Universidade de Brasília
Faculdade de Direito

MARCELLE MARTINS LEMES

# INTELIGÊNCIA ARTIFICIAL, ALGORITMOS E POLICIAMENTO PREDITIVO NO PODER PÚBLICO FEDERAL BRASILEIRO

Brasília – DF
2019

MARCELLE MARTINS LEMES

# INTELIGÊNCIA ARTIFICIAL, ALGORITMOS E POLICIAMENTO PREDITIVO NO PODER PÚBLICO FEDERAL BRASILEIRO

Monografia apresentada ao Programa de Graduação da Faculdade de Direito da Universidade de Brasília como requisito à obtenção do título de Bacharel em Direito.

Professora Orientadora: Dra. Christiana Soares de Freitas

Brasília – DF
2019

MARCELLE MARTINS LEMES

# INTELIGÊNCIA ARTIFICIAL, ALGORITMOS E POLICIAMENTO PREDITIVO NO PODER PÚBLICO FEDERAL BRASILEIRO

A Comissão Examinadora, abaixo identificada, aprova o Trabalho de Conclusão do Curso de Direito da Universidade de Brasília da aluna

**Marcelle Martins Lemes**

Dra. Christiana Soares de Freitas
Professora-Orientadora

Dr° Alexandre Kehrig Veronese Aguiar
Professor-Examinador 1

Dr° Daniel Pitangueira de Avelino
Professor-Examinador 2

Brasília, 3 de dezembro de 2019

À minha mãe, Thelma, que me inspira todos os dias a me tornar uma versão melhor e mais bondosa de mim mesma, ao meu pai, Sérgio, e à querida família. Em memória dos meus queridos avós, Dona Zilá e Seu Carneiro: sem vocês, nada disso seria possível.

# AGRADECIMENTOS

À Profa. Dra. Christiana Freitas pelos incontáveis conselhos e orientações, pela paciência, dedicação e confiança no meu trabalho. Você me inspira a ser uma pesquisadora cada vez melhor. À Amanda Espiñeira e à Edilenice Passos, minhas queridas leitoras, e a Leonardo Simi e Nathan Simões, meus queridos leitores, pelas preciosas sugestões e atenciosos comentários. A Égon Rafael, às amigas e aos amigos da Fiocruz e da DPU pelas frutíferas discussões, contribuições e incentivo.

"*As a society, we are now at a crucial juncture in determining how to deploy AI-based technologies in ways that promote, not hinder, democratic values such as freedom, equality and transparency.*"

(STONE et al., 2016)

# RESUMO

O surgimento das tecnologias de informação, com o uso de *big data* pelos governos e pelas empresas, e com o desenvolvimento de sistemas algorítmicos e de inteligência artificial, sinalizaram o início de uma nova etapa no capitalismo: o *Capitalismo de Vigilância*. Em face disso, procurou-se verificar de que maneira o poder público brasileiro se situa em relação às iniciativas algorítmicas e de inteligência artificial (IA). Foi realizada revisão bibliográfica em paralelo com pesquisa exploratória, a partir do levantamento de dados, nos endereços eletrônicos dos Ministérios e de órgãos públicos, utilizando argumentos booleanos nas ferramentas de pesquisa do Google. Os resultados encontrados foram analisados e as iniciativas de tecnologia da informação foram tabeladas e seus dados registrados. Entretanto, a falta de um registro oficial e central dos sistemas implementados impediu a realização de uma exploração rigorosamente quantitativa. Tendo em vista o número elevado de iniciativas mapeadas, se decidiu por estudar o projeto *Sinesp Big Data e Inteligência Artificial para Segurança Pública*, desenvolvido pelo Ministério da Justiça e Segurança Pública (MJSP) em parceria com o Departamento de Computação da Universidade Federal do Ceará (UFC). Essa escolha foi motivada pelos objetivos do projeto e por sua atuação orientarem à prática de policiamento preditivo. Foram encontradas escassas informações públicas sobre o *Sinesp Big Data*, em razão do que, encaminhou-se comunicações eletrônicas aos responsáveis pelo projeto, e solicitações de acesso à informação, amparadas pela Lei n° 12.527/11 (Lei de Acesso à Informação) ao MJSP e à UFC. Foram recebidas respostas vagas aos questionamentos formulados, bem como negativa de contribuição em face de acordos de confidencialidade. Apesar disso, foi possível identificar que o desenvolvimento do projeto se vincula diretamente à Lei 13.675/18 (Lei do Sistema Único de Segurança Pública) e aos sistemas de inteligência policial implementados pelo Governo do Ceará. Considerando os dados levantados e utilizando categorias teóricas de Foucault, Deleuze e Zuboff, bem como estudos de governança ética das tecnologias informacionais, foi possível identificar o forte traço disciplinar do *Sinesp Big Data*, que, entende-se, realizará uma governança disciplinar de indivíduos de risco, identificando-se com a figura do polipanóptico e apresentando-se como um sistema *black box* com prováveis efeitos discriminatórios.

Palavras-chave: Inteligência Artificial; Algoritmos; Vigilância; Segurança Pública; SINESP.

# ABSTRACT

The emergence of information technologies, with the use of big data by governments and companies, and with the development of algorithmic and artificial intelligence systems, signaled the beginning of a new stage in capitalism: Surveillance Capitalism. In view of this, we sought to verify how the Brazilian government is situated in relation to algorithmic and artificial intelligence (AI) initiatives. A parallel bibliographic review was carried out with exploratory research, based on data collection, in the electronic addresses of the Ministries and public agencies, using Boolean arguments in Google's search tools. The results found were analyzed and the information technology initiatives were tabulated and their data registered. However, the lack of an official and central registry of the systems implemented prevented a strictly quantitative exploration. In view of the large number of initiatives mapped, it was decided to study the Sinesp Big Data and Artificial Intelligence for Public Security project, developed by the Ministry of Justice and Public Security (MJSP) in partnership with the Computer Department of the Federal University of Ceará (UFC). This choice was motivated by the objectives of the project and by its operation to guide the practice of predictive policing. There was scarce public information about Sinesp Big Data, due to which, electronic communications were sent to those responsible for the project, and requests for access to information, supported by Law No. 12.527/11 (Law on Access to Information) to the MJSP and the UFC. Vague answers were received to the questions raised, as well as a negative contribution under confidentiality agreements. Nevertheless, it was possible to identify that the development of the project is directly linked to Law 13.675/18 (Law of the Unified Public Security System) and to the police intelligence systems implemented by the Government of Ceará. Considering the data collected and using the theoretical categories of Foucault, Deleuze and Zuboff, as well as studies on the ethical governance of information technologies, it was possible to identify the strong disciplinary trait of Sinesp Big Data, which, it is understood, will perform a disciplinary governance of individuals at risk, identifying itself with the polypanoid figure and presenting itself as a black box system with likely discriminatory effects.

Keywords: Artificial Intelligence; Algorithms; Surveillance; Public Security; SINESP.

# LISTA DE QUADROS

# LISTA DE ABREVIATURAS E SIGLAS

AI – *Artificial Intelligence*

CADE - Conselho Administrativo de Defesa Econômica

CNJ - Conselho Nacional de Justiça

COMPAS - *Correctional Offender Management Profiling for Alternative Sanctions*

DGI - Diretoria de Gestão e Integração de Informações

DTIC- Diretoria de Tecnologia da Informação e Comunicação

EUA – Estados Unidos da América

IA – Inteligência Artificial

ICDPPC - Conferência Internacional dos Delegados para a Proteção de Dados e Privacidade

LGPD - Lei Geral de Proteção de Dados do Brasil

MJSP - Ministério da Justiça e Segurança Pública

NESP - Nova Estratégia de Segurança Pública

PNSDPS - Plano Nacional de Segurança Pública e Defesa Social

SENASP - Secretaria Nacional de Segurança Pública

SINESP - Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas

SUSP - Sistema Único de Segurança Pública

UFC - Universidade Federal do Ceará

# SUMÁRIO

# INTRODUÇÃO

A presente pesquisa dedicou-se à análise do projeto *Sinesp Big Data e Inteligência Artificial para Segurança Pública*, bem como, de maneira ampla, dos sistemas de vigilância e de policiamento preditivo existentes no mundo, não apenas no governo brasileiro. O interesse pelo tema foi motivado pela crescente utilização das tecnologias digitais pelo setor público, com suas implicações éticas, políticas e democráticas.

Os avanços na Ciência e na Engenharia da Computação possibilitaram o desenvolvimento das tecnologias de informação, que impactaram e permanecem impactando profundamente as lógicas social, política, econômica. Nesse contexto, observou-se o surgimento do "texto eletrônico" e do trabalho "mediado por computadores" (ZUBOFF, 2015, p. 77)[1].

Essas inovações tecnológicas, juntamente com a ampliação da capacidade de armazenamento, de prospecção e de análise de dados, tiveram sua expressão organizada pela lógica de acumulação[2] do capitalismo de vigilância, "do qual '*big data*' é uma condição e uma expressão[3]" (ZUBOFF, 2015, p. 76-77). Nessa "civilização informacional", os mecanismos de subjetivação, de disciplina e de controle, bem como a relação com a própria democracia são transformados[4].

Como exemplos dos novos mecanismos de extração e controle, vejam-se o *Correctional Offender Management Profiling for Alternative Sanctions* (COMPAS) – sistema desenvolvido para avaliar o risco à reincidência de réus em processos criminais nos Estados Unidos da América (EUA)[5] –, e o *PredPol* – *software* norte-americano de policiamento

---

[1] Sobre isso, Zuboff (2015, p. 77) escreve: "As a result of pervasive computer mediation, nearly every aspect of the world is rendered in a new symbolic dimension of as events, objects, processes, and people become visible, knowable, and shareable in a new way. The world is reborn as data and the electronic text is universal in scale and scope".

[1] Zuboff escreve que "The logic of accumulation produces its own social relations and with that its conceptions and uses of authority and power."

[2] Zuboff escreve que "The logic of accumulation produces its own social relations and with that its conceptions and uses of authority and power." (2015, p.77).

[3] Tradução livre. No original: "[...] the wider logic of accumulation I call surveillance capitalism, of which '*big data*' is both a condition and an expression".

[4] Cf. em Zuboff (2015, p. 85–86): "Under surveillance capitalism, democracy no longer functions as a means to prosperity; democracy threatens surveillance revenues".

[5] Cf. EQUIVANT. **Do Risk Assessments Have a Place in Pretrial?**, 2019. Disponível em: <https://www.equivant.com/do-risk-assessments-have-a-place-in-pretrial/>. Acesso em: 27 out. 2019. (No endereço eletrônico, é possível verificar comentário da companhia responsável pelo COMPAS quanto ao uso de *risk assessment tools*: "[...] How can we possibly know enough about that person to make the right decision? How can we predict individual behavior? How can we know what the specific risks are? (…) Using a simple risk assessment with a few short questions, validated assessments can predict the level of risk an individual has related to re-offending or failing to appear on his or her court appointed date. The risk level associated to a

preditivo, desenhado para prever a localização geográfica de futuras ocorrências criminais e, com isso, auxiliar na alocação de oficiais de polícia em trabalho de campo[6].

Ainda, a título exemplificativo, observou-se a criação de sistemas voltados à análise de perfis de consumo de usuários de redes sociais; à seleção de candidatos a vagas de emprego; à produção de escalas de trabalho; e ao ranqueamento de universidades segundo critérios específicos[7].

Em face disso, e considerando os encadeamentos éticos e políticos da inteligência artificial e dos sistemas algorítmicos, viu-se como relevante o esforço de compreender o cenário brasileiro no tema. Assim, a presente pesquisa partiu do empenho inicial de se verificar o grau de envolvimento do governo federal no sentido de posicionar o País no novo contexto técnico-informacional.

Partiu-se, para tanto, da percepção de que se revestia de grande importância acompanhar a maneira como a experiência brasileira com as tecnologias algorítmicas e de IA tem se desenvolvido e por quais parâmetros tem se orientado. Em face disso, objetivou-se a criação de um banco de dados em que estivessem registradas as iniciativas artificialmente inteligentes em curso e em que fossem anotadas as informações relativas aos objetivos, à aplicação e à autoridade que as estivesse empreendendo. Isso permitiu contabilizar mais de 90 projetos[8] de diversas áreas[9].

---

person is **one piece of data** that can help decision-makers balance individual rights with public safety. As with all critical decisions, risk assessments are *not* the "be all, end all" solution, they should be fit into the overall decision making framework adopted by the justice agencies. Too often, this critical factor is overlooked. The framework itself is needed to drive what the agency does from start to finish; a risk assessment is not intended to replace a judicial decision-maker" (grifos no original)).

[6] Cf. **PredPol Mission | About Us | Aiming to reduce victimization keep communities safer**. [s.d.]. Disponível em: <https://www.predpol.com/about/>. Acesso em: 27 out. 2019. (No endereço eletrônico, é possível ter acesso à apresentação do *software*: "PredPol has a precise definition of predictive policing. For us and our customers, **it is the practice of identifying the times and locations where specific crimes are most likely to occur, then patrolling those areas to prevent those crimes from occurring**. Put simply, our mission is to help law enforcement keep communities safer by reducing victimization. **Our day-to-day operations tool identifies where and when crime is most likely to occur, enabling you to effectively allocate your resources and prevent crime**" (grifo nosso)).

[7] Cf. O'NEIL, Cathy. **Weapons of Math Destruction: How *Big data* Increases Inequality and Threatens Democracy**. Nova Iorque, Estados Unidos da América: Crown, 2016, (a autora explora casos em que sistemas algorítmicos foram empregados nos Estados Unidos, afetando negativamente muitos dos indivíduos a eles submetidos).

[8] Lista completa disponível no Apêndice [Digital] A.

[9] Observou-se, ainda, que o governo brasileiro tem dedicado esforços para avançar a agenda digital do País em iniciativas outras que não só o desenvolvimento de sistemas artificialmente inteligentes. Veja-se, por exemplo, o **Decreto nº 8.638, de 15 de janeiro de 2016**, que estabeleceu a *Política de Governança Digital*, destinada aos órgãos e entidades da administração pública federal direta, autárquica e fundacional; a **Portaria nº 68, de 7 de março de 2016**, que aprovou a *Estratégia de Governança Digital da Administração Pública Federal* para os anos de 2016 a 2019; e a **Portaria nº 107, de 02 de maio de 2018**, que revisou a estratégia e que atribuiu à Secretaria de Tecnologia da Informação e Comunicação a competência determinada na portaria. Veja-se, ainda, a **Estratégia Brasileira para a Transformação Digital (E-Digital),** publicada, em 2018, pelo Ministério da

A partir do exposto, e sabendo dos desafios democráticos e políticos advindos da nova lógica de acumulação, com seus mecanismos disciplinadores e seu controle sobre as subjetividades, vislumbrou-se na segurança pública um campo de estudo particularmente sensível, em especial frente às técnicas de policiamento preditivo. À vista disso, e a partir da identificação do projeto *Sinesp Big Data e Inteligência Artificial para Segurança Pública*, desenvolvido pelo Ministério da Justiça e da Segurança Pública (MJSP) em parceria com o Departamento de Computação da Universidade Federal do Ceará (UFC), delimitou-se nele o recorte do trabalho em tela.

Assim, o objetivo geral foi analisar o projeto a partir de enquadramentos éticos e tecnopolíticos, buscando situá-lo em relação ao *Capitalismo de Vigilância* e às lógicas de disciplina e de controle ligadas à vigilância e ao policiamento preditivo. Pretendeu-se, com isso, enquanto objetivos específicos, (1) analisar as características do *Sinesp Big Data e IA* em face das noções de governança algorítmica e de IA, e (2) ponderar suas implicações tecnopolíticas, segundo o pensamento de Michel Foucault e de Gilles Deleuze com vistas a identificar eventuais pontos críticos do projeto em relação à democracia e à proteção de direitos.

Com isso, tencionou-se contribuir com a agenda de pesquisa em IA e sistemas algorítmicos na América Latina e no mundo, no esforço de ampliar a compreensão do cenário tecnopolítico. Em adição, ao mapear as iniciativas em curso do governo brasileiro, objetivou-se gerar dados para possíveis explorações futuras.

O trabalho foi estruturado de forma que, no capítulo 1 trata-se da governança da IA, introduzindo conceitos de base para a análise do tema e discorrendo sobre os enquadramentos éticos e jurídicos aplicáveis. No capítulo 2, são revisitadas categorias teóricas foucaultianas e deleuzianas, utilizando-as para discorrer sobre *Capitalismo de Vigilância* e sobre policiamento preditivo. Por fim, no capítulo 3, são analisados e discutidos os resultados obtidos quanto ao projeto *Sinesp Big Data*.

---

Ciência, Tecnologia, Inovações e Comunicações, *se propondo a explicitar os desafios enfrentados, e a estabelecer ações estratégicas e indicadores para monitorar o progresso das metas digitais*.

# 1 GOVERNANÇA DA INTELIGÊNCIA ARTIFICIAL

Existem potenciais efeitos negativos que a tecnologia inteligente pode gerar para a democracia. Experiências prévias revelam que múltiplos fatores podem contribuir para gerar *outputs* com erros e distorções, reproduzindo desigualdades e gerando injustiças[10].

Neste capítulo, a fim de melhor compreender os desafios a que estão sujeitos os sistemas de IA, debruçou-se sobre a tecnologia[11], a ética e o direito, tidos como forças motrizes da governança algorítmica[12] (CATH, 2018). Para tanto, e considerando a complexidade e a amplitude do conceito de governança, referencia-se as principais proposições teóricas sobre o tema, sintetizadas por Yu Keping (2018) na lista a seguir:

> 1. A governança refere-se a um conjunto de instituições e atores que são extraídos de, mas também para além do governo. Desafia a autoridade do Estado ou do governo no sentido tradicional e sustenta que o governo não é o único centro de poder de um Estado. Desde que o poder exercido por uma instituição pública ou privada seja reconhecido pelo público, é possível tornar-se um centro de poder a um nível específico.
> 2. A governança identifica a indefinição de fronteiras e responsabilidades para lidar com questões sociais e econômicas. Indica que, na sociedade moderna, o Estado está transferindo suas responsabilidades, outrora exclusivas, para a sociedade civil (ou seja, organizações do setor privado e grupos voluntários, estão assumindo cada vez mais responsabilidades que antes estavam nas mãos do Estado). Como resultado, as fronteiras entre o Estado e a sociedade e entre os setores público e privado estão cada vez mais tênues, assim como as definições de suas responsabilidades.
> 3. A governança identifica a dependência de poder envolvida nas relações entre as instituições vinculadas à ação coletiva. Para ser específico, toda organização dedicada à ação coletiva tem que depender de outras organizações; para atingir seu propósito, precisa trocar recursos e negociar um objetivo comum com os demais, e o resultado do intercâmbio depende não só dos recursos de cada ator, mas também das regras do jogo e do ambiente em que o intercâmbio ocorre.
> 4. A governança enfatiza a importância de redes autônomas e autogovernadas de atores. Uma rede autônoma como tal tem autoridade para emitir ordens em uma determinada esfera e trabalhar com o governo nessa esfera e compartilhar suas responsabilidades na administração pública.
> 5. A governança reconhece a capacidade de realizar as atividades sem se basear no poder do governo para comandar ou usar sua autoridade [...][13] (KEPING, 2018, p. 2).

---

[10] Cf. *supra* nota 8.

[11] David Beer chama a atenção para a dificuldade de compreensão que os algoritmos, enquanto objetos de estudo, impõem e alerta para os perigos que essa dificuldade pode acarretar: "Uncertainty about the algorithm could lead us to misjudge their power, to overemphasise their importance, to misconceive of the algorithm as a lone detached actor, or to miss how power might actually be deployed through such technologies. " (2017, p.4).

[12]Cf. CATH, Corinne. **Governing artificial intelligence: Ethical, legal and technical opportunities and challengesPhilosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences**, p. 2, 2018 ("these three guiding forces in AI governance (law, ethics and technology) can be complementary)".

[13] Tradução livre. No original: "1. Governance refers to a set of institutions and actors that are drawn from but also beyond the Government. It challenges the authority of the State or the Government in the traditional sense and maintains that the Government is not the only power center of a state. As long as the power exercised by a

Como é possível depreender da síntese de Keping (2018), a governança envolve a participação de múltiplos atores, públicos e privados, na gestão de matérias coletivas, e relaciona-se intimamente com a liberdade e com a democracia. A boa governança se orienta à maximização do interesse público (KEPING, 2018, p. 4), e apresenta as seguintes características essenciais:

> 1. **Legitimidade**: refere-se ao estado ou qualidade em que a ordem social e a autoridade são voluntariamente reconhecidas e obedecidas. Não tem relevância direta para leis e regulamentos e, do ponto de vista jurídico, algo legal não é necessariamente legítimo. Somente a autoridade e as ordens genuinamente reconhecidas pelas pessoas dentro de um grupo específico são legítimas na ciência política. Quanto maior for o grau de legitimidade, maior será o nível de boa governança. A principal abordagem para alcançar e melhorar a legitimidade é maximizar o consenso e a identidade política compartilhada pelos cidadãos. Portanto, a boa governança requer que os órgãos administrativos e administradores relevantes gerenciem ao máximo os vários conflitos de interesse entre os cidadãos e entre eles e o Estado, a fim de obter o máximo consentimento e aprovação dos cidadãos sobre suas atividades de administração pública.
> 2. **Transparência**: refere-se à publicidade da informação política. Todos os cidadãos têm direito à informação sobre as políticas do Estado que estão relacionadas com os seus próprios interesses, incluindo atividades legislativas, elaboração de políticas, disposições legais, execução de políticas, orçamento administrativo, despesas públicas e outras informações políticas relevantes. A transparência exige que a informação política, acima mencionada, seja devidamente comunicada aos cidadãos através de vários veículos de comunicação, para que eles possam participar na elaboração de políticas públicas e supervisionar o processo de administração pública de forma eficaz. Quanto maior for o grau de transparência, maior será o nível de boa governança.
> 3. ***Accountability***: [...] significa responsabilizar cada pessoa pelo seu próprio comportamento. Na administração pública, refere-se, em particular, aos deveres relacionados com um determinado cargo ou instituição e suas obrigações correspondentes. *Accountability* significa que os administradores e órgãos administrativos devem cumprir as funções e obrigações dos cargos que ocupam. Se não cumprirem suas funções ou deveres vinculados, ou se o fizerem de maneira inadequada, sua conduta constitui negligência do dever ou falta de responsabilidade. Quanto maior for a *accountability* do público, especialmente dos funcionários públicos e dos órgãos administrativos, maior será o nível de boa governança. A este

---

public or private institution is recognized by the public, it is possible to become a power center at a specific level.

2. Governance identifies the blurring of boundaries and responsibilities for tackling social and economic issues. It indicates that, in modern society, the State is transferring its once exclusive responsibilities to civil society (i.e., private sector organizations and voluntary groups, which are undertaking more and more responsibilities that were formerly in the hands of the State). As a result, the boundaries between the State and society and between public and private sectors are becoming increasingly blurred, as are definitions of their responsibilities.

3. Governance identifies the power dependence involved in relationships between institutions involved in collective action. To be specific, every organization devoted to collective action has to depend on other organizations; to achieve its purpose, it has to exchange resources and negotiate a common goal with others, and the outcome of the exchange depends not only on the resources of each actor, but also on the rules of the game and the environment in which the exchange takes place.

4. Governance emphasizes the importance of autonomous self-governing networks of actors. A self-governing network as such has the authority to issue orders in a certain sphere and work with the Government in this sphere and share its responsibilities for public administration.

5. Governance recognizes the capacity to get things done without relying on the power of the Government to command or use its authority".

> respeito, a boa governança requer o emprego da lei e da ética para aumentar a responsabilização dos indivíduos e das instituições.
> 4. **Estado de direito**: essencialmente, [...] significa que a lei é o princípio supremo na administração política pública a ser observado por todos os funcionários públicos e cidadãos, devendo ser todos iguais perante a lei. O objetivo imediato do Estado de Direito é regular o comportamento dos cidadãos, gerir os assuntos sociais e manter uma ordem normal na vida social, enquanto que o seu objetivo final é proteger os direitos políticos básicos dos cidadãos, incluindo a liberdade e igualdade [...]. O Estado de Direito é um requisito básico da boa governança, o que seria impossível sem um sistema legal sólido, o devido respeito pela lei ou uma ordem social baseada na lei.
> 5. **Responsividade**: [...] está intimamente associada ao conceito de responsabilização acima mencionado. Em certo sentido, é uma extensão da *accountability*. Essencialmente, significa que os administradores públicos e os órgãos administrativos devem responder às exigências dos cidadãos de forma célere e responsável, e que é proibido retardar sem justa causa ou deixar qualquer questão sem resposta. Quando necessário, devem solicitar proativamente aos cidadãos orientação, explicar-lhes as suas políticas e responder regularmente às suas perguntas. Quanto maior for o nível de capacidade de resposta, maior será o nível de boa governança.
> 6. **Eficácia**: refere-se principalmente à eficiência da gestão. Tem dois significados essenciais: estrutura administrativa racional, procedimentos administrativos cientificamente concebidos e atividades administrativas flexíveis; e custos administrativos minimizados. As atividades administrativas ineficazes ou ineficientes estão em desacordo com a boa governança. Quanto mais elevado for o nível de boa governança, maior será a eficácia da administração[14] (KEPING, 2018, p. 5–6, grifo nosso, tradução nossa).

[14] Tradução livre. No original: "1. Legitimacy: It refers to the state or quality that social order and authority are voluntarily recognized and obeyed. It has no direct relevance to laws and regulations, and from the legal angle something legal is not necessarily legitimate. Only the authority and orders genuinely recognized by people within a specific group are legitimate in political science. The higher the degree of legitimacy is, the higher the level of good governance will be. The principal approach to achieving and improving legitimacy is to maximize the consensus and political identity shared by citizens. Therefore, good governance requires the relevant administrative bodies and administrators to manage various conflicts of interest among citizens and between them and the State to the maximum so as to obtain the citizens' maximum consent to and approval of their public administration activities.
2. Transparency: It refers to the publicity of political information. All citizens are entitled to the information on State policies that are related to their own interests, including legislative activities, policy-making, legal provisions, policy enforcement, administrative budget, public expenditure and other relevant political information. Transparency requires that the aforementioned political information be duly communicated to citizens through various media vehicles so that they can participate in public policy-making and supervise the process of public administration in an effective manner. The higher the degree of transparency is, the higher the level of good governance will be.
3. Accountability: (…) means holding every person accountable for his or her own behavior. In public administration, it refers in particular to the duties related to a certain position or institution and its corresponding obligations. Accountability means that administrators and administrative bodies must fulfill the functions and obligations of the positions they hold. If they fail to fulfill their bounden functions or duties, or if they do so in an inappropriate manner, their conduct constitutes dereliction of duty or lack of accountability. The more accountability the public, especially public officers and administrative bodies have, the higher the level of good governance will be. In this regard, good governance requires the employment of both law and ethics to enhance the accountability of individuals and institutions.
4. Rule of law: essentially, (…) means that law is the supreme principle in public political administration that should be observed by all government officials and citizens, who should be all equal before the law. The immediate goal of rule of law is to regulate citizens' behavior, manage social affairs and maintain a normal order in social life, while its ultimate goal is to protect citizens' basic political rights, including freedom and equality. In this sense, rule of law is opposite to rule of man as it both regulates citizens' behavior and restricts the conduct of the State. It is the arch-enemy of political autocracy. Rule of law is a basic requirement of good governance, which would be impossible without a sound legal system, due respect for the law or a social order based on the law.

Tais características essenciais estão, evidentemente, presentes no debate sobre a governança algorítmica, salvaguardadas as especificidades associadas aos aspectos novéis das tecnologias de informação, conforme se verá a seguir.

## 1.1 Conceito de inteligência artificial e de algoritmo

O que são algoritmos? E o que se entende por inteligência artificial? Esses são os questionamentos que se intentou discutir na presente Seção.

A definição de algoritmos não é matéria pacífica entre os estudiosos sobre o tema[15]. Procurando responder à indagação sobre a possibilidade de se definir rigorosamente o conceito, Yuri Gurevich (2012) afirma existirem duas perspectivas: uma entende ser possível definir, outra não.

A resposta positiva para o questionamento da existência de um conceito rigoroso se pauta pelo fato de determinados modelos algorítmicos terem se *cristalizado*, tornando possível defini-los estritamente. Encaixar-se-iam nessa categoria os algoritmos sequenciais clássicos[16] (GUREVICH, 2012, p. 33)[17].

---

5. Responsiveness (…) is closely associated with the aforementioned concept of accountability. In a sense, it is an extension of accountability. Essentially, it means that public administrators and administrative bodies must respond to the demands of citizens in a timely and responsible manner, and that it is forbidden to make delays without cause or leave any issue unresolved without response. When necessary, they should proactively solicit advice from citizens, explain their policies to them and answer their questions on a regular basis. The greater the level of responsiveness is, the higher the level of good governance will be.

6. Effectiveness: It mainly refers to management efficiency. It has two essential meanings: rational administrative structure, scientifically *design*ed administrative procedures and flexible administrative activities; and minimized administrative costs. Ineffective or inefficient administrative activities are out of tune with good governance. The higher the level of good governance is, the higher the effectiveness of administration will be".

[15] Além das dificuldades de compreensão técnica, Beer (2017) aponta que o estudo sociopolítico dos algoritmos impõe que se escolha uma abordagem para as análises: deve-se analisá-los isoladamente ou de maneira socialmente contextualizada? O autor sugere que "seeing the algorithm as a separate item of study outside of its social ecology is likely to be a mistake. Algorithms shouldn't be understood as an object that exists outside of those social processes (…). Their existence and *design* is a product of social forces, as are their implementations and re*design*s." (p.5-6). Para uma discussão sobre o conceito tecnopolítico de algoritmo, cf. *e.g.*, BEER, David. The social power of algorithms. **Information Communication and Society**, [s. l.], v. 20, n. 1, p. 13, 2017. Disponível em: <http://eprints.whiterose.ac.uk/104026/>. Acesso em: 3 abr. 2019, ("The notion of the algorithm is part of a wider vocabulary, a vocabulary that we might see deployed to promote a certain rationality, a rationality based upon the virtues of calculation, competition, efficiency, objectivity and the need to be strategic. As such, the notion of the algorithm can be powerful in shaping decisions, influencing behaviour and ushering in certain approaches and ideals").

[16] Para uma discussão simplificada sobre o conceito de algoritmo e sobre a definição de algoritmos sequenciais clássicos, cf. **Parallel Algorithm - Introduction - Tutorialspoint**. [s.d.]. Disponível em: <https://www.tutorialspoint.com/parallel_algorithm/parallel_algorithm_introduction.htm>. Acesso em: 2 dez. 2019: "An **algorithm** is a sequence of instructions followed to solve a problem. While designing an algorithm, we should consider the architecture of computer on which the algorithm will be executed. As per the

Por sua vez, a resposta negativa destaca a contínua multiplicação das noções numérica e algorítmica, de forma a não ser possível, até o momento, a construção de uma definição precisa, capaz de abarcar todos os modelos (GUREVICH, 2012, p. 3).

Detendo-se igualmente sobre o problema da teoria algorítmica, Yiannis N. Moschovakis (2001, p. 919)[18] propõe que os algoritmos sejam definidos de modo abstrato, entendendo-os como definições recursivas.

Quanto à inteligência artificial, Stuart Russel e Peter Norvig (2010) associam-na ao desenvolvimento de agentes inteligentes. Os autores explicam que o conceito de *agentes*[19] *inteligentes*, aparentemente simplista, não é incontroverso, mas depende da abordagem utilizada.

Para tanto, algumas das principais definições de inteligência artificial, de acordo com as distintas concepções de inteligência, retiradas dos escritos de Russell e de Norvig[20], foram reproduzidas a seguir: **Quadro 1 – Principais definições de IA, categorizadas**

---

architecture, there are two types of computers: sequential computer [and] parallel computer. Depending on the architecture of computers, we have two types of algorithms: **Sequential Algorithm** − An algorithm in which some consecutive steps of instructions are executed in a chronological order to solve a problem; **Parallel Algorithm** − The problem is divided into sub-problems and are executed in parallel to get individual outputs. Later on, these individual outputs are combined together to get the final desired output" (grifos do autor). (PARALLEL ALGORITHM - INTRODUCTION - TUTORIALSPOINT, [s.d.])

[17] Para uma análise mais aprofundada sobre o tema, conferir: GUREVICH, Yuri. What Is an Algorithm? In: **Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)**. [s.l: s.n.]. p. 31–42. Comentando sobre a resposta negativa à questão da definição rigorosa, o autor elucida que "[...] many kinds of algorithms have been introduced. In addition to classical sequencial algorithms, in use from antiquity, we have now parallel, interactive, distributed, real-time, analog, hybrid, quantum, etc. algorithms. New kinds of numbers and algorithms may be introduced and most probably will be. The notions of numbers and algorithms have not crystallized (and maybe never will) to support rigorous deffinitions" (p. 32-33, 2012). Conferir também: MOSCHOVAKIS, Yiannis N. What Is an Algorithm? In: **Mathematics Unlimited — 2001 and Beyond**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001. p. 919–936.

[18] Moschovakis esclarece: "When algorithms are defined rigorously in Computer Science literature (which only happens rarely), they are generally identified with *abstract machines*, mathematical models of computers, sometimes idealized by allowing access to "unbounded memory". My aims here are to argue that this not square with our intuitions about algorithms and the way we interpret and apply results about them" (2001, p. 919). Moschovakis oferece, ademais, observações esclarecedoras sobre as propriedades matemáticas dos algoritmos. Aprofundando as definições recursivas, ele explica: "A recursive definition is obtained from a system of fixed-point equations (…), by adding an "output mapping" (…) and dependence on a parameter" (p. 926; 2001). Ainda: "Algorithms are definable recursors (…)" (2001, p. 928); e "(…) algorithms are not absolute, but a set of "given" operations which represent the available resources (…)" (2001, p. 931).

[19] Os autores escrevem que "An agent is anything that can be viewed as perceiving its **environment** through **sensors** and acting upon that environment through **actuators**" (RUSSELL; NORVIG, 2010, p. 34, grifos do autor).

[20] Cf. RUSSELL, Stuart; NORVIG, Peter. **Artificial intelligence : a modern approach**. 3rd. ed. Upper Saddle River, New Jersey: Prentice Hall, 2010, p. 2. Tradução livre dos trechos:

"**Thinking Humanly**: "the exciting new effort to make computers think … *machines with minds*, in the full and literal sense." (Haugeland, 1985); "[the automation of] activities that we associate with human thinking, activities such as decision making, problem solving, learning …" (Bellman, 1978)";

"**Thinking Rationally**: "The study of mental faculties through the use of computational models." (Charniak and McDermott, 1985); "the study of the computations that make it possible to perceive, reason, and act." (Winston, 1992)";

| | |
|---|---|
| **1. Pensando Humanamente**<br>"O novo e excitante esforço para fazer os computadores pensarem... máquinas com mentes, no sentido literal e completo" (HAUGELAND, 1985).<br><br>"[A automatização de] atividades que nós associamos com o pensamento humano, atividades tais como a tomada de decisão, a resolução de problemas, a aprendizagem" (BELLMAN, 1978). | **3. Pensando Racionalmente**<br>"O estudo das faculdades mentais através do uso de modelos computacionais" (CHARNIAKA & MCDERMOTT, 1985).<br><br>"O estudo das computações que tornam possível perceber, raciocinar e agir" (WINSTON, 1992). |
| **2. Agindo Humanamente**<br>"A arte de criar máquinas que executam funções que requerem inteligência quando executadas por pessoas" (KURZWEIL, 1990).<br><br>"O estudo de como fazer com que os computadores façam coisas em que, no momento, as pessoas são melhores" (RICH & KNIGHT, 1991). | **4. Agindo Racionalmente**<br>"Inteligência Computacional é o estudo do *design* de agentes inteligentes" (POOLE *et. al.*, 1998).<br><br>"AI ... está preocupada com o comportamento inteligente em artefatos" (NILSSON, 1998). |

Fonte: RUSSEL e NORVIG (2010, p. 2)

Conforme se verifica, são expostas quatro correntes: as categorias superiores se baseiam na modelagem do pensamento, ao passo que as categorias inferiores focam no comportamento. A coluna da esquerda toma o humano como modelo, enquanto a coluna da direita baseia-se na racionalidade. As categorias foram assim organizadas na medida em que apresentam respostas, das diferentes correntes, às indagações: "preocupa-se com o pensamento ou com o comportamento? Pretende-se modelar o humano ou trabalhar a partir de um padrão ideal?"(RUSSELL; NORVIG, 2010, p. 29[21]).

"**Acting Humanly**: "The art of creating machines that perform functions that require intelligence when performed by people." (Kurzweil, 1990); "The study of how to make computers do things at which, at the moment, people are better." (Rich and Knight, 1991)". "Acting Rationally: "Computational Intelligence is the study of the *design* of intelligent agents." (Poole, *et. al.*,1998); "AI … is concerned with intelligent behavior in artifacts." (Nilsson, 1998)", e
"**Figure 1.1:** Some definitions of artificial intelligence, organized into four categories".

[21] Cf. no original: "Different people approach AI with different goals in mind. Two important questions to ask are: Are you concerned with thinking or behavior? Do you want to model human or work from an ideal standard?"

O *pensamento humano* de IA (1) busca compreender as funções cognitivas humanas para, então, replicar o processo de pensamento em agentes não humanos. A inteligência do agente seria medida pelo grau de correspondência entre o *input-output* do sistema e o de um humano sob as mesmas circunstâncias.

A *ação humana* de IA (2) pretende compreender os processos pelos quais as ações humanas são realizadas e, a partir desta compreensão, criar um modelo que permita desenvolver os agentes artificiais. Para a corrente, será inteligente o agente que for bem-sucedido no Teste de Turing[22].

O *pensamento racional* de IA (3) se volta para silogismos e para a lógica, baseando o grau de inteligência do sistema em sua capacidade de fazer inferências corretas. As conclusões deveriam se dar com base nas regras de funcionamento estabelecidas para o agente e com a aplicação aos *inputs* recebidos.

Por fim, a *ação racional* de IA (4) volta seu estudo para o comportamento racional, compreendendo a racionalidade como medida de inteligência. À vista disso, o agente racional deve cumprir corretamente a função para ele desenhada[23] e, "para cada possível sequência de percepção, deve selecionar uma ação que se espera, maximize sua medida de desempenho[24], dada a evidência fornecida pela sequência de percepção e qualquer conhecimento interno que o agente tenha" (RUSSELL; NORVIG, 2010, p. 37)[25].

Neste contexto, a racionalidade, sob a perspectiva exterior ao funcionamento do sistema de IA, envolve a coleta de informações e processos de aprendizagem, de maneira que o agente possa atuar autonomamente. Em outros termos, o agente "deveria aprender tudo que puder para compensar um conhecimento prévio que esteja incorreto ou que seja parcial" (RUSSELL; NORVIG, 2010, p. 39)[26].

---

[22] O teste foi criado por Alan Turing, em 1950, e consiste em perguntas escritas, elaboradas por humanos, respondidas por computadores, sendo as respostas posteriormente analisadas por humanos. O agente seria inteligente caso, pela análise humana, não fosse possível determinar se as respostas foram formuladas por computadores ou por humanos. Turing teria, ainda, elencado capacidades que o agente deveria possuir a fim de ser capaz de passar no teste, a saber, o processamento de linguagem natural, a representação de conhecimento, o aprendizado de máquina e o raciocínio automatizado.

[23] Segundo Russel e Norvig (2010, p. 35, grifo nosso), "the **agent function** is an abstract mathematical description; the **agent program** is a concrete implementation, running whithin some physical system.".

[24] O *sistema de medida de desempenho* avalia as consequências geradas no ambiente de acordo com a sequência de ações realizadas pelo agente.

[25] Cf. no original: "for each possible percept sequence, a rational agent should select an action that is expected to maximize its performance measure, given the evidence provided by the percept sequence and whatever built-in-knowledge the agent has".

[26] Cf. no original: "It should learn what it can to compensate for partial or incorrect prior knowledge".

Sob a perspectiva interior, por sua vez, a racionalidade compreende o *design* do sistema e o programa do agente[27]. O *design* seria, precisamente, o estágio em que se define a função e o programa do agente inteligente, delimitando como deverá se dar seu funcionamento.

Em síntese, a corrente *comportamento racional* de IA (4) identifica a inteligência com a racionalidade do sistema, cujo agente deve ser capaz de, autônoma e corretamente, cumprir a função para ele determinada, maximizar a medida de sua performance e aprender com sua sequência de percepções. Em razão disso, Russel e Norvig (2010) entendem que essa corrente apresenta vantagens em relação às demais[28]:

> A abordagem do agente racional tem duas vantagens sobre as outras abordagens. Em primeiro lugar, é mais geral do que a abordagem das **"leis do pensamento"** [pensamento racional] porque a inferência correta é apenas um dos vários mecanismos possíveis para alcançar a racionalidade. Em segundo lugar, é mais favorável ao desenvolvimento científico do que as abordagens baseadas no **comportamento humano** ou no **pensamento humano**. O padrão de racionalidade é matematicamente bem definido e completamente geral, e pode ser "desempacotado" para gerar projetos de agentes que provavelmente o alcançam. O comportamento humano, por outro lado, é bem adaptado para um ambiente específico e é definido pela soma total de todas as coisas que os humanos fazem[29] (RUSSELL; NORVIG, 2010, p. 4-5, grifos nossos).

## 1.2 Governança ética

Conforme anteriormente mencionado, o crescente desenvolvimento de IA e de sistemas algorítmicos tem levado pesquisadores a estudar os possíveis efeitos – positivos e negativos – de sua utilização[30]. Uma das questões sobre a qual se debruçam diz respeito a como colher os bens sociais proporcionados pelas novas tecnologias, garantindo, ao mesmo tempo, os direitos humanos fundamentais e a justiça social.

---

[27] Russel e Norvig (p. 46, 2010) definem o agente por meio da seguinte função: "agent = architecture + program".

[28] Russel e Norvig (2010), em seu manual *Artificial Intelligence: a Modern Approach*, conduzem seus estudos de IA igualmente sob a perspectiva da ação racional.

[29] Tradução livre. No original: "The rational-agent approach has two advantages over the other approaches. First, it is more general than the "laws of thought" approach because correct inference is just one of several possible mechanisms for achieving rationality. Second, it is more amenable to scientific development than are approaches based on human behavior or human thought. The standard of rationality is mathematically well defined and completely general, and can be "unpacked" to generate agent *design*s that provably achieve it. Human behavior, on the other hand, is well adapted for one specific environment and is defined by, well, the sum total of all the things that humans do.".

[30] Cf. *supra* nota 8.

Os pesquisadores têm, com isso, debatido sobre as implicações éticas do uso de IA e de algoritmos, endereçando tanto as tecnologias utilizadas pelo setor privado quanto pelo setor público. Este último tem recebido destaque nos trabalhos produzidos, justamente em razão do essencial traço de compromisso com os cidadãos e de garantia dos seus direitos fundamentais.

A partir disso, têm sido elaborados documentos[31], por diversas iniciativas, em que são listados princípios e quadros de referência como propostas para orientar uma utilização ética dos algoritmos e da IA, tais como a Declaração de Toronto (2018) e a Declaração sobre Ética e Proteção de Dados em IA (2018). Ao mesmo tempo, são desenvolvidos critérios para auxiliar na avaliação das tecnologias, de maneira a contribuir para que se possa analisar em que medida seu uso seria aceitável[32].

Conforme será visto a seguir, os documentos sublinham diversos dos principais desafios éticos impostos pela utilização da IA. Entre eles, encontram-se a complexidade técnica dos sistemas; sua opacidade; a qualidade das bases de dados utilizadas[33]; a dificuldade de situar as responsabilidades civil e criminal em razão de danos gerados pelos agentes artificiais; e o devido processo legal, muitas vezes desrespeitado.

Considerando o exposto, foram selecionados, por referência cruzada, oito documentos voltados à ética da IA e dos algoritmos, a fim de serem analisados[34]. Os documentos utilizados como referência foram produzidos pelos seguintes atores: a organização *Fairness, Accountability, and Transparency in Machine Learning (FATML)*[35]; o instituto *Future of Life,*

---

[31] Alguns trabalhos chegam, inclusive, a sugerir a criação de códigos de conduta. Cf., por exemplo, SANGOKOYA, David. **Algorithmic Accountability: Applying the concept to different contry contexts**, 2017, p.17 ("Potential areas for action: (…) Define and promote the use of a code of conduct for responsible use of data and algorithms").

[32] Cf. FREULER, J. Ortiz; IGLESIAS, C. **Algorithms and Artificial Intelligence in Latin America: A Study of Implementation by Governments in Argentina and Uruguay**. [s.l: s.n.]. Disponível em: http://webfoundation.org/docs/2018/09/WF_AI-in-LA_Report_Screen_AW.pdf, (os autores adotam a **efetividade** e a **legitimidade** enquanto requisitos para a implementação da IA pela administração pública).

[33] No preâmbulo de sua declaração, a *International Conference of Data Protection and Privacy Commissioners* (ICDPPC) destacou "that some data sets used to train machine learning-based and artificial intelligence systems habe been found to contain inherent bias resulting in decisions which can unfairly discriminate against certain individuals or groups, potentially restricting the availability of certain services or content, and thus interfering with individuals'rights such as freedom of expression and information or resulting in the exclusion of people from certain aspects of personal, social and professional life (…)" (DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICIAL INTELLIGENCE, 2018, p. 2).

[34] Para uma visão geral sobre as diretrizes éticas elaboradas até o momento, conferir o inventário produzido pela organização alemã *AlgorithmWatch:* ALGORITHM WATCH. **AI Ethics Guidelines Global Inventory – AlgorithmWatch**, 2019. Disponível em: <https://algorithmwatch.org/en/project/ai-ethics-guidelines-global-inventory/>. Acesso em: 10 nov. 2019 ("The way automated decision-making (ADM) systems should be regulated is hotly disputed. Recent months have seen a flurry of frameworks and principles that seek to set out principles of how ADM systems can be developed and implemented ethically. **There are governmental initiatives** (…) **and supra-national efforts** [...]. **The private and civil sectors have also not been idle**.") (grifo nosso).

[35] Cf. FATML. **Principles for Accountable Algorithms and a Social Impact Statement for Algorithms**, 2017. Disponível em: <https://www.fatml.org/resources/principles-for-accountable-algorithms>.

por meio da conferência *ASILOMAR*[36]; a fundação *NESTA*[37]; o instituto *Artificial Intelligence Now* (*AI NOW)*[38]; o governo britânico[39]; a Conferência Internacional dos Delegados para a Proteção de Dados e Privacidade, (*ICDPPC)*[40], e as organizações *Access Now* e Anistia Internacional[41]. As produções serão apresentadas, adiante, com maiores informações, e a lista compilada dos princípios mencionados poderá ser encontrada no Anexo I.

Assim, em face dos trabalhos estudados, identificou-se que os princípios recomendados se encaixavam sob as seguintes categorias principais: transparência, *accountability*[42], responsabilidade, inteligibilidade, explicabilidade, precisão, auditabilidade, respeito aos direitos humanos, engajamento público, justiça[43] e imparcialidade[44].

A ênfase recebida pela transparência e pela *accountability*[45] nos estudos algorítmicos e de IA deve-se à preocupação com os possíveis efeitos negativos de sua utilização, principalmente pelo setor público. Seu objetivo é de permitir que os *outputs* gerados[46] possam

---

[36] Cf. ASILOMAR. **ASILOMAR AI Principles**, 2017. Disponível em: <https://futureoflife.org/ai-principles/>.

[37] Cf. COPELAND, Eddie. **10 principles for public sector use of algorithmic decision making**, 2018. Disponível em: <https://www.nesta.org.uk/blog/10-principles-for-public-sector-use-of-algorithmic-decision-making/>. Sobre a Nesta, cf. COMISSION, European. **Regional Innovation Monitor Plus: NESTA**, [s.d.]. Disponível em: <https://ec.europa.eu/growth/tools-databases/regional-innovation-monitor/organisation/nesta-national-endowment-science-technology-and-arts>. Acesso em: 27 out. 2019 ("Nesta is an innovation charity with a mission to help people and organizations bring great ideas to life").

[38] Cf. REISMAN, Dillon et al. Algorithmic impact assessments: A practical framework for public agency accountability. **AI Now Institute**, [s. l.], n. April, p. 22, 2018. Disponível em: https://ainowinstitute.org/aiareport2018.pdf.

[39]Cf. **Data Ethics Framework**. . [s.l: s.n.]. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/737137/Data_Ethics_Framework.pdf>.

[40] Cf. **Declaration on Ethics and Data Protection in Artificial Intelligence**. Bruxelas, 2018. Disponível em: <https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf>.

[41] Cf. **The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems**. . Toronto. Disponível em: <http://www.ohchr.org/EN/ProfessionalInterest/Pages/Vienna.aspx>.

[42] Cf. *supra*, na nota 35, o conceito de accountability fornecido pela *FATML*: "Accountability in this context includes an obligation to report, explain, or justify algorithmic decision-making as well as mitigate any negative social impacts or potential harms" (p.1).

[43] Cf. SANGOKOYA, David. **Algorithmic Accountability: Applying the concept to different contry contexts**. [s.l: s.n.] (o autor destaca, nas páginas 10 a 13, quanto à forma de endereçar os danos e a discriminação provocados pela IA, o papel do *algorithmic accountability* e do *algorithmic justice*, inclusive retomando os princípios da *FATML*).

[44] Cf. ALTMAN, Micah; WOOD, Alexandra; VAYENA, Effy. A Harm-Reduction Framework for Algorithmic Fairness. **IEEE Security and Privacy**, [s. l.], v. 16, n. 3, p. 34–45, 2018. Disponível em: http://nrs.harvard.edu/urn-3:HUL.InstRepos:37356411, (os autores defendem que, para que um algoritmo seja considerado justo, seria necessário avaliar a distribuição de danos provocados pelo sistema entre os grupos populacionais afetados).

[45] A ICDPPC, em sua declaração, reforça "that artificial intelligence powered systems whose decisions cannot be explained raise fundamental questions of accountability not only for privacy and data protection law, but also liability in the event of errors and harm (…)"(DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICIAL INTELLIGENCE, 2018, p. 2).

[46] Por meio da revisão de literatura, foi possível observar o destaque recebido pela questão da opacidade em relação ao uso de IA pela administração pública. Cf., *e.g.*, BRAUNEIS, Robert; GOODMAN, Ellen P. Algorithmic Transparency for the Smart City. **SSRN Electronic Journal**, [s. l.], 2017, p. 103 ("In the public sector, the opacity of algorithmic decision making is particularly problematic, **both because governmental**

ser controlados pelo público. Entretanto, em razão da assimetria informacional entre os desenvolvedores da tecnologia e aqueles que irão operá-la ou que a ela sujeitar-se-ão, enfrenta-se o obstáculo da opacidade, que, a níveis máximos, confere aos sistemas inteligentes o título de *black boxes*[47] (PASQUALE, 2015).

Comentando a falta de transparência no uso governamental de *big data*, Robert Brauneis e Ellen P. Goodman apontam três principais fatores responsáveis pela opacidade, quais sejam:

> [...] (1) a ausência de uma prática de registo adequada em torno de processos algorítmicos; (2) insistência insuficiente do governo em práticas adequadas de divulgação; e (3) a alegação do sigilo comercial ou de outros privilégios confidenciais por empreiteiros do governo. [...]. Se estes problemas fossem resolvidos, Suspeitamos que, em alguns casos, haveria ainda um outro impedimento para a real transparência: a utilização de algoritmos altamente dinâmicos ou que usam modelagem, que os torna difíceis de serem interpretados até mesmo quando seus registos são revelados (2017, p. 110, tradução nossa)[48].

Conforme mencionado pelos autores, a falta de transparência é, muitas vezes, justificada pela alegação de se tratar de segredo industrial[49] ou pela defesa de que a divulgação das informações técnicas pode comprometer o resultado almejado pelo sistema e a obtenção de sucesso pela iniciativa[50].

---

**decisions may be especially weighty and because democratically elected governments have special duties of accountability**.") (grifo nosso).

[47] Cf. PASQUALE, Frank. **The Black Box Society**. [s.l.]: Harvard University Press, 2015, ("The term "black box" is a usefull metaphor for doing so [understending the problem of gaps in knowledge], given its own dual meaning. It can refer to a **recording device**, like the data-monitoring systems in planes, trains, and cars. Or it can mean a **system whose workings are mysterious**; **we can observe its inputs and *outputs*, but we cannot tell how one becomes the other. We face these two meanings daily: tracked ever more closely by firms and government, we have no clear idea of just how far much of this information can travel, how it is used, or its consequences**"(PASQUALE, 2015, p.3, grifo nosso)). Cf. também MATZNER, Tobias. **Opening black boxes is not enough - Data-based surveillance in discipline and punish and today**. Foucault Studies, p.28, 2017, (em relação às "black-box societies", Tobias Matzner assim resume a importância da transparência: "[...] if the algorithms determine important things in our lives, then we should know how they function and what they really do. Access to their inner workings is considered the prime lever for an ethics or governance of algorithms").

[48] Cf. no original: "there are three principal impediments to making government use of *big data* prediction transparent: (1) the absence of appropriate record generation practices around algorithmic processes; (2) insufficient government insistence on appropriate disclosure practices; and (3) the assertion of trade secrecy or other confidential privileges by government contractors. (…) If these problems were addressed, we Suspect that in some cases, there would be yet another impediment to real transparency: the use of algorithms that are highly dynamic or that use modeling which makes them difficult to interpret even when records are revealed."

[49] Cf., *e.g.*, SILVEIRA, Sérgio Amadeu Da. Economia da intrusão e modulação na internet. **Liinc em Revista**, [s. l.], v. 12, n. 1, p. 17-24, 2016. Disponível em: <http://www.ibict.br/liinchttp://dx.doi.org/10.18617/liinc.v12i1.883>. Acesso em: 3 abr. 2019.

[50] Cf., *e.g.*, VALENTE, Jonas. **Órgãos públicos usam inteligência artificial para combater corrupção | Agência Brasil**. 2018. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2018-08/orgaos-publicos-usam-inteligencia-artificial-para-combater-corrupcao>. Acesso em: 11 maio. 2019 (Em relação ao "sistema

Na tentativa de contornar as lacunas e a opacidade, o *Data Ethics Framework*, desenvolvido pelo Departamento de Assuntos Digitais, Culturais, Midiáticos e Esportivos do governo britânico, sugeriu práticas que poderiam contribuir com os mecanismos de transparência e de *accountability* no setor público. Para tanto, recomendaram aos gestores públicos que documentassem claramente seu trabalho; que compartilhassem os dados utilizados, caso não se tratasse de dados sensíveis ou pessoais; que compartilhassem os sistemas inteligentes desenvolvidos, a fim de permitir sua auditoria; e que buscassem orientar as políticas públicas a partir de sistemas interpretáveis[51].

A ICDPPC fornece, igualmente, sugestões para a melhoria da transparência e da inteligibilidade dos sistemas de IA, associando a consecução dos princípios à própria efetividade na execução dos sistemas. Entre suas proposições, destacam-se as seguintes:

> [...] b. promover a transparência, a inteligibilidade e a acessibilidade, por exemplo através do desenvolvimento de formas inovadoras de comunicação, tendo em conta os diferentes níveis de transparência e informações exigidas para cada audiência relevante,
> c. tornar as práticas das organizações mais transparentes, nomeadamente através da promoção da transparência algorítmica e a auditabilidade dos sistemas, assegurando simultaneamente a pertinência das informações fornecidas, e [...]
> e. Fornecer informações adequadas sobre a finalidade e os efeitos dos sistemas de inteligência artificial, a fim de verificar o alinhamento contínuo com as expectativas dos indivíduos e permitir o controlo humano global em tais sistemas (DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICIAL INTELLIGENCE, 2018, p. 4)[52].

Veja-se que, na medida em que se conhece e se compreende o funcionamento dos sistemas algorítmicos e de IA, não apenas por parte da equipe técnica, mas igualmente por seus operadores e pelos indivíduos sujeitos aos seus efeitos, garante-se que os sistemas sejam inteligíveis e explicáveis. Igualmente, a transparência cria condições para que os sistemas utilizados possam ser auditados interna e externamente, a depender do nível de sensibilidade das informações tratadas pelo algoritmo. Com isso, possibilita-se que os sistemas sejam

---

implantado pelo Ministério da Transparência e Controladoria-Geral da União (CGU) para encontrar indícios de desvios na atuação de servidores [...], **o representante da CGU disse que os critérios adotados na análise não são tornados públicos**. Ele justificou que **a decisão foi pensada para evitar que agentes possam burlar o sistema por identificar seus parâmetros**" (grifo nosso)).

[51] Cf. o princípio 6 do documento *supra*, nota 39.

[52] Cf. no original: "b. promoting transparency, intelligibility and reachability, for instance through the development of innovative ways of communication, taking into account the different levels of transparency and information required for each relevant audience,
c. making organizations' practices more transparent, notably by promoting algorithmic transparency and the auditability of systems, while ensuring meaningfulness of the information provided, and (…)
e. providing adequate information on the purpose and effects of artificial intelligence systems in order to verify continuous alignment with expectation of individuals and to enable overall human control on such systems."

monitorados, criando condições para se controlar possíveis falhas e para se garantir que os *outputs* produzidos sejam justos (*justice* e *fairness*) e em respeito aos direitos humanos[53].

Outro desdobramento do quadro é de contribuir para a fruição do direito ao devido processo legal pelos indivíduos afetados pelos *outputs* dos sistemas algorítmicos e de IA. Veja-se, ao contrário, o exemplo narrado por Cathy O'Neil (2016)[54] de situação em que o direito à defesa e ao processo foram violados.

Tratava-se de *software* desenvolvido e implementado para avaliar a qualidade dos professores, sob a justificativa de que o ensino deficitário estaria diretamente ligado aos educadores. A iniciativa inseria-se em um contexto maior de melhora dos índices de qualidade das escolas públicas.

Ocorreu que, na avaliação algorítmica, foram desconsiderados fatores como o entorno humano e material dos alunos, assim como suas facilidades e suas dificuldades de aprendizagem. Como resultado, houve professores reconhecidos e com qualificação validada pela comunidade escolar que obtiveram resultados ruins nos testes, sendo penalizados em razão disso. Alguns casos chegaram, até mesmo, a demissões.

Na situação mencionada, o sistema algorítmico utilizado era opaco e ininteligível, não tendo sido garantido aos professores prejudicados o direito a recorrer dos resultados ou das decisões tomadas pela administração pública por meio dos algoritmos[55]. Com isso, foi-lhes

---

[53] Sobre a relação entre a transparência nos sistemas algorítmicos e de IA e a proteção de direitos, cf.: "[...] inclusion, diversity and equity are key components of protecting and upholding the right to non-discrimination. All must be considered in the development and deployment of machine learning systems in order to prevent discrimination, particularly against marginalized groups. (…) Inclusion, diversity ad equity entails the active participation of, and meaningful consultation with, a diverse community, including end users, during the *design* and application of machine learning systems, to help ensure that systems are created and used in ways that respect rights – particularly the rights of marginalized groups who are vulnerable to discrimination" (THE TORONTO DECLARATION: PROTECTING THE RIGHT TO EQUALITY AND NON-DISCRIMINATION IN MACHINE LEARNING SYSTEMS, 2018, p. 6).

[54] Cf. *supra* nota 8.

[55] A Lei 13.709/2018, ou Lei Geral de Proteção de Dados do Brasil (LGPD), contempla o direito à explicação. Nas palavras de Renato Monteiro, "A LGPD, na forma como foi aprovada, prevê o direito à explicação no caso de decisões totalmente automatizadas que possam ter um impacto na vida do titular dos dados, principalmente no contexto de formação e uso de perfis comportamentais. A explicação deve incluir não somente informações sobre os dados pessoais que serviram de substrato para o algoritmo, mas também sobre a lógica por trás de tais decisões. O direito à explicação também é possível quando houver o tratamento de dados anonimizados, quando esse tipo de dado for utilizado na formação de perfis comportamentais de pessoas identificadas" (MONTEIRO, 2018, p. 13). Salienta-se a previsão legal de que a revisão deveria se dar por pessoa natural. Entretanto, após veto presidencial, a exigência foi excluída da norma. Noticiando o assunto, a Agência Brasil entrevistou o professor Renato Monteiro, o qual sublinhou que, "na prática o veto fará com que um pedido de revisão de uma decisão automatizada seja processado por outro sistema automatizado, em vez de uma pessoa. 'O titular dos dados perde porque se a vida da pessoa já é altamente impactada por algoritmos, então você pode ter um novo sistema para revisar o outro sistema – e todos eles serem pouco transparentes -. Assim, o titular continua sendo sujeito a processos discriminatórios e não terá possibilidade de auditar isso corretamente'[...] (VALENTE, 2019).

igualmente negado o direito à possibilidade de reparação, nos casos em que fosse, de fato, constatado que o processo foi injusto e falho[56].

O caso sublinha também a relação entre a transparência dos sistemas, a garantia de justiça e os dados utilizados. Para tanto, a transparência permite auditar a qualidade das bases de dados utilizadas no treinamento dos algoritmos, bem como verificar se o tratamento que lhes é prestado obedece às diretrizes para proteção de dados pessoais e para proteção da privacidade. A partir disso, ficaria melhor operacionalizado o enfrentamento à questão da responsabilização por danos gerados pela tecnologia, tal como salientado por O'Neil (2016).

A dificuldade atualmente encontrada reside em definir se a responsabilidade pelos danos deveria ser assumida pelos desenvolvedores ou pelos operadores da tecnologia. Sob a perspectiva do desenvolvedor, especialmente quando se trata de *machine learning*, o alegado é que, em razão da autonomia e da capacidade de aprendizagem do agente racional, a equipe de desenvolvimento deixa de possuir controle efetivo sobre o *comportamento* do sistema.

Por sua vez, sob a perspectiva dos operadores da tecnologia, sustenta-se que, em razão da complexidade técnica e da frequente falta de inteligibilidade dos sistemas, os servidores operam-no, muitas vezes, sem compreender seu funcionamento. Em razão disso, sustentam não possuírem real controle sobre os *outputs* gerados, não tendo contribuído efetivamente para a geração do resultado danoso. Com isso, ambos os lados discursam pela isenção de sua responsabilidade.

Assim, no sentido de fortalecer o princípio da responsabilidade, pesquisadores do *Berkman Klein Center* desenvolveram a tese da explicação[57]. Trata-se da ideia de que, mesmo em relação a sistemas opacos, os resultados e as decisões gerados pelos agentes artificiais deveriam ser justificados ou explicados. Compreendendo que, em algumas circunstâncias, é juridicamente mandatório que se forneçam explicações pelos danos causados por ações

---

[56] Nesse sentido, o Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation) adotou, em seus artigos 13,14 e 22, a previsão ao direito de ser informado (r*ight to be informed*) e ao direito à explicação (right to explanation). Para maiores esclarecimentos, cf.: EUROPEAN COMMISSION. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, p. 25, 2018. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>. Acesso em: 14 nov. 2019: "Articles 13(2) (f) and 14(2) (g) require controllers to provide specific, easily accessible information about automated decision-making, based solely on automated processing, including profiling, that produces legal or similarly significant effects. If the controller is making automated decisions as described in Article 22(1), **they must: tell the data subject that they are engaging in this type of activity; provide meaningful information about the logic involved; and explain the significance and envisaged consequences of the processing**." (grifo nosso).

[57] Cf. DOSHI-VELEZ, Finale *et al*. Accountability of AI Under the Law: The Role of Explanation. **SSRN Electronic Journal**, [s. l.], 2017.

humanas, os autores defendem que, nesses casos, minimamente *explicações* deveriam ser igualmente exigidas dos sistemas artificiais.

Para isso, elaborou-se a ideia de um sistema explicativo, autônomo do sistema artificial principal. Sem conhecer o algoritmo empregado, o sistema explicativo permitiria avaliar o sistema principal em termos de *input* e *output*, considerando as funções programadas. Assim, comparativamente, caso o resultado obtido pelo sistema explicativo fosse distinto do obtido pelo sistema principal, seria possível reconhecer a ocorrência de erros.

Em face disso e de todas as sugestões e teses expostas, vale mencionar a observação crítica de Corinne Cath (2018) no contexto geral de governança da IA:

> É crucial continuar a criticar os objetivos subjacentes às soluções de governança da IA, bem como os impactos culturais colaterais (imprevistos), especialmente em termos de legitimação do desenvolvimento de normas lideradas pelo setor privado em torno da ética, das normas e da regulamentação. Da mesma forma, devemos estar cientes das preocupações que não estão, ou estão apenas parcialmente, cobertas por frases como justiça, responsabilidade e transparência. Ao focar nessas questões, o que não se discute? Estamos assumindo que as questões em torno da IA e equidade, justiça social ou direitos humanos são automaticamente capturadas por essas siglas populares? Ou essas preocupações estão fora do escopo das organizações que promovem a agenda? [...] (2018, p. 5)[58].

## 1.3 O Direito e os impactos da inteligência artificial e dos algoritmos

A governança da IA e dos sistemas algorítmicos passa também pela observação da legislação e dos regulamentos aplicáveis às especificidades de cada contexto[59]. Nesse sentido, apontam igualmente a Declaração de Toronto (2018)[60] e o *Data Ethics Framework* (2018)[61], do governo britânico, destacando que não apenas os sistemas jurídicos nacionais devem ser obedecidos, mas igualmente os tratados internacionais[62].

---

[58] Cf. no original: "It is crucial to remain critical of the underlying aims of AI governance solutions as well as the (unforeseen) collateral cultural impacts, especially in terms of legitimizing private-sector led norm development around ethics, standards and regulation. Likewise, we must remain cognizant of the concerns not, or only partially, covered by phrases like fairness, accountability and transparency. In focusing in these issues what is not discussed? Are we assuming that issues around AI and equity, social justice or human rights are automatically caught by these popular acronyms? Or are these concerns out of scope for the organizations pushing the agenda? (…)".

[59] Cf. o princípio 2 – "Be aware of relevant legislation and codes of practice" - do documento *supra*, nota 39.

[60] Cf. *supra* nota 41.

[61] Cf. *supra* nota 39.

[62] Sobre o caráter constitucional dos tratados internacionais de direitos humanos no ordenamento brasileiro, cf. BRASIL. **Constituição da República Federativa do Brasil. Texto constitucional originalmente publicado**

Em face disso, e diante do sistema normativo brasileiro, sublinha-se o especial cuidado que deve ser destinado aos direitos humanos; à proteção dos dados pessoais; à promoção da igualdade e à vedação de práticas discriminatórias; aos direitos autorais e de propriedade intelectual. Deve-se, igualmente, atentar aos regulamentos específicos de cada setor[63], a depender do sistema algorítmico ou de inteligência artificial que se pretende desenvolver e/ou implementar.

Em relação às normas internas brasileiras[64], menciona-se trecho publicado na Estratégia Brasileira para Transformação Digital E-Digital[65]:

> É oportuno para o Brasil estabelecer o seu marco legal, protegendo direitos dos cidadãos e conferindo segurança jurídica para investimentos na economia digital. Há, contudo, diversas normas legais e infralegais que atualmente tratam da questão em âmbito setorial, como: o Código de Defesa do Consumidor (artigos 43 e 44), que resguarda os dados pessoais de consumidores; a Lei de Acesso à Informação (artigo 31 da Lei n° 12.527/2011), que protege os dados pessoais ao mesmo tempo em que promove a transparência do poder público; a Lei do Cadastro Positivo (Lei n° 12.414/2011), que salvaguarda os dados pessoais no âmbito de análises de crédito; entre outras. O próprio Marco Civil da Internet (artigo 3°, incisos II e III, 7° a 17 da Lei n° 12.965/2014) assegura a tutela da privacidade e da proteção de dados pessoais (BRASIL, 2018, p. 39).

---

**no Diário Oficial da União de 5 de outubro de 1988.**, 1988. Disponível em:<http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 10 nov. 2019:
"Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...]
§ 1º As normas definidoras dos direitos e garantias fundamentais têm **aplicação imediata**.
§ 2º Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos **tratados internacionais em que a República Federativa do Brasil seja parte**.
§ 3º **Os tratados e convenções internacionais sobre direitos humanos que forem aprovados, em cada Casa do Congresso Nacional, em dois turnos, por três quintos dos votos dos respectivos membros, serão equivalentes às emendas constitucionais**." (grifo nosso).

[63] Caso o sistema hipoteticamente desenvolvido envolvesse o setor de saúde pública, *e.g.*, teria que se adequar igualmente às Portarias de Consolidação MS/GM n° 1, 2, 3, 4, 5, e 6, de 28 de setembro de 2017, relativas ao Serviço Único de Saúde (SUS). Cf.: **Portarias de consolidação MS/GM - Secretaria da Saúde**, [s.d.]. Disponível em: <https://saude.rs.gov.br/portarias-de-consolidacao-ms-gm>.

[64] Até a conclusão deste trabalho, estava em tramitação, no Senado Federal, projeto de lei destinado a promover princípios para a utilização de IA no Brasil. Cf.: VALENTIM, Styvenson. **Projeto de Lei n° 5051, de 2019**. Estabelece os princípios para o uso da Inteligência Artificial no Brasil. Brasília, 2019. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=8009064&ts=1570126400907&disposition=inline>. Acesso em: 10 nov. 2019 ("[...] Art.2º A disciplina do uso da Inteligência Artificial no Brasil tem como fundamento o reconhecimento de que se trata de tecnologia desenvolvida para servir as pessoas com a finalidade de melhorar o bem-estar humano em geral, bem como: I – o respeito à dignidade humana, à liberdade, à democracia e à igualdade; II – o respeito aos direitos humanos, à pluralidade e à diversidade; III – a garantia da proteção da privacidade e dos dados pessoais; IV– a transparência, a confiabilidade e a possibilidade de auditoria dos sistemas; V – a supervisão humana.").

[65] Cf. BRASIL. **Estratégia Brasileira Para a Transformação Digital - E-Digital**. [s.l: s.n.]. Disponível em: <http://www.mctic.gov.br/mctic/export/sites/institucional/estrategiadigital.pdf>.

Ademais, cabe mencionar o marco regulatório da propriedade intelectual[66] (Lei n° 9.279/96, Lei n° 9.456/97, Lei n° 9.609/98 e Lei n° 9.610), a Lei nº 13.709/18[67] (Lei Geral de Proteção de Dados) e o Decreto n° 10.046/2019[68].

Por sua vez, no que se refere aos direitos humanos internacionais, cabe destacar a Declaração Universal dos Direitos do Homem (1948)[69], a Declaração Americana dos Direitos e Deveres do Homem (1948)[70], o Pacto Internacional de Direitos Civis e Políticos (1966)[71], o Pacto Internacional de Direitos Econômicos, Sociais e Culturais (1966)[72], o Pacto de San José da Costa Rica (1969)[73], a Declaração Sobre o Direito ao Desenvolvimento (1986)[74] e a Declaração e Programa de Ação de Viena (1993)[75], todos aprovados/ratificados pelo Brasil[76].

---

[66] Cf.: BRASIL. **Lei nº 9.279, de 14 de maio de 1996**. Regula direitos e obrigações relativos à propriedade industrial. 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9279.htm; BRASIL. **Lei nº 9.456, de 25 de abril de 1997**. Institui a Lei de Proteção de Cultivares e dá outras providências. 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9456.htm; BRASIL**. Lei nº 9.609 , de 19 de fevereiro de 1998.** Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Brasil, 1998a. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9609.htm; BRASIL. **Lei nº 9.610, de 19 de fevereiro de 1998**. Dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. 1998b. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9610.htm>.

[67] Cf. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>.

[68] Cf. BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília, 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm>. Acesso em: 10 nov. 2019.

[69] "Artigo II - 1. Toda pessoa tem capacidade para gozar os direitos e as liberdades estabelecidos nesta Declaração, sem distinção de qualquer espécie, seja de raça, cor, sexo, língua, religião, opinião política ou de outra natureza, origem nacional ou social, riqueza, nascimento, ou qualquer outra condição".

[70] "Artigo II. Todas as pessoas são iguais perante a lei e têm os direitos e deveres consagrados nesta Declaração, sem distinção de raça, língua, crença, ou qualquer outra".

[71] Art. 2º - "1. Os Estados-partes no presente Pacto comprometem-se a garantir a todos os indivíduos que se encontrem em seu território e que estejam sujeitos à sua jurisdição os direitos reconhecidos no presente Pacto, sem discriminação alguma por motivo de raça, cor, sexo, língua, religião, opinião política ou de qualquer outra natureza, origem nacional ou social, situação econômica, nascimento ou qualquer outra situação".

[72] Art. 2º -"2. Os Estados-partes nesta Convenção comprometem-se a respeitar os direitos e liberdades nela reconhecidos e a garantir seu livre e pleno exercício a toda pessoa que esteja sujeita à sua jurisdição, sem discriminação alguma, por motivo de raça, cor, sexo, idioma, religião, opiniões políticas ou de qualquer outra natureza, origem nacional ou social, posição econômica, nascimento ou qualquer outra condição social".

[73] Art. 1º - "1. Os Estados-partes nesta Convenção comprometem-se a respeitar os direitos e liberdades nela reconhecidos e a garantir seu livre e pleno exercício a toda pessoa que esteja sujeita à sua jurisdição, sem discriminação alguma, por motivo de raça, cor, sexo, idioma, religião, opiniões políticas ou de qualquer outra natureza, origem nacional ou social, posição econômica, nascimento ou qualquer outra condição social".

[74] "Artigo 1 - 1. O direito ao desenvolvimento é um direito humano inalienável em virtude do qual toda pessoa humana e todos os povos estão habilitados a participar do desenvolvimento econômico, social, cultural e político, a ele contribuir e dele desfrutar, no qual todos os direitos humanos e liberdades fundamentais possam ser plenamente realizados".

[75] "8. A democracia, o desenvolvimento e o respeito aos direitos humanos e liberdades fundamentais são conceitos interdependentes que se reforçam mutuamente. A democracia se baseia na vontade livremente expressa pelo povo de determinar seus próprios sistemas políticos, econômicos, sociais e culturais e em sua plena participação em todos os aspectos de suas vidas. Nesse contexto, a promoção e proteção dos direitos humanos e liberdades fundamentais, em níveis nacional e internacional, devem ser universais e incondicionais. A comunidade internacional deve apoiar o fortalecimento e a promoção de democracia e o desenvolvimento e respeito aos direitos humanos e liberdades fundamentais no mundo inteiro".

[76] SÃO PAULO (Estado). Procuradoria Geral do Estado de São Paulo. **Instrumentos Internacionais de Proteção dos Direitos Humanos.**São Paulo, 1996. Disponível em: <http://www.pge.sp.gov.br/centrodeestudos/bibliotecavirtual/instrumentos/sumario.htm>. Acesso em: 15 nov. 2019.

# 2 VIGILÂNCIA, PODER E INTELIGÊNCIA ARTIFICIAL

A seguir, adentrou-se na discussão política do tema. De que forma a IA e os algoritmos desenvolvidos, orientados à otimização da produtividade e da eficiência, e potencializados pelo número crescente de dados disponíveis, inserem- se na discussão sobre poder[77]? Como se relacionam o *Capitalismo de Vigilância* e a governança da IA? Como isso se mostra especialmente em relação a tecnologias voltadas à segurança pública?

A partir dessa reflexão, será realizada, posteriormente, análise do projeto *Sinesp Big Data e IA para Segurança Pública*.

## 2.1 Foucault e Deleuze revisitados

Debruçando-se sobre a genealogia do poder, Foucault buscou suas características nos diferentes períodos históricos, assim como a transição entre cada um desses momentos.

Assim, Richard A. Lynch resume as características básicas do poder, segundo a teoria de Foucault[78], como sendo "uma rede de relações de força por toda a sociedade, relações que são caracterizadas por resistência e que interagem mediante táticas locais e estratégias maiores. " (TAYLOR, 2008, cap. A Teoria do Poder de Foucault, p. 25). Sob outra perspectiva, o autor assim resume:

> [...] nós temos um conjunto de "relações de força"[79], processos pelos quais essas relações são transformadas, sistemas ou disjunções que são constituídos pela interação dessas relações de força e estratégias maiores (ou "formas terminais") com características gerais e institucionais que emergem destas relações, processos e sistemas (2008, p. 31).

[77] Cf.: "The notion of the algorithm is evoked to influence and convince, to suggest things and to envision a certain approach, governmentality and way of ordering. Plus, the term is also part of wider rationalities and ways of thinking. Together then, **this requires us to explore and illustrate the power of this term whilst also potentially using it as a focal point for opening up or revealing these wider rationalities**" (BEER, 2017, p. 13, grifo nosso).

[78] Foucault teria registrado sua ressalva em que seu trabalho fosse compreendido como uma teoria do poder, uma vez que o vislumbrava mais como um esforço no sentido de analisá-lo (LYNCH, 2008, p. 25-26).

[79] Lynch esclarece que, de acordo com a visão de Foucault, "em linhas gerais, as **relações de força** consistem no que quer que seja, nas interações sociais de alguém, algo que o empurre, incite ou obrigue a fazer algo" (2008, p. 31, grifo nosso).

Essa menção ao poder descentralizado evoca o entendimento de que o poder, por sua característica difusa[80], não seria "detido", mas exercido nas relações, aproximando-se do que foi chamado, por Foucault, de "microfísica do poder" (a análise do poder partiria do micro para o macro). Ademais, além da sua característica onipresente, o poder estaria sempre "acompanhado pela resistência" (TAYLOR, 2008, cap. A Teoria do Poder de Foucault, p. 38).

A partir disso, pode-se iniciar a revisão da genealogia do poder proposta por Foucault. Para tanto, inicialmente se observa a figura do soberano, em relação ao qual o poder se manifesta como subtração e morte. O soberano o exercia a partir de uma perspectiva pessoal, ou seja, os crimes representavam a usurpação de seu poder e constituíam-se como verdadeiras ofensas à sua autoridade. Seguindo esta lógica, as punições serviam como restauração e reafirmação do poder soberano (TAYLOR, 2008, p. 59-60).

Com a decadência do poder soberano, observa-se o surgimento do poder disciplinar, constituído como a disciplina dos indivíduos, a partir de instituições disciplinares — cadeias, hospitais, escolas — . Nesse estágio, o contexto punitivo transforma-se, passando, em geral, de penas corporais/capitais para penas privativas ou restritivas de liberdade. Os delitos não mais constituíam afronta à figura do soberano, mas eram reconhecidos como comportamentos anormais que deveriam ser corrigidos, de acordo com as normas e em atenção à segurança da população.

Cressida J. Heyes (TAYLOR, 2008, cap. Subjetividade e Poder) aponta que o surgimento do poder disciplinar sinalizaria uma nova configuração sociopolítica, marcada pela ressignificação das relações humanas com o espaço, com o tempo e com a subjetividade. Em outros termos, o poder disciplinar seria uma conformação de poder cujas características seriam a individualização, a sujeição, a compartimentalização dos espaços e o controle do tempo de trabalho. Segundo Marcelo Hoffman (TAYLOR, 2008, cap. O Poder Disciplinar), o exercício desse poder se destina a:

> [...] controlar meticulosa, exaustiva e continuamente as atividades dos corpos, de modo a constituí-los **como portadores de uma relação altamente particular entre utilidade e docilidade, pela qual um acréscimo na utilidade corresponda a um acréscimo na docilidade e vice-versa**" (p. 43, grifo nosso).

Por individualização, Foucault teria buscado expressar que o exercício do poder se dava prioritariamente com foco no indivíduo, a partir da disciplina imposta ao corpo, ao tempo –

[80] Ibid., Lynch observa quanto ao pensamento de Foucault que o poder "vem de toda parte" (p.34) e, em razão disso, para compreendê-lo "devemos olhar para as teias complexas de relações entrelaçadas" (p.35).

dividindo-o – e aos espaços – compartimentalizando-os. Em razão disso, seria possível identificar distintas modalidades de individualidade em curso: a celular, a genética, a orgânica e a combinatória (TAYLOR, 2008, cap. O Poder Disciplinar).

A *individualidade celular* representaria a separação física dos indivíduos, com o emprego da arquitetura na construção de fábricas, escolas, hospitais, presídios, entre outros. Em razão disso, Deleuze (1992, p. 223) escreveu que as sociedades disciplinares realizaram a "organização dos grandes meios de confinamento".

Nesses espaços, a disciplina dos corpos passava pela administração de seu tempo de trabalho, com o uso de cronogramas em que se prescreviam as atividades a serem realizadas nos períodos laborados. Assim, os indivíduos eram disciplinados pelas figuras de autoridade dos respectivos espaços de confinamento, que determinavam as normas a serem obedecidas, conformando o que Foucault chamou de *individualidade genética*. Sua principal direção era levar os indivíduos a se tornarem mais produtivos e eficientes.

Entretanto, ademais dos objetivos concretizados pelas individualidades celular e genética, aspirava-se a que a disciplina dos corpos se desse por meio da dócil conformação dos indivíduos a modelos de comportamento. Nas palavras de Rogério da Costa (2004, p. 161), tratar-se-ia de uma modelagem, "pois um mesmo molde fixo e definido poderia ser aplicado às mais diversas formas sociais". Isso tratou de representar a *individualidade orgânica*, que descrevia a internalização da disciplina por cada indivíduo.

Todas as referidas características do poder disciplinar teriam se projetado no tempo graças a determinadas estratégias. A primeira delas seria a observação hierárquica: os indivíduos estariam constantemente sob vigilância dentro de ambientes fechados [papel, também, da arquitetura]. Com isso, sabendo-se vigiados, mas desconhecendo quem os vigia[81], neles seria incutida a observação do próprio comportamento, levando-os a modulá-lo. A vigilância se completaria com uma "rede de vigilância dentro do grupo de indivíduos que ocupam um espaço arquitetônico particular [...], densa rede de olhares vigilantes e multidirecionais [...]" (TAYLOR, 2008, cap. O Poder Disciplinar, p.46-47).

A segunda técnica seria o julgamento normalizador, em que, a partir da criação de normas e de modelos de comportamento, ter-se-ia a criação de parâmetros que qualificariam os indivíduos e as situações como normais ou como anormais.

A terceira técnica seria o exame, uma comunhão da observação hierárquica e do julgamento normalizador, por meio da qual a observância aos modelos seria

[81] Costa(2004, p.162) observa que, em relação às informações, a sociedade seria marcada por um poder "vertical e hierarquizado", com uma polarização entre a transparência dos indivíduos e a opacidade do poder.

institucionalmente aferida. Exemplos da técnica seriam provas escolares e rondas em hospitais.

Conforme anteriormente mencionado, o poder disciplinar atua diretamente na subjetivação (*assujettissement*) dos indivíduos/formação de suas posições-sujeito. Para Foucault, a subjetividade seria um produto histórico e cultural das relações de poder. Para tanto, o sujeito moderno, no contexto da sociedade disciplinar, seria marcado pela docilidade, pela conformação às normas e pela autovigilância (TAYLOR, 2008, cap. Subjetividade e Poder).

Por essa perspectiva, restaria evidenciada a visão ambivalente de Foucault no sentido de que o poder possuiria duas dimensões, uma negativa e uma positiva. A dimensão negativa iria se referir ao aspecto de dominação pelo poder, ao passo que a dimensão positiva diria respeito à resistência dos sujeitos a essa dominação[82] (TAYLOR, 2008, cap. Subjetividade e Poder, p. 203-205).

Em razão dessa concepção, há críticos que entendem que o trabalho de Foucault destaca as relações disciplinares de poder, concebendo os sujeitos sem qualquer agência [ou poder de resistência][83]. Assim, na medida em que o poder disciplinar seria onipresente, não sendo possível identificá-lo com a figura de um soberano, os indivíduos acabariam desmobilizados em sua oposição e resistência.

Para tanto, em relação à crítica, Foucault teria respondido que sua teoria não seria essencialmente pessimista quanto ao poder de agência dos indivíduos, mas estimularia uma posição de permanente crítica e vigilância pelos sujeitos. Não se prestaria, assim, a delinear um modelo de subjetividade que fosse livre da opressão, justamente por compreender que o poder, concomitantemente, oprimiria os indivíduos e formaria sua subjetividade (TAYLOR, 2008, cap. Subjetividade e Poder)[84].

Para Foucault, tais características e estratégias do poder disciplinar seriam perfeitamente visíveis na arquitetura do *Panóptico* de Jeremy Bentham, com a compartimentalização dos

---

[82] Foucault teria demonstrado as duas dimensões analisando a história da sexualidade e exemplificando-as em relação à homossexualidade. A posição-sujeito *design*ada pela expressão, ao mesmo tempo em que denotaria uma "anormalidade", refletindo um julgamento normalizador histórico e culturalmente contingenciado, prestar-se-ia à resistência dos indivíduos enquadrados nessa posição, possibilitando seu reconhecimento mútuo, com a criação de uma identidade coletiva e sua mobilização, como em paradas do orgulho LGBTI, entre outros (TAYLOR, 2008, cap. Subjetividade e Poder, p. 203-205).

[83] Nesse sentido, cf., *i.e.*, FRASER, N. **Michel Foucault: A Young Conservative?**, 1994, In: KELLY, M. (ed.). *Critique and Power*: Recasting the Foucault/Habermas Debate. Cambridge, MA: MIT Press, p. 185-210.

[84] Heyes vislumbra que isso se relaciona diretamente com a discussão sobre individualidade: o processo de individualização, vivenciado nas sociedades disciplinares, ocorreria paralelamente ao aumento da sujeição pelos indivíduos e do controle sobre eles (TAYLOR, 2008, cap. Subjetividade e Poder).

espaços, com a individualização, a vigilância constante dos corpos e com a observação hierárquica. Veja-se a observação de Hoffman (2008):

> Foucault considera este edifício a perfeita expressão do poder disciplinar por uma série de razões. Em primeiro lugar, com cada uma das células destinada a ser ocupada por apenas um preso de cada vez, o edifício produz efeitos individualizantes na sua periferia. Em segundo lugar, persianas e divisórias na torre impedem ver se alguém realmente a ocupa, garantindo o anonimato no centro. Em terceiro lugar, a luz artificial a partir da torre central, bem como a entrada de luz natural a partir das janelas das celas asseguram visibilidade aos presos nas celas. Finalmente, esta visibilidade permite a escrita perpétua sobre os presos [...] (TAYLOR, 2008, cap. O Poder Disciplinar, p. 60).

Quanto ao biopoder, Foucault o descreve como o poder exercido sobre a população, buscando administrar-lhe a vida. Nisso, diferencia-se do poder disciplinar, cuja centralidade encontra-se nos indivíduos (TAYLOR, 2008, p. 60-62).

Essa distinção[85], entretanto, não implicaria que o poder disciplinar tenha sido superado pelo surgimento do biopoder, mas sinalizaria a existência de duas dimensões políticas: uma de "microtecnologia", aplicada a indivíduos, e outra de "macrotecnologia", aplicada a nível populacional (TAYLOR, 2008, p. 62-64). Nesse sentido, veja-se a distinção elaborada por Taylor:

[85] Para maiores esclarecimentos sobre a diferença entre poder soberano, poder disciplinar e biopoder, conferir a explicação de Taylor: "Sob o poder soberano, que predominou até o final do século XVII, quando Hobbes estava escrevendo, um indivíduo que transgredisse essas proibições do roubo e do assassinato seria submetido à lei ou punido; no entanto, já não seria meramente o seu crime que estaria em questão. Em vez disso, o poder agora estará pelo menos igualmente interessado no caráter do ladrão ou do assassino. Quererá conhecer as condições, tanto materiais quanto psicológicas, sob as quais o indivíduo cometeu seu crime. Esta informação será considerada importante para prever e intervir na probabilidade de o criminoso reincidir. A fim de antever e controlar as chances de reincidência do indivíduo, o criminoso deve ser submetido a exames psicológicos, vigilância e práticas reabilitativas desconhecidas sob o poder soberano. Por esta razão, a punição é menos propensa a pôr fim à vida do criminoso e mais propensa a controlar sua vida mediante táticas tais como a prisão, o tratamento psiquiátrico, a liberdade condicional e a liberdade vigiada. Finalmente, sob o biopoder, que emergiu no final do século XVIII, o foco e o alvo do poder tornam-se o número de roubos e assassinatos que ocorrem na população. **O poder agora se interessa por saber se as taxas de criminalidade estão subindo ou caindo, em quais grupos demográficos determinados crimes são predominantes e como as taxas de criminalidade podem ser reguladas ou controladas otimamente. Embora muitas das mesmas táticas sejam empregadas tanto sob o biopoder quanto sob o poder disciplinar, o foco agora estará sobre a população e não sobre o indivíduo**" (TAYLOR, 2008, p. 62, grifo nosso).

**Quadro 2 – Dois níveis de biopoder**

| Tipo | Alvo | Objetivo | Instituições | Táticas |
|---|---|---|---|---|
| Poder regulador (biopolítica) | Populações, espécies, raça | Saber/poder e controle da população | O Estado | Estudos e práticas de demógrafos, sociólogos e economistas, intervenções na taxa de natalidade, longevidade, saúde pública, moradia, migração |
| Poder disciplinar (anatomopolítica) | indivíduos, corpos | Conhecimento/ poder e subjugação dos corpos | Escolas, exércitos, prisões, asilos, hospitais, oficinas | Estudos e práticas de criminologistas, psicólogos, psiquiatras, educadores, aprendizes, testes, educação, treinamento |

Fonte: TAYLOR (2008, p. 64)

Essa lógica de regulação e de administração da vida[86] sugere que:

> O biopoder é capaz de acessar o corpo porque funciona através de normas em vez de leis, porque é internalizado por sujeitos, em vez de exercido de cima mediante atos ou ameaças de violência, e porque está disperso por toda sociedade em vez de localizado em um único indivíduo ou organismo do governo (TAYLOR, 2008, p. 61).

Assim, uma das formas de manifestação do biopoder seria o controle sobre a saúde e sobre a sexualidade das populações. Isso se veria na administração das taxas de natalidade e na preocupação com sistemas de previdência social frente ao envelhecimento dos indivíduos. Nesse sentido, exemplos emblemáticos de movimentos biopolíticos seriam o darwinismo social e a eugenia (TAYLOR, 2008, p. 71–75).

Outra manifestação da biopolítica seria a "desqualificação da morte", em que a extinção da vida passa a ser vista como um fenômeno a ser controlado, combatido e invisibilizado. Para tanto, observa-se os Estados destinando vultosos recursos a campos como segurança pública e saúde[87].

[86] Segundo exposto por Taylor (2008, p. 65), "os estados modernos reconheceram a necessidade de entender as características, estruturas e tendências das suas populações a fim de gerenciá-las ou para compensar o que não podiam controlar".

[87] Taylor cita, ainda, que as guerras e o combate ao crime passaram a ser justificados como medidas de proteção à população: morte como meio para que se proteja a vida. Sob a mesma lógica, estaria o controle sobre a sexualidade da população: censos demográficos, controle de natalidade, com incentivos positivos ou negativos a depender da realidade sociocultural e geográfica.

Ocorre que, com as transformações sociais, políticas, econômicas e científicas vivenciadas a partir do século XX, a sociedade disciplinar não estaria mais em curso, mas teria sido suplantada pela sociedade de controle. Em seu artigo *Post-Scriptum sobre as Sociedades de Controle* (1992), Gilles Deleuze escreve que o fim da Segunda Guerra Mundial teria marcado o surgimento dos novos moldes sociopolíticos. Para tanto, o filósofo discorre sobre os elementos que o levaram a sustentar a passagem de uma estrutura sociopolítica para a outra, explicitando as diferenças entre as sociedades disciplinar e de controle.

Assim, inicialmente, detendo-se sobre a arquitetura dos espaços, Deleuze (1992, p. 223) entende que o poder disciplinar se ocupava da "organização dos espaços de confinamento", com a vigilância ocorrendo em espaços fechados. Com a crise das instituições, a sociedade passaria a ser caracterizada por indivíduos em rede, vigiados virtualmente[88]. Em relação a esse ponto, Costa (2004, p. 161) aponta para o fato de que haveria uma "interpenetração dos espaços, por sua suposta ausência de limites definidos (rede) e pela instauração de um tempo contínuo [...]".

Quanto aos moldes da sociedade disciplinar, em que o exercício do poder se dava em relação aos indivíduos, representados por sua assinatura, e em relação à massa, representada pelo número de matrícula, Deleuze (1992, p. 225-226) contrapõe a modulação nas sociedades de controle. Isso se refere à fluidez e à rapidez das mudanças, com o indivíduo sendo substituído pelo "divíduo"[89], sinalizado pela cifra, e com a substituição das massas pelas "amostras e bancos de dados", na permanente tentativa de identificar padrões e modular comportamentos.

Deleuze (1992, p. 227-228) acrescenta que, na essência, as transformações referem-se à "mutação do capitalismo", antes marcado pela produção ("concentração", "propriedade") e agora caracterizado pela "sobreprodução" (venda de serviços e compra de ações).

Em resumo, a sociedade seria, agora, caracterizada por indivíduos em rede, vigiados virtualmente[90]. Assim, com a crescente disponibilidade de dados, haveria a permanente tentativa de identificação de padrões para a modulação de comportamentos. O tempo não seria mais compartimentalizado, mas caracterizado pelo que o autor chama de "prisão em espaço aberto", mesmo sem o prévio cometimento de crime algum.

---

[88] Rogério da Costa sinaliza que, com a passagem da sociedade disciplinar para a sociedade de controle, a lógica de vigilância teria se alterado, passando da interceptação de mensagens para a tentativa de identificação de padrões. Cf. COSTA, Rogério Da. Sociedade de controle. **São Paulo em Perspectiva**, 2004.

[89] "Os indivíduos tornaram-se *dividuais*, divisíveis, e as massas tornaram-se amostras, dados, mercados ou 'bancos'" (DELEUZE, 1990, p. 226).

[90] Rogério da Costa sinaliza que, com a passagem da sociedade disciplinar para a sociedade de controle, a lógica de vigilância teria se alterado, passando da interceptação de mensagens para a tentativa de identificação de padrões. Cf. COSTA, Rogério Da. Sociedade de controle. **São Paulo em Perspectiva**, 2004.

Em face disso, Deleuze (1992, p. 229) ainda alerta para o fato de que, na comparação entre a sociedade disciplinar e a sociedade de controle, as análises não devem ser dedicadas a produzir juízos de valor, mas devem se dar criticamente, em vista "[d]a implantação progressiva e dispersa de um novo regime de dominação". Em relação a isso, o filósofo alerta:

> Muitos jovens pedem estranhamente para serem 'motivados', e solicitam novos estágios e formação permanente; cabe a eles descobrir a que estão sendo levados a servir, assim como seus antecessores descobriram, não sem dor, a finalidade das disciplinas (DELEUZE, 1992, p. 230).

## 2.2 A inteligência artificial como instrumento disciplinar e de controle

> Assim, se a questão central de uma ética dos algoritmos é: 'O que fazem os algoritmos aos sujeitos?', com Foucault esta questão ganha um novo ângulo: 'O algoritmo e os dados que ele usa constituem estes sujeitos em primeiro lugar'[91] (MATZNER, 2017, p. 29, tradução nossa).

Após a introdução dos conceitos expostos na Seção anterior, cumpre questionar-se de que maneira os sistemas algorítmicos e de IA se situam em relação às ideias do poder disciplinar, do biopoder e da sociedade de controle.

Para iniciar a discussão, é válido ponderar a relação entre algoritmos e poder. Nesse sentido, escrevendo sobre o poder social dos algoritmos, David Beer (2017, p. 10) expõe o posicionamento de que os algoritmos não detêm poder de maneira intrínseca, mas que este seria produzido a partir do contexto social no qual aqueles estivessem inseridos.

Por essa perspectiva, o autor argumenta que o poder social algorítmico poderia ser analisado sob duas perspectivas: material ou discursiva. De acordo com a primeira, ele iria se manifestar na forma de "intervenções materiais realizadas pelos próprios algoritmos", ao passo que, sob a segunda perspectiva, iria surgir na forma de "intervenções discursivas" (2017, p. 11-12)[92].

---

[91] Tradução livre do trecho: "Thus, if the central question of an ethics of algorithms is: 'What do algorithms do to subjects?', with Foucault this question gets a new angle: 'The algorithm and the data it uses constitute these subjects in the first place'" (MATZNER, 2017, p. 29).

[92] Beer (2017, p.11) acrescenta que, em relação à dimensão material, "Power is then operationalized through the algorithm, in that the algorithmic output cements, maintains or produces certain truths". Quanto à dimensão discursiva, ele escreve que "[...] algorithms are also a notional presence in discourse. We might look at how that term or notion is deployed to create or perpetuate certain truths about social orders and the like, or how certain truths are cultivated through discussions or evocations of the algorithm" (2017, p. 12).

Essa segunda dimensão, ligada essencialmente à forma como os algoritmos são percebidos socialmente e às verdades às quais se articulam, dialoga com o pensamento de Foucault na questão dos "aparatos de conhecimento". Isso ocorre na medida em que os algoritmos desempenhariam o papel de instrumentos de conhecimento "por meio dos quais o poder seria exercido" (2017, p. 14).

Em razão disso, qual seja a interface entre algoritmos e poder, Beer (2017) sublinha a necessidade de maior transparência em relação aos sistemas algorítmicos. Ainda, sugere a análise política dos "processos algorítmicos" para que se possa

> [...] examinar a maneira pela qual os algoritmos são parte de racionalidades mais amplas, de programas mais amplos de mudança social e de desenvolvimento. Isso significa pensar sobre o conceito de algoritmo como também sendo parte das dinâmicas de poder (BEER, 2017, p. 15, tradução nossa)[93].

Aprofundando a discussão política, Tobias Matzner (2017) defende que o debate sobre a governança/ética algorítmica não deve se restringir à transparência dos sistemas e à abertura dos *black boxes*[94]. Com isso, não pretende negar a importância da transparência, mas destacar a necessidade de se debruçar sobre as relações de poder e os movimentos de subjetivação[95] que acontecem por meio dos algoritmos, especialmente daqueles empregados na vigilância baseada em dados.

Para tanto, como instrumento teórico de análise, Matzner (2017) pondera que a sociedade disciplinar, de Foucault, não mais seria suficiente para descrever e analisar as relações de poder na sociedade de informação, salvaguardados alguns elementos ainda aplicáveis. Segundo ele, os escritos de Deleuze, em seu *Post Scriptum* (1992), traduziriam com maior fidelidade a nova configuração sociopolítica, haja vista a organização social em rede, o tempo contínuo — aprendizado perpétuo —, a constante mudança das normas e a subjetividade moldada pelo autocontrole dos indivíduos.

---

[93] Cf. texto original: "[...] to examine the way that algorithms are part of broader rationalities, broader programs of social change and development. This is to think about the notion of an algorithm as also being a part of power dynamics".

[94] Cf., *supra*, nota 46.

[95] Cf. Heyes (TAYLOR, 2008, cap. Subjetividade e Poder) para uma elucidação quanto à subjetivação em Foucault: "[*assujettissement*] descreve um duplo processo das ações de poder em relação aos indivíduos que é, a um só tempo, negativo e positivo. Primeiro, *assujettissement* capta a ideia de que somos sujeitados ou oprimidos por relações de poder. Quando se nos impõe uma norma (que Foucault entende como um padrão ao qual os indivíduos são presos pelo qual as populações são definidas), somos pressionados a segui-la. Nesse sentido, *assujettissement* descreve um processo de constrangimento e limitação. [...] Para Foucault, no entanto, o poder também desempenha um papel positivo: ele permite certas posições-sujeito (ou certas ações ou capacidades para o indivíduo). "(p. 204). E ainda: "qualquer processo de *assujettissement* acontece em dois níveis: na gestão do corpo social e na gestão das forças disciplinares que atuam sobre o corpo do indivíduo" (p. 218).

Partindo disso, Matzner (2017) retoma os conceitos de normatização e de normalização para reforçar o argumento de que o novo contexto sociopolítico seria melhor compreendido pelas lentes da sociedade de controle. A normatização se referia à existência prévia de normas, cujo cumprimento pelos indivíduos era examinado e imposto por meio das técnicas disciplinares. Na normalização, por sua vez, partia-se do conjunto de dados existente, por meio do qual se identificavam padrões e relações, delimitavam-se parâmetros de normalidade e, a partir disso, construíam-se normas para, então, serem aplicadas. Com isso, se verifica que as lógicas são diametralmente opostas; entretanto, a observação desempenha, em ambas, papel central.

Na lógica disciplinar, a observação e o registro das informações ocorriam de forma regular e sistemática. Os dados dos indivíduos, obtidos a partir das instituições disciplinares, transformaram- se em instrumentos de controle político. A observação constante permitia a atualização das informações, que eram utilizadas para examinar os sujeitos. As rotinas eram fixas, os espaços disciplinares, fechados, e as normas aplicadas eram estáveis, impostas na tentativa de se homogeneizarem os indivíduos.

Por sua vez, na contemporaneidade, vislumbra-se que a observação não se restringe a determinado grupo de pessoas, mas se dá indistintamente à população como um todo, não estando contingenciada pelos limites físicos e temporais do confinamento nas instituições disciplinares. Com isso, e em razão do enorme volume de dados disponíveis, as normas teriam se tornado muito fluidas e mutáveis, em face do que a disciplina teria passado a ocorrer de maneira heterogênea e espaçada.

Em face disso, seria possível observar diversos paralelos entre as sociedades disciplinar e de controle e o regime de vigilância nas sociedades contemporâneas, precisamente quanto às rotinas de observação e de descrição dos sujeitos. Para tanto, Matzner (2017) retoma as explicações de Foucault sobre o surgimento da concepção de *delinquente* enquanto passagem do foco de análise do ato criminoso para a personalidade do agente do delito. Com isso, o momento da disciplina seria deslocado para antes da própria instituição disciplinar.

Assim, seria possível observar, na figura do *delinquente*, um dos elementos foucaultianos ainda aplicáveis à sociedade contemporânea. Isso dar-se-ia em razão dos métodos de vigilância orientados por dados que, utilizando técnicas preditivas, voltar-se-iam para a construção de perfis dos prováveis delinquentes. Esse quadro, na visão de Matzner (2017), representaria uma retomada da individualização segundo Foucault,

concomitantemente ao dividualismo de Deleuze (1990)[96], configurando uma intersecção entre elementos das duas teorias.

Diante de uma visão ampla, entretanto, a aproximação maior se dá com a sociedade de controle, sendo possível verificar elementos da sociedade disciplinar sobretudo nas fronteiras da sociedade liberal, cada qual produzindo efeitos subjetivadores diferentes.

Outra perspectiva sobre o tema é apresentada por Paul de Laat (2019), que procura explorar a situação dos algoritmos preditivos a partir da sociedade disciplinar. Para tanto, ele se posiciona contrariamente à ideia de que a teoria de Foucault seria insuficiente para analisar as relações de poder na sociedade contemporânea, em contraponto ao pensamento de Matzner.

De Laat (2019) escreve que, com a crise das instituições disciplinares e com o surgimento das sociedades em rede, teria surgido o posicionamento de que o panopticismo não mais se aplica à sociedade contemporânea. Entretanto, na visão do autor, o panopticismo não apenas conserva seu valor explicativo, como se manifesta, agora, de maneira potencializada, no que denominou de "polipanóptico".

A expressão refere-se justamente à ideia de que os indivíduos, antes sob vigilância oculta, no espaço fechado das instituições disciplinares, agora se encontram sob um regime de vigilância ubíqua e irrestrita. Com isso, os dados gerados são armazenados em *data sets* que se comunicam entre si, de maneira que as diversas esferas da vida se tornam conectadas e que a vigilância, antes restrita aos espaços de confinamento, passa a ser informada por dados de distintos setores e contextos, conformando algo como uma supervigilância (DE LAAT, 2019).

De Laat (2019) discorre ainda sobre a questão da governança por disciplina (*discipline governance*). Na acepção original de Foucault, a governança por disciplina se referia ao processo em que os indivíduos eram observados, analisados e examinados, e aqueles tidos como anormais, em relação às normas já existentes, eram, então, disciplinados. Com isso, pretendia-se que os corpos dos indivíduos, tornados dóceis, fossem homogeneizados por meio do cumprimento às normas previamente institucionalizadas.

Como contraponto, difundiu-se a concepção de uma passagem da governança disciplinar para a governança de [grupos de] risco (*risk governance*). Isso se deu na medida em que os indivíduos passaram a ser tomados como '*dividuos*', tendo seus dados

[96] "In fact, his Deleuzian perspective has inspired important steps in the discussion of data-based surveillance. It moves the focus away from the effects of being watched towards what can be done with the results of being watched, in particular data. (…) But (…) Foucault also has important things to say about the use of data that are still relevant today. In particular, *Discipline and Punish* provides a rewarding starting point for looking at the details of data processing practices, to which Deleuze alludes, and their effects on subjects. In fact, in many of the areas where data-based surveillance is used, subjectivizing moments happen." (MATZNER, 2017, p. 31).

fragmentados e armazenados em bases de dados. Com isso, as análises preditivas, especialmente nos campos de segurança e de justiça, passaram a se focar na identificação de padrões e, assim, de grupos de indivíduos que representassem risco. As ações de controle e de disciplina deixavam de se concentrar em indivíduos, para se concentrar em grupos; não mais ocorriam de modo puramente corretivo, mas, antes, de maneira preventiva.

No atual contexto, entretanto, ter-se-ia um retorno à lógica da governança disciplinar, uma vez que os dados fragmentados e utilizados para mineração e para identificação de padrões não apenas indicam grupos de risco, mas passam a indicar indivíduos de risco. Assim, ter-se-ia um retorno à disciplina individual, agora reconfigurada como governança de indivíduos de risco (DE LAAT, 2019).

No que toca à questão do delinquente, De Laat (2019) critica ainda a interpretação de Matzner de que a figura do "deliquente", em Foucault, seria já um precursor do uso de previsões algorítmicas. Ele escreve que, diferentemente dos especialistas de Foucault, que estudavam a biografia do condenado segundo uma perspectiva causal, os algoritmos preditivos da atualidade indicariam a existência de Suspeitos antes mesmo da ocorrência de qualquer crime ou delito, sem qualquer relação de causalidade, justamente pela configuração técnica dos sistemas que operam por *machine learning*.

De Laat (2019) se opõe a Matzner no tópico da normatização *vs*. normalização. Matzner (2017) expõe, em seu texto, que a vigilância, sob a lógica contemporânea de fragmentação dos dados e a sua utilização política, configura um quadro de normalização: a norma não está previamente posta, mas se constitui a partir da mineração dos dados e da identificação de padrões. A partir disso, dão-se o controle dos indivíduos tidos como anormais e a constituição das normas: "aqui o normal vem em primeiro lugar, e a norma é deduzida a partir dele[97]" (MATZNER, 2017, p. 36).

Ao contrário, De Laat (2019) compreende que o quadro é melhor descrito pela normatização: o desenvolvimento de sistemas com aprendizado de máquina exige que os algoritmos sejam treinados com variáveis de referência. Para tanto, o desenvolvedor deve fornecer parâmetros pelos quais o sistema irá se orientar, o que, na visão de De Laat (2019), constitui verdadeiras normas institucionalizadas. Assim, a previsão fornecida pelo sistema algorítmico constitui a própria identificação de indivíduos anormais, cujos perfis sejam identificados como destoantes da norma fornecida previamente pela instituição. Em resumo, a norma seria, em verdade, pré-existente, estando alinhada com a lógica disciplinar de Foucault.

[97] Cf. no original: "here the normal comes first and the norm is deduced from it".

Segundo a lógica clássica da sociedade disciplinar, a anormalidade é punida a partir do momento em que identificado o descumprimento da norma: pune-se o desvio concreto, a ação criminosa. Com o surgimento da figura do delinquente, na genealogia de Foucault, continua-se punindo o delito, mas agora com foco no criminoso ao invés da ação. Posteriormente, com as técnicas algorítmicas preditivas e com a recente capacidade de se identificar não apenas grupos, mas indivíduos de risco, o espaço do delinquente seria ocupado pelo do Suspeito. Assim, a técnica disciplinar corretiva adquire contornos preventivos: a norma não foi ainda violada, porém o indivíduo já se encontra sob a iminência de receber uma punição disciplinar – muitas vezes antes mesmo da violação normativa, agora, porém, sem o conhecimento de quais normas estaria violando ou de qual seria o comportamento desviante[98].

Tendo concluído que a tecnologia de *machine learning* e os algoritmos preditivos revestem-se de caráter disciplinar, De Laat (2019) retoma as reações dos indivíduos à disciplina a eles imposta na sociedade disciplinar: a docilidade e a internalização do olhar vigilante e das normas institucionalizadas. Ele, então, questiona a reação dos indivíduos a essas novas técnicas disciplinares.

A nível individual, ele conclui não existir grande resistência por falta de conhecimento dos indivíduos sobre o uso de suas informações e pela própria opacidade dos sistemas algorítmicos, seja ela inerente, seja imposta. A nível coletivo, ele observa que, em razão da mobilização de grupos diversos – academia, sociedade civil, empresas –, tem-se uma crescente movimentação para exigir o cumprimento de diretrizes éticas e de bom uso na utilização das tecnologias de informação.

Dessarte, e ainda que diante dos traços kafkaescos da situação, segundo a visão de De Laat (2019), ou talvez, em razão dos traços kafkaescos, destaca-se a necessidade de um controle externo sobre as atividades algorítmicas preditivas, a fim de se garantir que a governança ética seja devidamente realizada. Adicionalmente, a transparência desempenha a importante função de evitar, ao menos, que as *data-based decisions* sejam arbitrárias (DE LAAT, 2019).

Uma última observação pode ser feita quanto à camada política de análise do contexto, em relação à qual De Laat (2019) retoma e reforça a posição de Matzner (2017) quanto à necessidade de as relações de poder envolvidas nos processos algorítmicos e de inteligência artificial serem questionadas. A discussão remete diretamente à essência das ideais foucaultianas e possibilita enxergar a governança algorítmica e de IA por outra ótica.

[98] De Laat (2019) cita, como exemplos de punições, a negativa de contrair empréstimo no banco, a seleção para ser revistado no aeroporto e mesmo o impedimento de embarcar no avião.

## 2.3 A disciplina e o controle pela informação: *Capitalismo de Vigilância* e a nova lógica de acumulação

Seguindo a discussão sobre relações de poder nos processos algorítmicos e de IA, encontra-se em Shoshana Zuboff (2015) um interessante ponto adicional, focado, agora, nos fenômenos econômicos e na nova lógica de acumulação baseados na vigilância: o Capitalismo de Vigilância. Zuboff (2015) aponta para o fato de que a nova lógica teria surgido a partir de uma crise no capitalismo ocidental, que passa a ser orientado pela acumulação de informações objetivas e subjetivas sobre os indivíduos, bem como a interferir em seu comportamento (*everydayness commodification*).

Com a nova lógica informacional se expandindo e se tornando hegemônica, teriam se alterado as relações entre os indivíduos e as companhias. No contexto anterior, as empresas operavam sob um regime de reciprocidade entre os capitalistas e os empregados, tidos, ao mesmo tempo, como força de trabalho e como consumidores dos itens produzidos, relação que se refletia positivamente em termos democráticos. Nas palavras de Zuboff:

> A forma de mercado valorizava intrinsecamente suas populações de indivíduos recém modernizados como sua fonte de funcionários e clientes; dependia de suas populações de formas que, ao longo do tempo, levaram a reciprocidades institucionalizadas. Em troca de seus rigores, a forma oferecia um quid pro quo consistente com as características de autocompreensão e demanda de suas populações[99] (2015, p. 80, tradução nossa).

No novo contexto, por sua vez, a reciprocidade não encontra espaço, tendo em vista que a relação empregado/consumidor não é replicada nos *hyperscale businesses*. Isso se dá na medida em que os capitalistas de vigilância (*surveillance capitalists*) atuam como intermediários na nova economia: seus consumidores imediatos são empresas que desejam empregar os bens de vigilância (*surveillance assets*) para modular o comportamento dos indivíduos, levando-os a consumirem seus produtos e serviços. Nessa relação, os sujeitos são simultaneamente objetos, fontes de informação objetiva e subjetiva para os capitalistas de vigilância, e consumidores, estando a variável "força de trabalho" ausente da equação.

Em face disso, se tornam visíveis a impessoalidade formal e o distanciamento entre as firmas e os sujeitos. Para tanto, e observando o ciclo da informação, os dados seriam desagregados, para só depois serem reconstituídos, com a construção dos perfis dos

[99] Tradução livre do trecho: "The market form intrinsically valued its populations of newly modernizing individuals as its source of employees and customers; it depended upon its populations in ways that led over time to institutionalized reciprocities. In return for its rigors, the form offered a quid pro quo that was consistent with the self-understanding and demand characteristics of its populations" (ZUBOFF, 2015, p. 80).

indivíduos. Os sujeitos permaneceriam, assim, distantes dos capitalistas de vigilância, mas estariam sendo perpetuamente observados, disciplinados, controlados, subjetivados por eles. Esse traço de recolhimento e de armazenamento das informações individuais se manifesta por meio da vigilância, em sua lógica de extração de dados. Tais considerações ligam fortemente a descrição de Zuboff ao pensamento de Deleuze, com suas ideias sobre a sociedade em rede e os indivíduos.

Também nesse ponto, as ideias de Zuboff (2015) aproximam-se, em grande medida, do pensamento de De Laat (2019), quando trata da governança de indivíduos de risco[100]. Isso se dá, na medida em que, os sujeitos, em determinada parte do processo, seriam tratados como meros indivíduos, para, logo após, recobrarem a condição de indivíduos, assim considerados para fins de *marketing* das empresas e maximização dos seus lucros.

Para tanto, e retomando o ponto da acumulação, o *Capitalismo de Vigilância* trabalharia com a acumulação de informações sobre seus objetos, tendo em vista que bens de vigilância (*surveillance assets*) em maior quantidade permitiriam a criação de análises mais precisas. Observa-se, assim, que maior importância é relegada à quantidade, em detrimento da qualidade das informações, o que exige investimentos em vigilância (*surveillance investiments*) para produzir dados. Esses investimentos em vigilância poderão ser observados na Seção posterior, em que, a Lei n° 13.675, de 11 de junho de 2018 (Lei do Susp) institui o Sinesp como ferramenta para integração nacional das bases de dados e, sob a sombra do Sistema, está em desenvolvimento o *Sinesp Big Data*, cujas ferramentas permitirão robustecer os recursos para o policiamento preditivo.

As características anteriormente mencionadas, quando visualizadas em conjunto, terminariam por constituir a figura do *Big Other*[101], personificação da vigilância permanente e sem fronteiras, permeando todos os espaços da sociedade em rede. Com isso, Zuboff (2015) escreve que teria ocorrido uma transição: os indivíduos, anteriormente dotados de agência e, com isso, capazes de optar por se conformar ou não com os mecanismos de disciplina e de

[100] O autor cunha a expressão no contexto da vigilância preditiva. No entanto, entende-se que o conceito possa ser estendido à sociedade informacional como um todo.

[101] Zuboff define a figura do *Big Other* como "(…) a ubiquitous networked institutional regime that records, modifies, and commodifies everyday experience from toasters to bodies, communication to thought, all with a view to establishing new pathways to monetization and profit. Big Other is the sovereign power of a near future that annihilates the freedom achieved by the rule of law. It is a new regime of independent and independently controlled facts that supplants the need for contracts, governance and dynamism of a market democracy. Big Other is the 21st-century incarnation of the electronic text that aspires to encompass and reveal the comprehensive immanent facts of market, social, physical, and biological behaviours" (ZUBOFF, 2015, p. 81–82).

autocontrole, estariam agora esvaziados de autonomia, respondendo automaticamente às modulações comportamentais dos capitalistas de vigilância.

Essa visão proporciona interessante contraste com o pensamento de De Laat (2019): onde Zuboff enxerga a superação dos mecanismos disciplinares e de controle, assim como do modelo panóptico, De Laat vislumbra, na vigilância perene, o instrumento para a intensificação do panopticismo, fazendo referência à figura do pluripanóptico. Com isso, pretende expressar a ideia de que não apenas a teoria de Foucault ainda seria aplicável, como também os mecanismos disciplinares teriam sido intensificados na nova lógica social e econômica.

# 3 O USO DE IA PELA ADMINISTRAÇÃO PÚBLICA: MAPEAMENTO E RESULTADOS

Em vista de todo o exposto, sabe-se que o emprego de sistemas algorítmicos e de IA sob a lógica do capitalismo de vigilância, do polipanóptico/*Big Other*[102] e de seus mecanismos disciplinares e de controle dialoga diretamente com a democracia e coloca em disputa direitos fundamentais dos sujeitos. As interações entre governança e democracia, especialmente no que se refere à transparência e à liberdade, ficam ainda mais evidentes no contexto das tecnologias informacionais. Assim, e frente ao caráter intimamente subjetivador dos mecanismos preditivos, sua utilização pelo setor público demanda a prática de uma transparência significativa.

A acumulação com base na informação e a utilização da vigilância como instrumento de disciplina dos corpos reconfiguram as relações de poder, os regimes de verdade e as subjetividades. Com isso, a abertura das *black boxes*, com a garantia de transparência nos processos, reveste-se de grande importância, ao que Matzner acrescenta:

> [...] abrir *black boxes* é um elemento importante para uma ética ou governança de algoritmos. No entanto, [o movimento de transparência] tem de ser incorporado num quadro social, institucional e técnico mais amplo, que analise as mudanças de poder e as subjetividades em vez de preconceitos e exatidão nos dados e algoritmos[103] (2017, p.45, tradução nossa).

Com isso, e considerando os encadeamentos éticos e políticos da IA e dos sistemas algorítmicos, viu-se como relevante o esforço de compreender o cenário brasileiro no tema. Para tanto, a presente pesquisa partiu do empenho inicial de situar o País em relação ao novo contexto técnico-informacional, mapeando as iniciativas em desenvolvimento e em execução pela administração pública federal[104].

A partir de então, identificou-se o projeto *Sinesp Big Data e IA para Segurança Pública*, sabendo que o projeto se orienta a aumentar o conhecimento sobre a realidade criminológica brasileira para, com isso, tornar mais eficazes as ações das forças de segurança pública. Assim, dada a sensibilidade do tema, decidiu-se testar o nível de transparência do projeto e avaliá-lo em termos tecnopolíticos.

---

[102] Cf. *supra*, nota 102.
[103] Tradução livre do trecho: "[...] opening black boxes is an important element for an ethics or governance of algorithms. However, it has to be embedded in a larger social, institutional, and technical picture that analyzes shifts in power and subjectivities rather than biases and correctness in data and algorithms."
[104] Arquivo completo disponível no Apêndice [Digital] A.

A seguir, será discutido o *design* da pesquisa, apresentando o mapeamento realizado e as informações públicas obtidas sobre o *Sinesp Big Data e IA*, assim como as solicitações de acesso à informação encaminhadas. Em seguida, serão analisados os resultados.

## 3.1 O *design* da pesquisa exploratória e sua execução

Conforme apresentado na Seção anterior, a pesquisa exploratória partiu do esforço inicial de mapear as iniciativas algorítmicas e de IA em desenvolvimento ou em uso pelo setor público federal. Entretanto, a falta de um registro oficial e central dos sistemas implementados impediu a realização de uma exploração rigorosamente quantitativa. Brauneis e Goodman, que conduziram pesquisa empírica sobre os algoritmos governamentais preditivos nos Estados Unidos, escreveram sobre dificuldades semelhantes:

> Não há um registro central de algoritmos em uso pelos governos, e os algoritmos não são naturalmente visíveis da mesma forma que, por exemplo, arranha-céus ou pontes. Assim, não temos meios de saber quantos algoritmos estão atualmente em uso, quem os desenvolveu ou que governos os estão utilizando. Sem esse conhecimento, não podemos, de qualquer forma, desenvolver nenhum método de amostragem para o uso de algoritmos que nos permita generalizar as nossas descobertas[105]. (BRAUNEIS; GOODMAN, 2017, p. 136, tradução nossa).

Tendo em vista esse contexto, e utilizando-se de informações públicas, realizou-se amplo levantamento documental[106]. Inicialmente, foram tabulados os nomes e as URLs dos Ministérios, das principais instituições governamentais, e dos principais grupos midiáticos brasileiros. Com essas informações, foram realizadas pesquisas booleanas na ferramenta de pesquisa personalizada do Google (cse.google.com), sendo, os resultados obtidos, sistematizados para a identificação das iniciativas tecnológicas[107].

---

[105] Tradução livre do trecho: "There is no central registry of algorithms in use by governments, and algorithms are not naturally visible in the way that, say, skyscrapers or bridges are. Thus, we have no means of knowing how many algorithms are currently in use, who has developed them, or which governments are using them. Without that knowledge, we cannot develop any method for sampling algorithm use in any way that would allow us to generalize from our findings."

[106] A pesquisa utilizou, como base, o manual de investigação produzido pela Web Foundation e utilizado como metodologia no artigo: **Algorithms and Artificial Intelligence in Latin America: A Study of Implementation by Governments in Argentina and Uruguay**, World Wide Web Foundation, disponível em http://webfoundation.org/docs/2018/09/WF_AI-in-LA_Report_Screen_AW.pdf ). O *Research Handbook* se encontra disponível em: https://docs.google.com/document/d/10f75NIyRMSXePr8VvTxpXTzvgRJzhbA7jvjK4S2Cdso/edit?ts=5aae376c#heading=h.2et92p0.

[107] Nesse estágio foram registradas mais de 90 (noventa) iniciativas. A lista completa encontra-se disponível no apêndice digital.

A partir da identificação dos sistemas, e considerando o elevado número de iniciativas provenientes do Poder Judiciário, decidiu-se por iniciar comunicações eletrônicas com os responsáveis pelos projetos. Para tanto, as tentativas de contato e o recebimento das respostas às solicitações de informações tiveram como marco temporal os meses de outubro e de novembro de 2019.

Em relação às mensagens eletrônicas encaminhadas diretamente aos gestores de cada sistema, as solicitações não retornaram resultados significativos. Foi árduo identificar, inicialmente, os responsáveis pelas respectivas iniciativas, bem como suas informações de contato. Nos casos em que foi possível localizá-los, os questionários encaminhados não retornaram preenchidos.

Ocorreu que muitos não retornaram o contato inicial; outros interromperam a troca de mensagens após o envio do questionário; outros, ainda, alegaram a necessidade de fazer cumprir determinado procedimento interno para que as respostas fossem fornecidas, sendo preciso que o diretor da unidade autorizasse o preenchimento do questionário. O único projeto, entre os selecionados, que retornou prontamente o contato, inclusive encaminhando o questionário preenchido, foi o projeto *Cérebro*[108], do Conselho Administrativo de Defesa Econômica (CADE).

Assim, buscando melhor compreender as iniciativas de IA desenvolvidas e implantadas pelo Poder Judiciário, enviou-se solicitação de acesso à informação diretamente ao Conselho Nacional de Justiça (CNJ). Em face disso, foi respondido que, haja vista a extensão do pedido formulado e do trabalho demandado para levantar as informações solicitadas, não seria possível responder os questionamentos[109]. Anota-se que, em razão de constrições temporais da autora, não se recorreu da resposta obtida.

Então, considerando as dificuldades que se apresentaram; a existência de discussões tecnopolíticas em Foucault, Deleuze e Zuboff sobre o regime institucionalizado de vigilância, assim como os numerosos registros de controvérsias quanto à aplicação das tecnologias

---

[108] Nas palavras de Felipe Roquete (2019), o projeto objetiva "desenvolver ferramentas tecnológicas e técnicas que possibilitem agregar qualidade às investigações de infrações à ordem econômica, bem como a adoção de estratégias proativas de detecção de cartéis". ROQUETE, Felipe. Questionário semiestruturado (nov. 2019). Questionário respondido por e-mail e disponível integralmente no Anexo V.

[109] Segundo a comunicação eletrônica encaminhada pela ouvidoria do CNJ (2019), "Neste momento a solicitação em tela não está disponível para tratamento no âmbito deste Conselho por força de insuficiência de registros próprios dos Acordos Técnicos e dos projetos que julgamos pertinentes ao pedido de informação. Complementarmente, por se tratar de demanda que exige esforço e recursos adicionais para análise, produção e controle das informações solicitadas, **apresentamos nossas escusas pela falta de condições para gerar tais informações, uma vez que demandaria esforços exclusivos. Diante de tais fatos, consideramos prejudicada a possibilidade de atendimento ao pleito**" (grifo nosso). A íntegra do questionário e da resposta recebida encontra-se disponível no Anexo IV.

algorítmica e de IA à área de segurança pública, selecionou-se o *Sinesp Big Data e Inteligência Artificial para Segurança Pública*[110]. O projeto encontra-se em desenvolvimento pelo MJSP, em parceria com o Departamento de Computação da UFC. Pretendeu-se avaliá-lo em termos éticos e de dinâmicas políticas, especialmente quanto aos processos de subjetivação e de disciplina realizados por ele/por meio dele.

A partir de então, realizou-se novo levantamento de informações sobre o projeto e, em face de dados não disponíveis publicamente, elaborou-se questionário sobre os processos de desenvolvimento, implementação e execução do *Sinesp Big Data*. O questionário[111] foi enviado por meio de solicitações de acesso à informação[112] ao MJSP e à UFC, e encaminhado diretamente aos coordenadores da equipe de desenvolvimento do sistema, com os quais se buscou obter informações adicionais sobre o projeto.

Em face das solicitações enviadas, o quadro de dificuldades se repetiu, tendo sido recebidas respostas incompletas, sob a alegação de sigilo informacional[113]. Alegou-se que, em razão da promulgação da Lei n° 13.675, de 11 de junho de 2018 (Lei do Susp), e da fase inicial do projeto *Sinesp Big Data*, não seria "oportuno" compartilhar as informações solicitadas. Quanto à comunicação com os coordenadores da equipe, foi possível iniciar a comunicação direta, mas, a partir do envio do questionário, não se obteve retorno.

Todas as barreiras de acesso a informações aqui registradas apontam para a opacidade do sistema e para a falta de engajamento público no desenvolvimento do projeto. Veja-se, então, na Seção a seguir, a análise realizada a partir dos dados e dos resultados obtidos.

## 3.2 Discussão dos resultados

O projeto *Sinesp Big Data e IA* foi criado como meio e instrumento da Política Nacional de Segurança Pública e Defesa Social (PNSDPS). Como tal e para melhor compreender o próprio projeto, observe-se brevemente o Plano.

---

[110] Cf. **Ministério entrega aos estados primeiras ferramentas de *Big data* e Inteligência Artificial para combater a criminalidade — Ministério da Justiça e Segurança Pública**. Brasília, 2019. Disponível em: <https://www.justica.gov.br/news/collective-nitf-content-1566331890.72>. Acesso em: 4 nov. 2019, ("'Precisamos saber mais sobre os crimes, onde, como e quando eles ocorrem para ter uma orientação mais eficaz das ações das forças de segurança pública", afirmou o ministro Sergio Moro [...]'").

[111] O modelo de questionário enviado encontra-se disponível para conferência no apêndice B.

[112] Amparadas pela Lei nº 12.527/2011 (Lei de Acesso à Informação).

[113] Especificamente em relação à resposta enviada pela UFC, o coordenador do projeto junto à Universidade afirmou estar vinculado a um termo de confidencialidade com o próprio MJSP.

### *3.2.1 A criação da Política Nacional de Segurança Pública e Defesa Social*

Em 11 de junho de 2018, foi assinada a Lei nº 13.675, conhecida como Lei do SUSP, por meio da qual foi instituído o Sistema Único de Segurança Pública (SUSP) e criado o PNSDPS, ambos se orientando pela atuação integrada dos órgãos de segurança pública e de defesa social:

> **Art. 1º** Esta Lei institui o Sistema Único de Segurança Pública (Susp) e cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS), com a **finalidade de preservação da ordem pública e da incolumidade das pessoas e do patrimônio**, por meio de **atuação conjunta, coordenada, sistêmica e integrada dos órgãos de segurança pública e defesa social** da União, dos Estados, do Distrito Federal e dos Municípios, em articulação com a sociedade (BRASIL, 2018, grifo nosso).

A partir do texto legal, é possível observar os discursos de *eficiência*, de *otimização* e de *controle social* a permear os princípios. Ainda, estão previstos o respeito ao ordenamento jurídico, às garantias individuais e coletivas, aos direitos humanos, e o compromisso com a transparência:

> **Art. 4º** São princípios da PNSPDS:
> I - **respeito ao ordenamento jurídico e aos direitos e garantias individuais e coletivos**;
> II - proteção, valorização e reconhecimento dos profissionais de segurança pública;
> III - **proteção dos direitos humanos, respeito aos direitos fundamentais e promoção da cidadania e da dignidade da pessoa humana**;
> IV - **eficiência** na prevenção e no controle das infrações penais;
> V - **eficiência** na repressão e na apuração das infrações penais;
> VI - **eficiência** na prevenção e na redução de riscos em situações de emergência e desastres que afetam a vida, o patrimônio e o meio ambiente;
> VII - participação e **controle social**;
> VIII - resolução pacífica de conflitos;
> IX - uso comedido e proporcional da força;
> X - proteção da vida, do patrimônio e do meio ambiente;
> XI - **publicidade das informações não sigilosas**;
> XII - promoção da **produção de conhecimento sobre segurança pública**;
> XIII - **otimização** dos recursos materiais, humanos e financeiros das instituições;
> XIV - simplicidade, informalidade, economia procedimental e celeridade no serviço prestado à sociedade;
> XV - relação harmônica e colaborativa entre os Poderes;
> XVI - **transparência, responsabilização e prestação de contas** (BRASIL, 2018, grifo nosso).

A leitura dos dispositivos leva à indagação quanto à maneira como se dará o cumprimento das disposições e a compatibilização da lógica de acumulação informacional com a garantia de respeito aos direitos fundamentais. Frente aos obstáculos enfrentados para o levantamento de informações, questiona-se a efetividade das previsões de "transparência, responsabilização e prestação de contas".

Seguindo, verifica-se que o texto estabeleceu, como um dos meios e instrumentos para implementação do Plano, o Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas (SINESP), ao qual se vincula o desenvolvimento do projeto *Sinesp Big Data*. A finalidade expressa do Sistema Nacional é gerenciar dados e políticas relacionados ao tema geral da segurança pública:

> **Art. 8º** São meios e instrumentos para a implementação da PNSPDS:
> [...] b) o Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas (Sinesp);
> [...]
> **Art. 35**. É instituído o Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas (Sinesp), com a **finalidade de armazenar, tratar e integrar dados e informações para auxiliar na formulação, implementação, execução, acompanhamento e avaliação das políticas** relacionadas com:
> I - segurança pública e defesa social;
> II - sistema prisional e execução penal;
> III - rastreabilidade de armas e munições;
> IV - banco de dados de perfil genético e digitais;
> V - enfrentamento do tráfico de drogas ilícitas (BRASIL, 2018, grifo nosso).

Quanto aos objetivos específicos do SINESP, sobressaem-se a orientação de atuação integrada dos órgãos de defesa pública e de segurança social, bem como a promoção da interoperabilidade das redes de informação. Esse cenário representa, com clareza, a figura do polipanóptico (DE LAAT, 2019), com suas múltiplas redes de vigilância e a comunicação entre as bases de dados, sobre a qual o autor escreve:

> [...] o *machine learning* moderno funciona com base em um elaborado conjunto de bancos de dados que foram reunidos em uma variedade de contextos.
> Isso pode ser interpretado usando a metáfora do panóptico? Eu acho que este é de fato o caso, em um duplo sentido. No que diz respeito à instituição "focal", seus sujeitos devem assumir que **dados relevantes são gerados e coletados o tempo todo - um panóptico de rotina**. **Mas, além disso, eles devem assumir que, em muitos outros panópticos em que estão enredados, outros traços digitais sobre os eles são monitorados e armazenados. Subsequentemente, estes dados podem ser importados de volta para a instituição focal que estamos considerando**. Todas essas importações impulsionam consideravelmente os esforços de *machine learning*, muitas vezes de formas surpreendentes. **Com isso, os olhares panópticos de muitos contextos diferentes são acoplados: um "polipanóptico". Muitos domínios da vida, até agora separados, entrelaçam-se**[114] (DE LAAT, 2019, p. 5, grifo nosso).

[114] Tradução livre. No original: "[...] [M]odern machine learning operates on an elaborate pool of datasets that have been gathered in a variety of contexts. Can this be interpreted using the metaphor of the Panopticon? I think this is indeed the case, in a double sense. As far as the "focal" institution is concerned, its subjects must assume that relevant data are generated and collected all the time – a routine Panopticon. But in addition, they must assume that in many other Panoptica in which they are entangled, other digital traces about the are monitored

Avançando na análise do Sistema, há, ainda, a previsão de padrões éticos para o seu funcionamento, entre eles a disponibilidade e a confidencialidade dos sistemas informatizados, além da obrigação legal de fornecimento e de atualização dos dados pelos entes federados. Veja-se:

> **Art. 36**. O Sinesp tem por objetivos:
> I - **proceder à coleta, análise, atualização, sistematização, integração e interpretação de dados e informações relativos às políticas de segurança pública e defesa social**;
> II - **disponibilizar estudos, estatísticas, indicadores e outras informações para auxiliar na formulação, implementação, execução, monitoramento e avaliação de políticas públicas**;
> III - **promover a integração das redes e sistemas de dados e informações de segurança pública e defesa social, criminais, do sistema prisional e sobre drogas**;
> IV - **garantir a interoperabilidade dos sistemas de dados e informações, conforme os padrões definidos pelo conselho gestor**.
> Parágrafo único. O Sinesp adotará os **padrões de integridade, disponibilidade, confidencialidade, confiabilidade e tempestividade dos sistemas informatizados do governo federal**.
> **Art. 37**. Integram o Sinesp todos os entes federados, por intermédio de órgãos criados ou *design*ados para esse fim.
> § 1º Os dados e as informações de que trata esta Lei deverão ser padronizados e categorizados e serão fornecidos e atualizados pelos integrantes do Sinesp.
> § 2º **O integrante que deixar de fornecer ou atualizar seus dados e informações no Sinesp poderá não receber recursos nem celebrar parcerias com a União para financiamento** de programas, projetos ou ações de segurança pública e defesa social e do sistema prisional, na forma do regulamento.
> § 3º O Ministério Extraordinário da Segurança Pública é autorizado a celebrar **convênios com órgãos do Poder Executivo que não integrem o Susp, com o Poder Judiciário e com o Ministério Público**, para compatibilização de sistemas de informação e integração de dados, ressalvadas as vedações constitucionais de sigilo e desde que o objeto fundamental dos acordos seja a prevenção e a repressão da violência.
> § 4º **A omissão no fornecimento das informações legais implica responsabilidade administrativa do agente público** (BRASIL, 2018, grifo nosso).

Interessante notar que a promulgação da Lei do SUSP surge como tentativa governamental de reverter a falta de informações sobre políticas de segurança pública, traço apontado pela Edição 2019 do *Anuário Brasileiro de Segurança Pública* como característico do cenário brasileiro. Assim, referenciando os dados apurados em relação a 2018, os autores do *Anuário* escrevem:

> A compilação dos dados de 2018 revela um contexto político e institucional que, mesmo que em patamares diferentes entre si, é muito similar àquele relativo a 2014 [...]. Um contexto em que **alguns dos números agregados da violência**

---

and stored. Subsequently these data may be imported backwards into the focal institution that we are considering. All such imports boost machine learning efforts considerably, often in surprising ways. Thus, the panoptic gazes of many different contexts are coupled together: a "*Polypanopticon*". Many hitherto separated domains of life become intertwined".

> **apresentam quedas consideráveis, mas, paradoxalmente, pouco se sabe sobre as origens e razões desse movimento**.
> **O Brasil não tem a prática de documentar, monitorar e avaliar as políticas setoriais**, o que poderia contribuir para estimular o que deu certo, evitar o que deu errado e tornar sustentáveis no tempo as reduções nos indicadores criminais.
> [...] Se queremos vencer o medo e a violência, precisamos **consolidar repositórios de informações**, bem como monitorar e analisar as principais agendas de problemas e soluções existentes. E, ao mesmo tempo, **criar momentos de reflexão e debate que consigam traduzir fluxos cada vez maiores de dados em conhecimento e boas políticas públicas** (PIMENTEL *et al*., 2019, p. 12–13; grifo nosso).

O escrito é especialmente relevante, na medida em que sistemas algorítmicos e de IA aplicados à segurança pública apresentam elevado potencial de modulação comportamental[115] e de subjetivação. Assim, por se tratar, a segurança, de área particularmente sensível, o emprego dos sistemas tecnológicos exige rigoroso grau de governança ética e de controle dos *outputs* e *outcomes*, requisitos que restam comprometidos diante da falta de registro, de controle e de avaliação das políticas.

Paralelamente, o comentário sobre a necessidade de se "consolidar repertórios de informações" parece sugerir, paradoxalmente, que resistir aos movimentos de subjetivação e de disciplina ocasionados pelo/por meio do uso das tecnologias de informação deve se dar através dos próprios mecanismos disciplinares[116].

Em face do exposto, verifica-se que, apesar das múltiplas previsões de transparência e de disponibilidade dos sistemas informatizados do governo federal, a tentativa de obter informações sobre o *Sinesp Big Data e IA* foi obstaculizada pela opacidade da iniciativa. A seguir, deter-se-á sobre as respostas aos questionários enviados, analisando as informações obtidas relativamente ao projeto.

---

[115] Quanto à questão da modulação e do controle social em relação a tecnologias de policiamento preditivo, Rogério da Costa cita o TIA – *Total "Terrorism" Information Awareness*, projeto norte-americano, cuja estratégia "[...] é rastrear indivíduos, coletando tanta informação quanto possível e usando *softwares* inteligentes e análise humana para detectar suas atividades potenciais. [...] O objetivo básico do projeto é auxiliar analistas a compreender e mesmo prever uma ação futura, no caso, uma ação terrorista. [...] **E com a implantação de um tal projeto, chegamos definitivamente na modulação contínua da sociedade de controle de que nos fala Deleuze, pois deixamos de olhar para as informações como associadas a indivíduos, e sim como relacionadas entre si dentro de um quadro maior**. É justamente essa amostra ou conjunto de dados que deve ser modulado" (2004, p. 165-166, grifo nosso).

[116] Com isso, não se está sugerindo que a subjetivação e a disciplina se dão apenas por meio de tecnologias da informação. Pelo contrário, reconhecesse-se o caráter difuso e onipresente do poder nas relações.

### *3.2.2 O Projeto Sinesp Big Data e IA para Segurança Pública*

O *Sinesp Big Data e Inteligência Artificial para Segurança Pública* é uma "plataforma de processamento, em larga escala, de dados históricos e de fluxo de dados em tempo real, de forma escalável, distribuída e elástica" (JÚNIOR, 2019a)[117]. Trata-se de um projeto público desenvolvido pelo MJSP em cooperação com o Departamento de Computação da UFC[118], inspirado pelas experiências, tidas como exitosas, da Secretaria de Segurança Pública e Defesa Social do Ceará, em conjunto com a própria UFC.

Tais experiências são fruto da *Nova Estratégia de Segurança Pública* (NESP)[119] do estado do Ceará, criada no bojo do *Pacto por um Ceará Pacífico*[120], e estão diretamente relacionadas ao investimento em tecnologia da informação, realizado pelo estado cearense:

> Entendemos que a tecnologia, por si só, não resolve as questões da segurança, mas **ela é um dos mais importantes instrumentos de apoio para a ação das forças policiais, contribuindo tanto para a prevenção de delitos quanto para solucionar os crimes.** O Governo do Ceará tem investido em dispositivos e sistemas que contribuem para aprimorar o trabalho de inteligência policial (GOVERNO DO ESTADO DO CEARÁ, 2019, grifo nosso ).

Entre os sistemas locais desenvolvidos, e que se diz terem inspirado os moldes do *Sinesp Big Data* e IA, encontram-se[121]:

---

[117] Solicitação de acesso à informação respondida por Wanderley José Silva JÚNIOR, Diretor Substituto de Gestão e Integração de Informações, em 16 de outubro de 2019, na forma do Ofício n° 1130/2019/DGI/SENASP/MJ. A íntegra do ofício encontra-se disponível no Anexo II.

[118] O plano de trabalho simplificado do projeto, conforme acesso público pela internet encontra-se disponível no Anexo III.

[119] Cf. **Nova Estratégia de Segurança Pública - Governo do Estado do Ceará**. [s.d.]. Disponível em: <https://nesp.ceara.gov.br/#pacific>. Acesso em: 16 nov. 2019. ("A nova estratégia de combate à violência que está sendo desenvolvida no Ceará se baseia em integração, coordenação, cooperação e responsabilização em diferentes níveis**. Foram feitos investimentos em tecnologia da informação**, em sistemas e dispositivos que favoreçam um trabalho com efetividade e segurança. Estão sendo investidos recursos na motivação, qualificação e contratação de policiais, com ampliação do efetivo, valorização salarial e implementação de um novo plano de carreiras. Com foco no território, além da realização da reestruturação prisional e do sistema socioeducativo do estado, **há um aumento da presença policial nos municípios, o que tem inibido muitos crimes, principalmente contra o patrimônio**. No entanto, dentro da nova estratégia do Governo do Ceará, é entendido que apenas isso não seria bastante para o combate à violência. **Políticas públicas de educação, de redução da pobreza, de cultura, de esporte, e mesmo de saúde, também estão no centro das ações**. Isso vem sendo feito de forma planejada, a partir do atento acompanhamento de indicadores, o que tem mostrado bons resultados") (grifo nosso).

[120] Cf. *supra* nota 105: "O *Pacto por um Ceará Pacífico*é um amplo programa de redução da violência, com ações baseadas no seguinte tripé: 1) Aproximação com a população; 2) Uso intensivo de informações e aperfeiçoamento da inteligência e da investigação; 3) Articulação e integração das agências de segurança pública e justiça.").

[121] Cf. *supra* nota 105.

**Quadro 3: Sistemas de tecnologia da informação desenvolvidos no NESP**

| Sistema | Descrição |
|---|---|
| Centro Integrado de Inteligência e Segurança Pública - Regional Nordeste (CIISPR - NE) | Atuação conjunta do Governo do estado, dos poderes Legislativo e Judiciário, além do Ministério Público, da Defensoria Pública, da sociedade civil, e do Fórum Brasileiro de Segurança Pública, todos participando ativamente na construção do Pacto. |
| Centro Integrado de Inteligência e Segurança Pública Estadual | "[...] sistema de troca de informações baseado em *Big data*, que permite um melhor planejamento, produção de conhecimentos e elaboração de estratégias para o combate à violência." |
| ZOOM Cidade Segura | "Integra vigilância por câmera com sistemas de inteligência artificial, bancos de dados e profissionais capacitados de todas as forças de segurança e diversos órgãos, para garantir cada vez mais a segurança com trabalho, efetividade e inteligência." |
| Videomonitoramento, Tecnologia e Inteligência Policial | "São mais de três mil câmeras de videomonitoramento atuando na prevenção de crimes em Fortaleza e nas principais cidades do interior do estado." |
| SPIA - Sistema Policial Indicativo de Abordagem | "As imagens das câmeras de videomonitoramento são utilizadas pelo SPIA, que é capaz de reconhecer placas de veículos, facilitando a localização de automóveis roubados e usados na prática de diversos crimes. O Sistema melhora os resultados de abordagens policiais, com a identificação prévia dos veículos." |
| Superintendência de Pesquisa e Estratégica de Segurança Pública - SUPESP | "A Supesp realiza estudos, a partir de pesquisas, estatísticas de geoprocessamento e indicadores sociais, para ajudar a elaborar as políticas públicas do Pacto por um Ceará Pacífico. Todos os dados serão agrupados ao *Big data* da Segurança Pública do Ceará, ficando disponíveis para o Sistema de Segurança Pública." |
| Programa Cientista Chefe | "[E]sse programa está desenvolvendo pesquisas aplicadas à segurança pública e a outros setores com cientistas das universidades públicas do Ceará. [...] São, principalmente, pesquisas voltadas para a área de Inteligência Artificial, como o reconhecimento de placas de automóveis e reconhecimento facial. As pesquisas ainda se voltam para melhorar o armazenamento de dados e facilitar seu acesso, tendo como resultado maior agilidade no combate à criminalidade, aproveitando as inovações que estão sendo desenvolvidas." |
| Perícia Forense do Estado do Ceará – PEFOCE | "O Banco de Dados de DNA Forense cadastra perfis genéticos e compartilha as informações |

| | |
|---|---|
| | entre outros órgãos de segurança e perícias de todo o Brasil. A análise de DNA está ajudando a identificar criminosos, a partir de material genético encontrado nos locais dos crimes.” |
| Laboratório de Tecnologia Contra a Lavagem de Dinheiro | “A tecnologia permite analisar grandes volumes de informações bancárias, telemáticas, fiscais, entres outras. O estado pode, dessa forma, bloquear e recuperar o dinheiro provenientes de ações criminosas, como o tráfico de drogas e a corrupção.”. |

Fonte: Nova Estratégia de Segurança Pública - Governo do Estado do Ceará (2019)

Ressalta-se que, entre as informações públicas sobre os sistemas mencionados acima, não foi possível localizar dados sobre seu *design* técnico ou estudos rigorosos sobre os resultados de sua implementação[122]. Entretanto, devido ao escopo da pesquisa e a restrições de tempo, não foram enviadas solicitações de acesso a informações para o levantamento de tais dados.

A título de exemplo, a Seção de resultados do NESP, em relação aos anos de 2017 e 2018, disponibilizada no referido endereço eletrônico, informa ter ocorrido uma redução de 6,2% nas ocorrências de furto; de 15,2% no número de vítimas de crimes violentos contra o patrimônio; de 12% no número de vítimas de crimes violentos letais intencionais, e um aumento de 2,9% no número de armas apreendidas. No entanto, não são mencionadas informações sobre a forma de utilização dos sistemas; sobre a qualidade dos dados nem sobre a governança ética das iniciativas tecnológicas.

Mesmo frente à opacidade do NESP, seus resultados aparentemente ‘positivos’ inspiraram os moldes do *Sinesp Big Data e IA*, idealizado para gerar as seguintes soluções[123]:

**Quadro 4**: **Soluções de tecnologia da informação desenvolvidas no projeto *Sinesp Big Data***

| **Soluções** | **Objetivos** |
|---|---|
| Plataforma *Big Data* | “Base dos sistemas do Sinesp, com tecnologias e soluções para execução em larga escala.” |

[122] Cf. *supra* nota 105.

[123] As respostas recebidas pelas solicitações indicaram, ainda, que as soluções visavam permitir:
“a) A análise de eventos espaço-temporais relacionados com ações delituosas;
b) A busca e visualização dos analíticos sobre dados de segurança pública de todo o país;
c) A detecção de anomalias em dados históricos e fluxo de dados em tempo real;
d) O acompanhamento em tempo real de veículos, pessoas e objetos rastreados através de sensor de geolocalização;
e) O acompanhamento de rotas e **Mancha Criminal Dinâmica**;
f) A identificação automática de fraudes a partir do reconhecimento de padrões associados a este tipo de ações delituosas;
g) **A identificação de relacionamentos entre vetores que compõem o comportamento delitivo: local, agressor, vítima, objetos, ligações telefônicas, transferências bancárias,** etc.” (grifo nosso).

| | |
|---|---|
| Analisador de Crimes | "Proporcionar o georreferenciamento das ocorrências em relação ao tempo e o espaço em que são registradas, possibilitando, por exemplo, a **visualização de rotas de policiamento e mapas de calor dos locais e horários onde mais acontecem crimes**." |
| Painel Analítico | "Permitir a busca de informações em boletins de ocorrência de outros estados e municípios, além de **pesquisas a dados de pessoas, objetos e documentos**. " |
| Painel Governança | "Permitir o acompanhamento das integrações do Sinesp." |
| Processador de Eventos Complexos | "Processar eventos complexos visando a detecção de anomalias." |
| Rastreamento de Objetos Móveis | "[Realizar o] monitoramento inteligente para rápida intervenção, acompanhamento de ocorrências criminais, detecção por sensores, câmeras de segurança, viaturas e agentes de pessoas com restrição de liberdade que fazem uso de tornozeleiras eletrônicas." |
| Aplicativo Móvel para Policial | "(Aplicativo móvel para) gerenciar o policiamento ostensivo e comunitário." |
| Detector de Fraudes | "Identificar fraudes automaticamente a partir do reconhecimento de padrões associados a este tipo de ações delituosas." |
| Redes Delitivas | **Painel analítico de relacionamentos que compõem o comportamento delitivo** |
| Sistema de Indicativo de Abordagem Veicular | "Monitoramento, em tempo real, de veículos que transitem em vias urbanas." |
| Seminário de Transferência Tecnológica | "**Seminários para realização da transferência de tecnologia para a equipe do Ministério da Justiça e Segurança Pública**." |

Fonte: JÚNIOR (2019b, grifo nosso)[124]

Ainda em atenção às solicitações de informação encaminhadas, foram recebidos os seguintes esclarecimentos sobre o projeto:

[124] Solicitação de acesso à informação respondida por Wanderley José Silva JÚNIOR, Diretor Substituto de Gestão e Integração de Informações, em 16 de outubro de 2019, na forma do Ofício n° 1131/2019/DGI/SENASP/MJ. A íntegra do ofício encontra-se disponível no Anexo II.

**Quadro 5: Dados sobre o projeto *Sinesp Big Data e IA para Segurança Pública***

| ***Sinesp Big Data e Inteligência Artificial para Segurança Pública*** | |
|---|---|
| **Unidade Responsável** | DGI (Diretoria de Gestão e Integração de Informações)/ SENASP (Secretaria Nacional de Segurança Pública)/ MJSP (Ministério da Justiça e Segurança Pública) |
| **Desenvolvimento** | Público (Diretoria de Tecnologia da Informação e Comunicação – DTIC/MJSP e Universidade Federal do Ceará - UFC) |
| **Origem dos Dados** | Informação não revelada |
| **Disponibilidade Pública dos Dados** | Informação não revelada |
| **Seleção de variáveis** | Informação não revelada |
| **Variáveis capazes de desencadear discriminação indevida** | Informação não revelada |
| **Inteligibilidade do modelo** | Informação não revelada |
| **Output** | Informação não revelada |
| **Taxa de Erro Reportada** | Informação não revelada |
| **Toma ou Assiste a Tomada de Decisões** | Informação não revelada |
| **Consequência** | Informação não revelada |
| **Impacto (de acordo com os responsáveis pelo projeto)** | "[Espera-se] elevar a produção de conhecimento sobre os crimes, onde, como e quando eles ocorrem para ter uma orientação mais eficaz das ações das forças de segurança pública." |
| **Aplicação Geográfica** | Todas as unidades da federação. |
| **Prazo para Entrega do Projeto** | Entrega em etapas ao longo dos próximos quatro anos |

Fonte: JÚNIOR (2019a, 2019b) e MENDES (2019)[125]

As informações, organizadas no quadro, apontam para o fato de que diversos dos questionamentos realizados não chegaram a ser respondidos[126], sendo a negativa sustentada sob o fundamento de que,

[125] Solicitações de acesso à informação respondidas por Wanderley José Silva JÚNIOR, Diretor Substituto de Gestão e Integração de Informações, em 16 de outubro de 2019, na forma dos Ofícios n° 1130/2019/DGI/SENASP/MJ, e n °1131/2019/DGI/SENASP/MJ. As informações foram ainda prestadas por Luana MENDES, servidora mobilizada da Secretaria Nacional de Segurança Pública, em 16 de outubro de 2019, na forma do documento nº 37/2019/CGGI/DGI/SENASP. A íntegra das respostas recebidas, encontra-se disponível no Anexo II.

[126] Experiências em diversos contextos têm revelado a dificuldade enfrentada por jornalistas e pesquisadores para acessar informações sistemas algorítmicos e de IA em uso pelos governos. Nesse sentido, cf.: **Jamie Kalven joins other Chicago journalists in lawsuit against CPD - hpherald.com**. [s.d.]. Disponível em: <https://hpherald.com/2017/06/07/jamie-kalven-joins-chicago-journalists-lawsuit-cpd/>. Acesso em: 9 nov. 2019 (sobre a necessidade de formular pedidos judicias para acessar informações em casos ligados ao uso de algoritmos pelo departamento de polícia norte-americano). Cf. também: **We need to know the algorithms the government uses to make important decisions about us**. [s.d.]. Disponível em: <https://theconversation.com/we-need-to-know-the-algorithms-the-government-uses-to-make-important-decisions-about-us-57869>. Acesso em: 9 nov. 2019 (relatando as dificuldades enfrentadas na realização de estudo de caso em transparência algorítmica, conduzido no em relação ao sistema criminal de justiça norte-americano).

> [...] considerando a recente promulgação da Lei do SUSP e a atual fase do *Sinesp Big Data*, o momento não [seria] oportuno para apresentar respostas aos questionamentos [...], tendo em vista que a SENASP, por meio da DGI, tem trabalhado no levantamento de requisitos em conjunto com a DTIC/MJSP e a UFC para identificar as melhores práticas e tecnologias disponíveis (JÚNIOR, 2019a).

Com isso, as inconclusivas respostas aos questionamentos[127], juntamente das escassas informações disponíveis para consulta pública, apontaram a destacada falta de transparência na execução do projeto[128]. Assim, em razão dos obstáculos de acesso à informação, não foi possível analisar os sistemas em termos de qualidade dos dados utilizados para alimentá-los, inviabilizando que fossem tecidas considerações sobre possíveis *biases* ou sobre o grau de proteção dos dados. Tal situação se mostra especialmente problemática em vista de o policiamento preditivo ser um dos campos que apresentam maior risco de gerar discriminações indevidas[129].

Em vista disso, e tecendo considerações sobre possíveis distorções provocadas por tecnologias preditivas aplicadas à segurança pública, Freuer e Iglesias escrevem que

> Nem todos os crimes são relatados. As bases de dados da polícia são desenvolvidas usando crimes relatados e alguns crimes são notificados mais do que outros. [...] [Adicionalmente], a presença da polícia em uma área pode aumentar a probabilidade de um crime ser detectado ou denunciado[130] (FREULER; IGLESIAS, 2018, p. 27).

Por sua vez, no que se refere à análise do *design* das ferramentas, observou-se a completa ausência de participação pública, sendo ininteligíveis os modelos dos sistemas e protegidos os tipos de variáveis neles utilizados. Situação paralela se repete no cenário local

---

[127] Comentando sobre a questão da opacidade, Brauneis e Goodman escrevem: "Because the *design*ing entities typically do not disclose their predictive models or algorithms, there is a growing literature criticizing the "black box" opacity of these processes. **These black boxes are impervious to question, and many worry that they may be discriminatory, erroneous, or otherwise problematic. Journalists and scholars who have begun to seek details from public entities about these algorithms generally come short as their freedom of information requests are denied or go unanswered**." (BRAUNEIS; GOODMAN, 2017, p. 107–108, grifo nosso).

[128] Sobre a relação entre transparência, políticas públicas e democracia, cf.: "[...] entendemos que políticas públicas, principalmente as que envolvem grandes projetos e programas, precisem ser discutidas em um processo de deliberação pública, antes de serem implementadas. Mas entendemos, também, que as autoridades eleitas, os gestores nomeados e os funcionários envolvidos tenham que dar explicações públicas sobre suas decisões, ações e práticas sempre que forem solicitados a tanto, mesmo que seja depois da ação praticada. **A avaliação pública, como parte do processo de produção de boas decisões políticas, parece-nos inquestionável na maioria dos casos de produção de decisão política, mas a revisão pública *a posteriori*, por meio da qual outros órgãos do Estado e os próprios cidadãos podem realizar uma avaliação das decisões tomadas, com a possibilidade, inclusive de desaprovação das políticas e das decisões, além da responsabilização dos envolvidos, é fundamental para a democracia**" (GOMES; AMORIM; ALMADA, 2018, p. 8, grifo nosso).

[129] Nesse sentido, cf., *i.e.*, LUM, Kristian; ISAAC, William. To predict and serve? **Significance**, [s. l.], v. 13, n. 5, p. 14–19, 2016.

[130] Tradução livre. No original: "Not all crimes are reported. Police databases are developed using *reported* crimes and some crimes are reported more than others." (…) Police presence in an area may increase the likelihood of a crime being detected or reported" (FREULER; IGLESIAS, 2018, p. 27, grifos no original).

do NESP cearense, em relação ao qual não foi possível acessar quaisquer informações quanto ao *design* de suas iniciativas.

Ainda sobre o tema das variáveis, uma das respostas recebidas aponta para a intenção de que as soluções em desenvolvimento permitam identificar "relacionamentos entre vetores que compõem o comportamento delitivo: local, agressor, vítima, objetos, ligações telefônicas, transferências bancárias, etc." (JÚNIOR, 2019a, p. 2). Tais variáveis, ainda que não diretamente enviesadas, possuem potencial para gerar resultados discriminatórios, tendo em vista sua possível atuação como *proxis* para atributos protegidos, como dados raciais, por exemplo.

Nesse sentido, Altman, Wood e Vayena (2018, p. 8)destacam a conclusão amplamente apontada de que "a imparcialidade através da ocultação [de atributos protegidos] falha por causa de codificações redundantes[131]". Acrescentam ainda, quanto ao exemplo de discriminação racial, que "a remoção dos atributos protegidos [da análise algorítmica] não impedirá que outros atributos correlacionados com a raça tenham impacto na análise[132]" (Ibidem).

Em face disso – e sabendo ser inevitável a ocorrência de erros entre os *outputs* gerados pelos sistemas -, escolhas quanto ao *design* das ferramentas possuem papel ético importante, já que influenciarão na distribuição dos danos entre os grupos populacionais. Sabe-se também que:

> [...] nenhuma escolha prática de *design* algorítmico é neutra em termos de resultados. Assim, os *design*ers de algoritmos devem escolher, implícita ou explicitamente, quais tipos de erros são mais importantes e quais grupos devem ser classificados com mais precisão, a fim de produzir uma distribuição adequada de danos e benefícios. **As escolhas de *design* algorítmico devem, portanto, ser consideradas escolhas eticamente relevantes**.
> Além disso, quando os algoritmos são utilizados em processos legais e governamentais, existe frequentemente um problema de escolha social sendo implicitamente "resolvido". [...] Assim, **o objetivo do problema de escolha social implícito é equilibrar os benefícios para alguns, com os danos para os demais indivíduos avaliados e condenados[133]** (ALTMAN; WOOD; VAYENA, 2018, p. 17, grifo nosso, tradução nossa).

[131] Tradução livre de: "fairness through blindness fails because of redundant encodings."
[132] Tradução livre do trecho: "removing the protected attributes will not prevent other attributes correlated with race from having an impact on the analysis".
[133] Tradução livre do trecho: "(…) no practical algorithmic *design* choice is outcome- neutral. Thus, algorithm *design*ers must choose, implicitly or explicitly, which types of errors are most important, and which groups should be classified more accurately, in order to yield a preferred distribution of harms and benefits. Algorithmic *design* choices are therefore to be considered ethically relevant choices.
Further, when algorithms are used in legal and government processes, there is quite frequently a social- choice problem that is being implicitly "solved." (…) Thus the goal of the implied social choice problem is to balance the benefits to such individuals against the harms to the individuals scored and sentenced."

Considerando o exposto, questiona-se como serão feitas as escolhas sociais no projeto *Sinesp Big Data* e, consequentemente, como se darão as escolhas dos *design*s algorítmicos, ponto que permanece em aberto para avaliações futuras.

Igualmente opaca é a relação entre o *design* dos algoritmos e os *outputs* gerados: os sistemas serão utilizados para auxiliar a tomada de decisões pelos agentes públicos ou serão dotados de autonomia para tomar eles mesmos as decisões? Que tipo de *outputs* serão gerados e como se dará sua interpretação pelos usuários das ferramentas? Tais questionamentos são importantes na medida em que o exercício de poder pelos sistemas algorítmicos e de IA se define não apenas por seus desenvolvedores, mas também pelas autoridades que os utilizam.

Tais questões foram abordadas por Freuler e Iglesias (2018) em sua análise do emprego do PredPol, no Uruguai. Em face dos *outputs* gerados pelo sistema, identificou-se que as autoridades conferiram à ferramenta maior poder de decisão do que o previsto pelos próprios desenvolvedores do PredPol. Sobre isso, os autores escreveram que:

> Estes tipos de instruções aproximam esta implementação do grupo de algoritmos autoimplementadores e distanciam-na daqueles que apenas oferecem sugestões ou informações para a tomada de decisões. **Neste caso, a força policial torna-se o braço orgânico do computador**. Seria diferente, por exemplo, se cada comissário fosse capaz de definir onde alocar recursos, e considerasse o output como uma das muitas variáveis a serem equacionadas. Este exemplo ilustra muito claramente que **muitas vezes não são os projetistas do modelo, mas as autoridades políticas que definem quanto poder é concedido a um sistema de IA**[134] (FREULER; IGLESIAS, 2018, p. 28–29, grifo nosso, tradução nossa).

Essas considerações apontam para o fato de que a interpretação dos *outputs* gerados, assim como as decisões tomadas com base neles, são, em verdade, escolhas políticas. Isso implica que os efeitos dos sistemas algorítmicos e de IA não são resultado exclusivo de seus aspectos técnicos e do seu funcionamento interno, mas também das escolhas políticas tomadas a partir deles. Com isso, permanece a dúvida quanto a quais escolhas políticas serão tomadas a partir dos *outputs* do projeto *Sinesp Big Data*[135].

Adicionalmente, cabe tecer considerações sobre a própria proposta do projeto *Sinesp Big Data* enquanto instrumento de policiamento preditivo. Nesse sentido, há, na literatura,

---

[134] Tradução livre do trecho: "These types of instructions place this implementation closer to the group of self-implementing algorithms and distances it from the ones which merely offer suggestions or provide information for decision-making purposes. In this case, the police force becomes the organic arm of the computer. It would be different, for example, if each commissioner were able to define where to allocate resources, and regarded the output as one of many variables to be considered. This example illustrates very clearly that often it is not the *design*ers of the model, but the political authorities who define how much power is granted to an AI system" (FREULER; IGLESIAS, 2018, p. 28–29).

[135] Questiona-se, adicionalmente, como se dará o treinamento dos usuários do *Sinesp Big Data* quanto ao processamento e à análise dos dados, assumindo-se que haverá um treinamento.

autores que criticam o *design* de tais ferramentas preditivas, justamente em razão de os sistemas se orientarem por crimes "visíveis", mas não se aplicarem a delitos como corrupção e evasão de divisas. Outros criticam a suposição de que as ferramentas reduziriam as taxas de criminalidade, apontando que, em verdade, ter-se-ia um deslocamento das ocorrências criminais de um local a outro, e não sua redução de fato[136].

Outrossim, há críticos que se opõem às teorias de base dos sistemas preditivos, por entenderem que a maneira como a análise dos dados se dá desconsidera os fatores sociais que conduzem à ocorrência dos crimes. Isso deslocaria o debate para longe das necessárias políticas de inclusão assim como o distanciaria do amplo contexto socioeconômicos em relação ao qual a criminalidade está situada. Uma última crítica aponta para a possível ocorrência de *loops* de *feedback*[137], em que, a forma como a tecnologia é empregada "basicamente legitima o comportamento arbitrário da polícia, que se traduz em abuso policial e é, muitas vezes, produto de racismo ou classismo[138]" (FREULER; IGLESIAS, 2018, p. 30, tradução nossa).

Para tanto, e em face das considerações tecidas a partir das respostas às solicitações de informação, chegou-se à conclusão que, até o momento, os sistemas em desenvolvimento possuem modelos tipo *black box*[139] (PASQUALE, 2015):. o *design* das ferramentas não envolveu a participação pública, ademais de não haver informações acessíveis quanto aos dados utilizados, aos tipos de *outputs* gerados, à forma de interpretá-los ou às políticas públicas a serem desenvolvidas a partir do projeto. Isso desperta grande apreensão quanto ao potencial discriminatório das ferramentas, tanto pelas atuais características de seu desenvolvimento quanto pela teoria que embasa as tecnologias de policiamento preditivo[140].

Adicionalmente, foi possível vislumbrar o caráter disciplinar do *Sinesp Big Data e IA*, com seus modelos preditivos, projeto que materializa a figura do polipanóptico, invocando várias das ideias foucaultianas. Nesse sentido:

---

[136] Em relação ao NESP do estado do Ceará, seria possível que as estatísticas apresentadas, apontando a redução das taxas de criminalidade, tivessem relação com o "deslocamento do crime" e não com a eficiência das ferramentas empregadas?

[137] Cf., *e.g.*, O'NEIL, Cathy. **Weapons of Math Destruction: How *Big data* Increases Inequality and Threatens Democracy**. Nova Iorque, Estados Unidos da América: Crown, 2016.

[138] Tradução livre do trecho: "basically legitimizing arbitrary police behavior, which translates into police abuse, and is often the product of racism or classism."

[139] Cf. *supra* nota 48.

[140] Freuler e Iglesias escrevem que: "Local and international organizations have argued that tools like PredPol **tend to replicate the biases of training data and the historical power dynamics between law enforcement and minority or underprivileged populations**, and that they are used to **justify police presence in marginalized areas**." (FREULER; IGLESIAS, 2018, p. 30, grifo nosso).

> [...] a modelagem preditiva pode ser interpretada como um caso de disciplina foucaltiana, embora com uma reviravolta. No que diz respeito à normatização, a predição representa um mecanismo adicional que amplia uma normatização já existente. A conformidade com a norma é avaliada de uma forma preditiva melhorada, que substitui a forma clássica de mensurar. No que diz respeito aos dados, estes são obtidos tanto pela instituição focal como por outros contextos ("o polipanóptico"). Uma instituição pode olhar para os lados, por assim dizer, e olhar para os conjuntos de dados de outras instituições. **A disciplina do *machine learning* fortalece assim as relações de poder existentes, explorando o poder preditivo do *Big data*. Assim como a disciplina foucaultiana se infiltrou gradualmente nas várias instituições e fortaleceu suas modalidades de poder há alguns séculos, assim também o fazem as práticas preditivas nos dias de hoje**[141] (DE LAAT, 2019, p. 5, grifo nosso, tradução nossa).

Assim, considerando os mecanismos disciplinares das tecnologias preditivas em desenvolvimento, bem como suas implicações democráticas, conclui-se que:

> Em uma democracia, as forças policiais devem estar a serviço do povo. Enviar forças policiais para [determinadas] áreas, sob a expectativa de que encontrarão criminosos, **cria um ambiente no qual é provável que ocorram abusos de poder**. **O fato de essas decisões serem baseadas em sistemas não transparentes mina a legitimidade da força policial**. [Em face disso] os departamentos governamentais encarregados de financiar a infraestrutura e proteger direitos devem **engajar as comunidades afetadas no desenho de qualquer ferramenta relacionada com o exercício da força** (FREULER; IGLESIAS, 2018, p. 30, grifo nosso).

[141] Tradução livre. No original: "[...] predictive modelling may be interpreted as a case of Foucaldian discipline, though with a twist. As far as normation is concerned, prediction represents an additional mechanism which *extends* a normation already in existence. Compliance to the norm is measured in an enhanced predictive fashion which subsumes the classical way of measuring. As far as the data are concerned, these are procured by both the focal institution and by other contexts ("the Polypanopticon"). An institution can glance sideways as it were, and peer into the data pools of other institutions. The discipline of machine learning thus strengthens existing relations of power by harnessing the predictive power of *Big data*. Just as Foucauldian discipline gradually crept into the various institutions and strengthened their modalities of power a few centuries ago, so do predictive practices at the present day".

# 4 CONSIDERAÇÕES FINAIS

A presente pesquisa se orientou pela análise da adoção de sistemas algorítmicos e de IA pelo poder público brasileiro, dedicando-se, em especial, a analisar o *Sinesp Big Data e IA para Segurança Pública*. O projeto surge na novel conformação socioeconômica e política chamada, por Zuboff (2015), de *Capitalismo de Vigilância* e denota novos processos de subjetivação e de disciplina em curso.

No capítulo 1, discutiram-se os desafios da governança algorítmica e de IA, suscitando a miríade de princípios a serem observados no emprego das tecnologias informacionais para que se alcancem práticas transparentes, éticas, justas e *accountable*. Para tanto, sublinhou-se necessidade de que o poder público dos Estados adote as diretrizes apresentadas, especialmente considerando as interações democráticas oriundas da utilização das novas tecnologias informacionais e seus efeitos subjetivadores e disciplinares.

No capítulo 2, foram revisitados conceitos das teorias de Foucault, de Deleuze e de Zuboff, utilizando-os para analisar as novas dinâmicas de controle e poder da "civilização informacional". Deteve-se especialmente à prática do policiamento preditivo, compreendendo que os mecanismos de vigilância empregados conformam novas formas disciplinares, marcadas pela lógica do *Big Other* ou do polipanóptico. Tais formas são empregadas na governança disciplinar ou na governança de risco dos indivíduos, a depender da corrente, com a passagem da figura do "delinquente", em Foucault, para a figura do "Suspeito".

Com isso, o indivíduo considerado Suspeito passa a ser disciplinado antes mesmo de adotar o comportamento anormal, mediante a mera possibilidade futura de desvio das normas. Há, assim, um aprofundamento dos processos de subjetivação, com Zuboff (2015) entendendo não haver mais agência, mas apenas automação dos comportamentos humanos. Sinalizou-se, a partir disso, a existência de possíveis riscos à democracia em face das transformações desencadeadas pela nova lógica de acumulação do Capitalismo de Vigilância: as informações.

No capítulo 3, à luz das discussões desenvolvidas nos capítulos anteriores e após a pesquisa exploratória realizada, foi possível observar o rápido crescimento do número de iniciativas de uso algorítmico e de IA pelo setor público brasileiro. Dentre as ferramentas desenvolvidas, o Poder Judiciário mostrou grande destaque, implementando desde *bots* jurídicos, para facilitar o acesso dos cidadãos às informações públicas, até sistemas voltados a auxiliar na identificação de fraudes em processos licitatórios.

Entretanto, o levantamento de informações sobre o desenvolvimento e sobre o *design* dos ditos sistemas foi extremamente dificultoso. Com isso, e em razão da opacidade generalizada, não foi possível acessar as condições de governança algorítmica das ferramentas, inviabilizando que se analisassem possíveis riscos de sua utilização, tais como: manipulação; discriminação indevida; violação de direitos humanos, entre outros.

O quadro se repetiu em relação ao projeto *Sinesp Big Data e IA para Segurança Pública*. Apesar do envio de mensagens eletrônicas aos gestores do projeto, bem como de solicitações de acesso à informação, não se logrou obter dados suficientes para avaliá-lo segundo os parâmetros de governança algorítmica, conforme visto no capítulo 1. Com isso, apesar da magnitude do projeto, pensado para promover a integração nacional dos dados sobre segurança pública e para utilizar os frutos da vigilância em ações de inteligência policial, verificou-se que, até o momento, os sistemas são grandes *black boxes*.

Segundo mencionado nas respostas encaminhadas pelo MJSP, o projeto *Sinesp Big data* foi inspirado pelo NESP do Estado do Ceará, em razão da redução nas taxas de criminalidade a partir de sua implementação. A estratégia estadual, que se pauta igualmente por pilares de defesa social, orientou-se no sentido de aplicar tecnologias da informação à vigilância intensiva e ao policiamento preditivo.

Entretanto, não foram, igualmente, localizadas informações sobre aspectos técnicos do sistema, sobre a governança algorítmica nos seus estágios de desenvolvimento e de execução, sobre o treinamento dos agentes públicos para a manipulação das ferramentas ou mesmo para a interpretação dos *outputs*. Ainda, apesar de os resultados divulgados apontarem a redução nas taxas de criminalidade no Estado, não se verificou a existência de estudos sobre possíveis taxas de erro, vieses, discriminação indevida ou ainda sobre a real efetividade dos sistemas.

Tais constatações são especialmente preocupantes, na medida em que a NESP está sendo utilizada como parâmetro para o projeto *Sinesp Big Data*. Ademais, a equipe técnica responsável pelo desenvolvimento do projeto é a mesma que estivera antes encarregada pelas ferramentas da NESP. O semelhante grau de opacidade entre as iniciativas já aponta evidências do provável paralelo quanto à execução de ambas.

Nesse contexto, há de se ter em vista que o projeto *Sinesp Big Data* foi desenhado a partir da assinatura da Lei do SUSP, com a criação do PNSDPS, plano pautado pela integração nacional das forças de segurança pública. Para tanto, o instrumento normativo dedicou a integralidade de um de seus capítulos ao controle e à transparência, sendo a Seção III, em que fica instituída a criação do SINESP, pautada pelo tema da transparência e da integração de dados e informações.

Entretanto, “os padrões de integridade, disponibilidade, confidencialidade, confiabilidade e tempestividade dos sistemas informatizados do governo federal” (BRASIL, 2018, Art. 36, parágrafo único), cuja adoção, pelo SINESP, está prevista na Lei do SUSP, não tem se mostrado efetiva. Assim, em face da essência vigilante e disciplinar do SINESP, que orienta também o desenvolvimento do *Sinesp Big Data*, há de se acompanhar, com escrutínio, a implantação e os efeitos das ferramentas de IA do projeto, bem como do próprio PNSDPS.

O que esse cenário pode revelar em termos da dinâmica política na qual os sistemas algorítmicos e de IA estão situados? Como tais técnicas informatizadas e disciplinadoras estão moldando a subjetividade dos brasileiros? E, de acordo com essa lógica, que efeitos gerará o policiamento preditivo, segundo os moldes das recentes iniciativas governamentais? Que sujeitos esse poder tem criado ou aspira a criar? Como interagirão, dentro da realidade brasileira, o *Capitalismo de Vigilância* e a democracia? E qual o papel do Direito nesse novo contexto tecnológico, social e político?

Essas são questões que se apresentam, além da própria discussão sobre transparência e *accountability* das iniciativas algorítmicas e de IA e que necessitam ser endereçadas para que se possa avançar no diálogo sobre a agenda digital no Brasil e no mundo.

# REFERÊNCIAS


ALTMAN, Micah; WOOD, Alexandra; VAYENA, Effy. A Harm-Reduction Framework for Algorithmic Fairness. **IEEE Security and Privacy**, [s. l.], v. 16, n. 3, p. 34–45, 2018. Disponível em: <http://nrs.harvard.edu/urn-3:HUL.InstRepos:37356411>. Acesso em: 11 maio. 2019.

BEER, David. The social power of algorithms. **Information Communication and Society**, [s. l.], v. 20, n. 1, p. 1–13, 2017. Disponível em: <http://eprints.whiterose.ac.uk/104026/>. Acesso em: 3 abr. 2019.

BRASIL. Lei nº 13.675, de 11 de junho de 2018. . 2018.

BRAUNEIS, Robert; GOODMAN, Ellen P. Algorithmic Transparency for the Smart City. **SSRN Electronic Journal**, [s. l.], 2017.

CATH, Corinne. Governing artificial intelligence: ethical, legal and technical opportunities and challenges. **Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences**, [s. l.], v. 376, n. 2133, p. 20180080, 2018. Disponível em: <https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0080>

DE LAAT, Paul B. Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability? [s. l.], [s.d.]. Disponível em: <https://doi.org/10.1007/s13347-017-0293-z>. Acesso em: 20 nov. 2019.

DE LAAT, Paul B. **The disciplinary power of predictive algorithms: a Foucauldian perspectiveEthics and Information Technology**GroningenSpringer Berlin Heidelberg, , 2019. Disponível em: <http://link.springer.com/10.1007/s10676-019-09509-y>

**Declaration on Ethics and Data Protection in Artificial Intelligence**. Bruxelas, 2018. Disponível em: <https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf>. Acesso em: 26 out. 2019.

DELEUZE, Gilles. Post-scriptum sobre as Sociedades de controle. Conversações: 1972-1990. **Conversações:**, [s. l.], p. 219–226, 1992.

FREULER, J. Ortiz; IGLESIAS, C. **Algorithms and Artificial Intelligence in Latin America: A Study of Implementation by Governments in Argentina and Uruguay**. [s.l: s.n.]. Disponível em: <www.webfoundation.org>. Acesso em: 11 maio. 2019.

GOMES, Wilson; AMORIM, Paula Karini Dias Ferreira; ALMADA, Maria Paula. Novos desafios para a ideia de transparência pública. **E-Compós**, [s. l.], n. 1–21, 2018. Disponível em: <https://www.e-compos.org.br/e-compos/article/view/1446>

GOVERNO DO ESTADO DO CEARÁ. **Nova Estratégia de Segurança Pública - Governo do Estado do Ceará**. 2019. Disponível em: <https://nesp.ceara.gov.br/#pacific>. Acesso em: 16 nov. 2019.

GUREVICH, Yuri. What Is an Algorithm? In: **Lecture Notes in Computer Science**

**(including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)**. [s.l: s.n.]. p. 31–42.

JÚNIOR, Wanderly José Silva. **OFÍCIO Nº 1130/2019/DGI/SENASP/MJ**BrasíliaBrasil, , 2019. a.

JÚNIOR, Wanderly José Silva. **OFÍCIO Nº 1131/2019/DGI/SENASP/MJ**BrasíliaBrasil, , 2019. b.

KEPING, Yu. Governance and Good Governance: A New Framework for Political Analysis. **Fudan Journal of the Humanities and Social Sciences**, [s. l.], v. 11, n. 1, p. 1–8, 2018. Disponível em: <http://link.springer.com/10.1007/s40647-017-0197-4>

MATZNER, Tobias. Opening black boxes is not enough - Data-based surveillance in discipline and punish and today. **Foucault Studies**, [s. l.], 2017.

MENDES, Luana Manuella de Salles. **INFORMAÇÃO Nº 37/2019/CGGI/DGI/SENASP**BrasíliaBrasil, , 2019.

MONTEIRO, Renato Leite. **Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?**, 2018. Disponível em: <https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf>. Acesso em: 25 nov. 2019.

MOSCHOVAKIS, Yiannis N. What Is an Algorithm? In: **Mathematics Unlimited — 2001 and Beyond**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001. p. 919–936.

**Parallel Algorithm - Introduction - Tutorialspoint**. [s.d.]. Disponível em: <https://www.tutorialspoint.com/parallel_algorithm/parallel_algorithm_introduction.htm>. Acesso em: 2 dez. 2019.

PASQUALE, Frank. **The Black Box Society**. Cambridge, MA and London, England: Harvard University Press, 2015. Disponível em: <http://www.degruyter.com/view/books/harvard.9780674736061/harvard.9780674736061/harvard.9780674736061.xml>

PIMENTEL, André de Pieri et al. **Edição 2019 do Anuário Brasileiro de Segurança Pública**. [s.l: s.n.]. Disponível em: <http://www.forumseguranca.org.br/wp-content/uploads/2019/10/Anuario-2019-FINAL_21.10.19.pdf>.

RUSSELL, Stuart; NORVIG, Peter. **Artificial intelligence : a modern approach**. 3rd. ed. Upper Saddle River, New Jersey: Prentice Hall, 2010.

STONE, Peter et al. Artificial Intelligence and Life in 2030: One Hundred Year Study on Artificial Intelligence. **Stanford University**, [s. l.], 2016.

TAYLOR, Dianna (ED.). **Michel Foucault: conceitos fundamentais**. Petrópolis: Vozes, 2008.

**The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems**. . Toronto. Disponível em: <http://www.ohchr.org/EN/ProfessionalInterest/Pages/Vienna.aspx>. Acesso em: 26 out.

2019.

VALENTE, Jonas. Bolsonaro sanciona, com vetos, lei sobre proteção de dados. **Agência Brasil de Comunicação**, Brasília, 2019. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2019-07/bolsonaro-sanciona-com-vetos-lei-sobre-protecao-de-dados>. Acesso em: 25 nov. 2019.

ZUBOFF, Shoshana. Big other: Surveillance capitalism and the prospects of an information civilization. **Journal of Information Technology**, [s. l.], v. 30, n. 1, p. 75–89, 2015. Disponível em: <http://dx.doi.org/10.1057/jit.2015.5>

# APÊNDICES

## Apêndice [Digital] A – Resultados da Pesquisa Digital

Os resultados da pesquisa exploratória foram tabelados e se encontram disponíveis para consulta na planilha I e na planilha II, que são parte integrante do presente documento.

# Apêndice B – Questionário semiestruturado: projeto *Sinesp Big Data e IA*

Esta solicitação busca compreender melhor os processos técnicos pelos quais o desenvolvimento e a implementação do projeto *Sinesp Big Data de Inteligência Artificial para Segurança Pública* se orienta.

1. A partir do acesso público ao plano de trabalho simplificado, tomou-se conhecimento de que seriam desenvolvidas as seguintes funcionalidades:
    a. Plataforma *Big Data*;
    b. Analisador de crimes;
    c. Painel analítico;
    d. Painel governança;
    e. Processador de eventos complexos;
    f. Rastreamento objetos móveis;
    g. Aplicativo móvel para policial;
    h. Detector de fraudes;
    i. Redes delitivas;
    j. Sistema de indicativo de abordagem veicular;
    k. Seminários de transferência tecnológica.
2. Em relação a cada uma delas, o que se pretende desenvolver?
3. Em que áreas geográficas serão aplicadas?
4. Qual o objetivo de cada um?
5. Algum *software* foi desenvolvido ou utilizado? Em caso afirmativo, solicita-se:
    a. Nome (s) do (s) programa(s);
    b. O(s) programa(s) foi/foram desenvolvidos pela iniciativa pública ou privada?
    c. Informações sobre o processo pelo qual o programa foi adquirido ou desenvolvido;
    d. Cópia do contrato;
    e. Data da última atualização do programa;
    f. Informações sobre as auditorias feitas no *software* e os relatórios correspondentes;
    g. Avaliações internas ou externas da qualidade dos resultados;
    h. Estimativa quanto ao número de pessoas afetadas pelo(s) programa(s);
    i. O(s) algoritmo(s) utilizado(s) é/são aberto(s)?
    j. Número de variáveis levadas em consideração pelo *software*;

k. Lista das variáveis evadas em consideração;

l. Em quais bancos de dados o sistema se apoia para operar?

m. Qual entidade ou entidades gera esses dados? Como os dados são gerados? Solicita-se conhecer a entidade responsável por gerar os dados em relação a cada uma das variáveis que são levadas em consideração.

n. Algum dos dados subjacentes a essas variáveis não é produzido pelo Estado?

o. Com que frequência os dados são atualizados?

p. Houve alguma avaliação de possíveis vieses ou discriminação contra grupos específicos que podem ser desencadeados pelo sistema?

q. Os dados são públicos? Estão disponíveis em algum portal de dados ministerial ou nacional? Nesse caso, solicita-se que o link seja compartilhado.

r. Solicita-se anexar o banco de dados, em formato aberto (CSV ou XLSX), usado para o cálculo ou o link correspondente, se disponível na Internet.

s. Os sistemas foram desenvolvidos para tomar decisões autonomamente ou para auxiliar na tomada de decisões?

t. Como se deu o *design* das ferramentas? Quais foram os modelos escolhidos?

u. Quais são os *outputs* gerados por cada um dos sistemas? Como esses *outputs* são interpretados?

v. Qual o grau de inteligibilidade do modelo?

6. Qual o impacto social esperado em relação à implementação do projeto?

7. Como está sendo a execução e a implementação do projeto?

8. Desde a elaboração do plano de trabalho, houve a criação de alguma funcionalidade nova? Houve a modificação de alguma das funcionalidades previamente previstas?

9. Quais foram os desafios enfrentados no desenvolvimento do projeto *Sinesp Big Data de Inteligência Artificial para Segurança Pública*?

10. Como se deu a parceria entre a SENASP e a UFC para o desenvolvimento do projeto?

Grata.

# ANEXOS

## Anexo I - Princípios Compilados de Governança Ética

| ASILOMAR Principles | Toronto Declaration` |
|---|---|
| **Research Issues**<br>**1) Research Goal:** The goal of AI research should be to create not undirected intelligence, but beneficial intelligence.<br>**2) Research Funding:** Investments in AI should be accompanied by funding for research on ensuring its beneficial use, including thorny questions in computer science, economics, law, ethics, and social studies (…). | Governments have obligations and private sector actors have responsibilities to proactively prevent discrimination in order to comply with existing human rights law and standards. When prevention is not sufficient or satisfactory, and discrimination arises, a system should be interrogated and harms addressed immediately. |
| **3) Science-Policy Link:** There should be constructive and healthy exchange between AI researchers and policy-makers.<br>**4) Research Culture:** A culture of cooperation, trust, and transparency should be fostered among researchers and developers of AI.<br>**5) Race Avoidance:** Teams developing AI systems should actively cooperate to avoid corner-cutting on safety standards. | States must guarantee access to effective remedy for all individuals whose rights are violated or abused through use of these technologies |
| **Ethics and Values**<br>**6) Safety:** AI systems should be safe and secure throughout their operational lifetime, and verifiably so where applicable and feasible.<br>**7) Failure Transparency:** If an AI system causes harm, it should be possible to ascertain why.<br>**8) Judicial Transparency:** Any involvement by an autonomous system in judicial decision-making should provide a satisfactory explanation auditable by a competent human authority.<br>**9) Responsibility:** *Design*ers and builders of advanced AI systems are stakeholders in the moral implications of their use, misuse, and actions, with a responsibility and opportunity to shape those implications.<br>**10) Value Alignment:** Highly autonomous AI systems should be *design*ed so that their goals and behaviors can be assured to align with human values throughout their operation.<br>**11) Human Values:** AI systems should be *design*ed and operated so as to be compatible with | States must take the following steps to mitigate and reduce the harms of discrimination from machine learning in public sector systems:<br>**Identify risks**: Any state deploying machine learning technologies must thoroughly investigate systems for discrimination and other rights risks prior to development or acquisition, where possible, prior to use, and on an ongoing basis throughout the lifecycle of the technologies, in the contexts in which they are deployed.<br>**Ensure transparency and accountability**: States must ensure and require accountability and maximum possible transparency around public sector use of machine learning systems. This must include explainability and intelligibility in the use of these technologies so that the impact on |

| | |
|---|---|
| ideals of human dignity, rights, freedoms, and cultural diversity.<br>**12) Personal Privacy:** People should have the right to access, manage and control the data they generate, given AI systems' power to analyze and utilize that data.<br>**13) Liberty and Privacy:** The application of AI to personal data must not unreasonably curtail people's real or perceived liberty. | affected individuals and groups can be effectively scrutinized by independent entities, responsibilities established, and actors held to account.<br>**Enforce oversight**: States must take steps to ensure public officials are aware of and sensitive to the risks of discrimination and other rights harms in machine learning systems. |
| **14) Shared Benefit:** AI technologies should benefit and empower as many people as possible.<br>**15) Shared Prosperity:** The economic prosperity created by AI should be shared broadly, to benefit all of humanity.<br>**16) Human Control:** Humans should choose how and whether to delegate decisions to AI systems, to accomplish human-chosen objectives.<br>**17) Non-subversion:** The power conferred by control of highly advanced AI systems should respect and improve, rather than subvert, the social and civic processes on which the health of society depends.<br>**18) AI Arms Race:** An arms race in lethal autonomous weapons should be avoided. | [With regard to the private sector, the following steps must be taken:]<br>**Identify potential discriminatory outcomes**: During the development and deployment of any new machine learning technologies, non-state and private sector actors should assess the risk that the system will result in discrimination.<br>**Take effective action to prevent and mitigate discrimination and track responses**<br>**Be transparent about efforts to identify, prevent and mitigate against discrimination in machine learning systems**: Private sector actors that develop and implement machine learning systems should disclose the process of identifying risks, the risks that have been identified, and the concrete steps taken to prevent and mitigate identified human rights risks.<br>Companies and private sector actors designing and implementing machine learning systems should take action to ensure individuals and groups have access to meaningful, effective remedy and redress. |
| **19) Capability Caution:** There being no consensus, we should avoid strong assumptions regarding upper limits on future AI capabilities.<br>**20) Importance:** Advanced AI could represent a profound change in the history of life on Earth, and should be planned for and managed with commensurate care and resources.<br>**21) Risks:** Risks posed by AI systems, especially catastrophic or existential risks, must be subject to planning and mitigation efforts commensurate with their expected impact.<br>**22) Recursive Self-Improvement:** AI systems *design*ed to recursively self-improve or self- | States should put in place regulation compliant with human rights law for oversight of the use of machine learning by the private sector in contexts that present risk of discriminatory or other rights-harming outcomes, recognizing technical standards may be complementary to regulation. In addition, non-discrimination, data protection, privacy and other areas of law at national and regional levels may expand upon and reinforce international human rights obligations applicable to |

| | |
|---|---|
| replicate in a manner that could lead to rapidly increasing quality or quantity must be subject to strict safety and control measures.<br>**23) Common Good:** Superintelligence should only be developed in the service of widely shared ethical ideals, and for the benefit of all humanity rather than one state or organization. | machine learning. |

| **NESTA** | **ICDPPC** | **FAT ML** | **Data ethics workbook – UK** |
|---|---|---|---|
| Every algorithm used by a public sector organization should be accompanied with a description of its function, objectives and intended impact, made available to those who use it. | Artificial intelligence and machine learning technologies should be *design*ed, developed and used in respect of fundamental human rights and in accordance with the fairness principle (…). | **Responsibility**: Make available externally visible avenues of redress for adverse individual or societal effects of an algorithmic decision system, and *design*ate an internal role for the person who is responsible for the timely remedy of such issues. | Start with clear user need and public benefit. |
| Public sector organizations should publish details describing the data on which an algorithm was (or is continuously) trained, and the assumptions used in its creation, together with a risk assessment for mitigating potential biases. | Continued attention and vigilance, as well as accountability, for the potential effects and consequences of, artificial intelligence systems should be ensured (…). | **Explainability**: Ensure that algorithmic decisions as well as any data driving those decisions can be explained to end-users and other stakeholders in non-technical terms. | Be aware of relevant legislation and codes of practice. |
| Algorithms should be categorized on an Algorithmic Risk Scale of 1-5, with 5 referring to those whose impact on an individual could be very high, and 1 being very minor. | Artificial intelligence systems transparency and intelligibility should be improved, with the objective of effective implementation (…). | **Accuracy**: Identify, log, and articulate sources of error and uncertainty throughout the algorithm and its data sources so that expected and worst case implications can be understood and | Use data that is proportionate to the user need. |

| | | | |
|---|---|---|---|
| | | inform mitigation procedures. | |
| A list of all the *inputs* used by an algorithm to make a decision should be published. | As part of an overall "ethics by *design*" approach, artificial intelligence systems should be *design*ed and developed responsibly, by applying the principles of privacy by default and privacy by *design* (…). | **Auditability**: Enable interested third parties to probe, understand, and review the behavior of the algorithm through disclosure of information that enables monitoring, checking, or criticism, including through provision of detailed documentation, technically suitable APIs, and permissive terms of use. | Understand the limitations of the data. |
| Citizens must be informed when their treatment has been informed wholly or in part by an algorithm. | Empowerment of every individual should be promoted, and the exercise of individuals' rights should be encouraged, as well as the creation of opportunities for public engagement (…). | **Fairness**: Ensure that algorithmic decisions do not create discriminatory or unjust impacts when comparing across different demographics (e.g. race, sex, etc). | Ensure robust practices and work within your skillset. |
| Every algorithm should have an identical sandbox version for auditors to test the impact of different input conditions. | Unlawful biases or discriminations that may result from the use of data in artificial intelligence should be reduced and mitigated (…). | | Make your work transparent and be accountable |
| When using third parties to create or run algorithms on their behalf, public sector organizations should only procure from organizations able to meet Principles 1-6. | | | Embed data use responsibly. |
| A named member of senior staff (or their job role) should be held formally | | | |

| | | | |
|---|---|---|---|
| responsible for any actions taken as a result of an algorithmic decision. | | | |
| Public sector organizations wishing to adopt algorithmic decision making in high risk areas should sign up to a dedicated insurance scheme that provides compensation to individuals negatively impacted by a mistaken decision made by an algorithm. | | | |

# Anexo II – Projeto *Sinesp Big Data e IA*: Respostas às Solicitações de Informação

9989103 01390002235201971

Ministério da Justiça e Segurança Pública
Secretaria Nacional de Segurança Pública
Coordenação-Geral de Gestão e Integração de Dados

INFORMAÇÃO Nº 37/2019/CGGI/DGI/SENASP

Assunto: **SIC - Pedido de Acesso à Informação.**
Interessado (a): **Marcelle Martins Lemes**

Em atenção ao Despacho nº 835/2019/DGI/SENASP/MJ (9883186), que versa sobre Pedido de Acesso à Informação nº 01390002235201971 (9870411), de autoria da Senhora **MARCELLE MARTINS LEMES**, em que solicita a melhor compreensão dos processos técnicos (inteligência artificial, algoritmos, modelos estatísticos) pelos quais as práticas de segurança e de policiamento são informados por processos automatizados, segue abaixo as respostas aos questionamentos elencados nos itens constantes no Anexo (9872952):

1. **Há técnicas de previsão matemáticas em uso (algoritmos, inteligência artificial ou modelos estatísticos) - ou que tenham sido usadas nos últimos 5 anos - para identificar possíveis atividades criminosas?**

   *Conforme Lei nº 13.675, de 11 de Junho de 2018 - (Lei do Susp), o Sinesp é meio e instrumento do Plano Nacional de Segurança Pública e Defesa Social, tendo como um de seus objetivos a coleta, análise, atualização, sistematização, integração e interpretação de dados e informações relativos às políticas de segurança pública e defesa social. Neste contexto, existem diversos projetos em desenvolvimento pelo Ministério da Justiça e Segurança Pública, dentre eles, o Sinesp Big Data e Inteligência Artificial, que encontra-se em fase inicial de construção.*

2. **Em caso afirmativo, em que áreas geográficas?**

   *Todas as unidades da federação.*

3. **Que tipo de atividades se pretende identificar?**

   - *Análise de eventos espaço-temporais relacionados com ações delituosas;*
   - *Busca e visualização dos analíticos sobre dados de segurança pública de todo o país;*
   - *Detecção de anomalias em dados históricos e fluxo de dados em tempo*

*real;*

- *Acompanhamento em tempo real de veículos que transitem em vias urbanas;*
- *Acompanhamento de rotas e Mancha Criminal Dinâmica;*
- *Identificação automática de fraudes a partir do reconhecimento de padrões associados a este tipo de ações delituosas;*
- *Identificação de relacionamentos que compõem o comportamento delitivo.*

4. **Algum software é usado?**

   *O projeto Big Data e Inteligência Artificial está em fase inicial de construção, os processos estão sendo mapeados e as tecnologias estudadas, o projeto será constantemente aprimorado com novas soluções e recursos de tecnologias sem nenhum custo para os Estados.*

5. **Quais unidades do Ministério/Secretaria usam algoritmos para orientar e informar as práticas de segurança pública e de policiamento? Solicita-se anexar a documentação correspondente a cada uma delas, incluindo as variáveis utilizadas, os bancos de dados dos quais essas variáveis são extraídas, nome legal de cada uma das empresas privadas que fornecem o software pelo qual os algoritmos são executados, bem como os contratos correspondentes e a documentação que formalizou os processos de aquisição.**

   *A Secretaria Nacional de Segurança Pública - SENASP é responsável pela política de segurança pública no país. Todavia, não é possível atender a solicitação de encaminhamento da documentação sobre práticas de segurança pública, considerando a recente promulgação da Lei nº 13.675, de 11 de Junho de 2018 - (Lei do Susp) e a fase inicial da construção do Sinesp Big Data e Inteligência Artifical, esclarecemos que não dispomos de respostas para todos os questionamentos da interessada em tela, salientamos que a SENASP, por meio da Diretoria de Gestão e Integração de Informações, tem trabalhado no levantamento de requisitos em conjunto com a Diretoria de Tecnologia da Informação e Comunicação e a Universidade Federal do Ceará para identificar as melhores práticas e tecnologias disponíveis.*

É o que informamos para ciência superior e encaminhamentos cabíveis.

Atenciosamente,

**LUANA MANUELLA DE SALES MENDES**
Servidora Mobilizada

Documento assinado eletronicamente por **LUANA MANUELLA DE SALES MENDES**, **Servidor(a) Mobilizado(a) da Secretaria Nacional de Segurança Pública**, em 16/10/2019, às 13:59, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

9989648 00077002951201948

Ministério da Justiça e Segurança Pública
Secretaria Nacional de Segurança Pública
Diretoria de Gestão e Integração de Informações

OFÍCIO Nº 1130/2019/DGI/SENASP/MJ

Brasília, 16 de outubro de 2019.

A Senhora

**ROSANA FERNANDES GALVÃO**

Ponto Focal do SIC na SENASP

**Assunto: SIC - Pedido de Acesso à Informação.**

Senhora Ponto Focal,

1. Em atenção ao Despacho nº 744/2019/SIC-SENASP/SENASP/MJ (9895612) e encaminha Pedido de Acesso à Informação (9884261) e Anexo (9884419), com questionamentos referente aos processos técnicos pelos quais as práticas de segurança e de policiamento são informadas por processos automatizados.

2. Quanto às perguntas apresentadas no Anexo 9884419, informa-se

3. Conforme LEI Nº 13.675, DE 11 DE JUNHO DE 2018 (Lei do Susp) o Sinesp é meio e instrumento do Plano Nacional de Segurança Pública e Defesa Social, tendo como um de seus objetivos a coleta, análise, atualização, sistematização, integração e interpretação de dados e informações relativos às políticas de segurança pública e defesa social.

4. Com a promulgação em 2018 da Lei do Susp, o Ministério da Justiça e Segurança Pública intensificou seus trabalhos no que concerne ao fornecimento de tecnologias aos integrantes do Sinesp, buscando a ampliação das integrações entre sistemas e a melhoria da qualidade dos dados transmitidos pelos Estados.

5. Neste contexto, inicia-se a construção do Sinesp Big Data, plataforma de processamento de dados em larga escala, visando o processamento de dados históricos e fluxo de dados em tempo real, de forma escalável, distribuída e elástica.

6. Atrelados ao Sinesp Big Data, estão sendo estudadas, mapeadas e desenvolvidas

soluções que irão permitir:

a) Análise de eventos espaço-temporais relacionados com ações delituosas;

b) Busca e visualização dos analíticos sobre dados de segurança pública de todo o país

c) Detecção de anomalias em dados históricos e fluxo de dados em tempo real;

d) Acompanhamento em tempo real de veículos, pessoas e objetos rastreados através de sensor de geolocalização;

e) Acompanhamento de rotas e Mancha Criminal Dinâmica;

f) Identificação automática de fraudes a partir do reconhecimento de padrões associados a este tipo de ações delituosas;

g) Identificação de relacionamentos entre vetores que compõem o comportamento delitivo: local, agressor, vítima, objetos, ligações telefônicas, transferências bancárias, etc.

7. Assim, considerando a recente promulgação da Lei do Susp e a atual fase do Sinesp Big Data, o momento não é oportuno para apresentar respostas aos questionamentos da Sra. Marcelle Martins Lemes, tendo em vista que a Secretaria Nacional de Segurança Pública, por meio da Diretoria de Gestão e Integração de Informações, tem trabalhado no levantamento de requisitos em conjunto com a Diretoria de Tecnologia da Informação e Comunicação-Dtic/MJSP e a Universidade Federal do Ceará para identificar as melhores práticas e tecnologias disponíveis.

Atenciosamente,

**WANDERLEY JOSÉ SILVA JÚNIOR**
Diretor de Gestão e Integração de Informações - Substituto

Documento assinado eletronicamente por **Wanderley José Silva Júnior**, **Diretor(a) de Gestão e Integração de Informações - Substituto(a)**, em 16/10/2019, às 14:18, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **9989648** e o código CRC **C75D2DEB**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.



Esplanada dos Ministérios, Anexo II, Sala 520, 5º Andar, - Bairro Zona Cívico Administrativa, Brasília/DF, CEP 70064-900
Telefone: (61) 2025-3333 - www.justica.gov.br - E-mail para resposta: protocolo@mj.gov.br

9989691 08850005451201952

Ministério da Justiça e Segurança Pública
Secretaria Nacional de Segurança Pública
Diretoria de Gestão e Integração de Informações

OFÍCIO Nº 1131/2019/DGI/SENASP/MJ

Brasília, 16 de outubro de 2019.

A Senhora

**ROSANA FERNANDES GALVÃO**

Ponto Focal do SIC na SENASP

**Assunto: SIC - Pedido de Acesso à Informação.**

Senhora Ponto Focal,

1. Em atenção ao Despacho nº 742/2019/SIC-SENASP/SENASP/MJ (9887123) que encaminha Pedido de Acesso à Informação (9872970), de autoria da Senhora **MARCELLE MARTINS LEMES,** em que solicita a melhor compreensão dos processos técnicos pelos quais o desenvolvimento e a implementação do projeto "Sinesp Big Data e Inteligência Artificial para Segurança Pública" se orienta, segue abaixo as respostas aos questionamentos elencados nos itens constantes no Anexo (9883779)

I - **Em relação a cada uma delas, o que se pretende desenvolver?**

a) *Plataforma Big Data: base dos sistemas do Sinesp, com tecnologias e soluções para execução em larga escala;*

b) *Analisador de Crimes:proporcionar o georreferenciamento das ocorrências em relação ao tempo e o espaço em que é registrada, possibilitando, por exemplo, a visualização de rotas de policiamento e mapas de calor dos locais e horários onde mais acontecem crimes;*

c) *Painel Analítico: permitirá a busca de informações em boletins de ocorrência de outros estados e municípios, além de pesquisas a dados de pessoas, objetos e documentos.*

d) *Painel Governança: painel que permitirá o acompanhamento das integrações do*

*Sinesp.*

e) *Processador de Eventos Complexos: processamento de eventos complexos visando a detecção de anomalias.*

f) *Rastreamento Objetos Móveis: monitoramento inteligente para rápida intervenção, acompanhamento de ocorrências criminais, detecção por sensores, câmeras de segurança, viaturas e agentes e pessoas com restrição de liberdade que fazem uso de tornozeleiras eletrônicas;*

g) *Aplicativo Móvel para Policial: aplicativo móvel para o gerenciamento do policiamento ostensivo e comunitário;*

h) *Detector de Fraudes: possibilitará a identificação automática de fraudes a partir do reconhecimento de padrões associados a este tipo de ações delituosas.*

i) *Redes Delitivas: Painel analítico de relacionamentos que compõem o comportamento delitivo;*

j) *Sistema de indicativo de Abordagem Veicular: sistema para monitoramento em tempo real de veículos que transitem em vias urbanas;*

k) *Seminário de transferência tecnológica: Seminários para realização da transferência de tecnologia para a equipe do Ministério da Justiça e Segurança Pública.*

II - **Em que áreas geográficas serão aplicados?**

*Todas as unidades da federação.*

III - **Qual o objetivo de cada um?**

*Resposta contida no item 2.*

IV - **Algum software foi desenvolvido ou utilizado?**

*O projeto Big Data e Inteligência Artificial será desenvolvido e entregue em etapas ao longo dos próximos quatro anos.*

V - **Qual o impacto social esperado em relação à implementação do projeto?**

*Elevar a produção de conhecimento sobre os crimes, onde, como e quando eles ocorrem para ter uma orientação mais eficaz das ações das forças de segurança pública.*

VI - **Como está sendo a execução e a implementação do projeto?**

*O Big Data e Inteligência artificial, está sendo desenvolvido por cientistas da Universidade Federal do Ceará (UFC), o projeto será constantemente aprimorado com novas soluções e recursos de tecnologias sem nenhum custo para os Estados.*

VII - **Desde a elaboração do plano de trabalho, houve a criação de alguma funcionalidade nova? Houve a modificação de alguma das funcionalidades previamente previstas?**

*Não.*

VIII - **Quais foram os desafios enfrentados no desenvolvimento do projeto "Sinesp Big Data de Inteligência Artificial para Segurança Pública"?**

*Considerando que o projeto está em fase inicial, ainda não é possível mensurar, na presente data, os desafios enfrentados relativo ao desenvolvimento do Sinesp Big Data e Inteligência Artificial para Segurança Pública.*

IX - **Como se deu a parceria entre a SENASP e a UFC para o desenvolvimento**

**do projeto?**

*Em virtude do trabalho técnico e científico apresentado para fins de produção de conhecimento para políticas de segurança pública, bem como a existência de sistemas em produção utilizados por órgão de segurança pública, com resultados positivos, a seleção da proposta da UFC, foi pautada nas atividades e procedimentos técnicos profissionais especializados no projeto em tela caracterizado pela privatividade de sua execução e pesquisa científica, bem como a comprovada experiência de sucesso já mencionada junto a SSPDS/CE, que confirma a notória especialização na área do presente projeto, não só em ciência de dados, mas também em seu emprego na área de segurança pública, mitigando de forma significativa os riscos do projeto.*

Atenciosamente,

**WANDERLEY JOSÉ SILVA JÚNIOR**
Diretor de Gestão e Integração de Informações - Substituto

Documento assinado eletronicamente por **Wanderley José Silva Júnior**, **Diretor(a) de Gestão e Integração de Informações - Substituto(a)**, em 16/10/2019, às 14:19, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **9989691** e o código CRC **EFF891C8**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

**Referência:** Caso responda este Ofício, indicar expressamente o Processo nº 08850005451201952 SEI nº 9989691

Esplanada dos Ministérios, Anexo II, Sala 520, 5º Andar, - Bairro Zona Cívico Administrativa, Brasília/DF, CEP 70064-900
Telefone: (61) 2025-3333 - www.justica.gov.br - E-mail para resposta: protocolo@mj.gov.br

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO CEARA
REITORIA
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE COMPUTAÇÃO

OFÍCIO 153/2019/DC_CC/CC/REITORIA

Fortaleza, 16 de outubro de 2019.

À Senhora
LUCIANA ALBUQUERQUE CAVALCANTE
Ouvidora Geral Interina da UFC

**Assunto: Resposta ao Protocolo e-SIC Nº 23480022424201993**

Prezada senhora,

Ao iniciar o projeto assinei um termo de confidencialidade e sigilo (1051450) das informações e dados técnicos do projeto intitulado **"Sinesp Big Data de Inteligência Artificial para Segurança Pública",** vinculado ao Ministério da Justiça e Segurança Pública e Secretaria Nacional de Segurança Pública (SENASP), no qual sou coordenador, por tal razão, estou impossibilitado de fornecer informações técnicas a respeito do mesmo.

Atenciosamente,

José Antonio Fernandes de Macedo
Coordenador

Documento assinado eletronicamente por **JOSE ANTONIO FERNANDES DE MACEDO**, **Coordenador**, em 16/10/2019, às 17:45, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufc.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1050927** e o código CRC **DE60E1B3**.

Campus do Pici, s/n - (85) 3366-9837
CEP 60440-900 - Fortaleza/CE - http://ufc.br/

8961417 08020.004633/2019-89

**MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA**

**MINUTA DE TERMO DE CONFIDENCIALIDADE, SIGILO E DE BOM USO DOS RECURSOS DE TIC, INFORMAÇÕES E DADOS DO**

**PROJETO SINESP BIG DATA E INTELIGÊNCIA ARTIFICIAL PARA SEGURANÇA PÚBLICA**

Pelo presente Termo, eu José Antônio Fernandes de Macêdo, [redacted] vinculado à Fundação de Apoio a Serviços Técnicos, Ensino e Fomento a Pesquisas , CNPJ nº 08.918.421/0001-08, declaro ter recebido da SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA ou da UNIVERSIDADE FEDERAL DO CEARÁ informações confidenciais e reservadas do ambiente computacional, incluindo dados quantitativos ou qualitativos da estrutura e topologia da rede, de sistemas, de métodos ou processos atualmente utilizados, entre outras informações, todas fornecidas em razão da minha participação no projeto SINESP BIG DATA E INTELIGÊNCIA ARTIFICIAL PARA SEGURANÇA PÚBLICA, que, se expostas ao domínio público permitem a ação deletéria de softwares e agentes maliciosos, razão pelo qual, por meio do presente termo de responsabilidade, comprometo-me a manter sob sigilo as informações e dados obtidos; a eliminar todas as informações obtidas caso seja desligado do projeto; e, sob as penas da lei, comprometo-me a não divulgar as informações a que tive acesso.

Para os fins deste Termo, "*informação confidencial*" significa todos os esclarecimentos técnicos, minutas de documentos, documentos, dados, estudos, especificações técnicas, inovações ou aperfeiçoamento de que venha a ter acesso, ou que me venham a ser confiados em razão deste Termo, incluindo-se previsões, gráficos e todas e quaisquer outras informações, escritas, orais ou visuais, relacionadas com a execução da minha atividade no projeto, seja de natureza técnica, operacional, financeira, comercial e/ou legal, que possua valor tangível ou intangível para a SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA, incluindo, mas não se limitando, a existência deste Termo e suas condições, mas excluindo: a) informações que estejam ou venham a estar em domínio do público em geral por outra forma que não seja a violação deste Termo; ou b) informações que o signatário deste Termo pode comprovar que não foi adquirida, direta ou indiretamente, em caráter confidencial, neste ato; ou c) informações de propriedade da SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA, por ela divulgada, de maneira irrestrita e não confidencial; ou d) informações que tenham sua divulgação exigida por lei, incluindo por qualquer tribunal ou órgão regulatório com competência para tanto.

Declaro que a estrutura computacional e telefônica eventualmente disponibilizada pela SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA não poderá para fins particulares, que não devo fazer uso de equipamentos particulares no ambiente da SECRETARIA NACIONAL DE SEGURANÇA PÚBLICA e que a

navegação em sítios da Internet e as correspondências em meio eletrônico acessadas a partir dos seus equipamentos deverão ser utilizados somente para fins de trabalho e poderão ser auditadas.

Brasília, 12 de Junho de 2019.

José Antônio Fernandes de Macêdo

Documento assinado eletronicamente por **José Antonio Fernandes de Macedo**, **Usuário Externo**, em 24/06/2019, às 15:41, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **8961417** e o código CRC **D80C2940**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

**Referência:** Processo nº 08020.004633/2019-89 SEI nº 8961417

# Anexo III - Projeto *Sinesp Big Data e IA*: Plano de Trabalho Simplificado

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO CEARÁ

**PLANO DE TRABALHO SIMPLIFICADO**

**1. TIPO DE PROJETO**

**( ) Ensino**
**( X ) Pesquisa**
**( ) Extensão**
**( ) Desenvolvimento Institucional**
**( ) Desenvolvimento Científico e Tecnológico**
**( ) Fomento à Inovação**

**ANEXO 1 – DADOS CADASTRAIS**

**1. DADOS CADASTRAIS DO PROPONENTE**

| | | | |
|---|---|---|---|
| **1.1 Órgão/Entidade Proponente: UNIVERSIDADE FEDERAL DO CEARÁ** | | | **1.2 CNPJ: 07.272.636/0001-31** |
| **1.3 Endereço: AV. DA UNIVERSIDADE, 2932 Benfica, Fortaleza/CE** | | | |
| **1.4 Cidade: Fortaleza** | **1.5 UF: CE** | **1.6 CEP: 60.020-181** | **1.7 Esfera Administrativa: Administrativa Publica Federal** |
| **1.8 DDD: 85** | **1.9 Telefone: 3366-7300** | **1.10 Fax: 3366-7308** | **1.11 E-mail: greitor@ufc.br** |
| **1.12 Nº UG (Unidade Gestora): 153045** | | **1.13 Gestão (número):15224** | |
| **1.14 Conta Corrente:** | **1.15 Banco:** | **1.16 Agência:** | **1.17 Praça de Pagamento:** |
| **1.18 Nome do Responsável: HENRY DE HOLANDA CAMPOS** | | | **1.19 CPF: 081.333.873-53** |
| **1.20 RG/Órgão Expedidor:** | **1.21 Cargo:** | **1.22 Função:** | **1.23 SIAPE: 7292321** |
| **1.24 Endereço: RUA: OSVALDO CRUZ, 500 - MEIRELES** | | | **1.25 CEP:** 60.125-150 |

| | | |
|---|---|---|
| **1.26 Nome do Coordenador do Projeto: JOSÉ ANTONIO FERNANDES DE MACÊDO** | | **1.27 CPF: 000.280.177-90** |
| **1.28 Unidade/Departamento: Departamento de Computação** | | **1.29 SIAPE: 364969** |
| **1.30 E-mail: jose.macedo@dc.ufc.br** | **1.31 Telefone Fixo:** (85) 3366-9843 | **1.32 Telefone Celular:** (85) 99134-9000 |

| | | |
|---|---|---|
| **1.33 Nome do Fiscal do Convênio/Contrato: Fernando Antonio Mota Trinta** | | **1.34 CPF: 493.956.533-53** |
| **1.35 Unidade/Departamento: Departamento de Computação** | | **1.36 SIAPE: 2068098** |
| **1.37 E-mail: fernando.trinta@d.ufc.br** | **1.38 Telefone Fixo: (85)3366-9843** | **1.39 Telefone Celular:**(85) 98893-6876 |

| | | |
|---|---|---|
| **1.40 Nome do Suplente do Fiscal do Convênio/Contrato: Marcio Espíndola Freira Maia** | | **1.41 CPF: 617.051.103-63** |
| **1.42 Unidade/Departamento: Campus Quixadá** | | **1.43 SIAPE: 1764820** |
| **1.44 E-mail: marcioefmaia.ufc.br** | **1.45 Telefone Fixo:** (85) 3366-9843 | **1.46 Telefone Celular:** (85) 99922-5388 |

**2. OUTROS PARTÍCIPES**

**ANEXO 2 – ELABORAÇÃO DO PROJETO**

**1. DESCRIÇÃO DO PROJETO**

| 1.2.1 Título do Projeto | 1.2 Período de Execução |
|---|---|
| Sinesp Big Data de Inteligência Artificial para Segurança Pública | 48 meses a partir da assinatura do contrato |

**1.3 Identificação do Objeto:**

O objetivo geral deste projeto é desenvolver estudos científicos com intuito de criar uma plataforma inovadora que permitirá integrar e analisar fontes de dados de interesse para a segurança pública, possibilitando a implantação de um novo modelo de governança das estratégias de segurança pública. As soluções desenvolvidas proporcionarão a aplicação de ciência de dados, aprendizado de máquina e áreas afins, para descoberta de padrões, detecção de anomalias e predição de crimes, sendo necessária a análise e a gestão eficiente desse grande volume de dados (dos mais diversos tipos e fontes), ao qual denominamos Big Data.

**1.4 Objetivo:**

Este projeto tem como objetivo o desenho e a implementação de uma infraestrutura que facilite a integração e análise de grandes volumes de dados relacionados com a segurança pública. Esta infraestrutura permitirá coletar, integrar, gerenciar e analisar dados relacionados à segurança pública, bem como disponibilizar ferramentas para ajudar na governança das estratégias de segurança. Considerando que para subsidiar a transferência de conhecimento da plataforma para o Ministério da Justiça e Segurança Pública, assim como melhorar a sintonia entre as partes e a evolução mais adequada da solução, haverá a necessidade de qualificação dos servidores que estarão alocados nas atividades envolvidas para desenvolvimento das competências necessárias, garantindo a sustentação do projeto por meio de Mestrado Profissional, o que será viabilizado através de TED específico.

**1.5 Justificativa do Projeto:**

O crescimento desordenado das grandes cidades, aliado ao aumento da mobilidade urbana e ao barateamento dos meios de transportes, impactou fortemente na eficácia da segurança pública. O resultado da soma desses fatores foi uma grande desorganização social e o enfraquecimento da coerção social informal que, de acordo com a Teoria da Desorganização Social, favorece situações de conflitos, crime e violência, devido à falta de coesão entre os membros de uma comunidade. Aliado ao crescimento desordenado das cidades e ao aumento da mobilidade, vemos um grande crescimento populacional, que potencializou as oportunidades delitivas e permitiu uma "camuflagem urbana" para os infratores sociais devido à facilidade de se esconderem em meio aos cidadãos. Todos esses fatores estão fazendo a segurança pública enfrentar, de forma não convencional, uma verdadeira Guerra Assimétrica. Essa dificuldade de compreensão ao atual momento de crime e violência que enfrentamos vem deixando espaço para que infratores sociais se aproveitem de uma série de fatores inerentes a uma Guerra Assimétrica, como: alta mobilidade do crime; camuflagem urbana; baixa mobilidade do aparato preventivo e repressivo do Estado; burocracia e lentidão estatal nos ajustes de políticas de segurança pública; defasada tecnologia de identificação pessoal e veicular, o que facilita fraudes e a utilização por parte dos infratores de um sistema de redes, sem uma hierarquia vertical, dificultando a identificação de criminosos e o monitoramento e desarticulação de quadrilhas etc. Nesse sendo, a equipe da DGI/SENASP identificou que é imprescindível propor soluções para atacar as deficiências atuais dos procedimentos de segurança pública, ao mesmo tempo em que se busque otimizar os recursos existentes e cortar custos associados a tais procedimentos. Atualmente, vários são os campos de aplicações que têm se utilizado de tecnologias para oferecer novos e mais aperfeiçoados serviços a seus usuários. Mais recentemente, um tema recorrente é o da ciência de dados, onde por meio de técnicas de aprendizado de máquina, Big Data e otimização, o conhecimento sobre determinados assuntos é auxiliado pelo processamento de grandes volumes de dados, no intuito de se obter informações relevantes. Ademais, o Ministério da Justiça e Segurança Pública identificou a necessidade de fornecer soluções e ferramentas tecnológicas para as suas diferentes áreas, incluindo aplicações para processamento de grandes volumes de dados para fomentar políticas públicas e ações de combate à corrupção no âmbito da União, Estados e Municípios. É nesse contexto que se propõe o desenvolvimento de plataforma Big Data para integrar e analisar um grande volume de dados, com aplicação de soluções livres (não proprietárias) e fomento à independência tecnológica, para promover a eficiência e dinamismo que o sistema de segurança pública requer para melhor servir à população brasileira.

**1.6 Resultados Esperados (descrever sucintamente):**

1. Fazer levantamento do estado da arte das plataformas Big Data para processamento em larga escala de dados no domínio da segurança pública, a partir do desenvolvimento feito pela UFC para a SSPDS/CE e da expertise adquirida neste processo;

2. Implantar uma infraestrutura de processamento de larga escala (Big Data) para armazenar e processar os dados integrados da SENASP com o apoio da Diretoria de Tecnologia da Informação e Comunicação do MJSP;

3. Pesquisar e aplicar técnicas de ciência de dados de maneira eficiente para análise e descoberta de conhecimento nos dados Big Data da Segurança Pública;

4. Criar soluções para visualização de dados e inteligência situacional a partir de aplicações analíticas de Big Data relacionadas à segurança pública;

**1.7 Valor Total:** R$ 30.234.117,78

**Obs.: jamais iniciar a execução antes da aprovação final do instrumento.*

**ANEXO 3 – CRONOGRAMA DE EXECUÇÃO**

**1. EXECUÇÃO (Meta, Etapa, Especificação, Indicador Físico e Período de Execução)**

| 1.1 Meta | 1.2 Etapa/Fase | 1.3 Especificação | 1.4 Indicador Físico | | 1.5 Período de Execução | |
|---|---|---|---|---|---|---|
| | | | 1.4.1 Unid. Medida | 1.4.2 Qtde | 1.5.1 Início Mês | 1.5.2 Fim Mês |
| Pesquisa e Desenvolvimento de plataforma Big Data para coleta, processamento e análise de dados de segurança pública.<br>-<br>Pesquisa e Desenvolvimento de painel analítico para suporte à tomada de decisão e governança das integrações<br>-<br>Pesquisa e Desenvolvimento de sistemas para detecção e análise de alvos<br>-<br>Pesquisa e Desenvolvimento de sistema de detecção e abordagem de veículos roubados<br>-<br>Realizar a Prestação de Contas | A) Plataforma Big Data<br>B) Analisador de Crimes<br>C) Painel Analítico<br>D) Painel Governança<br>E) Processador de Eventos Completos<br>F) Rastreamento Objetos Móveis<br>G) Aplicativo Móvel para Policial<br>H) Detector de Fraudes<br>I) Redes Delitivas<br>J) Sistema de indicativo de abordagem veicular<br>K) Seminários de transferência tecnológica | 0A) Plataforma para processamento de dados em larga escala, visando o processamento de dados históricos e fluxo de dados em tempo real, de forma escalável, distribuída e elástica. Esta plataforma servirá como infraestrutura computacional para executar as implantações da SENASP.<br>B) Ferramenta que permitirá a análise de eventos espaço-temporais relacionados com ações delituosas, permitirá a visualização de diferentes camadas de analíticas, incluído mapas de kernel, modelos preditivos, algoritimos de otimização, etc. Esta ferramenta permitirá a criação de mancha criminal.<br>C) Painel para domada de decisão, o qual permitirá a busca e visualização dos analíticos sobre dados de segurança pública de todo país.<br>D) Painel de controle que permitirá o acompanhamento das integrações da SENASP com a secretarias de segurança dos estados da federação. este painel permitirá identificar o estado de cada integração, comunicação com os interessados e análises especificas para auxiliar na governança da DGTI.<br>E) Motor de processamento de eventos complexos visando a detecção de anomalias em dados históricos e fluxo de dados em tempo real. Este motor será responsável pelo envio de notificações | TED<br>TED<br>TED<br>TED<br>TED | 01<br>01<br>01<br>01<br>01 | A) 1<br>B) 2<br>C) 3<br>D) 9<br>E) 15<br>F) 12<br>G) 13<br>H) 14<br>I) 15<br>J) 5<br>H) 12 | A) 22<br>B) 48<br>C) 48<br>D) 30<br>E) 31<br>F) 23<br>G) 24<br>H) 25<br>I) 26<br>J) 24<br>H) 48 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | aos responsáveis, acompanhamento e auditoria das anomalias ocorridas.<br><br>F) Sistema para acompanhamento em tempo real de veículos, pessoas e objetos rastreados através de sensor de geolocalização. Este sistema permitirá a análise de padrões de mobilidade com objetivo de ajudar na gestão de ações policiais.<br><br>G) Aplicativo para dispositivo móvel para Android e IOS para o gerenciamento do policiamento ostensivo e comunitário, possibilitando consultas integradas às bases de dados da SENASP.<br><br>H) Ferramenta que possibilitará a identificação automática de fraudes a partir do reconhecimento de padrões associados a este tipo de ações delituosas, inicialmente com estruturação dos componentes a serem identificados e posteriormente com o uso de tecnologia de aprendizagem de máquina.<br><br>I) Painel Analítico de rede temporal de relacionamentos entre valores que compõem o comportamento delitivo: local, agressor, vitima, objetos, ligações telefônicas, transferências bancárias, etc.<br><br>J) Sistema para monitoramento em tempo real de veículos que transitem em vias urbanas, visando identificar se o carro foi roubado e pemitir o acionamento da polícia para captura do mesmo.<br><br>K) Seminários para realização da transferência de tecnologia para a equipe da SENASP e da TI do Ministério da Justiça. | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | |

**ANEXO 4 – PLANO DE APLICAÇÃO**

**1. PLANO DE APLICAÇÃO (em R$)**

| Especificação | ANO 1 | ANO 2 | ANO 3 | ANO 4 | TOTAL |
|---|---|---|---|---|---|
| **EQUIPE DO PROJETO - BOLSAS DE PESQUISA** | **1.632.000,00** | **1.632.000,00** | **1.632.000,00** | **1.402.000,00** | **6.298.000,00** |
| Coordenador | 252.000,00 | 252.000,00 | 252.000,00 | 252.000,00 | 1.008.000,00 |
| Pesquisador docente | 432.000,00 | 432.000,00 | 432.000,00 | 360.000,00 | 1.656.000,00 |
| Doutorando | 300.000,00 | 300.000,00 | 300.000,00 | 250.000,00 | 1.150.000,00 |
| Mestrando | 360.000,00 | 360.000,00 | 360.000,00 | 300.000,00 | 1.380.000,00 |
| Graduanto | 288.000,00 | 288.000,00 | 288.000,00 | 240.000,00 | 1.104.000,00 |
| **EQUIPE DO PROJETO - CLT** | **4.464.000,00** | **4.464.000,00** | **4.464.000,00** | **2.976.000,00** | **16.368.000,00** |
| Analista negocial | 600.000,00 | 600.000,00 | 600.000,00 | 400.000,00 | 2.200.000,00 |
| Gerente projeto | 240.000,00 | 240.000,00 | 240.000,00 | 160.000,00 | 880.000,00 |
| Analista senior | 1.152.000,00 | 1.152.000,00 | 1.152.000,00 | 768.000,00 | 4.224.000,00 |
| Analista pleno | 1.152.000,00 | 1.152.000,00 | 1.152.000,00 | 768.000,00 | 4.224.000,00 |
| Analista junior | 768.000,00 | 768.000,00 | 768.000,00 | 512.000,00 | 2.816.000,00 |
| Administrativo Pleno | 252.000,00 | 252.000,00 | 252.000,00 | 168.000,00 | 924.000,00 |
| Administrativo | 300.000,00 | 300.000,00 | 300.000,00 | 200.000,00 | 1.100.000,00 |
| **DIÁRIAS - CUSTEIO PARA VIAGENS** | **167.875,00** | **118.500,00** | **118.500,00** | **69.125,00** | **474.000,00** |
| Diárias | 167.875,00 | 118.500,00 | 118.500,00 | 69.125,00 | 474.000,00 |
| **PASSAGENS AÉREAS** | **246.500,00** | **174.000,00** | **174.000,00** | **101.500,00** | **696.000,00** |
| Passagens aéreas | 246.500,00 | 174.000,00 | 174.000,00 | 101.500,00 | 696.000,00 |
| **MATERIAL DE CONSUMO NACIONAL** | **29.151,33** | **22.578,17** | **21.576,51** | **9.000,00** | **82.306,01** |
| Material de escritório | 14.360,00 | 3.000,00 | 8.680,00 | 3.000,00 | 29.040,00 |
| Material de informática | 14.791,33 | 19.578,17 | 12.896,51 | 6.000,00 | 53.266,01 |
| **SERVIÇOS DE TERCEIROS PESSOA FÍSICA** | **888.600,00** | **669.600,00** | **669.600,00** | **408.600,00** | **2.636.400,00** |
| Contração de especialista em visualização analítica | 153.000,00 | 108.000,00 | 108.000,00 | 63.000,00 | 432.000,00 |
| Contração de especialista em inteligencia em tecnologia Big Data | 170.000,00 | 120.000,00 | 120.000,00 | 70.000,00 | 480.000,00 |
| Contração de especialista em integração de dados em Big Data | 85.000,00 | 60.000,00 | 60.000,00 | 35.000,00 | 240.000,00 |
| Contratação de especialista em processo policial de indicativo de abordagem veicular | 212.500,00 | 150.000,00 | 150.000,00 | 87.500,00 | 600.000,00 |
| Outros Serviços de Terceiros | 120.000,00 | 120.000,00 | 120.000,00 | 85.000,00 | 445.000,00 |
| INSS Patronal sobre prestação de serviço | 148.100,00 | 111.600,00 | 111.600,00 | 68.100,00 | 439.400,00 |
| **SERVIÇOS DE TERCEIROS PESSOA JURÍDICA** | **174.000,00** | **164.000,00** | **164.000,00** | **154.000,00** | **656.000,00** |
| Aluguel de espaço para laboratório | 72.000,00 | 72.000,00 | 72.000,00 | 72.000,00 | 288.000,00 |
| Inscrições em congressos | 30.000,00 | 20.000,00 | 20.000,00 | 10.000,00 | 80.000,00 |
| Contratação de provedor de infraestrutura de nuvem | 60.000,00 | 60.000,00 | 60.000,00 | 60.000,00 | 240.000,00 |
| Manutenção de laboratório | 12.000,00 | 12.000,00 | 12.000,00 | 12.000,00 | 48.000,00 |
| **TOTAL DE DESPESAS COM CUSTEIO** | **7.602.126,33** | **7.244.678,17** | **7.243.676,51** | **5.120.225,00** | **27.210.706,01** |
| Despesas operacionais administrativas - Fundação de Apoio | 808.646,05 | 804.964,24 | 804.852,95 | 604.948,54 | 3.023.411,77 |
| **TOTAL GERAL DO PROJETO** | **8.410.772,38** | **8.049.642,41** | **8.048.529,46** | **5.725.173,54** | **30.234.117,78** |

**Obs.: incluir somente os elementos de despesas pertinentes ao projeto.*

**ANEXO 5 – CRONOGRAMA DE DESEMBOLSO**

**1. VALORES (em R$)**

| METAS | DESCRIÇÃO DAS ATIVIDADES | % de execução | ANO 1 | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | MÊS 1 | MÊS 2 | MÊS 4 | MÊS 6 | MÊS 7 | MÊS 10 |
| **Meta 1 - Iniciação** | Elaborar Documentação inicial do projeto, realizando a aquisição de equipamento e a contratação e o treinamento do pessoal para a execução do projeto | 100% | 389.470,62 | | | | | |
| **Meta 2 - Elicitação** | Levantar e analisar problemas e requisitos, realizar pesquisa Científica em Big Data e Segurança Pública | 100% | 110.529,38 | 1.525.247,24 | | | | |
| **Meta 3 - Desenvolvimento** | Devolvimento, teste e implantação de artefatos especificados e desenvolvidos e a | 16% | | 1.713.670,74 | 1.843.494,28 | 545.258,87 | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | manutenção e transferência de tecnologia | | | | | | | |
| **Meta 4 - Conclusão** | Documentar os artefatos desenvolvidos e decidir sobre a aceitação dos artefatos | 11% | | | | 223.826,50 | | |
| **Total** | | | **500.000,00** | **3.238.917,98** | **1.843.494,28** | **769.085,37** | - | - |
| | | | | | | | | |
| **METAS** | **DESCRIÇÃO DAS ATIVIDADES** | **% de execução** | **ANO 2** | | | | | |
| | | | **MÊS 13** | **MÊS 14** | **MÊS 16** | **MÊS 18** | **MÊS 19** | **MÊS 22** |
| Meta 3 - Desenvolvimento | Devolvimento, teste e implantação de artefatos especificados e desenvolvidos e a manutenção e transferência de tecnologia | 28% | 1.843.215,75 | | 1.843.215,75 | | 1.843.215,75 | 1.843.215,75 |
| Meta 4 - Conclusão | Documentar os artefatos desenvolvidos e decidir sobre a aceitação dos artefatos | 26% | 126.123,36 | | 126.123,36 | | 126.123,36 | 126.123,37 |
| **Total** | | | **1.969.339,11** | - | **1.969.339,11** | - | **1.969.339,11** | **1.969.339,12** |
| | | | | | | | | |
| **METAS** | **DESCRIÇÃO DAS ATIVIDADES** | **% de execução** | **ANO 3** | | | | | |
| | | | **MÊS 25** | **MÊS 26** | **MÊS 28** | **MÊS 30** | **MÊS 31** | **MÊS 34** |
| Meta 3 - Desenvolvimento | Devolvimento, teste e implantação de artefatos especificados e desenvolvidos e a manutenção e transferência de tecnologia | 28% | 1.875.012,00 | | 1.875.012,00 | | 1.875.012,00 | 1.875.012,00 |
| Meta 4 - Conclusão | Documentar os artefatos desenvolvidos e decidir sobre a aceitação dos artefatos | 28% | 137.435,44 | | 137.435,44 | | 137.435,44 | 137.435,43 |
| **Total** | | | **2.012.447,44** | - | **2.012.447,44** | - | **2.012.447,44** | **2.012.447,43** |
| | | | | | | | | |
| **METAS** | **DESCRIÇÃO DAS ATIVIDADES** | **% de execução** | **ANO 4** | | | | | |
| | | | **MÊS 37** | **MÊS 38** | **MÊS 40** | **MÊS 42** | **MÊS 43** | **MÊS 46** |
| Meta 3 - Desenvolvimento | Devolvimento, teste e implantação de artefatos especificados e desenvolvidos e a manutenção e transferência de tecnologia | 28% | 1.817.414,31 | | 1.817.414,31 | | 1.817.414,31 | 1.817.414,30 |
| Meta 4 - Conclusão | Documentar os artefatos desenvolvidos e decidir sobre a aceitação dos artefatos | 35% | 171.454,18 | | 171.454,18 | | 171.454,18 | 171.454,18 |
| **Total** | | | **1.988.868,49** | - | **1.988.868,49** | - | **1.988.868,49** | **1.988.868,48** |

**ANEXO 6 – EQUIPE ENVOLVIDA NO PROJETO**

**1. RELAÇÃO DA EQUIPE ENVOLVIDA NO PROJETO** (Art. 6º, § 1º, incisos III e IV c/c § 3º do Decreto nº 7.423/2010)

| | Nome | CPF | SIAPE | Vinculação | Endereço | CEP | Município/UF | Telefone | E-mail | Função no Projeto | Ca Hor |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | José Antonio Fernandes de Macêdo | 00.208.177-90 | 364969 | Professor do Magistério Superior | Rua: Albuquerque, 3300 Aptº 1302 Bl B Torre Santorini, Bairro: Manuel Dias Branco | 60191-355 | Fortaleza/CE | (85) 99134-9000 | jose.macedo@dc.ufc.br | Coordenador | |
| 2 | Paulo Antonio Leal Rêgo | 672.422.273-72 | 2998175 | Professor do Magistério Superior | Rua: Costa Sousa, nº 100 - Aptº 1703 - Torre 1 Bairro: Benfica | 600020-300 | Fortaleza/CE | (85) 98854-6885 | pauloalr@gmail.com | Pesquisador | |

**Relacionar a Equipe Técnica constituída;*

***Observar carga horária e valores máximos permitidos;*

****Relacionar cada participante às metas e/ou atividades apresentadas no cronograma de execução.*

*Obs.: É obrigatório identificar quais participantes são funcionários públicos, bem como observar toda a legislação específica quanto à concessão de bolsas ou qualquer vantagem pecuniária ao servidor.*

**ANEXO 7 – PROJETO BÁSICO**

[INCLUIR PROJETO BÁSICO ELABORADO]

** A inclusão do Projeto Básico só se aplica em casos de projetos de "obras e instalações laboratoriais" e de "aquisição de equipamentos e materiais permanentes nacionais e importados".*

[Colocar Local], 29 de maio de 2019

[Colocar Nome do Coordenador(a) do Projeto]
Coordenador(a) do Projeto

*Formulário elaborado conforme:*

***LEI Nº 8.666, DE 21 DE JUNHO DE 1993***

*"Art. 116. Aplicam-se as disposições desta Lei, no que couber, aos convênios, acordos, ajustes e outros instrumentos congêneres celebrados por órgãos e entidades da Administração.*

*§ 1º A celebração de convênio, acordo ou ajuste pelos órgãos ou entidades da Administração Pública depende de prévia aprovação de competente plano de trabalho proposto pela organização interessada, o qual deverá conter, no mínimo, as seguintes informações:*

*I - identificação do objeto a ser executado;*

*II - metas a serem atingidas;*

*III - etapas ou fases de execução;*

*IV - plano de aplicação dos recursos financeiros;*

*V - cronograma de desembolso;*

*VI - previsão de início e fim da execução do objeto, bem assim da conclusão das etapas ou fases programadas;*

*VII - se o ajuste compreender obra ou serviço de engenharia, comprovação de que os recursos próprios para complementar a execução do objeto estão devidamente assegurados, salvo se o custo total do empreendimento recair sobre a entidade ou órgão descentralizador".*

***DECRETO Nº 7.423, DE 31 DE DEZEMBRO DE 2010***

*"Art. 6º O relacionamento entre a instituição apoiada e a fundação de apoio, especialmente no que diz respeito aos projetos específicos deve estar disciplinado em norma própria, aprovada pelo órgão colegiado superior da instituição apoiada, observado o disposto na Lei nº 8.958, de 1994, e neste Decreto.*

*§ 1º Os projetos desenvolvidos com a participação das fundações de apoio devem ser baseados em plano de trabalho, no qual sejam precisamente definidos:*

*I - objeto, projeto básico, prazo de execução limitado no tempo, bem como os resultados esperados, metas e respectivos indicadores;*

*II - os recursos da instituição apoiada envolvidos, com os ressarcimentos pertinentes, nos termos do art. 6º da Lei nº 8.958, de 1994;*

*III - os participantes vinculados à instituição apoiada e autorizados a participar do projeto, na forma das normas próprias da referida instituição, identificados por seus registros funcionais, na hipótese de docentes ou servidores técnico-administrativos, observadas as disposições deste artigo, sendo informados os valores das bolsas a serem concedidas; e*

*IV - pagamentos previstos a pessoas físicas e jurídicas, por prestação de serviços, devidamente identificados pelos números de CPF ou CNPJ, conforme o caso.*

*§ 2º Os projetos devem ser obrigatoriamente aprovados pelos órgãos colegiados acadêmicos competentes da instituição apoiada, segundo as mesmas regras e critérios aplicáveis aos projetos institucionais da instituição.*

*§ 3º Os projetos devem ser realizados por no mínimo dois terços de pessoas vinculadas à instituição apoiada, incluindo docentes, servidores técnico-administrativos, estudantes regulares, pesquisadores de pós-doutorado e bolsistas com vínculo formal a programas de pesquisa da instituição apoiada.*

*§ 4º Em casos devidamente justificados e aprovados pelo órgão colegiado superior da instituição apoiada poderão ser realizados projetos com a colaboração das fundações de apoio, com participação de pessoas vinculadas à instituição apoiada, em proporção inferior à prevista no § 3º, observado o mínimo de um terço.*

*§ 5º Em casos devidamente justificados e aprovados pelo órgão colegiado superior da instituição apoiada, poderão ser admitidos projetos com participação de pessoas vinculadas à instituição apoiada em proporção inferior a um terço, desde que não ultrapassem o limite de dez por cento do número total de projetos realizados em colaboração com as fundações de apoio.*

*§ 6º Para o cálculo da proporção referida no § 3º, não se incluem os participantes externos vinculados a empresa contratada.*

*§ 7º Em todos os projetos deve ser incentivada a participação de estudantes.*

*§ 8º A participação de estudantes em projetos institucionais de prestação de serviços, quando tal prestação for admitida como modalidade de extensão, nos termos da normatização própria da instituição apoiada, deverá observar a Lei nº 11.788, de 25 de setembro de 2008.*

*§ 9º A participação de docentes e servidores técnico-administrativos nos projetos de que trata o § 1º deste artigo deve atender a legislação prevista para o corpo docente e servidores técnico-administrativos da instituição apoiada, além das disposições específicas, na forma dos §§ 3º, 4º, 5º e 6º.*

*§ 10. No caso de projetos desenvolvidos em conjunto por mais de uma instituição, o percentual referido no § 3º poderá ser alcançado por meio da soma da participação de pessoas vinculadas às instituições envolvidas.*

*§ 11. No âmbito dos projetos de que trata o § 1º deste artigo, a instituição apoiada deve normatizar e fiscalizar a composição das equipes dos projetos, observadas as disposições do Decreto nº 7.203 de 04 de junho de 2010.*

*§ 12. É vedada a realização de projetos baseados em prestação de serviço de duração indeterminada, bem como aqueles que, pela não fixação prazo de finalização ou pela reapresentação reiterada, assim se configurem.*

*§ 13. Deve haver incorporação, à conta de recursos próprios da instituição apoiada, de parcela dos ganhos econômicos decorrentes dos projetos de que trata o § 1º, observada a legislação orçamentária".*

**MODELOS DE MEMÓRIA DE CÁLCULO DETALHADA**

| Natureza da Despesa | Bolsas | | | | | |
|---|---|---|---|---|---|---|
| Item | Nível/atividade | Horas/mês | Valor mensal da bolsa | Nº de bolsistas | Nº de meses | Total |
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| 5 | | | | | | |
| Subtotal | | | | | | |

| Natureza da Despesa | Diárias (Observar Decreto nº 5.992/2006 alterado pelo nº 6.907/2009) | | | | |
|---|---|---|---|---|---|
| Item | Discriminação da despesa | Unidade de Medida | Quantidade | Custo Unitário | Total |
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |
| Subtotal | | | | | |

| Natureza da Despesa | Passagens e Despesas com Locomoção | | | | |
|---|---|---|---|---|---|
| Item | Discriminação da despesa | Unidade de Medida | Quantidade | Custo Unitário | Total |
| 1 | Transporte urbano | | | | |
| 2 | Passagens áreas | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |
| Subtotal | | | | | |

| Natureza da Despesa | Material de Consumo | | | | |
|---|---|---|---|---|---|
| Item | Discriminação da despesa | Unidade de Medida | Quantidade | Custo Unitário | Total |
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |
| Subtotal | | | | | |

| Natureza da Despesa | Pagamento de retribuição pecuniária | | | | |
|---|---|---|---|---|---|
| Item | Discriminação da despesa | Unidade de Medida | Quantidade | Custo Unitário | Total |
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |
| Subtotal | | | | | |

| Natureza da Despesa | Impostos e contribuições patronais | | | | |
|---|---|---|---|---|---|
| Item | Discriminação da despesa | Unidade de Medida | Quantidade | Custo Unitário | Total |
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |
| Subtotal | | | | | |

**Os modelos também podem ser utilizados para outras naturezas de despesas.*

Documento assinado eletronicamente por **JOSE ANTONIO FERNANDES DE MACEDO, Coordenador**, em 29/05/2019, às 09:51, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufc.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0804140** e o código CRC **2B79A29E**.

**Referência:** Processo nº 23067.015836/2019-58 SEI nº 0804140

# Anexo IV – Questionário e Respostas: CNJ

Esta solicitação busca entender melhor *os processos técnicos pelos quais as práticas judiciárias são informadas por processos automatizados*. Objetiva-se ter maior conhecimento sobre o que está em desenvolvimento e o que está sendo implementado. Com isso, e conhecendo melhor as dificuldades impostas pelos diferentes projetos e os avanços neles alcançados, entende-se que os agentes públicos possam tomar decisões informadas, melhorando a efetividade dos serviços públicos.

Em razão disso, solicita-se, encarecidamente, que as seguintes perguntas sejam respondidas:

1. Sabe-se de técnicas de previsão matemáticas em uso (algoritmos, inteligência artificial ou modelos estatísticos) - ou que tenham sido usadas nos últimos 5 anos - para a tomada automatizada de decisões ou para informar a tomada de decisões pelos magistrados brasileiros?

2. Há uma compilação dos sistemas em uso? Esses dados estão disponíveis em algum portal de dados? *Nesse caso, solicita-se anexar o banco de dados usado para o cálculo (em formato aberto: CSV ou XLSX) ou o link correspondente, se disponível pela Internet*.

3. Sabe-se do objetivo de cada sistema automatizado? Seria possível informa-los?

4. São utilizados softwares nos sistemas?

Em caso afirmativo, solicita-se:

a. Nome (s) do (s) programa(s);

b. O(s) programa(s) foi/foram desenvolvidos pela iniciativa pública ou privada?

c. Nome da(s) empresa(s) fornecedora (s) ou da unidade responsável pelo desenvolvimento do programa;

d. Informações sobre o processo pelo qual o programa foi adquirido ou desenvolvido;

e. Quantia paga pelo programa, se aplicável;

f. Cópia dos contratos, se aplicável;

g. Data da última atualização do programa;

h Foram feitas auditorias no software? Os relatórios correspondentes estão disponíveis para consulta?

i. Foram feitas avaliações internas ou externas da qualidade dos resultados? Os relatórios correspondentes estão disponíveis para consulta?

j. Estimativa quanto ao número de processos nos quais os programas foram utilizados;

k. Quantas variáveis são levadas em consideração por cada um dos softwares?

l. *Solicita-se anexar, caso possível, a lista das variáveis levadas em consideração por cada um dos sistemas*;

m. Em quais bancos de dados o(s) sistema(s) se apoia(m) para operar?

n. Qual entidade ou entidades gera esses dados? Como os dados são gerados? *Solicita-se conhecer a entidade responsável por gerar os dados em relação a cada uma das variáveis que são levadas em consideração*.

o. Algum dos dados subjacentes a essas variáveis não é produzido pelo Estado?

p. Com que frequência os dados são atualizados?

q. Houve alguma avaliação de possíveis vieses ou discriminação indevida desencadeados pelo sistema contra grupos populacionais específicos, particularmente grupos marginalizados?

r. Os dados utilizados para alimentar os sistemas são públicos? Estão disponíveis em algum portal de dados ministerial ou nacional? *Em caso afirmativo, solicita-se anexar o banco de dados, em formato aberto (CSV ou XLSX), usado para o cálculo ou o link correspondente, se disponível na Internet.*

s. O(s) algoritmo(s) utilizado(s) é/são aberto(s)?

t. Como os algoritmos foram treinados?

**u. Quem são os responsáveis, caso cidadãos sejam prejudicados pelos sistemas automatizados?**

**w. Os operadores dos sistemas recebem treinamento técnico para manipulá-los? E para compreender os outputs gerados?**

5. Quais unidades do Ministério / Secretaria usam algoritmos para orientar e informar as práticas de segurança pública e de policiamento? Solicita-se anexar a documentação correspondente a cada uma delas, incluindo as variáveis utilizadas, os bancos de dados dos quais essas variáveis são extraídas, nome legal de cada uma das empresas privadas que fornecem o software pelo qual os algoritmos são executados, bem como os contratos correspondentes e a documentação que formalizou os processos de aquisição.

Grata.

Registro Ouvidoria/CNJ: **254877**
À Senhora

Encaminhamos as informações prestadas pelo(a) Departamento de Tecnologia da Informação do Conselho Nacional de Justiça, para seu conhecimento:

Prezados Senhores,

Neste momento a solicitação em tela não está disponível para tratamento no âmbito deste Conselho por força de insuficiência de registros próprios dos Acordos Técnicos e dos projetos que julgamos pertinentes ao pedido de informação. Complementarmente, por se tratar de demanda que exige esforço e recursos adicionais para análise, produção e controle das informações solicitadas, apresentamos nossas escusas pela falta de condições para gerar tais informações, uma vez que demandaria esforços exclusivos.

Diante de tais fatos, consideramos prejudicada a possibilidade de atendimento ao pleito. Entretanto, sugerimos as seguintes fontes para auxiliar na busca pelas respostas desejadas:

a) O item 4.h pode ser parcialmente acolhido mediante consulta ao Acórdão TCU. https://portal.tcu.gov.br/imprensa/noticias/tcu-aponta-atrasos-na-implementacao-do-processo-judicial-eletronico.htm

b) A página do PJe pode oferecer dados referenciais http://www.pje.jus.br/navegador/

c) No que tange ao uso de inteligência artificial, encaminhamos página de projeto desenvolvido em parceria com o CNJ: https://www.tjro.jus.br/noticias/item/10172-inteligencia-artificial-do-tjro-potencialidade-do-sinapses-e-apresentada-no-conipjud-2018

d) O Sistema Eletrônico de Execução Unificado – SEEU, também pode ser objeto de análise: https://seeu.pje.jus.br/seeu/

e) No link https://www.cnj.jus.br/sistemas/ há o portfólio de soluções de TI. Alguns sistemas possuem informações e documentação.

Departamento de Tecnologia da Informação e Comunicação

Conselho Nacional de Justiça

DTI@cnj.jus.br

+55 61 2326-5318"

Atenciosamente,

**Ouvidoria**
**Conselho Nacional de Justiça**
SEPN 514, bloco B, lote 7, 70760-542 Brasília (DF)
Telefone: (61) 2326-4607 / 2326-4608

CNJ CONSELHO NACIONAL DE JUSTIÇA

---

Solicita-se que, na medida do possível, as perguntas em anexo sejam respondidas.

---

Esta solicitação busca entender melhor os processos técnicos pelos quais as práticas judiciárias são informadas por processos automatizados. Objetiva-se ter maior conhecimento sobre o que está em desenvolvimento e o que está sendo implementado. Com isso, e conhecendo melhor as dificuldades impostas pelos diferentes projetos e os avanços neles alcançados, entende-se que os agentes públicos possam tomar decisões informadas, melhorando a efetividade dos serviços públicos. Em razão disso, solicita-se, encarecidamente, que as perguntas em anexo sejam respondidas.

Grata.

No caso de indeferimento de acesso a informações ou às razões da negativa do acesso, poderá o interessado interpor recurso contra a decisão no prazo de 10 (dez) dias a contar da sua ciência, conforme art. 15 da Lei n.º 12.527/2011 e art. 18 da Resolução CNJ n.º 215/2015. Caso considere haver necessidade,
clique aqui para fazer o recurso.

Clique AQUI para avaliar o atendimento.
Este é um e-mail automático. Por favor, não responda.
Para entrar em contato, utilize o portal do CNJ, www.cnj.jus.br, menu Fale Conosco
Este é um serviço meramente informativo, não tendo, portanto, cunho oficial.

---

**Solicitação de Informação - CNJ.pdf**
269K

# Anexo V - Questionário e Respostas: Projeto *Cérebro*

**Questionário Semiestruturado Respondido: Projeto Cérebro**

Este questionário busca entender melhor os processos técnicos pelos quais as práticas judiciárias são informadas por processos automatizados. Objetiva-se alcançar maior conhecimento sobre o que está em desenvolvimento e o que está sendo implementado. Com isso, e conhecendo melhor as dificuldades impostas pelos diferentes projetos e os avanços neles alcançados, entende-se que os agentes públicos possam tomar decisões informadas, melhorando a efetividade dos serviços públicos.

*Caso não haja possibilidade de fornecer as informações solicitadas, pede-se, encarecidamente, que se compartilhe o que for possível.*

**Seção 1 - Informações básicas sobre atores de IA.**

**1.** Informações biográficas

a. **Nome**: Felipe Leitão Valadares Roquete

b. **Título**: Servidor Público efetivo da carreira de Especialista em Políticas Públicas e Gestão Governamental do Ministério da Economia

Bacharel em Direito (UFMG) e Mestre em Ciência Política (UnB)

Coordenador-Geral de Análise Antitruste da Superintendência-Geral do Conselho Administrativo de Defesa Econômica

c. **Organização em que trabalha**: Conselho Administrativo de Defesa Econômica (Cade)

**Seção 2 - Detalhes sobre o Projeto Cérebro.**

***2.*** *Qual o objetivo do Projeto Cérebro?*

R.: Desenvolver ferramentas tecnológicas e técnicas que possibilitem agregar qualidade às investigações de infrações à ordem econômica, bem como a adoção de estratégias proativas de detecção de cartéis.

***3.*** *Quais são os principais benefícios do projeto?*

R.: Ampliação do escopo das investigações realizadas e redução no tempo de análise.

***4.*** *Houve algum impedimento ou dificuldade no desenvolvimento do projeto?*

R.: As principais dificuldades foram (i) as restrições para adaptar à realidade brasileira as técnicas desenvolvidas para realidades institucionais diversas e (ii) criação de massa crítica para o desenvolvimento de técnicas inovadoras.

***5.*** *Em quais áreas você acha que um sistema como o Projeto Cérebro geraria grandes benefícios?*

R.: Na área de investigação de cartéis em licitações.

***6.*** *O que você acha que os formuladores de políticas públicas ou operadores do sistema deveriam entender sobre o projeto?*

R.: Como todo projeto de inovação, é necessário compreender que a experimentação pode não prover resultados de curto prazo e/ou necessitar constantes aperfeiçoamentos/melhorias.

*7.* *Em relação aos softwares desenvolvidos:*

*a.* *Como os programas foram elaborados?*

R.: As ferramentas foram elaboradas utilizando-se os softwares R, Python, neo4J, Qlicksense e Elasticsearch.

*b.* *Foram feitas auditorias no software? Há relatórios correspondentes disponíveis?*

R.: Não foram realizadas auditorias, pois não se trata de um software, mas de diversas tarefas de mineração de dados, algoritmos e scripts que utilizam variáveis diversas, relacionadas à detecção de cartéis.

*c.* *Foram feitas avaliações internas ou externas quanto à qualidade dos resultados?*

R.: Sim, foram realizadas avaliações internas. Ademais, uma vez que várias das técnicas foram compartilhadas com órgãos de persecução e controle, tais órgãos realizaram avaliações quanto à acurácia dos resultados, possibilitando o aperfeiçoamento das ferramentas.

*d.* *O algoritmo utilizado é aberto?*

R.: Não.

*e.* *Quantas variáveis são levadas em consideração pelo software?*

R.: Não se trata de um software, mas de diversas tarefas de mineração de dados, algoritmos e scripts que utilizam variáveis diversas, relacionadas à detecção de cartéis.

*f. Seria possível fornecer uma lista das variáveis consideradas?*

R.: Não, dada a sensibilidade do objeto.

*g. Em quais bancos de dados o sistema se apoia para operar?*

R.: Bancos de dados de compras públicas.

*h. Como os dados são gerados? Qual entidade é responsável por gerar os dados em relação a cada uma das variáveis levadas em consideração?*

R.: Os dados são gerados (i) sob demanda e (ii) a partir de pesquisas realizadas pelos investigadores/analistas.

*i. Com que frequência os dados são atualizados?*

R.: Não há periodicidade fixa.

*j. Os dados são públicos? Estão disponíveis em algum portal de dados ministerial ou nacional? Seria possível compartilhar o link?*

R.: Os dados de compras públicas federais são públicos: http://compras.dados.gov.br/docs/home.html

*k. Houve alguma avaliação de possíveis vieses ou discriminação indevida desencadeados pelo sistema contra grupos populacionais específicos, particularmente grupos marginalizados?*

R.: A avaliação FAT (Fairness, Accountability, and Transparency) dos algoritmos estão no horizonte do projeto, ainda que não tenham sido implementadas, principalmente porque ainda não são utilizadas técnicas de aprendizagem de máquina, dada a reduzida casuística (base de treinamento).

*l. Os sistemas foram desenvolvidos para tomar decisões autonomamente ou para auxiliar na tomada de decisões?*

R.: No atual estágio do projeto, os resultados constituem insumos para a tomada de decisões.

*m. Como se deu o design das ferramentas? Quais foram os modelos escolhidos?*

R.: Informação restrita, dada a sensibilidade do objeto.

*n. Quais são os outputs gerados por cada um dos sistemas? Como esses outputs são interpretados?*

R.: Informação restrita, dada a sensibilidade do objeto.

**Seção 3 - Impactos e projeções gerais.**

Prevendo os próximos 5 a 10 anos ...

***8. Existe alguma estimativa quanto ao número de pessoas afetadas pelos programas?***

R.: Não.

***9.*** *Quais os desafios mais significativos que os cidadãos brasileiros enfrentarão devido ao uso de metodologias orientadas a dados (data-driven methodologies) para a prestação de serviços?*

R.: Desenvolver estratégias para evitar que modelos "black-box" de machine learning sejam utilizados para definição autônoma de políticas públicas, sem que passem (i) previamente, por uma análise de FAT e (ii) durante sua utilização, pela supervisão humana dos resultados produzidos, a fim de possibilitar a produção e perpetuação de vieses nos algoritmos.

***10.*** *O que você acha que os formuladores de políticas deveriam fazer agora para enfrentar esses desafios?*

R.: Devem olhar par trás e para o lado, em busca de experiências pretéritas e em curso, visando identificar boas práticas e evitar a reprodução acrítica de metodologias.

***11.*** *Quais são as principais oportunidades para que o governo brasileiro alavanque o uso, para o bem comum, de algoritmos, IA e outros métodos orientados a dados (data-driven)?*

R.: Existem diversas iniciativas isoladas no governo federal. Acredito que a principal oportunidade seria criar um ambiente para compartilhamento das experiências e resultados, a fim de evitar sobreposições, retrabalho e desperdício.