XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

LITON LANES PILAU SOBRINHO

LUIZ ERNANI BONESSO DE ARAUJO

AIRES JOSE ROVER

FERNANDO GALINDO AYUDA

D597

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

Coordenadores: Aires José Rover; Fernando Galindo Ayuda; Liton Lanes Pilau Sobrinho; Luiz Ernani Bonesso de Araujo.

– Florianópolis: CONPEDI, 2022.

Inclui bibliografia
ISBN: 978-65-5648-629-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constitucionalismo, Desenvolvimento, Sustentabilidade e Smart Cities

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias.

XXIX Congresso Nacional do CONPEDI Balneário Camboriu - SC (3: 2022: Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

Direito, Governança e Novas Tecnologias.

O presente Grupo de Trabalho, baseia-se na problemática dos impactos das novas tecnologias, a partir de sua regulação, interferências e impactos da Governança. O objetivo do mesmo é ampliar as discussões e reflexões acerca das pesquisas realizadas sobre a temática com a finalidade de buscar a difusão do conhecimento científico para a melhoria e para o benefício da sociedade atual. O paradoxo das novas tecnologias e seus impactos no sistema jurídico vislumbram uma necessidade de readequação e mostram-se preocupantes, pois nos últimos anos a velocidade e a quantidade de acontecimentos observados no mundo inteiro dão um tom dramático à sensibilidade e impactos das novas tecnologias nas relações de governança e regulação. O desenvolvimento tecnológico tem trazido grandes avanços e, em contrapartida, uma insegurança em relação aos limites impostos as relações do sistema jurídico e da governança. Vivencia-se uma crise paradoxal, principalmente pela incerteza dessas relações. Com todos os avanços e o desenvolvimento de novas tecnologias na área jurídica e de governança, se está diante de um paradoxo, ou seja, o Estado cada vez mais reduzindo o investimento em pesquisas e deixando para a iniciativa privada dominar o campo das novas tecnologias. Assim, resta a dúvida de qual é o papel do Estado, uma vez que, em assim sendo, a sociedade fica à mercê do mercado. Nesse sentido, faz-se necessário repensar a dinâmica dessas relações. Outrossim, os trabalhos apresentados neste GT tratam dessas reflexões necessárias para o amadurecimento e para a assimilação de seus impactos. Os organizadores agradecem a todos os colegas pesquisadores e autores que contribuíram com seus excelentes trabalhos, estes que compõem esta publicação. Sendo assim, constata-se que houve comprometimento na investigação das mais diversas temáticas aqui trabalhadas, o que permitirá ao leitor uma leitura acurada e esclarecedora dessa obra.

GESTÃO DE RISCOS E IMPLEMENTAÇÃO DE RELATÓRIOS DE IMPACTO NO USO DE INTELIGÊNCIA ARTIFICIAL

RISK MANAGEMENT AND IMPLEMENTATION OF IMPACT REPORTING IN USING ARTIFICIAL INTELLIGENCE

Cristina Godoy Bernardo De Oliveira [1]
André Luis Vedovato Amato [2]
Marco Borges Papp [3]

Resumo

Discute—se os conceitos de inteligência artificial e algumas de suas implicações junto ao direito de Privacidade. Por meio de uma pesquisa bibliográfica e normativa, é realizada uma análise crítica a partir de Evgene Morozov dos impactos do uso das tecnologias digitais automatizadas para o desenvolvimento e para a privacidade. Para em seguida, discutir os limites normativos existentes no Brasil, utilizando do direito comparado para melhor compreensão dos conceitos tratados. Traz-se as definições de relatório de impacto e relatório de gestão de risco e alguns elementos que podem ser neles incluídos a partir da ideia de transparência e democraticidade. As conclusões e discussões trazidas são extraídas de forma dialética entre o debate trazido entre a descrição do contexto fático em contrapartida dos conceitos normativos. Subdivide—se em seis itens organizados em dois capítulos no total, sem incluir a introdução e as considerações finais. Identificou-se insuficiência de uma extensão normativa a fim de garantir uma preservação da privacidade dos dados em relação às inteligências artificiais.

Palavras-chave: Gestão de riscos, Cibersegurança, Relatório de impacto, Proteção de dados, Inteligência artificial

Abstract/Resumen/Résumé

The concepts of artificial intelligence and some of its implications for privacy law are discussed. Through a bibliographic and normative research, a critical analysis is made based on Evgene Morozov of the impacts of the use of automated digital technologies for development and privacy. Then, the existing normative limits in Brazil are discussed, using comparative law for a better understanding of the concepts dealt with. We bring the definitions of impact report and risk management report and some elements that can be

[1] Professora doutora da FDRP/USP. Doutora em Filosofia do Direito e Graduada pela Faculdade de Direito da USP. Coordenadora do Grupo de Pesquisa “Tech Law” do IEA/USP.. PI do C4AI-USP-IBM-FAPESP

[2] Advogado. Bacharel e Mestre em Direito pela Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo. Especialista em Direito Internacional e Estudos Diplomáticos.

[3] Graduando em Direito pela Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo.

included in them from the idea of transparency and democracy. The conclusions and discussions are extracted in a dialectical way between the debate brought between the description of the factual context in contrast to the normative concepts. It is subdivided into six items organized into two chapters in total, not including the introduction and the final considerations. Insufficient regulatory extension was identified in order to guarantee the preservation of data privacy in relation to artificial intelligences.

Keywords/Palabras-claves/Mots-clés: Risk management, Cybersecurity, Data protection, Impact reporting, Artificial intelligence

I. INTRODUÇÃO

Além das diferenças conceituais entre a privacidade e a proteção de dados, com importantes consequências dogmáticas, é necessário identificar as possíveis ameaças que o tratamento de dados por decisões automatizadas via ferramentas de inteligência artificial representa até mesmo para os direitos básicos de uma sociedade que se oriente pela tecnologia, haja vista os direitos de privacidade e a recente legislação para a proteção de dados.

Pelo presente estudo buscar-se-á a compreensão de conceitos-chave que expliquem o uso de inteligência artificial na sociedade brasileira em relação à União Europeia (Bioni et al., 2018). Para tanto, faz-se necessário compreender a interrelação entre técnicas e tecnologias que juntas são capazes de criar um novo paradigma no tratamento de dados pessoais pela automatização inteligente da definição de perfis de pessoas naturais.

Em um país como o Brasil, que ainda adota técnicas imaturas de *compliance digital*, a legislação específica para o tratamento de dados, a chamada Lei Geral de Proteção de Dados (LGPD), menciona vagamente a possibilidade de requisição de relatórios de impacto de proteção de dados – denominados pelo acrônimo RIPD – mas não define claramente as metodologias e procedimentos que devem ser adotados quando da elaboração desses relatórios. Ainda, como se não bastasse a indefinição dos RIPDs, a LGPD não determina a necessidade de elaboração de relatórios de impacto para programas alimentados por ferramentas de Inteligência Artificial. O Brasil carece ainda de regulamentação específica do uso de inteligência artificial nos âmbitos público e privado.

Dessa forma, busca-se, no presente trabalho, contribuir para uma melhor compreensão geral daquilo que deveria ser definido como relatório de impacto, além de buscar proporcionar um melhor entendimento quanto a importância de sua implementação como uma das formas mais eficazes e sólidas para a mitigação de riscos acerca do tratamento de dados por decisões automatizadas oriundas de Sistemas de Inteligência Artificial (SIA).

Para enfrentar esses problemas, o presente artigo se valerá de uma metodologia embasada na pesquisa bibliográfica por meio da utilização de fontes legislativas nacionais e internacionais, além de entendimentos e posicionamentos oriundos tanto de doutrina; notícias de jornal e revistas científicas; jurisprudência tanto pátria quanto alienígenas.

Em virtude da matéria aqui tratada sobre as correlações entre inteligência artificial, privacidade, proteção de dados, metadados, gestão de risco e *compliance*, serão empregados os métodos analítico e comparativo. No que tange ao método analítico, cumpre-se ressaltar que será realizada a análise crítica das fontes de pesquisa a serem utilizadas, observando-se de forma

detida cada um dos elementos integrantes do argumento central defendido no presente artigo. Já em relação ao método comparativo, será analisada principalmente a legislação atual sobre proteção de dados no Brasil, na União Europeia, precursora dessas normas, a fim de constatar as regulações acerca da prática de tratamento de dados por ferramentas alimentadas por Inteligência Artificial e os riscos gerados por eventuais lacunas normativo-legislativas, buscando verificar e identificar eventuais avanços em países que já tenham experimentado tentativas de adequação legislativa para suprir necessidades advindas de problemáticas envolvendo tratamento de dados e metadados por decisões automatizadas via Inteligência Artificial.

Para além da análise dos questionamentos anteriores, é imperioso esmiuçar os conflitos e desafios regulatórios, legislativos, para assim compreender se há a necessidade de implementação de políticas públicas tanto no setor público quanto no setor privado. Produzindo como resultados esperados uma consequente categorização e listagem de riscos potenciais trazidos pelo uso dessas técnicas num cenário atual de incipiente - e insuficiente - regulamentação das arquiteturas dos programas movidos por ferramentas de inteligência artificial, dado que preceitos fundamentais de privacidade e transparência no tratamento automatizado de dados são diretamente afetados e, possivelmente, violados em virtude da dificuldade de rastreamento das “pegadas digitais” escondidas por trás dos processos das arquiteturas utilizadas em ferramentas de inteligência artificial.

II. DESENVOLVIMENTO

1. Cibersegurança e a Gestão de Riscos no uso de IA

Os sistemas de inteligência artificial[4] (Haugeland, 1985)possuem caráter altamente imprevisível e, nas avaliações de risco, torna-se complexo avaliar o risco que uma decisão automatizada ou advinda diretamente do uso de tecnologias cuja arquitetura se baseia em técnicas de *machine learning*[5] (Mitchell, 1997) poderia acarretar em situações específicas, potencializando a possibilidade de catástrofes em que pese as possíveis violações diretas aos direitos e liberdades fundamentais dos titulares de dados. Assim, compreende-se que as ferramentas *risk-based* devem abordar de maneira escalável e proporcional para o controlador em prol do *compliance* contínuo. Isto é, quanto maior for o risco que determinado processamento de dados poderá vir a oferecer de acordo com a amplitude de eventos que se pode prever em determinada arquitetura de *software* que baseie suas decisões por inteligência artificial, maior será a necessidade da avaliação de riscos por meio do RIPD pelos controladores. Portanto, o nível de obrigação de prestação de contas deve estar atrelado ao risco que a atividade acarreta.

Nesse sentido, extraindo-se dos princípios da segurança, da prevenção e da responsabilização e prestação de contas presentes no artigo sexto[6], a sistemática da LGPD preconiza a obrigação de implementação de medidas de segurança que resguardem os direitos do titular de dados a partir da documentação das atividades de processamento, independentemente do nível de risco da operação. Assim, a pergunta que surge é: se o fator *"alto risco ao titular"* determinaria a escalabilidade de obrigação de adequação à lei que o controlador de dados deve se submeter, qual seria, então, a forma de identificação desses riscos para que possam ser devidamente avaliados e mitigados? A resposta prevista em legislação seria a avaliação de impacto, gênero no qual a RIPD é espécie.

---

[4] Pela definição da OCDE (2019), inteligência artificial é "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy".

[5] Pode-se definir o uso de técnicas de *machine learning* (Salloum et al., 2020) pelo seu objetivo principal, qual seja, o desenvolvimento de modelos que recebem dados de entrada (*input data*) para, utilizando análises estatísticas, prever um valor de saída (*output value*) dentro de um intervalo adequado. Seus algoritmos podem ser classificados pela aprendizagem a) supervisionada; b) não supervisionada e c) reforçada. Ainda, como subdivisões adicionais dos algoritmos supervisionados, que são os mais utilizados, existem os por regressão e por classificação.

[6] Conforme previsão legal no artigo 6º, incisos VIII e X, que versam, respectivamente, sobre a "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais" e a "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

Assim, pode-se inferir, em consonância com a legislação brasileira vigente, que um dos indicadores demonstrativos de conformidade à lei apontados como ferramenta pela LGPD é a análise sistemática através da confecção de relatórios de impacto à proteção de dados. Todavia, a confusão teórica entre o que se qualificaria como risco e o que seria, por essência, uma violação direta faz com que a análise de risco seja postergada para fase posterior à avaliação de impacto. Essa negligência é também razão para o enfraquecimento dos mecanismos de prevenção e de mitigação de danos aos titulares de dados.

É notável, portanto, que a negligência ao relatório de impacto e à análise de risco vem da imaturidade dos agentes de tratamento em tratar tais ferramentas como meras burocracias e, portanto, ao não as fazer ou ao fazê-las a partir de documentações operacionais inconclusivas, incongruentes e incompletas. Essa negligência, por sua vez, reflete a incipiência do processo de aprendizado desses agentes em relação à governança de dados (Stirling, 2016).

A necessidade primeira e a finalidade última do relatório de impacto é conceber, a partir da documentação e análise dos tratamentos de dados realizados, um instrumento efetivo de governança de dados que propicie um solo fértil e seguro para que haja cada vez mais tomadas de decisões futuras mais seguras, previsíveis e potencialmente menos danosas, principalmente em se tratando de decisões automatizadas. Portanto, a cultura de análise de risco e de confecção de relatório de impacto deverá consistir no balizamento perene de um desenvolvimento saudável do uso de dados no Brasil pela atualização constante dos relatórios de impacto durante todo o percurso do processo de implementação de tecnologias de inteligência artificial que produzam decisões automatizadas no tratamento de dados em todo e qualquer setor da sociedade, seja ele privado ou público.

1.1 Algumas Definições sobre Inteligência Artificial

Devemos compreender a Inteligência Artificial como uma forma de autoprogramação que busca captar o máximo de recursos informacionais possíveis a fim de se aperfeiçoar, objetivando o maior número de estatísticas, interpretando o mundo de maneira racional e assim realizar seus objetivos finais, por meio de um processo conhecido como "*deep learning*"[7] —

[7] Pode ser definido (Lecun et al., 2015) como técnica que permite modelos computacionais compostos por múltiplas camadas de processamento a aprender representações de dados com múltiplos níveis de abstração. São utilizados para incrementar ferramentas de reconhecimento de voz, reconhecimento visual de objetos, detecção de objetos e diversos outros domínios. O *deep learning* tem a capacidade de descobrir estruturas intrincadas em grandes conjuntos de dados, utilizando o algoritmo de retropropagação para indicar como uma máquina deve alterar os seus parâmetros internos quando são utilizados para calcular a representação de determinada camada a partir da sua representação na camada anterior.

que busca assemelhar-se ao processo cognitivo humano (COZMAN, PLONSKI, NERI, 2021). É dizer, através da captação de recursos ou na análise de dados constantemente mutantes busca a conclusão de objetivos pré-estabelecidos e programados, de forma que possibilita que máquinas aprendam com experiências, se ajustem a novas entradas de dados e performem tarefas como seres humanos.

Com a exponencial expansão das capacidades computacionais e das análises computacionais, a aplicação e o desempenho dos algoritmos igualmente evoluem, permanecendo em constante mudança ao longo dos anos. Nisso, o esforço para a reprodução digital de estruturas de decisão similares às humanas pelo uso das chamadas "redes neurais artificiais" vem para programar um computador de tal maneira que os problemas possam ser processados de forma independente.

Usa-se a inteligência artificial, *e.g.*, como incremento em sistemas de busca, em plataformas de desempenho, em reconhecimento facial e oral, em diagnósticos e terapias médicas, em sistemas de produção ciberfísica, no setor militar e em decisões administrativas ou judiciais automatizadas. Ainda, novas formas de monitoramento e pesquisa sobre condições de vida e controle do comportamento são concebidas a partir do desenvolvimento de sistemas de análise e tomada de decisão que se baseiam em algoritmos que trabalham a partir de procedimentos, ferramentas e técnicas centradas na inteligência artificial.

Segundo a proposta apresentada para o Regulamento Europeu sobre Inteligência Artificial[8], podemos extrair a definição de Sistema de Inteligência Artificial como sendo um programa informático desenvolvido com uma ou várias das técnicas e abordagens[9], compreendidas como abordagens de aprendizagem automática, incluindo aprendizagem supervisionada, não supervisionada e por reforço, utilizando uma grande variedade de métodos,

[8] A proposta visa responder pedidos explícitos do Parlamento Europeu e do Conselho Europeu, que apelaram de forma reiterada em prol de uma ação legislativa, com a finalidade de assegurar o bom funcionamento do mercado interno de sistemas de inteligência artificial, no qual os benefícios e os riscos da IA sejam abordados de forma adequada a nível da União Europeia para que esteja na vanguarda mundial do desenvolvimento de uma inteligência artificial que seja segura, ética e de confiança.

[9] Conforme texto original da Comissão Europeia: "A proposta tem por base os atuais quadros jurídicos e é proporcionada e necessária para alcançar os objetivos a que se propõe, uma vez que segue uma abordagem baseada no risco e impõe encargos regulamentares apenas quando é provável que um sistema de IA represente riscos elevados para os direitos fundamentais e a segurança. Por outro lado, no caso dos sistemas de IA que não são de risco elevado, apenas são impostas obrigações de transparência bastante limitadas, por exemplo, no que diz respeito à prestação de informações para sinalizar a utilização de um sistema de IA quando este interage com seres humanos. No caso dos sistemas de IA de risco elevado, os requisitos relativos à elevada qualidade dos dados, à documentação e à rastreabilidade, à transparência, à supervisão humana, à exatidão e à solidez são estritamente necessários para atenuar os riscos para os direitos fundamentais e a segurança colocados pela inteligência artificial e que não abrangidos por outros quadros jurídicos existentes. As normas harmonizadas e as orientações de apoio, bem como as ferramentas de conformidade, auxiliarão os fornecedores e os utilizadores no cumprimento dos requisitos estabelecidos pela proposta e na minimização dos seus custos."

designadamente aprendizagem profunda; abordagens baseadas na lógica e no conhecimento, nomeadamente representação do conhecimento, programação (lógica) indutiva, bases de conhecimento, motores de inferência e de dedução, sistemas de raciocínio (simbólico) e sistemas periciais; assim como as abordagens estatísticas, estimação de Bayes, métodos de pesquisa e otimização, que podem ser capazes de, tendo em vista um determinado conjunto de objetivos definidos por seres humanos, criar resultados, tais como conteúdos, previsões, recomendações ou decisões, que influenciam os ambientes com os quais interage.

Dentre as razões[10] apresentadas para o referido regulamento encontra-se o estabelecimento de regras harmonizadas em matéria de inteligência artificial, compreendida como uma família de tecnologias em rápida evolução capaz de oferecer um vasto conjunto de benefícios econômicos e sociais a todo o leque de indústrias e atividades sociais.

Ao melhorar as previsões, otimizar as operações e a afetação de recursos e personalizar o fornecimento dos serviços, a utilização da inteligência artificial pode contribuir para resultados benéficos para a sociedade e o ambiente e conceder vantagens competitivas às empresas e à economia europeia. Essa ação torna-se especialmente necessária em setores de elevado impacto, incluindo os domínios das alterações climáticas, do ambiente e da saúde, do setor público, das finanças, da mobilidade, dos assuntos internos e da agricultura.

Contudo, os mesmos elementos e técnicas que produzem os benefícios socioeconómicos da IA também podem trazer novos riscos ou consequências negativas para os cidadãos e a sociedade (Weinberger, 2021). desenvolvendo um ecossistema de confiança mediante a proposta de um quadro jurídico para uma IA de confiança. A proposta tem como base os valores e os direitos fundamentais da UE e pretende dar às pessoas e a outros utilizadores a confiança necessária para adotarem soluções baseadas em IA, ao mesmo tempo que incentiva as empresas para que as desenvolvam. A inteligência artificial deve ser uma ferramenta ao serviço das pessoas e uma força positiva para a sociedade com o objetivo final de aumentar o bem-estar dos seres humanos.

[10] O Regulamento justifica sua proposta de estabelecimento de regras harmonizadas pelo fato de que a proposição "torna-se especialmente necessária em setores de elevado impacto, incluindo os domínios das alterações climáticas, do ambiente e da saúde, do setor público, das finanças, da mobilidade, dos assuntos internos e da agricultura. Contudo, os mesmos elementos e técnicas que produzem os benefícios socioeconómicos da IA também podem trazer novos riscos ou consequências negativas para os cidadãos e a sociedade. À luz da velocidade da evolução tecnológica e dos possíveis desafios, a UE está empenhada em alcançar uma abordagem equilibrada. É do interesse da União preservar a liderança tecnológica da UE e assegurar que novas tecnologias, desenvolvidas e exploradas respeitando os valores, os direitos fundamentais e os princípios da União, estejam ao serviço dos cidadãos europeus."

Há pesquisadores como Evgeny Morozov[11] (2018, p. 150) que alertam para algo negativo deste processo. a partir de uma profunda transformação na lógica econômica operada *em função de impressionantes avanços num dos rumos da inteligência artificial* que implica na necessidade de se encontrar maneiras de extrair enorme volume de dados, muitas vezes a partir de atividades periféricas às principais atividades, envolvendo pessoas em captação inadvertida de dados para operação e desenvolvimento de sistemas autônomos e inteligentes.

Está-se diante do uso de informações preditivas, que são rentabilizadas pelas IA's para o próprio desenvolvimento, trata-se do desenvolvimento, por meio da IA, da capacidade de aproveitar informações até então inutilizáveis (MOROZOV, 2018, p. 152). Adverte o autor para uma consequência da interconexão de todos os aparelhos, com a Inteligência Artificial, que implica em uma sociedade de hiper vigilância, pois todos os objetos inteligentes *são capazes de gerar um rastro de dados,* e quando as *informações originárias de vários desses objetos são recolhidas e combinadas, é possível – ao menos funcionalmente* gerar inferências e previsões.

1.2 O impacto do uso de IA, a Privacidade e o consentimento informado

A consolidação da sociedade em rede pelo desenvolvimento da Internet foi fator geratriz para que o poder econômico passasse a girar em torno do nivelamento pelo domínio da informação. Dessa forma, a necessidade pela regulamentação do direito à privacidade individual trouxe à tona o fundamento da imposição de limitações no tratamento dos dados pessoais.

A mediação dos dados pelas inteligências artificiais pode uma afetação no desenvolvimento de uma cultura democrática, impondo-se em seu lugar uma medição tecnocrata da sociedade e das ações humanas havendo uma interseção de lógicas complexas estabelecidas entre política, tecnologia e finanças, essa é outro alerta-crítico trazido pelo autor bielo-russo (MOROZOV, 2018, 163). Indicando ser necessário *desenhar fronteiras nítidas entre os algoritmos e os dados com que são alimentados;* ressaltando que *os dados são o operador oculto* da lógica algorítmica. (MOROZOV; 2018; p.178). Para o autor:

[11] Evgeny Morozov é um pesquisador Bielorrusso nascido em 1984, que foi professor visitante na Universidade de Stanford; seus estudos envolvem a análise de implicações políticas e sociais do progresso tecnológico e digital, tendo adotado uma posição cética em relação ao potencial democratizante, emancipatório e anti-totalitário que a internet pode promover de acordo com os solucionistas, visto entender esta ser uma ferramenta poderosa para o exercício de vigilância em massa, repressão política, e disseminação de discursos de ódio.

> *o método que sustenta os avanços recentes na IA ainda é alimentado por dados históricos – e os dados, como qualquer produto de técnicas racionais de administração, tendem a incorporar, ocultar e amplificar viesses-, tais revelações podem ajudar a enfraquecer a imensa confiança que quase todos nós depositamos nesses sistemas aparentemente objetivos (MOROZO, 2018, p. 179)*
>
> .

Vive-se em um processo de informacionalização do mundo, é dizer, um processo por meio quais se despoja um problema de suas dimensões materiais e políticas, colocando-o simplesmente como uma questão de insuficiência ou atraso de informação. (MOROZOV, 2018, p. 110). Disto, apresenta seu receio em relação à privacidade, pois essa se tornando uma mercadoria, deixando de ser uma garantia ou uma coisa que desfruta—se gratuitamente, sendo agora necessário gastar-se recursos para dominar as ferramentas que a garantam (MOROZOV, 2018, p.36). Fala-se da emergência de dois tipos de privacidade, uma conhecida como privacidade como serviço, que é oferecida aos utilizadores de determinados softwares; e a privacidade como direito, a partir de sua garantia pelo sistema constitucional (MOROZOV, 2018, p.177).

Compreendida a contextualização fática, social e político; passamos a analisar alguns requisitos normativos da atual situação. Dentre os requisitos para o tratamento de dados previsto nos artigos sétimo (dados pessoais) e onze (dados pessoais sensíveis) da Lei Geral de Proteção de Dados (LGPD), destaca-se, principalmente para a crítica fundamentada pela tese do presente artigo, o tratamento de dados a partir do oferecimento do consentimento pelo titular.

Tendo em vista que, de acordo com o artigo quinto da LGPD, dado pessoal sensível é caracterizado como todo dado que contenha informações individuais acerca de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, por exemplo, a implementação do uso de reconhecimento facial (Wright, 2019) em transportes públicos para controle de acesso e prevenção de fraudes é baseada em decisões automatizadas por meio de software cuja arquitetura se utiliza de dados biométricos para o mapeamento da métrica facial de todo e qualquer indivíduo que tenha seus dados cadastrados nos órgãos institucionais de infraestrutura de transporte público.

De acordo com a Lei, o consentimento se dá pela manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Constata-se, portanto, diante do instituto da manifestação da vontade, requisitos de validade presentes no diploma legal para que o exercício da autodeterminação informativa seja garantido.

No entanto, apesar de existir a hipótese em que o dado pessoal sensível pode ser tratado a partir do consentimento prévio, específico e destacado pelo titular desses dados (ou por seu responsável legal), existe também a hipótese prevista em lei que esse tratamento poderá ocorrer sem o fornecimento de consentimento do titular em situações em que, por exemplo, seja indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador, e para o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos, tais como a prevenção de fraudes na utilização de benefícios ou isenções pelo munícipe no transporte público municipal, tal como a problemática no caso aqui trabalhado.

Nesse diapasão, cabe discutir a segunda hipótese de tratamento de dados pessoais sensíveis supramencionada, dado o potencial de dano que pode ser causado ao titular pelo tratamento de dados sensíveis sem os devidos mecanismos de proteção, segurança, transparência e confidencialidade. A título de exemplo, existem premissas que devem ser atendidas mesmo quando o consentimento do titular é dispensado para o tratamento de seus dados, tais como preconiza o § 2º do artigo 11 quando impõe aos órgãos e às entidades públicas a obrigação de que a referida dispensa de consentimento seja publicizada.

Vale considerar, ainda, que a ausência de parâmetros de tratamento de dados que assegurem a boa-fé (principalmente em casos de tentativa de obtenção de vantagens econômicas) e que considerem os devidos padrões éticos de processamento, armazenamento e transferência de dados pessoais poderá configurar hipótese de nulidade do exercício do fluxo informacional em razão da perda de legitimação da atividade.

2. Relatório de Impacto e Gestão: conceituações iniciais.

A partir da implementação da Lei Geral de Proteção de Dados como cerne sistemático de proteção aos direitos de privacidade e dos titulares de dados pessoais, a gestão de risco como abordagem regulatória surgiu como novo instituto jurídico em que a tutela dos direitos fundamentais passa gradativamente a se basilar por meio de instrumentos de regulação *ex ante* (Zanatta, 2017, p. 176), tais como licenças, análises de risco, procedimentos de documentação e *accountability* dos agentes de tratamento. Assim é conceituada a sistemática preventiva, instrumento trazido pela experiência europeia[12] na necessidade por regulamentar o crescente e

[12] Detalhada no capítulo 4, dos artigos 24 ao 43, no texto do *General Data Protection Regulation* (GDPR), que determina parâmetros e ferramentas de implementação de medidas técnicas e organizacionais apropriadas para a devida demonstração de concordância do processamento de dados em relação ao GDPR.

desenfreado fluxo de dados pessoais no oceano cibernético nas dependências da jurisdição da União Europeia.

Segundo a Lei 13.709/2018[13], o relatório de impacto[14] à proteção de dados pessoais é elaborado a partir da documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos aos direitos fundamentais e às liberdades civis, bem como demais mecanismos de mitigação de risco.

Nesse diapasão, considerando-se que a base teórica do dispositivo legal que rege a proteção de dados no Brasil foi amplamente inspirada na experiência europeia (Kuner, 2012) de elaboração do General Data Protection Regulation (GDPR), dentre as obrigações e instrumentos semelhantes entre as duas legislações, uma das adaptações trazida pela LGPD foi o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), equivalente ao *Data Protection Impact Assessment* (DPIA)[15] implementado pelas autoridades europeias (Wright & De Hert, 2012).

Nesse lapso controverso de vacância de atuação fiscalizatória da Autoridade Nacional de Proteção de Dados (ANPD), a regulação pela implementação do RIPD enfrenta desafios pelo fato de ainda restar legislativamente indefinido e, portanto, incompreendido, dada as limitações inteligíveis dos dispositivos que o define.

Sobre isso, os principais desafios para a regulação pelo Relatório de Impacto à Proteção de Dados Pessoais (RIPD) sugerem que a ferramenta seja identificada em suas reais funções de acordo com seu papel na LGPD, amparado na noção de risco a partir de sua análise e documentação, baseada nas hipóteses de obrigatoriedade de elaboração de acordo com uma metodologia definida de forma adequada e que, por fim, tal prestação de contas à ANPD seja demonstrada a partir de parâmetros bem estabelecidos, não dispensando a possibilidade de uma eventual publicização (Gomes, 2019, p. 07).

[13] A chamada Lei Geral de Proteção de Dados de 14 de agosto de 2018, ou, como é comumente denominada em seu acrônimo, a LGPD.

[14] Definido pelo artigo 5º, inciso XVII, da Lei Geral de Proteção de Dados, como "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco".

[15] Conforme texto original do GDPR, define-se o *Data Protection Impact Assessment* (DPIA) pelo seguinte escopo: "Sempre que um tipo de tratamento, nomeadamente com recurso a novas tecnologias, e tendo em conta a natureza, âmbito, contexto e finalidades do tratamento, for susceptível de resultar num risco elevado para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento deve, antes do tratamento, proceder a uma avaliação do impacto das operações de tratamento previstas sobre a proteção dos dados pessoais. Uma única avaliação pode incidir sobre um conjunto de operações de tratamento semelhantes que apresentem riscos elevados semelhantes".

2.1 Abordagens regulatórias para a gestão de risco

Em prol de uma melhor compreensão da implementação de relatórios de impacto para mitigação de riscos, é mister compreender a dicotomia entre as abordagens regulatórias baseadas nos direitos fundamentais (*rights-based approach*) e aquelas baseadas nos riscos (*risk-based approach*).

Enquanto o controlador, a fim de respeitar os direitos fundamentais tutelados pela Constituição Federal, deve observar os princípios que regem a disciplina da proteção de dados pessoais por meio de juízos de adequação de necessidade e da razoabilidade do tratamento de dados de acordo com a finalidade específica (*rights-based approach*), é dever também do controlador determinar o tipo de processamento e os riscos de privacidade dos titulares dos dados para que possam implementar corretamente as medidas de responsabilidade, tais como a avaliação de impacto (*risk-based approach*).

2.2 A Proteção da Privacidade a partir da Transparência Informacional

É inegável o poder e o uso dos dados no desenvolvimento atual da sociedade, estando presente o não a possibilidade de opera-los via inteligência artificial é só uma questão de tempo. Ainda que haja desenvolvimento normativo ele se mostra até certo ponto insuficiente para responder de forma adequada as necessidades relativas a proteção da privacidade individual nesse contexto tecno-industrial-econômico vigente no início do século XXI. O Direito, enquanto ciência, deve se manter antenado a realidade histórica em que se encontra imbuído, devendo estar em constante aperfeiçoamento.

O que se evidenciou é que o desenvolvimento das inteligências artificiais requer uma coleta massiva de dados para a sua automação e aperfeiçoamento. O uso e a interligação entre diversos conectores que captam e analisam dados são cada vez maiores.

Morozov, em sua obra sobre A Cidade Inteligente: Tecnologia Urbanas e Democracia (2019, p. 77) nos remete a ideia de recuperarmos a soberania tecnológica como uma solução sendo necessário reavaliar as relações estabelecidas com a tecnologia, os dados e sua infraestrutura de redes (2019, p; 79)

Mas quais medidas seriam essas e quais seriam os seus impactos? Se, de um lado o que é oferecido é a otimização do uso de recursos, produção de novos recursos, modificação de comportamento, promovendo ganhos em termos de flexibilidade, segurança e sustentabilidade;

por outro a concentração desses dados nas mãos de poucas empresas desenvolvedoras desses softwares compartilhados de inteligência artificial.

Considerando essa realidade Morozov (2019, p.108) propõe alguns elementos a fim de estabelecer um controle público, de governança democrática a partir da auto-organização cidadã, passando pelo incentivo a regimes alternativos de propriedade de dados; realizando serviços de informação para plataformas de código padrão e abertos e adoção de ágeis de entrega; transformando o controle das plataformas digitais por meio da construção e expansão das infraestruturas digitais alternativas, desenvolvimento modelos cooperativos de fornecimento de serviços, visando a reavaliação de esquemas de bem—estar social e dos sistemas complementares por meio do fomento de inovações com valor social.

O que se espera é uma desfragmentação entre arranjos de dispositivos, pontes de ligação, plataformas e instrumentos de manejo de informações que impede o gerenciamento dos dados e, em última análise, afasta do controle do usuário final (MOROZOV, 2019, p. 109).

III. CONSIDERAÇÕES FINAIS

Nota-se a importância de tomar como padrões a disposição de análises conceituais acerca de ferramentas específicas e sólidas, tal como o Relatório de Impacto de Proteção de Dados (RIPD), a fim de garantir que os riscos aos titulares de dados – ou seja, nós todos – serão mitigados ao máximo e que a cibersegurança será garantida por meio de instrumentos que visem a transparência e o controle dos processos que envolvam tratamento de dados pessoais.

No entanto, para que o uso de Relatórios de Impacto de Proteção de Dados seja de fato eficaz e possível, faz-se necessário: 1) analisar a interrelação entre estratégias de definição de perfil automático pelo uso de Inteligência Artificial; 2) avaliar tipos de regulação já previstas em legislação no âmbito da União Europeia (GDPR); 3) estudar a abordagem setorial da Inteligência Artificial em programações que se utilizam de técnicas de machine learning e 4) avaliar as abordagens preexistentes acerca das arquiteturas utilizadas em softwares utilizados exclusivamente para estratégias de perfilamento para posterior categorização de usos e práticas que tragam riscos às pessoas naturais cujos dados são tratados de forma automatizada para fins comerciais e de controle e vigilância estatal.

Os Relatórios de Impacto de Proteção de Dados, se devidamente implementados e sistematizados para uso por empresas em suas atuações com consumidores e pelo aparato do estado em políticas públicas, não só trarão maior segurança para os titulares de dados, como

também possibilitarão que bancos de dados inteiros sejam alimentados com informações pormenorizadas acerca dos usos e desusos atribuídos a tarefas realizadas por ferramentas de inteligência artificial. Essas análises compreenderão especificações acerca de variados tipos de arquiteturas de sistemas de IA, bem como a forma como foram utilizados na sociedade de acordo com finalidades específicas.

Todavia, ainda que a haja legislações e normas que visam prevenir e proteger do abuso do extrativismo de dados por essas inteligências artificiais, elas se mostram insuficientes em sua maioria ante a uma perspectiva mais ampla.

IV. REFERÊNCIAS BIBLIOGRAFICAS

ALGORITHMWATCH. AI Ethics Guidelines Global Inventory, s/c, s/d. Disponível em: <https://inventory.algorithmwatch.org/database>.

ANDRADE, N. Promoting AI ethics research in Latin America and the Caribbean. [S.l.]: Facebook Research blog, July 2 2020.

AVANCI, Thiago Felipe S. Relatório sobre a inteligência artificial e o projeto de lei 21/20, que visa instituir o marco legal da inteligência artificial no Brasil. 2022.

BENNETT, Colin J.; RAAB, Charles D., The governance of privacy: policy instruments in global perspective, 2nd and updated ed. Cambridge, Mass: MIT Press, 2006.

BIONI, Bruno; Leite Monteiro, Renato; Oliveira, Maria Cecília. GDPR Matchup: Brazil's General Data Protection LAW, IAPP, 2018.

BLOEDORN, Eric; MANI, Inderjeet; MACMILLAN, T. Richard. Machine learning of user profiles: Representational issues. In: AAAI/IAAI, Vol. 1. 1996. p. 433-438. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.493.7639&rep=rep1&type=pdf>

CALO, Ryan, Artificial Intelligence Policy: A Primer and Roadmap (August 8, 2017). Available in SSRN: https://ssrn.com/abstract=3015350 or http://dx.doi.org/10.2139/ssrn.3015350

CETYS. GuIA.ia. Artificial Intelligence in Latin America and the Caribbean: Ethics, Governance and Policies, 2021. Disponível em: <GuAI.ia>.

COZMAN, Fábio G. PLONSKI, Guilherme Ary; NERI, Hugo (Org.) **Inteligência Artificial: Avanços e Tendências.** São Paulo: Instituto de Estudos Avançados, 2021. Disponível em: <http://www.livrosabertos.sibi.usp.br/portaldelivrosUSP/catalog/book/650#:~:text=A%20obra%20mostra%20que%20a,de%20fato%2C%20influencia%20a%20sociedade.&text=Cada%20um%20dos%20cap%C3%ADtulos%20busca,e%20aplicado%20a%20Intelig%C3%AAncia%20Artificial.>. Acesso em: 22 de setembro de 2022.

DOEDERLEIN, Natalia. Projeto cria marco legal para uso de inteligência artificial no Brasil: Texto determina que a inteligência artificial deverá respeitar os direitos humanos e os valores democráticos. Disponível em: <https://www.camara.leg.br/noticias/641927-projeto-cria-marco-legal-para-uso-de-inteligencia-artificial-nobrasil/#:~:text=O%20Projeto%20de%20Lei%2021,de%20governan%C3%A7a%20para%20a%20IA>.

FIDIS. Descriptive analysis and inventory of profiling practices. Disponível em: http://www.fidis.net/resources/fidis-deliverables/profiling/int-d72000/doc/4/. Acesso em: 16 jul. 2020.

COMISSÃO EUROPEIA. Regulamento Europeu sobre Inteligência Artificial. Bruxelas, 2021. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN#:~:text=A%20proposta%20estabelece%20regras%20harmonizadas,futuro%20de%20%C2%ABintelig%C3%AAncia%20artificial%C2%BB. Acesso em: 13 de outubro de 2022.

GOMES, Maria Cecília Oliveira. Relatório de Impacto a Proteção de Dados Pessoais: uma breve análise da sua definição e papel na LGPD (2019), Revista da AASP, n. 144. p. 07.

HAUGELAND, J. Artificial Intelligence: The Very Idea. Cambridge: Bradford Books, 1985.

HILDEBRANDT, Mireille. Defining Profiling: A New Type of Knowledge? In: GUTWIRTH, Serge; HILDEBRANDT, Mireille (Ed.). Profiling the European Citizen:Cross-Disciplinary Perspectives. New York: Springer, 2008. p. 20.

HILDEBRANDT, Mireille; DE VRIES, Katja (Ed.). Privacy, due process and the computational turn: The philosophy of law meets the philosophy of technology. Routledge, 2013.

HILDEBRANDT, Mireille (Ed.). Profiling the European Citizen:Cross-Disciplinary Perspectives. New York: Springer, 2008. p. 249)

HARTZOG, Woodrow. SELINGER, Evan. Facial recognition is the perfect tool for oppression. Disponível em: https://medium.com/s/story/facial-recognition-is-the-perfect-toolfor-oppression-bc2a08f0fe66

KUNER, Christopher. The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. Bloomberg BNA Privacy and Security Law Report, v. 6, n. 11, p. 1–15, 2012.

KRANZBERG, Melvin. Technology and History: "Kranzberg's Laws". Johns Hopkins University Press, v. 27, n. 3, p. 544-560, 1986, p. 545.

LECUN, Yann; BENGIO, Yoshua; HINTON, Geoffrey. Deep learning. **nature**, v. 521, n. 7553, p. 436-444, 2015.

MENECEUR, Y. L'intelligence artificielle en procès: plaidoyer pour une réglementation internationale et européene. Paris : Brulant, 2020.

MITCHELL, T. Machine Learning. New York: McGraw Hill, 1997.

MITTELSTADT, Brent. From Individual to Group Privacy in Big Data Analytics. Philosophy and Technology, v. 30, n. 4, p. 475-494, 2017.

MONT, C. G. et al. Artificial Intelligence for Social Good in Latin America and the Caribbean: The Regional Landscape and 12 Country Snapshots. [S.l.]: Inter-American Development Bank, July 2020.

MOROZV, Evgene. BigTech: **A Ascensão dos Dados e a Morte da Política**; trad. Claudio Marcondes. – São Paulo: Ubu Editora, 2018, 192, pp.

MOROZOV, Evgene; BRIA,Francesca. **A Cidade Inteligente: Tecnologias Urbanas e Democracia** ; trad. Humberto do Amaral. – São Paulo: Ubu Editora, 2019, 192, pp.

OECD's homepage on legal instruments: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449

QUELLE, Claudia, Privacy, Proceduralism and Self-Regulation in Data Protection Law, Rochester, NY: Social Science Research Network, 2017. p. 96.

SALLOUM, Said A. et al. Machine learning and deep learning techniques for cybersecurity: a review. In: **The International Conference on Artificial Intelligence and Computer Vision**. Springer, Cham, 2020. p. 50-57.

SANDVIK, Kristin; RAYMOND, Nathaniel. Beyond the Protective Effect: Towards a Theory of Harm for Information Communication Technologies in Mass Atrocity Response. Genocide Studies and Prevention, v. 11, n. 1, p. 9–24, 2017, p. 10.

STIRLING, Andrew. Precaution in the Governance of Technology. Working Paper. SPRU - Science Policy Research Unit, Brighton, 2016.

WEINBERGER, D. Playing with AI Fairness. Google's PAIR (People and AI Research), 2021. Disponível em: <https://pair-code.github.io/what-if-tool/ai-fairness.html>.

WRIGHT, David; DE HERT, Paul (Orgs.), Privacy Impact Assessment, Dordrecht: Springer Netherlands, 2012.

WRIGHT, Elias. The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector. In Fordham Intell. Prop. Media & Ent. L.J. 611 (2019). Disponível em: https://ir.lawnet.fordham.edu/iplj/vol29/iss2/6

ZANATTA, Rafael A.F. "PROTEÇÃO DE DADOS PESSOAIS COMO REGULAÇÃO DE RISCO: uma nova moldura teórica?" (2017). Artigos Selecionados REDE 2017. I Encontro da Rede de Pesquisa em Governança da Internet. p. 176.