CAROLINE VIVAS GONÇALVES

O DIREITO À EXPLICAÇÃO NA DIRETIVA (UE) 2016/680 E SUAS PERSPECTIVAS PARA O CENÁRIO BRASILEIRO

Dissertação de Mestrado com vistas à obtenção do grau de Mestre em Direito e Segurança, pela Faculdade de Direito da Universidade Nova de Lisboa.

Orientador:
Professor Doutor Eduardo Magrani

Julho de 2021

CAROLINE VIVAS GONÇALVES

Nº 6139

O DIREITO À EXPLICAÇÃO NA DIRETIVA (UE) 2016/680 E SUAS PERSPECTIVAS PARA O CENÁRIO BRASILEIRO

Dissertação de mestrado com vistas à obtenção do grau de Mestre em Direito e Segurança, pela Faculdade de Direito da Universidade Nova de Lisboa.

Orientador:

Professor Doutor Eduardo Magrani

Julho de 2021

NOVA SCHOOL OF LAW

O DIREITO À EXPLICAÇÃO NA DIRETIVA (UE) 2016/680 E SUAS PERSPECTIVAS PARA O CENÁRIO BRASILEIRO

Caroline Vivas Gonçalves

Julho
2021

DECLARAÇÃO DE COMPROMISSO ANTIPLÁGIO

Declaro por minha honra que o trabalho que apresento é original e que todas as minhas citações estão corretamente identificadas. Tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta ética e disciplinar.

Lisboa, julho de 2021.

Caroline Vivas Gonçalves

DECLARAÇÃO DE NÚMERO DE CARACTERES

Declaro que o corpo da dissertação que apresento, incluindo espaços e notas, ocupa um total de 193.802 caracteres.

Lisboa, julho de 2021.

Caroline Vivas Gonçalves

DEDICATÓRIA

À minha amada filha Isabela Temer.

AGRADECIMENTOS

A Jesus: o mestre dos mestres. O maior especialista na arte de ensinar. Aquele que, embora não tenha deixado sequer uma página escrita e não tenha lecionado em nenhuma Universidade, ainda assim foi o MAIOR MESTRE que este mundo já conheceu.

Aos meus pais, Angélica e Luiz, pelo amor, incentivo e apoio incondicional. Mãe, obrigada por acreditar em mim. Você é meu paradigma, meu porto seguro. À minha filha Isabela, por iluminar de maneira especial os meus pensamentos e a Dudu por alegrar os meus dias. À minha irmã Danny, ao meu sobrinho Daniel e à minha Tia Maria da Paz, pelo companheirismo, compreensão e amor.

Agradeço também, em especial, ao meu orientador, o professor Doutor Eduardo Magrani, pela disponibilidade e confiança depositadas nesse estudo e pela paciência e sabedoria demonstrada com os seus orientandos.

Uma particular gratidão aos funcionários e colegas da Faculdade de Direito da Universidade Nova de Lisboa e, de maneira muito especial, aos Coordenadores do Mestrado em Direito e Segurança, os doutos Professores Armando Marques Guedes e Felipe Pathé Duarte, cujo agradecimento estendo a todos os professores do curso.

À minha mentora Viviane Maldonado e aos meus amigos trilheiros, companheiros de jornada nessa aventura apaixonante que é a proteção de dados pessoais.

E a todos que, direta ou indiretamente, venceram comigo esta etapa: o meu muito obrigada!

LISTA DE ABREVIATURAS

ANPD – Autoridade Nacional de Proteção de Dados

ART. – Artigo

ARTS. – Artigos

CDC – Código de Defesa do Consumidor

CC – Código Civil

CP – Código Penal

CFTV – Circuito Fechado de Televisão

CNPD – Comissão Nacional de Proteção de Dados

CRP – Constituição da República Portuguesa

GPS – Global Positioning System

GT29 – Grupo de Trabalho do Artigo 29º.

IA – Inteligência Artificial

LGPD – Lei Geral de Proteção de Dados

N.º – Número

ONU – Organização das Nações Unidas

P. – página ou páginas

PNUD – Programa das Nações Unidas para o Desenvolvimento

RGPD – Regulamento Geral sobre a Proteção de Dados

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

TJUE – Tribunal de Justiça da União Europeia

UE – União Europeia

V. – volume

Wp251 – Documento do GT29: "Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679"

Wp258 – Documento do GT29: "Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (Diretiva (UE) 2016/680)"

RESUMO

O uso de técnicas relacionadas ao tratamento automatizado de dados, dentre os quais se incluem em grande escala os dados pessoais, é uma realidade que vem aumentando e que, hodiernamente, também tem crescido no cenário do policiamento preditivo e da justiça criminal, levantado preocupações de cunho ético e jurídico. Nesse sentido, pode-se afirmar que as decisões automatizadas são consideradas como um ponto de intersecção entre a proteção de dados pessoais e o uso de técnicas modernas por algoritmos. Esta dissertação tem como objetivo avaliar se esses modelos de tomada de decisões automatizadas utilizados na seara criminal tratam dados pessoais e, dessa forma, se estariam dentro do escopo das normas de proteção de dados pessoais, além de analisar se os indivíduos impactados por decisões desse tipo poderiam gozar os direitos e salvaguardas para obter uma explicação sobre as mesmas. Diante da análise do Regulamento Geral sobre a Proteção de Dados, da Diretiva (UE) 2016/680, da Lei Geral de Proteção de Dados brasileira e do Anteprojeto brasileiro da LGPD-Penal chega-se à conclusão que, apesar do léxico “explicação" não constar textualmente no corpo da lei, deve ser assegurado que os titulares dos dados, querendo, recebam uma explicação clara e suficiente acerca do resultado obtido, bem como dos dados pessoais utilizados e da lógica que envolveu o tratamento, além de terem direito a manifestar seu ponto de vista, contestar a decisão e obter intervenção humana.

Palavras-chave: policiamento preditivo, proteção de dados pessoais, inteligência artificial, decisões automatizadas, direito à explicação, ética.

ABSTRACT

The use of techniques related to automated data processing, which include on a large scale, personal data, is a reality that has been increasing and that, nowadays, has also grown in the scenario of predictive policing and criminal justice, raising concerns ethical and legal. In this sense, it can be said that automated decisions are considered as an intersection point between the protection of personal data and the use of modern techniques by algorithm programming. This dissertation aims to assess whether these automated decision-making models used in the criminal area, handling personal data, would be within the scope of personal data protection rules. In addition, it is analyzed if individuals impacted by such decisions type have formal rights and safeguards to obtain an explanation about the content of decisions. In view of the analysis of the General Data Protection Regulation, Directive (EU) 2016/680, the brazilian General Data Protection Law and the LGPD-Penal Draft, it is concluded that, despite the lexicon "explanation" does not appear expressly in the law, it must be ensured that the data subjects, willing, receive a clear and sufficient explanation about the data used and the logic involved in the decision process. Moreover, it is defended the entitlement of the interested persons to express their point of view, contest the decision and obtain human intervention.

Keywords: predictive policing, personal data protection, artificial intelligence, automated decision-making, right to explanation, ethics.

INTRODUÇÃO

O presente trabalho de dissertação, intitulado "O direito à explicação na Diretiva (UE) 2016/680 e suas perspectivas para o cenário brasileiro", foi elaborado no âmbito do Mestrado em Direito e Segurança da NOVA School of Law e surgiu por conta da pequena produção científica desenvolvida acerca da temática.

Muito se argumenta sobre a existência de um chamado "direito à explicação" em matéria de decisões automatizadas tomadas dentro do escopo do Regulamento Geral Europeu de Proteção de Dados (Regulamento 2016/679) e da Lei Geral Brasileira de Proteção de Dados (Lei nº 13.709/2018).

Porém, ainda são incipientes as discussões acerca desse mesmo direito no ramo da Diretiva (UE) 2016/680, que aborda, especificamente, o tratamento de dados pessoais realizado por autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais. Além disso, o ordenamento jurídico brasileiro sequer dispõe, no momento, de uma legislação sobre a proteção de dados em matéria penal, tendo em vista que ainda segue em tramitação, e por isso sem conclusão, o "Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Investigação Criminal".

O debate que se propõe mostra-se pertinente levando-se em consideração que a globalização e o advento da tecnologia alteraram a concepção de Estado; a economia; o comportamento humano; as relações interpessoais; a noção de espaço físico; e a própria noção de segurança que se viu impactada pela introjeção dessas novas técnicas e precisou se adaptar e modernizar para fazer frente aos desafios de uma nova sociedade de risco, transnacional e tecnológica.

A interação entre o homem e as máquinas também se viu diretamente afetada e, hodiernamente, é comum observar que o homem passa a delegar àquelas a atribuição de tomar importantes decisões que poderão impactar de forma significativa a sua vida e a dos demais, através de decisões autônomas por sistemas de Inteligência Artificial que se valem de um grande volume de dados, pessoais ou não, para criar correlações, aprender, replicar padrões e mesmo realizar predições.

As decisões automatizadas podem ser entendidas como um ponto de intersecção entre a proteção de dados pessoais e o uso de técnicas modernas por algoritmos.

Atualmente, tem-se observado um aumento do uso da técnica de criação de perfis e decisões automatizadas no contexto criminal das atividades de prevenção, investigação, detecção ou execução de sanções penais, sob a crença de que esses algoritmos seriam mais assertivos, imparciais e justos que os seres humanos ao tomar decisões, pois, em tese, estariam isentos dos preconceitos sociais.

Assim, o surgimento dessas novas técnicas juntamente com o contexto da atual sociedade de risco revelou a insuficiência do modelo tradicional de policiamento reativo e obrigou o surgimento de um novo paradigma no combate à criminalidade. Desse modo, utilizando-se da tecnologia, e tomando como base as estatísticas criminais passadas, percebeu-se a existência de padrões que permitiam obter um panorama acerca de prováveis eventos futuros, surgindo a noção do policiamento preditivo.

Neste trabalho, serão avaliados alguns programas que versam sobre avaliações de risco que podem ser utilizados no contexto do policiamento preditivo, frisando que a operabilidade desses sistemas é pouco transparente e que esses algoritmos ainda são protegidos por propriedade intelectual.

Mas esses modelos de tomada de decisões automatizadas na seara criminal tratam dados pessoais? O tratamento de dados realizado nesse contexto estaria dentro do escopo das normas de proteção de dados pessoais? Nesse sentido, como fica a situação dos indivíduos impactados por decisões desse tipo de processamento automatizado de dados pessoais? Eles poderiam gozar os direitos e salvaguardas para obter uma explicação sobre as mesmas? Efetivamente, existe um direito à explicação no bojo da Diretiva (UE) 2016/680? E quanto ao cenário brasileiro?

Essas são questões a serem respondidas por esse trabalho.

Os objetivos buscados são: demonstrar que os modelos expostos tratam dados pessoais e como a falta de transparência no tratamento automatizado desses dados podem ocasionar injustiças que não poderão ser retificadas se o titular não tiver acesso à uma explicação da decisão que se busca sindicar em âmbito penal; nortear o debate no Brasil que ainda está embrionário, ou praticamente inexistente, sobretudo quando se considera que a vindoura lei penal ainda não fora aprovada e a lei geral ainda é deveras desconhecida dentre os próprios destinatários da norma: os titulares; apontar que o direito à explicação e a intervenção humana são prerrogativas para que haja uma decisão mais justa, transparente e equitativa, ou pelo menos, para que o indivíduo compreenda os motivos que envolveram a

lógica subjacente da decisão para, querendo, expor seu ponto de vista e eventual contestação; e discutir a necessidade de uma eficaz regulamentação jurídica e ética que devem suportar essas decisões.

Tratando-se de questões cujas respostas implicam, necessariamente, o estudo da área do Direito e de novas tecnologias, seguiu-se a uma abordagem interdisciplinar, motivo pelo qual o resultado é uma bibliografia contendo obras de outros ramos do saber, além do próprio Direito.

A dissertação foi elaborada a partir de uma metodologia jurídico-exploratória que combinou bibliografia portuguesa, brasileira e estrangeira. Para esse estudo, foram analisadas questões conceituais de algoritmos, Inteligência Artificial, aprendizado de máquina, definições de perfis e tomadas de decisões automatizadas; bem como os mecanismos normativo-regulatórios relacionados à proteção de dados pessoais; como também as hipóteses e teorias que podem embasar a existência de um direito à explicação das decisões automatizadas tomadas no cenário da Diretiva (UE) 2016/680 e da vindoura lei brasileira.

De forma a atingir os objetivos acima mencionados, o presente trabalho acadêmico encontra-se estruturado ao longo de cinco capítulos da seguinte forma:

O primeiro capítulo aborda a alteração do paradigma do Estado e da segurança em face de diversos fenômenos como a globalização, o surgimento das novas tecnologias, as revoluções industriais e a ascensão da sociedade de risco, bem como, a forma que a tecnologia vem impactando a sociedade contemporânea e influenciado os comportamentos humanos, inclusive, aqueles de cunho decisório.

No capítulo posterior há uma breve análise do conceito e da evolução histórica do direito à privacidade e do direito à proteção de dados pessoais e a análise dos diplomas mais relevantes sobre o assunto, além da evolução legislativa sobre o tema no Brasil.

O terceiro capítulo ocupa-se de explicar os conceitos técnicos de Inteligência Artificial que interessam ao tema proposto, bem como o que são as decisões automatizadas e as definições de perfis dentro desse contexto, além de apontar a existência da opacidade nesses sistemas que se utilizam do tratamento automatizado e a possibilidade de ocorrerem discriminações. Ademais, discorre sobre o aumento do uso dessas técnicas no policiamento preditivo e pondera se esses programas fazem uso de dados pessoais.

Após, o quarto capítulo reflete os direitos do RGPD e da LGPD que versam sobre o direito do titular dos dados a uma explicação sobre a decisão tomada com base no tratamento automatizado e expõe as principais teorias quanto à existência desse direito no âmbito do regulamento geral europeu e da lei geral brasileira. Ato contínuo, defende que esse direito também pode ser extraído da Diretiva (UE) 2016/680 e da vindoura LGPD-Penal e apresenta os subsídios para justificar a existência dentro dos mesmos, ao passo que salienta a importância da intervenção humana, cuja ausência pode acarretar em graves violações aos direitos e liberdades dos titulares de dados afetados pelas decisões automatizadas sob análise.

O último capítulo aborda a possibilidade da extensão do conceito *by design* (oriundo do *privacy by design*) para o campo da ética e da justiça, como forma de garantir transparência nessa regulação, incorporando-se de forma criteriosa a ética e os direitos humanos desde o momento em que uma Inteligência Computacional, que será utilizada para a tomada de decisões que afetarão significativamente a vida de seres humanos, é projetada. Além disso, são analisados diversos documentos e os instrumentos de controle como as auditorias e as avaliações de impacto. Por fim, constam as considerações finais do trabalho.

Capítulo I – CONTEXTUALIZAÇÃO DO TEMA

1.1 - Visão clássica do Estado

O Estado, enquanto organização política e social, é responsável pela proteção de seu povo e garantia da segurança interna e externa de seu território. Essa proteção encontra amparo no *iusprotectionis* que é o "direito à proteção que todo cidadão pode reivindicar em decorrência de sua nacionalidade"[1].

Para que a segurança proporcionada pelo Estado fosse eficaz foi necessário que este interviesse na esfera particular dos indivíduos tolhendo parcialmente outro direito essencial, a liberdade, com vistas à garantia da estabilidade e segurança da sociedade, institucionalizando-se, inclusive, a força pública.

Entrementes, com a chamada Paz de Westefália, em 1648, a soberania passa a ser tradicionalmente considerada sob a ótica das fronteiras geograficamente definidas, delimitando-se assim o que é externo e interno e, via de consequência, as ameaças externas e internas[2].

O conceito tradicional de segurança nasce então refletindo o ideal estatocêntrico da época, com a monopolização do uso da força sob o argumento de que a coercibilidade, integrante da supremacia estatal, seria indispensável para a manutenção da ordem. Entretanto, o modelo estatal de estrutura centralista e monolítico foi gradualmente perdendo força devido à evolução própria da dinâmica social.

Em consonância, ante a complexidade de sua natureza polissêmica e sujeita a implicações políticas e ideológicas, o significado de segurança também passou, recorrentemente, por transformações que se relacionam com as exigências sociais de cada época e transcendeu a esfera da natureza fronteiriça do Estado.

Assim, pode-se afirmar que sua concepção evoluiu, sobremaneira, que saiu da seara estritamente político-estadual e colocou o ser humano como seu principal destinatário e objetivo, falando-se hodiernamente em Segurança Humana, conceito

[1] FELLMETH, A. X.; HORWITZ, M.**- Guide to Latin in International Law.** p. 158 (tradução própria)
[2] GUEDES, A. M. - Segurança Externa. In: AAVV, **Enciclopédia de Direito e Segurança**. p. 41

introduzido em 1994, através do Programa de Desenvolvimento das Nações Unidas (PNUD)[3].

1.2- O surgimento do conceito da segurança humana e suas potenciais extensões

A chamada segurança humana trata de um conceito holístico que ultrapassa o pensamento belicista ligado às tendências que atrofiavam a concepção clássica de Estado, compreendendo que, para além da ausência de conflitos, dever-se-iam valorar os direitos humanos e a proteção dos indivíduos.

Está diretamente atrelada ao processo de globalização e ligada aos direitos humanos, à dignidade humana e à proteção das liberdades essenciais das pessoas, de modo a ampliar suas escolhas e oportunidades e prever sua participação nas decisões que venham a afetar suas vidas, ao tempo que exige uma postura proativa de não discriminação, não importando qual seja sua religião, seu gênero ou sua origem étnica.[4]

Esse alargamento subjetivo acompanha as novas formas de evolução da sociedade, sendo esse um conceito integrador e humanocêntrico que visa uma vida digna e plena para todos ao nível ambiental, industrial e perante os novos riscos tecnológicos[5] e, para além dessas hipóteses, poder-se-iam citar ainda outras tipologias de dimensões como a segurança alimentar, comunitária e política[6].

Contudo, esse rol não é taxativo e vem sendo constantemente alargado podendo, hodiernamente, ser incluído em seu conceito a segurança humana no âmbito tecnológico e informacional e por que não considerá-la no âmbito da governança de dados e da proteção dos dados pessoais?

Amaro[7] ainda defende que a segurança humana envolve outras dimensões do ser humano, visando não apenas a proteção, como também a prevenção das pessoas em

[3] GOUVEIA, J. B. - **Direito da segurança**
[4] United Nations Development Programme (UNDP). **Human Development Report**. (tradução própria)
[5] AMARO, A. - Segurança humana e protecção civil na sociedade do risco. In: ***Territorium:*** **Revista Portuguesa de riscos, prevenção e segurança**
[6] GOUVEIA, J. B. – ***op. cit.***
[7] AMARO, A. - ***op. cit.***

situação de vulnerabilidade. Nesse ponto, o conceito da segurança humana agrega-se na sociedade de risco[8].

1. 3 - Sociedade de risco

Como dito alhures, a sociedade evoluiu e, acompanhando essas alterações, evoluíram os riscos, principalmente aqueles oriundos do influxo da globalização.

Considerável parcela dos riscos atuais fugiu ao controle dos convencionais modelos institucionais conhecidos do Estado, que se viu incapaz de regulá-los satisfatoriamente, sobretudo aqueles que detinham características espaciais e temporais que ultrapassam fronteiras geopolíticas nacionais[9], sendo imperiosa a adequação à nova realidade da sociedade atual, caracterizada pela evolução da violência, pelo aumento da criminalidade cada vez mais sofisticada e pelo impacto da ciência e da tecnologia.

Hodiernamente, "mais do que inimigos, os países atuais enfrentam riscos e perigos"[10], com potencial de atingir todas as partes do planeta e impactar diversas pessoas forma indiscriminada, o que se amolda perfeitamente ao conceito de Ulrick Beck de "sociedade de risco"[11].

Os tempos vividos se mostram cada vez mais incertos e imprevisíveis, gerando insegurança e medo a nível individual e sistêmico, haja vista que "o risco é ubíquo a toda a sociedade" e frequentemente é "associado ao perigo e à vulnerabilidade, sendo, por isso, transversal a quase todos os sectores da nossa vida"[12].

Além disso, calha ressaltar que a industrialização, latente nessa nova sociedade, culminou numa eclosão transformativa, trazendo modernização e impactando o globo como um todo, nomeadamente através do despontamento científico e das novas tecnologias, o que acarretou, inclusive, no surgimento de novas gerações de direitos fundamentais considerados pós-modernos, dos quais se destaca "os desafios do progresso tecnológico"[13].

---

[8] MENDES, 2007, *apud* AMARO, A. *Ibid.* p. 85
[9] BECK, U.; GIDDENS, A; LASCH, S. - **Modernização reflexiva**
[10] GIDDENS, A. - **O Mundo na Era da Globalização**. p. 28
[11] BECK, U. - **Sociedade de risco**
[12] DUARTE, F. P. - Sociedade de risco. In: AAVV, **Enciclopédia de direito e segurança.** p.451
[13] GOUVEIA, J. B. - ***op cit.*** p. 47

A despeito do entusiasmo e alvoroço gerados, tal evolução não veio isenta de riscos ou preocupações. E assim, ainda que pareça paradoxal, a ciência e a tecnologia, concomitantemente, podem proporcionar à sociedade infortúnios e benefícios, trazendo riscos e consequências que são desconhecidos e imensuráveis, razão pela qual as decisões tomadas nesse âmbito devem ser pautadas tendo por base o potencial impacto coletivo que poderão causar, tornando a todos participantes e corresponsáveis pelos seus desdobramentos. Indubitavelmente, é um maiores desafios enfrentados atualmente pela humanidade.

1.4 - As quatro Revoluções Industriais

As profundas mudanças sociais, culturais, políticas, científicas e tecnológicas tem um dos marcos nas chamadas Revoluções Industriais, as quais, através do surgimento de novas tecnologias, transformaram intensamente o modo de produzir e, via de consequência, a indústria e a economia.

Fazendo uma breve digressão do processo histórico que envolve tais eventos, tem-se que a Primeira Revolução Industrial iniciou-se na Inglaterra e foi um período marcado pelo emblemático uso das máquinas que usavam água e energia a vapor em substituição à produção artesanal, perdurando aproximadamente entre os séculos XVIII e XIX (1760-1860)[14].

Logo após e durando até 1900, inicia-se a Segunda Revolução Industrial, com expansão para a Alemanha, França, Rússia e Itália. Foi no decorrer dessa fase que Thomas Edison descobriu a eletricidade, acarretando um impressionante avanço na produção industrial e fabril. Ademais, esse período é marcado pela introdução da utilização de derivados do petróleo nos processos de industrialização e também pela chamada filosofia "fordista", representada pelas inovadoras e eficientes linhas de montagem, cujo lema era produzir mais em menos tempo e com menos custos[15].

Em meados do século XX, inicia-se a Terceira Revolução Industrial, retratada pelo avanço tecnológico e científico decorrente da corrida armamentista da

[14] SOUZA, E. RR. - **Entenda Sobre Indústria 4.0**
[15] *Ibid.*

Segunda Guerra Mundial e da Guerra Fria, chamada de "Revolução técnico-cientifica"[16]. Nesse momento, surgiram os computadores, as Tecnologias da Informação e Comunicação (TIC) e o protótipo da internet atual, a ARPANET.

O mundo do século XXI vive a Quarta Revolução Industrial, também chamada de Indústria 4.0 que, nas palavras de Klaus Schwab, tem como base (porém não podendo ser considerada como uma extensão) o conjunto de tecnologias disponibilizados ao longo da revolução anterior, sendo amplamente caracterizada pela convergência das inovações digitais, físicas e biológicas[17] e tendo na tecnologia sua grande protagonista, máxime, aquelas disruptivas, como a Inteligência Artificial, o *Big Data*, a nanotecnologia, a *Internet* das Coisas e a robótica e pela sinergia entre elas[18].

1.5 - Surgimento da Internet

Não é recente o desejo humano de elevar os domínios da comunicação a patamares cada vez maiores. Após a invenção da telegrafia por Samuel Finley Breese Morse, entre os anos de 1843 e 1844[19], o homem sentiu-se inspirado a alargar o âmbito da comunicação e assim surgiu a ideia de que seria possível que cabos fossem capazes de cruzar longas distâncias. Dessa noção, desenvolveram-se vários projetos e trabalhos até se chegar, com êxito, na primeira transmissão transatlântica de telégrafo em 1866, quando os cabos começaram a ser espalhados pelo mundo chegando até o Oriente. Em 1876 houve a invenção do telefone analógico por Graham Bell e, em 1956, o lançamento do primeiro cabo transatlântico de telefone.

Nesse interstício, na década de 1960, surge o embrião da internet, nomeada ARPANET (*Advanced Research Projects Agency Network*), rede fechada que servia para o uso exclusivo do serviço militar dos Estados Unidos na época da Guerra Fria que, pela altura de 1983, foi dividida em duas redes diferentes: a ARPANET e a MILNET, a primeira foi

[16] *Ibid*. p. 11
[17] SCHWAB, K. - **The Fourth Industrial Revolution** (tradução própria)
[18] NOVAIS, P.; FREITAS, P. M. - Inteligência Artificial e Regulação de Algoritmos. In: **Diálogos União Europeia-Brasil**
[19] MABEE, C. - **Samuel F.B. Morse** (tradução própria)

reservada ao uso civil e a segunda para uso militar[20], ambas conectadas, de modo que os seus usuários poderiam trocar informações, surgindo então a *Internet*.

Após um longo percurso evolutivo, toda essa rede de cabos migrou para a telefonia e a partir de 1988 os cabos passaram a ser produzidos com a tecnologia da fibra ótica, o que elevou de forma drástica sua capacidade de transmissão de dados[21]. Esse valioso conjunto de cabos submarinos cruza o planeta neste momento, levando desde simples mensagens trocadas entre cidadãos comuns em redes sociais até informações diplomáticas classificadas.

Destarte, a rede alcançou praticamente todos os pontos do Terra, tornando a largura de banda necessária para suportar a *World Wide Web*[22] e, posteriormente, a *Internet* tal como é conhecida em seu estágio contemporâneo.

A popularização da *Internet* criou uma nova era: a digital, podendo ser considerada como a mais impactante revolução tecnológica até o momento vivenciada pela humanidade, modificando o modo de vida e de comunicação da população mundial. Entretanto, ao mesmo passo que essas inovações diminuíram distâncias e aceleraram a troca de informações, também criaram novos tipos de conceitos e conflitos que repercutem tanto no âmbito público quanto no privado.

1.5.1. – O ciberespaço

O advento da *Internet* também alterou a noção de espaço, haja vista que sua extensão ultrapassa qualquer barreira ou fronteira espacial física de um dado território, o que gerou a necessidade de novas definições peculiares à sua condição, tal como a concepção do ciberespaço e da cibersegurança.

[20] SIQUEIRA, A. C. de M. - Big Data e justiça criminal. In: **Direito Digital**
[21] GUEDES, A. M. - Em rede. Os cabos de fibras ópticas submarinas e a centralidade portuguesa crescente num autêntico mar de conectividades. In: **Revista de Marinha**
[22] Desenvolvida no ano de 1991 pelo físico britânico Tim Bernes-Lee, quando a *Internet* que, desde o final dos anos 80 vinha se desenvolvendo em ambiente acadêmico, passou a ser comercializada no âmbito privado, entrando definitivamente nos lares de grande parte dos cidadãos, potencializando a massificação do processo comunicativo em escala global.

Por ciberespaço pode-se compreender como a "metáfora usada para descrever o espaço não físico criado por redes de computadores, nomeadamente pela *Internet*"[23].

Estruturado num complexo de redes que oferecem o suporte tecnológico, esse espaço virtual aterritorial[24] vem ganhando tamanha força em detrimento do plano físico "palpável", no que os estudiosos Guedes e Santos[25] afirmam que o ciberespaço "configura um espaço de visibilidade e presença, onde indivíduos, grupos e Estados interagem, comunicam, simbolizam, lutam e exercem o poder.".

E este complexo cenário moderno cria novos desafios a serem enfrentados, notadamente, na área das ciências jurídicas enquanto baluarte da proteção do indivíduo e reguladora das relações sociais.

1.5.2. - A cibersegurança

Com o alargamento do ciberespaço cresceram também as ameaças e, a par dessa nova realidade, restou claro que a ideia de espaço que se conhecia até momento, estava defasada.

Assim, a segurança em sua forma tradicional teria que se adequar a essa nova realidade imposta pela evolução das modernas tecnologias, surgindo então a noção de cibersegurança que, todavia, não se limita ao âmbito estatal podendo ser vista por duas perspectivas, como ensina Santos[26]:

> independemente de o objeto da cibersegurança ser o Estado, as organizações ou os indivíduos: a segurança do ciberespaço (na aceção física deste como entidade autónoma) e a segurança da componente 'ciber' de um qualquer sistema (segurança do ciberespaço deste sistema).

[23] Conceito extraído do Glossário do Centro Nacional de Cibersegurança de Portugal. Disponível em: https://www.cncs.gov.pt/recursos/glossario/ (consultado em 20/12 2019)
[24] SANTOS, L. - Ciberespaço. In**: Enciclopédia de Direito e Segurança**
[25] GUEDES, A, M; SANTOS, L. -. Breves reflexões sobre Poder e Ciberespaço. In: **Revista de Direito e Segurança**. p. 191
[26] SANTOS, L. - Cibersegurança. In: **Enciclopédia de Direito e Segurança** p. 63.

Desse modo, a cibersegurança pode ser entendida em várias acepções: como um conjunto de ferramentas, medidas de segurança, orientações, abordagens quanto à gestão de riscos, boas práticas, bem como, tecnologias que podem ser usadas para proteger o ciberespaço e os ativos tanto das organizações, quanto de seus usuários[27].

1.6- Impacto das modernas tecnologias

A vertiginosa evolução tecnológica, influenciada sobremaneira pela utilização maciça da *Internet* e pela globalização, alterou significativamente a economia mundial, cada vez mais dependente das novas tecnologias digitais. Não obstante, para além da economia, a tecnologia vem mudando e moldando o estilo de vida e os comportamentos humanos, não havendo margem para qualquer hipótese de retrocesso aos antigos modos de funcionamento social.

Com isso, tem-se testemunhado um novo movimento fenomenológico no qual a "vida real" passa a migrar para a dimensão virtual. Isso ocorre porque a tecnologia criou uma nova ordem social e vem impondo comportamentos sociais aos indivíduos e suas respectivas relações interpessoais. E como "onde há sociedade, há Direito" é imperiosa a criação de novas orientações jurídico-normativas pata tutelar essas relações.

O atual cenário vivido a partir do ano de 2020, em decorrência da pandemia da COVID-19[28], corrobora com veemência a assertiva anterior, mormente considerando que houve a inauguração de uma nova era na qual o mundo nunca foi tão virtual.

Em larga escala, o trabalho presencial tornou-se remoto; a rotina escolar adaptou-se às aulas on-line; as consultas médicas foram substituídas pela telemedicina; a transmissão da desinformação se alastrou galopantemente pelos aplicativos de mensagens; e o número de vazamento de dados pessoais aumentou. Da análise dessas dinâmicas,

[27] Conforme o Instituto da Defesa Nacional, no caderno nº 12, intitulado **"Estratégia da Informação e Segurança no Ciberespaço"**

[28] Conforme o sítio oficial da Organização Mundial da Saúde, "COVID-19 é a doença infecciosa causada pelo recém descoberto coronavírus. Este novo vírus e doença eram desconhecidos antes do início do surto em Wuhan, na China, em dezembro de 2019". Disponível em: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/q-a-coronaviruses (consultado em 04/01 2021) (tradução própria)

percebe-se que sociedade e a *Internet* passaram a ser facetas de uma mesma moeda, deixando de existir a divisão do 'eu virtual' e do 'eu real'[29].

Até o momento, mais do que em qualquer outra época da existência humana, as máquinas têm tido um protagonismo exponencial. Sem essas criaturas de metal, o mundo teria parado completamente.

Nesse diapasão, fica fácil compreender porque o estudo do impacto das modernas tecnologias na sociedade contemporânea exige uma abordagem holística acerca de seus diversos campos de aplicação e como esse aparato digital tem influenciado e modificado os comportamentos humanos.

1.7 - A crescente interação homem-máquina e a flexibilização da visão antropocêntrica

O antropocentrismo coloca o homem como centro ou medida de todo o universo, considerando-o "a referência máxima e absoluta de valores"[30]. Nesse sentido, nota-se que a própria filosofia da *segurança humana*, mencionada anteriormente, baseia-se nos ideários antropocêntricos, conquanto toma o ser humano como objeto central das preocupações estatais.

No entanto, não é surpresa para ninguém que a tecnologia está afetando a interação homem/máquina, ao tempo que vem diluindo a fronteira entre esses dois "sujeitos", denotando uma tendência à flexibilização do antropocentrismo, mormente quando se vislumbra que o homem passa a confiar às máquinas a atribuição de tomar importantes decisões que poderão impactar de forma significativa sua vida.

A dependência digital do homem pós-orgânico[31] aumenta essa simbiose, quando esses dispositivos passam a funcionar como se fossem uma extensão da própria personalidade humana, que delega a esses objetos tarefas e confia-lhes responsabilidades por seus compromissos, organização, memória e até segredos íntimos e decisões, denotando uma fé, quase cega, na tecnologia.

E assim, em certos domínios:

[29] SIQUEIRA. A. C. de M. – ***op. cit***. p. 84
[30] MILARÉ, E. - **Direito do ambiente**. p. 113
[31] SIBILIA, P. - **O homem pós-orgânico**

> [a] interacção social passa a ser profundamente transformada pela presença massiva de agentes não-humanos, mecânicos, que aparecem à interacção de tal modo que os agentes humanos envolvidos não têm meios para distinguira acção dos humanos da acção das máquinas[32]

Reforçando o explicitado, Magrani[33] cita ainda em sua obra "Entre dados e robôs" o entendimento do docente da Universidade Federal da Bahia, Marco Aurélio Castro Júnior, que reconhece não apenas a possibilidade de uma flexibilização do antropocentrismo, mas a sua queda, ante o avanço tecnológico, o qual permitirá, inclusive, a criação de "coisas potencialmente mais inteligentes que os humanos".

Registre-se ainda que o homem tem-se permitido estar tão à mercê das inovações que, não por outro motivo, já se fala da obsolescência humana, o que inclusive tem levado cientistas a estudar "melhorias" cognitivas e físicas em seres humanos, como forma de reduzir suas limitações, na prática nomeada de *human augmentation*[34].

Essa sinergia do homem com máquinas cada vez mais autônomas é um grande desafio a ser enfrentado pelo Direito que precisa ser capaz de regulamentar de forma eficaz a matéria no campo da ética e da proteção dos titulares dos dados disponibilizados para que a interação ocorra.

O Direito atual apesar de, ainda ser antropocêntrico e de matriz iluminista[35], deve estar preparado quando confrontado por temáticas vanguardistas, a exemplo do constante fluxo da evolução digital. Destarte, competem ao legislador e ao operador do Direito sopesar que novos problemas exigem estratégias inovadoras que destoam das clássicas abordagens regulatórias, visando assegurar que os avanços disruptivos da tecnologia não se sobreponham aos direitos humanos, buscando o equilíbrio entre a fluidez da tecnologia e a morosidade da burocracia jurídico-normativa.

Como exemplos da crescente automatização das diversas atividades, até então humanas, destacam-se como vantagens o aumento da eficiência e produtividade, a teórica *redução* de erro humano e a diminuição de custos; e como desvantagens, decisões

[32] SILVA, P. - Sociedades artificiais. In: **Fórum de Proteção de Dados**. p.16
[33] MAGRANI, E. – **Entre dados e robôs**. p. 60
[34] Nybø, E. F. - **O poder dos algoritmos**. p. 15-16
[35] MAGRANI, E.; SILVA P.; VIOLA R. - Novas perspectivas sobre ética e responsabilidade de inteligência artificial. In: **Inteligência Artificial e Direito**

enviesadas, erradas e imprecisas, suscetíveis de causar impactos nos direitos e liberdades das pessoas e até mesmo a desumanização das relações interpessoais, quando o indivíduo perde a capacidade de dissociar o homem da máquina.

Capítulo II – BREVES APONTAMENTOS SOBRE A PRIVACIDADE E PROTECAO DE DADOS PESSOAIS

2.1 – Da ressignificação da privacidade

Neste capítulo será realizada uma breve explanação acerca da evolução histórica e conceitos referentes aos direitos à privacidade e à proteção de dados pessoais.

Conceituar o termo "privacidade" não é uma tarefa fácil, ante a panóplia de sentidos que o mesmo pode adquirir, decorrente da pluralidade de interesses que englobam essa expressão. Trata-se, pois, de "um conceito em desordem"[36], pouco claro, permeado de subjetividades e geralmente ligados à ideia de família, vida doméstica, imagem, sigilo das correspondências, reputação e honra, de forma que para ser tutelado o operador do Direito deverá sempre valer-se do critério da ponderação de interesses.

A palavra privacidade tem suas origens na Antiguidade Clássica, notadamente, nos conhecidos discursos de Aristóteles[37] (385-323 AC), quando o filósofo diferenciou a esfera pública, a *polis*, associada à atividade política; da esfera privada, *oikos*, relacionada ao núcleo familiar.

Devido à própria dinâmica econômica, política e social o conceito de privacidade foi redefinido e ultrapassou a esfera filosófica, sendo que no final do século XIX, mais especificamente no ano de 1890, foi publicado na *Havard Law Review* o célebre estudo jurídico sobre a matéria, intitulado *The Right to Privacy*, em português "O Direito à Privacidade". Esse artigo, escrito por dois advogados americanos, Samuel D. Warren e Louis Brandeis, consagrou o direito à privacidade sob a perspectiva de uma liberdade negativa como o direito de ser deixado sozinho (*right to be let alone*).

Nesse ensaio, considerado o ponto de partida dos debates doutrinários sobre o tema, os autores abordaram a forma como as mutações sociais em conjunto com o surgimento de invenções tecnológicas modernísimas para a época, como as câmeras fotográficas portáteis, a massificação dos jornais e a ascensão da imprensa sensacionalista[38], impactaram a vida privada dos cidadãos. E diante desse cenário os autores buscavam

[36] SOLOVE, D. J. - **Understanding privacy.** p. 1 (tradução própria)
[37] ARISTÓTELES. **Política**
[38] LEONARDI, M. - **Tutela e privacidade na Internet.** p. 52

explicar se havia mecanismos jurídicos aptos a proteger a privacidade dos indivíduos e, caso existissem, qual seria a natureza e a extensão dessa proteção.

A conclusão de Warren e Brandeis, a partir da análise de precedentes das cortes inglesas, é que o direito à privacidade pode ser construído na *Common Law*, e que sua essência seria a inviolabilidade da personalidade, e não a propriedade privada; e seu valor consistiria na paz de espírito ou no alívio por impedir a própria publicação, e não no direito de receber indenização em decorrência dessa publicação[39], ressaltando ainda que esse direito cessaria caso o próprio indivíduo fornecesse deliberadamente essas informações ou consentisse para tal.

Ultrapassando essa conceituação inicial, no tocante a alguns dos relevantes documentos internacionais que se debruçaram sobre o direito à privacidade no decorrer do século XX, tem-se que o cenário pós-Segunda Guerra Mundial, para além dos óbvios e nefastos abusos contra os direitos humanos, propiciou a ocorrência de diversas violações à privacidade dos cidadãos, o que levou a Organização das Nações Unidas (ONU) a proclamar em 1948, a Declaração Universal dos Direitos do Homem, que em seu artigo 12 consagraram o direito à privacidade.

Após, outros documentos de cunho internacional também reafirmaram a relevância do direito à privacidade, dos quais se destacam a Convenção Europeia dos Direitos Humanos, de 1953; o Pacto Internacional relativo aos direitos civis e políticos, ONU, de 1966; a Convenção Americana sobre os Direitos do Homem, também conhecida como Pacto de São José, Costa Rica, de 1969.

Também fora plasmada na Convenção 108 de 1981, considerada a gênese da limitação dos tratamentos automatizados, por reconhecer a necessidade de salvaguarda do direito à proteção de dados pessoais. De igual modo, não se pode olvidar da Carta Dos Direitos Fundamentais Da União Europeia.

Para além dos diplomas internacionais mencionados, o direito à privacidade assume uma posição tão elevada que se encontra positivado como direito fundamental ao longo de Constituições de diversos países ao redor do mundo[40][41].

---

[39] *Ibid.* p. 53
[40] SOLOVE, D. J. – ***op. cit.***
[41] Consoante CARVALHO "o direito à privacidade é um direito fundamental, tanto no Brasil, como em Portugal, essencial para o desenvolvimento da personalidade individual de cada pessoa. (**Vigilância das forças de segurança através de câmeras de reconhecimento facial e o conflito com o direito à privacidade – Brasil e Portugal.** p. 2)

Apenas para fins explicativos, em síntese, leciona a mais abalizada doutrina, na pessoa de Canotilho, que os direitos fundamentais, num plano objetivo, constituem normas de competência negativa para os poderes públicos, proibindo ingerências destes na esfera jurídica individual; e na vertente subjetiva seria a liberdade positiva de exercer os direitos fundamentais e exigir omissões dos poderes públicos, visando evitar agressões lesivas por parte dos mesmos, ao que refere como liberdade negativa[42].

É dizer, o direito à privacidade está associado à reserva da vida privada e da intimidade, ambos umbilicalmente vinculados ao princípio da dignidade humana[43].

2.2 – Da proteção de dados pessoais

A evolução da sociedade, sobretudo após a Segunda Grande Guerra Mundial, aliada com o advento dos computadores e a ubiquidade da tecnologia, revelou os problemas decorrentes dessas inovações, tais como aqueles que afetavam significativamente a privacidade dos indivíduos.

O século XX foi um divisor de águas para a privacidade quanto ao seu desdobramento em outras dimensões, tendo em vista que restava cada vez mais latente a necessidade de sua modernização, de modo a fazer frente aos desafios trazidos pela introjeção da tecnologia. Foi nesse cenário que se estruturou o direito à proteção de dados pessoais.

Hodiernamente, o uso excessivo dos meios de comunicação e das redes sociais, nas quais os indivíduos estão expostos (ativa ou passivamente) em sua mais profunda intimidade, propiciando a difusão de toda sorte de dados (pessoais ou não), criou o ambiente

[42] CANOTILHO, G. - **Direito Constitucional e Teoria da Constituição**. p. 407.
[43] BAHIA explica que "A carga axiológica que lastreia o vértice dos direitos humanos ou dos direitos fundamentais é a mesma, é o centro dos direitos mais valiosos que nós temos. A vida, a liberdade, a propriedade, a segurança e a igualdade, com todos os seus desdobramentos, encontram-se protegidas por ambas as expressões, entretanto, a denominação 'direitos humanos' é utilizada pela Filosofia do Direito e ainda pelo Direito Internacional Público e Privado. Já os "direitos fundamentais" seriam os direitos humanos positivados em um sistema constitucional. Os direitos humanos, sob a análise do Direito Constitucional, podem ser denominados de direitos fundamentais. A título de exemplo, o Título li da Constituição de 1988 se refere aos 'direitos e garantias fundamentais' (tutelados pelo constituinte brasileiro), enquanto o art. 5°, § 3°, que trata da constitucionalização dos tratados, refere-se aos tratados sobre direitos humanos, fazendo referência aos documentos internacionais, dos quais o Brasil é signatário perante a comunidade jurídica internacional."

perfeito para uma alteração substancial de perspectiva do que seria vida privada e vida pública.

Essas mudanças acabaram por transmutar o sentido originalmente definido para a privacidade. Atualmente, esta pode ser delineada como "o direito de manter o controle sobre o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular"[44]. Em outras palavras, a privacidade passou a consistir numa autodeterminação informativa, que é a autonomia que cada pessoa tem de controlar suas informações pessoais e aquilo que deseja que se torne disponível aos outros.

Nesse ponto, avista-se a quebra do paradigma da privacidade vista como uma liberdade negativa (direito de ser deixado só) para ser atrelada a uma liberdade positiva, consubstanciada no controle efetivo dos dados pessoais "e um pressuposto para qualquer regime democrático"[45]

Dessa forma, a proteção de dados pessoais seria uma derivação da privacidade e, no momento presente, as duas coexistem em harmonia e devem ser devidamente tuteladas. Ambos os direitos teriam como fundamentos a tutela da personalidade e a dignidade da pessoa[46]. Além disso, cabe frisar que o direito à proteção de dados pessoais transcende o interesse individual, revestindo-se de um caráter mais coletivo[47].

Também é de fácil intelecção perceber que a proteção dos dados pessoais acaba por refletir na proteção da pessoa a qual esses se referem. Ora, os dados pessoais, como se extrai da literalidade do próprio termo, referem-se a informações acerca de um indivíduo específico, o que indica que são intrinsecamente ligados a uma pessoa determinada, daí a relevância de resguardá-los, tendo em vista que o processamento desses dados pode gerar uma discriminação ou mesmo perpetuar um estigma social.

Assim, o cenário de massificação de recolha de dados pessoais, notadamente, pelo alastramento das fontes de captação que forma o *big data*, entendido como o conteúdo em massa dos dados coletados, pode ameaçar os titulares, ou seja, os donos desses dados. À vista disso, o desiderato do debate sobre privacidade e proteção de dados pessoais é assegurar os direitos fundamentais e trazer segurança jurídica para os indivíduos,

[44] RODOTÀ, S. - **A vida na sociedade da vigilância**. p. 15
[45] MENDES, L. S. - **Privacidade, proteção de dados e defesa do consumidor**. p 29
[46] *Ibid.* p. 35
[47] DONEDA, D. - **Da privacidade à proteção de dados pessoais**

além de buscar viabilizar novos modelos de negócios e políticas públicas, dependentes desse tratamento[48].

2.2.1 – Instrumentos internacionais relevantes

O avanço da tecnologia obrigou os sistemas a se adaptarem, inclusive, os sistemas jurídicos, que devem ser capazes de fazer frente aos novos desafios e exigências da sociedade.

Apenas para citar alguns exemplos considerados relevantes para esta obra, como marco regulatório tem-se a lei de proteção de dados pessoais do Estado Alemão de Hesse, a *Datenshutz*, promulgada em 07 de abril de 1970 e considerada pioneira nesse assunto[49].

A partir da década de 1980 houve a adoção de outros instrumentos internacionais sobre o processamento de dados como, em 1980, as Diretrizes da OCDE (Organização para a Cooperação e Desenvolvimento Econômico) para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais, revisada e atualizada em 2013, versando sobre princípios básicos que devem nortear as já existentes e as novas legislações domésticas[50].

A Convenção 108, de 1981, que, por conta da entrada em vigor do Regulamento Geral sobre a Proteção de Dados foi modernizada, de modo a fazer frente aos novos desafios da tecnologia e, em 2018 e ficou conhecida como 108+, foi o primeiro instrumento internacional vinculante para os Estados signatários no domínio referente à proteção de dados pessoais, sobretudo visando evitar abusos que possam ocorrer no processamento de dados pessoais.

Em 2000, a Carta de Direitos Fundamentais da União Europeia reconheceu em seu Art. 7.º e 8.º a autonomia do direito a proteção de dados pessoais[51].

---

[48] GRUPO DE ENSINO E PESQUISA EM INOVAÇÃO. **Um Novo Mundo de Dados**. p 7

[49] DONEDA, D. Panorama histórico da proteção de dados pessoais. In: **Tratado de proteção de dados pessoais.** p. 21-40

[50] MENDES, L. S; FONSECA, G. C. S. da - Proteção de Dados para além do consentimento. In: **Tratado de Proteção de Dados Pessoais**

[51] Stefano Rodotà afirma que a Carta não somente considerou o direito à proteção de dados como um direito fundamental autônomo, como o tornou uma importante ferramenta para o livre desenvolvimento da personalidade

O Tratado de Lisboa, que entrou em vigor em dezembro de 2009, também se debruçou acerca da temática da proteção de dados pessoais, no artigo 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE) e no artigo 39.º do Tratado da União Europeia (TUE). Calha registrar que o Tratado de Lisboa consagrou a Carta dos Direitos Fundamentais da UE, acima mencionada, com valor jurídico vinculativo.

Adicionalmente, é válido mencionar que na ordem constitucional portuguesa a proteção de dados é um direito positivado desde 1976, tendo a Constituição da República Portuguesa feito referência ao mesmo em seu artigo 35º.

2.2.2 – Diretiva 95/46/CE

Diante da crescente monetização dos dados pessoais que trafegam no mundo virtual, considerados a nova espécie de moeda da economia, mostrou-se de crucial importância o uso e gerenciamento ético dos dados, o que levou a União Europeia a vislumbrar a necessidade de adotar um ato que: acompanhasse essas mudanças; fosse eficaz para proteger os dados dos titulares da rede; e harmonizasse o conjunto das leis nacionais já existentes e em vigor sobre a matéria em vários Estados-Membros da UE.

Assim, foi publicada a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995 (Diretiva Europeia de Proteção de Dados), "relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados".

A adoção da Diretiva visava estabelecer um regime geral, harmônico e uniforme que assegurasse um alto nível de proteção de dados no âmbito da União Europeia que, para além de fomentar o livre fluxo desses dados reforçando o mercado único[52], estabelecesse critérios quanto ao processamento dos dados pessoais.

Mister frisar que seu ponto fulcral era a proteção do indivíduo, permitindo que o mesmo fornecesse seu consentimento e fosse informando sobre o processamento de dados pessoais, sobretudo, quando se tratasse de dados sensíveis.

[52] Conforme disposto nos Considerandos 3, 5 e 7, da mencionada diretiva.

A despeito de ter estabelecido padrões mínimos de privacidade e segurança de dados, constatou-se o insucesso da Diretiva ante a falta da uniformização que a levou a uma desadequação funcional. Isso ocorreu no momento das respectivas transposições da Diretiva para a ordem jurídica interna dos Estados-Membros, posto que a margem de discricionariedade então permitida acarretou numa implementação relativamente diversificada pelos Estados-Membros, gerando uma espécie de mosaico de legislações de proteção de dados, dificultando a efetiva observância da mesma. Por esse motivo, foi necessário refletir sobre um instrumento jurídico hábil que pudesse suprir essas lacunas.

2.2.3 – Regulamento Geral sobre a Proteção de Dados

As fragmentações observadas nas transposições da Diretiva 95/46/CE exigiram uma avaliação apurada quanto ao instrumento a ser escolhido no lugar daquela. Nesse sentido, com o objetivo de redução dessas assimetrias foi adotado o Regulamento, que se consubstancia num instrumento de caráter geral, obrigatório em todos os seus elementos e diretamente aplicável a todos os Estados-Membros[53], sendo a solução perfeita para o caso posto, de modo a evitar as disparidades da margem de manobra conferida aos Estados-Membros no momento da transposição, promovendo a harmonização pretendida e trazendo maior segurança jurídica

Aprovado em 2016 pelo Parlamento Europeu e pelo Conselho, o Regulamento (UE) 2016/679, de 27 de abril, conhecido como Regulamento Geral sobre a Proteção de Dados, doravante referido como RGPD, entrou em vigor no mesmo ano, porém, tornou-se aplicável a partir de 25 de maio de 2018 e é tido como a mais importante legislação sobre a proteção de dados pessoais da atualidade, sendo ainda referida por alguns como a lei de privacidade e segurança mais rígida do mundo[54].

Deveras a relevância e impacto do Regulamento é que este ostenta uma característica extraterritorial, podendo ser aplicável para além do território da União, conforme explicita o art. 3.º do RGPD, inclusive, para impor obrigações, dentro do seu escopo legal, a organizações de outros países.

[53] Conforme artigo 288.º do TFUE
[54] WOLFORD, B. - **What is the GDPR, the EU's new data protection law?**

Assim como na Diretiva anterior, o ser humano está no centro de toda essa tutela e o foco do regulamento é a salvaguarda dos direitos e garantias fundamentais das pessoas singulares[55], em relação ao controle do tratamento de seus dados pessoais.

O RGPD assegura aos cidadãos uma gama de direitos como o direito à informação sobre o processamento de seus dados pessoais, o direito de correção de dados incorretos, incompletos ou inexatos, o direito de objeção ao processamento automatizado, o direito à explicação dessas decisões, o direito à intervenção humana nesse contexto, dentre outros. É um exemplo de modelo a ser seguido pelos legisladores brasileiros, ante seu estágio mais avançado de vigência e os bons resultados observados desde a sua entrada em vigor.

2.2.4 – Diretiva (UE) 2016/680

Juntamente com o RGPD foram aprovadas e publicadas a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no tratamento de dados pessoais pelas autoridades competentes nos contextos a seguir determinados; e a Diretiva (UE) 2016/681, que dispõe sobre dados de identificação de passageiros para efeitos de prevenção, detecção, investigação e repressão das infrações terroristas e da criminalidade grave.

Para efeitos desta pesquisa, haverá apenas a análise da existência do direito à explicação no seio da Diretiva (UE) 2016/680. Esta, revoga a Decisão-Quadro 2008/977/JAI do Conselho e aborda, especificamente, o tratamento de dados pessoais realizado por autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, com a finalidade de proteger os direitos e as liberdades fundamentais das pessoas naturais.

A intenção desse diploma é assegurar um elevado nível de proteção de dados das pessoais singulares, resguardando seus direitos e liberdades fundamentais e, ao mesmo tempo, garantindo o intercâmbio de dados pessoais entre autoridades competentes da União e dos Estados-Membros, nos casos previstos (Cf. art. 1.º, n.º 2, alíneas a e b).

[55] No presente trabalho acadêmico os termos pessoas singulares e pessoas naturais serão abordados como sinônimos. Ambos tratam dos destinatários das normas de proteção de dados pessoais, sendo que o RGPD, na versão em português de Portugal, utiliza a primeira terminologia e a Lei Brasileira, a segunda.

A adoção da Diretiva como instrumento regulatório encontra lógica na ideia de que cada Estado-Membro possa dispor, com certa discricionariedade em pontos específicos no âmbito das suas particularidades em matéria de Direito Penal e Direito Processual Penal interno, de modo a não afetar sua soberania numa perspectiva política, judicial e policial e técnica[56].

Ademais, a Diretiva não obsta que os Estados-Membros prevejam garantias mais elevadas do que as nela estabelecidas para a proteção dos direitos e liberdades do titular, no que diz respeito ao tratamento de seus dados pessoais pelas autoridades competentes.

2.2.5- Lei Geral de Proteção de Dados

No tocante ao panorama brasileiro, este era composto por leis esparsas e setoriais sobre o assunto, de modo que se exigia uma leitura sistemática de normas como a Lei do *Habeas Data* (Lei n.º 9.507/1997); artigos 20 e 21, do Código Civil Brasileiro (Lei n.º 10.406/2002); artigo 43 do Código de Defesa do Consumidor (Lei n.º 8.078/ 90); o Marco Civil da Internet (Lei n.º 12.965/2014); a Lei de Acesso à Informação Pública (Lei n.º 12.527/ 2011); e a Lei do Cadastro Positivo (Lei n.º 12.414/2011), que, contudo, não ofereciam grau um satisfatório de segurança jurídica aos titulares de dados pessoais.

Atualmente, o Brasil vem avançando e amadurecendo na área da proteção de dados e em 2020 entrou em vigor a Lei nº 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados Brasileira (LGPD). Assim, ainda que com considerável atraso, o Brasil passou a ter um novo marco regulatório, sendo o 127º país a ter, oficialmente, uma legislação sobre proteção de dados pessoais[57].

Importante ressaltar que, apesar de ainda não ser um direito positivado na Constituição Federal Brasileira, existe uma Proposta de Emenda à Constituição (PEC n.º 17/2019), que tramita na Casa Legislativa Brasileira para acrescentar o inciso XII-A, ao art.

[56] No caso de Portugal, a Diretiva (UE) 2016/680 foi transposta pela Lei nº 59/19 que, conforme descrição do seu sumário: "Aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016". Dessa forma, os objetivos da mencionada diretiva passam a ser cumpridos em Portugal através da referida lei.
[57] Abrusio, J. **Proteção de dados na cultura do algoritmo**.

5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria[58].

Contudo, isso não impediu o Supremo Tribunal Federal (STF), órgão de cúpula do Poder Judiciário brasileiro, de se antecipar a essa positivação e reconhecer, no julgamento histórico de maio de 2020, o direito fundamental à proteção de dados pessoais na ordem constitucional brasileira, ao julgar as Ações Diretas de Inconstitucionalidade tombadas sob os números 6.387, 6.388, 6.389, 6.390 e 6.393[59]. A decisão referendada suspendeu a eficácia da Medida Provisória nº 954, de 17/4/2020[60].

2.2.6- Anteprojeto da LGPD-Penal

A LGPD excluiu de seu âmbito de aplicação determinados tratamentos de dados pessoais. Essas exceções de incidência estão descritas no art. 4º da mencionada lei sendo "diretamente relacionadas à finalidade do tratamento de dados pessoais dentro de contextos específicos"[61]. Dentre outras hipóteses elencadas, destaca-se aqui o inciso III do artigo, o qual dispõe sobre o tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

Assim, calha asseverar que

> a regra da inaplicabilidade não se dirige a 'quem' realiza o tratamento. Desse modo, ainda que uma autoridade seja competente, por exemplo, para a atividade de investigação criminal, tão somente dentro desse escopo incidirá a exceção da não aplicação da lei. Em contrapartida, tendo em conta que todos os órgãos e entes públicos tratam dados pessoais em

[58] O trâmite da PEC está disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594
[59] As referidas Ações Diretas de Inconstitucionalidade podem ser consultadas através do *link:* http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=462167&ori=1
[60] Conforme se extrai do sítio http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm: "A Medida Provisória nº 954/2020, DE 17 DE ABRIL DE 2020 Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020" (consultado em 17/09 2020)
[61] VIVAS, C. **- LGPD e Poder Público**

> contextos diversos do expresso acima (cujo exemplo mais óbvio refere-se ao tratamento de dados pessoais de seus próprios agentes), remanescerá, para todos os efeitos, a plena incidência da norma [geral][62]

Para dar efetividade ao inciso III do art. 4º, a LGPD apontou que o tratamento de dados pessoais ali narrado deveria ser regido por legislação específica que previsse medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais e os direitos do titular previstos na LGPD.

Diferentemente do que ocorreu no cenário europeu, o legislador brasileiro não entregou, juntamente com a legislação geral, a lei em sede criminal. Nesse sentido, calha dizer que a equivalente brasileira da Diretiva (UE) 2016/680 ainda se encontra em tramitação perante o Congresso Nacional Brasileiro. Ou seja, dito com outras palavras, a regulamentação sobre a matéria no Brasil ainda é inexistente.

De qualquer sorte, convém ressaltar que em 26 de novembro de 2019 foi instituída, através de ato do presidente da Câmara dos Deputados, uma comissão de juristas para elaborar o texto do "Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Investigação Criminal", o qual foi apresentado em 5 de novembro de 2020 sob o apelido de "Anteprojeto da LGPD-Penal", cujo trabalho foi inspirado tanto na LGPD como em dispositivos da Diretiva nº 680/16[63].

Segundo a exposição de motivos constantes no documento do anteprojeto, este se fundamenta:

> Na necessidade prática de que os órgãos responsáveis por atividades de segurança pública e de investigação/repressão criminais detenham segurança jurídica para exercer suas funções com maior eficiência e eficácia – como pela participação em mecanismos de cooperação internacional –, porém sempre de forma compatível com as garantias processuais e os direitos fundamentais dos titulares de dados envolvidos. Trata-se, portanto, de projeto que oferece balizas e parâmetros para operações de tratamento de dados pessoais no âmbito de atividades de segurança pública e de persecução criminal, equilibrando tanto a proteção

[62] *Ibid.*
[63] Tal como expresso nas páginas 2-3 da "Exposição de motivos" do Anteprojeto: "Nessa dimensão, destacam-se pontos deste anteprojeto de confluência com os da supracitada Diretiva, a saber: (i) os registros de atividade de tratamento; (ii) a segurança e o sigilo dos dados; e (iii) a transferência internacional de dados."

> do titular contra mau uso e abusos como acesso de autoridades a todo potencial de ferramentas e plataformas modernas para segurança pública e investigações.

No mais, tendo em vista a abstratividade da norma, que sequer virou um projeto de lei, haverá menções pontuais ao referido documento, apenas naquilo que for útil ao debate proposto. E aqui, reforça-se a necessidade de uma maior celeridade no andamento desse processo legislativo, visando destinar aos titulares a segurança jurídica necessária para privá-los da discriminação, das injustiças e de um eventual uso antiético de seus dados pessoais, inclusive, podendo restringir direitos relevantes como a liberdade individual, gerando efeitos irreparáveis na vida de uma pessoa.

2.2.6.1- Críticas ao anteprojeto

Diversas entidades representativas de categorias da segurança pública nacional[64] manifestaram seu descontentamento com o texto do anteprojeto, chamado pelos mesmos de "nefasto", razão pela qual emitiram um "alerta à sociedade brasileira e aos parlamentares do Congresso Nacional" acerca do suposto retrocesso que a sua aprovação poderia ocasionar ao criar "um ambiente hostil à cooperação com a prevenção e repressão de delitos" (cf. item 5).

A justificativa central da irresignação é que o

> documento possui um conjunto de proposições de normas inviabilizadoras de qualquer trabalho de pesquisa, acessibilidade e apuração desenvolvido por profissionais de segurança pública no Brasil, criando-se até mesmo responsabilidades de natureza civil e disciplinar alheias aos estatutos próprios das corporações, além de dificultar demasiadamente o acesso e

[64] ADEPOL do Brasil – Associação dos Delegados de Polícia do Brasil; Associação Nacional dos Delegados de Polícia Federal – ADPF; Confederação Nacional dos Trabalhadores Policiais Civis – COBRAPOL; Federação Nacional dos Oficiais Militares Estaduais – FENEME; Federação Nacional dos Delegados de Polícia Federal – FENADEPOL; Federação Nacional dos Delegados de Polícia Civil – FENDEPOL. O documento pode ser consultado através do *link*: https://images.jota.info/wp-content/uploads/2020/12/alerta-geral-contra-lgpd-penal-ult.pdf

> uso de bancos de dados em investigações e atividades de segurança pública como um todo. (cf. introdução do documento)

Ademais, os representantes das entidades de segurança pública apontam a existência de "vícios insanáveis de inconstitucionalidade" (cf. item 1), a exemplo da "transformação do Conselho Nacional de Justiça - CNJ em órgão de controle externo de atividades de acesso aos dados pelos profissionais de segurança pública" (cf. item 1), a qual, alegam, não teria atribuição constitucional para a atividade de controle externo das polícias e das forças de segurança pública.

Sustentam também que o texto cria dificuldades para a dinâmica operacional das forças de segurança pública através de burocracias desnecessárias. Além disso, aduzem que o artigo 15, ao vedar o acesso automatizado e massificado a quaisquer documentos, como provas colhidas, peças processuais, laudos periciais e documentos análogos, colide com outros dispositivos já previstos em legislações rigorosas acerca da questão, dentre outras críticas que podem ser lidas no documento.

Capítulo III – DAS DECISÕES AUTOMATIZADAS

3.1 - Inteligência humana *versus* Inteligência Artificial

Tegmark[65] afirma que não existe um consenso acerca da definição de inteligência e a conceitua genericamente como sendo "a capacidade de realizar objetivos complexos". Por esse conceito, poder-se-ia citar a notória inteligência de outras criaturas não humanas, a exemplo de animais capazes de realizar feitos incríveis (como os golfinhos, polvos e chimpanzés) e os computadores.

Ocorre que a inteligência atribuída à máquina é deveras diferente da humana e, por mais impressionante que pareça, a máquina não pensa, ela apenas simula a inteligência humana, ao que se denomina de "Inteligência Artificial" (IA).

Essa expressão foi utilizada pela primeira vez por John McCarthy, no ano de 1956, em uma conferência sobre o tema realizada em Dartmouth, organizado por ele juntamente com Marvin Minsky e foi chamada de *Dartmouth Summer Research Project on Artificial Intelligence* (DSRPAI)[66]

Por inteligência artificial, ou em sua concepção mais técnica, computacional, entende-se a ciência de projetar sistemas "inteligentes" que são capazes de emular o pensamento e raciocínio humanos, correlacionando as informações fornecidas às máquinas com o fito de proceder a tomadas de decisões.

Contudo, ainda que esse conceito, por si só, já seja fascinante, as máquinas são completamente objetivas e não conhecem, ou não conseguem entender, as subjetividades humanas. Um exemplo interessante dessa não compreensão pela máquina é o sentido de "algo quase". O que seria um ônibus (autocarro) "quase" cheio ou um celular (telemóvel) "quase" sem bateria? E ainda que a ideia do "quase" seja relativa, inclusive para as pessoas, parece existir um consenso *quase* universal sobre a extensão desse sentido.

Além disso, esses aparatos também não conhecem, ou ainda que saibam na teoria, não compreendem no âmago de seu "ser" o que é a empatia, o humor, a ironia ou o gosto pela poesia (ou os arrepios que uma declaração de amor podem causar numa pessoa apaixonada), características tão demasiadamente humanas dos seres humanos.

---

[65] TEGMARK, M. - **Life 3.0**, p. 77
[66] SILVA, N. C. - Inteligência Artificial. In: **Inteligência artificial e Direito**

Uma máquina não se aflige por uma injustiça ocorrida, não se sensibiliza com a tristeza de um igual, nem se alegra quando conquista algo especial. Quando o programa *AlphaGo*, desenvolvido pela *DeepMind Technologies*, venceu o jogador profissional Lee Sedol no jogo *Go*, ele não se gabou de seu grande feito bebendo uma cerveja gelada numa roda de amigos.

Contudo, mesmo que ainda exista esse abismo social, emocional e até sentimental entre o modo de "pensar" da máquina e do homem, a verdade é que a evolução tecnológica continua se expandindo e a cada dia surgem tecnologias mais recentes que se valem de poderosos algoritmos e da inteligência artificial. Nos dias atuais, a IA é parte essencial do mercado tecnológico que cria máquinas inteligentes que são capazes de aprender sozinhas ao assimilarem grandes conjuntos de dados introduzidos em seus sistemas.

Assim, um *software* pode programar essas máquinas para que adquiram habilidades para escolher dentre opções predefinidas qual a melhor decisão para determinado caso concreto. E essa "experiência" da máquina gera padrões que vão sendo catalogados em sua memória.

Dessa forma, "[a] todo o momento que as máquinas adquirem mais informações, mais padrões são criados e elas ficam paulatinamente mais *inteligentes*"[67], e por conseguinte, o intelecto já não poderia mais ser considerado como um atributo exclusivamente humano[68], o que leva alguns seguidores da corrente *dataísta* a afirmarem categoricamente que a máquina substituirá o "orgânico" *Homo Sapiens* que se tornará um "algoritmo obsoleto"[69].

Neste ponto, de forma a estabelecer um grau mínimo de conhecimento técnico sobre os conceitos relativos a IA, entende-se que algoritmos, grosso modo, são conjuntos de regras que seguem uma série de passos predefinidos para atingir um objetivo determinado. Tomando por base a definição técnica de Hill[70], algoritmo consiste em "uma estrutura de controle composta, finita, abstrata, eficaz, dada de forma imperativa, cumprindo um determinado propósito sob determinadas disposições.".

---

[67] VETTORAZZI, K. M.; BOTTINI, J. M. - **A lei de proteção de dados e a inteligência artificial**
[68] ČERKAA, P; GRIGIENĖA, J; SIRBIKYTĖB, G. - **Liability for damages caused by artificial intelligence**
[69] HARARI, Y. N. - **Homo Deus**. p. 426
[70] HILL RK, 2015, p. 47, *apud* MITTELSTADT, B. D. [et. al.] - **The ethics of algorithms**, p. 2 (tradução própria)

Monteiro define que algoritmos são "sequências pré-definidas de comandos automatizados que, com base em dados pessoais e não pessoais, chegam a conclusões que podem sujeitar alguém a uma determinada ação, a qual pode ou não ter impacto significativo na sua vida"[71]. Complementando, leciona Abrusio que mais utilizados atualmente são aqueles relativos às técnicas de *machine learning* e *deep learning*[72].

Por *machine learning*, ou aprendizado de máquina, compreende-se a subdivisão da IA formada pelo conjunto de técnicas algorítmicas no qual o sistema, geralmente[73], passa por uma programação inicial, ou seja, é treinada e parametrizada por um humano, com dados rotulados em determinado cenário (*v.g.* na área da medicina para reconhecer células cancerígenas em determinada amostra de tecido humano), porém, é construída de maneira que possa ser capaz de aprender a partir da interação com um ambiente dinâmico e dessa experiência fazer correlações e detectar padrões, de modo a obter um resultado aceitável sobre alguma tarefa ou até mesmo tomar decisões autônomas.

Outra técnica bastante comentada no contexto de IA refere-se ao aprendizado profundo, ou *deep learning* em inglês. É uma subespécie do aprendizado de máquina que funciona através de uma complexa estrutura tecnológica chamada de redes neurais artificiais, formada por redes de camadas interconectadas, similares ao cérebro humano.

Tanto em uma como na outra o que mais surpreende é que, muitas vezes, nem os operadores, nem seus próprios programadores compreendem o modo e a razão de o algoritmo chegar às suas conclusões, podendo trazer alguns resultados não previstos e que não são passíveis de explicabilidade nem mesmo pelos humanos que os desenvolveram.

3.2. -Decisões automatizadas e definições de perfis

Conforme dito, a trajetória disruptiva oriunda dos progressos tecnológicos vem permitindo que os sistemas de IA adquiram a cada dia mais capacidade para gerenciar

[71] MONTEIRO, R. L. - **Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?**
[72] ABRUSIO, J. – ***op. cit.*** p. 88
[73] Diz-se "geralmente" porque há estruturações algorítmicas que aprendem sem que sejam explicitamente programadas para realizar uma dada tarefa.

um número descomunal de dados, criar correlações, observar, aprender, replicar padrões e até realizar previsões.

Tem-se vivenciado a introdução, no cotidiano popular, da automatização dos mais variados processos, incluindo-se decisões tomadas por algoritmos de forma completamente autônoma, sem que haja a *human on the loop*[74], ou seja, um humano participando da operação de tomada decisões que podem produzir efeitos consideráveis na esfera particular das pessoas.

Consoante o Grupo de Trabalho do Artigo 29.º (doravante referido por GT29)[75], nas orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, o uso dessas técnicas tem sido cada vez mais comum, tanto pelo setor privado como pelo setor público, por proporcionarem vantagens como aumento da eficiência e economia de recursos[76]. Contudo, o GT29 alerta para o fato de que a definição de perfis e as decisões automatizadas podem gerar riscos significativos para os direitos e as liberdades dos indivíduos, motivo pelo qual exigem garantias adequadas, sobretudo, considerando que são dotadas de pouca, ou nenhuma, transparência.

Tomando como base a definição extraída do art. 4.º, n.º 4, do Regulamento (cuja conceituação é repetida pelo art. 3.º, n.º 4 da Diretiva (UE) 2016/680[77], por definição de perfis, entende-se como

> qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações;

[74] EDWARDS, L.; VEALE, M. - **Enslaving the Algorithm**. p. 47

[75] Órgão consultivo criado pela Diretiva 95/46/CE e posteriormente substituído pelo Comité Europeu para a Proteção de Dados, desde sua concepção fornece importantes recomendações, ainda que não vinculativas, para uma melhor interpretação acerca dos diplomas sobre o tema da proteção de dados pessoais.

[76] GT29 - **WP251rev.01**, versão em português. p. 5. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (consultado em 29/10 2020)

[77] Registre-se por oportuno que o legislador brasileiro não definiu no corpo do texto legal os conceitos sob análise. Assim, considerando que a LGPD se inspirou no regulamento europeu e ainda não existem regulamentações sobre a matéria editadas pela Autoridade Brasileira (denominada Autoridade Nacional de Proteção de Dados -ANPD), "é possível - com as devidas particularidades entre os diplomas legais, naquilo que eventualmente não for contrário à norma brasileira e valendo-se de cuidados metodológico - socorrer-se de alguns parâmetros interpretativos orientadores da matéria no cenário europeu" (VIVAS, C. – ***op. cit***.)

O GT29 menciona que o termo "qualquer forma de tratamento automatizado" não quer dizer que o tratamento deva ser "exclusivamente" autônomo, de modo que a ocorrência de intervenção humana no bojo do processamento não desnatura o âmbito da definição[78].

A técnica foca em agregar uma grande variedade de fontes dados para analisar características e predições comportamentais sobre uma pessoa ou grupo, tal como corrobora Doneda[79]:

> Esta técnica, conhecida como *profiling*, pode ser aplicada a indivíduos, bem como estendida a grupos. Com ela, os dados pessoais são tratados com o auxílio de métodos estatísticos e de técnicas de inteligência artificial, com o fim de se obter uma "metainformação", que consistiria numa síntese dos hábitos, preferências pessoais e outros registros da vida desta pessoa. O resultado pode ser utilizado para traçar um quadro das tendências de futuras decisões, comportamentos e destino de uma pessoa ou grupo.

Por isso, necessária a análise crítica dessas inferências considerando que "o perfil formado a partir do seu uso da tecnologia torna-se uma representação virtual da pessoa e pode até mesmo ser confundido com ela"[80]. Ademais, categorizar pessoas pode tanto perpetuar estereótipos como engessar a autonomia e tolher a evolução do indivíduo, que fica limitado a escolher entre opções já predeterminadas com base em seu perfil.

Um dos exemplos mais comuns de abuso algorítmico nesse contexto é que, após coletar uma gama de informações sobre os indivíduos, esses algoritmos podem valer-se das mesmas para influenciar e manipular, ainda que de modo imperceptível, as decisões dessa pessoa de acordo com suas próprias preferências. Desse modo, o indivíduo acredita que tomou aquela decisão conscientemente quando, na verdade, fora induzido àquele resultado.

É preciso ressaltar que a definição de perfis e as decisões automatizadas podem ocorrer no mesmo contexto ou separadamente, bem como, podem existir decisões

[78] GT29 - **WP251rev.01**, versão em português. p. 7
[79] DONEDA, D. – ***op. cit.*** posição RB-2.6 [livroeletrônico]
[80] MAGRANI, E.; OLIVEIRA, R. M. - Lei Geral de Proteção de Dados. In: **Revista do Advogado.** p. 86

automatizadas sem definições de perfis e, ainda, definições de perfis realizados sem a intervenção de processos decisórios automatizados[81].

A definição de perfis no contexto das decisões automatizadas tem por intuito classificar estatisticamente indivíduos, ao passo que, partindo-se de inferências, analisa determinados aspectos pessoais daqueles para posteriormente traçar padrões comportamentais e realizar análises preditivas. Porém, "[e]m certos casos, a definição de perfis é suscetível de resultar em previsões imprecisas. Noutros casos, poderá dar origem a uma negação de serviços e bens e a uma discriminação injustificada"[82].

Já decisões exclusivamente automatizadas, são aquelas tomadas através dos aparatos tecnológicos de forma autônoma, sem a participação de uma entidade humana. Calha asseverar que o processo ainda será considerado unicamente automatizado quando, ainda que haja uma atuação humana, essa interferência não seja significativa e não seja tomada por quem não tenha autoridade ou competência para alterá-la[83].

Segundo o GT29, essas decisões podem se basear em diversos tipos de dados, como aqueles fornecidos diretamente pelas pessoas; observados sobre elas; ou inferidos de um perfil criado[84].

Este "novo" modelo de decisão pode ser facilmente vislumbrado desde os "simples" e "inofensivos" aplicativos que "escolhem*"* para o usuário as melhores rotas, até sua ampla utilização por instituições de crédito e sociedades financeiras para fins de *score* de crédito; no âmbito da saúde que, com base na análise dos dados pessoais genéticos dos pacientes, pode-se determinar de maneira mais precisa diagnósticos e tratamentos; além de classificar os "melhores" candidatos a uma vaga de emprego; e "inferir" se um indivíduo seria um potencial reincidente criminal.

Assim, essa técnica favorece a análise descritiva sobre pessoas ou cria projeções de comportamento sobre alguém que, "provavelmente poderá" tomar determinada

---

[81] Apesar da assertiva parecer confusa, colaciona-se o exemplo apresentado no GT29 no WP251rev.01 (p.9) por sua didática e clareza quanto à diferenciação e intercambiamento das duas técnicas: "A aplicação de coimas por excesso de velocidade com base exclusivamente em provas obtidas através de radares de velocidade constitui um processo de decisão automatizada que não implica necessariamente uma definição de perfis. No entanto, passaria a constituir uma decisão tomada com base na definição de perfis se os hábitos de condução da pessoa fossem controlados ao longo do tempo e, por exemplo, se o montante da coima aplicada resultasse de uma avaliação que tivesse em conta outros fatores, como a reincidência ou não do excesso de velocidade ou o facto de o condutor ter incorrido recentemente em infrações rodoviárias.".
[82] *Ibid.* p. 6
[83] *Ibid.*
[84] *Ibid.*

decisão, a certa altura de sua vida. Isso se torna ainda mais sério quando essas inferências visam prever possíveis comportamentos criminosos que talvez nunca venham a se concretizar no futuro.

Ainda assim, a cada dia cresce a delegação de tomada de decisões para os sistemas de IA, ao que

> observamos a construção de novas relações que estamos estabelecendo com as máquinas e demais dispositivos interconectados permitindo que algoritmos passem a tomar decisões e a pautar avaliações e ações que *antes* eram tomadas por humano[85]

Tendo em vista o impacto que algumas decisões de máquinas podem gerar na vida de pessoais reais, produzindo efeitos na sua esfera jurídica ou gerando efeitos adversos (como é fácil percepcionar no caso de uma decisão de cunho criminal), é necessário que se estabeleçam salvaguardas e se instituam direitos para proteger seus dados pessoais e, consequentemente, o próprio indivíduo. E, como grande parte dos substratos utilizados em ambas as situações são dados pessoais, mister garantir o pleno respeito da legislação relativa à proteção de dados pessoais.

Partindo-se das premissas apresentadas anteriormente, pode-se concluir que a proteção dos dados pessoais pode ser observável sob dois prismas distintos: consagrado como um direito em si mesmo e como garantia do exercício de outros direitos ou bens jurídicos, haja vista que, protegendo os dados pessoais dos hipotéticos indivíduos sujeitos àquelas decisões automatizadas que impactariam suas vidas, estar-se-ia também a proteger a dignidade da pessoa humana; a igualdade; o direito à obtenção de um crédito justo; o direito à saúde; à liberdade e ressocialização; e ao direito social ao trabalho e à renda.

Ocorre que esses algoritmos são em sua grande maioria dotados de opacidade e não há como saber ao certo em quais dados, critérios e finalidades ele se baseou para tomar uma decisão com poder de repercutir na vida de um particular.

[85] MAGRANI, E. – **Entre dados e robôs.** p. 19

3.3 – Opacidade e discriminação

A opacidade é um dos grandes desafios dentro dos sistemas de IA, haja vista que impede que os potenciais afetados por uma decisão automatizada compreendam, ou mesmo, verifiquem se seus dados pessoais estavam corretos e/ou foram tratados de modo legítimo e proporcional pela máquina. Essa nebulosidade mantém uma indesejável assimetria informacional oriunda do mundo das "caixas pretas" dos sistemas algorítmicos.

A opacidade impede de avaliar se o processo automatizado foi justo ou discriminatório; se negou direitos; ou se foi baseado em informações erradas, imprecisas ou retiradas de contexto. Os riscos procedentes dessas situações são os resultados falsos, imprecisos, enviesados, parciais, incompletos ou sem exatidão, e que, além de tudo, fornecem pouca, ou nenhuma, explicação para o destinário da decisão.

A opacidade é o exato oposto da almejada transparência nos processos algorítmicos, porém, não é o único obstáculo encontrado no caminho de quem busca compreender um resultado decisório da máquina, havendo também o direito de propriedade intelectual do *software*[86].

A opacidade pode ser tamanha que em determinados contextos não se conhecem nem os dados de entrada, nem o funcionamento interno do programa, não havendo margem para retificação pelo titular. E quando uma infraestrutura tem o condão de afetar de modo negativo uma pessoa, sem que esta tenha ferramentas para efetivar sequer uma correção[87], Pasquale a denomina de "*defective by design*"[88].

Daí a relevância de se capacitar profissionais (de áreas técnicas e humanas) que possam compreender o processo algorítmico e, assim, venham a ser realmente efetivadas mudanças e sejam introduzidos mecanismos de explicabilidade, responsabilização e

[86] A lei brasileira resguarda os segredos comerciais e industriais, sem, entretanto, delimitar limites para tal. O regulamento europeu não prevê de forma expressa essa situação, porém o GT29 esclarece que, nos moldes do considerando 63, o direito de acesso do titular não deve afetar o segredo comercial ou a propriedade intelectual, bem como, que os responsáveis pelo tratamento não podem invocar esse direito como pretexto para negar o acesso ou recusar informações ao titular dos dados. Frank Pasquale reflete sobre essa hipótese em seu livro "*The Black Box Society*", quando suscita que a opacidade seria uma estratégia proposital e o segredo de negócios invocado como uma desculpa para que os algoritmos sejam mantidos secretos, dificultando a sua auditoria e controle para continuar a atender a interesses escusos de poderosas organizações e do Estado, que tentam esconder possíveis condutas anticompetitivas ou mesmo discriminatórias sob o falso manto da impossibilidade técnica de desmontar o algoritmo (Pasquale, F. - **The Black Box Society**) (tradução própria)
[87] O que fulmina de morte o princípio da exatidão, resguardado pelas leis de proteção de dados.
[88] Kobie, N. - **Who do you blame when an algorithm gets you fired?**

transparência para que a opacidade não continue a ser usada como desculpa para violar direitos.

Além das hipóteses em que os resultados poderão apresentar imprecisões, erros ou vieses[89] cognitivos, a tomada de decisões automatizadas pode ainda reproduzir, disseminar ou reforçar preconceitos e estereótipos racistas, sexistas, religiosos, dentre outros, ignorando injustiças sociais históricas e os direitos das minorias e dos grupos vulneráveis.

Entretanto, as decisões automatizadas, *per se*, não podem ser consideradas discriminatórias, posto que os algoritmos responsáveis pelas mesmas são baseados em predileções e funcionam como um mero *eco* de uma sociedade enviesada, historicamente marcada por injustiças, desigualdades e preconceitos.

Nibø complementa o entendimento:

> As decisões que os algoritmos tomam estão baseadas nas informações que eles recebem. Assim, tendo como base a interação com informações fornecidas por humanos, as máquinas apresentarão os resultados daquilo que lhe é solicitado. A partir desse momento, os algoritmos passam a ter efeito de feedback – ao retornar determinados resultados, a máquina também passará a moldar determinados comportamentos dos humanos. Assim, os humanos passam a tomar suas decisões em tempo real, com base nas respostas feitas por um algoritmo que chegou a conclusões com base em dados passados fornecidos por humanos. É nesse contexto que nasce o perigo do preconceito presente nas máquinas, pois é fruto dos vieses humanos que influenciaram a decisão da máquina. Por outro lado, essa máquina passará a influenciar o comportamento dos humanos, reforçando qualquer preconceito existente na sociedade[90]

Ora, sendo a máquina objetiva, ela não está livre dos subjetivos preconceitos humanos? Ou melhor, a sua objetividade neutralizaria a parcialidade? Nesse sentido, mister consignar os relevantes apontamentos de Braga, discordando da neutralidade:

> considerando que o *output* é apenas tão bom quanto o *input*, os resultados obtidos pelo algoritmo serão contaminados pelas distorções dos programadores que criaram o algoritmo, assim como pelos dados com que

[89] Vieses não são embutidos de forma proposital nas bases de dados, eles existem em decorrência dos próprios preconceitos sociais, sendo meros reflexos da sociedade.
[90] Nibø, E. F. – ***op. cit***. p. 137

> foi alimentado e treinado (Evidência má orientada que leva a distorções). Dessa forma, as decisões tomadas pela máquina podem ser tão falíveis, ou até mais, do que as realizadas pelo ser humano[91]

Nenhum algoritmo é bom ou mau em si mesmo. Isso irá depender da forma como o sistema é utilizado. Eles não são preconceituosos, entretanto suas decisões podem produzir efeitos discriminatórios se seu banco de dados estiver enviesado, cabendo ressaltar ainda o problema da sub-representação de alguns grupos nos dados usados para moldar a IA em seu treinamento[92].

Nybø menciona uma situação real ocorrida com a gigante *Amazon* que, ao utilizar um algoritmo para selecionar candidatos com o intuito de recrutar colaboradores para a *Big Tech*, percebeu que o mesmo demonstrou ser bastante enviesado em relação às candidatas do sexo feminino. Trata-se, nesse caso, de uma discriminação estatística que, mesmo não intencional, ocorrera porque o sistema foi treinado com dados do passado que refletiam a predominância masculina na indústria da tecnologia e fez a máquina entender, de forma completamente equivocada, que o fato de haver mais homens que mulheres nesse nicho de emprego é porque eles seriam mais competentes que as mulheres.

O autor então conclui pela importância de uma supervisão humana já que

> a decisão puramente lógica não está necessariamente certa e, muitas vezes, não é a decisão desejável. Em alguns casos é necessário adicionar um componente emocional, até mesmo para que possamos atender aos critérios de justiça exigidos pela moralidade de uma sociedade que vive em uma determinada época[93].

Essa situação confirma, com veemência, que os sistemas algorítmicos devem ser assistidos por um humano, já que a despeito de serem programados por eles, "pensam" de forma diferente deles, tal como afirmou Alan Turing. Desse modo, o humano irá analisar se os critérios utilizados estão corretos, se são transparentes, não discriminatórios e se são justos, sobretudo considerando o papel social da IA no seio da sociedade

[91] Braga, C. H. da C - **Decisões automatizadas e discriminação**. p. 65
[92] Braga indica que "a forma mais comum de discriminação gerada pelas decisões autônomas ocorre por meio dos dados utilizados em seu treinamento" (***Ibid.*** p. 47)
[93] Nibø, E. F. – ***op. cit***. p. 105

contemporânea. E para que um modelo de inteligência computacional seja ético, este deve ser desenvolvido com cautela e supervisão humana.

Tamanha a relevância da matéria que o legislador europeu destacou que o tratamento automatizado de dados deve revestir-se de um caráter excepcional, apenas admitido nos permissivos legais, e sempre ressalvando a necessidade de salvaguardas.

Some-se a isso que o GT29 no "Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (Diretiva (UE) 2016/680)"[94], dispõe sobre a proibição contra a discriminação como uma consequência das decisões automatizadas. Ainda que mencione apenas essa restrição em relação às categorias especiais de dados e que tal princípio não esteja explícito no corpo do RGPD ou da Diretiva (UE) 2016/680, sabe-se do cuidado do legislador europeu com a proteção real o titular, de modo que tal interpretação pode ser extraída da leitura correlacionada dos arts. 5.º e 22.º, juntamente com os considerandos 39 e 71 a 75 do RGPD. No bojo da Diretiva (UE) 680/2016 é observável através do art. 11.º cumulado com os considerandos 38, 51 e 61.

Já a LGPD, compreendendo a seriedade do tema, previu a não discriminação como um dos princípios basilares da lei (cf. art. 6º, inciso IX), a ser aplicado juntamente com outros relevantes, tal como a boa-fé e a transparência, e ainda determinou de forma expressa o direito a um tratamento automatizado não discriminatório, conforme se avista da simples leitura do art. 20, §2º. Além disso, o princípio da não discriminação deve ser refletido em todas as circunstâncias em que o uso de dados, sensíveis ou não, gere algum tipo de "desvalor ou indução a resultados que seriam inequitativos"[95].

Destaque-se que nem toda decisão tomada exclusivamente por algoritmos produz efeitos jurídicos[96]; afeta significativamente de forma similar[97]; ou ainda gera efeitos adversos. Alguns processos decisórios podem ser tidos como "inofensivos", tais como

---

[94] GT29 - **WP 258**, versão em português. Disponível em: https://ec.europa.eu/newsroom/article29/items/610178/en (consultado em 29/12 2020)

[95] Mulholland C.; Frajhof I. Z. - Inteligência Artificial e a Lei Geral de Proteção de Dados Pessoais, In: **Inteligência Artificial e Direito**. Posição RB-13.2 [livroeletrônico]

[96] Quando se considera que a decisão pode afetar direitos legais de um indivíduo. O GT29 cita alguns exemplos: uma rescisão contratual; a recusa de uma prestação social ou de admissão num país, entre outros. (WP251rev.01, versão em português. p. 23)

[97] Ocorre quando a decisão impacta de forma suficientemente significativa a vida de alguém, podendo, inclusive, em casos extremos gerar discriminação, a exemplo daquelas decisões que afetam o acesso à rede de saúde (*Ibid*. p. 24).

aqueles que apenas indicam um filme de gosto duvidoso numa plataforma de *streaming*, cujo efeito produzido talvez não cause mais que mero um aborrecimento.

Porém, como visto, algumas dessas decisões tem o condão de gerar efeitos substanciais bem adversos na vida de um indivíduo, como os que podem impactar um dos maiores direitos do homem: a liberdade. O próximo tópico abordará, especificamente, as decisões automatizadas, que utilizam dados pessoais, no contexto do policiamento e da justiça criminal.

3.4. - Policiamento preditivo

A atual sociedade de risco, marcada pelo crescimento da criminalidade transacional, insegurança e terrorismo revelou a insuficiência do modelo tradicional de policiamento reativo[98] e obrigou o surgimento de um novo paradigma quanto à forma de atuação em relação aos crimes, ganhando como uma grande aliada nesse combate à criminalidade, a tecnologia.

Analisando estatísticas criminais passadas, percebeu-se que, das informações ali contidas, poder-se-iam extrair padrões e assim obter um panorama acerca de prováveis eventos futuros.

A ideia de buscar padrões no cometimento de crimes não é recente, remontando aos anos de 1820, quando o advogado André-Michel Guerry, visando definir padrões geográficos, passou a registrar violações, homicídios e roubos que ocorriam em diversos pontos da França, tendo reconhecido a repetição de padrões nos crimes cometidos, como e por quem, e que estes padrões não se alteravam com o decorrer do tempo. Assim, "os jovens cometiam mais crimes que os velhos, os homens mais que as mulheres, os pobres mais que os ricos" [99]. Desse modo, concluiu que "o crime não é aleatório, as pessoas são previsíveis"[100].

Tal percepção foi utilizada posteriormente pelo policial canadense Kim Rossmo que desenvolveu um algoritmo que, para definir padrões, passou a focar a

[98] MOLEIRINHO, P. - Policiamento orientado pelas informações. In: AAVV, **Enciclopédia de Direito e Segurança**
[99] RAFTER, N. H., 2009 *apud*, FRY, H. - **Olá Futuro**, p. 180
[100] RAFTER, N. H., 2009 *apud*, FRY, H. - **Olá Futuro**, p. 180

investigação exclusivamente no fator geográfico. Com isso, esse revolucionário algoritmo de *geoprofiling* conseguiu localizar um violador em série, na famosa operação "*Lynx*"[101]. Também foi utilizada nos chamados Mapas do Futuro de Jack Maple[102].

Da evolução desses métodos científicos que se baseiam em evidências e análises de dados, dos quais se extraem padrões para que se possam antecipar eventos futuros (numa tríplice análise de risco entre espaço, tempo e oportunidade) surgiu a noção do policiamento preditivo.

O policiamento preditivo objetiva combater a criminalidade, através da prevenção, com base em análise de dados que, após serem devidamente agregados, indicam a possibilidade de ocorrer um crime em determinado local, num dado período de tempo ou ainda os eventuais envolvidos em um crime, seja como vítima ou infrator, reduzindo tempo de ação, recursos e esforços humanos.

É uma forma estratégica e tática de, através da análise de dados, prevenir crimes potenciais. Atualmente, tem-se observado um aumento do uso da técnica de criação de perfis e decisões automatizadas no contexto criminal das atividades de prevenção, investigação, detecção ou execução de sanções penais. Um dos principais fundamentos seria a crença de que esses algoritmos seriam mais imparciais e justos que os seres humanos ao tomar decisões, posto que isentos dos preconceitos sociais[103].

Existem dois tipos mais amplos de metodologias de policiamento preditivo que utilizam o programa de análise de dados, podendo se baseiam em local ou em pessoa[104].

O método "baseado em localização" relaciona lugares, eventos propícios a haver grande aglomeração de pessoas (como os concertos, jogos de futebol) e dados passados de crimes para antever o tipo, o período e o local onde novos delitos podem ocorrer no futuro para, então, "impedi-los". Busca identificar pontos considerados críticos para então direcionar, tática e estrategicamente, patrulhas policiais para as áreas definidas. Um desses *softwares* é o PredPol.

A outra metodologia "baseada em pessoas" utiliza como substrato dados como idade, estado civil, sexo, uso de substâncias entorpecentes e antecedentes criminais para gerar um prognóstico sobre quem teria probabilidade de cometer um crime futuramente.

---

[101] FRY, H. - **Olá Futuro**
[102] *Ibid.*
[103] BRAGA, C. H. da C. B. – ***op. cit***.
[104] *Ibid.* p 35

Essa antecipação, em tese, serve para auxiliar as autoridades policiais a prevenir crimes e também para auxiliar os magistrados nas tomadas de decisões, como avaliar a possibilidade de uma pessoa vir a reincidir em atividades criminosas futuras. Como exemplos têm-se o COMPAS e o HART.

Rosamunde van Brakel[105] define que o policiamento preditivo pode ser usado tanto para tomada de decisões sistêmicas (aquelas relacionadas aos horários e locais dos crimes), bem como para decisões de identificação (por exemplo, prever a identidade de supostos infratores ou vítimas de crime).

Todos esses programas se fundamentam numa avaliação de risco que quantifica uma probabilidade e, um dos maiores problemas observados nesse ponto, é que os dados históricos utilizados no treinamento desses sistemas incluem registros passados de detenções e relatórios policiais. Contudo, sua operabilidade é pouco transparente. Além disso, esses algoritmos são protegidos por propriedade intelectual, não tendo seu código disponível para escrutínio.

No próximo tópico serão abordados alguns desses sistemas, no que interessa à apreciação do presente trabalho acadêmico.

3.4.1 - COMPAS

Um dos algoritmos mais emblemáticos acerca da questão diz respeito ao famoso e controverso *software* da empresa americana *Northpointe* conhecido pelo acrônimo de COMPAS: *Correctional Offender Management Profiling for Alternativo Sanctions*.

Ressalte-se que, a despeito de ser o programa de predição *a la* "minority report"[106] mais mencionado, é apenas um dos vários algoritmos utilizados para avaliação de risco nesse contexto.

---

[105] BRAKEL, R. van, 2016, *apud* LYNSKEY, O. - **Criminal justice profiling and EU data protection Law**

[106] *Minority Report* é uma obra de ficção científica escrita por Philip K. Dick no ano de 1956 que deu origem ao famoso filme com o mesmo título, lançado em 2002 sob a direção de Steven Spielberg e tendo como protoganista o ator Tom Cruise. A história se passa no ano de 2054, "em que há um departamento de polícia especializada, que apreende criminosos tendo por base o 'Pré-Crime', ou seja, o conhecimento prévio de crimes que ainda acontecerão no futuro, mas que a partir da previsão por três videntes chamados 'precogs', o departamento de justiça se mobiliza no sentido de evita-los e dessa forma, age punitivamente antes dos delitos ocorrerem.". Cf. artigo escrito por Vanessa Guerra, em 2019, intitulado: "Minority Report: ficção ou

Esses *softwares* fazem parte de um moderno grupo de tecnologias computacionais e preditivas utilizados

> como suporte para a tomada de decisões relacionadas à condenação, ao tratamento, ao gerenciamento de casos e à probabilidade de reincidência - com impactos significativos na possibilidade de progressão de regime de apenados. Ele se propõe a utilizar teorias consolidadas da criminologia para fundamentar de maneira orientada as avaliações correcionais.[107]

Segundo o guia oficial da ferramenta ("Practitioner's Guide to COMPAS Core"), o sistema foi projetado para aplicações em pré-julgamento, liberdade condicional, prisão e correções comunitárias, voltado para criminosos do sexo masculino e feminino[108].

Essa avaliação correcional é feita com base nas respostas de 137 itens um questionário contendo - além de dados pessoais como nome e gênero - tópicos como antecedentes criminais, uso de substâncias, recursos educacionais, envolvimento social e índice de criminalidade da vizinhança, que, após analisados em conjunto com a vida pregressa dos ofensores, gera uma pontuação[109] do potencial risco que esses indivíduos representariam para a sociedade[110].

Por diversas vezes o algoritmo foi "acusado" de ser discriminatório quanto aos ofensores de determinadas raças e classes sociais, o que ensejaria numa solidificação de estereótipos de minorias já historicamente estigmatizadas[111]. A despeito disso, o COMPAS foi considerado aceitável após um estudo realizado, em 2010, pelo Departamento de Correção e Reabilitação da Califórnia para avaliar sua validação para ser utilizado em

---

realidade?". Disponível em: https://ab2l.org.br/minority-report-ficcao-ou-realidade/ (consultado em 01/02 2020)

[107] MOURÃO, C. E. R.; OLIVEIRA, D. T. N. - ***Softwares* de tomada de decisão e poder público**

[108] O guia está disponível em: https://www.equivant.com/wp-content/uploads/Practitioners-Guide-to-COMPAS-Core-040419.pdf (informações extraídas da p.1) (consultado em 01/02 2021)

[109] A ferramenta funciona a partir da técnica de árvore decisória, que classifica os infratores em um espectro de risco. (MENDES, L. S.; MATTIUZZO, M. - **Discriminação Algorítmica**)

[110] Uma cópia do documento completo está disponível no *link:* https://assets.documentcloud.org/documents/2702103/Sample-Risk-Assessment-COMPAS-CORE.pdf

[111] Um fato interessante é que a raça não está incluída como um fator determinante no funcionamento do COMPAS. Todavia, apenas fazer a retirada de dados sensíveis do sistema não garante que estes não possam ser extraídos de uma análise conjunta com outros dados. Excluir um dado, ou um conjunto de dados, que possa levar à uma discriminação, não significa que o sistema inteligente de algoritmos não possa gerar um *proxy* que, de qualquer modo, irá categorizar e segmentar o indivíduo. Por exemplo, ainda que a classe social não esteja englobada num determinado conjunto de informações, o algoritmo pode facilmente deduzi-lo ao analisar o bairro onde a pessoa mora.

relação a índices de reincidência como um todo, haja vista que ter alcançado um resultado de 70% de exatidão.

Contudo, um estudo realizado pela instituição ProPublica questionou os números oficiais e constatou que os resultados encontrados pela organização divergiam dos dados divulgados pelo COMPAS, no que tange ao percentual de erros de previsão quanto à média da pontuação entre negros e brancos, havendo um número significativamente maior de erros preditivos quando se tratava de ofensores negros.

Ou seja, nos casos em que o programa errou a análise preditiva, não tendo ocorrido a reincidência "esperada", houve um percentual de 50% de erro a mais para as pessoas negras avaliadas, que tinham duas vezes mais chances de serem classificadas como de um alto risco de reincidência[112].

Alguns casos tortuosos já ocorreram em decorrência do uso desse programa, a exemplo da história de Paul Zilly, em 2013, em Wisconsin. Condenado pelo roubo de um cortador de grama e, a despeito de ter conseguido um acordo judicial entre a acusação e a defesa, viu suas expectativas frustradas devido ao famigerado COMPAS que calculou sua estimativa para atividades delitógenas, considerando-o de alto risco para o cometimento de um crime violento no futuro e de médio risco para ser um reincidente[113]. O magistrado responsável por sua sentença, com base na avaliação da ferramenta correcional, não só rejeitou o acordo judicial como lhe impôs uma sentença mais dura que a anteriormente prevista.

Os bastidores do COMPAS e a metodologia por trás do programa é um segredo comercial, não se sabendo ao certo como essas pontuações de risco no interior da máquina ou como os dados de entrada são ponderados, por isso o *software* é criticado por sua opacidade e pela possibilidade de prolatar decisões manifestamente enviesadas, reforçando estereótipos e perpetuando a marginalização de grupos já tidos como vulneráveis.

[112] ANGWIN, J. [*et. al.*] – **Machine Bias**
[113] FRY, H. ***op cit.***

3.4.2 - HART

Outros países também adotaram sistemas de predição, como é o caso do Reino Unido que se vale do "*Harm Assessment Risk Tool*" (HART), construído usando florestas aleatórias. O sistema foi desenvolvido, num esforço conjunto entre a polícia de Durham e pesquisadores da Universidade de Cambridge, com o objetivo de prever o risco (baixo, médio, alto) de suspeitos cometerem novos crimes num período de dois anos[114].

Foi projetado para reduzir o número de pessoas e processos através do sistema judicial do Reino Unido, auxiliando as autoridades policiais a avaliar a possibilidade do encaminhamento dos infratores considerados como de risco moderado para um programa de reabilitação chamado *Checkpoint*, com o objetivo de reduzir a reincidência[115].

As previsões do Hart levam em conta um total de 34 variáveis preditoras divididos da seguinte forma: idade, sexo, duas formas de código postal residencial e número de relatórios de inteligência policial relacionados ao infrator e outras 29 sobre o histórico de ofensas do suspeito[116].

Nesse ponto, cabe registrar que os ativistas do grupo independente do Reino Unido chamado *Big Brother Watch* indicaram que juntamente com os dados de código postal residencial eram incluídas outras informações, como benefícios e suporte para crianças, além de dados coletados *online*, o que acabava por criar um estereótipo quanto ao código postal[117].

Nos moldes da metodologia de Rosamunde van Brakel, citado acima, tanto o COMPAS, como o HART se enquadram no escopo da categoria dos *softwares* de policiamento preditivo para a tomada de decisões de identificação, posto que suas previsões recaem, especificamente, sobre o comportamento de pessoas que podem se tornar criminosos reais ou potenciais[118].

Outros exemplos desse modelo seriam a ferramenta *Beware*, da Intrado, pela qual a polícia analisa dados publicamente disponíveis, tais como os de mídia social, para verificar a "pontuação de ameaça" de uma pessoa e categorizá-la em níveis diferentes

[114] OSWALD, M. [et al] - **Algorithmic risk assessment policing models**
[115] BURGESS, M. - **UK police are using AI to inform custodial decisions**
[116] OSWALD, M. [et al]. op cit. p. 228
[117] BIG BROTHER WATCH, 2018, *apud* LYSNKEY, O. ***op. cit*** .
[118] LYNSKEY, O. - ***op. cit***.

de risco; e ainda a compilação das listas de calor (*heat list*) utilizadas em Chicago, as quais contém os nomes das pessoais mais prováveis de se envolverem futuramente em um crime, com base em seu histórico criminal, ou identificado como parte de algum grupo suspeito, passando a ser monitorados pela polícia[119].

Todos esses programas que se valem de pontuações de risco realizadas por algoritmos nada mais são que um prognóstico comportamental de pessoas. Grosso modo, existem, dois erros que o sistema pode cometer: gerar falsos positivos ou falsos negativos. Isso ocorre no momento da identificação quanto ao risco, ou seja, quando a máquina classifica alguém de baixo risco como de algo risco, gerando um falso positivo e vice-versa.

3.4.3- PREDPOL

O PredPol surgiu de um projeto desenvolvido pelo Departamento de Polícia de Los Angeles e pela Universidade da Califórnia (UCLA)[120]. Essa metodologia se foca em locais mais propícios a ocorrer um novo crime (chamados pontos quentes) para, de posse dessa informação, tomar decisões sistêmicas (relacionando tipo de crime, horário e local) e assim direcionar de forma eficiente agentes policiais para aquela área, o que poupa recursos humanos e financeiros.

O PredPol não visa especificamente pessoais, nem prevê exatamente quem irá cometer um crime no futuro. O que ele faz é mapear áreas geográficas com maior risco de ser um cenário para crimes futuros e indicar para onde devem ser concentrados atenção e esforços.

Contudo, esse programa também não é isento de ser discriminatório, posto que suas previsões podem criar um efeito de *feedback* ao apontar sistematicamente locais mais pobres e vulneráveis como mais perigosos e propensos ao crime. Fry[121] descreve, então, uma situação bem provável

[119] BRAGA, C. H. da C. – ***op cit.***
[120] Informação extraída do sítio oficial da ferramenta. Disponível no *link*: https://www.predpol.com/about/ (consultado em 08/05 2021) (tradução própria)
[121] FRY, H**. -** ***op cit***. p. 195

> se, digamos, um bairro mais pobre tinha um nível de crime mais alto num primeiro momento, o algoritmo poderá muito bem prever que irão ali ocorrer mais crimes no futuro. Consequentemente, serão enviados agentes para o bairro, o que significa que detetarão mais crimes. Assim, o algoritmo preverá ainda mais, e serão enviados mais agentes, e por aí afora.

Desse modo, esses dados enviesados retroalimentam o sistema que volta a repetir os mesmos padrões discriminatórios, perpetuando preconceitos, segregando pessoas e punindo, inclusive, a vizinhança como um todo, seja pelo aumento da vigilância, seja gerando um falso estigma de que todas as pessoas daquele meio incorrerão em determinado comportamento.

3.5. - Vieses na polícia

Braga aponta que três camadas de vieses que podem gerar discriminações no âmbito desse tipo de policiamento: o entendimento de justiça pelo programa empregado, a qualidade dos dados e a preparação desses dados.

Quanto ao primeiro ponto, pondera que é necessária uma definição estatística de justiça, o que, por si só, é complexo, ante as diferentes percepções de justiça que podem existir. A segunda camada busca encontrar vieses nos dados coletados a serem utilizados pelo modelo de decisão. Por fim, a última camada busca responder se é justo que o resultado de uma decisão sobre um indivíduo se baseie em dados de outras pessoas.

A mesma autora aponta então que a solução para esses problemas seria reformar, desde a raiz, os mecanismos sociais e políticos que geram esses dados "sujos". Porém, reconhece que, enquanto isso for uma utopia, deve-se avaliar formas concretas de regular o uso dessas ferramentas que versam sobre decisões automatizadas sob uma perspectiva regulatória, jurídica e ética[122].

[122] BRAGA, C. H. da C. – ***op cit.***

3.6. - Esses modelos de tomada de decisões automatizadas tratam dados pessoais?

A pergunta pertinente é: esses modelos de policiamento preditivo tratam dados pessoais e, assim, estariam sob o abrigo da incidência das normas de proteção de dados pessoais?

Este trabalho acadêmico adotou as considerações de Orla Lynskey para justificar a resposta à pergunta anterior. Lynskey questiona se o tratamento de dados pessoais realizado através das tecnologias de policiamento preditivo se enquadraria realmente no escopo da Diretiva (UE) 2016/680 e, caso positivo, qual seria o alcance da aplicação[123].

A autora então explana acerca da interpretação dada ao conceito de dados pessoais: pelo próprio regulamento; pelas opiniões do GT29[124]; através das decisões exaradas pelo Tribunal de Justiça da União Europeia (TJUE)[125]; e da doutrina de Purtova, concluindo que há fundamentos para afirmar que tanto as decisões de identificação como as sistêmicas processam dados pessoais, ainda que exista uma margem de dúvida em relação a esta última.

Iniciando pela análise das decisões sistêmicas, Lynskey distingue três etapas diversas no funcionamento desses programas de análise preditiva: a etapa da entrada *(inputs)* dos dados; a etapa da aplicação do algoritmo do sistema a esses dados; e a saída (*output)* que, no caso, é a recomendação do sistema.

Desta feita, mesmo que as organizações que desenvolvem essas tecnologias neguem fazer uso de dados e informações de cunho pessoal[126], com base na jurisprudência do TJUE e na doutrina de Purtova[127], Lynskey acredita existirem subsídios

[123] LYNSKEY, O. – ***op. cit.*** p 162.
[124] Contidas no "Parecer sobre algumas questões essenciais da Diretiva de Aplicação da Lei (UE 2016/680)" , WP258, adotado em 29 de novembro de 2017.
[125] Dos quais, a autora cita: *Processos apensos C-141/12 e 372/12 YS v. Minister voor Immigratie, Integratie en Asiel e Minister voor Immigratie, Integratie en Asiel v. MS EU: C: 2014: 2081; Processo C-582/14, Breyer EU: C: 2016: 779; Processo C-434/16, Nowak v. Data Protection Commissioner EU: C: 2017: 994.*
[126] Como é o caso do PREDPOL que em seu sítio oficial informa que utiliza como dados de entrada apenas o tipo de crime, o local do crime e a data e hora do crime, sem fazer uso de dados pessoais e respeitando os limites de privacidade e dos direitos civis do residentes onde esse programa é aplicado.
[127] Nadezhda Purtova é professora de Tilburg e publicou, em 02 de abril de 2018, um interessante artigo intitulado "The law of everything. Broad concept of personal data and future of EU data protection law" no qual afirma que "tudo em breve se enquadrará na definição de dados pessoais interpretados pelo WP29 e pelo Tribunal de Justiça" (cf. p. 78, do artigo referido – tradução própria). A docente menciona que "mesmo as informações que não são de forma alguma sobre alguém podem ser consideradas 'relacionadas a' uma pessoa determinada". Nesse caso, sustenta que podem se referir a uma pessoa "em propósito", o que ocorreria casos esses dados fossem usados para avaliar, tratar uma pessoa de determinada maneira ou mesmo para influenciar um comportamento (cf. p. 55, do artigo referido – tradução própria)

para sustentar que em todas as três etapas mencionadas ocorram o processamento de dados pessoais, já que em todas as fases os dados utilizados são susceptíveis de serem relacionados com um sujeito, devido ao seu propósito (que no caso seria o de tratar as pessoas identificadas pelo algoritmo de uma determinada forma) ou ao seu efeito (que aqui seria o de impactar as pessoas então identificadas nos pontos de acesso identificados)[128].

Contudo, a autora reflete se esses dados poderiam realmente ser associados a uma pessoa identificável, (*v.g.* se combinados com outros dados de entrada, como imagens de CFTV), ao que argumenta que, apesar de ser hipoteticamente possível vincular dados de localização de um crime a um indivíduo, esse não é um padrão "provavelmente razoável"[129] a ser utilizado pelos agentes de polícia. A mesma lógica pode ser aplicada às outras duas etapas do funcionamento desses programas[130].

Outro argumento, que poderia ser suscitado para negar a configuração de dados pessoais no cenário de decisões sistêmicas, seria o de que essas incidem sobre um grupo de pessoas e não uma pessoa individualmente considerada.

Consoante a professora Maja Brkan, o art. 22.º do RGPD (alinhado com o art. 11.º da Diretiva 2016/680) traz a obrigação de os Estados Membros proibirem decisões automatizadas com determinadas características[131]. Para isso, essa decisão: tem que ser individual (a mesma condição é imposta pela diretiva); o processamento deve ser automatizado (o mesmo vale para a diretiva); e ele precisa gerar efeitos, jurídicos ou significativamente similares, sobre o titular dos dados (nesse ponto, a diretiva se refere a efeitos "adversos").

A autora traz uma reflexão se uma decisão coletiva automatizada em matéria penal estaria então dentro do escopo do regulamento ou da diretiva, haja vista que ambos os diplomas direcionam sua proteção a pessoas singulares.

Brkan observa que, não obstante o art. 11.º da Diretiva e o art. 22.º do RGPD, interpretados em correlação com seus respectivos art. 1.º, não abranjam a decisão coletiva, esses também não a proíbem. Desta feita, afirma que, aparentemente, a razão da

---

A despeito de entender essa extensão como positiva, a autora do artigo reflete que num futuro próximo, quando o mundo estará ainda mais hiperconectado, "O sistema de proteção legal baseado em tal abrangente noção e alta intensidade de obrigações de conformidade positiva não vai ser sustentável no longo prazo." (p. 58) (tradução própria)

[128] LYNSKEY, O. - ***op. cit.*** (tradução própria)

[129] *Ibid.* p. 171(tradução própria)

[130] *Ibid.* (tradução própria)

[131] BRKAN, M. - **Do algorithms rule the world?** p. 7 (tradução própria)

diferenciação da proteção de dados pessoais de uma pessoa individualizada e de um grupo de titulares esbarra na justificativa de que os dados utilizados para uma decisão coletiva estão (ou deveriam estar) anonimizados[132], por isso, fora do escopo da legislação de proteção de dados europeia.

Contudo, esse argumento, segundo a autora, não deve se sustentar: a um): porque existem situações em que o titular dos dados permanece identificável; e a dois): porque a "reidentificação de um indivíduo pertencente a um determinado grupo é significativamente facilitada"[133], mormente considerando que os avanços nos estudos de métodos de reversão da anonimização.

Por fim, Brkan propõe que, para uma efetiva proteção do titular dos dados, essas decisões também sejam abrangidas pelo âmbito de aplicação do art. 22.º do RGPD e do art. 11.º da Diretiva, posto que uma decisão sobre um grupo seria, em verdade, "um feixe de decisões individuais"[134].

Após esse esforço interpretativo, de ser possível que decisões sistêmicas procedam ao processamento de dados pessoais, há ainda mais embasamento para se afirmar que as decisões de identificação também envolvam esse tipo de tratamento.

Antes porém de adentrar ao cerne da argumentação, cabe o questionamento: supondo um mundo ideal no qual uma autoridade competente[135], dentro no âmbito de aplicação legal[136], vale-se de um programa computacional de IA análogo aos expostos anteriormente para proceder às suas atividades de policiamento preditivo, o tratamento de dados realizado nesse contexto estaria dentro do escopo das normas de proteção de dados pessoais?

Ora, tudo irá depender de como o processo de decisão realmente ocorreu na prática, calhando relembrar que o art. 11.º da Diretiva (UE) 2016/680 determina a proibição de "decisões tomadas exclusivamente com base no tratamento automatizado" que "produzam efeitos adversos na esfera jurídica" ou "afetem significativamente" o titular. Em complemento, deve ainda ser considerado se houve uma intervenção humana ao longo do processo decisório e se essa foi substancial e/ou tomada por alguém com competência para

[132] *Ibid.* p. 7 (tradução própria)
[133] *Ibid.* p. 8. (tradução própria)
[134] *Ibid.* p. 8. (tradução própria)
[135] Cf. artigo. 3.º da Diretiva (UE) 2016/680.
[136] Cf. artigo 2.º da Diretiva (UE) 2016/680.

alterar a decisão. Dependendo desses fatores, de logo, não há que se falar em aplicação da Diretiva.

Voltando ao "mundo ideal" e admitindo uma hipótese permissiva na qual, um Estado-Membro passe a utilizar um programa de predição no estilo do HART ou COMPAS, é cabível asseverar, com veemência, que esses sistemas operacionais de IA valem-se de dados pessoais. No caso do HART, ainda que se desconsiderassem todos os 34 preditores relativos ao histórico pessoal do infrator, certo é que existem pelo menos dois tipos de dados de entrada que dizem respeito, de forma direta, a dados pessoais da pessoa avaliada, como a indicação de gênero e o código postal residencial, que se enquadram, indubitavelmente, no escopo de dados pessoais, tanto do Regulamento[137], como da Diretiva[138].

Os outros dados de entrada, segundo Lynskey, também são dados pessoais, tendo em vista que "seu conteúdo diz respeito a uma pessoa identificada"[139]. De igual forma, os dados de saída também devem ser tidos como dados pessoais, já que se consubstanciam "numa probabilidade sugerida de reincidência e sua finalidade e efeito irão influenciar as perspectivas futuras de um indivíduo identificado"[140].

Quanto ao estágio intermediário da operação, a autora pondera acerca da configuração desses como dados pessoais, mas conclui que, na mesma linha da jurisprudência do TJUE, no caso Nowak[141], pode-se argumentar que a aplicação do modelo

---

[137] Cf. artigo 4.º (1)
[138] Cf. artigo 3.º (1)
[139] Lynskey, O. – ***op. cit***. p. 172
[140] *Ibid.* p. 172
[141] O Tribunal de Justiça da União Europeia declarou no caso Nowak que o termo *qualquer informação* refletiria o objetivo do legislador de "atribuir um amplo âmbito a esse conceito". O caso se desenrolou após o senhor Nowak ter sido reprovado, pela quarta vez, no exame de Finança Estratégica e Contabilidade de Gestão, na Irlanda,e ver recusado seu acesso à folha de respostas.
Insatisfeito com a recusa, no ano de 2010, submeteu perante o *Institute of Chartered Accountants of Ireland* (CAI) pleito de acesso aos seus dados, com base na legislação irlandesa em matéria de proteção de dados, sendo-lhe fornecido pelo CAI o acesso a 17 documentos, exceto a folha de respostas do exame, sob o fundamento de que esta não se constituía um dado pessoal.
Inconformado, o senhor Nowak levou a questão à apreciação da Autoridade Irlandesa de Proteção de Dados, a qual endossou o alegado pelo CAI, de que a folha em questão não se tratava de um dado pessoal.
Nowak, então, recorreu desta decisão para os tribunais irlandeses, ocasião na qual seu processo foi submetido ao Tribunal de Justiça da EU para avaliar: 1) Se as informações contidas nas respostas do candidato, durante um exame profissional, poderiam ser consideradas dados pessoais ao abrigo da Diretiva 95/46/CE (vigente na época); e 2) quais são/seriam os fatores relevantes para determinar isso.
O TJUE decidiu então: "Uma folha de respostas de exame manuscrita, que pode ser atribuída a um candidato, incluindo eventuais comentários dos examinadores que nela figurem, constitui um conjunto de dados pessoais na aceção do artigo 2.º, alínea a), da Diretiva 95/46/CE relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados." Para maiores informações,

de aprendizado de máquina usado pelo HART nos dados de entrada dos 34 preditores do sistema são dados pessoais, ainda que seja difícil, na prática, considerar o modo como os direitos decorrentes dessa classificação (*v.g.* o direito à retificação), seriam levados a cabo pelos indivíduos envolvidos no tratamento[142]. A jurisprudência, futuramente, talvez venha a se debruçar sobre a questão, para confirmar ou rejeitar esse entendimento.

Destarte, adotando os argumentos expostos nesse capítulo, pode-se verificar que essas duas formas de modelos de policiamento preditivo podem ser enquadradas no âmbito de aplicação do quadro de proteção de dados europeu. Nesse sentido, como fica a situação dos indivíduos impactados por decisões desse tipo de processamento automatizado de dados pessoais? Eles poderiam gozar os direitos e salvaguardas para obter uma explicação sobre as mesmas?

consultar o caso completo em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=193042&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=2602823#Footref2 (acessado em 04/05 2021)

[142] Lynskey, O. – ***op. cit.***

CAPÍTULO IV – DIREITO À EXPLICAÇÃO NA DIRETIVA (UE) 2016/680

4.1. - Direitos extraídos do RGPD e LGPD

O tratamento automatizado de dados pessoais é uma realidade irrefreável que vem repercutindo de forma cada vez mais intensa na esfera individual de cada um. E isso tende a acontecer por conta do uso crescente da tecnologia nas atividades essenciais de empresas privadas e públicas.

Nesse momento, serão abordados, brevemente, quais os direitos avistáveis no âmbito do regulamento europeu e da lei geral do Brasil.

No cenário europeu, a regra geral é de uma proibição sobre a tomada de decisão exclusivamente com base no tratamento automatizado, incluindo a formação de perfis, que produza efeitos legais, adversos ou o afete similarmente a vida das pessoas de modo significativo (conforme art. 22.º, n.º 2, do RGPD e art. 11.º da Diretiva). Contudo, existem exceções para esta regra.

Os permissivos legais são aqueles previstos ao abrigo do art. 22º, n.º 2 (alíneas *a*, *b*, *c*)[143], desde que presentes os necessários mecanismos de salvaguarda (constantes no art. 22º, n.º 3 c/c considerando 71) que o tratamento exige, além dos casos em que esse tipo de decisão não seja suficiente para produzir efeitos em sua esfera jurídica ou afetá-lo significativamente de outro modo.

Nesses casos, deve-se instituir salvaguardas para efetivamente proteger os direitos e liberdades dos titulares de dados envolvidos, "designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão"[144].

De mais a mais, dentre outros, o titular tem ainda o direito, independentemente se os dados foram ou não facultados pelo mesmo, de receber *informações sobre a existência de decisões automatizadas, incluindo a definição de perfis,*

[143] São eles: a) quando necessária para a celebração ou a execução de um contrato; autorizada pelo direito da União ou do Estado-Membro e desde que previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; baseada no consentimento explícito do titular dos dados.

[144] MEDON, F.; MARRAFON, M. A. - **Importância da revisão humana das decisões automatizadas na Lei Geral de Proteção de Dados**

e obter informações úteis relativas: à lógica subjacente, à importância e às consequências previstas de tal tratamento (art. 13.º e art. 14.º).

Outrossim, o regulamento veda decisões tomadas exclusivamente com base no tratamento automatizado que se baseiem em categorias especiais de dados pessoais[145], exceto se o titular dos dados tiver consentido expressamente ou nos casos em que direito da UE ou Estado-Membro preveja que a proibição prevista no n.º 1, do art. 9. º, não possa ser anulada pelo titular dos dados (art. 9.º, n.º 2, alínea a). Também serão vedadas se o tratamento for necessário por motivos de interesse público relevante, fundado no direito da UE ou do Estado-Membro, devendo ainda ser proporcional ao objetivo visado, respeitar o direito à proteção dos dados pessoais e prever garantias adequadas e específicas que salvaguardem os direitos fundamentais e os interesses dos titulares dos dados (art. 9.º, n.º 2, alínea g).

A LGPD não é tão protetiva como o regulamento europeu e não proíbe as decisões unicamente automatizadas. Pelo contrário, a legislação permite o amplo uso dessas técnicas, desde que o controlador tenha estabelecido um sistema de salvaguardas, com direitos para os titulares de dados, dentre os quais se incluem a revisão[146], prevista expressamente no art. 20, do referido diploma legal.

Alguns direitos que podem ser invocados pelo titular de dados no contexto legal brasileiro são: livre acesso, que garante a consulta facilitada e gratuita sobre o tratamento (art. 6º, IV, LGPD); transparência, garantia de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e seus respectivos agentes (art. 6º, VI, LGPD); não discriminação, que proíbe tratamento com fins discriminatórios, ilícitos ou abusivos (art. 6º, IX, LGPD); qualidade dos dados, o qual assegura exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (art. 6, V, LGPD); e prestação de contas, que versa sobre responsabilização e demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância, a eficácia e o cumprimento das normas de proteção de dados pessoais (art. 6º, X, LGPD).

[145] Cfr. artigo 9.º, n.º 1, do RGPD: "que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa"

[146] MAGRANI, E. ; PERRONE, C.; SOUZA, C. A. O Direito à explicação entre a experiência europeia e sua positivação na LGPD. In: **Tratado de Proteção de Dados**

A lei brasileira não traz nenhuma disposição acerca da possibilidade do tratamento em comento com base em dados sensíveis, sendo esse um ponto a ser futuramente regulado pela ANPD.

4.2- Afinal, existe mesmo um direito à explicação?

Nas hipóteses permissivas da tomada de decisões automatizadas, o titular de dados pode ter direito a obter uma explicação sobre os motivos que levaram a determinado resultado?

Em síntese, o direito à explicação consiste no direito de receber informações que sejam suficientes e compreensíveis, possibilitando ao titular dos dados compreender a lógica utilizada nesse processamento e assim exercer seus direitos, caso queira. Ocorre que não há um consenso doutrinário se esse direito existe. A partir de agora, serão explanadas as principais teorias sobre o assunto.

4.3. Principais teorias quanto à existência do direito à explicação no RGPD

Muito se discute acerca da real existência do chamado "direito à explicação" na acepção do Regulamento Geral sobre a Proteção de Dados, enquanto uma corrente afirma que tal direito existe (Selbst; Powles[147] e Goodman; Flaxman[148]); outra corrente o nega, sustentando que o mesmo seria impraticável (Wachter; Mittelstadt; Florid[149]).

Os trabalhos mais proeminentes nesse debate interpretativo são, sem dúvidas, os dos autores Bryce Goodman e Seth Flaxman; as ideias de Sandra Wachter, Brent Mittelstadt e Luciano Floridi e os argumentados aventados por Andrew Selbst e Julia

[147] SELBST, A. D.; POWLES, J. - **Meaningful information and the right to explanation**
[148] GOODMAN, B; FLAXMAN, S. - **EU Regulations on Algorithmic Decision-Making and a "Right to an Explanation**
[149] WACHTER, S.; MITTELSTADT, B.; FLORIDI, L. - **Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation**

Powles. E esses artigos tem como marco normativo o regulamento europeu sobre proteção de dados.

Os estudiosos Bryce Goodman e Seth Flaxman, ainda que considerem os desafios técnicos oriundos da própria complexidade dos algoritmos, notadamente aqueles que empregam técnicas de aprendizado de máquina, insistem em defender a existência de um direito à explicação no bojo do regulamento, o qual seria decorrente da combinação dos seus arts. 13.º, 14.º e 15.º. Assim, explicitam a necessidade de serem fornecidas ao titular informações úteis quanto à lógica subjacente e quanto às consequências possíveis do tratamento de dados pessoais, juntamente com as salvaguardas dispostas no art. 22.º do mesmo diploma. O texto, apesar de trazer argumentos sucintos sobre o tema, foi o ponto de partida necessário para os debates sobre a questão.

Em contrapartida, os investigadores Sandra Wachter, Brent Mittelstadt e Luciano Floridi contestam a existência de tal direito, bem como a sua viabilidade na prática e afirmam que essa "omissão" no corpo do texto legal quanto a um possível direito à explicação fora intencional, no momento da elaboração do RGPD e que não existiria qualquer ambiguidade na linguagem de seu art. 22.º, o qual traz uma lista das salvaguardas oferecidas ao titular no bojo da tomada de decisões automatizadas, as quais são: obter intervenção humana; manifestar o seu ponto de vista e contestar a decisão.

O artigo então gerou grande polêmica ao negar a possibilidade de se extrair um direito à explicação da norma europeia, alegando que é permitido ao titular apenas um "direito a ser informado", de limitada extensão. Além disso, os autores argumentam que existem dois tipos de explicação: uma que precede a tomada da decisão automatizada (*ex ante*) e por isso diz respeito à funcionalidade do sistema; e outra que se relaciona aos motivos concretos que desencadearam aquela decisão individual específica, já tomada pelo algoritmo (*ex post*). Nesse ponto, os autores concluem, com fulcro nos arts. 13.º e 14.º do RGPD, que as informações ali mencionadas tratam somente sobre as funcionalidades dos sistemas.

Os outros personagens desse debate são Andrew Selbst e Julia Powles que, no artigo intitulado "*Meaningful Information and the Right to Explanation*", criticam essa conclusão de Wachter, Mittelstadt e Floridi e sustentam que existe a possibilidade de se extrair um direito à explicação do RGPD, amparado por seus arts. 13.º, 14.º e 15.º.

Afirmam que o direito de o usuário obter as informações sobre a lógica subjacente poderia ser interpretado, a favor da proteção ao titular de dados, *como* um direito

à explicação, permitindo que esse direito seja exercido de maneira funcional e flexível e que a explicação, para ser adequada, seja útil para a pessoa afetada pela decisão automatizada.

4.4. – Teorias no âmbito da LGPD

Renato Leite Monteiro escreveu um artigo, em dezembro de 2018, intitulado "Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?", no qual proclama a existência de tal direito no bojo da legislação brasileira.

A justificativa do autor é que, dentro do ordenamento jurídico brasileiro, tanto o Código de Defesa do Consumidor (Lei 8.078/90)[150], como a Lei do Cadastro Positivo (Lei 12.414/2011)[151] já reconheciam a possibilidade de os interessados terem acesso a informações sobre seus dados pessoais nos respectivos contextos e que esse direitos "formam a espinha dorsal do direito à explicação de decisões automatizadas em relações de consumo"[152].

Monteiro certifica ainda que

> quando houver decisão automatizada no contexto de uma relação de consumo, como a concessão ou não de um financiamento de veículo, por exemplo, o consumidor tem o direito de acessar os (seus) dados que basearam a tomada da decisão. Caso seja criada uma obrigação jurídica, é seu direito, também, ter conhecimento de suas finalidades e propósitos, seu alcance e como foi formada, incluindo critérios e valoração dos atributos utilizados para tomar a decisão. Em outras palavras, entender como se deu a formação da obrigação jurídica é essencial para a sua aceitação e

[150] No Código de Defesa do Consumidor a disposição estaria plasmada em seu artigo 43, que determina que o consumidor terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão e havendo inexatidão nos seus dados e cadastros, o consumidor poderá exigir sua imediata correção, sendo que todas as informações de que trata o artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

[151] O artigo 5º dessa lei preleciona que o cadastrado no bancos de dados com informações de adimplemento tem direito de: IV - conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial; V - ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais; VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; e VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados.

[152] MONTEIRO, R. L. – ***op. cit.***

> exercício dos direitos previstos no CDC. E isso inclui entender como um algoritmo deu origem a tal obrigação.[153]

Para consolidar ainda mais seu raciocínio menciona o entendimento do Egrégio Superior Tribunal de Justiça Brasileiro (STJ) que, no julgamento do RESP nº 1.304.736/RS estabeleceu um critério "que até então não encontrava respaldo na lei, possibilitando reconhecer a existência do direito à explicação de decisões totalmente automatizadas, desde que tais decisões tenham um impacto específico na vida das pessoas"[154]. Porém, o autor reconhece que essas leis são setoriais, regulando somente as relações que estejam em seu escopo de aplicação.

Sob a égide específica da Lei Geral de Proteção de Dados, Monteiro explicita que o princípio da transparência deve embasar toda a relação entre o responsável pelo tratamento e o titular dos dados pessoais, sendo garantido ao último o direito de acessar seus dados pessoais e pressupondo que essa informação verse sobre as finalidades e os critérios de tratamentos utilizados no tratamento de seus dados, tudo isso através de informações claras, precisas e acessíveis.

O entendimento de Monteiro é corroborado com maestria por outros grandes estudiosos no assunto como Magrani, Perrone e Souza[155] ainda complementam:

> Quanto à natureza da informação que deve ser apresentada ao titular, a LGPD novamente é similar ao GDPR. Enquanto no GDPR, como vimos, há a menção à 'informação útil' sobre a 'lógica subjacente' e a 'importância e as consequências previstas'; na LGPD, há referência a 'informações claras e adequadas" e "critérios e procedimentos utilizados'. É possível dizer que existem paralelos entre ambas as normas. 'Informações úteis' parece implicar um possível uso para atingir um determinado resultado, que, no caso, seria permitir o exercício dos outros direitos, como de apresentar os seus pontos de vista ou contestar. Similarmente, a expressão 'informação adequada' também passa a impressão de que a informação deve ser adequada para atingir um fim, que, no caso, é permitir ao titular exercer seus outros direitos, mormente solicitar a revisão da decisão.

[153] *Ibid.* p. 7
[154] MONTEIRO, R. L. – ***op. cit*** . p. 10
[155] MAGRANI, E.; PERRONE, C.; SOUZA, C. A. – ***op. cit***. p. 275

Os autores reforçam que explicar, de modo inteligível, ao titular de dados os critérios e procedimentos que foram utilizados na decisão não significa a divulgação de elementos técnicos, mas sim a prestação de informações suficientes para os titulares exercerem eficientemente os seus outros direitos, nomeadamente o pedido de revisão, previsto no art. 20, *caput*, da LGPD, já que, por lógica, seria impraticável o titular requerer a revisão sem conhecimento de como os dados foram processados e se houve alguma impropriedade nesse tratamento[156]. Por fim, fundamentam a existência desse direito nos arts. 9º, I e II[157]; 18, I e II[158]; e 20, § 1º[159], da LGPD.

Em resumo, no Brasil, o direito à explicação existe, ainda que a LGPD não aluda expressamente ao seu termo. E este pode ser extraído do princípio da boa-fé objetiva, bem como observado dos princípios da transparência, do livre acesso, da finalidade, da adequação e da finalidade.

A base legal se fundamenta no art. 20 da lei brasileira que determina que o titular de dados, de um lado, tem o direito de "solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade". De outro lado, é dever do responsável pelo tratamento "fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada", respeitando-se os segredos comercial e industrial.

---

[156] *Ibid.*

[157] Art. 9º. O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial;

[158] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados;

[159] Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

4.5 - Diretiva (EU) 2016/680 e Anteprojeto da LGPD Penal: Direitos

Assim como no Regulamento Geral sobre a Proteção de Dados, na Diretiva (UE) 2016/680 a regra quanto às decisões automatizadas também é a da proibição. Todavia, para que esta vedação incida na Diretiva os efeitos a serem considerados devem ser mais que meramente triviais e que estas decisões sejam aptas a produzir não apenas "efeitos na esfera jurídica" de um titular de dados, mas que esse efeitos sejam "adversos".

O GT29 aclara a situação citando o seguinte exemplo do que seria um *efeito adverso*: "a aplicação de medidas de segurança reforçadas ou de vigilância pelas autoridades competentes"[160]. Como *efeito bem significativos* ilustra o caso "em que não é autorizada a entrada de um passageiro a bordo pelo facto de este estar registado numa lista negra"[161]. Nessa linha, em ambas as ocasiões, esse modelo de decisões deve ser proibido.

A diretiva prevê uma única exceção à regra da proibição, nos moldes do art. 11º, n.º 1, no caso de essas decisões serem autorizadas pelo direito da União ou do Estado-Membro e desde que estes prevejam garantias adequadas dos direitos e liberdades do titular dos dados, ao menos o direito de obter a intervenção humana do responsável pelo tratamento.

As decisões automatizadas baseadas em dados sensíveis só podem ser tomadas se o Estado-Membro aplicar as medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular (art. 11.º, n.º 1 e n.º 2).

Ademais, uma das características do tratamento realizado nesse cenário é que o consentimento "nunca pode servir de base jurídica, uma vez que existe um claro desequilíbrio de poder entre o titular dos dados e o responsável pelo tratamento"[162].

No Anteprojeto da LGPD Penal, as decisões tomadas com base no tratamento automatizado de dados pessoais estão regulamentadas dos arts. 23 ao 26.

Logo na exposição de motivos, a comissão de juristas traz uma relevante preocupação quanto ao direitos dos titulares estarem "alinhados às tendências contemporâneas de regulação das decisões automatizadas, como o direito à proteção contra

[160] GT29, **WP258**. p. 14
[161] *Ibid.* p. 14
[162] *Ibid.* p 13

a discriminação e o direito à explicação de processos automatizados"[163]. Essa disposição é refletida no art. 25 do anteprojeto.

Caso esse dispositivo se mantenha numa possível lei futura acerca da proteção de dados pessoais em âmbito penal, isso aponta para um importante reconhecimento acerca das questões defendidas neste trabalho acadêmico, no sentido de efetivamente proteger o titular e trazer mais transparência, justiça e confiança no tratamento de seus dados.

No mais, outros dispositivos do anteprojeto apontam as hipóteses que deverão ser precedidas de autorização do Conselho Nacional de Justiça (no papel da autoridade supervisora prevista pelo documento); e/ou por publicação de relatório de impacto (art. 23, *caput)*[164]; e/ou autorizadas por lei, nos casos de tratamento automatizado que enseje um elevado risco para o titular (art. 24, *caput).*

O anteprojeto prevê ainda que o titular tem o direito de solicitar a revisão da decisão por uma pessoa natural. Veja-se que a comissão de juristas optou por manter a revisão da decisão automatizada por uma pessoa natural, o que, *per se*, já é deveras louvável, sobretudo considerando que a relevância dos direitos em jogo.

Além disso, o titular deve ser notificado da utilização de decisões automatizadas (art. 24, §4º do anteprojeto) e essas decisões não podem se basear em dados sensíveis, exceto os dados biométricos (art. 24, §5º), bem como, esses sistemas devem ser auditáveis, não discriminatórios e passíveis de comprovação sobre seu grau de precisão e acurácia (art. 25, *caput*).

Registre-se ainda que as informações prestadas pela autoridade competente devem ser claras e adequadas acerca dos critérios e dos procedimentos utilizados para a decisão automatizada (art. 25, §1º) e o CNJ poderá solicitar que sejam feitas auditorias com o intuito de verificar a precisão do algoritmo, a relevância dos fatores estatísticos e ainda se no tratamento automatizado desses dados pessoais existem vieses ou alguma forma de discriminação (art. 25, §2)º, sendo garantido ao titular a possibilidade de solicitar a

[163] Anteprojeto de LGPD-Penal, p. 4
[164] O relatório de impacto verificará as medidas tomadas para a garantia da não-discriminação e transparência, cujos parâmetros contemplarão o peso de dados pessoais, incluindo aqueles potencialmente capazes de revelar informações sensíveis, como situação socioeconômica e os dados relacionados à residência. Esses sistemas responsáveis devem ser auditáveis nos termos a serem determinados pelo Conselho Nacional de Justiça, porém considerados a precisão, a reprodutibilidade e disponibilidade de documentação acerca do seu funcionamento (cf. artigo 26 do anteprojeto).

revisão da decisão automatizada por uma pessoa natural (art. §3º) e ainda sendo proibida a adoção de medidas coercitivas ou restritivas de direitos tomadas exclusivamente com base em decisões automatizadas (art. 25, §4º).

4.6. Teoria possível de aplicação do Direito à Explicação na Diretiva (UE) 2016/680

Muito se debate acerca dos direitos existentes no âmbito das decisões automatizadas tomadas no contexto do Regulamento Europeu, porém as discussões acerca desses no ramo da Diretiva (UE) 2016/680 ainda são incipientes. Tal situação não deveria se justificar, mormente quando se considera a relevância dos direitos fundamentais que podem ser violados nesse contexto, como o direito à liberdade.

Um dos documentos que versam sobre a temática advém do Berkman Klein Center, produzido em conjunto por juristas, cientistas da computação e cientistas cognitivos[165], no qual referem que o termo explicação denota a descrição de um processo de decisão que pode ser interpretável por humanos e que deve possuir um conteúdo útil[166][167].

Os autores explanam que, para isso, "uma explicação deve permitir que um observador determine até que ponto um dado de entrada foi determinante ou influente na saída"[168], que é o resultado ou a decisão.

Outrossim, formulam que, para uma decisão ser explicada de forma compreensível, ela deve ser capaz de responder a pelo menos uma dessas questões: 1. Quais os principais fatores que foram levados em consideração na decisão? (*v.g.* se a raça do indivíduo foi sopesada numa acusação); 2. A alteração de determinado fator afetaria a decisão? (ou seja, qual o peso desse item para o resultado final?); e 3. Por que casos semelhantes resultaram em decisões diferentes? (essa resposta se relaciona à consistência e justiça das decisões)[169].

[165] DOSHI-VELEZ, F.; KORTZ, M. - **Accountability of AI Under the Law**. p 2 (tradução própria)
[166] *Ibid.* (tradução própria)
[167] Apesar do texto se debruçar acerca do instituto dentro sistema jurídico dos Estados Unidos, traz relevantes contribuições que podem servir de base para uma futura interpretação na diretiva e na pretensa lei brasileira que está por vir.
[168] DOSHI-VELEZ, F.; KORTZ, M. – ***op. cit.*** p. 5 (tradução própria)
[169] *Ibid.* (tradução própria)

Em 2018, Sandra Wachter, Brent Mittelstadt e Chris Russel (relembrando que os dois primeiros foram autores de artigo "Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation", já mencionado) submeteram um artigo de título "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR", no qual reiteram a ideia de que não existe no regulamento um direito à explicação juridicamente vinculativo, porém, levantam a hipótese de que, ainda que existisse, sua aplicabilidade seria restrita a situações específicas.

Os estudiosos reconhecem as dificuldades ligadas à complexidade do algoritmo, tanto em relação ao entendimento pelo titular, como por ser tecnicamente desafiador para os controladores e afirmam que, mais importante que abrir a caixa-preta da funcionalidade do sistema, é buscar mecanismos que permitam ao titular de dados pessoais não apenas a compreender a decisão, mas a exercer seus direitos.

Propõem como objetivos para uma explicação, que realmente auxilie os titulares, que essa: informe porque uma determinada decisão foi alcançada; forneça fundamentos para contestar as decisões que lhe são adversas; e permita perceber, com base no modelo atual de tomada de decisão, qual fator poderia ser alterado para que ele recebesse, no futuro, o resultado almejado.

Assim, sustentam que o modelo de explicação contrafactual incondicional seria o mais adequado no contexto das decisões automatizadas individuais, devendo ser aplicado de forma irrestrita, independentemente se as decisões em causa são unicamente automatizadas ou aptas a produzir efeitos, jurídicos ou significativos na esfera particular do titular.

Para facilitar o entendimento e clarificar a questão, o exemplo trazido pelos autores é o seguinte "Um empréstimo lhe foi negado porque sua renda anual é de £ 30.000. Se a sua renda fosse de £ 45.000, então, um empréstimo teria sido oferecido a você"[170].

Nesse exemplo simples, então, a decisão é a negativa do empréstimo e o contrafactual é a declaração posterior "de como o mundo teria que ser diferente para que um resultado desejável ocorresse"[171]. Ou seja, o direito teria se concretizado *se* a renda do sujeito do exemplo fosse de £ 45.000.

---

[170] WACHTER, S.; MITTELSTADT, B.; RUSSELL, C. -**Counterfactual Explanations Without Opening the Black Box**. p. 844 (tradução própria)
[171] *Ibid.* p. 845

Segundo o artigo, a literatura existente se preocupa muito em buscar uma explicação acerca da lógica do algoritmo ou de como o mesmo se relaciona com a decisão, o que, ainda que viável, não teria um valor prático para os titulares, ante a complexidade dos sistemas de aprendizado de máquina. Em vez disso, os contrafactuais teriam a vantagem, na visão dos autores, de fornecer informações sobre quais fatos externos podem interferir no resultado pretendido e o que seria necessário para alcançá-lo.

Essa é a sugestão também apresentada, em março de 2021, pelo Laboratório de Políticas Públicas e Internet na Nota Técnica sobre o Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Investigação Criminal[172].

4.7 – Subsídios para sustentar a existência do Direito à Explicação na Diretiva (UE) 2016/680

Tal como no regulamento geral, a Diretiva (UE) 2016/680 prevê uma gama de direitos aos titulares, dos quais se destacam: o art. 12.º, que prevê que o responsável pelo tratamento forneça informações como: identidade do responsável pelo tratamento e do encarregado; finalidades do tratamento; e existência do direito de solicitar acesso aos seus dados pessoais, bem como a sua retificação, apagamento e limitação do tratamento; e ainda efetuar comunicações (com uma linguagem clara e simples, inclusive por meios eletrônicos), dentre outras, acerca da existência de decisões individuais automatizadas.

Além do direito à informação, o art. 14.º preleciona que o titular dos dados tem o direito de confirmar a existência de tratamento de seus dados pessoais e, em caso afirmativo, acessá-los e ainda obter informações sobre as finalidades e o fundamento jurídico do tratamento; categorias dos dados; destinatários aos quais os dados pessoais foram

[172] "Uma sugestão de solução que poderia auxiliar no fornecimento de explicações é o uso de contra-fatos (counterfactuals), isto é, informações sobre que parâmetros deveriam ser alterados para que uma decisão fosse diferente". p. 21-22.
Ainda segundo a nota técnica, "deve ser objeto de escrutínio o funcionamento não só dos algoritmos, que variam de acordo com cada marca e modelo de software, mas também dos dados sobre os quais eles se apoiam para gerar as predições e do hardware que se utiliza para coletar novos dados. (já que existem no mercado atualmente várias empresas de IA que podem utilizar sistemas e algoritmos diferentes)" p. 18. Disponível em https://lapin.org.br/wp-content/uploads/2021/03/NT_APJ-para-Seguranca-Publica-e-Investigacao-Criminal.pdf

divulgados, além de poder solicitar ao responsável pelo tratamento a retificação, apagamento a limitação do tratamento dos dados pessoais.

O art. 16.º determina que os Estados-Membros permitam ao titular o direito de obter a retificação de seus dados pessoais, quando inexatos, e o direito de complementá-los, quando incompletos, inclusive por meio de declaração adicional. E não apenas isso, esse dispositivo prevê ainda o direito ao apagamento dos dados nos casos em que o tratamento infrinja princípios, licitude, verse sobre tratamento de categorias especiais de dados pessoais, ou tenham de ser apagados como cumprimento de uma obrigação legal a que o responsável pelo tratamento esteja sujeito.

O artigo ainda dispõe que, em vez de proceder ao apagamento, o responsável pelo tratamento pode limitá-lo, *v.g.* no caso de o titular dos dados contestar a exatidão dos dados pessoais e a sua exatidão ou inexatidão não puder ser apurada.

Uma das diferenças entre o Regulamento Geral e a Diretiva sob exame refere-se à extensão do direito de informação, de acesso e de retificação aos titulares de dados envolvidos no respectivo tratamento. A justificativa, por óbvio, encontra guarida no fato de, em âmbito penal, existe um nível, ainda que temporário, de sigilo intrinsecamente necessário às investigações e procedimentos penais, o que legitima a possibilidade de limitação desses direitos.

No mais, o art. 19.º da diretiva reforça a responsabilidade que o responsável pelo tratamento deve ter ao tratar dados pessoais, levando em conta sua natureza, âmbito, contexto e finalidades, além dos riscos de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas singulares, devendo aplicar medidas técnicas e organizativas adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com a diretiva.

Com essa elucidação esse trabalho acadêmico defende então que, apesar do léxico “explicação" não constar expressamente do corpo da lei, estando disposto apenas no Considerando 38 da Diretiva, sem força normativa, essas informações sobre os dados pessoais utilizados no tratamento e as possíveis consequência e impactos deste, a bem da verdade, consubstanciam-se num verdadeiro direito à explicação *lato sensu*, desde que, essas informações sejam significativas, úteis e suficientes a explicitar, de uma forma compreensível ao requerente, a lógica envolvida no processamento, bem como que permita

ao mesmo que obtenha intervenção humana, que possa expressar seu ponto de vista e que possa contestar a decisão.

Ora, se tem sido aceito, através de trabalhos hermenêuticos e principiológicos, a efetiva existência desse direito no seio do RGPD, não há como se esperar que seja diferente no bojo da Diretiva. Em outras palavras, se se pode aceitar a existência do direito à explicação num contexto de negação de um direito como o crédito, ante o resultado de uma decisão automatizada, imagine quando o impacto incorre na restrição da liberdade de um cidadão, cuja violação de direitos é latente e nefastas são as consequências para a sua vida.

Então, considerando que o escopo da Diretiva (UE) 2016/680 é a proteção dos dados pessoais dos titulares dentro de um contexto capaz de gerar impactos tão adversos em sua vida, seria ilógico negar-lhes o direito de receber uma explicação clara, concisa e suficiente acerca do resultado obtido, bem como dos dados utilizados e da lógica que envolveu o tratamento, além de poder requerer manifestar seu ponto de vista, contestar a decisão e obter intervenção humana.

Destarte, essa *clarificação* seria uma prerrogativa do titular com a finalidade de obter um tratamento justo, ético, e equitativo, evitando-se vieses, erros, discriminação, abusividade e, o mais grave, o cometimento de uma injustiça por parte do responsável pelo tratamento. Desse modo, o direito à explicação seria então o corolário, por excelência, do princípio da transparência.

Nesse sentido, como forma de garantir justiça, ética e transparência num cenário de proteção dos dados pessoais, além de uma efetiva segurança para o titular, com o fito de coibir a violação de suas liberdades e de seus direitos fundamentais

> [d]aí que tenhamos de criar novos meios de proteger a liberdade individual e os direitos de cidadania, num quadro jurídico de regras previsíveis e credíveis, capaz de assegurar o funcionamento dos mecanismos de impugnação das decisões individuais na base das quais se constrói a sua legitimidade[173]

[173] CALDAS, G. – O direito à explicação no Regulamento Geral sobre a Proteção de Dados. In: **Anuário de Proteção de Dados**

Ademais, imprescindível que haja garantias mínimas de segurança jurídica, não deixando os titulares dos dados à mercê de interpretações equivocadas e vulnerabilidades estruturais. A segurança jurídica se consubstancia na necessidade de motivação e fundamentação de decisões oriundas de esferas públicas, de modo a permitir à pessoa atingida avaliar se o processo decisório derivou-se de premissas conhecidas para a obtenção daquele resultado e, caso assim o queira, recorrer da decisão.

Nessa linha,

> A segurança jurídica implica a necessidade da publicitação das decisões jurídico-públicas, não podendo haver decisões de surpresa e para além disso, com a publicação, cumpre-se outra vertente da segurança jurídica, não já a da publicidade da regulação jurídica: a da clareza e da certeza do sentido dessa regulação, assim se tornando mais objetivas as fontes do Ordenamento Jurídico.[174]

Notadamente em relação às técnicas *machine learning* e outras formas de IA, um dos pontos desfavoráveis dessa delegação de decisões humanas para a máquina é que esta tem o *poder* de encontrar soluções para questões postas, cujo caminho percorrido até o desfecho pode não fazer sentido aos olhos de um observador humano. Assim, o que se defende é que, não desconsiderando as nuances da complexidade técnica envolvida, haja um modo de que as respostas automatizadas sejam explicáveis às pessoas que venham a ser afetadas pelos resultados.

Tomando por base os apontamentos de Frazão[175], sugere-se que as informações a ser fornecidas pelo responsável pelo tratamento ao titular dos dados pessoais sejam, pelo menos, essas:

> "(i) os dados que são coletados, de que fonte e de que maneira, (ii) quais as linhas gerais de programação dos algoritmos e seus objetivos, (iii) como se deu a programação e o desenvolvimento do algoritmo, (iv) se o algoritmo pode ou não modificar seu próprio código, (v) se tais modificações são previsíveis ou ao menos verificáveis, (vi) quais as categorias relevantes dos perfis e os critérios para cada uma delas, (vii) quais são os outputs do processo decisório e como avaliar a sua adequação e acurácia, (viii) se há mecanismos de feedback, (viii) se há intervenção

[174] BACELAR, J. G. – ***op. cit.***, p 95
[175] FRAZÃO, A. - **A nova Lei Geral de Proteção de Dados Pessoais**

> humana e em que nível, (ix) quais são os principais impactos e riscos para os titulares de danos, (x) que medidas foram tomadas para conter tais riscos.

E nesse ponto, mister asseverar que a explicação não deve ser meramente simbólica, sendo importante que as informações prestadas ao titular sejam sindicáveis, compreensíveis e o mais completas como possível, sob o risco de tornar letra morta todas as disposições expostas aqui.

4.8 – Importância da intervenção humana

Como é de fácil constatação esses sistemas dotados de inteligência computacional possuem uma linguagem complexa geralmente incompreensível e insindicável pelo homem comum, motivo pelo qual a aplicação de salvaguardas mostra-se fundamental para a proteção dos indivíduos afetados por essas decisões automatizadas.

Mister então que haja o aprimoramento de técnicas direcionadas a operacionalizar uma compreensível interpretação dos códigos produzidos pelos algoritmos e como realizar o controle dos mesmos. Assim, nos casos excepcionais em que esse tipo de decisão poderá ocorrer ele terá também o direito de, pelo menos, obter intervenção humana por parte do responsável e a possibilidade de manifestar seu ponto de vista e, se assim desejar, contestá-la, além de poder requerer uma explicação sobre a lógica subjacente da decisão.

No que pertine à possibilidade da intervenção humana, sua existência é tida por fundamental na ótica desta dissertação, tomando por base que

> "[e]xistirão situações nas quais o computador ficará impotente para realizar um processo dedutivo, exigindo a presença de agentes externos. Quando diversos sistemas lógicos devem ser utilizados, não haverá garantia de que a sua combinação (diferentes computadores em operação conjunta) resultará em decisões racionais. Não se consegue garantir consistência de um sistema formal. Daí a necessidade da presença de

> agentes externos. São eles quem deverão lidar com as situações conflitantes."[176]

Assim, a intervenção humana nesses sistemas automatizados tem a função de reduzir o que se chama de 'falsos positivos', sendo que, a inserção de um humano na revisão pode tornar o processo mais plural, ao passo que reforça a confiança do usuário nesse processo[177].

Desta feita, o direito à explicação e à intervenção humana são prerrogativas para o que o usuário dos dados pessoais obtenha uma decisão mais justa, transparente e equitativa, ou pelo menos, compreenda os motivos que envolveram a lógica subjacente da decisão, para querendo, expor seu ponto de vista e eventualmente apresentar uma contestação.

[176] VEGA, I. S. - Inteligência Artificial e tomada de decisão. In: **Inteligência artificial e Direito.** Posição RB-7-5 [livroeletrônico]
[177] MAGRANI. E; PERRONE. C.; SOUZA. C. A. – ***op. cit.***

CAPÍTULO V – ENTRE AS REGULAÇÕES JURÍDICAS E ÉTICAS

5-1- Regulação jurídica da IA

A ascensão de uma nova sociedade, tecnológica e transnacional, vem impactando as relações sociais e desafiando a própria essência do Direito, haja vista que a ligação entre Direito, ciência e tecnologia perpassa a análise fenomenológica "do risco, da incerteza e da insegurança que a ciência e inovação trazem consigo"[178].

E quando a sociedade muda o Direito deve evoluir conjuntamente para proteger as pessoas e ser capaz de regular, da perspectiva jurídica, as novas relações sociais formadas nessa nova sociedade, cujo epicentro de sua configuração é a tecnologia. Segundo leciona Abrusio[179]:

> a tecnologia enquanto ferramenta que impacta a relação social, deve ser levada aos debates jurídicos, os quais podem conduzir a entendimentos sobre sua ontologia que em breve se normatizam em forma de regras jurídicas. A lei, portanto, constrói a ontologia e a função da tecnologia incorporando em normas legais que se aplicam por sua vontade soberana.

Em contrapartida, o descompasso que há entre uma efetiva regulação pelo Direito e a fluidez da inovação gera insegurança jurídica e expõe as vulnerabilidades estruturais do sistema legal. Essa lacuna escancara a premente adaptação de todo o modelo jurídico a esses novos parâmetros impostos pelo momento atual vivenciado pela sociedade.

O que se observa é que, na corrida entre os programadores e os juristas, os primeiros avançam a larguíssimos passos na criação de novas técnicas, o que acarreta numa autorregulação do mercado tecnológico, e assim

> [e]m um cenário tecnorregulatório, no qual ferramentas tecnológicas não normativas dominam o ambiente regulatório, parecemos estar sujeitos à regra da tecnologia e não ao Estado de Direito. A tecnorregulação sinaliza o desaparecimento de nossa capacidade de argumentar e resistir, e, assim, pode resultar em um desvio ainda maior dos valores que nos tornam

[178] MOLINARO, C. A; SARLET, I. W. - Apontamentos sobre direito, ciência e tecnologia na perspectiva de políticas públicas sobre regulação em ciência e tecnologia. In: **Direito, inovação e tecnologia.** p. 99
[179] Abrusio, J. - ***op. cit***. p. 103

> humanos, afetando as esferas de verdade e justiça regidas pelo Estado de Direito.[180]

Dessa maneira, a autorregulação e a teoria do jusfilósofo norte-americano Lawrence Lessig de que "code is law", não podem subverter a lógica ético-jurídica, já que o Direito é quem devem regular as relações sociais e a tecnologia, e nunca o oposto. E apenas assim, consoante ensina Magrani, "o Direito, lastreado por um embasamento ético adequado, servirá como um canalizador do processamento de dados e demais materialidades tecnológicas evitando uma tecnorregulação nociva à humanidade"[181].

Quando então o Direito, regulador de comportamentos humanos, passa a regulamentar também a inovação tecnólogica a lei pode ser concebida como uma metatecnologia e assim a regulação buscada deve fluir a partir dessa perspectiva[182], construído sobre uma nova base normativa centrada no ser humano e incorporando valores sensíveis desde o seu desenho[183].

Mais a mais, considerando a grande importância dos dados pessoais para a sociedade moderna, bem como que hodiernamente muitas decisões que atingem a vida das pessoas advém de sistemas tecnológicos de inteligência artificial, calha asseverar a necessidade do reforço da aplicação das leis de proteção de dados pessoais, que também devem acompanhar avanço das novas tecnologias. As leis de proteção de dados acabam por ser um ponto de equilíbrio entre o desafio de se proteger os direitos fundamentais das pessoas e ao mesmo tempo permitir que a evolução tecnológica continue fluindo, dentro dos parâmetros legais.

Todavia, a mera conformidade com as leis é insuficiente para regular a questão, sendo imprescindível considerar a dimensão ética do processamento de dados, cabendo, como prelecionado por Magrani, ao Direito a construção dessas bases normativas éticas[184].

Considerando que a evolução da tecnologia, nomeadamente as de inteligência artificial com potencial de tomar decisões autônomas, só tenciona a aumentar, o

---

[180] MAGRANI, E - **Direito como metatecnologia**
[181] *Ibid.*
[182] *Ibid.*
[183] MAGRANI, E. - **New perspectives on ethics and the laws of artificial intelligence** (tradução própria)
[184] MAGRINI, E - Id.

objetivo deste capítulo é expor a necessidade de um debate sobre a ética dos algoritmos envolvidos em sistemas de decisões automatizadas, bem como algumas das iniciativas nesse sentido em andamento ao redor do mundo.

5-2- Riscos éticos que podem decorrer das decisões automatizadas

Mittelstadt [et. al] afirmam que algoritmos são eticamente desafiadores pela complexidade, incerteza e opacidade[185]. Cientes dessa questão, os autores então mapearam alguns problemas éticos que podem decorrer quando um algoritmo toma uma decisão que pode afetar a vida de um indivíduo. Para tanto, apontam possíveis preocupações a serem analisadas e, ato contínuo, defendem a adição da rastreabilidade nesse processo como uma preocupação "final e abrangente" a ser almejada[186].

O primeiro dos riscos indicados por Mittelstadt [et. al], são as "evidências inconclusivas". Essas são conclusões que os algoritmos extraem dos dados que lhe são fornecidos, mas que são apenas probabilidades e não certezas. Tomando por base um programa de predição, tal como os de pontuação expostos anteriormente, não há como se afirmar, com certeza, que as previsões desses sistemas se concretizarão.

Por exemplo, no caso citado no capítulo 3, Paul Zilly teve sua pena aumentada por ser considerado alguém com alto risco de se envolver em crimes no futuro. Essa é uma probabilidade que talvez venha a ocorrer num tempo futuro. Ou que talvez não se concretize na realidade, nunca ultrapassando sua hipótese de abstração.

Essas incertezas existem porque os algoritmos não têm como fazer inferências sobre diversos aspectos subjetivos do ser humano, e que poderiam afetar, ou não, o resultado final de uma decisão. O motivo para tanto é simples: esses sistemas funcionam com fórmulas matemáticas que trabalham sobre dados de entrada predefinidos (como o formulário do COMPAS).

Desconhecendo os aspectos subjacentes que envolvem a personalidade humana, não são capazes de atribuir valores a situações como a forma que uma base familiar afeta a personalidade de uma pessoa, como o desemprego abala um "pai de família", como

[185] Mittelstadt, B. D. [et. al]. **The ethics of algorithms**. p. 3 (tradução própria)
[186] *Ibid.* p 4-12

o arrependimento se manifesta após o indivíduo cometer um erro. Todas essas subjetivas incertezas podem interferir numa projeção comportamental.

Após, têm-se as "evidência inescrutáveis", ligadas à opacidade. Segundo os autores, essa opacidade ocorre quando a conexão entre os dados usados (ainda que conhecidos) e a conclusão oriunda da operação não é acessível, nem compreensível, havendo pouca, ou nenhuma, transparência no processo. Como solução, uma "combinação particular de abordagens" poderia mitigar essa questão, como auditorias (do código e do funcionamento dos algoritmos); utilização de alternativas mais transparentes, abertura dos códigos-fonte, sensibilização dos programadores, educação do público e regulação da matéria[187].

Já quando há uma "evidência má orientada", a preocupação cinge-se ao fato de que "as conclusões devem ser fiáveis quanto os dados em que se baseiam"[188].

Quanto aos "resultados injustos", tratam-se das consequências ou efeitos que uma decisão por algoritmos pode acarretar, inclusive, levando à discriminação. Os autores afirmam que várias são as razões para considerar os efeitos discriminatórios como adversos e, portanto, eticamente problemático, já que a discriminação contribui para estigmatizar grupos e excluí-los da participação social ativa[189].

Os "efeitos transformadores", tal como asseverado no texto, são a inserção dos algoritmos no cotidiano popular e o modo como os mesmos mudaram a forma como as pessoas veem o mundo e a si mesmas e como "podem representar uma ameaça à autonomia dos titulares dos dados."[190]

Por fim, o último risco mapeado e abordado pelos autores refere-se à rastreabilidade, a qual se relaciona com a detecção de danos e a responsabilização dos culpados.

[187] BURREL, J. - **How the machine 'thinks'.** p. 10 (tradução própria)
[188] MITTELSTAD, B. D. [et al] – ***op. cit.*** p. 5
[189] *Ibid.* p. 9
[190] *Ibid.* p. 9

5.3 - Desde a concepção

Como exposto, vários desafios éticos podem decorrer do uso dos algoritmos. Assim, uma abordagem possível no sentido de redução desses riscos seria a de implementar princípios éticos e justos desde a concepção do projeto de uma IA.

Nesse ponto, entende-se que, tal qual é amplamente aceito o conceito de *privacy by design* na proteção dos titulares dos dados pessoais, deve haver também uma extensão deste conceito para outros campos, como a ética e a equidade.

A ideia de *by design* ou "por desenho" ou "desde a concepção" está ligada às interfaces da própria arquitetura do projeto de tecnologia e já é aceitável quanto à questão da privacidade[191] e da própria proteção de dados pessoais[192], o que não impede uma ampliação do conceito para englobar as questões da ética e da justiça, tanto desde a concepção (*by design*), como por defeito, ou padrão (*by default*)[193].

[191] "*Privacy by design",* termo atribuído a então Comissária de Informação e Privacidade de Ontário, Canadá (1997-2014), Ann Cavoukian, denota em síntese, a ideia de que privacidade deveria ser incorporada, desde a concepção, em todos os projetos de tecnologia. Com o objetivo de proteger a privacidade do usuário do produto/serviço.

[192] Definida conceitualmente pelo Considerando 78 do RGPD como "A defesa dos direitos e liberdades das pessoas singulares relativamente ao tratamento dos seus dados pessoais exige a adoção de medidas técnicas e organizativas adequadas, a fim de assegurar o cumprimento dos requisitos do presente regulamento. Para poder comprovar a conformidade com o presente regulamento, o responsável pelo tratamento deverá adotar orientações internas e aplicar medidas que respeitem, em especial, os princípios da proteção de dados desde a conceção e da proteção de dados por defeito. Tais medidas podem incluir a minimização do tratamento de dados pessoais, a pseudonimização de dados pessoais o mais cedo possível, a transparência no que toca às funções e ao tratamento de dados pessoais, a possibilidade de o titular dos dados controlar o tratamento de dados e a possibilidade de o responsável pelo tratamento criar e melhorar medidas de segurança. No contexto do desenvolvimento, conceção, seleção e utilização de aplicações, serviços e produtos que se baseiam no tratamento de dados pessoais ou recorrem a este tratamento para executarem as suas funções, haverá que incentivar os fabricantes dos produtos, serviços e aplicações a ter em conta o direito à proteção de dados quando do seu desenvolvimento e conceção e, no devido respeito pelas técnicas mais avançadas, a garantir que os responsáveis pelo tratamento e os subcontratantes estejam em condições de cumprir as suas obrigações em matéria de proteção de dados. Os princípios de proteção de dados desde a conceção e, por defeito, deverão também ser tomados em consideração no contexto dos contratos públicos."

[193] Esse conceito decorre do "privacy by design" e "se refere à metodologia que adota por padrão a configuração de privacidade mais restritiva possível na fase da coleta de dados pessoais por qualquer sistema de tecnologia da informação, a fim de garantir a proteção dos dados pessoais de forma automática, ainda que nenhuma interação com a máquina tenha sido feita pelo usuário nesse sentido." (JIMENE, C. do V. – Reflexões sobre *privacy by design e privacy by default*. In: **Comentários ao GDPR**. posição 4424 [versão Ebook kindle])

5.3.1 – Ética *by design*

A implementação da ética *by design*, ou ética desde a concepção, seria uma mais-valia na garantia da transparência, confiança e da governança dos algoritmos computacionais. Por essa razão, Magrani sustenta a importância da regulação da ética *by design*[194], ou seja, a incorporação da ética e dos direitos humanos desde o momento em que uma Inteligência Computacional é projetada.

Corroborando essa assertiva, em recente discurso proferido, a atual Comissária para os Direitos Humanos do Conselho da Europa, Dunja Mijatović, afirmou que

> (...)
> A IA influencia as decisões que tomamos. Ela pode fortalecer nossas liberdades ou oprimi-las. Pode reforçar a participação ou se tornar uma ameaça à democracia. Pode empoderar as pessoas ou empurrá-las para a margem da sociedade. Cabe a nós conduzir a IA, e não o contrário.
>
> Para este fim, a estrutura de direitos humanos existente deve ser aplicada e as preocupações e direitos de todos colocados no centro do projeto, desenvolvimento e implementação de sistemas de IA. Isso se aplica tanto para as entidades públicas como para as do setor privado.
>
> Uma vez que é responsabilidade dos Estados respeitar, proteger e cumprir os direitos humanos de cada pessoa, é seu dever garantir que as empresas privadas que projetam, desenvolvem ou usam sistemas de IA não violem os padrões de direitos humanos.
>
> Isso pode acontecer ao se engajar mais resolutamente com as indústrias de tecnologia para torná-las conscientes da necessidade de incorporar os direitos humanos nos projetos de sistemas de IA e incentivá-las a avaliar o impacto desses sistemas sobre os direitos humanos. Uma conversa pública entre atores estatais, setor privado, academia, ONGs, mídia e cidadãos ajudaria bastante neste sentido.
>
> O Estado também deve reforçar o monitoramento da conformidade dos direitos humanos pelos sistemas de IA e agir sempre que esses direitos forem infringidos. Deve fortalecer a supervisão independente e capacitar as estruturas nacionais de direitos humanos a se engajarem nessa área também.

[194] Magrani, E. - **Direito como metatecnologia**

> Finalmente, eles devem promover a "alfabetização em IA" entre a população, e em particular nas escolas, para ajudar as pessoas a entender como funciona e reconhecer quando as prejudica. Para que isso aconteça, os Estados devem investir mais em iniciativas de conscientização pública, treinamentos e iniciativas de educação para desenvolver as competências de todos os cidadãos e colmatar as lacunas de conhecimento. Pode ser um investimento alto, mas com um enorme retorno para a democracia. [195].

Assim, a inclusão de uma forte base ética visa prevenir, na gênese, o surgimento de problemas éticos e trazer confiabilidade, transparência e segurança para os titulares dos dados.

Para que isso ocorra, a máquina deve compreender que cada ser humano tem em si um valor inerente e nesse ponto devem ser incutidos em seu sistema valores que reflitam o respeito à humanidade e à diversidade de raças, culturas e opiniões, prezando sempre por uma programação inclusiva, justa e não discriminatória.

Ademais, devem ser mapeados todos os resultados antiéticos encontrados para então corrigi-los, reforçando o aprendizado do sistema quanto a requisitos como igualdade, privacidade e justiça, de modo a buscar que esses resultados não afetem negativamente a vida pessoal e social, a autonomia, a liberdade e a dignidade humana, ou ainda a participação democrática desses titulares enquanto cidadãos.

Por essa razão, a supervisão humana, tal como já retratada, é essencial para garantir a conformidade com esses princípios, sendo essencial também que os programadores e suas equipes, ao desenhar um novo projeto sobre tais sistemas, estejam aptos para, além dos requisitos técnicos e busca de acurácia e precisão, vislumbrar potenciais resultados e impactos que essa tecnologia pode acarretar na vida das pessoas reais. Destarte, treinar esses desenvolvedores para "compreender aspectos éticos e morais de sua tomada de decisão, portanto, é fundamental."[196], ao passo que "na era dos algoritmos, os seres humanos nunca foram tão importantes"[197].

---

[195] Discurso proferido na conferência "Governing the Game Changer - Impacts of artificial intelligence development on human rights, democracy and the rule of law" em Helsínquia, Finlândia, no dia 26 de Fevereiro de 2019 (tradução própria)
[196] MENDES, L. S.; MATTIUZZO, M. – ***op. cit.,*** p. 26
[197] FRY, H. – ***op. cit.*** p 245

5.3.2 – Justiça *by design*

O aumento do uso da IA em diversas áreas, a exemplo do policiamento preditivo citado nesta dissertação, intensifica a necessidade da inclusão do ideal de justiça desde o desenho de uma arquitetura de IA. Isso tem a ver com o compromisso ético e social de garantir que a prestação do "serviço" realizado pela máquina seja justo e equitativo; verse sobre valores inclusivos; e respeite os direitos fundamentais e a dignidade humana.

Assim, os sistemas referenciados devem ser planejados para evitar vieses tanto nos dados de entrada como na concepção. Para isso, o desenvolvimento desses programas deve delimitar bem suas etapas para assegurar que os dados a serem incluídos sobre as pessoas sejam representativos, diversificados e inclusivos.

No mesmo sentido, deve-se avaliar se os dados de entrada selecionados tem algum potencial de causar danos, ou impactar de forma similar, a grupos vulneráveis de pessoas, causando uma indesejável exclusão, um tratamento desigual, discriminatório ou ainda uma estigmatização.

Além da etapa do projeto, o conceito também deve permear a fase de treinamento dos dados utilizados para ensinar a máquina, pois os mesmos também podem conter vieses decorrentes de injustiças e de preconceitos históricos.

Assim, o objetivo de introduzir a justiça desde o desenho do algoritmo é o de mitigar preconceitos, discriminações, reduzir estereótipos e evitar a exclusão social.

No mais, após o desenvolvimento de um *design* com esses requisitos, o sistema algorítmico deve ainda passar por constantes avaliações no sentido de validá-lo, verificá-lo e avaliá-lo.

Nibø chama a atenção ainda para o fato de que, assim como as decisões tomadas no passado influenciaram o presente, as decisões tomadas no momento atual impactarão as sociedades futuras, ao que chama justiça intergeracional. E complementa,

> Quando pensamos no impacto que certas decisões no presente podem ter no futuro, também devemos levar em consideração que aquilo que é considerado ético atualmente pode sofrer variações numa sociedade futura. Assim, a análise do que é desejável do ponto de vista ético deve partir da

> noção atual que temos sobre o que é ético e os possíveis impactos que ações e omissões da sociedade atual podem ter nas próximas gerações[198]

Por essa razão, cristalina a necessidade de uma reflexão séria acerca das ações e omissões decorrentes da era atual, sob a égide da justiça e da ética, posto que as decisões tomadas hoje influenciarão nas gerações futuras.

5.4- Inteligência Artificial Explicável (XAI)

É cediço que decisões inteligentes são complexas por natureza, seja humana ou artificial. Nesse ponto, surgem alguns questionamentos: é possível justificar de forma pormenorizada a decisão de um ser humano? O cérebro orgânico também não poderia ser tido como uma caixa preta? Há hipótese de destrinchar um pensamento humano para procurar vieses ou preconceitos (até mesmo inconscientes) e assim proceder a uma reprogramação mental de um indivíduo? A resposta é negativa. Então, qual seria a razão de tanta preocupação em conseguir criar máquinas cada vez mais dotadas de explicabilidade?

Ora, como explicitado no primeiro capítulo, o paradigma humano, em sede antropológica e sociológica, tem sido alterado a galope desde o advento da tecnologia. Muito se especula se a IA veio para substituir o homem em sua força de trabalho e em sua cognição.

Contudo, ainda que a performance de uma máquina seja, em muito, superior a de um homem, esta surgiu para auxiliar os seres humanos em suas mais diversas acepções. Desse modo, "a IA precisa ser pensada como ideia, algo que não seja apenas um substituto da mente humana, mas paralelo"[199].

Daí a vantagem de estimular soluções como a Explainable Artificial Intelligence (XAI) ou Inteligência Artificial Explicável. Segundo Almada mister que haja o

> estímulo a soluções tecnológicas, o que inclui tanto a chamada Explainable Artificial Intelligence (XAI) quanto o desenho de interfaces que apresentem a informação relevante de formas apreensíveis ao titular de dados, como a construção de visualizações dos fatores relevantes. As abordagens tecnológicas podem ou não ser combinadas, também, com a

[198] Nibø, E. - ***op cit***. p 146

[199] STEIBEL, F.; VICENTE, V. F; JESUS, D. S. V. de. - Possibilidades e potenciais da utilização da Inteligência Artificial. In **Inteligência artificial e Direito.** posição. RB-4.1 [livroeletrônico]

> abordagem jurídica de definir os requisitos legais de explicação de formas compatíveis com a capacidade cognitiva dos titulares de dados, como uma exigência de que sejam explicadas apenas as regras externas, que transformam as saídas computacionais em efeitos no mundo real.[200]

Assim, para o futuro, o que se espera dessa estratégia revolucionária é que

> Os novos sistemas de aprendizado de máquina terão a capacidade de explicar seus fundamentos, caracterizar seus pontos fortes e fracos e transmitir uma compreensão de como se comportarão no futuro. A estratégia para atingir esse objetivo é desenvolver técnicas de aprendizado de máquina novas ou modificadas que produzirão modelos mais explicáveis. Esses modelos serão combinados com técnicas de interface homem-computador de última geração, capazes de traduzir modelos em diálogos de explicação compreensíveis e úteis para o usuário final. Nossa estratégia é buscar uma variedade de técnicas a fim de gerar um portfólio de métodos que fornecerá aos futuros desenvolvedores uma gama de opções de design cobrindo o espaço comercial de desempenho versus explicabilidade.[201]

Dessa maneira, a resposta às perguntas anteriores converge para o fato de que é mais factível, ou ao menos é o que se espera num futuro relativamente próximo, que se consiga desvendar a caixa preta de uma máquina do que a de um ser humano. Um sistema de computador é objetivo, direto. Um algoritmo não irá "esconder" algo ou "inventar" uma mentira caso seu código-fonte esteja na iminência de ser aberto.

Ademais, há a possibilidade de a máquina ser programada para catalogar e documentar todos os processos e tratamentos de dados, pessoais ou não, nas diversas etapas de seu uso, gerando relatórios (que, por óbvio devem constar em linguagem clara e plausível de compreensão) acerca da funcionalidade do sistema e da forma como os dados, as inferências e as correlações se manifestam dentro do modelo.

---

[200] ALMADA, M. - **Cognição humana e a regulação de decisões automatizadas**. p. 3

[201] TUREK, M. - **Explainable Artificial Intelligence (XAI).** Disponível em: https://www.darpa.mil/program/explainable-artificial-intelligence (consultado em 01/06 2021) (tradução própria)

5.5 - Documentos

Em âmbito global, vários Estados e organizações, sensíveis a necessidade prover uma IA com mais ética, justiça, transparência e confiança, têm desenvolvido uma gama de documentos relevantes na busca de uma uniformização sobre o tema. Vejam-se alguns:

5.5.1 - Agencia Española de Protección de Datos

A Agência Espanhola de Proteção de Dados (Agencia Española de Protección de Datos) publicou no mês de fevereiro de 2020 um interessante documento acerca da temática, voltado para quem utiliza a IA em seus tratamentos, bem como desenvolvedores, encarregados e outros que forneçam suporte a tais tratamentos. [202]

O documento dispõe de um tópico para tratar da "proteção de dados e dimensão ética" que afirma que "a ética da IA deve proteger valores como dignidade, liberdade, democracia, igualdade, autonomia individual e justiça contra governo de um raciocínio mecânico." [203].

5.5.2 – Comissão Europeia

Em 21 abril de 2021, a Comissão Europeia apresentou sua mais nova proposta sobre novas regras e ações para promover a excelência e a confiança na inteligência artificial, "destinadas a transformar a Europa no polo mundial da inteligência artificial fiável"[204].

A proposta de regulamento visa o estabelecimento de regras harmonizadas sobre IA e possui os seguintes objetivos específicos: "assegurar que os sistemas de IA colocados no mercado da União e utilizados são seguros e respeitam legislação em vigor sobre direitos fundamentais e valores da União; assegurar segurança jurídica para facilitar o

[202] Agencia Española de Protección de Datos. "**Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial**". p. 2
[203] *Ibid.* p. 7
[204] Conforme comunicado de imprensa datado de 21 de abril de 2021

investimento e a inovação em IA; melhorar a governança e a aplicação eficaz das leis existentes sobre os direitos fundamentais e requisitos de segurança aplicáveis aos sistemas de IA; facilitar o desenvolvimento de um mercado único para aplicação de uma IA lícita, segura e confiável e evitar a fragmentação do mercado".[205]

O instrumento também visa assegurar um alto nível de proteção dos direitos fundamentais e traz uma abordagem sobre várias fontes de riscos, que devem ser bem definidas. Em relação aos sistemas considerados de alto risco, determina que são "estritamente necessários" o cumprimento dos seguintes requisitos: alta qualidade dos dados, documentação e rastreabilidade, transparência, supervisão humana, precisão e robustez, visando mitigar riscos aos direitos fundamentais e à segurança, quando não são cobertos por outros quadros jurídicos existentes[206].

No mais, seu Considerando 38 dispõe especificamente sobre o uso dos sistemas de IA pelas autoridades policiais, rotulando seu uso como de um grau significativo de desequilíbrio de poder que pode levar à vigilância, prisão ou privação da liberdade de uma pessoa natural, bem como outros impactos adversos. Esses sistemas devem ser treinados com dados de alta qualidade; atender aos requisitos de precisão ou robustez; e serem devidamente projetados e testados antes de serem disponibilizados para uso ou comercialização, já que podem ocasionar um tratamento discriminatório contra pessoas ou ainda, de outra forma, serem incorretos ou injustos.

Ainda segundo o dispositivo acima, o exercício de importantes direitos fundamentais processuais podem ser dificultados se não houver transparência, explicação das decisões e documentação. Consta ainda que esses sistemas devem ser precisos, confiáveis e transparentes, de modo a gerar confiança pública e garantir a responsabilização aquando da ocorrência de danos[207].

[205] European Comission. **Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts.** p. 4 (tradução própria)
[206] *Ibid.* p. 08
[207] *Ibid.* p. 27-28 (tradução própria)

5.5.3 – Relatório "Justice by algorithm – the role of artificial intelligence in policing and criminal justice systems"

Outro documento relevante é o Relatório "*Justice by algorithm – the role of artificial intelligence in policing and criminal justice systems*" da Assembleia Parlamentar do Conselho da Europa que reconhece as possíveis implicações éticas que podem ocorrer em decorrência do uso da IA no policiamento e no sistema de justiça criminal e propõe um projeto de resolução no qual uma futura regulamentação da IA contenha "princípios éticos fundamentais universalmente aceitos e aplicáveis", tais como: transparência, incluindo acessibilidade e explicabilidade; justiça e equidade; responsabilidade humana pelas decisões; proteção e segurança; e privacidade e proteção de dados[208].

5.6.Procedimentos de controle sobre sistemas de decisão automatizados

5.6.1 - Auditorias

A auditoria é um mecanismo relevante, de competência das autoridades de proteção de dados, no âmbito de seu poder de controle e fiscalização, consubstanciado para detectar impropriedades, inacurácias e vieses que podem causar riscos no tratamento de dados pessoais relativos à justiça, precisão, confiabilidade, segurança e direitos fundamentais.

A auditabilidade tem, pois, o condão de atestar conformidade, por isso sua aplicação não deve ser tomada de forma leviana, posto que esse instrumento "[é] uma peça chave dentro de um plano de governança de inteligência artificial explicável e confiável da empresa"[209]

Deveras a importância da aplicação dessas metodologias que a doutrina tem afirmado que sua prática, juntamente com as técnicas de *by design*, poderá ser considerada o novo "padrão ouro" para as empresas que trabalham com a implementação

[208] Cf. p. 1
[209] Abrusio, J. - ***op cit***. p 351

desses sistemas de aprendizado de máquina, seja dentro ou fora da UE[210].Saliente-se ainda que o uso desses métodos mostra-se relevante para detectar vieses algorítmicos em diversos setores[211], o que ajudaria a mitigar várias formas de discriminação.

No cenário brasileiro, dentro do contexto da LGPD, as auditorias serão levadas a cabo pela Autoridade Nacional de Proteção de Dados. Conforme determina o artigo 20, parágrafo 2º, da referida lei, em não sendo oferecidas as informações sobre os critérios e procedimentos utilizados para a decisão automatizada, resguardados os segredos comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Tal competência está expressa no artigo 55-J, inciso XVI, do mesmo diploma legal de cujo conteúdo ressai que cabe à ANPD "realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público".

O Anteprojeto da LGPG-Penal também dispôs sobre o assunto no bojo de seu artigo 25, o qual reverbera que "os sistemas responsáveis por decisões automatizadas a que se referem os artigos 23 e 24 devem ser auditáveis, não discriminatórios e passíveis de comprovação acerca de sua precisão e grau de acurácia", bem como que caberá ao Conselho Nacional de Justiça solicitar a realização de auditoria para verificação da precisão do algoritmo, da relevância dos fatores estatísticos ou da existência de vieses e aspectos discriminatórios no tratamento automatizado de dados pessoais (artigo 25, § 2º).

5.6.2 - Realização de avaliação de impacto

Sempre que um tratamento for suscetível de constituir um elevado risco para os direitos e liberdades dos titulares dos dados, devido à sua natureza, âmbito ou finalidades, deverá ser realizada, pelo responsável pelo tratamento, uma avaliação sobre esse impacto na proteção dos dados pessoais. Essa avaliação objetiva delimitar, antes da implementação do sistema, eventuais e potenciais riscos relacionados aos tratamentos de

[210] CASEY, B; FARHANGI, A.; VOGL, R. - **Rethinking Explainable Machines**
[211] *Ibid.*

dados, de modo a elucidar e antecipar de possíveis problemas técnicos, sendo um valioso instrumento de promoção da responsabilidade e transparência.

No âmbito europeu, calha relembrar que essa obrigação está disposta no artigo 27.º, n.º 1, da Diretiva (UE) 2016/680 e no artigo 35.º, n.º 1, do RGPD.

Tendo em vista a similaridade das redações, e tomando por base as orientações do GT29 no documento WP251, a realização dessas avaliações é vista como uma mais valia, além de ser considerada como uma garantia adequada, a qual deve ser feita com uma constante frequência. Essa feitura deverá ser levada a cabo pelo responsável pelo tratamento nos conjuntos de dados a serem tratados, com o fito de observar se existem enviesamentos, erros e imprecisões e devem ser realizadas de modo cíclico, desde a fase da concepção até enquanto ocorrer o processamento[212].

O GT29 recomenda também que os legisladores nacionais criem uma obrigação para que os responsáveis pelo tratamento realizem essa avaliação de impacto sobre a proteção de dados sempre que seu tratamento verse sobre a definição de perfis e dados sensíveis, ante o risco que podem implicar para os direitos e liberdades dos titulares dos dados.

No Brasil, a LGPD trouxe a previsão de um "Relatório de Impacto", contido em seu artigo 38. Porém, o dispositivo não elenca em quais hipóteses o controlador (o mesmo que responsável pelo tratamento) estaria obrigado a realizá-lo, ao que se aguarda que a autoridade brasileira edite a necessária regulamentação sobre a matéria.

Já o Anteprojeto da LGPD-Penal detalhou com muito mais precisão o que poderá ser o "Relatório de Impacto à Proteção de Dados" a ser efetivado dentro de seu escopo. Desse modo, prevê seu artigo 26 que o relatório de impacto que fundamentar decisões automatizadas deverá conter medidas que garantam a não-discriminação e a transparência e assegura que esses sistemas deverão ser auditáveis nos termos a serem determinados pelo CNJ e que não serão restringidos pelo segredo industrial e comercial (§ 2º). Por fim, elenca como parâmetros a serem considerados na auditoria, entre outros: a precisão, incluindo a taxa de falsos positivos ou falsos negativos; e a reprodutibilidade e disponibilidade de documentação acerca do seu funcionamento (§ 3º, incisos I e II).

[212] GT29 - **WP251rev.01**, versão em português

Por todo o exposto ao longo desse trabalho acadêmico, resta clara a necessidade de se discutir a elaboração de regulamentações e diretrizes, jurídicas e éticas, que devem suportar as decisões automatizadas, bem como que abranjam hipóteses de situações futuras, de forma a fazer parte do acervo legal da proteção dos dados pessoais, em consonância com os direitos humanos.

Estabelecer uma construção principiológica quanto aos princípios da ética desde a concepção e da justiça desde a concepção, que podem servir, tanto para mitigar possíveis efeitos negativos do uso das decisões automatizadas no âmbito penal, como para gerar confiança dos titulares nas decisões tomadas pela máquina. No que a esse último ponto, saliente-se a confiança infere diretamente na necessidade de transparência e prestação de contas (*accountability),* por parte do responsável

Ressalta-se que não foram abordadas aqui as formas técnicas de como esses princípios devem ser incorporados aos respectivos sistemas, posto que este trabalho cabe aos profissionais que lidam diretamente com a programação e desenvolvimento dessas tecnologias. O que se busca é incrementar o debate acerca do tema, buscando que essas tecnologias se pautem em parâmetros éticos, justos, democráticos.

Tal como no teste "Moral Machine" [213] a questão das máquinas autônomas é sempre delicada e demanda bastante reflexão ética, jurídica, filosófica e humana sobre quem deve ser priorizado numa possível situação de erro algorítmico: a sociedade já duramente vitimizada pela criminalidade ou as eventuais pessoas inocentes que podem ser vítimas de uma possível análise errada ou injusta pelo algoritmo. É uma conta difícil de fechar e que precisará ser parametrizada no campo da tecnologia, da ética e do Direito.

Ademais, no campo brasileiro ainda existem muitos pontos de extrema relevância que caberão a ANPD, a qual deverá definir diretrizes sobre os parâmetros técnicos que deverão ser adotadas visando sempre a preocupação com os direitos fundamentais.

[213]O teste, desenvolvido por pesquisadores do MIT, funciona como uma espécie de jogo no qual o jogador se depara com o dilema ético e moral de um carro autônomo que deve "escolher", no contexto de uma possível falha técnica do veículo, quem ele deve "matar", se os passageiros do veículos ou os pedestres no exterior do carro. O teste serve "para coletar a perspectiva humana em relação às decisões morais feitas pela inteligência das máquinas e está disponível em: https://www.moralmachine.net/hl/pt

CONCLUSÃO

É indubitável o grande impacto que a tecnologia vem causando na vida de todas as pessoas da sociedade atual. Parafraseando Alan Turing em sua icônica pergunta proposta pelos idos anos de 1950 se "as máquinas podem pensar", o debate atual é ampliado e surgem mais perguntas em relação a esses seres metálicos: elas também podem decidir? E mais, podem tomar decisões no lugar de seres humanos?

Essa reflexão ressoa, cada vez com mais intensidade, quando se observa o protagonismo que os algoritmos construídos pelos homens tem tido em diversos âmbitos do cotidiano popular: seja na área da saúde, dos carros autônomos, dos aplicativos de namoro que escolhem parceiros amorosos e sexuais ou até aqueles que decidem qual indivíduo será um potencial reincidente criminal. E assim, as máquinas passam a ter o *poder* de tomar decisões que impactam (ou impactarão) diretamente a vida das pessoas, podendo produzir efeitos na sua esfera jurídica ou ainda gerar efeitos adversos, sobretudo quando se consideram as decisões que podem afetar direitos fundamentais protegidos pelas constituições ao redor do mundo, como a liberdade.

O irrefreável tratamento automatizado de dados, dentre os quais se incluem os dados pessoais, é uma realidade que vem aumentando e hodiernamente essas técnicas tem crescido no cenário do policiamento preditivo e da justiça criminal. Nesse ponto, como dito anteriormente, grande parte dos substratos utilizados por esses programas são dados considerados de cunho pessoal, por isso é necessário assegurar o respeito, dentre outros diplomas, aqueles relativos à proteção de dados pessoais.

Ocorre que os algoritmos utilizados por esses sistemas são em sua grande maioria dotados de opacidade e, exatamente por isso, é necessário que se estabeleçam salvaguardas e se instituam direitos para proteger os indivíduos eventualmente impactados pelas decisões dos mesmos. Daí a relevância de que sejam introduzidos mecanismos de explicabilidade, responsabilização e transparência, podendo-se afirmar que, dentre os direitos que os titulares gozam para sua efetiva proteção, encontra-se o chamado direito à explicação das decisões automatizadas.

Esse trabalho conclui que o direito à explicação também deve ser amplamente reconhecido no contexto da Diretiva (UE) 2016/680, principalmente considerando a possibilidade de violações de direitos relativos à liberdade pessoal, motivo

pelo qual deve ser assegurado que os titulares dos dados, querendo, recebam uma explicação clara e suficiente acerca do resultado obtido, bem como dos dados utilizados e da lógica que envolveu o tratamento, além de terem direito a manifestar seu ponto de vista, contestar a decisão e obter intervenção humana.

Essa prerrogativa permitirá ao titular obter um tratamento justo, ético e equitativo, evitando-se a discriminação, abusividade e visando coibir injustiças, para assim proteger os direitos e liberdades fundamentais dos indivíduos. Ademais, cabe salientar que o modelo de explicação contrafactual incondicional seria o mais adequado no contexto das decisões automatizadas, tal como mencionado no capítulo quarto desta dissertação.

O tema é recente, técnico e desafiador, por isso, ainda é necessário o aprofundamento dos debates acerca de como os sistemas futuros poderão ser aperfeiçoados para permitir uma facilitação na correção de erros e vieses; para aprimorar técnicas direcionadas a operacionalizar uma compreensível interpretação dos códigos produzidos pelos algoritmos; além do modo como deverão ser introduzidas diretrizes éticas desde a concepção dos programas. Calha ressaltar os avanços importantes que tem surgido, como a recentíssima proposta de abril de 2021 da Comissão Europeia sobre novas regras e ações para promover a excelência e a confiança na inteligência artificial.

Assim, deve-se garantir que essas decisões tenham um viés ético, sendo reguladas tanto no campo jurídico e ético, de modo a garantir a transparência, justiça e equidade das mencionadas decisões.

BIBLIOGRAFIA

ABRUSIO, Juliana - **Proteção de Dados Pessoais na Cultura do Algoritmo.** Belo Horizonte: Editora D'Placido, 2020. 1ª edição. ISBN 978-65-5589-085-3

ALMADA, Marco - **Cognição humana e a regulação de decisões automatizadas**. EBICC: 2019. DOI:10.13140/RG.2.2.30134.86083. Disponível em: https://www.researchgate.net/publication/336444605_COGNICAO_HUMANA_E_A_REGULACAO_DE_DECISOES_AUTOMATIZADAS (consultado em 02/01 2021)

AMARO, António - Segurança humana e protecção civil na sociedade do risco: a crise do estatocêntrico na(s) segurança(s)**. Territorium: Revista Portuguesa de riscos, prevenção e segurança.** nº 15. 2008 . p. 83-94. ISSN: 1647-7723

ANGWIN, Julia ; LARSON, Jeff ; MATTU, Surya ; KIRCHNER, Lauren - **Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks**. ProPublica. 23/05/2016. Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (consultado em 30/09 2020)

ARISTÓTELES. **Política** - São Paulo, SP: Martin Claret, 2007. 6ª edição. Coleção a Obra-Prima de Cada Autor. ISBN-13 : 979-8572324563

BAHIA, Flavia - **Direito Constitucional**. Recife, PE: Armador, 2017. 3ª Edição. Coleção Descomplicando. Coordenação: Sabrina Dourado. ISBN: 978-8594830104

BECK, Ulrich ; GIDDENS, Anthony ; LASCH, Scott - **Modernização reflexiva: Política, tradição e estética na ordem social moderna**. Tradução de Maria Amélia Augusto. Oeiras: Editora Celta, 2000. ISBN 972-774-082-0.

BECK, Ulrich - **Sociedade de risco: rumo a uma outra modernidade**. Tradução de Sebastiao Nascimento. 2ª edição. São Paulo, 2013. ISBN: 13: 978-85-7326450-0.

BRAGA, Carolina Henrique da Costa - **Decisões automatizadas e discriminação: pesquisa de propostas éticas e regulatórias no policiamento preditivo.** Brasil: Universidade Estácio de Sá, 2019. Dissertação de mestrado. Disponível em: https://portal.estacio.br/media/4679621/carolina-henrique-da-costa-braga.pdf (consultado em 23/03 2021)

BRKAN, Maja - **Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond.** August 1, 2017. DOI; 10.1093/ijlit/eay017, Disponível em: http://dx.doi.org/10.2139/ssrn.3124901

BURGESS, Matt - **UK police are using AI to inform custodial decisions – but it could be discriminating against the poor**. 01.03.2018. Disponível em

https://www.wired.co.uk/article/police-ai-uk-durham-hart-checkpoint-algorithm-edit (consultado em 20/02 2021)

BURRELL, Jenna - How the machine ‘‘thinks’’: Understanding opacity in machine learning algorithms, in **Big Data & Society**, jan.-jun. 2016, p. 1-12. Disponível em: journals.sagepub.com/doi/pdf/10.1177/2053951715622512. (consultado em 09/10 2020)

CALDAS, Gabriela - O Direito à explicação no Regulamento Geral sobre a Proteção de Dados. Anuário 2019. In **CEDIS, 2019**: Universidade Nova de Lisboa, Faculdade de Direito. p. 37-53. ISSN 2184-5468

CANOTILHO, Gomes - **Direito Constitucional e Teoria da Constituição**. Coimbra: Almedina, 2002. 6ª edição.

CARVALHO, William Anderson Eloi de - **Vigilância das forças de segurança através de câmeras de reconhecimento facial e o conflito com o direito à privacidade – Brasil e Portugal**. Lisboa: Universidade Nova de Lisboa, 2019 Dissertação de mestrado. Disponível em: https://run.unl.pt/bitstream/10362/97545/1/Carvalho_2020.pdf (consultado em 05/05 2021)

CASEY, Bryan ; FARHANGI, Ashkon ; VOGL, Roland - **Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise.** Berkeley Technology Law Journal, Vol. 34, 2019. Disponível em: SSRN: https://ssrn.com/abstract=3143325 (consultado em 03/05 2021)

ČERKAA, Paulius ; GRIGIENĖA, Jurgita ; SIRBIKYTĖB, Gintarė - **Liability for damages caused by artificial intelligence**. Computer Law & Security Review. Vol 31. Nº.3. Junho de 2015. p. 376-389. Disponível em: https://doi.org/10.1016/j.clsr.2015.03.008 (consultado em 05/11 2019)

DONEDA, Danilo - **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2020. ISBN: 978-85-5321-904-9 [livroeletrônico]

DONEDA, Danilo - Panorama histórico da proteção de dados pessoais. In: **Tratado de proteção de dados pessoais**. Rio de Janeiro: Editora Forense, 2021. Coordenação de Laura Schertel Mendes [et. al.]. p. 21-40. ISBN: 978-85-309-9219-4 [versão eBook Kindle]

DOSHI-VELEZ, Finale ; KORTZ, Mason - **Accountability of AI Under the Law: The Role of Explanation**. Berkman Klein Center Working Group on Explanation and the Law, Berkman Klein Center for Internet & Society working paper. 2017. Disponível em: nrs.harvard.edu/urn-3:HUL.InstRepos:34372584 (consultado em 05/06 2021)

DUARTE, Felipe Pathé - Sociedade de risco. In: AAVV, **Enciclopédia de Direito e Segurança.** Coordenação de Jorge Bacelar Gouveia e Sofia Santos. p.451- 453. ISBN 978-972-40-5494.

EDWARDS, Lilian ; VEALE, Michael - **Enslaving the Algorithm: from a "Right to an Explanation" to a "Right to Better Decisions"?** IEEE Security & Privacy, 16(3), p. 46-54, 2018. DOI:10.1109/MSP.2018.2701152

FELLMETH, Aaron X. ; HORWITZ, Maurice - **Guide to Latin in International Law.** Oxford University Press, Oxford, 2009. p. 158. ISBN-13: 9780195369380.

FRAZÃO, Ana**. A nova Lei Geral de Proteção de Dados Pessoais**. 2019 Disponível em: http://www.professoraanafrazao.com.br/files/publicacoes/2019-10-28-A_nova_Lei_Geral_de_Protecao_de_Dados_Pessoais_Principais_repercussoes_para_a_atividade_empresarial_perspectivas_a_respeito_da_eficacia_do_direito_a_explicacao_e_a_oposicao_diante_de_decisoes_totalmente_automatizadas_Parte_XVII.pdf (consultado em 28/06 2021)

FRY, Hannah - **Olá Futuro: Como ser humano na era dos algoritmos**. Lisboa: Grupo Planeta, 2019. ISBN 978-989-777-291-7

GIDDENS, Anthony - **O Mundo na Era da Globalização**. Tradução de Saul Barata. Lisboa: Editorial Presença, 2006. 6.ª edição. ISBN: 972-23-2573-6.

GOODMAN, Bryce ; FLAXMAN, Seth - **EU Regulations on Algorithmic Decision-Making and a "Right to an Explanation**". AI Magazine, 38(3) pp. 50–57. Disponível em: https://doi.org/10.1609/aimag.v38i3.2741 (consultado em 13/06 2021)

GOUVEIA, Jorge Bacelar - **Direito da Segurança: cidadania, soberania e cosmopolitismo**. Coimbra: Almedina, 2018. ISBN: 978-972-40-7492-4

GUEDES, Armando Marques - Segurança Externa. In: AAVV, **Enciclopédia de Direito e Segurança**. Coordenação de Jorge Bacelar Gouveia e Sofia Santos. Coimbra: Almedina. 2015. p. 411-418 . ISBN: 9789724059945

GUEDES, Armando Marques ; SANTOS, Lino - Breves reflexões sobre Poder e Ciberespaço. In: **Revista de Direito e Segurança** (Direção de Jorge Bacelar Gouveia), n.° 6, Ano III. Julho/dezembro de 2015: CEDIS: Lisboa. p. 189-209. ISSN: 2182-8970

GUEDES, Armando Marques - Valor estratégico e económico dos cabos submarinos, in **Jornal da Economia do Mar**, 19 nº. especial de aniversário, 2018, pp. 9-12.

GUEDES, Armando Marques - Em rede. Os cabos de fibras ópticas submarinas e a centralidade portuguesa crescente num autêntico mar de conectividades**.** In: **Revista de Marinha, Especial**. Nº. 1000, Lisboa. p. 20-25.

HARARI, Yuval Noah - **Homo Deus - História Breve do Amanhã**.. Editora: Elsinore. 2018. 7ª Edição .ISBN: 9781784703936

JIMENE, Camilla do Vale - Reflexões sobre *privacy by design e privacy by default*: da idealização à positivação. In: **Comentários ao GDPR: Regulamento Geral de Proteção**

de Dados da União Europeia. Coordenação de Viviane Nóbrega Maldonado e Renato Opice Blum. São Paulo: Ed. RT, 2019, posição 4327-4694 [versão eBook Kindle]

KOBIE, Nicole - **Who do you blame when an algorithm gets you fired? When Uber's algorithm can put you out of a job, we need to think very carefully about the power they hold over our lives.** BUSINESS. 29.01.2016. Disponível em: https://www.wired.co.uk/article/make-algorithms-accountable (consultado em 12/05 2021)

LEONARDI, Marcel - **Tutela e Privacidade na Internet.** São Paulo: Saraiva, 2011, ISBN 978-85-02-00000-0

LYNSKEY, Orla - **Criminal justice profiling and EU data protection law: Precarious protection from predictive policing. International Journal of Law in Context**, 15(2), 2019. P. 162-176. DOI:10.1017/S1744552319000090. Disponível em: https://www.cambridge.org/core/journals/international-journal-of-law-in-context/article/criminal-justice-profiling-and-eu-data-protection-law-precarious-protection-from-predictive-policing/10FD4B64364191B619FBCB864CD40A7F (consultado em 03/04 2021)

MABEE, Carleton. - **Samuel F.B. Morse: American artist and inventor**. Encyclopedia Britannica. Última atualização em 23/04 2021. Disponível em: https://www.britannica.com/biography/Samuel-F-B-Morse (consultado em 01/05 2021)

MAGRANI, Eduardo ; OLIVEIRA, Renan Medeiros de - **Lei Geral de Proteção de Dados: reflexões sobre os desafios do consentimento e direito à explicação** (p. 80/89), In: Revista do Advogado. AASP. Ano XXXIX, n 144, novembro, 2019. ISSN-0101-7497

MAGRANI, Eduardo ; PERRONE, Christian.; SOUZA, Carlos Affonso - O Direito à explicação entre a experiência europeia e sua positivação na LGPD. In: **Tratado de proteção de dados pessoais**. Coordenação de Laura Schertel Mendes [et. al.]. Rio de Janeiro: Editora Forense, 2021. p. 254-282. ISBN: 978-85-309-9219-4 [versão eBook Kindle]

MAGRANI, Eduardo ; SILVA, Priscila ; VIOLA, Rafael - Novas perspectivas sobre ética e responsabilidade de inteligência artificial. In: **Inteligência Artificial e Direito: ética, regulação e responsabilidade**. Coordenação de Ana Frazão e Caitlin Mulholland. 1ª edição. São Paulo: Thomson Reuters Brasil, 2019. Posição RB-8.1 a RB-8.4 [livro eletrônico]ISBN: 978-85-5321-745-8

MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**.. Porto Alegre: Arquipélago Editorial, 2019. 2ª edição.o ISBN: 978-95-5450-029-0.

MAGRANI, Eduardo - **New perspectives on ethics and the laws of artificial intelligence.** Internet Policy Review. Journal on internet regulation, 8(3). 2019. Disponível em: https://policyreview.info/articles/analysis/new-perspectives-ethics-and-laws-artificial-intelligence. DOI: 10.14763/2019.3.1420 (consultado em 08/07 2020)

MAGRANI, Eduardo - **Direito como metatecnologia: A importância do "by design" em um mundo tecnorregulado**. 2019. Disponível em: https://www.cesar.org.br/index.php/2019/06/03/direito-como-metatecnologia-a-importancia-do-by-design-em-um-mundo-tecnorregulado/ (consultado em 03/09 2020)

MENDES, Laura Schertel - **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**.. São Paulo: Saraiva, 2014. 1ª edição ISBN-13: 978-8502218963

MENDES, Laura Schertel ; MATTIUZZO, Marcela - **Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia.** RDU, Porto Alegre, Volume 16, n. 90, 2019, p. 39-64, nov-dez 2019

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. - Proteção de Dados para além do consentimento: tendências de materialização. In: **Tratado de proteção de dados pessoais**. Coordenação de Laura Schertel Mendes [et. al.[. Rio de Janeiro: Editora Forense, 2021. p. 90-112. ISBN: 978-85-309-9219-4 [versão eBook Kindle]

MEDON, Filipe; MARRAFON, Marco Aurélio - **Importância da revisão humana das decisões automatizadas na Lei Geral de Proteção de Dados**. 2019. Disponível em: https://www.conjur.com.br/2019-set-09/constituicao-poder-importancia-revisao-humana-decisoes-automatizadas-lgpd (consultado em 03/05 2021)

MILARÉ, Édis - **Direito do ambiente: a gestão ambiental em foco: doutrina, jurisprudência.**. São Paulo: RT, 2011. 7ª edição. p. 113 ISBN: 9788520339183

MITTELSTADT, Brent ; RUSSELL, Chris ; WACHTER, Sandra - **Explaining Explanations in AI.** Proceedings of FAT* '19: Conference on Fairness, Accountability, and Transparency (FAT* '19), January 29–31, 2019, Atlanta, GA, USA. ACM, New York, NY, USA. doi/10.1145/3287560.3287574. ISBN: 978-1-4503-6125-5. Disponível em: SSRN: https://ssrn.com/abstract=3278331 (consultado em 06/06 2021)

MONTEIRO, Renato Leite. **Existe um direito à explicaçãona lei geral de proteção de dados do Brasil?** Artigo estratégico n. 39, p.1-14, dez. 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf (consultado em 19/07 2020)

MOURÃO, Carlos Eduardo Rabelo ; OLIVEIRA, Davi Teofilo Nunes - **Softwares de tomada de decisão e poder público: estudo de casos e efeitos regulatórios.** 2019. Disponível em: https://itsrio.org/wp-content/uploads/2019/03/Kadu-e-Davi.pdf (consultado em 19/12 2020)

MOLEIRINHO, Pedro - Policiamento orientado pelas informações. In: AAVV, **Enciclopédia de Direito e Segurança.** Coordenação de de Jorge Bacelar Gouveia e Sofia Santos. Coimbra: Almedina, 2015. p. 322-330. ISBN: 978-972-40-5494

MOLINARO, Carlos Alberto; SARLET, Ingo Wolfgang - Apontamentos sobre direito, ciência e tecnologia na perspectiva de políticas públicas sobre regulação em ciência e

tecnologia. In: **Direito, inovação e tecnologia** (Coordenação de Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Alexandre Zavaglia P. Coelho). São Paulo: Saraiva, 2015. v. 1.. p. 85-122. ISBN: 9788502227200

MULHOLLAND Caitlin.; FRAJHOF, Isabella Z. - Inteligência Artificial e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de machine learning. In: **Inteligência Artificial e Direito: ética, regulação e responsabilidade.** Coordenação de Ana Frazão e Caitlin Mulholland. 1ª edição. São Paulo: Thomson Reuters Brasil, 2019. Posição RB-13.1 a RB-13.6. ISBN: 978-85-5321-745-8 [livro eletrônico]

NOVAIS, Paulo ; FREITAS, Pedro Miguel. Inteligência Artificial e Regulação de Algoritmos. In: **Diálogos União Europeia – Brasil. 2018**. Disponível em: http://antigo.mctic.gov.br/mctic/export/sites/institucional/inovacao/paginas/politicasDigitais/assuntosCiberneticos/Inteligencia-Artificial-e-Regulacao-de-Algoritmos.pdf (consultado em 09/09 2020)

NYBØ, Erik Fontenele - **O Poder dos Algoritmos**. Enlaw, São Paulo: 2019. ISBN: 978-65-80484-00-3

OSWALD, Marion ; GRACE, Jamie ; URWIN, Sheena; BARNES, Geoffrey C. - **Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality, Information & Communications Technology Law**. 2018. 27:2, p. 223-250. DOI: 10.1080/13600834.2018.1458455

PASQUALE, Frank - **The Black Box Society: The Secret Algorithms That Control Money and Information**. Harvard University Press; 2015. ISBN-13: 978-0674970847

PURTOVA, Nadezhd**. "The law of everything. Broad concept of personal data and future of EU data protection law". 02 de abril de 2018**, Law, Innovation and Technology, 10:1, 40-81, (DOI:10.1080/17579961.2018.1452176). Disponível em: https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176 (consultado em 23/05 2021)

RODOTÁ, Stefano - **A vida da sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008. ISBN-13 : 978-8571476882

SANTOS, Lino - Ciberespaço. In: AAVV, **Enciclopédia de Direito e Segurança** (coordenação de Jorge Bacelar Gouveia e Sofia Santos). Coimbra: Almedina, 2015. p. 60-63. ISBN: 978-972-40-5494

SANTOS, Lino - Cibersegurança. In: AAVV, **Enciclopédia de Direito e Segurança** (coordenação de Jorge Bacelar Gouveia e Sofia Santos). Coimbra: Almedina, 2015. p. 63-67. ISBN: 978-972-40-5494

SCHWAB, Klaus. - **The Fourth Industrial Revolution.** Encyclopedia Britannica. Última atualização em 23/03 2021. Disponível em: https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734 (consultado em 06/04 2021)

SELBST, Andrew; POWLES, Julia. **Meaningful information and the right to explanation.** International Data Privacy Law, vol. 7, nº 4, p. 233-242, 2017. Disponível em: https://ssrn.com/abstract=3039125 (consultado em 07/05 2021)

SIBILIA, Paula - **O homem pós-orgânico: A alquimia dos corpos e das almas à luz das tecnologias digitais**. Rio de Janeiro: Editora Contraponto, 2015. 2ª edição revisada. ISBN 9788578661083.

SILVA, Nilton Correia da - Inteligência Artificial. In: **Inteligência Artificial e Direito: ética, regulação e responsabilidade.** Coordenação de Ana Frazão e Caitlin Mulholland. São Paulo: Thomson Reuters Brasil, 2019. 1ª edição. Posição RB-3.1 a RB-3.8. ISBN: 978-85-5321-745-8 [livro eletrônico]

SILVA, Porfírio - Sociedades artificiais: desafios e responsabilidades. In: **Fórum de Proteção de Dados,** n.4. Julho de 2017, Lisboa: Comissão Nacional de Protecção de Dados. p.12-25. ISSN 2183-5977

SIQUEIRA, Alessandra Cristina de Mendonça. - *Big Data* e justiça criminal: uso e implicações da análise massiva de dados no sistema judicial. In: **Direito Digital: Debates contemporâneos** (Coordenação: Ana Paula M. Canto de Lima; Carmina Bezerra Hissa; Paloma Mendes Saldanha). São Paulo: Thomson Reuters Brasil, 2019. 1ª edição. p. 83-93. ISBN: 978-85-5321-804-2.

SOLOVE, Daniel J. - **Understanding privacy**. Cambridge, London: Harvard University Press, 2008, ISBN-13: 978-0-674-02772-5

SOUZA, Erick RR - **Entenda Sobre Indústria 4.0: A Quarta Revolução Industrial que estamos vivendo Hoje!** AMAZON ASIN: B07K2D49RL. 2018. [versão eBook Kindle]

STEIBEL, Fabro ; VICENTE, Victor Freitas ; JESUS, Diego Santos Vieira de - Possibilidades e potenciais da utilização da Inteligência Artificial. In: **Inteligência Artificial e Direito: ética, regulação e responsabilidade**. Coordenação de Ana Frazão e Caitlin Mulholland. São Paulo: Thomson Reuters Brasil, 2019. 1ª edição. Posição RB-4.1 a RB-4.6 ISBN: 978-85-5321-745-8 [livro eletrônico]

TEGMARK, Max – **Life 30: Ser-se humano na era da Inteligência Artificial**. Tradução de João Van Zeller. Alfragide: Editora D. Quixote, 2019. ISBN 978-972-20-6833-8

TUREK, M. - **Explainable Artificial** Intelligence (XAI). Disponível em: https://www.darpa.mil/program/explainable-artificial-intelligence (consultado em 01/06 2021)

VEGA, Italo S - Inteligência Artificial e tomada de decisão – a necessidade de agentes externos. In: **Inteligência Artificial e Direito: ética, regulação e responsabilidade**. Coordenação de Ana Frazão e Caitlin Mulholland. São Paulo: Thomson Reuters Brasil, 2019. 1ª edição Posição RB-7.1 a RB-7.6 ISBN: 978-85-5321-745-8 [livro eletrônico]

VETTORAZZI, Karlo Messa ; BOTTINI, Julia de Mello - **A lei de proteção de dados e a inteligência artificial - A.Isplaining.** 2018. Disponível em: https://www.migalhas.com.br/depeso/286794/a-lei-de-protecao-de-dados-e-a-inteligencia-artificial---a-isplaining

VIVAS, Caroline - **LGPD e Poder Público: aspectos que você precisa compreender. Nextlaw Academy. Última atualização em** 22/10/2020. Disponível em: https://www.nextlawacademy.com.br/blog/lgpd-e-poder-publico-aspectos-que-voce-precisa-compreender (consultado em 01/05 2021)

WACHTER, Sandra ; MITTELSTADT, Brent ; FLORIDI, Luciano - **Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation (December 28, 2016).** International Data Privacy Law, 2017, Disponível em: http://dx.doi.org/10.2139/ssrn.2903469 (consultado em 22/04 2021)

WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris - **Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR (October 6, 2017).** Harvard Journal of Law & Technology, 31 (2), 2018, Disponível em: https://ssrn.com/abstract=3063289 or http://dx.doi.org/10.2139/ssrn.3063289 (consultado em 22/04 2021)

WARREN, Samuel D.; BRANDEIS, Louis D. **The right to privacy**. Harvard Law Review, v. 4, n. 5, p. 193-220, dez. 1890

WOLFORD, Ben - **What is the GDPR, the EU's new data protection law? GDPR.EU,** 2019. Disponível em: https://gdpr.eu/what-is-gdpr/

LEGISLAÇÃO, NORMAS E DOCUMENTOS

Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Investigação Criminal. Disponível em: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf (consultado em 29/04 2021)

Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción. Agencia Española de Protección de Datos. Disponível em: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf (consultado em 15/04 2021)

Alerta geral à nação sobre o nefasto anteprojeto da LGPD PENAL: o fim da prevenção e repressão a crimes no Brasil. ADEPOL do Brasil – Associação dos Delegados de Polícia do Brasil [et. al.] Brasília. 2020. Disponível em: https://images.jota.info/wp-content/uploads/2020/12/alerta-geral-contra-lgpd-penal-ult.pdf (consultado em 25/06 2021)

Assembleia Parlamentar do Conselho da Europa. Relatório "Justice by algorithm – the role of artificial intelligence in policing and criminal justice systems". Documento

disponível em: https://assembly.coe.int/LifeRay/JUR/Pdf/DocsAndDecs/2020/AS-JUR-2020-22-EN.pdf (consultado em 03/06 2021)

Carta Dos Direitos Fundamentais Da União Europeia. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf (consultado em 11/04 2021)

Código Civil Brasileiro (Lei n.º 10.406/2002). Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm (consultado em 15/04 2021)

Código de Defesa do Consumidor (Lei n.º 8.078/ 90). Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm (consultado em 15/04 2021)

CommDH/Speech(2019)1 - Speech at the High level conference "Governing the Game Changer - Impacts of artificial intelligence development on human rights, democracy and the rule of law" in Helsinki, Finland. 26 de Fevereiro de 2019. Disponível em: https://rm.coe.int/hlc-helsinki-feb-2019-commhr-intervention-final/16809331b8 (consultado em 15/12 2019)

Convenção 108. Disponível em: https://www.coe.int/en/web/data-protection/convention108/modernised (consultado em 11/04 2021)

Convenção Europeia dos Direitos do Homem. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf (consultado em 11/04 2021)

Convenção Americana sobre os Direitos do Homem. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm (consultado em 11/04 2021)

Constituição da República Portuguesa. Disponível em; https://dre.pt/legislacao-consolidada/-/lc/34520775/view (consultado em 30/03 2021)

Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm (consultado em 30/03 2021)

Declaração Universal dos Direitos Humanos. Disponível em: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf (consultado em 11/04 2021)

Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995. Disponível em: Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046 (consultado em 22/03 2021)

Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0680 (consultado em 22/03 2021)

Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais. Disponível em: http://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (consultado em 09/04 2021)

European Comission. Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts. Brussels, 21.4.2021, COM(2021) 206 final. 2021/0106 (COD). Documento disponível em: https://digital-strategy.ec.europa.eu/en (consultado em 29/06 2021)

Grupo de Trabalho do Artigo 29º.: "Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (Diretiva (UE) 2016/680)" Wp258. Disponível em: https://ec.europa.eu/newsroom/article29/items/610178/en (consultado em 15/04 2021)

Grupo de Trabalho do Artigo 29º.: "Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679" Wp251. Disponível em: https://ec.europa.eu/newsroom/article29/items/612053/en (consultado em 15/04 2021)

Grupo de ensino e pesquisa em inovação: Um Novo Mundo de Dados. Policy Paper. São Paulo: FGV, 2017. Coordenação de Alexandre Pacheco da Silva. p 7. (consultado em 09/02 2021). Disponível em https://www.academia.edu/36327945/Um_Novo_Mundo_de_Dados_Policy_Paper_2017_?email_work_card=view-paper (consultado em 18/04 2021)

Instituto da Defesa Nacional (IDN). IDN Cadernos: **Estratégia da Informação e Segurança no Ciberespaço**. Direção de Vitor Rodrigues Viana. Caderno nº 12. Imprensa Nacional – Casa da Meoda, Lisboa: 2013. ISSN 1647-9068. Disponível em: https://www.idn.gov.pt/pt/publicacoes/idncadernos/Paginas/IDN-Cadernos-12.aspx (consultado em 03/02 2021)

Lei n.º 59/2019. Disponível em: https://dre.pt/home/-/dre/123815983/details/maximized (consultado em 07/04 2021)

Lei Geral de Proteção de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm (consultado em 22/03 2021)

Lei do Habeas Data (Lei n.º 9.507/1997). Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9507.htm (consultado em 15/04 2021)

Lei de Acesso à Informação Pública (Lei n.º 12.527/ 2011). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm (consultado em 15/04 2021)

Lei do Cadastro Positivo (Lei n.º 12.414/2011). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm (consultado em 15/04 2021)

Marco Civil da Internet (Lei n.º 12.965/2014). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm (consultado em 15/04 2021)

Nota Técnica sobre o Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Investigação Criminal. Laboratório de Políticas Públicas e Internet. 2021. Disponível em: https://lapin.org.br/wp-content/uploads/2021/03/NT_APJ-para-Seguranca-Publica-e-Investigacao-Criminal.pdf (consultado em 03/06 2021)

Pacto Internacional relativo aos direitos civis e políticos. Disponível em: https://www.ohchr.org/documents/professionalinterest/ccpr.pdf (consultado em 11/04 2021)

Regulamento Geral sobre a Proteção de Dados. Disponível em: https://eur-lex.europa.eu/search.html?scope=EURLEX&text=gdpr&lang=en&type=quick&qid=1623798778442 (consultado em 22/03 2021)

Tratado da União Europeia (TUE). Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF(consultado em 09/04 2021)

Tratado sobre o Funcionamento da União Europeia (TFUE). Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF (consultado em 09/04 2021)

United Nations Development Programme (UNDP). Human Development Report. Oxford University Press, Oxford, 1994. Disponível em: http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf (consultado em 08/08 2020)

Sumário