. Bruxelas, 08 abr. 2019. Disponível em: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. Acesso em: 09 nov. 2023.

UNIÃO EUROPEIA. **Livro Branco sobre Inteligência Artificial – Uma abordagem europeia para excelência e confiança**. Bruxelas, 19 fev. 2020. Disponível em: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en. Acesso em: 09 nov. 2023.

UNIÃO EUROPEIA. **Proposta de Regulamento do Parlamento Europeu e do Conselho que Estabelece Regras Harmonizadas em Matéria de Inteligência Artificial (Regulamento Inteligência Artificial) e Altera Determinados Atos Legislativos Da União**. Bruxelas, 26 abr. 2021. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206. Acesso em: 09 nov. 2023.

UNIÃO EUROPEIA. **Decisão de Execução (UE) 2021/914 da Comissão, de 4 de junho de 2021, relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**. Bruxelas, 04 jun. 2021. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32021D0914. Acesso em: 04 nov. 2023.

UNIÃO EUROPEIA. **Decisão de Execução (UE) 2021/915 da Comissão, de 4 de junho de 2021, relativa às cláusulas contratuais-tipo entre os responsáveis pelo tratamento de dados pessoais e os subcontratantes nos termos do artigo 28.o, n.o 7, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho e do artigo 29.o, n.o 7, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho**. Bruxelas, 04 jun. 2021. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32021D0915. Acesso em: 04 nov. 2023.

UNIÃO EUROPEIA. **Decisão (UE) 2021/156 da Comissão, de 9 de fevereiro de 2021, que renova o mandato do Grupo Europeu de Ética para as Ciências e as Novas Tecnologias**. Bruxelas, 10 fev. 2021. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32021D0156. Acesso em 09 nov. 2023.

UNIÃO EUROPEIA. **Decisão de Execução (UE) 2023/1795 da Comissão, de 10 de julho de 2023, nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais no âmbito Quadro de Privacidade de Dados UE-EUA**. Bruxelas, 10 jul. 2023. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32023D1795. Acesso em: 04 nov. 2023.

VERONESE, ALEXANDRE. Transferências internacionais de dados pessoais: o debate transatlântico norte e sua repercussão no Brasil e na América Latina. *In*: SCHERTEL, Laura; DONEDO, Danilo; SARLET, Ingo; RODRIGUES JR. Otavio; BIONI, Bruno. (Org.). **Tratado de Proteção de Dados Pessoais**. 1ed. Rio de Janeiro: Forense, 2021, v. , p. 689-726.

VERONESE, Alexandre; MENDONÇA, Luiza. Padrões de Conformidade Nacionais de Proteção de Dados: Anotações na Perspectiva de *Compliance* após a invalidação do *Privacy Shield* firmado entre os Estados Unidos e a União Europeia. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (org). **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021. p. 97-136.

WIKIPEDIA CONTRIBUTORS. Computer cluster. **Wikipedia, The Free Encyclopedia**. Wikipedia, 6 Nov. 2023. Disponível em: https://en.wikipedia.org/w/index.php?title=Special:CiteThisPage&page=Computer_cluster&id=1183761322&wpFormIdentifier=titleform. Acesso em: 19 nov. 2023.

WHEELER, Michael. Relinquishing Control. *In*: DUBBER, Markus; PASQUALE, Frank; DAS, Sunit. **The Oxford Handbook of Ethics of AI**. Nova Iorque: Oxford University Press, 2020, pp. 350-.357.

WHITE HOUSE. FACT SHEET: **President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence**. Whasington D. C., 30 out. 2023. Disponivel em: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/. Acesso em: 10 nov. 2023.

WHITE HOUSE. WHAT THEY ARE SAYING: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence. Whasington D. C., 31 out. 2023. Disponível em: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/31/what-they-are-saying-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/. Acesso em: 10 nov. 2023.

ANEXO 1 – TABELA COMPARATIVA DOS PRINCÍPIOS DA DIRETIVA 95/46/CE E DO RGPD

	Diretiva 95/46/CE	RGPD
Princípio de licitude	Artigo 6º 1.(a) Objecto de um tratamento leal e lícito;	Artigo 5º 1. (a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);
Princípio da finalidade	Artigo 6º 1. (b) Recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades. O tratamento posterior para fins históricos, estatísticos ou científicos não é considerado incompatível desde que os Estados-membros estabeleçam garantias adequadas;	Artigo 5º 1. (b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.o, n.o 1 («limitação das finalidades»);
Princípio da minimização dos dados	Artigo 6º 1. (c) Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente;	Artigo 5º 1. (c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);
Princípio da exatidão	Artigo 6º 1. (d) Exactos e, se necessário, actualizados; devem ser tomadas todas as medidas razoáveis para assegurar que os dados inexactos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados	Artigo 5º 1. (d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»);

	posteriormente, sejam apagados ou rectificados;	
Princípio da limitação da conservação	Artigo 6º 1. (e) Conservados de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente. Os Estados-membros estabelecerão garantias apropriadas para os dados pessoais conservados durante períodos mais longos do que o referido, para fins históricos, estatísticos ou científicos.	Artigo 5º 1. (e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n.o 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»);
Princípio da integridade e confidencialidade	Artigo 16º Qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, bem como o próprio subcontratante, tenha acesso a dados pessoais, não procederá ao seu tratamento sem instruções do responsável pelo tratamento, salvo por força de obrigações legais. Artigo 17º 1. Os Estados-membros estabelecerão que o responsável pelo tratamento deve pôr em prática medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito. Estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger. 2. Os Estados-membros estabelecerão que o responsável pelo tratamento, em caso de tratamento por sua conta, deverá escolher um subcontratante que ofereça garantias suficientes em relação às medidas de segurança técnica e de organização do tratamento a efectuar e deverá zelar pelo cumprimento dessas medidas 3. A realização de operações de tratamento em subcontratação deve ser regida por um contrato ou acto jurídico que vincule o subcontratante ao	Artigo 5º 1 (f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»); Artigo 32.o 1. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado: a) A pseudonimização e a cifragem dos dados pessoais; b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento. 2. Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento. 3. O cumprimento de um código de conduta aprovado conforme referido no artigo 40.o ou de um procedimento de certificação aprovado

	responsável pelo tratamento e que estipule, designadamente, que: - o subcontratante apenas actuará mediante instruções do responsável pelo tratamento, - as obrigações referidas no nº 1, tal como definidas pela legislação do Estado-membro onde o subcontratante está estabelecido, incumbem igualmente a este último. 4. Para efeitos de conservação de provas, os elementos do contrato ou do acto jurídico relativos à protecção dos dados, bem como as exigências relativas às medidas referidas no nº 1, deverão ficar consignados por escrito ou sob forma equivalente.	conforme referido no artigo 42.o pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas no n.o 1 do presente artigo. 4. O responsável pelo tratamento e o subcontratante tomam medidas para assegurar que qualquer pessoa singular que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenha acesso a dados pessoais, só procede ao seu tratamento mediante instruções do responsável pelo tratamento, exceto se tal lhe for exigido pelo direito da União ou de um Estado-Membro.
Princípio da responsabilidade	Artigo 6º 2. Incumbe ao responsável pelo tratamento assegurar a observância do disposto no nº 1.	Artigo 5º 2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.o 1 e tem de poder comprová-lo («responsabilidade»).
Consentimento	Artigo 7º Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efectuado se: a) A pessoa em causa tiver dado de forma inequívoca o seu consentimento; ou b) O tratamento for necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa; ou c) O tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito; ou d) O tratamento for necessário para a protecção de interesses vitais da pessoa em causa; ou e) O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados; ou f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do artigo 1º.	Artigo 6º 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança. O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica. 2. Os Estados-Membros podem manter ou aprovar disposições mais específicas com o objetivo de adaptar a aplicação das regras do presente regulamento no que diz respeito ao tratamento de dados para o cumprimento do n.o 1, alíneas c) e e), determinando, de forma mais

		precisa, requisitos específicos para o tratamento e outras medidas destinadas a garantir a licitude e lealdade do tratamento, inclusive para outras situações específicas de tratamento em conformidade com o capítulo IX. 3. O fundamento jurídico para o tratamento referido no n.o 1, alíneas c) e e), é definido: a) Pelo direito da União; ou b) Pelo direito do Estado-Membro ao qual o responsável pelo tratamento está sujeito. A finalidade do tratamento é determinada com esse fundamento jurídico ou, no que respeita ao tratamento referido no n.o 1, alínea e), deve ser necessária ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento. Esse fundamento jurídico pode prever disposições específicas para adaptar a aplicação das regras do presente regulamento, nomeadamente: as condições gerais de licitude do tratamento pelo responsável pelo seu tratamento; os tipos de dados objeto de tratamento; os titulares dos dados em questão; as entidades a que os dados pessoais poderão ser comunicados e para que efeitos; os limites a que as finalidades do tratamento devem obedecer; os prazos de conservação; e as operações e procedimentos de tratamento, incluindo as medidas destinadas a garantir a legalidade e lealdade do tratamento, como as medidas relativas a outras situações específicas de tratamento em conformidade com o capítulo IX. O direito da União ou do Estado-Membro deve responder a um objetivo de interesse público e ser proporcional ao objetivo legítimo prosseguido. 4. Quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23.o, n.o 1, o responsável pelo tratamento, a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, tem nomeadamente 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) A existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização.
Direito de informação (dados recolhidos junto ao titular)	Artigo 10º Os Estados-membros estabelecerão que o responsável pelo tratamento ou o seu representante deve fornecer à pessoa em causa junto da qual recolha dados que lhe digam respeito, pelo menos as seguintes informações, salvo se a pessoa já delas tiver conhecimento: a) Identidade do responsável pelo tratamento e, eventualmente, do seu representante; b) Finalidades do tratamento a que os dados se destinam; c) Outras informações, tais como: - os destinatários ou categorias de destinatários dos dados, - o carácter obrigatório ou facultativo da resposta, bem como as possíveis consequências se não responder, - a existência do direito de acesso aos dados que lhe digam respeito e do direito de os rectificar, desde que sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir à pessoa em causa um tratamento leal dos mesmos.	Artigo 13.o 1. Quando os dados pessoais forem recolhidos junto do titular, o responsável pelo tratamento faculta-lhe, aquando da recolha desses dados pessoais, as seguintes informações: a) A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante; b) Os contactos do encarregado da proteção de dados, se for caso disso; c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento; d) Se o tratamento dos dados se basear no artigo 6.o, n.o 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro; e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver; f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.o ou 47.o, ou no artigo 49.o, n.o 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas. 2. Para além das informações referidas no n.o 1, aquando da recolha dos dados pessoais, o responsável pelo tratamento fornece ao titular as seguintes informações adicionais, necessárias para garantir um tratamento equitativo e transparente: a) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo; b) A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados; c) Se o tratamento dos dados se basear no artigo 6.o, n.o 1, alínea a), ou no artigo 9.o, n.o 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado; d) O direito de apresentar reclamação a uma autoridade de controlo;

		e) Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados; f) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.o, n.os 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.3. Quando o responsável pelo tratamento de dados pessoais tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados tenham sido recolhidos, antes desse tratamento o responsável fornece ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes, nos termos do n.o 2. 4. Os n.os 1, 2 e 3 não se aplicam quando e na medida em que o titular dos dados já tiver conhecimento das informações.
Direito de informação (dados não recolhidos junto ao titular)	Artigo 11º 1. Se os dados não tiverem sido recolhidos junto da pessoa em causa, os Estados-membros estabelecerão que o responsável pelo tratamento, ou o seu representante, deve fornecer à pessoa em causa, no momento em que os dados forem registados ou, se estiver prevista a comunicação de dados a terceiros, o mais tardar aquando da primeira comunicação desses dados, pelo menos as seguintes informações, salvo se a referida pessoa já delas tiver conhecimento: a) Identidade do responsável pelo tratamento e, eventualmente, do seu representante; b) Finalidades do tratamento; c) Outras informações, tais como: - as categorias de dados envolvidos, - os destinatários ou categorias de destinatários dos dados, - a existência do direito de acesso aos dados que lhe digam respeito e do direito de os rectificar, desde que sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir à pessoa em causa um tratamento leal dos mesmos. 2. O nº 1 não se aplica quando, nomeadamente no caso do tratamento de dados com finalidades estatísticas, históricas ou de investigação científica, a informação da pessoa em causa se revelar impossível ou implicar esforços desproporcionados ou quando	Artigo 14.o 1. Quando os dados pessoais não forem recolhidos junto do titular, o responsável pelo tratamento fornece-lhe as seguintes informações: a) A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante; b) Os contactos do encarregado da proteção de dados, se for caso disso; c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento; d) As categorias dos dados pessoais em questão; e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver; f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.o ou 47.o, ou no artigo 49.o, n.o 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas; 2. Para além das informações referidas no n.o 1, o responsável pelo tratamento fornece ao titular as seguintes informações, necessárias para lhe garantir um tratamento equitativo e transparente: a) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para fixar esse prazo; b) Se o tratamento dos dados se basear no artigo 6.o, n.o 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro;

	a lei dispuser expressamente o registo dos dados ou a sua divulgação. Nestes casos, os Estados-membros estabelecerão as garantias adequadas.	c) A existência do direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais que lhe digam respeito, e a retificação ou o apagamento, ou a limitação do tratamentor no que disser respeito ao titular dos dados, e do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados; d) Se o tratamento dos dados se basear no artigo 6.o, n.o 1, alínea a), ou no artigo 9.o, n.o 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado; e) O direito de apresentar reclamação a uma autoridade de controlo; f) A origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público; g) A existência de decisões automatizadas, incluindo a definição de perfis referida no artigo 22.o, n.os 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados. 3. O responsável pelo tratamento comunica as informações referidas nos n.os 1 e 2: a) Num prazo razoável após a obtenção dos dados pessoais, mas o mais tardar no prazo de um mês, tendo em conta as circunstâncias específicas em que estes forem tratados; b) Se os dados pessoais se destinarem a ser utilizados para fins de comunicação com o titular dos dados, o mais tardar no momento da primeira comunicação ao titular dos dados; ou c) Se estiver prevista a divulgação dos dados pessoais a outro destinatário, o mais tardar aquando da primeira divulgação desses dados. 4. Quando o responsável pelo tratamento tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados pessoais tenham sido obtidos, antes desse tratamento o responsável fornece ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes referidas no n.o 2. 5. Os n.os 1 a 4 não se aplicam quando e na medida em que: a) O titular dos dados já tenha conhecimento das informações; b) Se comprove a impossibilidade de disponibilizar a informação, ou que o esforço envolvido seja desproporcionado, nomeadamente para o tratamento para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, sob reserva das condições e garantias previstas no artigo 89.o, n.o 1, e na medida em que a obrigação referida no n.o 1 do presente artigo seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento. Nesses casos, o

		responsável pelo tratamento toma as medidas adequadas para defender os direitos, liberdades e interesses legítimos do titular dos dados, inclusive através da divulgação da informação ao público; c) A obtenção ou divulgação dos dados esteja expressamente prevista no direito da União ou do Estado-Membro ao qual o responsável pelo tratamento estiver sujeito, prevendo medidas adequadas para proteger os legítimos interesses do titular dos dados; ou d) Os dados pessoais devam permanecer confidenciais em virtude de uma obrigação de sigilo profissional regulamentada pelo direito da União ou de um Estado-Membro, inclusive uma obrigação legal de confidencialidade.
Direito de acesso	Artigo 12º Os Estados-membros garantirão às pessoas em causa o direito de obterem do responsável pelo tratamento: a) Livremente e sem restrições, com periodicidade razoável e sem demora ou custos excessivos: - a confirmação de terem ou não sido tratados dados que lhes digam respeito, e informações pelo menos sobre os fins a que se destina esse tratamento, as categorias de dados sobre que incide e os destinatários ou categorias de destinatários a quem são comunicados os dados, - a comunicação, sob forma inteligível, dos dados sujeitos a tratamento e de quaisquer informações disponíveis sobre a origem dos dados, - o conhecimento da lógica subjacente ao tratamento automatizado dos dados que lhe digam respeito, pelo menos no que se refere às decisões automatizadas referidas no nº 1 do artigo 15º; b) Consoante o caso, a rectificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpra o disposto na presente directiva, nomeadamente devido ao carácter incompleto ou inexacto desses dados; c) A notificação aos terceiros a quem os dados tenham sido comunicados de qualquer rectificação, apagamento ou bloqueio efectuado nos termos da alínea b), salvo se isso for comprovadamente impossível ou implicar um esforço desproporcionado.	Artigo 15.o 1. O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações: a) As finalidades do tratamento dos dados; b) As categorias dos dados pessoais em questão; c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais; d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo; e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento; f) O direito de apresentar reclamação a uma autoridade de controlo; g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados; h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.o, n.os 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados. 2. Quando os dados pessoais forem transferidos para um país terceiro ou uma organização internacional, o titular dos dados tem o direito de ser informado das garantias adequadas, nos termos do artigo 46.o relativo à transferência de dados. 3. O responsável pelo tratamento fornece uma cópia dos dados pessoais em fase de tratamento. Para fornecer outras cópias solicitadas pelo titular dos dados, o responsável pelo tratamento pode exigir o pagamento de uma taxa razoável tendo

		em conta os custos administrativos. Se o titular dos dados apresentar o pedido por meios eletrónicos, e salvo pedido em contrário do titular dos dados, a informação é fornecida num formato eletrónico de uso corrente. 4. O direito de obter uma cópia a que se refere o n.o 3 não prejudica os direitos e as liberdades de terceiros.
Direito de retificação		Artigo 16.o O titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional.
Direito ao apagamento de dados ou ao esquecimento		Artigo 17.o 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos: a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.o, n.o 1, alínea a), ou do artigo 9.o, n.o 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento; c) O titular opõe-se ao tratamento nos termos do artigo 21.o, n.o 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.o, n.o 2; d) Os dados pessoais foram tratados ilicitamente; e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.o, n.o 1. 2. Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.o 1, toma as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos. 3. Os n.os 1 e 2 não se aplicam na medida em que o tratamento se revele necessário:

		a) Ao exercício da liberdade de expressão e de informação; b) Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento; c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9.o, n.o 2, alíneas h) e i), bem como do artigo 9.o, n.o 3; d) Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.o, n.o 1, na medida em que o direito referido no n.o 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento; ou e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial.
Direito à limitação do tratamento		Artigo 18.o 1. O titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento, se se aplicar uma das seguintes situações: a) Contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão; b) O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização; c) O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial; d) Se tiver oposto ao tratamento nos termos do artigo 21.o, n.o 1, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados. 2. Quando o tratamento tiver sido limitado nos termos do n.o 1, os dados pessoais só podem, à exceção da conservação, ser objeto de tratamento com o consentimento do titular, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa singular ou coletiva, ou por motivos ponderosos de interesse público da União ou de um Estado-Membro. 3. O titular que tiver obtido a limitação do tratamento nos termos do n.o 1 é informado pelo responsável pelo tratamento antes de ser anulada a limitação ao referido tratamento.
Direito de portabilidade dos dados		Artigo 20.o Direito de portabilidade dos dados 1. O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num

		formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se: a) O tratamento se basear no consentimento dado nos termos do artigo 6.o, n.o 1, alínea a), ou do artigo 9.o, n.o 2, alínea a), ou num contrato referido no artigo 6.o, n.o 1, alínea b); e b) O tratamento for realizado por meios automatizados. 2 Ao exercer o seu direito de portabilidade dos dados nos termos do n.o 1, o titular dos dados tem o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível. 3. O exercício do direito a que se refere o n.o 1 do presente artigo aplica-se sem prejuízo do artigo 17.o. Esse direito não se aplica ao tratamento necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento. 4. O direito a que se refere o n.o 1 não prejudica os direitos e as liberdades de terceiros.
Direito de oposição	Artigo 14º Os Estados-membros reconhecerão à pessoa em causa o direito de: a) Pelo menos nos casos referidos nas alíneas e) e f) do artigo 7º, se opor em qualquer altura, por razões preponderantes e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objecto de tratamento, salvo disposição em contrário do direito nacional. Em caso de oposição justificada, o tratamento efectuado pelo responsável deixa de poder incidir sobre esses dados; b) Se opor, a seu pedido e gratuitamente, ao tratamento dos dados pessoais que lhe digam respeito previsto pelo responsável pelo tratamento para efeitos de mala directa; ou ser informada antes de os dados pessoais serem comunicados pela primeira vez a terceiros para fins de mala directa ou utilizados por conta de terceiros, e de lhe ser expressamente facultado o direito de se opor, sem despesas, a tais comunicações ou utilizações. Os Estados-membros tomarão as medidas necessárias para garantir que as pessoas em causa tenham conhecimento do direito referido no primeiro parágrafo da alínea b).	Artigo 21.o 1. O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6.o, n.o 1, alínea e) ou f), ou no artigo 6.o, n.o 4, incluindo a definição de perfis com base nessas disposições. O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial. 2. Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta. 3. Caso o titular dos dados se oponha ao tratamento para efeitos de comercialização direta, os dados pessoais deixam de ser tratados para esse fim. 4. O mais tardar no momento da primeira comunicação ao titular dos dados, o direito a que se referem os n.os 1 e 2 é explicitamente levado à atenção do titular dos dados e é apresentado de modo claro e distinto de quaisquer outras informações.

		5. No contexto da utilização dos serviços da sociedade da informação, e sem prejuízo da Diretiva 2002/58/CE, o titular dos dados pode exercer o seu direito de oposição por meios automatizados, utilizando especificações técnicas. 6. Quando os dados pessoais forem tratados para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.o, n.o 1, o titular dos dados tem o direito de se opor, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, salvo se o tratamento for necessário para a prossecução de atribuições de interesse público.
Direito de oposição (decisões automatizadas)	Artigo 15º 1. Os Estados-membros reconhecerão a qualquer pessoa o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afecte de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, como por exemplo a sua capacidade profissional, o seu crédito, confiança de que é merecedora, comportamento. 2. Os Estados-membros estabelecerão, sob reserva das restantes disposições da presente directiva, que uma pessoa pode ficar sujeita a uma decisão do tipo referido no nº 1 se a mesma: a) For tomada no âmbito da celebração ou da execução de um contrato, na condição de o pedido de celebração ou execução do contrato apresentado pela pessoa em causa ter sido satisfeito, ou de existirem medidas adequadas, tais como a possibilidade de apresentar o seu ponto de vista, que garantam a defesa dos seus interesses legítimos; ou b) For autorizada por uma lei que estabeleça medidas que garantam a defesa dos interesses legítimos da pessoa em causa.	Artigo 22.o 1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar. 2. O n.o 1 não se aplica se a decisão: a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou c) For baseada no consentimento explícito do titular dos dados. 3. Nos casos a que se referem o n.o 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão. 4. As decisões a que se refere o n.o 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9.o, n.o 1, a não ser que o n.o 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular.

Tabela 1 – comparação entre os princípios e direitos dos titulares previstos pela Diretiva 95/46/CE e pelo RGPD – elaboração própria