

Universidade do Minho
Escola de Direito

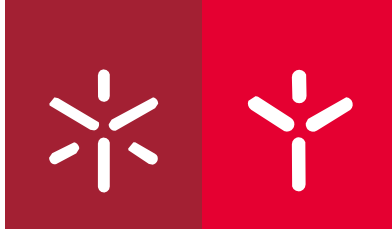
TAHENA VIDAL ANDRADE

O USO DA INTELIGÊNCIA ARTIFICIAL NO POLICIAMENTO PREDITIVO

O USO DA INTELIGÊNCIA ARTIFICIAL NO POLICIAMENTO
PREDITIVO

UMinho | 2022

Abril de 2022



Universidade do Minho
Escola de Direito

TAHENA VIDAL ANDRADE

O USO DA INTELIGÊNCIA ARTIFICIAL NO POLICIAMENTO PREDITIVO

Dissertação de Mestrado em Direito e Informática

Trabalho realizado sob a orientação da
Professora Doutora Flávia Novera Loureiro
e do Professor Doutor Paulo Novais

Abril de 2022

Direitos de autor e condições de utilização do trabalho por terceiros

Este é um trabalho académico que pode ser utilizado por terceiros desde que respeitadas as regras e boas práticas internacionalmente aceites, no que concerne aos direitos de autor e direitos conexos. Assim, o presente trabalho pode ser utilizado nos termos previstos na licença abaixo indicada.

Caso o utilizador necessite de permissão para poder fazer um uso do trabalho em condições não previstas no licenciamento indicado, deverá contactar o autor, através do RepositóriUM da Universidade do Minho.



Atribuição-NãoComercial-SemDerivaçõesCC BY-NC-ND

Agradecimentos

Agradeço em especial aos meus orientadores, Professora Doutora Flávia Novera Loureiro e ao Professor Doutor Paulo Novais, bem como, aos demais professores do Mestrado em Direito e Informática da Universidade do Minho.

Também agradeço ao Professor Doutor Giovanni Sartor, da Universidade de Bolonha, com quem tive a honra de obter um pouco de seus conhecimentos por meio do Programa Erasmus+.

Finalizo agradecendo também o Doutor Elia Lombardo, que gentilmente me cedeu materiais para o trabalho a seguir apresentado.

Minha eterna gratidão a todos.

Declaração de Integridade

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração. Declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

Resumo

O presente estudo trata do Policiamento Preditivo por meio do uso do *Big Data* e da Inteligência Artificial. Com o crescente uso de métodos preditivos, aumenta a preocupação com a utilização correta dos meios com o intuito de proteger os dados de milhares de pessoas, além da proteção dos direitos inerentes à sua condição humana. A pesquisa define os termos relacionados ao *big data*, tais como algoritmos, inteligência artificial e *machine learning*. Também analisa o uso da inteligência artificial no contexto do Regulamento Geral de Proteção de Dados, o RGPD, além de regulamentos dos órgãos responsáveis na União Europeia. Por fim, são demonstrados os resultados do funcionamento do programa de policiamento preditivo XLAW, que é utilizado pela Polícia Italiana. Tais resultados permitiram contemplar o uso do *Big Data* como prevenção da criminalidade.

Palavras-chave: *Big Data*; Inteligência Artificial; Algoritmos; Policiamento Preditivo; Justiça Criminal.

Abstract

This paper deals with Predictive Policing using Big Data and Artificial Intelligence. With the increasing use of predictive methods, there is a growing concern about the correct use of the means in order to protect the data of thousands of people, in addition to the protection of the rights inherent to their human condition. The research defines terms related to big data, such as algorithms, artificial intelligence and machine learning. It also analyzes the use of artificial intelligence in the context of the General Data Protection Regulation, the GDPR, and documents from the European Union. Finally, the results of the operation of the predictive policing program XLAW, which is used by the Italian Police, are demonstrated. These results allow us to contemplate the use of Big Data as crime prevention.

Keywords: Big Data; Artificial Intelligence; Algorithms; Predictive Policing; Criminal Justice.

Lista de siglas e abreviaturas

AI	Artificial Intelligence
BD	Big Data
CAHAI	Ad hoc Committee on Artificial Intelligence
CEDH	Convenção Europeia dos Direitos Humanos
CEPEJ	Comissão Europeia pela eficácia da Justiça
CDFUE	Carta dos Direitos Fundamentais da União Europeia
COMPAS	Correctional Offender Managment Profiling for Alternative Sanctions
DL	Deep Learning
DM	Data Mining
EDPB	Conselho Europeu de Proteção de Dados
EDPS	European Data Protection Supervisor
GDPR	General Data Protection Regulation
IA	Inteligência Artificial
ML	Machine Learning
RGPD	Regulamento Geral sobre a Proteção de Dados
RNAs	Redes neuronais artificiais
SIG	Sistema de Informação Geográfica
TFUE	Tratado sobre o Funcionamento da União Europeia
TI	Tecnologia da Informação
UE	União Europeia

Lista de figuras e tabelas

Figura 1: Artificial Intelligence

Figura 2: Porcentagem de eficácia do programa entre cidades que o utilizam, *versus* cidades que não utilizam o programa

Tabela 1: Porcentagem de eficácia do programa

Tabela 2: Tabela com dados das cidades parte do experimento

Tabela 3: Tabela com resultado de Nápoles

Tabela 4: Tabela com resultado de Salerno

Tabela 5: Tabela com resultado de Prato

Tabela 6: Tabela com resultado de Veneza

Tabela 7: Tabela com resultado de Parma

Tabela 8: Tabela com resultado de Módena

Sumário

Resumo	vii
Abstract.....	viii
Lista de siglas e abreviaturas.....	ix
Lista de figuras e tabelas	x
Introdução	1
Capítulo 1: Conceitos aplicados ao Policiamento Preditivo	5
1. Algoritmos	5
1.1. Sistemas de <i>Big Data</i>	7
1.2. Inteligência Artificial	9
1.3. <i>Machine Learning</i>	12
1.3.1 Aprendizagem supervisionada e não supervisionada	13
1.3.2. Redes neurais artificiais: um exemplo do uso de <i>Machine Learning</i>	16
1.3.3. Uso das redes neurais	17
1.4. <i>Deep Learning</i>	18
1.5. <i>Black Box problem</i>	20
Capítulo 2: Enquadramento normativo	23
1. Inteligência Artificial e a proteção de dados no contexto Europeu	23
1.1. Propostas de Regulamento em Matéria de Inteligência Artificial na União Europeia	29
1.2 Ética e direitos humanos no âmbito da Inteligência Artificial	31
1.3 Direito Penal e Inteligência Artificial.....	35
Capítulo 3: Reflexos dos avanços tecnológicos na aplicação do Direito Penal	41
1. O uso do <i>Big Data</i> no contexto do policiamento preditivo	41
1.1. <i>Machine Bias</i>	44
1.2. Análise algorítmica do perfil criminológico	46
1.3. Análise do <i>Software XLAW</i> : o <i>software</i> de IA da polícia italiana.....	48
1.3.1 <i>Método de análise para verificação dos resultados</i>	52
1.3.2 <i>Eficácia do método preditivo</i>	54
1.4. A utilização dos <i>softwares</i> de policiamento preditivo e o impacto no Processo Penal	60
1.5. Conclusão do capítulo.....	63
Considerações finais	65
Bibliografia.....	67
Relatórios	77
Websítios	81

Introdução

A dissertação a seguir apresentada tem como problema de pesquisa o funcionamento de programas de Inteligência Artificial (IA) desenvolvidos para o uso no direito penal, especificamente na seara do policiamento preditivo, bem como as consequências de sua aplicabilidade. O estudo da inteligência artificial é um dos campos mais estimulantes na área da tecnologia informática, pois, além dos sistemas tradicionais, também se desenvolveu uma busca por tentar simular comportamentos característicos do intelecto humano. Ou seja, a inteligência artificial é a ciência que tende a desenvolver modelos computacionais de comportamento inteligente para que os computadores possam realizar tarefas que exigiriam inteligência humana.

A inteligência artificial se baseia na ciência cognitiva, que estuda a inteligência humana para representá-la em modelos que podem ser transferidos para aplicações informáticas, seja criando computadores capazes de compreender e possuir estados cognitivos, ou sistemas de computador capazes de desempenho normalmente atribuído à inteligência humana¹.

Os sistemas baseados em conhecimento são representados em uma linguagem de alto nível, ou seja, de uma forma relativamente próxima da linguagem usada na comunicação humana, deixando o sistema identificar o procedimento a ser seguido para executar essa tarefa. O conhecimento é usado por um mecanismo inferencial, que é um mecanismo capaz de interpretar o conteúdo da base de conhecimento e fazer deduções lógicas para resolver o problema colocado no sistema, pois, a base de conhecimento pode ser enriquecida com novas informações sem intervenção no mecanismo inferencial. Além disso, o sistema é capaz de explicar de maneira compreensível as premissas e inferências que levam a um resultado específico, justificando as conclusões. Sistemas baseados em conhecimento são frequentemente complementados por interfaces que facilitam a interrogação e a preparação da base de conhecimento².

Portanto, os principais atributos que são reconhecidos pelos sistemas inteligentes devem ser a transparência ou a possibilidade de fornecer explicações sobre as linhas de raciocínio seguidas para chegar à conclusão, a adoção de estratégias típicas de especialistas humanos e a flexibilidade ou a capacidade de seguir sem grandes dificuldades, modificações em suas bases de conhecimento, como no caso de *softwares* utilizados para a justiça criminal. Recentemente, os

¹ Traversi, Alessandro. *Intelligenza artificiale e giustizia, verso un giudice robot?* Altalex, 19 marzo 2019. In: <https://www.altalex.com/documents/news/2019/03/19/intelligenza-artificiale-e-giustizia-giudice-robot>.

² *Idem, ibidem.*

sistemas inteligentes se uniram ao campo da inteligência artificial aplicada ao direito pelas chamadas redes neuronais³.

O período histórico atual é caracterizado por um maior interesse na inteligência artificial nos mais diversos setores, inclusive no Direito, como é o caso do chamado policiamento preditivo. O policiamento preditivo é um assunto muito discutido, pois o uso de inteligência artificial já é uma realidade. É um sistema heurístico que permite prever um resultado, pois elabora um mapa das áreas de maior risco, horários propensos ao cometimento de crimes, dias da semana, etc⁴.

Assim sendo, a dissertação será centrada na abordagem da inteligência artificial para o policiamento preditivo. Para tal, será necessário responder as seguintes questões fundamentais: os programas de inteligência artificial utilizados no campo da justiça preditiva funcionam? Se sim, qual é o mecanismo e suas linhas de raciocínio? Quais os riscos da utilização dos programas de IA no policiamento preditivo? Quais as implicações nas decisões tomadas por esses *softwares*?

Tais perguntas possibilitaram ser analisadas e respondidas de acordo com o estudo dos programas de IA e seu funcionamento e com base no estudo das legislações pertinentes. Sabe-se que as proteções legais são máximas no Direito Criminal. Existem limites legais (especialmente os constitucionais) e direitos e liberdades fundamentais da pessoa em questão (principalmente o direito ao contraditório e da ampla defesa, da presunção de inocência, bem como do princípio da proibição da analogia "*in malam partem*", que é a proibição da adequação típica por semelhança entre os factos) que poderiam ser comprometidos com o uso de um algoritmo.

Alguns *softwares* de policiamento preditivo concentram-se principalmente na capacidade de cometer crimes de um sujeito, ou seja, no modo de ser do sujeito, do qual se deduz a probabilidade de ele cometer novos crimes. O que difere da capacidade criminosa, que sempre existe em maior ou menor grau, devido ao facto de que o sujeito já cometeu o crime. Portanto, o primeiro é a possibilidade, enquanto o segundo é a probabilidade de realizar novos delitos⁵.

³ Traversi, Alessandro. *Intelligenza artificiale e giustizia, verso un giudice robot?* Altalex, 19 marzo 2019. In: <https://www.altalex.com/documents/news/2019/03/19/intelligenza-artificiale-e-giustizia-giudice-robot>

⁴ Martirano, Valentino Vescio di. *Algoritmo e giustizia predittiva in campo penale.* Altalex, 14 giugno 2018. In: <https://www.altalex.com/documents/news/2019/06/14/algoritmo-e-la-giustizia-predittiva-in-campo-penale>

⁵ Morelli, Claudia. *Processo Penale: operativa la prima applicazione di intelligenza artificiale?* In: <https://www.altalex.com/documents/news/2018/06/18/processo-penale-operativa-la-prima-applicazione-di-intelligenza-artificiale>.

Neste sentido, a dificuldade adicional de programar o algoritmo é inserida. Com efeito, a aplicação, mesmo antes da avaliação do perigo deve ser um raciocínio concreto e lógico. O algoritmo geralmente funciona de maneira presumida e é baseado em critérios de possibilidade e probabilidade, enquanto poderíamos definir lógica como herança exclusiva do ser humano. Ou seja, o perigo não pode ser apenas presumido⁶.

A dissertação tem três capítulos subdivididos em tópicos. No primeiro capítulo, o tópico de conceitos aplicados ao policiamento preditivo, procura explicar brevemente e com uma linguagem menos técnica possível e de fácil compreensão para pessoas de todas as áreas, o que significa algoritmos, sistemas de *big data*, inteligência artificial, *machine learning* e *deep learning*. Em cada um desses tópicos foi explicado, ainda que superficialmente, como funciona e quais suas aplicabilidades.

O capítulo seguinte trata das leis e regulamentos acerca da inteligência artificial, *big data* e proteção de dados. O primeiro tópico do segundo capítulo trata da inteligência artificial e proteção de dados no contexto europeu. No tópico seguinte relaciona-se a ética e os direitos humanos no uso da inteligência artificial. Nesse tópico ressaltam-se os direitos inerentes à pessoa humana no que diz respeito a proteção de seus dados, à dignidade, à liberdade, à igualdade, a não discriminação e exclusão, ao respeito à democracia e ao Estado de Direito. O último tópico do segundo capítulo, trata da relação jurídica entre o Direito Penal e a Inteligência Artificial. Neste tema, também são analisados regulamentos importantes, tais como, o documento elaborado pela Comissão Europeia pela Eficácia da Justiça e também a Resolução do Parlamento Europeu, de 6 de outubro de 2021, sobre a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais.

No terceiro e último capítulo, em seu primeiro tópico, é descrito o uso do *Big Data* no contexto do policiamento preditivo. Neste tópico explica-se o que é o policiamento preditivo e o uso do *Big Data*. O tópico seguinte, ainda em correlação ao primeiro, explica-se o viés algoritmo ou *Machine Bias*, que são os algoritmos que, a depender dos dados que os alimentam e de quem os programou, podem ser preconceituosos. No terceiro tópico é tratado sobre o perfil criminológico feito pelos *softwares* preditivos. O próximo tópico trata da análise do *software* preditivo utilizado pela Polícia Italiana, o chamado XLAW. Nesse tópico é demonstrado a base do funcionamento do

⁶ Morelli, Claudia. *Processo Penale: operativa la prima applicazione di intelligenza artificiale?* In: <https://www.altalex.com/documents/news/2018/06/18/processo-penale-operativa-la-prima-applicazione-di-intelligenza-artificiale>.

programa. Não sua análise profunda em termos da sua engenharia estrutural, mas em uma linguagem não técnica. Demonstra-se também o método de análise dos dados e a eficácia do método nas cidades testadas em comparação com as não testadas. O quarto tópico trata da aplicação do processo penal frente ao uso de provas obtidas pelos *softwares* de policiamento preditivo. E por fim, uma breve síntese do terceiro capítulo.

O trabalho foi fundamentado em estudos e pesquisas que são de extrema importância para a definição e construção dos conceitos apresentados. Por conseguinte, foram utilizadas fontes primárias e secundárias, tais como trabalhos acadêmicos, artigos, livros e afins. Para obter os resultados e respostas acerca da problematização apresentada, foi feita a análise pelo método de pesquisa descritiva com a finalidade de responder os problemas da pesquisa, partindo de uma revisão bibliográfica, pois, foram utilizados conceitos e ideias dos principais autores das áreas de Direito e Inteligência Artificial.

Como objeto empírico, foi utilizado o programa de Inteligência Artificial XLAW, utilizados no Policiamento Preditivo pela Polícia da Itália. A escolha se deu pela importância e atualidade do tema. Partindo dos conceitos apresentados, o trabalho a seguir analisará o funcionamento do programa, que são os objetos empíricos, bem como, sua utilização no policiamento preditivo.

Capítulo 1: Conceitos aplicados ao Policiamento Preditivo

1. Algoritmos

Algoritmo pode ser definido como uma sequência finita de instruções para resolver um problema, ou a especificação de uma sequência ordenada de passos que deve ser realizada, garantindo a sua repetibilidade com eficiência⁷. Entretanto, é necessário clareza e exatidão em cada um dos passos a ser realizado, bem como a sequência correta em que estes passos devem ser realizados. Para que um computador desempenhe uma tarefa, é preciso que esta seja detalhada de tal forma que a máquina entenda, ou seja, utilizando um programa computacional que na verdade é um algoritmo escrito em uma linguagem de programação ⁸.

Ao desenvolver um algoritmo deve se estabelecer um padrão de comportamento que deverá ser executado para alcançar o resultado de um problema. Assim sendo, pode se perceber que o algoritmo não é uma solução para o problema, mas uma maneira de realizá-la. Portanto, os algoritmos são capazes de realizar tarefas como ler e escrever dados, avaliar expressões lógicas, tomar decisões tendo como base os resultados e repetir um conjunto de ações de acordo com a condição. Ou seja, para o desenvolvimento funcional de um algoritmo se faz necessário seguir passos básicos para a sua construção, tais como, definir ações simples, organizar ações ordenadamente e estabelecer ações em uma sequência finita de passos⁹. Um algoritmo computacional é constituído pelo menos de três partes¹⁰:

Parte 1: A entrada de dados, onde são fornecidas as informações necessárias para que o algoritmo possa ser executado. Informações estas que, podem ser fornecidas no momento da execução do programa ou já estarem embutidas;

Parte 2: O processamento de dados, parte em que são avaliadas todas as expressões lógicas ou algébricas, além das estruturas de condição ou repetição existentes no algoritmo;

Parte 3: A saída dos dados, que são os resultados do processamento enviados para um ou mais dispositivos de saída.

⁷ Ferrari, Fabricio. Cechinel, Cristian. *Introdução a Algoritmos e Programação*. In <https://www.ferrari.pro.br/home/documents/FFerrari-CCechinel-Introducao-a-algoritmos.pdf>, p.15.

⁸ Algoritmo e Lógica de programação. Universidade Federal do Rio Grande do Norte, Centro de Tecnologia, Departamento de Computação e Automação Algoritmo e Lógica de Programação. Algoritmos, Parte 1. Eng. Química, maio 2004. In https://www.dca.ufrn.br/~affonso/DCA800/pdf/algoritmos_parte1.pdf, p. 03.

⁹ Ferrari, Fabricio. Cechinel, Cristian. *Introdução a Algoritmos e Programação*. In <https://www.ferrari.pro.br/home/documents/FFerrari-CCechinel-Introducao-a-algoritmos.pdf>, pp.15-17.

¹⁰ *Idem, ibidem*.

As formas de representação de algoritmos mais conhecidas são a descrição narrativa, o fluxograma convencional e o pseudocódigo. Na descrição narrativa, os algoritmos são expressos diretamente em linguagem natural, contudo é pouco usada na prática porque o uso da linguagem natural pode gerar ambiguidades e imprecisões. Como por exemplo a afirmação "afrouxar as porcas", em um algoritmo para uma máquina de troca de pneus está sujeita a interpretações. Uma instrução mais precisa seria: "afrouxar a porca, girando-a 45° no sentido anti-horário"¹¹.

Os fluxogramas são apresentações de algoritmo em formato gráficos ou geométricos. Cada ação ou situação é representada por um quadrado ou retângulo. As instruções ou comandos, ou seja, as decisões, são indicadas por caixas diferentes, facilitando o entendimento das ideias que estão nos algoritmos¹². Ou seja, um fluxograma se resume a um símbolo inicial (onde a execução do algoritmo começa) e um ou mais símbolos finais (pontos onde a execução do algoritmo encerra). A partir do símbolo inicial existe um único caminho a ser seguido, ou seja, uma única sequência de execução das instruções. Nos símbolos finais não há nenhum fluxo saindo, e nos símbolos de decisão pode existir mais de um caminho de saída¹³.

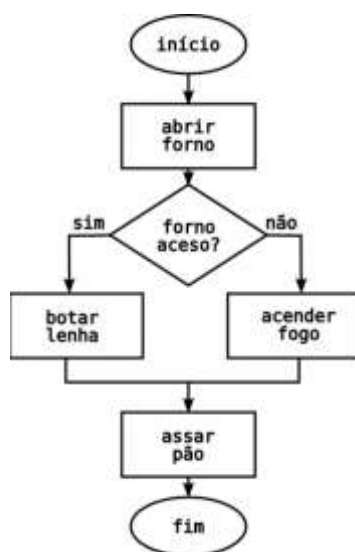


Figura 1: Exemplo de fluxograma algorítmico¹⁴

¹¹ Algoritmo e Lógica de programação. Universidade Federal do Rio Grande do Norte, Centro de Tecnologia, Departamento de Computação e Automação Algoritmo e Lógica de Programação. Algoritmos, Parte 1. Eng. Química, maio 2004. In https://www.dca.ufrn.br/~affonso/DCA800/pdf/algoritmos_parte1.pdf, pp. 5-6.

¹² *Idem, ibidem*, pp. 6-7.

¹³ *Idem, ibidem*.

¹⁴ In: http://www.cristiancechinel.pro.br/my_files/algorithms/bookhtml/node15.html.

Já a forma de representação de algoritmos em pseudocódigo tem muitos detalhes, como a definição dos tipos das variáveis usadas. Esta representação, por ser muito parecida com as linguagens de programação, acaba por permitir diretamente (na maioria das vezes) a tradução de um algoritmo nela representado para uma linguagem de programação específica¹⁵.

```
leia (x, y) {Esta linha é um comentário}
se x > y então
    escreva ("x é maior")
senão
    se y > x então
        escreva ("y é maior")
    senão
        escreva ("x e y são iguais")
    fim-se
fim-se
```

Figura 2: Exemplo de representação de algoritmo por pseudocódigo¹⁶

Portanto, as diversas formas de representação de algoritmos diferem entre si pela quantidade de detalhes de implementação que fornecem, bem como dependem em qual e para qual situação serão utilizadas.

1.1. Sistemas de *Big Data*

Primeiramente deve-se entender o que são os dados. Dados são conjuntos de valores de variáveis qualitativas ou quantitativas sobre eventos, pessoas ou objetos, ou seja, factos individuais ou estatísticos obtidos por meio de coletas de dados, seja como observação ou medição. Ressalta-se que dados e informações têm significados diferentes. Os dados são factos, tais como números, palavras, observações ou apenas descrições de coisas que, se não colocados em contexto não possuem valor. Entretanto, a informação é o dado de maneira organizada e que pode gerar conhecimento¹⁷.

O *Big Data*, segundo a classificação de alguns autores, é descrito como “5 v”, ou seja, tem grande *volume*, consistindo em petabytes, zettabytes de dados; *velocidade*, que consiste na rápida criação dos dados; *variedade*, que se refere aos dados estruturados e os não

¹⁵ Algoritmo e Lógica de programação. Universidade Federal do Rio Grande do Norte, Centro de Tecnologia, Departamento de Computação e Automação Algoritmo e Lógica de Programação. Algoritmos, Parte 1. Eng. Química, maio 2004. In https://www.dca.ufrn.br/~affonso/DCA800/pdf/algoritmos_parte1.pdf, p. 05.

¹⁶ In: http://www.cristiancechinell.pro.br/my_files/algorithms/bookhtml/node15.html.

¹⁷ In <https://www.datascienceacademy.com.br/course/intro-ciencia-de-dados-3>.

estruturados, que nesse último são a maioria e são extraídos de redes sociais, internet, etc.; *veracidade*, que se refere à qualidade dos dados, pois devido ao enorme volume e variedade de informações é preciso saber gerenciar o conteúdo e a qualidade dos dados. E por último o *valor*, que é o valor de um dado, propriamente dito, passível de análise e que possa ser aplicado no processo a que foi destinado¹⁸.

Em Gartner temos que *Big Data* são ativos de informações de alto volume, alta velocidade e alta variedade que exigem formas inovadoras e econômicas de processamento de informações que permitem uma visão aprimorada, tomada de decisões e automação de processos¹⁹. Ou seja, é uma imensa quantidade de dados disponíveis que não conseguem ser analisados por processos computacionais tradicionais e que geram conhecimento e inteligência a partir dessas grandes quantidades de dados²⁰.

Contudo, toda essa quantidade de dados precisa ser coletada e estudada para se obter conhecimento, ou seja, a análise dos dados é essencial. A analítica dos dados pode ser classificada em prescritiva, diagnóstica, descritiva e preditiva. Vejamos²¹:

- *Análise Prescritiva* é a análise baseada em estudos de casos ou factos, avaliando possíveis consequências sobre as ações tomadas. Identifica cada possível resultado em cada ação;
- *Análise Diagnóstica* considera eventos ocorridos para viabilização de tomadas de decisões baseadas em factos;
- *Análise Descritiva* avalia os dados em tempo real atribuindo respostas para o momento;
- *Análise Preditiva* utiliza a mineração de dados históricos para analisar tendências ou possibilidades futuras.

Uma das etapas do *Big Data* é o chamado *Data mining*, ou mineração de dados. De acordo com Aggarwal, *Big Data* é a coleta, limpeza, processamento, análise e obtenção de percepções de dados²². Para Giudici, *Data mining* é o processo de seleção, exploração e modelagem de grandes quantidades de dados com o intuito de descobrir regularidades ou relações que são inicialmente desconhecidas com o objetivo de obter resultados para a base de dados²³.

¹⁸ Kitchin, Rob. *Big Data, new epistemologies and paradigm shifts*. Big Data & Society, 2014. In: DOI: 10.1177/2053951714528481, p. 01-02.

¹⁹ In <https://www.gartner.com/en/information-technology/glossary/big-data>.

²⁰ Saisse, Renan. *Big data contra o crime: efeito minority report*. In <http://direitoeti.com.br/artigos/big-data-contra-o-crime-efeito-minority-report/>.

²¹ *Idem, ibidem*.

²² Aggarwal, Charu C. *Data Mining, The Textbook*. Springer, 2015, p.01.

²³ Giudici, Paolo. *Applied Data Mining Statistical Methods for Business and Industry*. Wiley, 2003. In: [http://index-of.co.uk/Data-Mining/Applied%20Data%20Mining-Statistical%20Methods%20for%20Business%20and%20Industry_Giudici%20P%20\(2003\).pdf](http://index-of.co.uk/Data-Mining/Applied%20Data%20Mining-Statistical%20Methods%20for%20Business%20and%20Industry_Giudici%20P%20(2003).pdf), p. 11.

Softwares de Data Mining utilizam algoritmos de reconhecimento de padrões, aliados a uma diversidade de técnicas matemáticas e estatísticas para observar um grande volume de dados e extrair informações relevantes e úteis até então desconhecidas e que aos olhos humanos seriam quase impossíveis de descobri-las, dado a grande quantidade de dados²⁴.

A mineração de dados utiliza a estatística clássica, a inteligência artificial e *machine learning*. A primeira é um dos principais métodos utilizados. A IA analisa os dados como se fosse o cérebro humano e o ML é a junção dos dois. É por meio desta técnica que é possível induzir os computadores a tomarem decisões, por meio do uso de algoritmos ao reconhecerem padrões e se tornarem capazes de realizar previsões. O processo de *Data Mining* ocorre por meio das seguintes etapas: definição do problema, exploração de dados, preparação de dados, modelagem, avaliação e implementação. É nessa última fase que acontece a importação dos resultados obtidos para os bancos de dados²⁵.

Portanto, pode-se concluir rapidamente que *Big Data* é caracterizado pela enorme quantidade de dados produzidos, e *Data mining* faz o reconhecimento dos padrões que estão inseridos nesses dados. Tanto o *Big Data* quanto o *Data Mining*, visto que se complementam, estão sendo utilizados nas mais diversas áreas atualmente. Podemos citar os avanços nos cuidados de saúde, contra fraudes governamentais, na educação, na infraestrutura das cidades (*smart cities*) e na aplicação da lei, como por exemplo, no caso da predição de crimes²⁶.

1.2. Inteligência Artificial

Big Data e inteligência artificial são tecnologias que se integram, pois a inteligência artificial precisa de uma grande quantidade de dados para funcionar e o *Big Data* é a solução. A inteligência artificial permite que as informações coletadas por *softwares* e máquinas sejam utilizadas para agilizar processos e minimizar erros. Assim sendo, inteligência artificial, ou IA (*Artificial Intelligence - AI*), é o campo da ciência da computação que estuda os agentes computacionais que agem de maneira inteligente. Ou seja, agente inteligente é um sistema computacional que tem a percepção por meio de sensores, agindo de forma autônoma em um ambiente, além de possuir capacidades de comunicação de alto-nível com outros agentes ou

²⁴ Pereira, Jorge Luis. *Análise Preditiva em Sistemas de Informação no Contexto do Big Data*. Marília, 2014. In: <https://aberto.univem.edu.br/bitstream/handle/11077/1003/Jorge%20Lu%3%ads%20Pereira.pdf?sequence=1&isAllowed=y>, p. 27.

²⁵ In: <https://www.voitto.com.br/blog/artigo/data-mining>.

²⁶ Bramer, Max. *Principles of Data Mining*, Third Edition. Springer, 2016, pp. 01-05.

humanos, desempenhando a função para a qual foi projetado²⁷.

O objetivo central da IA é criar entidades que ajam de maneira inteligente. Por conseguinte, se diz agente inteligente quando esse realiza atos que são apropriados para suas circunstâncias e objetivos, ou então, é flexível para mudar ambientes, mudar objetivos, e, portanto, aprende com as experiências anteriores, fazendo escolhas apropriadas dadas suas limitações perceptivas e computacionais²⁸.

Historicamente, foram feitas quatro abordagens à IA, mas com diferentes métodos. Um dos métodos mais famosos, é o método de Alan Turing, o chamado “Teste de Turing”, elaborado em 1950 e que é classificado como um método de fazer com que a IA “aja humanamente”²⁹.

O Teste de Turing³⁰ foi projetado para testar a capacidade de uma máquina em exibir um comportamento inteligente equivalente a um ser humano. No referido teste, um computador é aprovado se um interrogador humano, após fazer algumas perguntas escritas, não for capaz de dizer se as respostas escritas vêm de uma pessoa ou de um computador. Para possuir as capacidades de passar no teste de Turing, o computador deve ser rigorosamente programado para que tenha as habilidades de processamento de linguagem natural para permitir a comunicação em inglês, a representação do conhecimento para armazenar o que sabe e o que ouve, ter raciocínio automatizado para usar as informações armazenadas com o intuito de responder perguntas e, assim, tirar novas conclusões, bem como, se adaptar a novas circunstâncias e para detectar e extrapolar padrões. Para passar completamente no teste de Turing, o computador precisaria de uma visão computacional para entender objetos, robótica para manipular objetos, bem como, movimentar-se³¹.

Outro método utilizado para fazer com que as máquinas pensem como seres humanos é o da modelagem cognitiva. Ou seja, para dizer que um determinado programa pensa como um ser humano, é necessário existir alguma maneira de determinar como os humanos pensam, entrar no funcionamento real das mentes humanas. De acordo com esse método, há três maneiras de se fazer isso: por meio da introspecção, ou seja, tentar capturar os pensamentos;

²⁷ In <https://paginas.fe.up.pt/~lpreis/ai2002/Documents/1.Agentes.PDF>.

²⁸ Poole, David L. Mackworth, Alan K. *Artificial Intelligence: Foundations of Computational Agents*. Cambridge University Press, e-book, New York, 2010, pp. 3-10.

²⁹ Russel, Stuart J; Norvig, Peter. *Artificial Intelligence a Modern Approach*. Third Edition. E-Book Kindle, 2010, pp. 2-3.

³⁰ *Idem, ibidem*.

³¹ *Idem, ibidem*, p. 3.

através de experimentos psicológicos ao observar uma pessoa em ação; e através de imagem cerebral, que é observar o cérebro em ação. Entretanto, os pesquisadores, Allen Newell e Herbert Simon, por não se contentarem apenas que seu programa resolvesse os problemas corretamente, desenvolveram o GPS, o “*General Problem Solver*”, com o intuito de comparar o traço das etapas de raciocínio com traços dos raciocínios dos humanos ao resolver os mesmos problemas³².

Portanto, o campo interdisciplinar da ciência cognitiva reúne modelos de computador que utilizam IA e técnicas experimentais da psicologia com o intuito de construir teorias da mente humana que possam ser testadas. Tanto a inteligência artificial quanto a ciência cognitiva se desenvolveram rapidamente e continuam a se desenvolver e a se misturar, principalmente na visão computacional, que incorpora evidências neurofisiológicas em seus modelos computacionais. Outra abordagem, é a chamada abordagem das "leis do pensamento". Aristóteles foi um dos primeiros filósofos a tentar codificar o "pensamento correto", ou seja, processos de raciocínio irrefutáveis. Seus silogismos forneceram padrões para argumentos que sempre produziam conclusões corretas quando recebiam as premissas corretas, as chamadas condicionais. Como exemplo temos que, “Sócrates é um homem; todos os homens são mortais; portanto, Sócrates é mortal.” E com isso se deu o início do estudo da lógica³³.

A partir de 1965, começaram a existir programas que poderiam, em princípio, resolver qualquer problema descrito em notação lógica. Seguindo esse padrão, a lógica e a inteligência artificial aproveitaram esses programas para criar os chamados “sistemas inteligentes”. Contudo, existiram dois principais obstáculos a essa abordagem. O primeiro é o facto de não ser fácil transformar conhecimentos informais em conhecimentos formais exigidos pela linguagem lógica. E, em segundo, há uma grande diferença entre resolver um problema na teoria e resolvê-lo na prática. Embora esses dois obstáculos se apliquem a qualquer tentativa para construir sistemas de raciocínio computacional, eles apareceram primeiro na lógica tradicional³⁴.

A quarta abordagem é a do agente racional. Sabe-se que agente é apenas algo que age. Por óbvio, todos os programas de computador fazem alguma coisa, agem de alguma maneira, contudo, espera-se que os agentes de computador façam muito mais coisas, tais como operar autonomamente, entender seu ambiente, adaptar-se às mudanças, bem como criar e buscar objetivos. Por conseguinte, podemos dizer que um agente racional é aquele que age de

³² Russel, Stuart J; Norvig, Peter. *Artificial Intelligence a Modern Approach*. Third Edition. E-Book Kindle, 2010, p. 3.

³³ *Idem*, *ibidem* p. 4.

³⁴ *Idem*, *ibidem*.

modo a alcançar o melhor resultado ou, quando não houver certeza, ter o melhor resultado esperado³⁵.

Nessa fase se dá ênfase às inferências corretas. Fazer inferências corretas faz parte de ser um agente racional, pois agir racionalmente é raciocinar logicamente até à conclusão de que uma determinada ação alcançará os objetivos e depois irá agir sobre essa conclusão. Contudo, em algumas situações não há nada de correto a ser feito, porém deve ser feito algo. Existem também maneiras de agir racionalmente que não se pode dizer que envolvam inferência³⁶.

A abordagem do agente racional é mais geral do que a abordagem das "leis do pensamento", pois a inferência correta é apenas um dos vários mecanismos possíveis para alcançar a racionalidade. Também é mais favorável ao desenvolvimento científico do que as abordagens baseadas no comportamento ou no pensamento humano, além do padrão de racionalidade ser matematicamente bem definido. O comportamento humano, por outro lado, é definido pela soma de todas as coisas que os humanos fazem³⁷.

Portanto, o objetivo científico central da inteligência artificial é entender os princípios que tornam o comportamento inteligente possível em sistemas naturais ou artificiais. Esse entendimento é feito por meio de análise de agentes naturais e artificiais, formulação de hipóteses sobre o que é necessário para a construção de agentes, bem como projeção, construção e experimentação de sistemas computacionais que executem tarefas que exijam alto nível de inteligência³⁸.

1.3. *Machine Learning*

Um dos maiores desafios enfrentados atualmente pelas empresas e organizações é conseguir estruturar a grande quantidade de informações que possuem, bem como, uma maneira de utilizá-las. *Machine learning* (ML) ou aprendizagem de máquina, é definido como um processo automatizado que extrai padrões de dados. Ou seja, é o campo de estudo que dá aos computadores a capacidade de aprender sem ser explicitamente programado³⁹.

³⁵ Russel, Stuart J.; Norvig, Peter. *Artificial Intelligence a Modern Approach*. Third Edition. E-Book Kindle, 2010, p. 3.

³⁶ Poole, David L. Mackworth, Alan K. *Artificial Intelligence: Foundations of Computational Agents*. Cambridge University Press, New York, 2010, pp. 10-12.

³⁷ *Idem, ibidem*.

³⁸ *Idem, ibidem*.

³⁹ Kelleher, John; Namee, M. Brian; Darcy, Aoife. *Fundamentals of machine learning for predictive data analytics: algorithms, worked examples, and case studies*. E-book, 2015, p. 43.

Mas como funciona o *machine learning*? Para que o ML funcione são necessários os algoritmos. Como já visto anteriormente, algoritmos são sequências de instruções dadas ao computador para que este execute determinada tarefa. Contudo, não há muitas vezes um algoritmo para realizar esse processamento e é necessário criá-lo. Como o exemplo, no *spam* de *e-mail* o algoritmo criado é para detectar quais *e-mails* são *spam* e quais não são. Através do uso do algoritmo o programa vai entender qual tarefa ele precisa executar, porém, ele precisa saber separar o que é um *spam* do que não é. Nesse caso específico, o problema é um arquivo de texto, e a resposta deve ser do tipo sim/não, indicando se a mensagem é ou não um *spam*. Assim sendo, utilizando o ML o algoritmo vai aumentando sua base de dados e entendendo quais os tipos de mensagens são *spam* ou não. Pode ser que nem sempre acerte, mas com o passar do tempo e das informações, os acertos se tornam mais frequentes⁴⁰.

Daumé III define em uma linguagem simples que ML é uma tarefa de prever o futuro com base em factos do passado⁴¹. Ou seja, *Machine learning* é uma área de pesquisa da IA voltada ao desenvolvimento de programas de *software* com a capacidade de aprender a executar uma tarefa, tendo como base sua própria experiência⁴². São *softwares* capazes de aprender sozinhos, utilizando-se de um conjunto de dados que representam experiências e conhecimentos já obtidos.

1.3.1 Aprendizagem supervisionada e não supervisionada

Para *machine learning*, existem as técnicas de aprendizagem supervisionada e não supervisionada, a depender do tamanho da quantidade e volume das informações. Na aprendizagem de máquina supervisionada e seus algoritmos, é essencial que exista a participação humana para a obtenção de um melhor resultado. A aprendizagem supervisionada ocorre ao elaborar um modelo que faz previsões baseadas em evidências. Portanto, um algoritmo de aprendizagem supervisionada ocorre quando se utiliza um conjunto conhecido de exemplos, bem como suas respostas conhecidas, treinando assim, um modelo para gerar previsões satisfatórias para as respostas dos novos dados. Ou seja, treina um modelo em dados de entrada e saída

⁴⁰ Franco, Cristiano Roberto. *Inteligência artificial*. Editora e Distribuidora Educacional S.A. Londrina, 2014, pp. 79-81.

⁴¹ Daumé III, Hal. *A Course in Machine Learning*, 2012. In: http://ciml.info/dl/v0_8/ciml-v0_8-all.pdf, p. 8.

⁴² Cerri, Ricardo; Ferreira de Carvalho, André Carlos Ponce de Leon. *Aprendizagem de Máquina: Breve Introdução e Aplicações*. Cadernos de Ciência & Tecnologia, Brasília, v. 34, n. 3, p. 297-313, set./dez. 2017. In: <https://ainfo.cnptia.embrapa.br/digital/bitstream/item/184785/1/Aprendizagem-de-maquina-breve-introducao.pdf>, p. 298.

conhecidos, fazendo com que ele possa prever resultados futuros⁴³. Assim sendo, para cada sequência de entrada é dada uma saída desejada, sendo que o objetivo da máquina é aprender a produzir a saída correta para entradas novas, que não fizeram parte de seu conjunto de treinamento⁴⁴.

Para construir os modelos usados em aplicativos preditivos de análise de dados, utiliza-se técnicas de aprendizagem de máquina supervisionada. Estas técnicas aprendem automaticamente um modelo da relação entre um conjunto de recursos descritivos e um recurso de destino com base em um conjunto de exemplos ou instâncias. Podemos então usar esse modelo para fazer previsões ou novas instâncias de treinamentos (amostras). Por exemplo, o filtro de *spam* é um programa de ML que pode aprender a sinalizar *spam*, dado segundo exemplos de *e-mails* de *spam* e exemplos de não *spam*⁴⁵.

A aprendizagem supervisionada utiliza técnicas de classificação e de regressão para desenvolver os modelos preditivos. As técnicas de classificação preveem respostas discretas, como no caso do exemplo do *e-mail*, se é ou não *spam*. São previsões já pré-definidas. Já a técnica de regressão são previsões baseadas em valores numéricos contínuos⁴⁶.

Portanto, o algoritmo de aprendizagem é um indutor que recebe um conjunto de exemplos para os quais os rótulos da classe associada são conhecidos. Cada exemplo é descrito por um vetor de valores e pelo rótulo da classe associada. O objetivo do indutor é que se possa determinar corretamente a classe de novos exemplos que ainda não foram rotulados⁴⁷. Dentro do método de aprendizagem supervisionada existe um método chamado de árvore de decisão, um dos métodos de aprendizagem mais utilizados na prática e que utiliza a estratégia em que um problema mais complexo é dividido em problemas mais simples, resolvidos de forma recursiva. Ou seja, é um método de aprendizagem supervisionada que constrói árvores de classificação a partir de exemplos⁴⁸.

A chamada aprendizagem não supervisionada é aquela que encontra padrões ocultos ou estruturas intrínsecas nos dados. Ou seja, a máquina recebe um conjunto de entradas,

⁴³ In: <https://www.mathworks.com/discovery/machine-learning.html>.

⁴⁴ Franco, Cristiano Roberto. *Inteligência artificial*. Uniasselvi, 2017. In: <https://www.uniasselvi.com.br/extranet/layout/request/trilha/materiais/livro/livro.php?codigo=22869>, p.127.

⁴⁵ Géron, Aurélien. *Hands-On Machine Learning with Scikit-Learn and TensorFlow*. Editora O'Reilly Media, E-book 2017, pp. 19-20.

⁴⁶ *Idem, ibidem*.

⁴⁷ Machado, Vinicius Ponte. *Inteligência Artificial*. In: http://www.uece.br/computacaoead/index.php/downloads/doc_download/2177-inteligencia-artificial, p.42.

⁴⁸ *Idem, ibidem*, p.43.

mas nenhum conjunto de saída correspondente. Assim sendo, o *software* deve encontrar padrões de semelhanças e diferenças entre os dados e com esses padrões gerar novas saídas corretas⁴⁹.

Destaca-se que, na aprendizagem não supervisionada, a máquina aprende os padrões sozinha, sem interferência humana⁵⁰. É utilizado para extrair inferências de conjuntos de dados que consistem em dados de entrada sem respostas rotuladas, ou seja, para análise exploratória de dados com o intuito de encontrar informações ocultas, padrões ou agrupamentos de dados, os chamados *clusters*⁵¹. O agrupamento conceitual foi introduzido por Michalski, como um processo de construção de uma rede de conceitos. Após a determinação dos agrupamentos, é necessária uma análise para determinar o que cada agrupamento significa no contexto do problema⁵².

Ou seja, o agrupamento ou “clusterização” ocorre através de iterações, isto é, uma sequência de passos em que se busca agrupar os dados de forma que esses agrupamentos façam sentido, sendo este agrupamento, o tipo de aprendizagem não supervisionada mais comum⁵³. Como exemplo de pedidos de agrupamento estão as análises de sequência genética, pesquisa de mercado e reconhecimento de objetos⁵⁴.

É necessário utilizar a aprendizagem de máquina ou *machine learning* quando tiver uma tarefa complexa ou um problema envolvendo uma grande quantidade de dados e muitas variáveis. Contudo, escolher o algoritmo certo pode ser complicado, pois existem inúmeros algoritmos de ML supervisionado e não supervisionado, sendo que cada um adota uma abordagem diferente para a aprendizagem, não existindo um método melhor. É quase um método de tentativa e erro, porém, a seleção de algoritmos depende do tamanho, tipo de dados, das informações que deseja obter e como essas informações serão usadas⁵⁵.

⁴⁹Franco, Cristiano Roberto. *Inteligência artificial*. Uniasselvi, 2017. In: <https://www.uniasselvi.com.br/extranet/layout/request/trilha/materiais/livro/livro.php?codigo=22869>, p.128.

⁵⁰ *Idem, ibidem*, p. 131.

⁵¹ In: <https://www.mathworks.com/discovery/machine-learning.html>

⁵² Machado, Vinicius Ponte. *Inteligência Artificial*. In: http://www.uece.br/computacaoead/index.php/downloads/doc_download/2177-inteligencia-artificial, p.46.

⁵³Franco, Cristiano Roberto. *Inteligência artificial*. Uniasselvi, 2017. In: <https://www.uniasselvi.com.br/extranet/layout/request/trilha/materiais/livro/livro.php?codigo=22869>, p.130.

⁵⁴ *Idem, ibidem*.

⁵⁵ In: <https://www.mathworks.com/discovery/machine-learning.html>.

1.3.2. Redes neurais artificiais: um exemplo do uso de *Machine Learning*

As redes neurais artificiais foram introduzidas pela primeira vez em 1943 pelo neurofisiologista Warren McCulloch e pelo matemático Walter Pitts. Eles apresentaram um modelo computacional simplificado de análise biológica de neurônio, que mais tarde ficou conhecido como neurônio artificial, ou seja, possuía uma ou mais entradas e uma saída binária. O neurônio artificial simplesmente ativa sua saída quando mais de um determinado número de entradas estiver ativo. McCulloch e Pitts mostraram que mesmo com um modelo tão simplificado é possível construir uma rede de neurônios artificiais que calculam qualquer proposição lógica que você deseja, usando lógica proposicional. Esta foi a primeira rede neuronal artificial⁵⁶.

Contudo, somente na década de 90, com técnicas de *Machine Learning* os pesquisadores obtiveram bases teóricas mais fortes. Atualmente, existe uma enorme quantidade de dados disponíveis para treinar redes neurais. Por tal motivo que as RNAs frequentemente superam outras técnicas de ML em áreas muito grandes e complexas⁵⁷. As Redes Neurais Artificiais (RNAs) são modelos de aprendizagem de máquina (*machine learning*) baseados na atividade das redes de neurônios biológicos. A forma como o cérebro processa as informações é extremamente complexa, pois o cérebro tem a capacidade de organizar seus neurônios de forma a realizar processamentos, tais como, reconhecimento de padrões, controle motor, etc., de maneira muito mais rápida e eficiente do que uma máquina. Ou seja, as redes neurais artificiais são máquinas elaboradas para realizar funções que o cérebro realizaria normalmente⁵⁸.

Um neurônio biológico é composto pelos dendrites, que são responsáveis pela coleta dos impulsos oriundos de outros neurônios; pelo corpo celular que processa os sinais recebidos pelos dendrites; pelos axônios, que são encarregados pela multiplicação dos sinais e pelas sinapses, que são as conexões do axônio de um neurônio com a dendrite de outro. Assim sendo, um neurônio processa informações fundamentais para a operação de uma rede neuronal⁵⁹.

O modelo de neurônio computacional, que é o neurônio artificial, exhibe características semelhantes ao modelo biológico. Esses modelos artificiais são os pilares para os projetos de redes neurais, quais também possuem o conjunto de sinapses, que neste caso é

⁵⁶ Patterson, Josh. Gibson, Adam. *Deep Learning a Practitioner's Approach*. Ed. O'Reilly Media, E-book., 2017, p.87.

⁵⁷ Géron, Aurélien. *Hands-On Machine Learning with Scikit-Learn and TensorFlow*. Editora O'Reilly Media, E-book, 2017, p.318.

⁵⁸ Pacheco, César Augusto Rodrigues. Pereira, Natasha Sophie. *Deep Learning Conceitos e Utilização nas Diversas Áreas do Conhecimento*. Revista Ada Lovelace. v. 2 (2018) jan-dez p. 34-49 In: <http://anais.unievangelica.edu.br/index.php/lovelace>, p.37.

⁵⁹ In: <https://pt.khanacademy.org/science/biology/human-biology/neuron-nervous-system/a/overview-of-neuron-structure-and-function>.

composto pelos sinais de entrada e pesos sinápticos, de modo que, cada sinal de entrada será multiplicado pelo peso sináptico associado e ele. Por conseguinte, o neurônio irá tratar de maneira diferente cada impulso recebido, atribuindo a cada um, um valor diferente. Existem os somadores responsáveis por somar os sinais de entrada, bem como, a função de ativação que é utilizada para restringir a amplitude do sinal de saída do neurônio. Ou seja, são sistemas adaptados para modificarem sua própria estrutura por meio de informações novas durante a aprendizagem de máquina, que pode ser o supervisionada ou não supervisionada⁶⁰.

1.3.3. Uso das redes neurais

Uma rede neuronal requer a especificação de sua arquitetura sendo definida pelo número de neurônios das camadas de entrada e de saída, o número de camadas ocultas, bem como a quantidade de neurônios e o valor dos pesos entre entrada e saída⁶¹. O principal objetivo da pesquisa sobre redes neurais artificiais é desenvolver modelos neurais baseados em modelos matemáticos, para que estes possam realizar as mais diversas funções. Uma rede neuronal passa por um processo de treinamento com base em casos reais para que com os dados recebidos possa executar adequadamente o processamento esperado. E é nesse sentido que as redes neurais diferem da computação básica convencional. Nesta última, existem um conjunto de regras pré-fixadas, já as RNAs são capazes de extrair regras básicas dos dados reais. Ou seja, elas aprendem com cada dado que entra e melhoram seu desempenho por meio de ajustes. Sua aprendizagem é finda quando a rede neuronal consegue criar soluções para vários problemas⁶².

Existem diversos tipos de algoritmos de aprendizagem e cada um é específico para determinado modelo de RNA. E como já dito acima, as principais formas de aprendizagem podem ser divididas em aprendizagem supervisionada e aprendizagem não supervisionada⁶³. Na supervisionada é utilizada um agente externo que indica para a RNA um comportamento de acordo com o padrão de entrada. A rede, por conseguinte, é treinada para fornecer a saída desejada para

⁶⁰ Pacheco, César Augusto Rodrigues. Pereira, Natasha Sophie. *Deep Learning Conceitos e Utilização nas Diversas Áreas do Conhecimento*. Revista Ada Lovelace. v. 2 (2018) jan-dez p. 34-49. In: <http://anais.unievangelica.edu.br/index.php/lovelace>, pp.38-39.

⁶¹ Santos, Murilo Alves. Souza, Daniel Henrique Silva de. Penedo, Antonio Sergio Torres. Martins, Elvis Silveira. *Aplicação de redes neurais no Brasil: um estudo bibliométrico*. Biblionline, João Pessoa, v. 12, n. 2, 2016..In: https://www.researchgate.net/publication/303957049_APLICACAO_DE_REDES_NEURONAIIS_NO_BRASIL_UM_ESTUDO_BIBLIOMETRICO, p. 101 – 116.

⁶² Finocchio, Marco Antonio Ferreira. *Noções de Redes Neurais Artificiais*. UTFPR, 2014.In: <http://paginapessoal.utfpr.edu.br/mafinocchio/labs-laboratorio-de-seguranca-e-iluminacao/redes-neurais-artificiais/NOCaO%20DE%20REDES%20NEURONAIIS%20ARTIFICIAIS.pdf/view>, pp.22-24.

⁶³ In <https://pt.khanacademy.org/science/biology/human-biology/neuron-nervous-system/a/overview-of-neuron-structure-and-function>.

aquela entrada específica. Os valores de entrada e saída do conjunto de treinamento são aplicados sequencialmente, e as diferenças vão sendo ajustadas. Já na aprendizagem não supervisionada, dispensa-se o agente externo que indica a resposta desejada para os padrões de entrada e passam a ser utilizados exemplos análogos para que a rede neuronal possa responder de maneira similar. Por conseguinte, o algoritmo de treinamento modifica os pesos da rede para produzir valores similares entre si e que produzirão o mesmo padrão de saída. Esse sistema de aprendizagem deve descobrir características, desenvolvendo sua própria representação de entrada⁶⁴.

As RNAs possuem inúmeras aplicações como, por exemplo no uso bancário, diagnósticos médicos e na justiça preditiva, como será explicado melhor em tópico dedicado ao tema. O aumento do uso reside na capacidade dessas redes de se modelarem ao cérebro humano. As RNAs aparecem cada vez mais em áreas com funções de previsão e classificação, em que se destaca o potencial prévio assertivo, bem como na precisão de diagnóstico⁶⁵.

Como dito, são incontáveis as aplicações que utilizam as redes neurais artificiais, contudo, é importante salientar que o uso deve ser utilizado como uma ferramenta de auxílio a depender da área, e não como substituto ao humano.

1.4. *Deep Learning*

Atualmente, a inteligência artificial está progredindo rapidamente e a aprendizagem profunda ou *deep learning* é o que mais contribui para isso. Uma definição de *deep learning* (DL) que seja simples e fácil de compreender, é a de que *deep learning* é um subcampo do *machine learning* ou aprendizagem de máquina. Resumidamente, o *deep learning* faz parte do *machine learning* e utiliza as redes neurais (algoritmos que simulam a capacidade das células neurais com o intuito de reproduzir os cérebros humanos) para melhorar o aprendizagem de máquina, e por conseguinte, a inteligência artificial⁶⁶. A hierarquia pode ser representada pela seguinte figura⁶⁷:

⁶⁴ Finocchio, Marco Antonio Ferreira. *Noções de Redes Neurais Artificiais*. UTFPR, 2014. In: <http://paginapessoal.utfpr.edu.br/mafinocchio/labs-laboratorio-de-seguranca-e-iluminacao/redes-neuronais-artificiais/NOCaO%20DE%20REDES%20NEURONAI%20ARTIFICIAIS.pdf/view>, pp.22-24.

⁶⁵ Santos, Murilo Alves. Souza, Daniel Henrique Silva de. Penedo, Antonio Sergio Torres. Martins, Elvis Silveira. *Aplicação de redes neurais no Brasil: um estudo bibliométrico*. Biblionline, João Pessoa, v. 12, n. 2, 2016. In: https://www.researchgate.net/publication/303957049_APLICACAO_DE_REDES_NEURONAI%20NO_BRASIL_UM_ESTUDO_BIBLIOMETRICO, pp. 101 – 116.

⁶⁶ Patterson, Josh. Gibson, Adam. *Deep Learning a Practitioner's Approach*. Ed. O'Reilly Media, E-book, 2017, pp.11-12.

⁶⁷ In <https://medium.com/data-hackers/deep-learning-do-conceito-%C3%A0s-aplica%C3%A7%C3%B5es-e8e91a7c7eaf>.

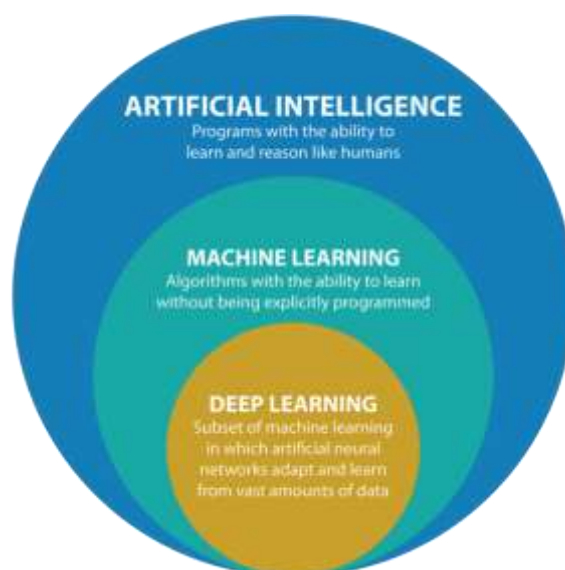


Figura 3: *Artificial Intelligence*

Um dos principais motivos para o uso do *deep learning* está relacionado com os dados que são capazes de usar, pois estes tendem a ter um bom desempenho com uma grande quantidade de dados⁶⁸. O *deep learning* se difundiu rapidamente devido à busca por algoritmos de aprendizagem não supervisionada com o intuito de aprender características de dados não rotulados, e assim, suas estruturas de múltiplas camadas começaram a obter resultados positivos depois da elaboração do algoritmo de treinamento⁶⁹.

Esses algoritmos relacionam termos e palavras com o intuito de inferir um significado para que as máquinas que utilizem o *deep learning* possam decifrar com uma linguagem natural a grande quantidade de dados presentes nos algoritmos⁷⁰. Uma das grandes vantagens em utilizar o *deep learning* ao invés de somente algoritmos tradicionais é o facto de a extração de recursos ser automática. Ou seja, automatiza o processo de decisão de quais características de um conjunto de dados podem ser usados como indicadores para rotular esses dados de maneira confiável e rápida⁷¹.

Portanto, o *deep learning* deixa menos complexo o uso dos algoritmos, deixando a aprendizagem mais fácil e proporcionando a aplicação da inteligência artificial nas mais diversas

⁶⁸ In: <https://mc.ai/deep-learning-series-chapter-1-introduction-to-deep-learning/>.

⁶⁹ Pacheco, César Augusto Rodrigues. Pereira, Natasha Sophie. *Deep Learning Conceitos e Utilização nas Diversas Áreas do Conhecimento*. Revista Ada Lovelace. In <http://anais.unievangelica.edu.br/index.php/lovelace>, v. 2, 2018, p.41.

⁷⁰ In <https://gaea.com.br/afinal-o-que-e-deep-learning/>.

⁷¹ Patterson, Josh. Gibson, Adam. *Deep Learning a Practitioner's Approach*. Ed. O'Reilly Media, E-book., 2017, pp.11-12.

áreas. Com a precisão do DL, algumas áreas melhoraram significativamente ao longo dos anos e continuam a evoluir, dentre elas pode-se destacar⁷² o reconhecimento facial; carros autônomos; reconhecimento de fala (humanoides): *Siri, a Cortana, Google Now*. Isso graças ao avanço do DL e PNL⁷³ que tornou possível essa interação eficiente. Além destas, também são muito utilizados nas áreas do *e-commerce*, medicina e diagnóstico, redes sociais, detecção de fraudes e previsão. Este último será abordado em tópico específico sobre a previsão de crimes.

1.5. *Black Box problem*

Um dos desafios que a IA enfrenta é a confiança às decisões e respostas fornecidas por ela, principalmente em relação ao uso de modelos de aprendizagem de máquina e do *black box*. Os modelos de aprendizagem de máquina *black box* estão sendo muito utilizados para tomadas de decisão de alto risco em diversas áreas, dentre elas, a medicina e justiça criminal⁷⁴. Esse problema ocorre porque as ferramentas baseadas em inteligência artificial não demonstram como e por qual razão chegam a determinadas conclusões. Apenas se sabe que um algoritmo decidiu qual seria a melhor resposta. Na computação, uma caixa preta é um dispositivo, sistema ou programa que permite que você veja a entrada e a saída dos dados, mas não dá nenhuma visão dos processos e funcionamento entre eles. O problema ocorre nessa fase, pois se não se pode entender a maneira como é tomada a decisão, como saber se ela é uma decisão fundamentada ou se ela é eticamente e moralmente correta?⁷⁵

Cynthia Rudin, Professora de Ciências da Computação da Universidade de Duke, diferencia dois tipos de sistemas de *black box*. O primeiro tipo inclui redes neurais que é a arquitetura utilizada em algoritmos de aprendizagem profunda. Esses algoritmos são compostos de camadas sobre camadas de variáveis interconectadas que se ajustam conforme a rede é treinada, com milhões ou até bilhões de dados (*big data*). O segundo tipo são os algoritmos proprietários, que fazem referência as empresas que ocultam os detalhes de seus sistemas, a fim de proteger a propriedade intelectual por exemplo. Ou seja, as pessoas que criaram o sistema de

⁷² In: <https://mc.ai/deep-learning-series-chapter-1-introduction-to-deep-learning/>.

⁷³ Processamento de língua natural é uma subárea da ciência da computação, inteligência artificial e da linguística que estuda os problemas da geração e compreensão automática de línguas humanas naturais. In https://en.wikipedia.org/wiki/Neuro-linguistic_programming.

⁷⁴ Stop, Rudin, C. Explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nat Mach Intell* 1, 206–215 (2019). In <https://doi.org/10.1038/s42256-019-0048-x>.

⁷⁵ In <https://www.thinkautomation.com/bots-and-ai/the-ai-black-box-problem/>.

IA podem ter conhecimento de sua lógica interna, mas as pessoas que os usam não⁷⁶.

A literatura tenta explicar o funcionamento do *black box* utilizando os termos IA explicável e IA interpretável. A chamada IA interpretável utiliza algoritmos que fornecem uma explicação clara de seus processos de tomada de decisão, qual pode ser traçado o caminho que seus dados de entrada percorrem ao passar pelo modelo de IA, que nesses casos são geralmente de *machine learning*. Entretanto, a IA explicável são ferramentas que se aplicam a algoritmos que não fornecem uma explicação clara de suas decisões. Ainda segundo Rudin, os métodos de explicabilidade não fornecem necessariamente *insights* sobre como o modelo de IA de *black box* funciona, apenas mostram como as previsões estão relacionadas aos recursos⁷⁷.

Essa tendência é especialmente preocupante em áreas da saúde e justiça criminal. Em razão disso, já existem grupos de pesquisa sobre viés algorítmico e sistemas de IA. Porém, como o funcionamento dos algoritmos ainda são inacessíveis em sua maior parte, não há como ter uma investigação ampla e concreta de seu funcionamento. De acordo com Novais e Freitas⁷⁸, o Parlamento Europeu considera⁷⁹ importante que reduza a opacidade de funcionamento dos robôs e inteligência artificial, especialmente quando se esteja perante decisões tomadas por esses sistemas cujo impacto sobre a vida das pessoas seja substancial.

⁷⁶ Dickson, Ben. *The dangers of trusting black-box machine learning*. In <https://bdtechtalks.com/2020/07/27/black-box-ai-models/>

⁷⁷ *Idem, ibidem*.

⁷⁸ Novais, Paulo. Freitas, Pedro Miguel. *Inteligência Artificial e regulação de algoritmos*. Universidade do Minho, 2018, p.36.

⁷⁹ Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (2015/2103(INL)). In: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html?redirect#BKMD-13

Capítulo 2: Enquadramento normativo

1. Inteligência Artificial e a proteção de dados no contexto Europeu

Com o crescente uso da inteligência artificial e do *big data* se faz necessário a proteção e regulamentação do uso dos dados, com o intuito de resguardar os direitos e garantias fundamentais dos indivíduos. O artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia⁸⁰ e o artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE)⁸¹ estabelecem que todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito. Ainda, conforme o Conselho Europeu de Proteção de Dados (EDPB), “todo o processamento de dados pessoais através de um algoritmo enquadra-se no âmbito do RGPD”⁸². Ou seja, quando os dados pessoais são processados por um sistema de IA o RGPD deve ser aplicado.

No prefácio do Regulamento 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, o chamado RGPD (Regulamento Geral sobre a Proteção de Dados), diz-se, entre outras coisas, o seguinte, que merece aqui ser destacado: “a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. E acrescenta-se ainda, “os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais”⁸³.

O Regulamento Geral sobre a Proteção de Dados (RGPD) trata sobre a regulação dos dados e sua proteção e não sobre a IA em específico (toda a tecnologia que utiliza dados é englobada pelo RGPD). Entretanto, existem disposições do RGPD que tratam especificamente de alguns dos problemas e riscos comumente associados à IA, como aqueles relacionados ao princípio de proteção de dados, de minimização de dados e a exigência de que os dados pessoais sejam processados de forma legal, bem como, disposições que fazem alusão a tecnologias que

⁸⁰ Carta dos Direitos Fundamentais da União Europeia. In <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR>.

⁸¹ Tratado sobre o Funcionamento da União Europeia. In <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12012E/TXT&from=PT>.

⁸² In https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out2020_0004_intveldalgorithms_en.pdf, p. 2.

⁸³ Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. In <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>, p. 1.

incorporam aspectos da IA, como por exemplo, as disposições sobre decisões automatizadas.

Em junho de 2020, o *European Parliamentary Research Service*, no Departamento *Scientific Foresight Unit*, elaborou um estudo para o “*Panel for the Future of Science and Technology*”, intitulado “*The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*” sob a direção do Professor Giovanni Sartor e coautoria da Dra. Francesca Lagioia⁸⁴. Nesse estudo, que merece muita atenção pois é de grande importância e aprofundamento no assunto, os autores destacam a aplicabilidade do RGPD na IA⁸⁵.

O RGPD contém alguns termos que se referem à *Internet*, porém, não existe o termo inteligência artificial. Contudo, muitas disposições do RGPD são relevantes para IA. A começar pelo artigo 4º do RGPD, onde se encontram as definições dos atores presentes na respectiva lei. Todavia, para o respectivo estudo serão explicados apenas algumas dessas definições, ou seja, as que têm maior uso na inteligência artificial e *big data*. Vejamos⁸⁶:

- *Dados pessoais*: o conceito de dados pessoais desempenha um papel fundamental no RGPD, pois a conexão entre a natureza pessoal da informação e o desenvolvimento tecnológico é mencionado no Regulamento 2018/1807, na consideração 9 – se o desenvolvimento tecnológico possibilitar a transformação de dados anônimos em pessoais, tais dados devem ser tratados como dados pessoais, e o Regulamento (UE) 2016/679 deve aplicar-se em conformidade⁸⁷;
- *Criação de perfil*: para essa, embora não use referência explícita à IA, trata do processamento que é atualmente realizado com tecnologias de IA. Este processamento consiste em usar os dados relativos à pessoa para inferir informações sobre outros aspectos dessa pessoa. As abordagens baseadas em *machine learning*, muitas vezes servem para fornecer inferências, ou seja, classificações, previsões ou decisões, quando estas são aplicadas a dados relativos a indivíduos. Como por exemplo, a probabilidade de que pessoas condenadas podem reincidir, previsto com base em seu histórico criminal, seu caráter e antecedentes pessoais⁸⁸;

Consentimento: esse deve ser dado livremente, ser específico, informado e ser expresso por meio de uma ação afirmativa clara e deve abranger todas as atividades de processamento realizadas

⁸⁴ The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. In [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf).

⁸⁵ Idem, *ibidem*.

⁸⁶ Idem, *ibidem*, pp.35-43.

⁸⁷ Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho, 14/11/2018. In: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018R1807&from=PT>.

⁸⁸ The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. In [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf), pp. 35-43.

para a mesma finalidade ou quando o processamento tiver múltiplas finalidades, o consentimento deve ser dado à todos, pois tem papel fundamental na proteção de dados, exceto para os dados que forem coletados para determinados fins sejam processados para outros fins, desde que sejam compatíveis com os originais, que é permitido pelo RGPD.

Como muitos autores destacam, a IA e o *big data* desafiam os princípios de proteção de dados. De acordo com o referido estudo, “*The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*”, deve-se considerar cada princípio separadamente⁸⁹. Desta maneira, no artigo 5º do RGPD estão elencados os princípios relativos ao tratamento de dados pessoais, dentre eles destaca-se⁹⁰:

- Artigo 5º1(a): justiça e transparência, pois exige-se que os dados pessoais sejam tratados “de forma legal, justa e transparente em relação ao titular dos dados”. Ou seja, o princípio da transparência exige que qualquer informação dirigida ao público ou para o titular dos dados deve ser acessível e de fácil entendimento;
- Artigo 5º1(b): limitação da finalidade, segundo o qual os dados pessoais devem ser coletados para fins específicos e explícitos. Esse mesmo princípio também aparece nos artigos 13 (1, c) e 14 (1, c), exigindo que os controladores forneçam informações sobre “os fins do tratamento para o qual os dados pessoais se destinam, bem como a base jurídica para o tratamento”;
- Artigo 5º1(c): minimização de dados, segundo o qual os dados pessoais devem ser “adequados, relevantes e limitados ao que é necessário em relação aos fins para os quais são processados”;
- Artigo 5º1(d): precisão, que exige que os dados sejam “precisos e, sempre que necessário, mantido atualizados”, além de que iniciativas sejam tomadas para corrigir possíveis inexatidões. Este princípio também se aplica a dados pessoais que são usados como uma entrada para o sistema de IA, especialmente quando os dados pessoais são usados para fazer inferências ou decisões. Para o uso dos dados em *machine learning*, é preciso distinguir se tais dados pessoais serão usados apenas em um conjunto de treinamento, para um algoritmo específico⁹¹;
- Artigo 5º1(e): limitação de armazenamento, que proíbe manter dados pessoais quando já não são necessários para efeitos de processamento, ou seja, apenas pelo tempo necessário para o fim que se destina.

⁸⁹ The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. In [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf), pp.44-49.

⁹⁰ *Idem, ibidem*, pp. 44-49.

⁹¹ *Idem, ibidem*.

O Artigo 6º do RGPD declara que todo processamento de dados pessoais requer uma base legal. Ou seja, o tratamento só é lícito se e na medida em que se verifique pelo menos uma das situações elencadas no artigo⁹². Essa ideia foi a primeira introduzida na Diretiva de Proteção de Dados de 1995⁹³ (que foi substituída pelo RGPD) e posteriormente elencada no artigo 8.º da Carta Europeia dos Direitos Fundamentais⁹⁴. Destaca-se no artigo 6º do RGPD⁹⁵:

- Artigo 6º1(a): consentimento. O consentimento do titular dos dados para o processamento de seus dados pessoais por um sistema de IA pode ter dois objetos, incluindo tais dados em um conjunto de treinamento, ou fornecendo-os a um modelo algorítmico destinado a fornecer respostas individualizadas.
- Artigo 6º1(b-e): necessidade. Realizar ou inserir (a pedido) em um contrato, para o cumprimento de uma obrigação legal, ou proteger interesses vitais, ou desempenhar uma função de interesse público ou no exercício da autoridade pública. Portanto, tais bases legais não se aplicam ao processamento baseado em IA independentemente de tais objetivos.
- Artigo 6º1(f): Interesses legítimos. Ou seja, necessidade do processamento para os fins dos interesses legítimos perseguidos pelo controlador ou por um terceiro parte, exceto quando tais interesses são anulados pelos interesses ou direitos e liberdades do titular dos dados que requerem proteção de dados pessoais.
- Artigo 6º4: reaproveitamento. Uma das questões mais importantes em relação a IA diz respeito ao reaproveitamento de dados pessoais. A ideia geral é declarada no Artigo 5 (1, b) como uma articulação do princípio da limitação da finalidade. Os dados pessoais não serão processados posteriormente em uma forma que é incompatível com os propósitos originais. É, no entanto, presumida, de acordo com 5 (1, b) quando o processamento posterior se destina a propósitos relativos a arquivamento, pesquisa científica ou histórica ou estatística, ou ainda, a processamento posterior para fins de arquivo de interesse público, científico ou histórico para fins de investigação

⁹² The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. In [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf), pp.44-49.

⁹³ A Diretiva 95/46/CE constitui o texto de referência, a nível europeu, em matéria de proteção dos dados pessoais. Institui um quadro regulamentar a fim de estabelecer um equilíbrio entre um nível elevado de proteção da vida privada das pessoas e a livre circulação de dados pessoais no interior da União Europeia (UE). Para este efeito, fixa limites estritos à recolha e à utilização de dados pessoais e solicita a criação, em cada Estado-Membro, de um organismo nacional independente encarregado do controlo de todas as atividades relacionadas com o tratamento de dados pessoais. In <https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex:31995L0046>.

⁹⁴ Art. 8º, I: Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. In https://www.europarl.europa.eu/charter/pdf/text_pt.pdf.

⁹⁵ The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. In [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf), pp. 49-53.

ou estatísticos, nos termos do n.º 1 do artigo 89º. A compatibilidade também é presumida quando o novo processamento for baseado em lei, por razões de interesse público⁹⁶.

Ressalta-se que o reaproveitamento é fundamental no domínio do *big data* e IA, uma vez que a construção de conjuntos de *big data* frequentemente envolve a fusão de dados que foram coletados separadamente para finalidades diferentes. Por conseguinte, dois requisitos são necessários para que o reaproveitamento seja permissível: o novo processamento deve ser compatível com a finalidade para a qual os dados foram coletados, e deve ter uma base legal. Ao aplicar esses critérios para a reutilização de dados com base em IA, devemos distinguir se os dados são reutilizados para fins estatísticos ou para perfis⁹⁷.

O artigo 9.º do RGPD aborda os chamados dados sensíveis: “é proibido o tratamento de dados pessoais 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”⁹⁸.

Esses dados pessoais, a depender do tratamento, podem afetar em maior medida os titulares, expondo-os a graves riscos e desafios. O primeiro desafio está relacionado à reidentificabilidade, pois com a utilização da IA e *big data*, pedaços de dados que aparentemente não seriam identificados podem ser reidentificados e reconectados aos indivíduos em questão, o que pode ter consequências graves para o titular dos dados. O segundo desafio está conectado à inferência. Por meio da IA e do *big data*, pode ser possível vincular comportamento observável e características conhecidas de indivíduos, como por exemplo, atividades *online*, compras, etc., e a dados sensíveis não observáveis, como os descritos no artigo acima referido. Tais inferências podem expor os indivíduos interessados à discriminação ou manipulação⁹⁹.

O artigo 12º do RGPD trata da transparência. Contudo, a complexidade do processamento baseado em IA e o facto de que tal processamento não pode ser completamente antecipado, por se tratar de aprendizagem de máquina, torna-se demasiadamente difícil garantir transparência. Os artigos 13º e 14º do RGPD trazem os deveres de informação, que exigem que

⁹⁶ The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. In [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf), pp. 49-53.

⁹⁷ *Idem, ibidem*, p.59.

⁹⁸ Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. In [https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%](https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679).

⁹⁹ The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. In [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf), p.15.

o titular dos dados seja informado sobre as finalidades do processamento para o qual os dados pessoais se destinam, bem como, a base jurídica para o tratamento¹⁰⁰.

Quando os dados são processados para fins que não possam ser previstos no momento em que os dados foram coletados (no uso de *machine learning*, por exemplo) as informações devem ser fornecidas antes do novo processamento, onde o controlador pretende continuar a processar os dados pessoais para uma finalidade diferente do que aquele para o qual os dados pessoais foram coletados. Essa informação só é dispensada quando o cumprimento é impossível e requer um esforço desproporcional ou prejudica a realização do objetivo do processamento. Os artigos 13º 2(f) e 14º 2(g) do RGPD abordam um aspecto fundamental das aplicações de IA, ou seja, decisão automatizada, requisito que tem sido relacionado com a questão mais geral e fundamental de explicar a IA sistemas e seus resultados¹⁰¹.

O artigo 22º, 4, este introduz uma proibição, limitada por uma exceção, de fundamentar decisões automatizadas sobre dados sensíveis, ou seja, as categorias especiais estabelecidas no artigo 9º 1. Portanto, a IA desafia a proibição de processamento de dados confidenciais, pois, dados confidenciais podem ser inferidos de dados não confidenciais.

Nesse caso, a inferência de dados confidenciais deve contar como um processamento de dados confidenciais e, portanto, teriam que ser considerados ilegais, a menos que sejam cumpridas as condições do artigo 9º. Há também o facto de os dados não confidenciais funcionarem como *proxies* para dados confidenciais correlacionados a eles, embora os últimos não sejam inferidos pelo sistema. Por exemplo, o local de residência pode atuar como um *proxy* para etnia. Nesse caso, pode ocorrer uma discriminação ilegal por uso de dado sensível¹⁰².

Por fim, como já explicado, a IA não é explicitamente mencionada no RGPD, mas muitas de suas disposições são relevantes para IA, principalmente no que tange à sua limitação da finalidade, minimização de dados, o tratamento especial dos chamados dados sensíveis, a limitação de decisões automatizadas, bem como a implantação total da IA e do *big data*. Pois, este último envolve grandes quantidades de dados relativos aos indivíduos e suas relações sociais.

Assim sendo, as disposições do RGPD sobre medidas preventivas e aquelas relativas à privacidade não impedem o desenvolvimento de sistemas de IA, se corretamente

¹⁰⁰ Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. In [https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%](https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%2032016R0679).

¹⁰¹ The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. In [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf), pp. 54-56.

¹⁰² *Idem*, *ibidem* p. 62.

projetados e implementados. Caberá aos técnicos e juristas, em particular aqueles que desempenham o papel de responsáveis pela proteção de dados, fornecer soluções adequadas para o cumprimento da proteção de dados e também na proposição e promoção de normas adequadas¹⁰³.

1.1. Propostas de Regulamento em Matéria de Inteligência Artificial na União Europeia

A Comissão Europeia em Junho de 2018, criou um Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial com o intuito de elaborar Diretrizes para alcançar uma IA de confiança, e que deve compreender os seguintes requisitos principais: agência humana e supervisão, robustez técnica e segurança, privacidade e governança de dados, transparência, diversidade, não discriminação e justiça, bem-estar ambiental e social e prestação de contas¹⁰⁴. Tais princípios não se limitam à privacidade de dados e abordam um conjunto mais amplo de preocupações decorrentes de IA¹⁰⁵.

Em 21 de abril de 2021 a Comissão Europeia apresentou o *Artificial Intelligence Act (AIA)*, a Proposta de Regulamento do Parlamento e do Conselho Europeu estabelecendo regras harmonizadas sobre Inteligência Artificial e alteração de Atos Legislativos. A Proposta tem implicações importantes na proteção de dados e tem como base jurídica o artigo 114.º do Tratado sobre o Funcionamento da União Europeia, que prevê a adoção de medidas para assegurar o estabelecimento e o funcionamento do mercado interno¹⁰⁶.

Resumidamente e limitado à pesquisa em questão, a Comissão apresenta uma proposta de quadro regulamentar em matéria de inteligência artificial com os seguintes objetivos específicos¹⁰⁷:

¹⁰³ Recommendation CM/Rec (2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. Adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies. In: <https://rm.coe.int/09000016809e1154>, pp. 01-03.

¹⁰⁴ Diretrizes do Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial, criado pela Comissão Europeia em Junho de 2018. In <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>, pp.2-4.

¹⁰⁵ Artificial Intelligence and Data Protection. How the GDPR Regulates AI Centre for Information Policy Leadership (CIPL). March 2020. In https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai_12_march_2020_.pdf

¹⁰⁶ EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). 18 June 2021. In: https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en.

¹⁰⁷ *Idem, ibidem*, pp.8-13.

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

A proposta visa uma abordagem baseada no risco para a regulamentação dos sistemas de IA, dividindo as aplicações de IA em quatro categorias diferentes com base no grau de risco: as que apresentam risco inaceitável, alto risco, risco limitado e risco baixo ou mínimo. As aplicações na primeira categoria devam ser totalmente proibidas e as demais regulamentadas¹⁰⁸:

1. Risco inaceitável: são situações proibidas, como por exemplo, pontuação social baseada em IA para fins gerais feita por autoridades públicas; sistemas de identificação biométrica remota em tempo real em espaços acessíveis ao público para fins de aplicação da lei (com as devidas exceções);
2. Alto risco: riscos para a saúde, segurança ou direitos fundamentais dos indivíduos; esses sistemas de IA de alto risco são permitidos sujeitos ao cumprimento de requisitos obrigatórios e avaliação de conformidade;
3. Risco limitado: são aqueles permitidos mas sujeitos às obrigações de informação, ou seja, notificar os humanos que eles estão interagindo com sistemas de IA ou que estão expostos a sistemas de reconhecimento;
4. Risco baixo ou mínimo: sem restrições, apenas um código de conduta voluntário é proposto.

Tanto a EDPB quanto a EDPS apelam a uma proibição geral de qualquer utilização de IA com o intuito de reconhecimento automático de características humanas em espaços acessíveis ao público, como rostos, impressões digitais, DNA, voz e outros sinais biométricos ou comportamentais em qualquer contexto. Outra proibição é em relação a sistemas de IA que

¹⁰⁸ EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). 18 June 2021. In: https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en, pp.8-13.

categorizam indivíduos em grupos de acordo com a etnia, gênero, orientação política ou sexual, ou outros motivos de discriminação, nos termos do artigo 21.º da Carta¹⁰⁹.

As discussões sobre o *Artificial Intelligence Act* demonstram os desafios envolvidos na busca do equilíbrio entre os direitos humanos com a necessidade de promover a inovação tecnológica e os benefícios econômicos e sociais que a acompanham na União Europeia¹¹⁰.

1.2 Ética e direitos humanos no âmbito da Inteligência Artificial

A abordagem baseada em direitos para a proteção de dados, tem os dados como uma questão de proteção de direitos individuais. Em uma primeira linha, a preocupação inclui os direitos fundamentais à privacidade e proteção de dados, que são conectados com os princípios fundamentais de dignidade, liberdade de pensamento, não discriminação, etc. Já a outra linha de abordagem é constituída pelos direitos de proteção de dados, de que trata o RGPD, como o poder de consentir e retirar o consentimento, o direito à informação, o acesso, etc¹¹¹. Um dos maiores problemas envolvendo essa temática de IA e direitos é como conciliar a inovação da IA com direitos individuais e valores sociais e, ainda assim, garantir a adoção de regras e princípios de proteção de dados¹¹².

Essa discussão acerca das tecnologias de IA e seu impacto na sociedade, fez com que a UE criasse uma abordagem mais centrada no ser humano, com o intuito de que o uso da IA respeite valores e princípios éticos. Em uma de suas ações, a Presidente eleita da Comissão Europeia, Ursula Von Der Leyen, anunciou que a Comissão deveria apresentar novas propostas legislativas para uma abordagem às implicações humanas e éticas da IA. Tal documento foi preparado pelo Grupo de Peritos de Alto Nível da Comissão em IA, composto por 52 especialistas independentes, que visa oferecer orientações sobre como promover e assegurar o desenvolvimento de sistemas de IA éticos na UE¹¹³.

¹⁰⁹ EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). 18 June 2021. In: https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en, p.11.

¹¹⁰ *Idem*, *Ibidem*.

¹¹¹ Diretrizes do Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial, criado pela Comissão Europeia em Junho de 2018. In <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>, pp. 01-55.

¹¹² The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. In [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf), p.73.

¹¹³ Diretrizes do Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial, criado pela Comissão Europeia em Junho de 2018. In <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>

O documento criado pelo Grupo Independente de Peritos de alto nível sobre Inteligência Artificial da Comissão Europeia, em junho de 2018¹¹⁴, tem como objetivo promover uma IA de confiança e, para isso, a IA de confiança deve ter três componentes: 1) deve ser legal, a fim de cumprir toda a legislação e regulamentação aplicável; 2) deve ser ética, garantindo a observância de princípios e valores éticos; 3) deve ser sólida, tanto do ponto de vista técnico como do ponto de vista social¹¹⁵.

De acordo com as orientações, toda a ética aplicada à IA se baseia nos direitos fundamentais consagrados nos Tratados da UE, na Carta dos Direitos Fundamentais da União Europeia e no direito internacional em matéria de direitos humanos¹¹⁶. Por conseguinte, os Estados-Membros e as instituições da UE são legalmente obrigados a respeitar quando aplicam o direito da União. Contudo, ressalta-se que, ainda que os direitos definidos na Carta da UE sejam juridicamente vinculativos, é importante reconhecer que os direitos fundamentais nem sempre proporcionam uma proteção jurídica global, o que, nesse caso, gera efeitos somente nos domínios da União Europeia, a não ser que seja de matéria de direito internacional em direitos humanos¹¹⁷.

As orientações são apresentadas em três níveis. O primeiro descreve as bases de uma IA de confiança, definindo a abordagem baseada nos direitos fundamentais e identifica os princípios éticos que devem ser respeitados. O segundo trata da concretização de uma IA de confiança sob o fundamento de princípios éticos que os sistemas de IA devem aplicar e cumprir. E o último nível propõe uma avaliação para uma IA de confiança que deve ser adaptada à aplicação específica do sistema¹¹⁸.

Conforme o estudo¹¹⁹, os sistemas de IA devem melhorar o bem-estar individual e coletivo baseados em quatro princípios éticos, que são parte dos direitos fundamentais, e que devem ser respeitados imperativamente para assegurar que os sistemas de IA sejam confiáveis. Segundo o mesmo estudo, os princípios refletem a ordem em que os direitos fundamentais estão apresentados na Carta da UE. Os princípios são: o respeito da autonomia humana, a prevenção

¹¹⁴ Diretrizes do Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial, criado pela Comissão Europeia em Junho de 2018. In <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>, p.02.

¹¹⁵ *Idem, ibidem*.

¹¹⁶ In: <https://www.europarl.europa.eu/about-parliament/pt/democracy-and-human-rights/fundamental-rights-in-the-eu>

¹¹⁷ Diretrizes do Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial, criado pela Comissão Europeia em Junho de 2018. In <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>, p.10

¹¹⁸ Diretrizes do Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial, criado pela Comissão Europeia em Junho de 2018. In <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>, p.05

¹¹⁹ *Idem, ibidem*, pp. 12-13

de danos, a equidade e a explicabilidade.

E, para se obter essa IA de confiança, deve haver requisitos baseados nesses princípios e que sejam aplicáveis às partes interessadas no uso dos sistemas de IA. A lista descrita no estudo não é exaustiva e inclui aspectos individuais e coletivos. Os requisitos são: ação e supervisão humana, solidez técnica e segurança, privacidade dos dados, transparência, diversidade, não discriminação e igualdade, responsabilização e bem-estar social e ambiental. Para aplicar os requisitos referidos, deve ser realizada uma avaliação contínua dos métodos utilizados, bem como, comunicar qualquer alteração feita nos processos de IA. Os métodos podem ser técnicos e não técnicos e podem ser complementares ou utilizados em separado. O estudo também apresenta métodos sugestivos com o intuito de ajudar a criar uma IA de confiança¹²⁰.

Os métodos técnicos podem ser incorporados nas fases de concepção, desenvolvimento e utilização de um sistema de IA, tais como, arquiteturas para uma IA de confiança, ética e Estado de direito desde a concepção (*by design*), métodos de explicação, testes e validação e indicadores de qualidade e serviço. Já os métodos não técnicos têm um papel importante para manter uma IA de confiança e que também devem ser avaliados de forma contínua, tais como, regulamentação, códigos de conduta, normalização, certificação, responsabilização por meio de quadros de governação, educação e sensibilização ética, participação das partes interessadas, diálogo social, e equipes de concepção inclusiva¹²¹.

Outro documento muito importante para a IA é o *Recommendation CM/Rec(2020) of the Committee of Ministers to Member States on the human rights impacts of algorithmic systems*, que recorda a obrigação dos Estados membros da UE, nos termos da Convenção, de se abster de violações dos direitos humanos, inclusive por meio de sistemas algorítmicos. O documento também tem como base normas e padrões regionais e internacionais e recomendações relacionadas à proteção dos direitos humanos e liberdades fundamentais, bem como, a evolução da jurisprudência do Tribunal Europeu dos Direitos do Homem, além de reiterarem a importância das normas existentes de proteção de dados pessoais, nomeadamente as Convenção para a Proteção de Indivíduos com relação ao Processamento Automático de Dados Pessoais (ETS N° 108), conforme modernizado pelo Protocolo de Alteração (CETS n° 223), enfatizando que os impactos dos sistemas algorítmicos sobre os direitos são mais amplos e exigem

¹²⁰ Diretrizes do Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial, criado pela Comissão Europeia em Junho de 2018. In <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>, p.14.

¹²¹ Diretrizes do Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial, criado pela Comissão Europeia em Junho de 2018. In <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>, pp.21-22.

proteções adicionais¹²².

No referido documento, o Comitê recomenda que os governos dos Estados membros revejam suas estruturas legislativas e políticas, bem como, suas próprias práticas com relação a implantação de sistemas algorítmicos e que promovam a implementação e avaliação em todas as áreas relevantes em intervalos regulares. Também recomenda que os Estados garantam por meio de estruturas legislativas, regulamentos de supervisão adequados aos sistemas algorítmicos, e que o desenvolvimento e implantação de tais sistemas estejam em conformidade com as leis aplicáveis para cumprir suas responsabilidades e respeitar direitos humanos de acordo com os Princípios Orientadores das Nações Unidas sobre Negócios e Direitos Humanos¹²³.

Ainda de acordo com a recomendação do Comitê, o processo de elaboração, promulgação e avaliação de políticas e legislação ou regulamentação aplicável ao *design*, desenvolvimento e implantação contínua de sistemas algorítmicos deve ser transparente, responsável e inclusivo. Os Estados devem consultar regularmente todas as partes interessadas relevantes e partes afetadas, bem como, garantir a executoriedade e aplicação das leis, verificação da conformidade legal e responsabilização por não cumprimento¹²⁴.

Seguindo na mesma seara, na data de 08 de maio de 2021, foi promulgada a Lei 27/2021 que aprova a Carta Portuguesa de Direitos Humanos na Era Digital. Já de início, no artigo 2º n.º 2, temos que, “as normas que na ordem jurídica portuguesa consagram e tutelam direitos, liberdades e garantias são plenamente aplicáveis no ciberespaço”¹²⁵.

Já no artigo 8º, que dispõe sobre o direito à privacidade em ambiente digital, ressalta-se que “todos têm direito a comunicar eletronicamente usando a criptografia e outras formas de proteção da identidade ou que evitem a recolha de dados pessoais, designadamente para exercer liberdades civis e políticas sem censura ou discriminação”, bem como que “o direito à proteção de dados pessoais, incluindo o controlo sobre a sua recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição, é assegurado nos termos legais”¹²⁶.

¹²² Recommendation CM/Rec (2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. Adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies. In: <https://rm.coe.int/09000016809e1154>

¹²³ *Idem, ibidem*, pp.02-03.

¹²⁴ *Idem, ibidem*, pp. 06-07.

¹²⁵ Lei 27/2021, Carta Portuguesa de Direitos Humanos na Era Digital <https://data.dre.pt/eli/lei/27/2021/05/17/p/dre>

¹²⁶ *Idem, ibidem*.

Em relação ao uso da inteligência artificial e de robôs, estabelece o artigo 9º que “a utilização da inteligência artificial deve ser orientada pelo respeito dos direitos fundamentais, garantindo um justo equilíbrio entre os princípios da explicabilidade, da segurança, da transparência e da responsabilidade, que atenda às circunstâncias de cada caso concreto e estabeleça processos destinados a evitar quaisquer preconceitos e formas de discriminação”. O mesmo artigo também ressalta que “as decisões com impacto significativo na esfera dos destinatários que sejam tomadas mediante o uso de algoritmos devem ser comunicadas aos interessados, sendo suscetíveis de recurso e auditáveis, nos termos previstos na lei”, além da aplicabilidade dos princípios e valores consagrados no artigo 2º do Tratado da União Europeia, designadamente a não discriminação e a tolerância¹²⁷.

Ainda, o artigo 17º sobre o direito à proteção contra a geolocalização abusiva, dispõe sobre o direito à proteção contra a recolha e o tratamento ilegais de informação sobre a sua localização quando efetuarem uma chamada obtida a partir de qualquer equipamento ou a utilização dos dados da posição geográfica do equipamento de um utilizador só pode ser feita com o seu consentimento ou autorização legal¹²⁸.

Por fim, é importante destacar que para se obter uma IA de confiança não basta apenas preenchimentos de formulários e simples adequação à legislação no momento de sua concepção, pois trata-se de um processo contínuo de identificação e cumprimento de requisitos e normas, adequação às constantes mudanças legais, adequações aos princípios e garantias legais, aos princípios éticos, além de avaliação e garantia de resultados enquanto o sistema de IA desenvolvido perdurar¹²⁹.

1.3 Direito Penal e Inteligência Artificial

Em 4 de dezembro de 2018, foi publicada a Carta ética europeia para a utilização de IA nos sistemas de justiça e ambientes relacionados. O documento foi elaborado pela CEPEJ, Comissão Europeia pela eficácia da Justiça, com o objetivo de monitorizar e medir a qualidade dos sistemas de autoridades judiciais dos países membros¹³⁰. Na Carta estão descritos os cinco

¹²⁷ Lei 27/2021, Carta Portuguesa de Direitos Humanos na Era Digital <https://data.dre.pt/eli/lei/27/2021/05/17/p/dre>

¹²⁸ *Idem, ibidem*.

¹²⁹ Diretrizes do Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial, criado pela Comissão Europeia em Junho de 2018. In <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>, p.41.

¹³⁰ Carta ética europeia para a utilização de inteligência artificial nos sistemas de justiça e ambientes relacionados. In <https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0>

princípios sobre o uso da inteligência artificial nos sistemas judiciais e no respectivo ambiente: princípio de respeito aos direitos fundamentais, princípio de não-discriminação, princípio de qualidade e segurança, princípio da transparência, imparcialidade e equidade e princípio sobre o controlo do usuário¹³¹.

Na seara da justiça criminal, o impacto em relação ao uso da inteligência artificial nos sistemas judiciais ocorreu principalmente em nível probatório, em que dados gerados por ferramentas digitais se tornaram comumente utilizados por meio de novas formas de captura de conversas e outros dados confidenciais. A preocupação com a inviolabilidade dos dados confidenciais de maneira ética assume um valor ainda maior no contexto do direito penal, particularmente no que diz respeito ao julgamento criminal, no qual um dos mais valiosos bens jurídicos, a liberdade, está em risco. O interesse da justiça deve prevalecer em equilíbrio com os interesses privados de desenvolvedores de *software* e isso só pode acontecer se todo o ciclo do modelo, desde o *design*, sejam pautados na transparência, imparcialidade e justiça¹³².

Um exemplo grave de violação dos direitos são as decisões pautadas pela IA por meio de *softwares* que não respeitam as diretrizes, como é o caso do *software* preditivo COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*), que tem seu código-fonte e seu funcionamento protegido como segredo comercial. Em um dos casos polêmicos, o arguido, chamado Eric Loomis, teve sua sentença proferida em 2016 pela Suprema Corte de Wisconsin, tendo sido condenado à pena de seis anos de prisão e cinco anos de “vigilância”. Apelou à Suprema Corte do Estados Unidos, alegando que o uso de tal *software* na sentença viola o direito do arguido ao devido processo, pois o impede de contestar a validade científica e a exatidão de tal teste, além de que o COMPAS viola os direitos do devido processo ao levar em consideração gênero e raça, que são os chamados dados sensíveis¹³³.

Embora esse tipo de *software* seja recebido com entusiasmo, geralmente pela polícia, a solução principal preconizada pela Carta é a transparência técnica acompanhada de uma explicação do processo computacional em linguagem acessível e clara. Sabe-se, de facto, que apesar da ênfase dada ao conceito de transparência, isso por si só não representa a solução

¹³¹ Carta ética europeia para a utilização de inteligência artificial nos sistemas de justiça e ambientes relacionados. In <https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0>

¹³² Quattrocchio, Serena. *Intelligenza Artificiale e Giustizia: nella Cornice della Carta Etica Europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*. In: <http://www.lalegislazionepenale.eu/intelligenza-artificiale-e-giustizia-nella-cornice-della-carta-etica-europea-gli-spunti-per-unurgente-discussione-tra-scienze-penali-e-informatiche-serena-quattrocchio/>, p.07.

¹³³ Loomis v. Wisconsin. In <https://www.scotusblog.com/case-files/cases/loomis-v-wisconsin/>

de todos desequilíbrios gerados pelo uso de dados produzidos automaticamente, pois entender o funcionamento do modelo permanece limitado apenas aos especialistas, excluindo os destinatários da decisão automatizada¹³⁴.

Estudos citados pela Carta¹³⁵ destacam que os dados que são usados para avaliação de risco e comportamentos violentos na realidade não têm relevância a nível criminológico, mas apenas demonstram as maiores vulnerabilidades sociais, e que, com o uso generalizado de tais *softwares* nos tribunais americanos, revelam uma discriminação existente. O apêndice da Carta aponta que a tomada de decisão humana sendo regulada por uma inserção no modelo computacional, onde enorme quantidade de dados são colocados e a grande maioria pertencem à pessoas de um determinado grupo social, pode significar que o comportamento anterior de um determinado grupo pode afetar o destino do acusado (se este pertencer ao mesmo grupo social), sem que o *software* seja capaz de inferir, de facto, a ação ocorrida. O uso de tais *softwares* não precisa ser rejeitado, mas deve haver um debate científico com a máxima atenção às ferramentas que os sistemas jurídicos utilizam. É preciso ter uma reflexão necessária e cuidadosa, com base nos direitos e garantias fundamentais¹³⁶.

Recentemente, em julho de 2020, foi publicado um estudo¹³⁷ sobre a Inteligência Artificial e aplicação da lei e os impactos sobre os Direitos Fundamentais, com o intuito de fornecer uma visão geral das principais tendências atuais relacionadas à IA e seus impactos nos direitos, bem como na aplicação da lei e justiça criminal a nível da UE, pois, a justiça criminal tem recorrido muito à IA, contando com um uso cada vez mais extenso de grandes dados e algoritmos, o que pode ser um problema, pois, para o uso dessas tecnologias podem ser utilizados dados que não foram coletados originalmente para tais fins, levantando, nessa medida, uma série de questões sobre ética e respeito às normas e princípios. Ocorre que, falta uma regulamentação e governança para o uso da IA na aplicação da lei, em especial na justiça criminal, o que é preocupante, pois o uso de sistemas de IA no campo da aplicação da lei e da justiça criminal geralmente pode levantar preocupações relacionadas com os padrões elencados no artigo 6º da CEDH, em particular a

¹³⁴ Quattrocolo, Serena. *Intelligenza Artificiale e Giustizia: nella Cornice della Carta Etica Europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*. In <http://www.lalegislazionepenale.eu/intelligenza-artificiale-e-giustizia-nella-cornice-della-carta-etica-europea-gli-spunti-per-unurgente-discussione-tra-scienze-penali-e-informatiche-serena-quattrocolo/>, p.08.

¹³⁵ In <https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0>

¹³⁶ *Idem*, *ibidem* p.03.

¹³⁷ Fuster, Prof. Dr. Gloria González. *Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights*. European Parliament's Committee on Civil Liberties, Justice and Home Affairs. In: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU\(2020\)656295_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf)

presunção de inocência, o direito de ser informado imediatamente da causa e natureza de uma acusação, o direito a um julgamento justo e o direito de se defender pessoalmente. O possível uso de sistemas algorítmicos no contexto da justiça tem sido destacado como um setor em que esses sistemas podem entrar em conflito com direitos protegidos constitucionalmente¹³⁸.

Todas essas garantias e cuidados que se deve ter em relação à matéria penal estão também relacionados com a preocupação com os meios de obtenção de prova, que, no uso da IA, são conseguidas por um algoritmo usado como meio de adquirir a evidência. Por conseguinte, a qualidade das evidências digitais depende do *software* adotado, pois, a presença de erros em seu projeto e uso afetará diretamente o resultado, o que é fundamental para a validade da prova. Como ressalta Francesca Palmiotto, a defesa deve saber qual o *software* e como foi utilizado¹³⁹.

Fazendo uma comparação com as leis que regulamentam a admissibilidade das provas, antes de excluir ou declarar provas inadmissíveis, a defesa deve ser capaz de reclamar de possível violação da lei. E, mesmo que as provas sejam declaradas admissíveis, a defesa ainda pode examiná-las. Portanto, mesmo nos casos do uso de IA, a defesa deve ter acesso às informações sobre o algoritmo através do qual as provas foram obtidas. Ocorre que, é preciso que a defesa possa exercer esse direito, porém os algoritmos usados e seu código-fonte permanecem ocultos. É a chamada “opacidade algorítmica”, ou seja, o não conhecimento que pode referir-se à falta de acesso à informação ou à sua compreensibilidade. No primeiro, o acesso à informação pode ser impedido por direitos autorais, por segredos comerciais, etc. Já em relação à possibilidade de compreensão das informações, nota-se a falta de competência técnica do defensor ou, de forma mais geral, a falta de compreensão do próprio sistema, afetando assim, o julgamento justo¹⁴⁰.

A decisão ou avaliação criminal tem algo que, por si só, parece irreconciliável com o enorme potencial da IA, pois o problema é ter uma decisão lógica, cognitiva e psicológica. Nesse caso é o programador que prepara não apenas os algoritmos e a seleção de dados e informações a serem usados, mas também os critérios de avaliação que fazem o resultado de uma elaboração poder ser considerada como uma decisão. Não se trata apenas da transparência do sistema, da

¹³⁸ Carta ética europeia para a utilização de inteligência artificial nos sistemas de justiça e ambientes relacionados. In <https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0>

¹³⁹ Palmiotto, Francesca. *Giustizia penale e nuove tecnologie. La legislazione penale. 2020. Captatori Informatici e Diritto alla Difesa: Il Caso Exodus*. In: <http://www.lalegislazionepenale.eu/wp-content/uploads/2020/10/Palmiotto-Revisione-Finale.pdf>, p.18.

¹⁴⁰ *Idem, ibidem*, p.19.

verificabilidade dos critérios adotados, da correção e completude dos dados e informações, da confidencialidade. É uma questão de entender quais variáveis podem ou devem contribuir para a formação de um “produto” que o sistema pode aceitar como uma decisão criminal¹⁴¹.

No que diz respeito ao combate à criminalidade grave e à prevenção de ameaças graves à segurança pública, um Estado Membro também pode prever a retenção direcionada desses dados, bem como sua retenção acelerada, mas tal interferência nos direitos fundamentais deve ser acompanhada por salvaguardas eficazes e ser revista por um tribunal ou por uma autoridade administrativa independente¹⁴².

Em 6 de outubro de 2021, o Parlamento Europeu adotou uma resolução (Resolução 405) a respeito do uso da inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais (*Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters*)¹⁴³. A resolução aponta para o risco de viés algorítmico em aplicações de IA e enfatizam que a supervisão humana e fortes poderes legais são necessários para prevenir a discriminação por IA. De acordo com o texto, os sistemas de identificação baseados em IA identificam grupos étnicos minoritários, pessoas LGBTI, idosos e mulheres, o que é preocupante no contexto da aplicação da lei e do judiciário. Para garantir que os direitos fundamentais sejam respeitados ao usar essas tecnologias, os algoritmos devem ser transparentes, rastreáveis e documentados¹⁴⁴.

No sentido de respeitar a privacidade e a dignidade humana, deve-se proibir permanentemente o reconhecimento automatizado de indivíduos em espaços públicos, ressalvando que os cidadãos apenas devem ser monitorizados quando suspeitos de um crime. O Parlamento solicita também a proibição do uso de bancos de dados privados de reconhecimento facial e a oposição ao policiamento preditivo baseado em dados comportamentais, bem como a proibição de sistemas de pontuação social, que procuram avaliar a fiabilidade dos cidadãos com base no seu comportamento ou personalidade. Ainda, o reconhecimento automatizado não deve ser usado para controlo de fronteira ou em espaços públicos¹⁴⁵.

¹⁴¹ Parodi, Cesare; Sellaroli, Valentina. Sistema Penale e Intelligenza Artificiale: Molte Speranze e Qualche Equivoco. in Dir. pen. cont., fasc. 1/2017, In: <https://archiviodpc.dirittopenaleuomo.org/upload/6695-parodisellaroli2019a.pdf>, p.55.

¹⁴² *Idem, ibidem*.

¹⁴³ <https://www.europarl.europa.eu/news/pt/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance>

¹⁴⁴ Resolução do Parlamento Europeu, de 6 de outubro de 2021, sobre a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais. In https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_PT.html

¹⁴⁵ *Idem, ibidem*.

Em suma, devido a enorme extensão dos impactos na vida privada e social dos cidadãos, a IA se enquadra em diferentes regimes jurídicos. Portanto, é necessário um amplo debate envolvendo autoridades políticas e administrativas, bem como a sociedade civil. Este debate precisa abordar as questões sobre quais padrões devem ser aplicados ao processamento de dados pessoais de IA, especialmente para garantir a aceitabilidade, justiça e razoabilidade das decisões sobre os indivíduos¹⁴⁶.

¹⁴⁶ Sartor, Giovanni. *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*.
[https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU\(2020\)641530](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)641530), p.80.

Capítulo 3: Reflexos dos avanços tecnológicos na aplicação do Direito Penal

1. O uso do *Big Data* no contexto do policiamento preditivo

Primeiramente, ao utilizar *big data* e algoritmos é necessário avaliar se tais usos são compatíveis com os direitos individuais, pois, além de ajudar a melhorar a eficiência dos sistemas judiciais, a IA deve reforçar as garantias do Estado de direito¹⁴⁷.

O desenvolvimento de sistemas de IA baseados em *machine learning* pressupõe a criação de enormes conjuntos de dados, ou seja, o *big data*. A integração entre IA e *big data* pode trazer muitos benefícios para o progresso econômico, científico e social, mas também gera sérios riscos para os indivíduos e a sociedade, tais como vigilância intensificada, controlo, manipulação, injustiça e discriminação. Mesmo quando o processamento de dados não é discriminatório e é baseado em tecnologias confiáveis, pode levar a níveis inaceitáveis de vigilância e controlo¹⁴⁸.

Como já explicado no primeiro capítulo, os sistemas de IA baseados em conhecimento funcionam com uma grande base de dados, os chamados *big datas*, que são sempre alimentados com novas informações. São nessas bases de dados que o conhecimento obtido é representado em uma linguagem próxima da linguagem usada pelos humanos. O conhecimento é utilizado por inferência, que é capaz de interpretar o conteúdo da base de dados e fazer deduções lógicas com o intuito de levar a determinado resultado para justificar as conclusões a que se chega¹⁴⁹. Os sistemas baseados em conhecimento têm três componentes fundamentais: a base de dados, o motor inferencial e as interfaces dirigidas ao usuário e ao desenvolvedor do *software*¹⁵⁰.

Os dados são essenciais para o desenvolvimento da IA, quanto mais dados disponíveis, mais a IA é capaz de melhorar a sua capacidade preditiva. Porém, em termos de proteção de dados, as principais dúvidas referem-se à análise dos dados usados por *softwares* preditivos. A justiça preditiva, que faz uso da IA, é um exemplo de aplicação algorítmica que é

¹⁴⁷ Comissão Europeia para a eficácia da Justiça (CEPEJ). *Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seu ambiente*, (2018). In <https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0>

¹⁴⁸ Recommendation CM/Rec (2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. (Adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies. In: <https://rm.coe.int/09000016809e1154>, p.08.

¹⁴⁹ Iaselli, Michele. *X-LAW: la polizia predittiva è realtà?* Altalex, 28/11/2018. In: <https://www.altalex.com/documents/news/2018/11/28/x-law-la-polizia-predittiva>

¹⁵⁰ *Idem, ibidem*

alimentada com enorme quantidade de dados. E é na utilização desses algoritmos que deve ser utilizado o princípio da precaução aplicado às políticas de avaliação dos riscos na utilização dos dados pessoais, empregando políticas preventivas para combater esses riscos¹⁵¹.

Portanto, os sistemas inteligentes que trabalham com a justiça preditiva devem priorizar a transparência sobre as linhas de raciocínio seguidas para se chegar às conclusões, bem como a flexibilidade, ou seja, a capacidade de acompanhar modificações em suas bases de dados sem que isso influencie em suas inferências, além de se apoiar nas chamadas redes neurais¹⁵².

A IA não produz inteligência por si só mas usa uma abordagem indutiva por meio de seus algoritmos, ou seja, é alimentada por um grande conjunto de dados, que são as entradas, e que possuem um conjunto de resultados possíveis, as saídas. Especificamente na justiça preditiva, a ligação ocorre entre os dados identificados na entrada e os dados identificados na saída, e que, ao final, são classificados. A confiabilidade do modelo depende da qualidade dos dados utilizados e da escolha da técnica de *machine learning*, que incluem as redes neurais e o *deep learning*¹⁵³.

As abordagens preditivas na aplicação da lei por vezes dependem do processamento de dados que nem sempre estão relacionados ao crime, mas que têm como fontes empresas privadas que coletaram tais dados no contexto de sua atividade. E, por esse motivo, a eventual rotulagem de indivíduos como suspeitos pode levar a situações que requerem atenção tanto na proteção de dados como no direito à presunção de inocência¹⁵⁴.

O interesse pela IA se firma em diversos setores, inclusive no setor jurídico. São várias as soluções úteis que os juristas e operadores do direito propõem, em especial a chamada justiça preditiva, que é o foco do presente estudo. Como já dito, o estudo da IA é, sem dúvida, um dos campos da tecnologia da computação mais estudados atualmente. Além da tecnologia da computação, envolve filosofia, psicologia cognitiva, linguística, entre outros campos relacionados. E, como também já explicado, a inteligência artificial pode ser considerada como uma ciência que

¹⁵¹ Comissão Europeia para a eficácia da Justiça (CEPEJ). *Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seu ambiente*, 2018. In <https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0>

¹⁵² Iaselli, Michele. X-LAW: la polizia predittiva è realtà? *Altalex*, 28/11/2018. In: <https://www.altalex.com/documents/news/2018/11/28/x-law-la-polizia-predittiva>

¹⁵³ Comissão Europeia para a eficácia da Justiça (CEPEJ). *Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seu ambiente*, 2018. In <https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0>

¹⁵⁴ Fuster, Gloria González. *Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights European Parliament's Committee on Civil Liberties, Justice and Home Affairs*. In: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU\(2020\)656295_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf), p. 22.

desenvolve modelos computacionais de comportamento inteligente, para que os computadores possam realizar tarefas que exigiriam inteligência humana. Existem tipos diferentes de métodos de policiamento preditivo, tais como métodos de previsão de crimes ou previsão de locais e horários com risco aumentado de crime; métodos preditivos de infratores ou de identificar indivíduos em risco de ofender (ou reincidir) no futuro; métodos preditivos para prever vítimas de crimes, usados para identificar grupos ou indivíduos que têm probabilidade de se tornarem vítimas de crime; e métodos para criar perfis semelhantes aos do passado dos infratores. Todos esses métodos se baseiam em dados algorítmicos ou análise dos grandes dados, ou *big data*, no campo da inteligência artificial¹⁵⁵.

O chamado policiamento preditivo é utilizado para prevenir tipos de infrações de menor potencial ofensivo, tais como furto, pois é capaz de determinar com precisão onde e quando estas infrações podem ser cometidas e de reproduzir estas informações num mapa geográfico sob a forma de pontos críticos que são monitorados em tempo real. Alguns *softwares* utilizam histórico de localização de crimes, relatórios policiais, geolocalização, etc¹⁵⁶.

O processamento automatizado de dados pessoais com o objetivo de produzir conhecimento por meio da inferência de correlações de dados na forma de perfis que podem posteriormente ser aplicados como base para a tomada de decisões, é chamado de “*profiling*”. Ou seja, é um conjunto de dados correlacionados que representam um sujeito, que pode ser individual ou coletivo. Por meio de tecnologias de IA e *big data*, os indivíduos podem estar sujeitos à vigilância em muitos mais casos e contextos com base em um conjunto mais amplo de características pessoais. Ao correlacionar os dados sobre os indivíduos às classificações correspondentes e previsões, a IA aumenta o potencial de criação de perfil, ou seja, para inferir informações sobre indivíduos ou grupos e adotando avaliações e decisões¹⁵⁷.

Em relação ao RGPD, esse não exclui a tomada de decisão automatizada, uma vez que oferece amplas exceções e permite inferências com base em dados pessoais, incluindo perfis. Entretanto, deve-se observar as condições corretas e adotar as salvaguardas apropriadas. As disposições do RGPD sobre medidas preventivas e, em particular, aquelas relativas à

¹⁵⁵ Fuster, Gloria González. *Artificial Intelligence and Law Enforcement*. Impact on Fundamental Rights European Parliament's Committee on Civil Liberties, Justice and Home Affairs. In: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU\(2020\)656295_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf), p. 22.

¹⁵⁶ Comissão Europeia para a Eficácia da Justiça (CEPEJ). *Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seu ambiente*, 2018. In: <https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0>

¹⁵⁷ Sartor, Giovanni. *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*. In [https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU\(2020\)641530](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)641530), p.23.

privacidade, desde a concepção e por padrão, também não se deve impedir o desenvolvimento de aplicativos de IA se corretamente projetados e implementados¹⁵⁸.

Por fim, ressalta-se mais uma vez, que é indiscutível a relevância que a correta seleção de dados tem para construir e treinar um modelo matemático com qualidade e origem não manipulada, configurando assim, uma ferramenta útil e confiável. Além disso, a escolha dos dados, bem como as formas como são avaliados pelo modelo e sua qualidade, devem ser objetos de comunicação transparente aos usuários¹⁵⁹.

1.1. *Machine Bias*

Machine bias, *Algorithm bias* ou *Bias* é um viés, um preconceito algorítmico em relação a uma pessoa ou posição. Algoritmos não são imparciais. O viés algorítmico pode surgir de várias maneiras nos sistemas de IA que utilizam *machine learning* e *big data*, especialmente no uso preditivo. Geralmente ocorre na coleta dos dados em grandes e indiscriminadas quantidades, e que, junto com o treinamento ou personalização de quem criou o *software* podem resultar em um sistema de IA que demonstra preconceito em seus resultados. Vieses podem ou não ser intencionais, mas, em alguns casos, o preconceito pode gerar discriminação ou resultado injusto¹⁶⁰.

O ponto mais delicado da questão sobre o uso de modelos preditivos no campo judicial não é em relação ao algoritmo em si e nem ao tipo de tarefas atribuídas à ferramenta de IA. Certamente, algoritmos sem os dados não servem, pois desenvolvem informações de acordo com um determinado modelo matemático e com as informações contidas nesses dados. É, portanto, na quantidade e na qualidade dos dados que a inteligência artificial e todas as ferramentas matemáticas baseadas em algoritmos modelam uma determinada realidade para obter respostas mais ou menos probabilísticas para interpretar e prever. Contudo, a qualidade dos dados depende de sua origem e relevância para a realidade a ser representada e o propósito a ser alcançado. Muitas vezes, os desenvolvedores ou usuários desses modelos não têm dados diretos

¹⁵⁸ Sartor, Giovanni. The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. In [https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU\(2020\)641530](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)641530), p.23.

¹⁵⁹ Parodi di Cesare, Sellaroli Valentina. *Sistema Penale e Intelligenza Artificiale: molte speranze e qualche equivoco*. Diritto Penale Contemporaneo. Fascicolo 6/2019. In: <https://archiviopdc.dirittopenaleuomo.org/upload/6695-parodisellaroli2019a.pdf>, p.69.

¹⁶⁰ Diretrizes do Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial, criado pela Comissão Europeia em Junho de 2018. In <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>, p.36.

para a construção do modelo e então eles os substituem por dados de *proxy* ou indiretos¹⁶¹.

Muitas das preocupações levantadas sobre o uso de algoritmos na justiça criminal referem-se ao viés racial indireto em modelos que preveem reincidências. Os sistemas algorítmicos utilizam grandes dados que dependem da priorização de certos valores sobre outros. A discriminação algorítmica não pode ser evitada ou mitigada apenas pela regulamentação dos conjuntos de dados, uma vez que também pode ser desencadeada pelo projeto dos algoritmos ou pelo projeto do sistema que os implementa¹⁶².

O Livro Branco sobre Inteligência Artificial publicado em 2020, observa que o processamento de dados pessoais relacionados à IA podem desencadear riscos aos direitos fundamentais que afetam diretamente o direito à proteção de dados pessoais e a privacidade. Como exemplo, algoritmos usados na IA que podem apresentar preconceitos de natureza sexista e racial que são riscos inerentes a qualquer atividade humana, que não é imune a erros. Contudo, no âmbito da IA pode ter um efeito muito maior, afetando e discriminando muitas pessoas¹⁶³.

Certamente que, em termos de velocidade e volume de dados processados, a tomada de decisão feita por meio dos algoritmos tem enormes vantagens sobre alguns tipos de tomada de decisão humana. Contudo, os algoritmos podem ter embutidos preconceitos quando se usam os dados sensíveis, que são dados protegidos e que não podem ser utilizados, salvo o disposto em lei¹⁶⁴. Ou seja, em alguns modelos preditivos, uma avaliação errada que o algoritmo forneça e que alimentará ainda mais o banco de dados e os recursos de avaliação da máquina, aumenta a margem de erro, se afastando do modelo da realidade e aumentando a discriminação¹⁶⁵.

Algumas iniciativas para evitar os vieses estão surgindo e concentram-se em processos e métodos, tais como “*data sheets for data sets*” e “*model cards for model reporting*”, que trazem transparência à construção, testes de conjuntos de dados, auditorias para verificar a imparcialidade dos sistemas, além de técnicas de explicabilidade que podem ajudar a identificar os factores levados em conta em uma decisão, ou seja, se os dados utilizados refletem vieses¹⁶⁶.

¹⁶¹ Parodi di Cesare, Sellaroli Valentina. *Sistema Penale e Intelligenza Artificiale: molte speranze e qualche equivoco*. Diritto Penale Contemporaneo. Fascicolo 6/2019. In: <https://archiviodpc.dirittopenaleuomo.org/upload/6695-parodisellaroli2019a.pdf>, p.68.

¹⁶² Fuster, Gloria González. *Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights European Parliament's Committee on Civil Liberties, Justice and Home Affairs*. In: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU\(2020\)656295_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf), p. 42.

¹⁶³ White Paper on Artificial Intelligence: A European approach to excellence and trust 19 February 2020. In https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en, p.11.

¹⁶⁴ Artigo 9º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

¹⁶⁵ Artigo 9º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016

¹⁶⁶ In: <https://www.mckinsey.com/featured-insights/artificial-intelligence/tackling-bias-in-artificial-intelligence-and-in-humans>

Embora o uso de algoritmos seja muito útil, ele não é capaz de considerar o contexto social nem a forma como os dados foram coletados. Assim sendo, é importante reconsiderar em quais casos o julgamento humano deve ser preterido em relação ao uso do julgamento algorítmico.

1.2. Análise algorítmica do perfil criminológico

A identificação dos chamados pontos quentes (*hotspots*) em que se supõe que os agrupamentos de crimes anteriores persistirão no futuro, trata-se, na verdade, de policiamento preditivo no sentido mais estrito e leva a uma mudança no comportamento indutor do crime. A aplicação do policiamento preditivo não se baseia apenas no desenvolvimento de algoritmos, mas sim em uma análise multidisciplinar, principalmente ao analisar conceitos criminológicos por meio do estudo de teorias criminológicas. Algumas dessas teorias assumem que o crime é um processo previsível, segundo a qual os criminosos, assim como as vítimas, seguem certos padrões de comportamento estatisticamente verificáveis. A teoria das janelas quebradas, também é usada como base para o policiamento preditivo, pois a desordem social sinaliza o que o controlo social fraco promove o comportamento criminoso. Ou seja, as premissas criminológicas do policiamento preditivo são extensas e as abordagens estão intimamente ligadas¹⁶⁷.

Classificar o potencial criminoso de pessoas com base em gênero, raça, idade, religião, etnia, antecedentes não é nenhuma novidade, pois eram classificações usadas pelas teorias criminológicas das escolas positivistas dos séculos passados. A diferença está no uso dos algoritmos para fazer essa análise. Cesare Lombroso foi um dos fundadores da Escola Positiva no século XIX. Em seus estudos como médico psiquiatra, atribuiu ao criminoso certas características físicas e psicológicas comuns, influenciando estudiosos a realizarem pesquisas entre a morfologia humana e a ação delituosa. Sua obra principal foi *L'uomo delinquente* (O homem delinquente) que analisou milhares de reclusos de prisões da época¹⁶⁸.

¹⁶⁷ Verlag, Helbing Lichtenhahn. Monika Simmler (Hrsg.). *Smart Criminal Justice - Der Einsatz von Algorithmen in der Polizeiarbeit und Strafrechtspflege*. Basileia, 2021. In: <https://www.helbing.ch/annotstream/9783719043971/PDF/Smart-Criminal-Justice.pdf?sq=27>, pp.103-145.

¹⁶⁸ Molina, Antonio Garcia-Pablos; Gomes, Luiz Flávio. *Criminologia: introdução a seus fundamentos teóricos; introdução às bases criminológicas da Lei nº 9.099/95, Lei dos juizados especiais criminais*. 5. ed. São Paulo: Revista dos Tribunais, 2006.

Para Lombroso o criminoso era um ser que já nascia delinquente, um doente imutável e que deveria ser afastado da sociedade antes de cometer qualquer delito, com o intuito de preservar a sociedade. Muito resumidamente, pode-se dizer que a Escola Positiva considera o criminoso como sujeito determinado ao crime, ou seja, o homem não é livre na sua vontade, pois, com base em seu determinismo biológico carrega certa hereditariedade da demência moral e, portanto, é predeterminado à prática de infrações¹⁶⁹.

E nessa mesma linha surge o direito do autor, que pune o indivíduo pelo que ele é não pelo facto que cometeu. Ou seja, o indivíduo era tido como criminoso em razão das suas características ou atitudes e deveria ser preso mesmo sem ter provas de que tivesse cometido algum crime. O direito do autor defende que o Estado pode proceder de dois modos contra os delinquentes: pode vê-los como pessoas que praticam crimes e devem ser punidas, ou como indivíduos que apresentam perigo e devem ser enfrentados preventivamente como perigo¹⁷⁰. Desse pensamento surgem duas diferentes vertentes do Direito Penal. Uma que pune o facto e todas as garantias constitucionais, penais e processuais devem ser respeitadas, e a outra que pune o autor do facto por ser quem ele é, se revelando o inimigo do direito¹⁷¹.

Mais tarde, outra teoria passou a ser estudada, a teoria do etiquetamento social, o chamado *Labelling Approach*. Para Baratta, “as maiores chances de ser selecionado para fazer parte da população criminosa aparecem concentradas nos níveis mais baixos da escala social. A falta de trabalho, falta de estudo e desestruturação familiar são características dos indivíduos pertencentes aos níveis mais baixos, e que na criminologia positivista e em boa parte da criminologia liberal contemporânea são indicativos como as causas da criminalidade, revelam ser, antes, conotações sobre a base das quais o status de criminoso é atribuído”¹⁷². Ou seja, com a estigmatização dos indivíduos, colocando-os perante a sociedade como criminosos, acabavam por contribuir para que estes indivíduos se tornassem criminosos.

A sociedade evoluiu e junto com ela também os direitos humanos e as garantias fundamentais, mesmo que ainda sejam usadas leis com resquícios dos pensamentos das escolas positivistas e da teoria do direito penal do autor¹⁷³. Como por exemplo Portugal, que é um dos

¹⁶⁹ Lombroso, Cesare. *O homem delinquente*, São Paulo, Ícone, 2013, p. 211-212.

¹⁷⁰ Jakobs, Günther; Meliá, Manuel Cancio. *Direito penal do inimigo: noções e críticas*, pp. 30-35.

¹⁷¹ Moraes, Alexandre Rocha Almeida de Moraes. *Direito penal do inimigo*. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Álvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Penal. Christiano Jorge Santos (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/419/edicao-1/direito-penal-do-inimigo>

¹⁷² Baratta, Alessandro. *Criminologia crítica e crítica do Direito Penal. Introdução à sociologia do Direito Penal*. Rio de Janeiro: Revan, 2002, p.165.

¹⁷³ Moraes, Alexandre Rocha Almeida de Moraes. *Direito penal do inimigo*. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Álvaro de

países que ainda possui resquícios do direito do autor que podem ser observados no Código Penal Português, Decreto-Lei n.º 48/95, quando se trata das medidas de segurança aplicadas aos inimputáveis, pois estas acontecem em função da periculosidade do agente e não pela sua conduta, conforme o art. 91 e seguintes do CP¹⁷⁴. Também a reincidência, elencada no artigo 75º e seguintes do mesmo código¹⁷⁵ pode ser assim considerada, pois pune o agente com base em crimes anteriormente feitos, elevando assim sua pena.

E é nesse sentido que aqui se faz um paralelo entre esse pensamento positivista criminológico e uso indiscriminado do *Big Data* e dos algoritmos preditivos usados na polícia preditiva. O estudo do pensamento criminológico das diversas teorias existentes antes da criação de programas preditivos, deveria servir para a conscientização da não utilização de dados sensíveis armazenados, pois, do contrário, os algoritmos tendem a classificar os indivíduos por suas características físicas e sociais ou pela reincidência, alegando que esses indivíduos representam um perigo para a sociedade, marginalizando ainda mais esses grupos. A leitura incorreta desses dados faz com que haja um policiamento excessivo nos mesmos locais, tendo como base critérios étnicos e sociais¹⁷⁶. É também nesse sentido a preocupação com o *black box problem*, pois os algoritmos não estão livres dos vieses humanos e por isso devem ser transparentes em sua concepção, com o intuito de evitar o *profiling* criminológico dos indivíduos analisados.

1.3. Análise do *Software* XLAW: o *software* de IA da polícia italiana

Softwares utilizados no policiamento preditivo podem ser basicamente dividido em dois tipos: os inspirados na criminologia ambiental que identificam os chamados “*hotspots*”, ou

Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Penal. Christiano Jorge Santos (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/419/edicao-1/direito-penal-do-inimigo>

¹⁷⁴ Artigo 91.º Código Penal. Decreto-Lei n.º 48/95 - Diário da República n.º 63/1995, Série I-A de 1995-03-15

1 - Quem tiver praticado um facto ilícito típico e for considerado inimputável, nos termos do artigo 20.º, é mandado internar pelo tribunal em estabelecimento de cura, tratamento ou segurança, sempre que, por virtude da anomalia psíquica e da gravidade do facto praticado, houver fundado receio de que venha a cometer outros factos da mesma espécie.

¹⁷⁵ Artigo 75.º Código Penal. Decreto-Lei n.º 48/95 - Diário da República n.º 63/1995, Série I-A de 1995-03-15

1 - É punido como reincidente quem, por si só ou sob qualquer forma de comparticipação, cometer um crime doloso que deva ser punido com prisão efectiva superior a 6 meses, depois de ter sido condenado por sentença transitada em julgado em pena de prisão efectiva superior a 6 meses por outro crime doloso, se, de acordo com as circunstâncias do caso, o agente for de censurar a condenação ou as condenações anteriores não lhe terem servido de suficiente advertência contra o crime.

¹⁷⁶ Lucena, Pedro Arthur Capelari de. *Policiamento preditivo, discriminação algorítmica e racismo: potencialidades e reflexos no Brasil*. Salvador, 2019. In: <https://lavits.org/wp-content/uploads/2019/12/Lucena-2019-LAVITSS.pdf>

seja, locais que possivelmente terão práticas de determinados crimes futuros onde há maior incidência de tais crimes, e os que usam a vinculação do crime e seguem o sujeito ativo do crime, ou quem o algoritmo acha que seja, para prever onde e quando cometerá o próximo crime. No primeiro caso, temos o uso da Modelagem de Risco de Terreno (RTM), ou seja, um algoritmo que, ao analisar enormes quantidades de dados relativos a factores ambientais e espaciais que favorecem o crime, emite uma “previsão” da prática de delitos de tráfico de drogas, por exemplo, em determinadas áreas de grandes centros urbanos, possibilitando um mapeamento e identificando áreas onde o risco é maior. Consequentemente, podem ser planeadas e implementadas intervenções de prevenção da criminalidade¹⁷⁷.

O *software* XLAW foi concebido pelo Inspetor Superior da Polícia de Nápoles, Doutor Elia Lombardo, como um projeto de pesquisa e desenvolvimento de abordagem multidisciplinar, com a contribuição da segurança pública e privada, do meio acadêmico, de criminologistas, sociólogos, urbanistas, juristas, cientistas da computação, economistas¹⁷⁸.

Para montar a base de dados do programa, Lombardo analisou 20 anos de dados de crimes e os estudou um por um, descobrindo que entre os muitos crimes, a maioria deles são previsíveis. São os chamados crimes predatórios: furto, roubo, furto de carteira¹⁷⁹. O inspetor criou esta ferramenta tecnológica para o trabalho de aplicação da lei inicialmente para ser usado na Itália, na inovadora área de Segurança Urbana Preditiva, que revoluciona o método tradicional de prevenção da ilegalidade generalizada porque se baseia no uso da Inteligência Artificial para prever assaltos, roubos, furtos, batedores de carteira, golpes e outros crimes predatórios comuns das cidades grandes¹⁸⁰.

O *software* XLAW é baseado em um algoritmo capaz de analisar uma enorme quantidade de dados das denúncias encaminhadas à Polícia Estadual, permitindo evidenciar factores recorrentes ou coincidentes, como a prática repetida de roubos nos mesmos locais e com métodos semelhantes. Por meio desse sistema foi traçado um mapa do território onde as áreas de maior risco são destacadas até o nível máximo em determinados momentos, destacando as áreas e horários com maior incidência dos crimes¹⁸¹. Ou seja, uma ferramenta digital com um

¹⁷⁷ Basile, Fabio. *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine. Artificial intelligence and criminal law: four possible research leads*. Diritto Penale e Uomo, Milano, 2018. In: <https://archiviopdc.dirittopenaleuomo.org/upload/3089-basile2019.pdf>, pp.10-12

¹⁷⁸ In: <https://www.xlaw.it/presentazione/>.

¹⁷⁹ In: <https://www.tpi.it/tecnologia/xlaw-algoritmo-prevede-furti-rapine-20190730383409/>

¹⁸⁰ In: <https://www.xlaw.it/presentazione/>

¹⁸¹ Basile, Fabio. *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine. Artificial intelligence and criminal law: four possible research leads*. Diritto Penale e Uomo, Milano, 2018. In: <https://archiviopdc.dirittopenaleuomo.org/upload/3089-basile2019.pdf>, pp.10-12.

algoritmo sofisticado baseado em heurística e semânticas avançadas, alimentam uma base de dados relativos a cada crime predatório isolado ou pertencentes a grupo criminoso, criando uma estratégia para prever crimes no território em questão¹⁸²

O programa consiste em um protocolo técnico-metodológico configurado para gerar e georreferenciar alarmes preditivos (Sistema de Informação Geográfica SIG) processados em modelo exclusivo de *machine learning*. A diferença entre os alarmes preditivos e os de uso tradicionais é que esses avisam somente após a ocorrência das infrações, já os preditivos monitorizam seletivamente e sequencialmente, de acordo com o princípio de causa e efeito, aqueles lugares onde está cientificamente e empiricamente previsto que um ato ilícito irá acontecer e não onde se pensa que poderia acontecer ou onde já aconteceu¹⁸³.

Especificamente, é um sistema do tipo heurístico (como a medicina que é baseada em sinais e sintomas podendo apenas fazer previsões prováveis), ou seja, é um sistema de inteligência artificial baseado em *machine learning*, dotado de um algoritmo heurístico que, a partir da aquisição das características socioambientais do território em questão e dos crimes diários cometidos e descobertos por denúncias de cidadãos ou outras informações policiais que se configuram no território de forma cíclica, proporciona a distribuição única e regular do espaço e do tempo¹⁸⁴.

É uma técnica de *machine learning* que visa treinar um sistema informático de forma a permitir-lhe a resolução autônoma de problemas a partir de dados de exemplos, constituídos por pares de entrada e saída, tornando-se assim, uma aplicação de um modelo estratégico de prevenção e vigilância territorial¹⁸⁵. A solução, graças à técnica do SIG, dá ao policial um mapa de risco que mostra a cada 30 minutos por meio de um APP os locais e horários precisos em que um crime pode ser consumado descrevendo o tipo de crime, o *modus operandi* do autor, o tipo de vítima e de alvo¹⁸⁶.

Por meio da análise e observação do contexto do local, não somente dos crimes, é possível isolar as áreas definidas como áreas de “reserva de caça” que são áreas onde o crime

¹⁸² Crupi, Giuseppe. *XLaw- Innovazione strategica e tecnologica per la prevenzione dei reati predatori urbani*. In Periodico mensile ufficiale appartenente polizia n° 69. Direzione Nazionale SIAP. In: <https://docplayer.it/105316492-Polizia-speciale-previdenza-le-nuove-pensioni-il-governo-apra-al-confronto-e-l-opposizione-svolga-il-suo-ruolo-pubblica-sicurezza-n-69.html>, p.63.

¹⁸³ <https://www.xlaw.it/presentazione/>

¹⁸⁴ <https://www.smau.it/casi-di-successo/xlaw-lalgoritmo-poliziotto-che-prevede-furti-e-rapine>

¹⁸⁵ Giacomo, Di Gennaro; Elia Lombardo. *Intelligenza artificiale tra etica e diritti. Prime riflessioni a seguito del libro bianco dell'Unione Europea*. In: <https://www.sicurezza4p.it/blog/index.asp?Q=2E5H98EB47D5XA4HK0J7>

¹⁸⁶ <https://www.smau.it/casi-di-successo/xlaw-lalgoritmo-poliziotto-che-prevede-furti-e-rapine>

ocorre com mais facilidade. Assim sendo, foi possível perceber facilmente o momento em que o crime pode ocorrer devido à regularidade e sequencialidade das ações dos criminosos¹⁸⁷.

O programa já opera há anos em várias cidades italianas, incluindo Nápoles, Salerno, Veneza, Livorno, Módena, Trieste, Trento e Prato. Sua eficácia foi submetida a julgamento livre de forma transparente e recebeu o consentimento independente não só dos especialistas, mas também da opinião acadêmica, jurídica e pública. O XLAW é um programa transparente, um sistema *White Box*, e tanto o utilizador como algum eventual avaliador externo conseguem ter acesso às finalidades de seu uso¹⁸⁸.

Além disso, seu funcionamento e o tipo de informações coletadas foram atestados por um estudo do Professor Giacomo di Gennaro, da Universidade de Nápoles Federico II, e de Professor Riccardo Marselli, do Partenope de Nápoles¹⁸⁹. De acordo com as primeiras estatísticas analisadas, em Nápoles o *software* teve uma precisão entre 87% a 93%, em Veneza entre 92 e 93%, e em Prato cerca de 94%¹⁹⁰, o que permitiu estabelecer que a IA, se implementada e utilizada de forma adequada para as atividades de segurança urbana, dada a elevada fiabilidade e precisão operacional, pode ajudar no monitoramento do território com maior precisão e eficácia com base no grau real de risco e de acordo com princípios matemáticos, colocando-o em condições ideais para interceptar a origem do delito, evitando ou interrompendo sua ação¹⁹¹. O *software* também atingiu o nível máximo de maturidade das novas tecnologias (TRL9 na escala de referência internacional)¹⁹².

Elia Lombardo destaca que criou duas camadas dentro do *software*: na primeira é uma espécie de cidade virtual onde inseriu todas as informações sociodemográficas da cidade, tais como número de habitantes, de domicílios, lojas, bancos, correios, horários de comboios, de autocarros, ou seja, todas as informações úteis para entender como a cidade funciona e se movimenta. Após, definiu as características do criminoso, ou seja, o tipo de agressor (sexo, idade e *modus operandi*), tipo de dia, horário, tipo da vítima (estudante, profissional, idoso, dona de casa) e tipo de alvo (relógio, dinheiro, celular, veículo)¹⁹³.

¹⁸⁷ Blog Sicurezza 4P. *Perché la Polizia predittiva per la sicurezza urbana in Italia ha funzionato*. In:

<https://www.sicurezza4p.it/blog/index.asp?Q=HD1Q56756E0EG2PNB79N>

¹⁸⁸ <https://www.xlaw.it/presentazione/>

¹⁸⁹ <https://www.tpi.it/tecnologia/xlaw-algoritmo-prevede-furti-rapine-20190730383409/>

¹⁹⁰ *Idem, ibidem*

¹⁹¹ <https://www.xlaw.it/presentazione/>

¹⁹² <https://www.smau.it/casi-di-successo/xlaw-lalgoritmo-poliziotto-che-prevede-furti-e-rapine>

¹⁹³ Lombardo, Elia. *Sicurezza 4P. Lo studio alla base del software XLaw per prevedere e prevenire i crimini*. Mazzanti Libri, 2019, p. 97.

Segundo Lombardo, essas informações definem um modelo criminoso e, combinando todos estes dados, chega-se à identificação do crime¹⁹⁴. Por conseguinte, o patrulhamento dos lugares que serão potencialmente alvos remove os elementos de regularidade e previsibilidade do criminoso, fazendo com que o sujeito acabe por desistir do próprio roubo¹⁹⁵. Por meio de uma estrutura articulada, o XLAW utiliza um protocolo denominado *Sicurezza 4P* (Segurança 4P) ou abreviadamente S4P, que quer dizer: 1) Prevenção: que é a melhor saída para evitar os crimes predatórios urbanos; 2) Precisão: Deve haver intervenções cirúrgicas graças as análises previsionais utilizando a tecnologia para a detecção de risco iminente; 3) Proatividade: Atividade e atitudes proativas por parte dos responsáveis pela segurança e controlo; 4) Participação: de todos as pessoas envolvidas no projeto de detecção do risco¹⁹⁶.

No ano de 1999 se iniciou o estudo sobre fenômenos dos desvios urbanos e dos crimes predatórios urbanos em Nápoles. Em 2003 foi criado o programa XLAW, como modelo preditivo e, em 2004, Nápoles foi a primeira cidade a experimentar o programa. No ano de 2012 foi criado o protocolo de Segurança 4P, que teve junto com o programa XLAW, a sua validação acadêmica e lançamento da estrutura para colocação em vários escritórios operacionais da polícia italiana. De 2013 a 2019 ocorreu a experimentação oficial nos escritórios operacionais da Polícia de Nápoles, Prato, Salerno, Veneza, Modena e Parma¹⁹⁷.

1.3.1 *Método de análise para verificação dos resultados*

O estudo de prevenção da criminalidade predatória realizado por meio do algoritmo heurístico XLAW fornece alertas precisos de onde podem ocorrer os crimes predatórios, pois trabalha o modelo criminoso, a sequência de ataque, o *modus operandi* do autor e o tipo de alvo, sendo capaz de identificar onde e quando o crime pode ocorrer. Os locais identificados pelo algoritmo são definidos como “reserva de caça” que são as áreas limitadas no mapa, por onde circulam os criminosos e (predadores) e os alvos (presas). Assim sendo, nessas áreas existem regras precisas induzidas pela constância de factores presentes e repetidamente verificados, bem como a necessidade do estudo espacial urbano, constituindo a malha urbana, que é o conjunto

¹⁹⁴ <https://www.tpi.it/tecnologia/xlaw-algoritmo-prevede-furti-rapine-20190730383409/>

¹⁹⁵ *Idem, ibidem*

¹⁹⁶ Lombardo, Elia. *Sicurezza 4P. Lo studio alla base del software XLaw per prevedere e prevenire i crimini*. Mazzanti Libri, 2019, p. 141.

¹⁹⁷ In <https://www.xlaw.it/presentazione/>

de espaços públicos destinados à todos¹⁹⁸.

Segundo dados fornecidos pelo sítio do programa XLAW, para a análise da experimentação oficial, foram escolhidas seis das onze cidades que até agora utilizam da tecnologia. Elas levam em consideração a superfície, o número de habitantes, a densidade habitacional, o número de sedes de Polícia, o número de delegacias de polícia, e o índice de pressão criminal¹⁹⁹.

A análise quantitativa levou em consideração os seguintes dados: *1) redução de crimes cometidos*: foi considerado o número de crimes cometidos no ano anterior ao experimento e no ano em que ocorreu o experimento, comparando os resultados com os obtidos em outras cidades com dados semelhantes e que não utilizaram o programa; *2) falha na localização do crime*: distribuição georreferenciada dos crimes cometidos no ano anterior ao desenvolvimento do experimento e no ano em que ocorreu o experimento; *3) eficácia do método de prevenção tradicional e preditivo*: diferença entre o número de crimes cometidos com o método tradicional de previsão e o utilizado por meio do programa; *4) redução de quilômetros percorridos por patrulhas policiais e desgaste de veículos*: diferença entre os dados anteriores e posteriores ao uso do programa preditivo²⁰⁰.

A análise qualitativa levou em consideração: *1) a confiabilidade das previsões*: os crimes cometidos e as previsões eram comparados diariamente por meio de ferramenta de verificação específica, processados pelo *software* para avaliar a confiabilidade e precisão do relatório; *2) a participação das polícias locais*: o número de verificações de prevenção realizadas por iniciativa de policiais utilizando o método tradicional e o método preditivo apurado, elaborando, assim, a diferença entre os dois; *3) a segurança real e segurança sentida*: com o intuito de verificar quaisquer diferenças entre a segurança real e sentida foi utilizado o índice de pressão criminal (PCrime²⁰¹). Por último, foi levado em consideração o impacto na mídia e na opinião pública²⁰².

Por meio de uma ferramenta de verificação do programa foi possível avaliar a confiabilidade das previsões feitas diariamente pelo XLAW. O experimento constituiu em uma análise relativa ao lugar, o tipo, a data e a hora do evento, resultando na porcentagem de previsão.

¹⁹⁸ Piccoli, Donato; Lombardo, Elia; Bettoni, Raffaella. *Il modello predittivo XLAW correla i crimini con la configurazione fisica della città: urbanistica e informazione INU edizione*. In: <https://www.sicurezza4p.it/blog/index.asp?Q=NA6V4HA8990G544IV789>

¹⁹⁹ *Idem, ibidem*.

²⁰⁰ In <https://www.xlaw.it/presentazione/>

²⁰¹ Mede a pressão do crime no território em exame em função do número de crimes cometidos em relação ao número de cidadãos residentes e não residentes, ao número de residências, empresas, teatros, cinemas, etc., ao tamanho do território e à dinâmica socioeconômica

²⁰² In <https://www.xlaw.it/presentazione/>

Os números finais de precisão das previsões utilizando o programa foram 84% em Nápoles, 87% em Salerno 87%, 89% em Prato 89%, 83% em Veneza, 82% em Parma e 86% em Módena²⁰³.

1.3.2 Eficácia do método preditivo

Uma das críticas atribuídas ao método de previsão era a possibilidade de deslocamento do crime. Para isso, ocorreu uma verificação por meio de diagramas. Partiu-se de um ponto onde o fenômeno se concentrava antes do tratamento e foi sobreposto um diagrama que une vários pontos por onde a criminalidade poderia ter se deslocado após o a utilização do programa, tendo por base a morfologia e as características do território. Após um ano de utilização do programa observou-se a diminuição da criminalidade, bem como, a não ocorrência do aumento nos pontos alternativos. Ou seja, a criminalidade não se movimentou²⁰⁴.

Nas figura abaixo, os locais indicados pelos círculos numerados, são os únicos locais possíveis para onde a criminalidade poderia ter se concentrado após o uso do XLAW²⁰⁵.



Em comparação com cidades que não fizeram parte do estudo, houve significativa redução da criminalidade nas que utilizaram o *software*. Foram testadas e verificadas cidades com características sociodemográficas bem semelhantes, abaixo listadas²⁰⁶:

²⁰³ In <https://www.xlaw.it/presentazione/>

²⁰⁴ Material privado cedido pelo autor, Elia Lombardo.

²⁰⁵ *Idem, ibidem*

²⁰⁶ *Idem, ibidem.*

Cidade	Redução dos crimes % (no período do experimento)	Número de crimes a menos
Parma	43%	1.600
Taranto**	19,5%	577
Salerno	38,8%	642
Ferrara**	4,2%	192
Veneza	19,1%	923
Catania**	1,8%	243

** cidades que não fizeram parte do experimento.

Tabela 1: Percentagem de eficácia do programa²⁰⁷

Nas cidades testadas, a produtividade da Polícia Estadual que adotou a tecnologia do XLAW foi significativamente superior, ou seja, os crimes foram cometidos em maior número nas áreas de competência das cidades que adotaram o método tradicional de prevenção, como demonstrado a seguir²⁰⁸.

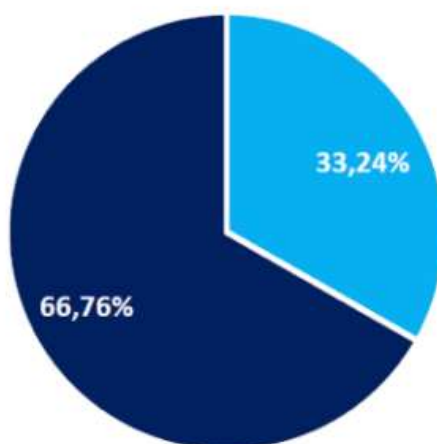


Figura 2: Porcentagem de eficácia do programa entre cidades que o utilizam *versus* cidades que não utilizam o programa.

Onde se lê 66,76%, corresponde aos crimes que ocorreram nas cidades que utilizaram os métodos tradicionais de prevenção. E onde se lê 33,24% são nas cidades que utilizaram o programa²⁰⁹. A tabela a seguir mostra as cidades que fizeram parte do experimento, utilizando o modelo preditivo XLAW, bem como sua população, densidade populacional, território e índice de pressão criminal²¹⁰.

²⁰⁷ Material privado cedido pelo autor, Elia Lombardo.

²⁰⁸ *Idem, ibidem*

²⁰⁹ *Idem, ibidem.*

²¹⁰ Material privado cedido pelo autor, Elia Lombardo

	Área	Habitantes	Densidade populacional	Índice de pressão criminal
Nápoles	117,27 km ²	972.130	8.148,22 por km ²	9
Salerno	59,85 km ²	134.850	2.215,89 por km ²	19
Prato	97,35 km ²	185.089	2,004 por km ²	9
Veneza	415,9 km ²	259.809	624,69 por km ²	12
Parma	260,6 km ²	197.499	757,86 por km ²	13
Módena	183,19 km ²	186.307	1.017,02 por km ²	15

Tabela 2: Tabela com dados das cidades parte do experimento²¹¹

Já nas tabelas abaixo, demonstra-se, como resultado, a diminuição de alguns tipos de crimes (os crimes alvo do experimento), bem como da economia em dinheiro com a utilização do programa em cada cidade. Vejamos²¹²:

NÁPOLES

Resultados obtidos com o uso do XLAW

Furtos de bolsas	-3,9%
Roubos	-23,9%
Batedores de carteira	-5%
Furtos em casas e empresas	-12,6%
Furtos de veículos	-1,6%
Índice de pressão criminal	-66,7%

Resultados econômicos

Economia para a cidade com base nos resultados de prevenção	€ 555.800
Economia de quilômetros rodados pela Polícia	61%
Economia de combustível utilizado pela Polícia	€ 33.580

Tabela 3: Tabela com resultado de Nápoles

SALERNO

Resultados obtidos com o uso do XLAW

Furtos de bolsas	-44,2%
Roubos	-48,9%
Batedores de carteira	-19,5%
Furtos em casas e empresas	-21,2%
Furtos de veículos	-1,7%
Índice de pressão criminal	-36,8%

²¹¹ Material privado cedido pelo autor, Elia Lombardo.

²¹² *Idem, ibidem*

Resultados econômicos

Economia para a cidade com base nos resultados de prevenção	€ 101.400
Economia de quilômetros rodados pela Polícia	47,8%
Economia de combustível utilizado pela Polícia	€ 80.300

Tabela 4: Tabela com resultado de Salerno

PRATO

Resultados obtidos com o uso do XLAW

Furtos de bolsas	-10%
Roubos	-5%
Batedores de carteira	-21%
Furtos em casas e empresas	-10%
Furtos de veículos	-28%
Índice de pressão criminal	-55,6%

Resultados econômicos

Economia para a cidade com base nos resultados de prevenção	€ 522.600
Economia de quilômetros rodados pela Polícia	40,9%
Economia de combustível utilizado pela Polícia	€ 75.920

Tabela 5: Tabela com resultado de Prato

VENEZA

Resultados obtidos com o uso do XLAW

Furtos de bolsas	-23,8%
Roubos	-15,5%
Batedores de carteira	-1%
Furtos em casas e empresas	-22,8%
Furtos de veículos	-24,3%
Índice de pressão criminal	-50%

Resultados econômicos

Economia para a cidade com base nos resultados de prevenção	€ 134.800
Economia de quilômetros rodados pela Polícia	37%
Economia de combustível utilizado pela Polícia	€ 54.020

Tabela 6: Tabela com resultado de Veneza

PARMA

Resultados obtidos com o uso do XLAW

Furtos de bolsas	-44,2%
Roubos	-15,4%
Batedores de carteira	-5,4%
Furtos em casas e empresas	-25,8%
Furtos de veículos	-30,6%
Índice de pressão criminal	-50%

Resultados econômicos

Economia para a cidade com base nos resultados de prevenção	€ 303.800
Economia de quilômetros rodados pela Polícia	40,9%
Economia de combustível utilizado pela Polícia	€ 75.920

Tabela 7: Tabela com resultado de Parma

MÓDENA

Resultados obtidos com o uso do XLAW

Furtos de bolsas	-6,4%
Roubos	-10,1%
Batedores de carteira	-6%
Furtos em casas e empresas	-14%
Furtos de veículos	-5,9%
Índice de pressão criminal	-25%

Resultados econômicos

Economia para a cidade com base nos resultados de prevenção	€ 36.300
Economia de quilômetros rodados pela Polícia	40,9%
Economia de combustível utilizado pela Polícia	€ 68.620

Tabela 8: Tabela com resultado de Módena

Assim sendo, conclui-se que o estudo do XLAW baseia-se principalmente na aplicação de estratégias de controlo territorial, bem como em análises criminológicas anteriores, capazes de simular situações futuras, colocando a polícia em uma posição antecipada dos movimentos (prevenção) ao interromper as condições com alta probabilidade de determinar os casos que originariam o evento. Ou seja, é um modelo de avaliação de risco baseado na lógica do uso de "*big data*", sendo possível prever certos tipos de crimes urbanos que têm a característica de se repetirem no tempo e no espaço, desde que se consiga definir e implementar um método de previsão adequado com base na elevada fiabilidade e precisão das elaborações do modelo

preditivo desenvolvido²¹³.

É facto que o uso indiscriminado e muitas vezes indevido da inteligência artificial, em especial na área da segurança pública, seja preocupante, pois o uso de *big data* e IA podem interferir seriamente na privacidade de dados e liberdade. E a preocupação é tamanha que, alguns cientistas e pesquisadores peticionaram à comunidade científica internacional para pararem de utilizar o policiamento preditivo. Contudo, esse não é o caso do *software* XLAW, pois o programa italiano foi desenvolvido e implementado utilizando a IA, mas não sendo esta ferramenta um factor determinante. Não utiliza dados sensíveis, se baseando nos tipos de crimes objetivamente e não nos autores dos crimes²¹⁴.

O experimento que ocorreu na Itália supera essas questões críticas, pois antes de tudo o sistema não visa prender os autores, mas criar um sistema de avaliação de risco adequado e, portanto, de maior prevenção, que é a primeira tarefa das instituições para com os cidadãos. Na verdade o XLAW não recolhe dados pessoais, mas apenas dados sobre acontecimentos e dados da dinâmica sócio urbana, sendo possível traçar números que não dizem respeito ao aspecto subjetivo, mas sim ao aspecto objetivo do local onde ocorrem²¹⁵. Diferentemente de outros programas de policiamento preditivo que fornecem dados aos seus algoritmos (maioria das vezes dados sensíveis) que pode acabar resultando em um viés algorítmico. Esses tipos de programas analisam dados referentes aos cidadãos e não aos crimes em si.

Como já anteriormente explicado, para evitar esse tipo de viés o *software* italiano não foi elaborado apenas por engenheiros de computação, mas também por especialistas em criminologia, sociólogos, urbanistas, além de não ter colocado o infrator como o centro do problema, mas sim considerado as condições estruturais e sociais do contexto local de onde ocorrem os crimes. Assim sendo, foi possível a criação de um modelo preditivo que leva em conta todo o contexto, condições socioeconômicas, tipos de vítimas, horários, época do ano, datas e não utilizando o aspecto subjetivo, que é a análise do infrator²¹⁶.

Os objetivos do programa XLAW não eram de resolver a criminalidade em geral, mas os crimes recorrentes diários que mais preocupam os cidadãos, além de não identificar sujeitos, pois, nesse caso, teria o risco de tornar alvo grupos de sujeitos ou etnias diferentes, classe social ou raça. Também não era o objetivo a militarização do território para não ocorrer em

²¹³ In <https://www.xlaw.it/presentazione/>. Pesquisa realizada em 20/09/2020.

²¹⁴ <https://www.sicurezza4p.it/blog/index.asp?Q=HD1Q56756E0EG2PNB79N>

²¹⁵ Resposta de Elia Lombardo ao e-mail enviado pela autora da presente dissertação.

²¹⁶ In: <https://www.sicurezza4p.it/blog/index.asp?Q=HD1Q56756E0EG2PNB79N>

discriminação de determinadas áreas ou lugares com pontos críticos. O objetivo do programa era valorizar a prevenção ao construir um modelo de avaliação de risco utilizando a inteligência artificial com limites éticos respeitados, com o intuito de poder construir um modelo de ação de controlo estratégico e uma visão restaurativa do dano e probabilística de risco²¹⁷.

1.4. A utilização dos *softwares* de policiamento preditivo e o impacto no Processo Penal

Algoritmos estão sendo projetados para prever crimes, automatizar processos judiciais e prever reincidências. Atualmente, observa-se uma mudança de paradigma no trabalho policial provocada pelo policiamento preditivo, passando o foco da acusação para a prevenção do crime. Esses aplicativos exibem um certo nível de inteligência algorítmica, pois modelam áreas de risco a partir de dados anteriores²¹⁸. Vários são os sistemas de IA que podem ser aplicados no direito penal e utilizados no processo penal, tais como, policiamento preditivo, sistemas de identificação biométrica, sistemas de decisão automatizados, ferramentas de avaliação de risco. Na dissertação ora apresentada, destacamos somente o policiamento preditivo²¹⁹.

A utilização de sistemas de IA na aplicação da lei e da justiça penal pode suscitar preocupações relacionadas com a presunção de inocência, o direito de ser informado prontamente sobre a causa e uma acusação, o direito a um julgamento justo e o direito de se defender pessoalmente. Esses sistemas podem entrar em conflito com direitos constitucionalmente protegidos de suma importância, pelo que seu uso deve ser permitido apenas em condições monitoradas ou então, serem proibidos²²⁰.

Para proteger esses direitos, a proposta legislativa formulada pela Comissão Europeia em abril de 2021, legitima a utilização da IA para efeitos de aplicação da lei penal. Contudo, essa aplicação deve ser transparente, segura e que respeite os direitos fundamentais, a fim de que não se tornem ferramentas que produzam avaliações injustificadas e discriminatórias no processo penal²²¹.

²¹⁷ In: <https://www.sicurezza4p.it/blog/index.asp?Q=HD1Q56756E0EG2PNB79N>

²¹⁸ Simmler, Monika. Canova, Giulia. *The rise of algorithms in the criminal justice system*. In: <https://blog.ai-laws.org/the-rise-of-algorithms-in-the-criminal-justice-system/?cn-reloaded=1&cn-reloaded=1&cn-reloaded=1>

²¹⁹ In: <https://www.riskmanagement360.it/analisti-ed-esperti/intelligenza-artificiale-e-processo-penale-un-vuoto-normativo-da-colmare/>

²²⁰ González Fuster, Prof. Dr. Gloria. *Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights*. July 2020 European Union, 2020. In <http://www.europarl.europa.eu/supporting-analyses>, p43.

²²¹ Proposta de Regulamento do Parlamento Europeu e do Conselho em matéria de Inteligência Artificial. In: <https://eur-lex.europa.eu/legal-content/pt/txt/html/?uri=celex:52021pc0206&from=en>

Em relação às ferramentas de IA utilizadas no policiamento preditivo, essas podem ser divididas em quatro categorias: para prever crimes ou prever lugares e horários com risco aumentado de crime, para prever infratores ou identificar indivíduos em risco de ofender ou reincidir no futuro, para prever ou criar perfis semelhantes aos do passado infratores e, métodos destinados a prever vítimas de crimes, usados para identificar grupos ou indivíduos que provavelmente se tornarão vítimas de crimes²²². Essas ferramentas são usadas como apoio à polícia e a sua utilização ocorre num momento anterior à instauração do processo penal, para efeitos de prevenção geral de infracções penais relevantes (como no caso do XLAW). Esses programas são utilizados em áreas territoriais de maior risco criminal (*hotspots*) e também na disponibilização de métodos e prazos para o cometimento de delitos por determinados sujeitos (*criminal profiling*)²²³. Esses últimos são baseados em algoritmos capazes de prever se e quando uma determinada pessoa cometerá um determinado crime²²⁴.

O processo penal centra-se nas hipóteses e factos, pistas e provas. No julgamento, quando não se tem uma prova irrefutável de autoria e é julgado por probabilidades, há o risco de que a decisão possa ser prejudicada por distorções ou erros. Por conseguinte, alguns princípios devem se sobressair, tais como, a presunção de inocência do acusado e o princípio do contraditório²²⁵. Portanto, a autenticidade das evidências derivadas dos resultados do *software* polícia preditiva depende da legitimidade e integridade dos dados coletados durante as investigações preliminares que foram inseridos dentro do programa, ou seja, a confiabilidade do algoritmo é estritamente conectada com a qualidade das informações com as quais o sistema é alimentado, bem como com a possibilidade acessar os métodos operacionais do programa utilizado²²⁶.

Uma das questões relevantes para apoiar a possibilidade de aplicação no processo de um sistema de inteligência artificial é a verificação dos algoritmos que eles contêm,

²²² Proposta de Regulamento do Parlamento Europeu e do Conselho em matéria de Inteligência Artificial. In: <https://eur-lex.europa.eu/legal-content/pt/bxt/html/?uri=celex:52021pc0206&from=en>, p.23.

²²³ In: <https://www.riskmanagement360.it/analisti-ed-esperti/intelligenza-artificiale-e-processo-penale-un-vuoto-normativo-da-colmare/>

²²⁴ Polidoro, Donato. *Tecnologie informatiche e procedimento penale: la giustizia penale "messa alla prova" dall'intelligenza artificiale*. In <https://archiviopenale.it/tecnologie-informatiche-e-procedimento-penale-la-giustizia-penale-messa-alla-prova-dallintelligenza-artificiale/articoli/25993>

²²⁵ Canzio Giovanni. *Intelligenza artificiale, algoritmi e giustizia penale*. In: <https://www.sistemapenale.it/it/articolo/canzio-intelligenza-artificiale-algoritmi-giustizia-penale>

²²⁶ Polidoro, Donato. *Tecnologie informatiche e procedimento penale: la giustizia penale "messa alla prova" dall'intelligenza artificiale*. In <https://archiviopenale.it/tecnologie-informatiche-e-procedimento-penale-la-giustizia-penale-messa-alla-prova-dallintelligenza-artificiale/articoli/25993>

prestando atenção tanto para a possibilidade que ele possa apresentar preconceitos, de acordo com os interesses ou inclinações dos programadores, quanto ao seu grau de confiabilidade preditiva, que muitas vezes dependerá da qualidade dos dados utilizados em sua elaboração²²⁷.

Por esta razão, o Parlamento Europeu salientou que serão necessárias avaliações periódicas sobre a representatividade dos conjuntos de dados, bem como, examinar a precisão e a significância das previsões. Por conseguinte, antes de tomar uma decisão sobre a possibilidade de usar esses mecanismos no ordenamento jurídico é necessário resolver a questão de como regular os mecanismos que irão garantir uma auditoria adequada do seu funcionamento, adequando ao sistema de proteção, garantindo assim, os direitos fundamentais e garantias processuais. Além disso, a lógica do algoritmo deve ser compreensível pelas partes do processo de forma que seja garantido o direito de defesa. A avaliação da prova no processo penal corresponde ao juiz, mas é possível utilizar a inteligência artificial no processo penal seja como meio de prova ou utilizados em conjunto com os meios tradicionais de prova para que possam ser mais eficazes e, assim, auxiliar o juiz na avaliação judicial da prova²²⁸.

O método de policiamento preditivo feito por análise preditiva e que identifica indivíduos com maior probabilidade de cometer crimes futuros é o mais preocupante em relação ao uso de provas no processo penal. Além dos dados geográficos e sociodemográficos, os dados pessoais também são inseridos no *software* alimentado. E é nesse tipo de análise de dados que ocorrem sérias interferências nos direitos básicos e pessoais dos indivíduos, que por uma previsão algorítmica podem ter suas garantias processuais penais e constitucionais, tais como, a presunção de inocência, postas em risco. A falta de transparência por parte dos fabricantes de *software* e seus métodos de avaliação também geram problemas. É, portanto, de particular importância que os interesses dos indivíduos, sua liberdade e seus direitos básicos, devam sempre ser ponderados em detrimento do policiamento preditivo. As previsões de periculosidade agem contra a garantia da presunção de inocência, uma vez que os prognósticos jurídicos negativos se baseiam na presunção de culpa futura, levando em consideração antecedentes criminais, prisão ou outra interferência na liberdade da pessoa em causa²²⁹.

²²⁷ Pérez Estrada, Miren Josune. *La inteligencia artificial como prueba científica en el proceso penal español*. In: <https://revista.ibraspp.com.br/RBDPP/article/view/505>

²²⁸ *Idem, ibidem*.

²²⁹ Verlag, Helbing Lichtenhahn. Monika Simmler (Hrsg.). *Smart Criminal Justice - Der Einsatz von Algorithmen in der Polizeiarbeit und Strafrechtspflege*. Basileia, 2021. In: <https://www.helbing.ch/annotstream/9783719043971/PDF/Smart-Criminal-Justice.pdf?sq=27>, pp.103-145.

A mudança no direito penal de um propósito repressivo para um preventivo, impulsionado por essa mudança social, traz uma mudança na área de intervenção no âmbito do direito penal, bem como uma expansão dos poderes de intervenção da polícia. Renunciar a liberdade em favor de mais segurança e mais controlo é uma decisão séria. Deve ser garantido uma maneira que permite uma defesa contra as classificações de periculosidade, de modo que o direito a um julgamento justo seja prioridade²³⁰.

1.5. Conclusão do capítulo

É inegável que a utilização de novas tecnologias, como os *softwares* preditivos colaboram com o trabalho da polícia, seja na investigação ou na prevenção. Mas a que custo? No caso de *softwares* que fazem o uso de predição de crimes, até que ponto é ético a imputação dos crimes? Esperar o criminoso terminar a ação, somente o observando ou o prender no mínimo de ação possível para lhe imputar um crime? Seria válido e ético essa atitude no processo penal, apenas com a presunção de que o indivíduo realmente praticaria tal delito? Seria salutar essa utilização do *Big Data* e do uso da inteligência artificial sem ferir os direitos e garantias individuais? Essas são as perguntas que devem ser feitas por juristas, programadores, engenheiros, ou seja, todos que trabalham na área da inteligência artificial e do big data que fazem e trabalham com *softwares* e algoritmos aplicados na justiça preditiva.

No caso do programa XLAW, objeto de estudo da presente dissertação, é levada em consideração essa análise de dados sensíveis e por isso não é utilizado, sendo observado apenas o tipo de crime, a hora, data e local, sem nenhum tipo de identificação do autor ou vítima. Também verificou-se que no programa objeto de estudo, que não houve o deslocamento do crime, além de que houve uma redução dos crimes de menor potencial ofensivo em relação às cidades que não participaram do programa (levando em consideração cidades com mesmo índice criminal e população). Na atualidade, vislumbra-se a necessidade de construção de uma verdadeira cultura jurídica que reconheça os benefícios do enlace entre Direito e Inteligência Artificial²³¹, pois, o uso do *big data* na seara do direito penal é cada vez mais importante e deve ter como objetivo auxiliar o trabalho policial nas atividades investigativas e operacionais auxiliando na redução de crimes e

²³⁰ Verlag, Helbing Lichtenhahn. Monika Simmler (Hrsg.). *Smart Criminal Justice - Der Einsatz von Algorithmen in der Polizeiarbeit und Strafrechtspflege*. Basileia, 2021. In: <https://www.helbing.ch/annotstream/9783719043971/PDF/Smart-Criminal-Justice.pdf?sq=27>, pp.103-145.

²³¹ Lopes, Álvaro Luiz Primão. Brígido, Edimar Inocêncio. *Ética e Direito no mundo digital*, Tabulæ - Revista de Filosofia - ISSN 1980-0231, p.110.

garantindo a segurança pública, porém, os direitos e garantias individuais não devem ser violados, pelo contrário, devem ser os primeiros a serem garantidos e observados.

Considerações finais

O uso de algoritmos, especialmente os utilizados em aprendizagem de máquina, promovem inovação e eficiência aos usos que se destinam, como é no caso da justiça criminal. Polícias e judiciário de vários locais já fazem uso dessas ferramentas e com isso o policiamento preditivo traz um novo paradigma para a detecção de crimes. Existem diversos tipos de algoritmos, desde os que alegadamente preveem reincidência, quanto os que preveem crimes, seja baseado em perfis criminológicos, seja baseado no local, horário e no tipo de crime, como é o caso do presente estudo. Por conseguinte, o uso indiscriminado desses programas e a utilização de dados sensíveis para a base de dados acarreta o chamado viés algoritmo. Ou seja, acaba ocorrendo uma discriminação ao imputar um crime a pessoa pelo que ela é e não pelo crime que supostamente cometeu. A pessoa passa a ser suspeita pela sua vida pregressa, pela sua raça, religião. Esses programas que utilizam algoritmos com viés devem ser proibidos, pois situa o foco na acusação e não na prevenção do crime.

O presente estudo ao analisar como funciona a justiça preditiva, permitiu tirar conclusões gerais sobre o uso dessa tecnologia. Também permitiu conclusões e problematizações sobre o uso indiscriminado da inteligência artificial e suas ferramentas na seara da justiça criminal. Tais usos podem trazer graves consequências se não observados os direitos fundamentais, a proteção de dados e as leis processuais.

O programa estudado, XLAW, mostra a polícia em uma posição de antecipar os movimentos, ou seja, prevenir, ao interromper as condições que originaram o evento. Uma grande questão se diz ao facto de ser possível ou não a transferência da ação para outros crimes. De acordo com a serialidade, especialização e modus operandi, sim, pode ser possível. Para tanto, é importante a atualização e especialização dos órgãos policiais e dos especialistas criadores dos projetos. O programa apresentado muda a estratégia, passando a ter uma visão probabilística do risco ao invés de uma visão restauradora do facto ocorrido, passando a atuar na prevenção.

Assim sendo, o problema da pesquisa pôde ser respondido, pois a questão central era como funcionaria o *software* preditivo e se esse tinha eficácia, se funcionava aos fins que se destinavam. Portanto, pelo programa analisado, sim. Claro que é um tema extremamente extenso e que existem diversos programas com algoritmos e inferências diferentes. Contudo, a pesquisa empírica aqui apresentada obteve grande êxito. A pesquisa destacou que a prevenção criminal como principal função da polícia, está se adaptando aos novos métodos de policiamento preditivo, bem como sua preocupação em não ultrapassar os limites éticos e a demonstração da

transparência no uso. Assim sendo, as instituições precisam promover um amplo debate social sobre as aplicações e as implicações do uso da inteligência artificial. As discussões devem ser a nível dos princípios de proteção de dados, da liberdade, da dignidade da pessoa humana, combinados com a capacidade de contribuição da inteligência artificial para contribuir para o sucesso dos programas de IA e *Big Data*, a fim de gerar confiança e prevenir riscos.

Policimento preditivo tem como objetivo prever onde e quando os crimes ocorrerão no futuro, utilizando ferramentas de inteligência artificial para a prevenção e aplicação da lei. Porém ao substituir as decisões humanas por algoritmos, esses ficam no meio questões de ordem ética e jurídica. Portanto, se faz necessário regulamentar o uso dos algoritmos equilibrando ética e direito. A pesquisa apresentada, forneceu uma visão geral do policiamento preditivo, como deve funcionar e algumas ferramentas utilizadas. O objetivo da pesquisa não foi de afirmar se as ferramentas de policiamento preditivo são ruins ou se não deveriam ser usadas, mas sim de tentar entender, mesmo que de maneira generalista, como funciona o policiamento preditivo (em especial o *software* XLAW), a fim de demonstrar seus benefícios, limitações e implicações. O policiamento preditivo fornece ferramentas que têm o potencial de alavancar o desenvolvimento na área da justiça criminal, assim como de qualquer outra área. Contudo, se faz necessário respeitar os limites éticos e legais para sua aplicabilidade.

Por fim, se pôde observar que os métodos computacionais podem ser adequados para apoiar a análise criminal e os seus dispositivos de inteligência, especialmente na detecção de padrões no policiamento preditivo, em conjunto com profissionais de diversas áreas. No entanto, esses padrões não devem ser formados com dados sensíveis, dados que acabam por deixar o algoritmo com viés de discriminação em relação à raça, sexo, religião, orientação sexual. Do contrário, esses programas podem se tornar uma releitura de Lombroso.

Bibliografia

Aggarwal, Charu C. *Data Mining, The Textbook*. Springer, 2015.

Albuquerque, Paulo Pinto de. *Comentário ao Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*. Universidade Católica, 4ª edição, 2011.

Algoritmo e Lógica de programação. Universidade Federal do Rio Grande do Norte, Centro de Tecnologia, Departamento de Computação e Automação Algoritmo e Lógica de Programação. Algoritmos, Parte 1. Eng. Química, maio 2004. In https://www.dca.ufrn.br/~affonso/DCA800/pdf/algoritmos_parte1.pdf

Baratta, Alessandro. *Criminologia crítica e crítica do Direito Penal. Introdução à sociologia do Direito Penal*. Rio de Janeiro: Revan, 2002.

Basile, Fabio. *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine. Artificial intelligence and criminal law: four possible research leads*. Diritto Penale e Uomo, Milano, 2018. In: <https://archiviodpc.dirittopenaleuomo.org/upload/3089-basile2019.pdf>

Bengio, Yoshua; Goodfellow, Ian; Courville, Aaron. *Deep Learning*. Ed. The MIT Press, 2015.

Besse, Philippe. Castets-Renard, Céline. Garivier, Aurélien. *Loyauté des Décisions Algorithmiques Contribution au débat public initié par la CNIL : Éthique et Numérique*. In: <https://hal.archives-ouvertes.fr/hal-01544701>

Bex, Floris; Prakken, Henry; Engers, Tom van; Verheij, Bart. *Introduction to the special issue on Artificial Intelligence for Justice (AI4J)*. Springer Science Business Media Dordrecht, 2017.

BigData: *Discrimination in data-supported decision making. European Union Agency for Fundamental Rights, 2018*. In: <https://super-ai.diascreative.net/bigdata-discrimination-in-data-supported-decision-making>

Bramer, Max. *Principles of Data Mining*, Third Edition. Springer, 2016.

Brozek, Bartosz; Hage, Jaap; Indurkha, Bipin. *Introduction to the special issue on machine law. Artif Intell Law (2017)* 25:251–253. In DOI 10.1007/s10506-017-9213-x

Campagna, Marco Francesco. *Gli scambi attraverso algoritmi e il problema del linguaggio. Appunti minimi*. Il Mulino - Rivisteweb, 2019. In: <https://www.rivisteweb.it/doi/10.1433/94549>

Casanovas, Pompeu. De Koker, Louis. Mendelson, Danuta. Watts, David. *Regulation of Big Data: Perspectives on strategy, policy, law and privacy*. Health Technol. 2017, DOI 10.1007/s12553-017-0190-6.

Castelli, Claudio; Piana, Daniela. *Giusto processo e intelligenza artificiale*. Maggioli Editore, 2019.

Castelli, Mauro; Sormani, Raul; Trujillo, Leonardo; Popovic, Ales. *Predicting per capita violent*

crimes in urban areas: an artificial intelligence approach. Springer-Verlag Berlin Heidelberg 2015.
J Ambient Intell Human Comput (2017) 8:29–36. In DOI 10.1007/s12652-015-0334-3

Celotto, Alfonso. *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*. Il Mulino - Rivisteweb, 2019. doi: 10.1433/94544

Cerri, Ricardo; Ferreira de Carvalho, André Carlos Ponce de Leon. *Aprendizagem de Máquina: Breve Introdução e Aplicações*. Cadernos de Ciência & Tecnologia, Brasília, v. 34, n. 3, p. 297-313, set./dez. 2017 In:
<https://ainfo.cnptia.embrapa.br/digital/bitstream/item/184785/1/Aprendizagem-de-maquina-breve-introducao.pdf>

Chalkidis, Ilias; Kampas, Dimitrios. *Deep learning in law: early adaptation and legal word embeddings trained on large Corporation*. Springer Nature B.V. 2018. Artificial Intelligence and Law (2019) 27:171–198. In <https://doi.org/10.1007/s10506-018-9238-9>

Chen, D.L. *Judicial analytics and the great transformation of American Law*. Artif Intell Law 27, 15–42 (2019). <https://doi.org/10.1007/s10506-018-9237-x>

Comandé, Giovanni. *Intelligenza artificiale e responsabilità 'a tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*. Il Mulino - Rivisteweb, 2019. In: <https://www.rivisteweb.it/doi/10.1433/94550>

Contissa, Giuseppe; Docter, Koen; Lagioia, Francesca; Lippi, Marco; Micklitz, Hans-Wolfgang; Palka, Przemyslaw; Sartor, Giovanni; Torroni, Paolo. *Automated processing of privacy policies under the EU general data protection regulation, Legal Knowledge and Information Systems*, Amsterdam. In: <http://ebooks.iospress.nl/publication/50834>

Crupi, Giuseppe. *XLAW- Innovazione strategica e tecnologica per la prevenzione dei reati predatori urbani*. In Periodico mensile ufficiale appartenente polizia. Polizia Pubblica Sicurezza n° 69, speciale previdenza, le nuove pensioni. Direzione Nazionale SIAP. In:
<https://docplayer.it/105316492-Polizia-speciale-previdenza-le-nuove-pensioni-il-governo-apra-al-confronto-e-l-opposizione-svolga-il-suo-ruolo-pubblica-sicurezza-n-69.html>

Daimi, Kevin. *Computer and Network Security Essentials*. Springer International Publishing, 2018.

Daumé III, Hal. *A Course in Machine Learning*, 2012. In: http://ciml.info/dl/v0_8/ciml-v0_8-all.pdf

Devins, Caryn. Felin, Teppo. Kauffman, Stuart. Koppl, Roger. *The Law and Big Data*. Cornell Journal of Law and Public Policy, Vol. 27. In:
<https://scholarship.law.cornell.edu/cjlp/vol27/iss2/3/>

Di Bello, Marcello; Verheij, Bart. *Evidence & decision making in the law: theoretical, computational and empirical approaches*. Springer Nature B.V. 2019. Artificial Intelligence and Law. In <https://doi.org/10.1007/s10506-019-09253-0>

Di Gennaro, Giacomo. Lombardo, Elia. Marselli, Riccardo. Spina, Michele. *Tolleranza zero o*

deterrenza selettiva: quali strade intraprendere per rispondere più efficacemente alla domanda di sicurezza? Criminalità e sicurezza a Napoli. Secondo rapporto. In:
<https://core.ac.uk/download/pdf/154857984.pdf>

Eco, Umberto. *Como se faz uma tese*; tradução Gilson Cesar Cardoso de Souza. - São Paulo: Perspectiva, 2008. 21. ed.

Evas, Tatjana. *European framework on ethical aspects of artificial intelligence, robotics and related Technologies*. European Parliamentary Research Service. Brussels, September 2020. In:
[https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU\(2020\)654179](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)654179)

Faro, Sebastiano; Pietrangelo, Marina. *Rivista Internazionale Informatica e diritto*, XLIII annata, Vol. XXVI, 2017, n. 1-2, 565 p. In:
https://www.iris.unina.it/retrieve/handle/11588/739339/228760/Rivista_IeD_1-2-2017_PrimePagine%20%281%29.pdf

Felipe, Bruno Farage da Costa; Perrota, Raquel Pinto Coelho. *Inteligência Artificial no Direito – uma realidade a ser desbravada*. Revista de Direito, Governança e Novas Tecnologias, v. 4, n. 1, p. 01 – 16, Jan/Jun. 2018. In:
<https://indexlaw.org/index.php/revistadgnt/article/download/4136/pdf>

Ferrari, Fabricio. Cechinel, Cristian. *Introdução a Algoritmos e Programação*. In:
<https://www.ferrari.pro.br/home/documents/FFerrari-CCechinel-Introducao-a-algoritmos.pdf>

Finocchio, Marco Antonio Ferreira. *Noções de Redes Neurais Artificiais*. UTFPR, 2014. In:
<http://paginapessoal.utfpr.edu.br/mafinocchio/labsi-laboratorio-de-seguranca-e-iluminacao/redes-neurais-artificiais/NOCaO%20DE%20REDES%20NEURONAI%20ARTIFICIAIS.pdf/view>

Foucault, Michel. *Vigiar e punir: nascimento da prisão*. Tradução de Raquel Ramallete. Petrópolis, Vozes, 1987.

Franco, Cristiano Roberto. *Inteligência artificial*. Uniasselvi, 2017. In:
<https://www.uniasselvi.com.br/extranet/layout/request/trilha/materiais/livro/livro.php?codigo=22869>

Gerards, Janneke. Xenidis, Raphaële. *Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law. A special report*. European network of legal experts in gender equality and non-discrimination. European Commission. Brussels, 2020. In:
<https://www.europeanfutures.ed.ac.uk/algorithmic-discrimination-in-europe-challenges-and-opportunities-for-eu-equality-law/>

Géron, Aurélien. *Hands-On Machine Learning with Scikit-Learn and TensorFlow*. Editora O'Reilly Media, E-book, 2017.

Giacomo, Di Gennaro; Elia Lombardo. *Intelligenza artificiale tra etica e diritti. Prime riflessioni a seguito del libro bianco dell'Unione Europea*. In:

<https://www.sicurezza4p.it/blog/index.asp?Q=2E5H98EB47D5XA4HK0J7>

Giménez, María Hernández. *Inteligencia Artificial y Derecho Penal*. Actualidad Jurídica Iberoamericana N.º 10, junio 2019, pp. 792-843. In: <http://www.revista-aji.com/wp-content/uploads/2019/06/792-843.pdf>

Giudici, Paolo. *Applied Data Mining Statistical Methods for Business and Industry*. Wiley, 2003. In: [http://index-of.co.uk/Data-Mining/Applied%20Data%20Mining-Statistical%20Methods%20for%20Business%20and%20Industry_Giudici%20P%20\(2003\).pdf](http://index-of.co.uk/Data-Mining/Applied%20Data%20Mining-Statistical%20Methods%20for%20Business%20and%20Industry_Giudici%20P%20(2003).pdf)

Gless, Sabine. *Predictive Policing in Defense Of 'True Positives.'* In: Bayamlio Lu, Emre; Baraliuc, Irina; Janssens, Liisa; Hildebrandt, Mireille (Ed.). *Being Profiled: Cogitas Ergo Sum. 10 Years of Profiling the European Citizen*, Amsterdam University Press, 2018. Tradutores: Heloisa Estellita e Miguel Lima Carneiro. Escola de Direito da FGV. Revista Direito Gv, SP, 2020. In: <http://bibliotecadigital.fgv.br/ojs/index.php/revdireitogv/article/download/81697/77918/174348>

González Fuster, Prof. Dr. Gloria. *Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights*. July 2020 European Union, 2020. In: <http://www.europarl.europa.eu/supporting-analyses>.

Goodfellow, Ian; Bengio, Yoshua; Courville, Aaron. *Deep learning*. Cambridge, MA MIT Press. Series: Adaptive computation and machine learning series, 2017.

Guimarães, Rodrigo Régner Chemim. *A Inteligência Artificial e a disputa por diferentes caminhos em sua utilização preditiva no processo penal*. 2019. In: <http://www.ibraspp.com.br/revista/index.php/RBDPP/article/view/260>.

Heaton, Jeff. AIFH. *Deep Learning and Neuronal Networks*. E-book, 2015.

Huws, C. F.; Finnis, J. C. *On computable numbers with an application to the Alan Turing problem*. Artif Intell Law (2017) 25:181–203 DOI 10.1007/s10506-017-9200-2

Iaselli, Michele. *IA nel settore legale: ma è vera intelligenza artificiale?* In: <https://www.altalex.com/documents/news/2019/05/10/ia-nel-settore-legale-intelligenza-artificiale>

Iaselli, Michele. *X-LAW: la polizia predittiva è realtà?* In: <https://www.altalex.com/documents/news/2018/11/28/x-law-la-polizia-predittiva>

Italiano, Giuseppe Francesco. *Le sfide interdisciplinari dell'intelligenza artificiale*. Il Mulino - Rivisteweb, 2019. In: <https://www.rivisteweb.it/doi/10.1433/94541>

Jakobs, Gunther. *Direito Penal do Inimigo: Noções e Críticas*. Editora Livraria do Advogado 6ªed.2015.

Jean-Meire, Caroline. *Les Nouvelles Technologies et la Lutte Contre la Délinquance : Regards Croisés* France/Royaume-Uni. Université de Paris 1 Panthéon-Sorbonne, École de droit de la Sorbonne, 2016. In: <https://ecm.univ-paris1.fr/nuxeo/síto/esupversions/e3fc7e62-562d-4c3d->

João, Paulo Abel de Almeida. *Modelo Preditivo da Criminalidade. Georeferenciação ao Concelho de Lisboa*. Universidade Nova de Lisboa, 2009. In: <https://run.unl.pt/handle/10362/3424>

Kelleher, John; Namee, M. Brian; Darcy, Aoife. *Fundamentals of machine learning for predictive data analytics: algorithms, worked examples, and case studies*. E-book, 2015.

Kemp, Richard. *Big data and data protection (GDPR and DPA 2018)*. Kemp IT Law and Practical Law Data Protection. European Union, International, United Kingdom. In: http://www.kempitlaw.com/wp-content/uploads/2014/10/Big-Data-and-Data-Protection-White-Paper-v1_0-November-2014.pdf

Kitchin, Rob. *Big Data, new epistemologies and paradigm shifts*. *Big Data & Society*, 2014. In: DOI: 10.1177/2053951714528481, p. 01-02.

Lagioia, Francesca; Sartor, Giovanni. *AI Systems Under Criminal Law: A Legal Analysis and a Regulatory Perspective*. Springer Nature B.V. 2019. Philosophy & Technology In <https://doi.org/10.1007/s13347-019-00362-x>

Leslie, D., Burr, C., Aitken, M., Cowls, J., Katell, M., and Briggs, M. (2021). *Artificial intelligence, human rights, democracy, and the rule of law: a primer*. The Council of Europe. In: <https://www.turing.ac.uk/research/publications/ai-human-rights-democracy-and-rule-law-primer-prepared-council-europe>

Leslie, D. Understanding artificial intelligence ethics and safety: *A guide for the responsible design and implementation of AI systems in the public sector*. The Alan Turing Institute, 2019. <https://doi.org/10.5281/zenodo.3240529>

Lombardo, Elia. *Intelligenza Artificiale e Human Intelligence per la Prevenzione dei Crimini*. Società Italiana di Intelligence – Socint, 2020. In: https://press.socint.org/index.php/home/catalog/book/2020_07_lombardo

Lombardo, Elia. *Sicurezza 4P. Lo studio alla base del software per prevedere e prevenire i crimini*. Ed. Mazzanti Libri, 2019.

Lombroso, Cesare. *O homem delinqüente*; tradução Sebastião José Roque. Coleção fundamentos de direito. São Paulo, editora Ícone, 2013.

López Cobo, M., Righi, R., Samoil, S., Vázquez-Prada Baillet, M., Cardona, M., and De Prato, G., *AI Watch Index. Policy relevant dimensions to assess Europe's performance in artificial intelligence*, EUR 30681 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-36359-0, doi:10.2760/506611, JRC124424.

Lopes, Álvaro Luiz Primão. Brígido, Edimar Inocência. *Ética e Direito no mundo digital* Tabulæ - Revista de Filosofia - ISSN 1980-0231

Lucena, Pedro Arthur Capelari de. *Policamento preditivo, discriminação algorítmica e racismo*:

potencialidades e reflexos no Brasil. Salvador, 2019. In: <https://lavits.org/wp-content/uploads/2019/12/Lucena-2019-LAVITSS.pdf>

Lyria, Bennett Moses. Janet, Chan. *Algorithmic prediction in policing: assumptions, evaluation, and accountability, Policing and Society*, 28:7, 806-822, In: <https://doi.org/10.1080/10439463.2016.1253695>

Machado, Vinicius Ponte. *Inteligência Artificial*. In http://www.uece.br/computacaoead/index.php/downloads/doc_download/2177-inteligencia-artificial

Magnolo, Stefano; Taurino, Alessandro. *Il Diritto, La Scienza e la Tecnologia*. Editora responsável: Profa. Dra. Fayga Bedê. In <https://orcid.org/0000-0001-6444-2631>

Maranhão, Juliano. *A pesquisa em inteligência artificial e Direito no Brasil*, 2017. In: <https://www.conjur.com.br/2017-dez-09/juliano-maranhao-pesquisa-inteligencia-artificial-direito-pais?imprimir=1>

Martirano di, Valentino Vescio. *Algoritmo e giustizia predittiva in campo penale*. In: <https://www.altalex.com/documents/news/2019/06/14/algoritmo-e-la-giustizia-predittiva-in-campo-penale>

Medvedeva, Masha; Vols, Michel; Wieling, Martijn. *Using machine learning to predict decisions of the European Court of Human Rights*. Artificial Intelligence and Law, 2019. In <https://doi.org/10.1007/s10506-019-09255-y>

Mello, P. *Sul concetto di "intelligenza artificiale" e relativi ambiti applicativi*, cfr. P. Mello, *Intelligenza artificiale*, in <http://disf.org/intelligenza-artificiale> (Documentazione Interdisciplinare di Scienza & Fede), 2002, nonché il saggio di J. Bernstein, *Uomini e macchine intelligenti*, Adelphi, Milano, 2013.

Molina, Antonio García-Pablos; Gomes, Luiz Flávio. *Criminologia: introdução a seus fundamentos teóricos; introdução às bases criminológicas da Lei nº 9.099/95, Lei dos juizados especiais criminais*. 5. ed. São Paulo: Revista dos Tribunais, 2006.

Molinari, Giulia. *La sfida della discriminazione algoritmica nella giustizia di Europa e Stati Uniti. Analytica for intelligence and security studies*. Paper Cyber security. In: <https://www.analyticaintelligenceandsecurity.it/ricerca-e-analisi/la-sfida-della-discriminazione-algoritmica-nella-giustizia-di-europa-e-stati-uniti/>

Moraes, Alexandre Rocha Almeida de Moraes. *Direito penal do inimigo*. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Álvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Penal. Christiano Jorge Santos (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/419/edicao-1/direito-penal-do-inimigo>

Morelli, Claudia. *Processo Penale: operativa la prima applicazione di intelligenza artificiale?* In: <https://www.altalex.com/documents/news/2018/06/18/processo-penale-operativa-la-prima-applicazione-di-intelligenza-artificiale>

Morelli, Claudia. *Intelligenza artificiale nella Giustizia: approvata la Carta Etica Europea*. In: <https://www.altalex.com/documents/leggi/2018/12/04/intelligenza-artificiale-nella-giustizia-carta-etica-europea>

Morelli, Claudia. *Algoritmi e diritti umani: si rischia la collisione (immaginate a danno di chi?)*. In: <https://www.altalex.com/documents/news/2018/07/09/algoritmi-e-impatto-sui-diritti-umani>

Morelli, Claudia. *Furti e rapine: a sventarli ci pensa l'intelligenza artificiale!* 06/06/2019. In: <https://www.altalex.com/documents/news/2019/05/06/polizia-predittiva-intelligenza-artificiale>

Neiva, Laura. *Big Data na Investigação Criminal: Desafios e Expectativas na União Europeia*. Edições Húmus, Lda. e Autora, 2020. In: https://www.cfbdadosadn.pt/Documents/Fundo%20Documental/BigDataInvCriminal_UE.pdf

Nils J. Nilsson. *The quest for artificial intelligence. A history of ideas and achievements*. Cambridge University Press, e-book, 2009.

Nissan, Ephraim. *Computer Applications for Handling Legal Evidence, Police Investigation and Case Argumentation*. Volumes 1 e 2. Editora Springer, 2012.

Novais, Paulo. Freitas, Pedro Miguel. *Inteligência Artificial e regulação de algoritmos*. Universidade do Minho, 2018.

Nuzzo, Antonio. *Algoritmi e regole*. Il Mulino, Rivisteweb, 2019. In: <https://www.rivisteweb.it/doi/10.1433/94543>

Pacheco, César Augusto Rodrigues. Pereira, Natasha Sophie. *Deep Learning Conceitos e Utilização nas Diversas Áreas do Conhecimento*. Revista Ada Lovelace. In <http://anais.unievangelica.edu.br/index.php/lovelace>. v. 2 (2018) jan-dez p. 34-49.

Palmiotto, Francesca. *Giustizia penale e nuove tecnologie. La legislazione penale*. 2020. Captatori Informatici e Diritto alla Difesa: Il Caso Exodus. In <http://www.lalegislationepenale.eu/wp-content/uploads/2020/10/Palmiotto-Revisione-Finale.pdf>

Parodi, Cesare; Sellaroli, Valentina. *Sistema Penale e Intelligenza Artificiale: Molte Speranze e Qualche Equivoco*. in Dir. pen. cont., fasc. 1/2017. In: <https://archiviodpc.dirittopenaleuomo.org/upload/6695-parodisellaroli2019a.pdf>

Palm, Rasmus Berg. *Prediction as a candidate for learning deep hierarchical models of data*. Kongens Lyngby 2012, DTU-Informatic-Msc. -2012. In: <https://www2.imm.dtu.dk/pubdb/edoc/imm6284.pdf>

Patterson, Josh. Gibson, Adam. *Deep Learning a Practitioner's Approach*. Ed. O'Reilly Media, Inc., E-book, 2017.

Pereira, Jorge Luis. *Análise Preditiva em Sistemas de Informação no Contexto do Big Data*. Marília, 2014. In:

<https://aberto.univem.edu.br/bitstream/handle/11077/1003/Jorge%20Lu%c3%ads%20Pereira.pdf?sequence=1&isAllowed=y>

Pérez Estrada, Miren Josune. *La inteligencia artificial como prueba científica en el proceso penal español*. In: <https://revista.ibraspp.com.br/RBDPP/article/view/505>

Perry, Walter L. McInnis, Brian. Price, Carter C. Smith, Susan C. Hollywood, John S. *Predictive policing. The Role of Crime Forecasting in Law Enforcement Operations*. National Institute of Justice, 2013. In: https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf

Perrucci, Antonio. *Dai Big Data all'ecosistema digitale. Dinamiche tecnologiche e di mercato e ruolo delle politiche pubbliche*. Il Mulino, Rivisteweb, 2019. In: <https://www.rivisteweb.it/doi/10.1433/94545>

Pezzoli, Andrea; Tonazzi, Alessandra. *Discriminazione e collusione tacita tra lessico, intelligenza artificiale e algoritmi*. Il Mulino, Rivisteweb, 2019. In: <https://www.rivisteweb.it/doi/10.1433/94552>

Piccoli, Donato; Lombardo, Elia; Bettoni, Raffaella. *Il modello predittivo XLAW correla i crimini con la configurazione fisica della città: urbanistica e informazione INU edizione*. In: <https://www.sicurezza4p.it/blog/index.asp?Q=NA6V4HA8990G544IV789>

Pittelli, Teresa. *Intelligenza Artificiale, proteggere non solo privacy ma anche libero arbitrio*. In: <https://www.altalex.com/documents/news/2019/03/18/intelligenza-artificiale-privacy-libero-arbitrio>

Poole, David L. Mackworth, Alan K. *Artificial Intelligence: Foundations of Computational Agents*. Cambridge University Press, e-book, New York, 2010.

Polidoro, Donato. Tecnologie informatiche e procedimento penale: la giustizia penale “messa alla prova” dall’intelligenza artificiale. In <https://archiviopenale.it/tecnologie-informatiche-e-procedimento-penale-la-giustizia-penale-messa-alla-prova-dallintelligenza-artificiale/articoli/25993>

Quarta, Elena. *Giustizia e predizione: l'algoritmo che legge il futuro*. In: <https://www.giustiziainsieme.it/it/cultura-e-societa/600-giustizia-e-predizione-l-algoritmo-che-legge-il-futuro?tmpl=component&print=1&layout=def%E2%80%A6>

Quattrocolo, Serena. *Intelligenza Artificiale e Giustizia: Nella Cornice della Carta Etica Europea, gli Spunti per un'urgente Discussione tra Scienze Penali e Informatiche*. In: <http://www.lalegislazionepenale.eu/intelligenza-artificiale-e-giustizia-nella-cornice-della-carta-etica-europea-gli-spunti-per-unurgente-discussione-tra-scienze-penali-e-informatiche-serena-quattrocolo/>

Renda, Andrea. *Artificial Intelligence Ethics, governance and policy. Challenges Report of a CEPS Task Force*. Centre for European Policy Studies (CEPS), Brussels, 2019. In: <https://ec.europa.eu/jrc/communities/en/node/1286/document/artificial-intelligence-ethics-governance-and-policy-challenges>

Rulli, Edoardo. *Giustizia predittiva, intelligenza artificiale e modelli probabilistici. Chi ha paura degli algoritmi?* Il Mulino - Rivisteweb, 2018. In: <https://www.rivisteweb.it/doi/10.1433/92116>

Russel, Stuart J; Norvig, Peter. *Artificial Intelligence a Modern Approach*. Third Edition. E-Book, 2010.

Saisse, Renan. *Big data contra o crime: efeito minority report*. In <http://direitoeti.com.br/artigos/big-data-contra-o-crime-efeito-minority-report/>

Santos, Murilo Alves. Souza, Daniel Henrique Silva de. Penedo, Antonio Sergio Torres. Martins, Elvis Silveira. *Aplicação de redes neuronais no Brasil: um estudo bibliométrico*. Biblionline, João Pessoa, v. 12, n. 2, p. 101 – 116, 2016. In: https://www.researchgate.net/publication/303957049_APLICACAO_DE_REDES_NEURONAIIS_NO_BRASIL_UM_ESTUDO_BIBLIOMETRICO

Sartor, Giovanni. Lagioia, Francesca. *AI Systems Under Criminal Law: A Legal Analysis and a Regulatory Perspective*, 2019. <https://link.springer.com/article/10.1007/s13347-019-00362-x>

Sartor, Giovanni. *Legal validity: an Inferential analysis*. European University Departament of Law, 2007. In https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1024106

Sartor, Giovanni. *Corso di Informatica giuridica. L'informatica giuridica e le tecnologie dell'informazione*. 2nd. Giappichelli, 2010.

Sartor, Giovanni. *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*. In: [https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU\(2020\)641530](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)641530)

Sassi, Silvia. *Gli algoritmi nelle decisioni pubbliche tra trasparenza e Responsabilità*. Il Mulino - Rivisteweb, 2019. In: <https://www.rivisteweb.it/doi/10.1433/94547>

Schlehahn, Eva. Aichroth, Patrick. Mann, Sebastian. Schreiner, Rudolf. Shepherd, Ifan. Wong, B.L. William. *Benefits and Pitfalls of Predictive Policing*. In: https://www.researchgate.net/profile/Bl-Wong/publication/304293638_Benefits_and_Pitfalls_of_Predictive_Policing/links/582ae60308aef19cb8062095/Benefits-and-Pitfalls-of-Predictive-Policing.pdf

Simões-Gomes, Leticia. Roberto, Enrico. Mendonça, Jônatas. *Viés algorítmico – um balanço provisório*. Estud. sociol. Araraquara v.25 n.48 p.139-166 jan. - jun. 2020. In: <https://nev.prp.usp.br/wp-content/uploads/2020/08/13402-42914-1-PB.pdf>

Simmler, Monika. Canova, Giulia. *The rise of algorithms in the criminal justice system*. In: <https://blog.ai-laws.org/the-rise-of-algorithms-in-the-criminal-justice-system/?cn-reloaded=1&cn-reloaded=1>

Theben, Alexandra. Gunderson, Laura. López-Forés, Laura. Misuraca, Gianluca. Lupiáñez-Villanueva, Francisco. *Challenges and limits of an open-source approach to Artificial Intelligence*. Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for

Internal Policies, 2021. In:
[https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662908/IPOL_STU\(2021\)662908_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662908/IPOL_STU(2021)662908_EN.pdf)

Traversi, Alessandro. *Intelligenza artificiale e giustizia, verso un giudice robot?* Altalex, 19 marzo 2019. In: <https://www.altalex.com/documents/news/2019/03/19/intelligenza-artificiale-e-giustizia-giudice-robot>

Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias. Technical Paper. Australian Human Rights Commission 2020. In: <https://humanrights.gov.au/our-work/rights-and-freedoms/publications/using-artificial-intelligence-make-decisions-addressing>

Van Brakel, Rosamunde. De Hert, Paul. *Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies*. Cahiers Politiestudies Jaargang 2011-3, nr. 20 p. 163-192. In: https://www.researchgate.net/publication/233831922_Policing_surveillance_and_law_in_a_pre-crime_society_Understanding_the_consequences_of_technology_based_strategies

Veale, Michael. *Algorithms in the Criminal Justice System*, v 1 The Law Society of England and Wales, 2019. In: <https://www.ailir.com/wp-content/uploads/2019/06/algorithms-in-criminal-justice-system-report-2019.pdf>

Verlag, Helbing Lichtenhahn. Simmler, Monika (Hrsg.). *Smart Criminal Justice - Der Einsatz von Algorithmen in der Polizeiarbeit und Strafrechtspflege*. Basilea, 2021. In: <https://www.helbing.ch/annotstream/9783719043971/PDF/Smart-Criminal-Justice.pdf?sq=27>

Wenin, Roberto. Fornasari, Gabriele. *Diritto Penale e Modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*. Università degli Studi di Trento. Quaderni della Facoltà di Giurisprudenza, 2017. In: <https://archiviodpc.dirittopenaleuomo.org/d/5492-diritto-penale-e-modernita-le-nuove-sfide-tra-terrorismo-sviluppo-tecnologico-e-garanzie-fondamenta>

West, S.M., Whittaker, M. and Crawford, K. (2019). *Discriminating Systems: Gender, Race and Power in AI*. AI Now Institute. In: <https://ainowinstitute.org/discriminatingystems.html>.

Yavuz, Can. *Machine Bias: Artificial Intelligence and Discrimination*. Faculty of Law. Lund University, 2019. In: https://www.researchgate.net/publication/334721591_Machine_Bias_Artificial_Intelligence_and_Discrimination

Yeung, Karen. *A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework*. Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence, 2019. In: <https://rm.coe.int/draft-study-of-the-implications-of-advanced-digital-technologies-inclu/16808ef255>

Relatórios

Agencia Española de Protección datos. *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*. Feb 2020. In: <https://www.aepd.es/es/media/guias/adequacion-rgpd-ia.pdf>

Algorithms in the Criminal Justice System. The Law Society of England and Wales, 2019. In: <https://www.ailir.com/wp-content/uploads/2019/06/algorithms-in-criminal-justice-system-report-2019.pdf>

AI Portugal 2030. *Portuguese National Initiative on Digital Skills. An innovation and growth strategy to foster Artificial Intelligence in Portugal in the European*. In: https://www.incode2030.gov.pt/sitios/default/files/julho_incode_brochura.pdf

Artificial Intelligence and Data Protection. *How the GDPR Regulates AI Centre for Information Policy Leadership (CIPL)*. March 2020. In: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf

Artificial intelligence and privacy Report, January 2018. *The Norwegian Data Protection Authority*. In: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>

Artificial Intelligence and Law Enforcement Impact on Fundamental Rights. European Parliament, July 2020. In: <https://op.europa.eu/en/publication-detail/-/publication/97fcdc04-01a3-11eb-974f-01aa75ed71a1>

Borgesius, Frederik Zuiderveen. Discrimination, artificial intelligence, and algorithmic decision-making. Council of Europe, 2018. In: <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73>

Carta ética europeia para a utilização de inteligência artificial nos sistemas de justiça e ambientes relacionados. In <https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0>

Carta Portuguesa de Direitos Humanos na Era Digital. Lei n.º 27/2021 <https://data.dre.pt/eli/lei/27/2021/05/17/p/dre>

Código Penal. Decreto-Lei n.º 48/95 - Diário da República n.º 63/1995

Comissão Europeia para a eficácia da Justiça (CEPEJ). *Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seu ambiente, 2018*. In <https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0>

Communication from the Commission to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions Fostering a European approach to Artificial Intelligence. European Commission, Brussels, 21.4.2021. In: <https://op.europa.eu/en/publication-detail/-/publication/01ff45fa-a375-11eb-9585-01aa75ed71a1/language-en>

Communication From the Commission to The European Parliament, The European Council, The Council, *The European Economic and Social Committee and The Committee of The Regions Coordinated Plan on Artificial Intelligence*. Brussels, 2018. In: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:795:FIN>

Consultative Committee of the Convention for the Protection of individuals with regard to Automatic Processing of Personal Data. Convention 108. Council of Europe, 28 January 2021. In: <https://www.coe.int/en/web/data-protection>

Conselho Europeu de Proteção de Dados. In: https://edpb.europa.eu/sitios/edpb/files/file1/edpb_letter_out2020_0004_intveldaalgorithmms_en.pdf

Council of Europe. *Algorithms and Human Rights Study on the human rights dimensions of automated data processing techniques and possible regulatory implications, 2018*. In <https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html>

Council of Europe. *Guidelines on Artificial Intelligence and Data Protection*. In: <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8>

Council of Europe. *Report on Artificial Intelligence. Artificial Intelligence and Data Protection: Challenges and Possible Remedies*. Report by Alessandro Mantelero. In <https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6>

Council of Europe. *Discrimination, artificial intelligence, and algorithmic decision-making*. Study by Zuiderveen Borgesius, 2018, In <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73>

Diretrizes do Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial, criado pela Comissão Europeia em Junho de 2018. In: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>

EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) 18 June 2021. In: https://edpb.europa.eu/our-work-tools/our-documents/edpbbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_cs

EU guidelines on ethics in artificial intelligence: Context and implementation. In [https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI\(2019\)640163](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2019)640163)

European Parliament. <https://www.europarl.europa.eu/about-parliament/pt/democracy-and-human-rights/fundamental-rights-in-the-eu>

European Ethical Charter. *Use of Artificial Intelligence in Judicial Systems and their environment*. CEPEJ during its 31st Plenary meeting (Strasbourg, 3-4/12/2018).

European Group. *Ethics in Science and New Technologies, Statement on Artificial Intelligence, Robotics and "Autonomous" Systems*, Brussels, March 9, 2018, In: https://ec.europa.eu/info/news/ethics-artificial-intelligence-statement-ege-released-2018-apr-24_en.

Feasibility Study. Ad Hoc Committee on Artificial Intelligence (CAHAI). Strasbourg, 17 December 2020. In: <https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da>

Fuster, Prof. Dr. Gloria González. *Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights*. European Parliament's Committee on Civil Liberties, Justice and Home Affairs. In: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU\(2020\)656295_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf)

FW2050 – Images of the Future Worlds Facing the Legal Profession 2020-2030. The Law Society. In: <https://www.lawsociety.org.uk/topics/research/future-worlds-2050-images-of-the-future-worlds-facing-the-legal-profession-2020-2030>

Getting the Future Right. *Artificial Intelligence and Fundamental Rights*. Luxembourg: Publications Office of the European Union, 2020. In: https://fra.europa.eu/sitios/default/files/fra_uploads/fra-2020-artificial-intelligence_en.pdf

Guidelines 4/2019 on Article 25. Data Protection by Design and by Default. In: https://edpb.europa.eu/sitios/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

How Can Humans Keep the Upper Hand? The ethical matters raised by algorithms and artificial intelligence. Report on the Public Debate Led by the French Data Protection Authority (CNIL) as Part of the Ethical Discussion Assignment set by the Digital Republic Bill. December 2017. In: https://www.cnil.fr/sitios/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf

Loomis v. Wisconsin. In <https://www.scotusblog.com/case-files/cases/loomis-v-wisconsin/>

Madiega, Tambiama. *EU guidelines on ethics in artificial intelligence: Context and implementation*. European Parliamentary Research Service, September 2019. In: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI\(2019\)640163_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf)

Preventing unlawful profiling today and in the future: a guide. European Union Agency for Fundamental Rights. Luxembourg: Publications Office of the European Union, 2018. In: <https://lib.ugent.be/en/catalog/rug01:002822492>

Possible introduction of a mechanism for certifying artificial intelligence tools and services in the sphere of justice and the judiciary: Feasibility Study. European Commission for the Efficiency of Justice (CEPEJ), 8 December 2020. In: <https://rm.coe.int/feasability-study-en-cepej-2020-15/1680a0adf4>

Recommendation CM/Rec (2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. (Adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies). In: <https://rm.coe.int/09000016809e1154>

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27/04/2016. In: [https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%](https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679&from=PT)

Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho de 14/11/2018. In: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018R1807&from=PT>

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. European Commission, Brussels, 21.4.2021. In: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>

Relatório da Comissão ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social Europeu. Relatório sobre as implicações em matéria de segurança e de responsabilidade decorrentes da inteligência artificial, da Internet das coisas e da robótica. Comissão Europeia, Bruxelas, 2020. In: <https://op.europa.eu/es/publication-detail/-/publication/4ce205b8-53d2-11ea-aece-01aa75ed71a1/language-pt/format-PDF>

Resolução do Parlamento Europeu, de 6 de outubro de 2021, sobre a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais. In: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_PT.html

Special Collection on Artificial Intelligence. United Nations Interregional Crime and Justice Research Institute (UNICRI), 2020. In: <http://www.unicri.it/News/Artificial%20Intelligence%20Collection>

Study on The Human Rights Dimensions of Automated Data Processing Techniques (In Particular Algorithms) And Possible Regulatory Implications. Committee Of Experts on Internet Intermediaries (MSI-Net), 2017. In: <https://rm.coe.int/study-hr-dimension-of-automated-data-processing-incl-algorithms/168075b94a>

The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. In: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf)

The AI Index 2021 Annual Report by Stanford University. In: <https://aiindex.stanford.edu/report/>

The use of predictive analysis in spatiotemporal crime forecasting: Building and testing a model in an urban context. In:

Towards Regulation of AI Systems. Global perspectives on the development of a legal framework on Artificial Intelligence systems based on the Council of Europe's standards on human rights, democracy, and the rule of law. Compilation of contributions prepared by the CAHAI Secretariat, December 2020. In: <https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a>

White Paper on Artificial Intelligence: A European approach to excellence and trust 19 February 2020. In https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

Websítios

<https://paginas.fe.up.pt/~lpreis/ai2002/Documents/1.Agentes.PDF>

<https://pt.khanacademy.org/science/biology/human-biology/neuron-nervous-system/a/overview-of-neuron-structure-and-function>

<https://blog.hdstore.com.br/o-que-e-o-tensorflow/>

<https://medium.com/data-hackers/deep-learning-do-conceito-%C3%A0s-aplica%C3%A7%C3%B5es-e8e91a7c7eaf>

<https://mc.ai/deep-learning-series-chapter-1-introduction-to-deep-learning/>

<https://gaea.com.br/afinal-o-que-e-deep-learning/>

<https://mc.ai/deep-learning-series-chapter-1-introduction-to-deep-learning>

<https://www.gartner.com/en/information-technology/glossary/big-data>

<https://www.voitto.com.br/blog/artigo/data-mining>

<http://curia.europa.eu/juris/documents.jsf?num=C-623/17>

https://ec.europa.eu/knowledge4policy/ai-watch_en

https://www.europarl.europa.eu/doceo/document/B-9-2020-0189_PT.html

https://edpb.europa.eu/sitios/edpb/files/files/file1/edpb_letter_out2020_0004_intveldaalgorithm_en.pdf

<https://www.europarl.europa.eu/about-parliament/pt/democracy-and-human-rights/fundamental-rights-in-the-eu>

<https://www.xlaw.it/presentazione/>

<https://www.tpi.it/tecnologia/xlaw-algoritmo-prevede-furti-rapine-20190730383409>

<https://www.smau.it/casi-di-successo/xlaw-lalgoritmo-poliziotto-che-prevede-furti-e-rapine>

<https://www.sicurezza4p.it/blog/index.asp?Q=HD1Q56756E0EG2PNB79N>

<https://www.mathworks.com/discovery/machine-learning.html>

<https://www.mckinsey.com/featured-insights/artificial-intelligence/tackling-bias-in-artificial-intelligence-and-in-humans>

http://www.cristiancechinel.pro.br/my_files/algorithms/bookhtml/node15.html

<https://www.europarl.europa.eu/news/pt/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance>

<https://www.riskmanagement360.it/analisti-ed-esperti/intelligenza-artificiale-e-processo-penale-un-vuoto-normativo-da-colmare/>

https://www.researchgate.net/publication/317718776_The_use_of_predictive_analysis_in_spatiotemporal_crime_forecasting_Building_and_testing_a_model_in_an_urban_context