FGV DIREITO SP
MESTRADO PROFISSIONAL

Machine learning: desafios do direito de revisão das decisões automatizadas

Alex Silva dos Santos

Anteprojeto de pesquisa apresentado ao
Mestrado Profissional da FGV Direito SP.

Versão de 17 de outubro de 2020.

1. Tema, contexto e modelo de pesquisa predominante

A regulação da proteção de dados pessoais é um movimento relativamente recente e global, e que tem como principal objetivo moderar a utilização de informações que identifiquem ou que possam identificar pessoais naturais. Esse avanço regulatório traz novos obstáculos à inovação tecnológica, mormente a atual tendência mundial em se adotar como padrão predominante o modelo restritivo de operações de tratamento dos dados pessoais adotado pela União Europeia, denominado Regulamento Geral de Proteção de Dados Pessoais - GDPR, pelo qual há a necessidade de preenchimento de diversos requisitos legais para que o tratamento de dados pessoais possa ser considerado lícito. Essa realidade é especialmente desafiadora para modelos de negócio altamente dependentes de dados pessoais para desenvolvimento de seus produtos e serviços, como provedores de redes sociais, empresas de marketing digital e, especialmente, desenvolvedores de aplicações que utilizem a tecnologia de *machine learning* (aprendizado de máquina).

De forma muito simples, entende-se por *machine learning* (aprendizado de máquina) a tecnologia que concede aos computadores a capacidade de aprender, analisar e decidir de acordo com respostas e associações de imagens, números, informações e qualquer dado passível de identificação. Em uma primeira etapa, conjuntos de instruções para realização de determinadas tarefas (denominados algoritmos) são criados a partir de uma base de dados (ponto de partida) a ser analisada e de um conjunto de respostas ou resultados que decorrem da análise pretendida. O algoritmo é, então, submetido a um "treinamento" guiado por humanos, pelo qual realiza associações com base em uma quantidade massiva de informações. Em um segundo momento, por meio de métodos de melhoria automática e gradual, o sistema passar a criar seus próprios métodos para otimizar a análise e as respostas esperadas, sem interferência humana. Nessa etapa, surge então uma grande dificuldade técnica em explicar como que a máquina chega aos resultados obtidos, dando espaço para dilemas éticos e debates sobre possíveis abusos por meio de manipulação, viés, censura, discriminação social, violações de privacidade, direitos proprietários, abuso do poder de mercado e demais direitos dos titulares de dados pessoais.

Essa obscuridade deu origem aos acalorados debates (sobretudo na academia europeia) sobre a necessidade de transparência na forma como os dados pessoais são tratados e, especialmente, sobre a existência de um direito de explicação das decisões automatizadas ou de apenas um direito à informação sobre a funcionalidade do algoritmo ou sobre a racionalidade, dados utilizados e sua qualificação, e fluxo lógico por trás da decisão automatizada. Essa discussão ganha cada vez mais importância conforme decisões automatizadas passam a ser responsáveis por produzir efeitos jurídicos e, consequentemente, passam a ter potencial de produzir danos aos titulares dos dados pessoais tratados. Por exemplo, pedidos de concessão de crédito podem ser negados ou taxas de juros podem se fixadas em patamares elevados com base em decisões automatizadas tomadas por meio de perfis criados com informações comportamentais e modelos preditivos com viés, por exemplo.

A regulação brasileira sobre proteção de dados pessoais (Lei nº 13.709, d 14 de agosto de 2018, denominada "Lei Geral de Proteção de Dados Pessoais" - LGPD) foi além do modelo europeu e instituiu expressamente o direito de revisão (LGPD, art.20, *caput*). Nesse sentido, enquanto o direito à explicação pode ser entendido como o direito de receber informações suficientes e inteligíveis que permitam ao titular dos dados entender a lógica e os critérios utilizados para tratar seus dados pessoais para uma ou várias finalidades (§1º), o direito à revisão compreende o direito do titular de requisitar a revisão de uma decisão totalmente automatizada que possa ter um impacto nos seus interesses, principalmente os relacionados à definição do seu perfil pessoal, profissional, de consumo e de crédito ou os aspecto de sua personalidade (*caput*).

Nesse contexto, há um potencial conflito de interesses entre a regulação da proteção de dados pessoais e o desenvolvimento de aplicações com *machine learning*, especialmente diante da exigência regulatória de transparência, direito de informação e direito de revisão de decisões automatizadas e, por outro lado, o interesse na preservação de segredos industriais e comerciais, além da proteção de propriedade intelectual e direitos autorais.

O grande desafio é investigar o tema e propor soluções para conciliar esse movimento de regulação da proteção de dados pessoais com o desenvolvimento de aplicações com *machine learning*, que depende massivamente de dados, especialmente com relação ao direito de revisão das decisões automatizadas que possam impactar interesses de pessoas naturais com relação ao seu perfil pessoal, profissional, de consumo e de crédito ou sobre algum aspecto de sua personalidade. Para tanto, será adotado o modelo de pesquisa para resolução dos problemas identificados, com proposição de metodologia para implantação de procedimento interno para atendimento de requisições de revisão de decisões automatizadas, assegurando a proteção de segredos industriais e comerciais, propriedade intelectual e direitos autorais do controlador/operador.

2. **Quesitos, fontes de pesquisa e formas de acesso**

[Quesito 1:] No que consiste a tecnologia de *machine learning* e suas principais características, técnicas, etapas de desenvolvimento, abordagens e grau de dependência com relação ao tipo e volume de dados pessoais? Quais são as principais questões em debate no meio acadêmico sobre proteção de dados pessoais e decisões automatizadas?

[Fontes e formas de acesso:] Serão consultadas obras de referência na área da tecnologia da informação, doutrina nacional e estrangeira sobre o tema, artigos, white papers, monografias, teses e dissertações.

[Quesito 2:] Qual é o contexto atual da regulação da proteção de dados pessoais e *machine learning* no Brasil e no direito comparado, e quais são as principais referências de regulação da proteção de dados pessoais no mundo? Quais são os fundamentos e princípios que norteiam a proteção de dados pessoais e, em especial, o direito de revisão das decisões automatizadas? Quais são os principais agentes envolvidos no contexto da proteção de dados pessoais e como a regulação define seus papéis, direitos, deveres e responsabilidades? Quais são os possíveis problemas, entraves normativos, morais e éticos de quem desenvolve, administra e organiza o uso de sistemas autômatos do ponto de vista da proteção de dados pessoais, especialmente com relação ao direito de revisão de decisões automatizadas? O que é revisar? Como deve ser feita a revisão das decisões automatizadas? Qual é o nível de transparência exigido? O que é preciso ser comunicado ao titular?

[Fontes e formas de acesso:] Pesquisar legislação e decisões (administrativas e judiciais) nacionais e internacionais sobre proteção de dados pessoais, com foco na União Europeia, Reino Unido e Estados Unidos da América, para fins de análise de direito comparado. Serão consultadas obras de referência na área da tecnologia da informação, doutrina jurídica nacional e estrangeira sobre o tema, artigos, white papers, monografias, teses e dissertações.

[Quesito 3:] Quais as possíveis estratégias a serem adotadas no sentido de evitar litígios ou mitigar o impacto do exercício do direito de revisão de decisões automatizadas pelo titulares com relação aos dados pessoais utilizados em *machine learning*? Como conciliar os interesses dos titulares dos dados pessoais, das autoridades nacionais de proteção de dados pessoais e dos agentes desenvolvedores de aplicações com *machine learning*, principalmente com relação à proteção dos segredos industriais e comerciais, além dos direitos autorais e propriedade intelectual? Como lidar com a disparidade evolutiva entre tecnológica e regulação?

[Fontes e formas de acesso:] Pesquisar legislação e decisões (administrativas e judiciais) nacionais e internacionais sobre proteção de dados pessoais, com foco na União Europeia, Reino Unido e Estados Unidos da América, para fins de análise de direito comparado. Serão consultadas obras de referência na área da tecnologia da informação, doutrina jurídica nacional e estrangeira sobre o tema, artigos, white papers, monografias, teses e dissertações.

[Quesito 4:] Quais são as condutas ou ações práticas recomendadas para evitar ou ao menos mitigar os efeitos decorrentes da regulação da proteção de dados pessoais com relação ao desenvolvimento de aplicações com *machine learning*, especificamente com relação ao exercício do direito de revisão das decisões automatizadas? Quais condutas, ações práticas ou metodologias podem ser adotadas para efetiva adequação à regulação no que diz respeito à instauração de procedimento interno para atendimento das solicitações de direito de revisão, respeitadas as características da tecnologia de *machine learning* e os segredos industriais e comerciais do controlador/operador?

[Fontes e formas de acesso:] Serão consultadas obras de referência na área da tecnologia da informação, doutrina nacional e estrangeira sobre o tema, artigos, *white papers, guidelines* emitidos por instituições e organizações que lidam como tema, monografias, teses e dissertações.

3. **Relevância prática, caráter inovador e potencial de impacto**

A tecnologia de *machine learning* está em franco desenvolvimento e tem sido utilizada com sucesso no desenvolvimento de aplicações nos mais diversos ramos empresariais, sobretudo diante do potencial de se obter resultados com níveis de celeridade e confiabilidade muito superiores aos comumente obtidos com interferência humana. Em razão dessa automação no processo de modelagem, essa tecnologia permite a predição de resultados (com alto grau de eficiência) que podem fundamentar a adoção de mudanças significativas nos negócios e, assim, promover inovação. A tomada de decisões empresariais assistida por análises preditivas obtidas via *machine learning* será cada vez mais comum, sendo difícil projetar um futuro dissociado de, ao menos, um certo grau de dependência dessa tecnologia.

São muitos os exemplos de sucesso do uso de *machine learning* para aprimoramento de produtos e serviços já existentes, principalmente quando relacionados à intenção de predição de eventos e comportamentos. Há relatos na mídia de uso *machine learning* para diagnósticos médicos (ex.: detecção precoce de enfermidades por meio da análise dados de biopsias), no desenvolvimento de "assistentes pessoais" por voz para execução de diversas tarefas (efetuar ligações, enviar mensagens de texto, iniciar aplicativos, agendar reuniões e compromissos, cadastrar lembretes, responder perguntas simples, buscar informações, preencher solicitações de serviço, e até mesmo atuar na automação de casas com acender luzes, abrir e fechar portões); em sistema de segurança para antecipar, identificar e bloquear tentativas de fraudes bancárias; além da análise de crédito, por meio da criação de modelos preditivos para qualificar consumidores e avaliar solicitações de crédito com mais precisão.

Apesar dos diversos benefícios econômicos, sociais e científicos que poderão decorrer dessa associação de *machine learning* com quantidades massivas de dados (big data), o movimento global de regulação dessa tecnologia e, em especial, da privacidade e da proteção de dados pessoais, trouxe questões para debate relacionadas aos riscos de monitoramento invasivo, abusos, discriminação e sobre a necessidade de imposição de restrições normativas. Na medida em que há iniciativas no sentido de regular sua utilização e, consequentemente, impor limites, surge então a relevância prática de antecipar os conflitos entre a regulação e

inovação, momento no qual a análise desses impactos sob o ponto de vista jurídica será relevante para o desenvolvimento dessas aplicações, especialmente com relação ao direito de revisão das decisões automatizadas.

A metodologia a ser proposta permitirá a adoção de um procedimento interno adequado à atender as solicitações de revisão de decisões automatizadas em total observância aos direitos dos titulares e aos interesses do controlador/processador em preservar os segredos industriais e comerciais, propriedade intelectual e direitos autorais de sua aplicação com *machine learning*.

4. **Familiaridade do pesquisador com o objeto da pesquisa**

Embora o pesquisador tenha formação acadêmica estritamente em Ciências Humanas e Sociais (Direito), o pesquisador sempre esteve contato com computadores e acompanhou o desenvolvimento da tecnologia e da Internet no Brasil ao longo das últimas décadas. Em paralelo às atividades de advocacia empresarial, o pesquisador iniciou os estudos no novo ramo do direito que denominam "direito digital" em meados de 2018. Nesse caminho, o pesquisador concluiu curso de extensão universitária em Direito Digital pela FGV Direito e, também, fez curso livre de gestão de produtos digitais pela Digital House, tendo, assim, conhecimentos técnicos elementares com relação ao processo de transformação digital e desenvolvimento de produtos/serviços no meio digital. Atualmente, o pesquisador presta serviços na área de direito digital, ajudando empresas a se adequarem às normas de proteção de dados pessoais e Internet, além de dar treinamentos e palestras sobre o tema. Especificamente com relação à *machine learning*, o pesquisador tem noções básicas de programação e ciência da computação que, possivelmente, ajudarão no processo de aprendizado e aprofundamento sobre o tema, considerando os limites da pesquisa.

5. **Bibliografia preliminar**

ASHLEY, K. D.. **Artificial Intelligence and Legal Analytics**. Cambridge University Press.

CATE, F. H.; Cullen F. H., Cate, F. H., Mayer-Schönberger. **Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines**. Oxford Internet Institute.

EDWARDS, L., VEALE, M. **Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for**. Duke Law and Technology Review, 16-84.

HILDEBRANDT, M.. Location data, purpose binding and contextual integrity: What's the message? In Floridi, L., editor, **The protection of information and the right to privacy**, 31–62. Springer.

HURWITZ, Judith; KIRSCH, Daniel. **Machine learning for dummies**. IBM edition. John Wiley & Sons, Inc., 2018. Disponível em: https://www.ibm.com/downloads/cas/GB8ZMQZ3. Acessado em: 14 de junho de 2020.

KAHNEMAN, Daniel. **Thinking: fast and slow.** Allen Lane.

KALPOKAS, Ignas. **Algorithmic Governance: Politics and Law in the Post-Human Era**. 1ed. Palgrave Pivot. 2019.

LESSIG, Lawrence. **Code: And Other Laws of Cyberspace, version 2.0.** 2.ed., rev. e atual. Basic Books: New York, 2006. Disponível em: http://codev2.cc/download+remix/Lessig-Codev2.pdf. Acessado em: 14 de junho de 2020;

O´NEIL, Cathy. **Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy**. Crown; 1ed., 2016.

PASQUALE, Frank. **The second wave of algorithmic accountability.** Law and Political Economy.

PASQUALE, Frank. **The Black Box Society: The Secret Algorithms That Control Money And Information**. Harvard University Press, Reprint Edition, 2016.

SELBST, Andrew D.; POWLES, Julia. **Meaningful information and the right to explanation**. International Data Privacy Law, 2017.

USTARAN, Eduardo. **European Data Protection Law, Law and Practice**. International Association of Privacy Professionals (IAPP).

WATCHER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. **Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation**. International Data Privacy Law, 2017.

Big data, artificial intelligence, machine learning and data protection. Information Comissioner Officer ICO.

6. **Cronograma de execução**

	2020			2021												
Atividade	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	Horas
Revisão bibliográfica																[90h]
Redação: Intro e Capítulo I																[40h]
Coleta de decisões																[20h]
Redação: Capítulo II																[30h]
Redação: Capítulo III																[30h.]
Redação: Capítulo IV																[30h]
Primeira revisão																[20h]
Redação: Conclusão																[10h]
Segunda revisão																[30h]