UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS

FACULDADE NACIONAL DE DIREITO

SEGURANÇA PÚBLICA DATIFICADA E POLICIAMENTO PREDITIVO:

Uma breve análise acerca do uso do *Big Data* pela polícia, seus métodos e vulnerabilidades.

GABRIELLA DE SOUSA RODRIGUES

Rio de Janeiro

2022

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS

FACULDADE NACIONAL DE DIREITO

SEGURANÇA PÚBLICA DATIFICADA E POLICIAMENTO PREDITIVO:

Uma breve análise acerca do uso do *Big Data* pela polícia, seus métodos e vulnerabilidades.

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em direito, sob a orientação do Professor Philippe Oliveira de Almeida.

Rio de Janeiro

2022

GABRIELLA DE SOUSA RODRIGUES

SEGURANÇA PÚBLICA DATIFICADA E POLICIAMENTO PREDITIVO:

Uma breve análise acerca do uso do *Big Data* pela polícia, seus métodos e vulnerabilidades.

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em direito, sob a orientação do Professor Philippe Oliveira de Almeida.

Data da Aprovação: __ / __ / ____.

Banca Examinadora:

_____

Philippe Oliveira de Almeida - Orientador

_____

XXX – Membro da Banca

_____

XXX – Membro da Banca

Rio de Janeiro

2022

AGRADECIMENTOS

"Eu nunca desisti, então eu queria muito agradecer a mim hoje." — Discurso de Anitta em seu show no Rock In Rio, 2019.

À eterna Silvia Silva de Souza, minha avó, obrigada por sempre te me encorajado a ser uma mulher independente.

À Mônica Machado de Sousa Rodrigues e Edvaldo Macedo Rodrigues, meus pais, agradeço pelo carinho, incentivo e por todo o esforço que fizeram para que eu tivesse acesso a melhor educação possível, desde sempre. Obrigada por acreditarem em mim.

À Isabella de Sousa Rodrigues, minha irmã e melhor amiga, agradeço por sempre enxergar o melhor em mim e me ter como um exemplo a ser seguido.

Ao Thallis Lima Câmara, primeiro amigo que fiz na vida, aos três anos de idade, e cuja amizade perdura até hoje. Obrigada por todos os conselhos e por sempre ter estado ao meu lado, ainda que de longe.

Às minhas amigas de sempre: Beatriz Carlos Andrade de Oliveira, Carolina Miguel das Chagas, Juliana Lopes Marques, Larissa Rodrigues Ferreira e Thamiris de Castro Abrantes, há quase vinte anos juntas. Obrigada por todos os momentos compartilhados, na alegria e na tristeza.

À Ana Carolina Barros e Marcela Medrado, o trio inseparável da Nacional. Agradeço pelas risadas compartilhadas, pelo colo e incentivo.

À Vitória Ornellas, Ana Carolina Mendes e Edson Cezário, amigos da FND e da cena (k)lubber. Agradeço por toda a diversão compartilhada.

Às amizades que fiz na Nacional: Bruna Mussi, Cynthia, Fernanda Benevides, Flávia Delgadillo, Luísa Lousada. Obrigada por pela companhia durante esses cincos anos.

Ao Professor Philippe Oliveira de Almeida, meu orientador. Agradeço pela paciência e ensinamentos.

Por fim, à UFRJ, por todas as oportunidades, experiências e por ter sido meu segundo lar durante cinco anos. Sempre foi o meu sonho ser aluna desta Universidade e tive o imenso prazer de realiza-lo. Obrigada por tudo.

“All I ever wanted was the world.”

– Marina and the Diamonds

RESUMO

O presente trabalho pretende analisar objetivamente o instituto do policiamento preditivo, ferramenta aplicada na seara da segurança pública como método para prever crimes, a partir da utilização do *Big Data* e amplamente difundido em diversos países, tais como Estados Unidos, Reino Unido, Brasil e Japão. Para tanto, prioristicamente, será explorada a vigilância hierárquica à luz da teoria foucaultiana, bem como o surgimento da nova lógica de acumulação capitalista, ou seja, o capitalismo de vigilância, de acordo com os ensinamentos de Zuboff. Em seguida, será oferecida uma breve definição sobre o conceito e aplicações do *Big Data*, principalmente no contexto criminal. Também apresentaremos uma definição sobre o policiamento preditivo, acrescido de um estudo detalhado sobre suas modalidades (*place-based*, *person-based* e *suspect-based*), observando os seus mitos e vulnerabilidades (discriminação racial, *bad data*, transparência e *accountability*), além da questão regulatória. Por fim, o método utilizado foi o hipotético-dedutivo.

Palavras-chaves: Policiamento Preditivo; Big Data; Tecnologia; Capitalismo de vigilância; Segurança Pública.

ABSTRACT

This paper aims to objectively analyze the institute of predictive policing, a tool applied in the field of public safety as a method to predict crimes, from the use of Big Data and widely spread in several countries, such as the United States, United Kingdom, Brazil and Japan. To this end, we will explore hierarchical surveillance in the light of Foucauldian theory, as well as the emergence of the new logic of capitalist accumulation, i.e., surveillance capitalism, according to the teachings of Zuboff. Next, a brief definition will be offered on the concept and applications of Big Data, especially in the criminal context. We will also present a definition of predictive policing, plus a detailed study of its modalities (place-based, person-based, and suspect-based), noting its myths and vulnerabilities (racial discrimination, bad data, transparency, and accountability), as well as the regulatory issue. Finally, the hypothetical-deductive method was used.

Keywords: Predictive Policing; Big Data; Technology; Surveillance Capitalism; Public Security.

SUMÁRIO

1 INTRODUÇÃO

Uma história onde as normas de convívio são ditadas por um sistema composto por uma rede de computadores, onisciente, com olhos (câmera de vigilância) espalhadas por todos os cantos da cidade, capaz de analisar a mente de cada cidadão, operando uma verdadeira varredura. O resultado dessa análise revela o estado mental do indivíduo e o classifica por cores e números, gerando uma estatística denominada de coeficiente criminal. A partir desse valor, mede-se a probabilidade daquele sujeito cometer um crime, antes mesmo dele sequer cogitar agir. O coeficiente, gerado pela análise de dados proveniente do ser humano, de sua alma, pode gerar dois resultados: o primeiro, uma intervenção que se procederá com a prisão e tratamento do indivíduo (uma verdadeira internação); o segundo, na hipótese do sujeito apresentar um coeficiente de criminalidade muito elevado, ele será executado por um inspetor. Novamente, quem decide? A máquina.

Esse é o enredo do anime *Psycho-Pass* (2012) que se passa num futuro distópico localizado no Japão. Uma obra com influências cyberpunk, cuja trama já foi retratada em outras obras de sci-fi, na qual os algoritmos de previsão são um ponto central. No anime, o sistema Sybil é o responsável por ditar as regras sociais, julgando os cidadãos por seus sentimentos e desejos, e não por suas ações.

Em que ponto se interligam o enredo da animação japonesa com a realidade? Algoritmos de previsão de crime já são uma realidade! e estão sendo vastamente empregados pelas forças policiais. Na maioria dos casos, num contexto de ausência normativa e, portanto, operando sem limites e utilizando a máscara da neutralidade e efetividade como fundamento para sua aplicação.

Em *SEGURANÇA PÚBLICA DATIFICADA E POLICIAMENTO PREDITIVO: Uma breve análise acerca do uso do Big Data pela polícia, seus métodos e vulnerabilidades,* pretende-se analisar o conjunto de técnicas denominado de policiamento preditivo, definindo tal processo, investigando seus métodos e analisando seus desafios e consequências. Esta técnica que importa no uso do *Big Data,* a partir análise coleta, análise e processamento de dados por um algoritmo na esfera criminal, com o propósito de predizer crimes vem sendo

empregada em diversos países, tais como Estados Unidos, Brasil, Reino Unido e Japão. O cenário atual revela que as consequências decorrentes do uso de *softwares* de predição pelo aparato policial são perigosas e cruéis. Concatenado a isso, a ausência de normas reguladoras que direcionem e limitem o uso dessa tecnologia agravam ainda mais a atual conjuntura. Desse modo, justifica-se a urgência em debater o assunto, a fim de esclarecer sobre o que se trata o policiamento preditivo, como ele funciona e suas consequências, tendo em vista que seus efeitos atuam diretamente sobre os princípios e garantias fundamentais dos indivíduos.

Para a construção do trabalho proposto, inicialmente, será feita uma breve introdução sobre o surgimento da internet e, a partir disto, o nascimento da sociedade informacional. Após, examinaremos o fenômeno da vigilância hierárquica sob a égide da teoria foucaultiana. Ainda no mesmo capítulo, apresentaremos a nova lógica capitalista, ou seja, o capitalismo de vigilância, à luz dos fundamentos apresentados por Soshanna Zuboff, e finalmente trataremos das tecnologias de vigilância, com ênfase no *Big Data*, partindo para sua definição e aplicação. Por fim, será apresentada uma breve introdução ao policiamento preditivo.

No segundo capítulo, trataremos exclusivamente do policiamento preditivo. Inicialmente, daremos continuidade ao estudo do *software* da Predpol, introduzido no capítulo anterior. Em seguida, apresentaremos uma definição de policiamento preditivo e examinaremos os métodos de análise de crime, sua taxonomia, e seus desafios. Depois, trataremos brevemente dos mitos, desafios (discriminação racial, *bad data*, transparência e *accountability)* sobre o policiamento preditivo. Finalmente, abordaremos brevemente a questão da regulação sobre a problemática.

2 INTERNET, VIGILÂNCIA E NOVAS TECNOLOGIAS: A ASCENSÃO DA ERA DOS DADOS

Este primeiro capítulo tem o intuito de introduzir o tema concernente à vigilância na contemporaneidade e o advento de novas tecnologias que propiciam a sua consumação, em especial o *Big Data*. Daremos partida com a contextualização histórica sobre o surgimento e difusão da internet, ferramenta crucial nos dias atuais e responsável pela estruturação da sociedade em rede.

Após, abordaremos a questão da vigilância, principalmente à luz da teoria foucaultiana, perpassando pela instituição de um novo modelo de capitalismo (de vigilância) e, finalmente, dissertaremos acerca das novas tecnologias de vigilância digitais com enfoque no *Big Data*, e introduzindo ao final a temática em comento inserida no contexto da segurança pública.

2.1 Surgimento da internet e o desenvolvimento da sociedade informacional

Inicialmente, antes de adentrarmos no tema concernente à vigilância e novas tecnologias de vigilância, há de se discorrer, ainda que brevemente, sobre o surgimento e evolução da internet, visto que essa ferramenta pode ser considerada como uma das maiores invenções da humanidade, responsável por abrir espaço para o surgimento de demais invenções e por revolucionar a maneira como a sociedade existe e se comporta nos dias atuais.

O pontapé inaugural da internet se inicia no contexto de pós Segunda Guerra Mundial. Com a vitória dos aliados (aliança composta pelos Estados Unidos, Reino Unido e União Soviética) sobre o grupo do eixo (aliança composta pela Alemanha, Japão e Itália) em 1945, uma nova ordem se estabeleceu, culminando em novos sistemas econômicos, políticos e sociais adotados por diversos países. Nesse sentido, as superpotências da época, Estados Unidos e União Soviética, deram início embate ideológico que ficou conhecido como Guerra Fria.

Nesse sentido, durante a Guerra Fria, a disputa entre o eixo capitalista e o eixo comunista resultou num imenso desenvolvimento tecnológico e armamentista. Em 4 de outubro

de 1957 a URSS lançou o primeiro satélite artificial da Terra, conhecido como "*Sputinik*". Como resposta, no ano de 1963, o Departamento de Defesa dos EUA lançou a Agência de Projetos de Pesquisa Avança (ARPA), que mais tarde daria origem à internet.[1]

Em continuidade, em 1969 os Estados Unidos criaram a internet, na época chamada de Arpanet e que tinha como objetivo interligar laboratórios de pesquisa no país. Contudo, somente no final da década de 1980 o uso comercial da internet foi liberado no país. Foi então a partir da década de 90 que a internet começou a gerar um impacto na sociedade e modificar o dia a dia das pessoas da época e que perdura até os dias atuais.

À vista disso, o sociólogo espanhol e referência no assunto, Manuel Castells[2], compara a internet a uma rede elétrica ou motor elétrico, tendo em vista a sua aptidão em distribuir o poder da informação em todas as atividades humanas. De acordo com o professor:

> A Internet é o tecido de nossas vidas. Se a tecnologia da informação é hoje o que a eletricidade foi na Era Industrial, em nossa época a Internet poderia ser equiparada tanto a uma rede elétrica quanto ao motor elétrico, em razão de sua capacidade de distribuir a força da informação por todo o domínio da atividade humana. Ademais, à medida que novas tecnologias de geração e distribuição de energia tornaram possível a fábrica e a grane corporação como os fundamentos organizacionais da sociedade industrial, a Internet passou a ser a base tecnológicas para a forma organizacional da Era da Informação: a rede.
>
> Uma rede é um conjunto de nós interconectados. A formação de redes é uma prática humana muito antiga, mas as redes ganharam vida nova em nosso tempo transformando-se em redes de informação energizadas pela Internet. As redes têm

[1]Segundo Manuel Castells: "A ARPA foi formada em 1958 pelo Departamento de Defesa dos Estados Unidos com a missão de mobilizar recursos de pesquisa, particularmente do mundo universitário, com o objetivo de alcançar superioridade tecnológica militar em relação à União Soviética na esteira do lançamento do primeiro Sputnik em 1957. A Arpanet não passava de um pequeno programa que surgiu de um dos departamentos da ARPA, o Information Processing Techniques Office (IPTO), fundado em 1962 com base numa unidade preexistente. O objetivo desse departamento, tal como definido por seu primeiro diretor, Joseph Licklider, um psicólogo transformado em cientista da computação no Massachusetts Institute of Technology (MIT), era estimular a pesquisa em computação interativa. Como parte desse esforço, a montagem da Arpanet foi justificada como uma maneira de permitir aos vários centros de computadores e grupos de pesquisa que trabalhavam para a agência compartilhar on-line tempo de computação." In: CASTELLS, Manuel. **A galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade**. Trad. Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar, 2003, p. 16.

[2] Manuel Castells é Doutor em sociologia pela Universidade de Paris, é professor nas áreas de sociologia, comunicação e planejamento urbano. É conhecido por suas pesquisas sobre a sociedade da informação, sociedade em rede e o capitalismo informacional.

> vantagens extraordinárias como ferramentas de organização em virtude de sua flexibilidade e adaptabilidade inerentes, características essenciais para se sobreviver e prosperar num ambiente em rápida mutação. É por isso que as redes estão proliferando em todos os domínios da economia e da sociedade, desbancando corporações verticalmente organizadas e burocracias centralizadas e superando-as em desempenho.[3]

Além disso, de acordo com o sociólogo, a união de três processos independentes culminou no surgimento de uma nova estrutural social fundamentada em redes, dando origem assim à sociedade de rede. Em suas palavras:

> No final do século XX, três processos independentes se uniram, inaugurando uma nova estrutura social predominantemente baseada em redes: as exigências da economia por flexibilidade administrativa e por globalização do capital, da produção e do comércio; as demandas da sociedade, em que os valores da liberdade individual e da comunicação aberta tornaram-se supremos; e os avanços extraordinários na computação e nas telecomunicações possibilitados pela revolução microeletrônica. Sob essas condições, a Internet, uma tecnologia obscura sem muita aplicação além dos mundos isolados dos cientistas computacionais, dos hackers e das comunidades contraculturais, tornou-se a alavanca na transição para uma nova forma de sociedade — a sociedade de rede —, e com ela para uma nova economia.[4]

Em termos práticos, observa-se que o acesso à internet se tornou imprescindível para a vida em sociedade. Seja nas atividades cotidianas de uma única pessoa, facilitando atos comuns do dia a dia, como utilizar um aplicativo para pedir comida ou se conectar com amigos à distância, quer seja promovendo uma alteração nas relações econômicas, com empresas passando a utilizar a internet para comunicação, processamentos de informações, aquecendo um mercado global interdependente.

A partir disso, é possível visualizar o que Castells conceitua como sociedade de informação. Isto é, a ocorrência de uma revolução de cunho tecnológico, constituída pelas tecnologias digitais de informação e de comunicação, cuja operação é oriunda de uma estrutura

---

[3] CASTELLS, Manuel. **A galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade**. Trad. Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar, 2003, p. 1.
[4] CASTELLS, Manuel. **A galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade**. Trad. Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar, 2003, p. 8.

social em rede, que perpassa em todos os campos da atividade humana de forma interdependente e multidimensional. Além disso, também se compreende que o termo "informacional" intitula um modo de organização social cuja produtividade e exercício do poder são medidos pela tríade: produção, processamento e propagação da informação. [5]

Sob essa lógica, outro ponto importante trazido pelo autor espanhol é o surgimento de um novo modelo de economia, baseada no exercício do poder a partir do modelo de redes. Nesse sentido, surge assim o que o sociólogo denomina de "Capitalismo Informacional", sendo este o modelo vigente atualmente. A partir dos anos 70, com o desenvolvimento tecnológico, surge esse novo modelo econômico, cuja fonte de poder é a própria tecnologia. Assim, se pode afirmar que os quatro objetivos centrais desse processo de reestruturação capitalista foram: a maximização do lucro nas relações capital/trabalho (flexibilização, terceirização, enxugamento); aumento da produtividade do trabalho; globalização da produção, circulação e mercados; e direcionamento dos recursos estatais para garantir ganhos de produtividade e competitividade.

Em continuidade, Castells afirma que o modelo novo é informacional e global. Primeiramente, deve ser encarado como informacional porque "a produtividade e a competitividade dependem da capacidade dos agentes econômicos (empresas, regiões, nações) para gerar, processar e aplicar de forma eficiente a informação baseada em conhecimentos". E também é global, visto que "as principais atividades produtivas, o consumo e a circulação, assim como seus componentes (capital, trabalho, matéria-prima, administração, informação, tecnologia, mercados) estão organizados e escala global, diretamente ou mediante uma rede de conexões entre agentes econômicos" (1999, p. 4).

Destarte, o autor espanhol entende que após a difusão da internet nos anos 90, a ferramenta foi responsável por transmutar a forma como os negócios eram feitos na prática. Por conseguinte, a internet modificou a maneira como as empresas se relacionam com seus fornecedores, compradores, sua própria administração, a forma como cooperam com outras empresas e seu processo de produção. Desse modo, no contexto desse modelo econômico "a ligação entre consultores, subcontratadores e firmas na web tornam-se tão importantes quanto

[5] BRANDÃO, Lucas. **A Sociedade da informação aos olhos de Manuel Castells**. Comunidade Cultura e Arte. Online.

as operações da própria firma", originando assim "uma economia interconectada com um sistema nervoso eletrônico" (2003, p. 69-70).

Dentro deste cenário, surge um novo conceito de empresas denominado "empresas eletrônicas". Segundo Castells:

> Por empresas eletrônicas entendo qualquer atividade de negócio cujas operações-chave de administração, financiamento, inovação, produção, distribuição, vendas, relações com empregados e relações com clientes tenham lugar predominantemente pela/na Internet ou outras redes de computadores, seja qual for o tipo de conexão entre as dimensões virtuais e físicas da firma. Ao usar a Internet como um meio fundamental de comunicação e processamento de informação, a empresa adota a rede como sua forma organizacional. Essa transformação sociotécnica permeia o sistema econômico em sua totalidade, e afeta todos os processos de criação, de troca e de distribuição de valor. Assim, capital e trabalho, os componentes-chave de todos os processos de negócios, são modificados em suas características, bem como no modo como operam. Sem dúvida as leis da economia de mercado continuam a vigorar nessa economia interconectada, mas o fazem de uma maneira específica, cuja compreensão é crucial para se viver, sobreviver e prosperar nesse admirável mundo novo econômico.[6]

Portanto, torna-se evidente que o surgimento da internet revolucionou a sociedade, quer seja na vida cotidiana do indivíduo, utilizando a ferramenta para trabalhar, se comunicar, acessar aplicativos, pedir uma refeição ou comprar o ingresso para um evento, quer seja num contexto global, impactando diretamente na maneira como as relações econômicas transmutaram e perduram até os dias atuais, dando origem a uma nova economia.

Diante disso, a partir da contextualização apresentada no presente subcapítulo, abordaremos, a seguir, a questão da vigilância inserida na contemporaneidade, bem como a aparição da nova ordem do sistema capitalista – o capitalismo de vigilância –, e o surgimento de novas tecnologias de vigilância, especialmente o *big data*.

2.2 Vigilância e a nova lógica capitalista: o capitalismo de vigilância

[6] CASTELLS, Manuel. **A galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade**. Trad. Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar, 2003, p. 70.

Inicialmente, é necessário que façamos uma exposição sucinta sobre o que se entende por vigilância. Nesse sentido, a primeira parte deste subcapítulo tem como objetivo discorrer resumidamente sobre a definição de vigilância, a partir – principalmente – do pensamento foucaultiano.

Nos anos 70 o filósofo francês Michel Foucault discorreu e analisou a sociedade da vigilância na obra intitulada *Vigiar e Punir* (1977), desenvolvendo sua teoria sobre a problemática da vigilância e a aplicação do poder com o objetivo de exercer o controle sobre o corpo social. Nesse sentido, o teórico entende que o comportamento dos indivíduos e da sociedade é encarada como uma questão epistemológica e que deve ser analisada a partir da Idade Moderna, visto que é nesse contexto que o poder passa por transformações, tomando como ferramenta para seu exercício a vigilância hierárquica. Assim, Foucault afirma que para o exercício do poder disciplinar, são utilizados os seguintes instrumentos: a vigilância hierárquica, a sanção normalizadora e o exame.[7] Em suas palavras:

> O poder disciplinar é com efeito um poder que, em vez de se apropriar e de retirar, tem como função maior "adestrar"; ou sem dúvida adestrar para retirar e se apropriar ainda mais e melhor. Ele não amarra as forças para reduzi-las; procura ligá-las para multiplica-las e utilizá-las num todo. Em vez de dobrar uniformemente e por massa tudo o que lhe está submetido, separa, analisa, diferencia, leva seus processos de decomposição até às singularidades necessárias e suficientes.
>
> (...)
>
> A disciplina "fabrica" indivíduos; ela é a técnica específica de um poder eu toma os indivíduos ao mesmo tempo como objetos e como instrumentos de seu exercício. Não é um poder triunfante que, a partir de seu próprio excesso, pode-se fiar em seu superpoderio; é um poder modesto, desconfiado, que funciona no modo de uma economia calculada, mas permanente. Humildades modalidades, procedimentos menores se os compararmos com os rituais majestosos da soberania ou aos grandes aparelhos do Estado. E são eles justamente que vão pouco a pouco invadir essas formas maiores, modificar-lhes os mecanismos e impor-lhes os seus processos. O aparelho judiciário não escapará a esta invasão, malsecreta. O sucesso do poder disciplinar se deve sem dúvida ao uso de instrumentos simples: o olhar hierárquico, a

[7] BARRICHELLO**,** Eugenia Maria Mariano da Rocha; MOREIRA, Elizabeth Huber**. A análise da vigilância de Foucault e sua aplicação na sociedade contemporânea: estudo de aspectos da vigilância e sua relação com as novas tecnologias de comunicação.** Intexto, Porto Alegre, UFRGS, n. 33, p. 64-75, maio/ago. 2015, p. 2.

> sanção normalizadora e sua combinação destes num procedimento que lhe é específico, o exame.[8]

À vista disso, no capítulo segundo da obra em comento, o teórico disserta minuciosamente sobre ferramentas supracitadas – sendo a vigilância hierárquica aquela que será explorada neste subcapítulo e, mais a frente, será relacionada ao advento de novas tecnologias e a popularização da internet que, por conseguinte, operam como instrumentos modernos da vigilância. Será comprovado, portanto, que o poder se dá também através da vigilância e, esta, por sua vez, pode ser concebida pela tecnologia.

A aplicabilidade da vigilância como instrumento de instituição do poder disciplinar viabiliza a produção de conhecimento sobre os indivíduos vigiados. Isto posto, poder e saber são a combinação que propicia um controle categórico, "vigiar viabiliza a produção do saber e torna possível conhecer o objeto que está sob a vigilância, uma vez que o saber produzido reforça as possibilidades de exercer poder sobre tal objeto".[9] Dessa forma, Foucault assevera que para que se exerça a disciplina, faz-se necessário "um dispositivo que obrigue pelo jogo do olhar: um aparelho onde as técnicas que permitem ver induzam a efeitos de poder e, onde, em troca, os meios de coerção tornem claramente visíveis aqueles sobre quem se aplicam"[10].

Em continuidade, é possível extrair da obra de Foucault algumas características sobre a vigilância hierárquica. Ao todo, são cinco as qualidades que constituem a ferramenta em questão: sua invisibilidade; suas formas de se instituir; suas estruturas arquiteturais; sua discrição; e seu funcionamento como máquina.

A primeira qualidade da vigilância hierárquica é a sua invisibilidade, segundo Foucault os "olhares que devem ver sem ser vistos: uma arte obscura da luz e do visível preparou e surdina um saber novo sobre o homem, através de técnicas para sujeita-lo e processos para utilizá-lo"[11]. Nesse sentido, entende-se que a vigilância é exercida de modo que

---

[8] MICHEL, Foucault. **Vigiar e Punir: nascimento da prisão**; tradução de Raquel Ramalhete. 42. Ed. Petrópolis, RJ: Vozes, 2014, p. 167.
[9] BARRICHELLO**,** Eugenia Maria Mariano da Rocha; MOREIRA, Elizabeth Huber**. A análise da vigilância de Foucault e sua aplicação na sociedade contemporânea: estudo de aspectos da vigilância e sua relação com as novas tecnologias de comunicação.** Intexto, Porto Alegre, UFRGS, n. 33, p. 64-75, maio/ago. 2015, p. 65.
[10] MICHEL, Foucault. **Vigiar e Punir: nascimento da prisão**; tradução de Raquel Ramalhete. 42. Ed. Petrópolis, RJ: Vozes, 2014, p. 168.
[11] MICHEL, Foucault. **Vigiar e Punir: nascimento da prisão**; tradução de Raquel Ramalhete. 42. Ed. Petrópolis, RJ: Vozes, 2014, p. 168.

o ser responsável por a executar se torna invisível, de forma tal que a sua capacidade de vigiar é ampliada proporcionalmente à sua invisibilidade. Contudo, apesar de não ser possível visualizar a figura deste vigia, sua presença será sempre pressentida. De acordo com Elizabeth Huber Moreira e Eugenia Maria Mariano da Rocha Barrichello:

> O homem moderno está sempre se sentindo vigiado, vive em espaços projetados para este fim. Mas a real presença daquele que vigia nem sempre é notada, ela não se dá a perceber justamente para potencializar a vigilância. E, assim, é uma presença pressentida, sempre tomada como real, apesar de nem sempre poder ser verificada.[12]

A segunda característica diz respeito a maneira como a vigilância opera, de acordo com o filósofo "ao lado da grande tecnologia dos óculos, das lentes, dos feixes luminosos, unida à fundação da física e da cosmologia novas, houve as pequenas técnicas das vigilâncias múltiplas e entrecruzadas"[13] Isto quer dizer que a vigilância é instrumentalizada a partir de uma metodologia cujo objetivo é registrar dos comportamentos dos indivíduos, proporcionando a análise e uso dos elementos coletados. Barrichello e Moreira explicam:

> Para melhor conhecer é preciso bem vigiar, e a efetividade da vigilância depende do entrecruzamento de formas de vigilância e de informações. Assim, forma-se um saber sobre o outro. Nesse sentido, a vigilância deve ser hierarquizada, ou seja, ela depende da formação de uma hierarquia entre os indivíduos, que permite definir quem vigia quem, como e quando, de tal forma que poucos podem vigiar muitos.[14]

Nesse sentido, Foucault trata de um modelo piramidal que consiste em:

> "[...] formar uma rede sem lacuna – possibilidade em consequência de multiplicar seus degraus, e de espalhá-los sobre toda a superfície a controlar; e, entretanto ser bastante discreta para não pesar como uma massa inerte sobre a atividade a disciplinar".[15]

---

[12] BARRICHELLO**,** Eugenia Maria Mariano da Rocha; MOREIRA, Elizabeth Huber**. A análise da vigilância de Foucault e sua aplicação na sociedade contemporânea: estudo de aspectos da vigilância e sua relação com as novas tecnologias de comunicação.** Intexto, Porto Alegre, UFRGS, n. 33, p. 64-75, maio/ago. 2015, p. 4.
[13] MICHEL, Foucault. **Vigiar e Punir: nascimento da prisão**; tradução de Raquel Ramalhete. 42. Ed. Petrópolis, RJ: Vozes, 2014, p. 168.
[14] BARRICHELLO**,** Eugenia Maria Mariano da Rocha; MOREIRA, Elizabeth Huber**. A análise da vigilância de Foucault e sua aplicação na sociedade contemporânea: estudo de aspectos da vigilância e sua relação com as novas tecnologias de comunicação.** Intexto, Porto Alegre, UFRGS, n. 33, p. 64-75, maio/ago. 2015, p. 67.

[15] MICHEL, Foucault. **Vigiar e Punir: nascimento da prisão**; tradução de Raquel Ramalhete. 42. Ed. Petrópolis, RJ: Vozes, 2014, p. 171.

Quanto a essas particularidades, Foucault utiliza como exemplo do modelo ideal de observatório o acampamento militar. Segundo o professor, o acampamento é a esquematização do poder que atua por meio da visibilidade generalizada. Em suas palavras, o acampamento:

> É a cidade apressada e artificial, que se constrói e remodela quase à vontade; é o ápice de um poder que deve ter ainda mais intensidade, mas também mais discrição, por se exercer sobre homens de armas. No acampamento perfeito, todo o poder seria exercido somente pelo jogo de uma vigilância exata; e cada olhar seria uma peça no funcionamento global do poder.[16]

Outra particularidade da vigilância é a sua arquitetura, isto é, o "encaixamento espacial das vigilâncias hierarquizadas". Dessa forma, Foucault[17] sustenta que é possível observar a estruturação da vigilância no espaço físico, como por exemplo nas cidades operárias, hospitais, asilos e prisões. Espaços que contém em si o "princípio do encastramento". Assim, a arquitetura não é mais projetada para ser contemplada, ou para monitorar o ambiente exterior, mas sim para viabilizar o controle interno detalhadamente, de forma que esse domínio culminaria na influência direta sobre a maneira como o indivíduo se comporta naquele local.

Ainda sobre essa característica, Foucault entende que o modelo arquitetônico ideal para as prisões seria o panóptico:

> Foucault (1996) cita o panóptico, modelo arquitetural sugerido por Jeremy Bentham, no final do século XVIII, como o ideal para as prisões. Trata-se de uma torre central que permite ver todas as celas dispostas ao seu redor; porém, a presença de alguém na torre não é possível de ser percebida pelos indivíduos que estão nas celas. É impossível saber se há alguém na torre vigiando ou não. A vigilância torna-se, portanto, contínua, pela impossibilidade de ser detectada. O panoptismo, para Foucault (1996), pode ser traduzido na interiorização do olhar daquele que vigia a tal ponto que o indivíduo passa a se vigiar, não há mais necessidade de outra pessoa em tal tarefa. É o nível mais alto da vigilância, quando o indivíduo vigia a si mesmo e não se permite agir fora das regras que introjetou.[18]

---

[16] Idem, p. 168.
[17] Idem, p. 169.

[18] BARRICHELLO**,** Eugenia Maria Mariano da Rocha; MOREIRA, Elizabeth Huber**. A análise da vigilância de Foucault e sua aplicação na sociedade contemporânea: estudo de aspectos da vigilância e sua relação com as novas tecnologias de comunicação.** Intexto, Porto Alegre, UFRGS, n. 33, p. 64-75, maio/ago. 2015, p. 67.-68.

Sob esse ponto de vista, tentando trazer referências externas para a presente discussão, é interessante observar como a teoria foucaultiana respinga não só nos debates acadêmicos, como também nas obras ficcionais. Exemplo cristalino disso pode ser notado na animê[19] *Ataque de Titãs (Shingeki no Kyojin)*[20]. Isso porque na produção japonesa o ambiente em que a história se passa é uma cidade contornada por muralhas de 50 metros de altura, longas e resistentes, com objetivo de proporcionar uma vigilância completa do espaço, além de proteger a população da ameaça titã.

Nesse sentido, o espaço geográfico em questão é composto por três muralhas (Muralha Maria, Rose e Sina), sendo no centro delas a residência do soberano e nobres, protegida a polícia militar. Desse modo, conforme as figuras abaixo, é possível comparar o modelo da prisão panóptica com as muralhas da animação, não só arquitetonicamente, como também num nível principiológico, visto que as três muralhas são a materialização do controle espacial que o soberano exercia sob a população, controlando a narrativa sobre o mundo do lado de fora dos grandes muros.

Por fim, importante descrever um trecho da obra do filósofo francês que exprime exatamente o que se verifica na arquitetura de vigilância em *Ataque de Titãs*:

> (...) No centro dos edifícios dispostos em círculo e que se abriam todos para o interior, uma alta construção devia acumular as funções administrativas de direção, policiais de vigilância, econômicas de controle e de verificação, religiosas de encorajamento à obediência e ao trabalho; de lá viriam todas as ordens, lá seriam registradas todas as atividades, percebidas e julgadas todas as faltas; e isso imediatamente, sem quase nenhum suporte a não ser uma geometria exata. Entre todas as razões do prestígio que foi dado, na segunda metade do século XVIII, às arquiteturas circulares, é preciso sem dúvida contar com esta: elas exprimiam uma certa utopia política.[21]

---

[19] De acordo com o dicionário Michaelis, "animê" é: "Desenho animado criado no Japão, porém realizado em vários países do mundo, com técnicas, assuntos e personagens japoneses."

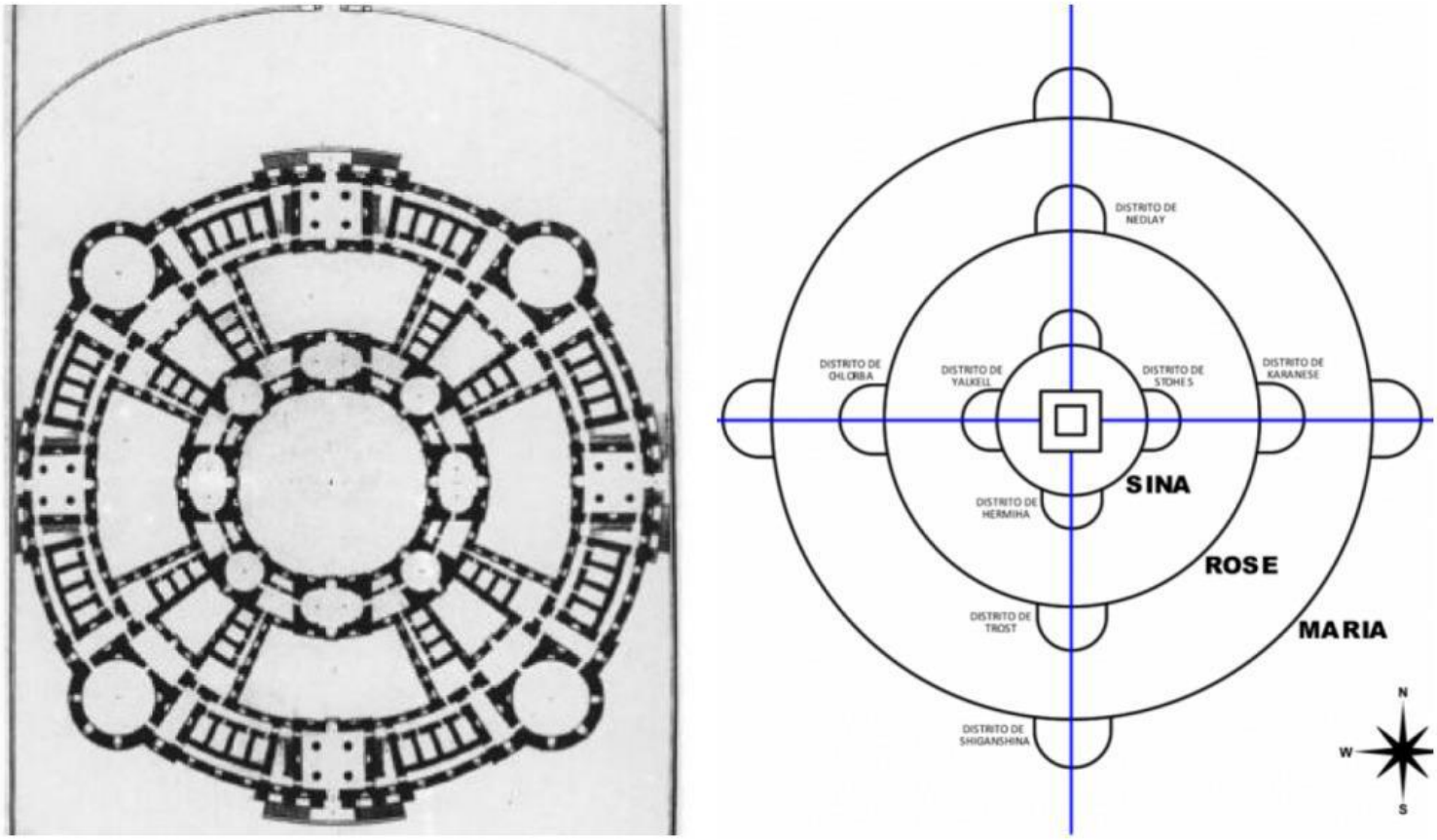
[20] Ataque de Titãs, também conhecido como *Attack on Titan* e *Shingeki no Kyojin*, é uma série de mangá (espécie de quadrinho japonês) escrita e ilustrada por Hajime Isayama e que foi adaptada para uma série de anime de televisão. Em síntese, "trata da história ambientado em um mundo onde a humanidade vive dentro de cidades cercadas por três enormes muralhas que os protegem dos gigantescos humanóides devoradores de humanos chamados de Titãs; a história segue Eren Yeager, que jura exterminar os Titãs após um Titã causar a destruição de sua cidade natal e a morte de sua mãe".

[21] MICHEL, Foucault. **Vigiar e Punir: nascimento da prisão**; tradução de Raquel Ramalhete. 42. Ed. Petrópolis, RJ: Vozes, 2014, p. 170-171.

Figura 1 - Primeiro as muralhas da animação e abaixo a prisão de Petite Roquete

Fonte: Imagem 1: representação gráfica da topografia de *Ataque dos* Titãs, extraída do wikipedia; Imagem 2: foto área da prisão Petite Roquete, extraída da obra Vigiar e Punir: nascimento da prisão de Michel Foucault.

Figura 2 - Projeto de prisão e esquema das muralhas da animação



Fonte: Fonte: Imagem 1: representação gráfica da topografia de *Ataque dos* Titãs, extraída do wikipedia; Imagem 2: foto do projeto de prisão, extraída da obra Vigiar e Punir: nascimento da prisão de Michel Foucault.

Perpassada essa sucinta observação, daremos continuidade ao exercício de qualificação da hierarquia de vigilância. A característica seguinte diz respeito à capacidade da vigilância ser exercida de forma velada, discreta. Isso porque a instrumentalização e aperfeiçoamento da vigilância se dá de forma silenciosa, não há mais a figura de um único indivíduo poderoso, como era o soberano no absolutismo. Agora aqueles que exercem a vigilância ficam encobertos e o feixe de luz paira sobre o vigiado, com objetivo de extrair dele um saber sobre ele próprio.

Por fim, a última característica concerne ao funcionamento da vigilância hierárquica como uma máquina, na qual as engrenagens se unem calculadamente e com a intenção de exercer o poder através desse aparelhamento. Desse modo, para Foucault o aparelho

disciplinar perfeito possibilitaria um vislumbre singular de tudo, assim "um ponto central seria ao mesmo tempo fonte de luz que iluminasse as coisas, e lugar de convergência para tudo o que deve ser sabido: olho perfeito a que nada escapa e centro em direção ao qual todos os olhares convergem".[22]

Para encerrar essa primeira parte de exposição acerca das características da vigilância hierárquica, insta ressaltar, enfim, que esse instrumento de poder não deve ser entendido como uma invenção excepcional do século VXIII, mas seu prolongamento se dá pelas novas mecânicas de poder que traz em si.[23] Assim, continua o filósofo afirmando que o poder disciplinar se torna um sistema integrado justamente por conta do exercício dessa vigilância. Foucault explica:

> O poder disciplinar, graças a ela [vigilância], torna-se um sistema "integrado", ligado do interior à economia e aos fins do dispositivo onde é exercido. Organiza-se assim como um poder múltiplo, automático e autônimo; pois se é verdade que a vigilância repousa sobre indivíduos, seu funcionamento é de uma rede de relações de alto a baixo, mas também até um certo ponto de baixo para cima e lateralmente; essa rede "sustenta" o conjunto, e o perpassa de efeitos de poder que se apoiam uns sobre os outros: fiscais perpetuamente fiscalizados. O poder na vigilância hierarquizada das disciplinas não se detém como uma coisa, não se transfere como uma propriedade; funciona como uma máquina. E se é verdade que sua organização piramidal lhe dá um "chefe", é o aparelho inteiro que produz "poder" e distribui os indivíduos nesse campo permanente e contínuo. O que permite ao poder disciplinar ser absolutamente indiscreto, pois está em toda parte e sempre alerta, pois em princípio não deixa nenhuma parte às escuras e controla continuamente os mesmos que estão encarregados de controlar; e absolutamente "discreto", pois funciona permanentemente e em grande parte em silêncio. A disciplina faz "funcionar" um poder relacional que se autossustenta por seus próprios mecanismos e substitui o brilho das manifestações pelo jogo ininterrupto dos olhares calculados.[24]

À vista do exposto, depreende-se que o modelo de vigilância apresentado por Foucault proporciona a estrutura pelo qual as instituições e as cidades são constituídas, de acordo com os métodos disciplinares e de controle utilizados. Assim, se pensarmos na

---

[22] MICHEL, Foucault. **Vigiar e Punir: nascimento da prisão**; tradução de Raquel Ramalhete. 42. Ed. Petrópolis, RJ: Vozes, 2014, p. 170.
[23] Idem, p. 173.
[24]MICHEL, Foucault. **Vigiar e Punir: nascimento da prisão**; tradução de Raquel Ramalhete. 42. Ed. Petrópolis, RJ: Vozes, 2014, p. 173.

vigilância nos dias atuais, é possível fazer uma correlação entre o apontado pelo filósofo e a sociedade contemporânea no que diz respeito a criação de novas tecnologias de vigilância. Desse modo, para o exercício do poder, conforme apontado por Foucault, é preciso ter um instrumento de "vigilância permanente, exaustiva, onipresente, capaz de tornar tudo visível, mas com a condição de se tornar ela mesma invisível"[25]. São como "milhares de olhos postados em toda parte, atenções móveis e sempre alerta, uma longa rede hierarquizada"[26], e segundo Da Costa "assim como as milhares de câmeras espalhadas pelas cidades ou uso de massivas bases de dados que analisam os comportamentos humanos. Ambos são utilizados com a finalidade de manutenção da ordem e da segurança pública."[27]

Apesar de diferir da ideia de vigilância de Foucault, é interessante abordamos rapidamente a definição de vigilância sob a ótica de Fernanda Bruno[28] e Gilles Deleuze[29]. Primeiramente, segundo Bruno (2009, p.2), a vigilância é compreendida como sendo do tipo distribuída, para ela a vigilância é a "a atividade de observação sistemática e focalizada de indivíduos, populações ou informações relativas a eles, tendo em vista extrair conhecimento e intervir sobre os mesmos, de modo a governar suas condutas ou subjetividades". Desse modo, a vigilância é dita como distribuída, uma vez que se incorpora a diversos ambientes e dispositivos, incluindo aqueles que, a priori, não possuem a vigilância finalidade primária. Explica Bruno:

> Proponho o termo vigilância distribuída como definição do estado geral da vigilância nas sociedades contemporâneas. Em linhas breves, trata-se de uma vigilância que tende a se tornar incorporada a diversos dispositivos, serviços e ambientes que usamos cotidianamente, mas que se exerce de modo descentralizado, não hierárquico e com uma diversidade de propósitos, funções e significações nos mais diferentes setores: nas medidas de segurança e circulação de pessoas, informações e bens; nas estratégias de consumo e marketing; nas formas de comunicação, entretenimento e sociabilidade; na prestação de serviços etc. Nota-se que em certos casos ela se exerce misturada a

[25] Idem, p. 207.
[26] Idem, p. 207.
[27] DA COSTA, Camila Mattos**. "We are watching you": policiamento preditivo, controle, disciplina e vigilância.** Anais do 8º Encontro Internacional de Política Social, 15º Encontro Nacional de Política Social. v. 1 n. 1 (2020): "Questão social, violência e segurança pública: desafios e perspectivas. Vitória, ES. 2020, p. 4.
[28] Fernanda Bruno é doutora em Comunicação pela Universidade Federal do Rio de Janeiro em 2001. É pós-doutora pelo *Institut d"études politiques de Paris (Sciences Po)*. Suas áreas de interesses e pesquisa são: tecnologia, subjetividade, corpo, tecnologias de comunicação, cibercultura, cognição, vigilância e visibilidade. Coordena o CiberIdea: Núcleo de Pesquisa em tecnologias da comunicação, cultura e subjetividade, da ECO/UFRJ.
[29] Gilles Deleuze foi um professor e filósofo francês.

> dispositivos que não são prioritariamente voltados para a vigilância, sendo assim uma função potencial ou um efeito secundário de dispositivos que são projetados inicialmente para outras finalidades – comunicação, publicidade, geolocalização etc.[30]

Nesse sentido, Bruno entende que não há como confundir a vigilância distribuída com a vigilância panóptica "que supõe sistemas centralizados, hierarquizados, dirigidos a grupos ou indivíduos previamente delimitados cujas identidades supostamente portam uma periculosidade que demanda vigilância e se inscreve num projeto de normalização"[31]. Isso porque a vigilância distribuída caracteriza-se por não fazer uma distinção dentre os grupos vigiados, não há mais a necessidade do indivíduo ser um suspeito ou criminoso, "mas podem ser todos e qualquer um – consumidores, transeuntes, internautas, criminosos, participantes de reality shows etc". O que passa a ser monitorado, nesse contexto, são "os comportamentos, hábitos e rastros no ciberespaço"[32].

Já no entendimento de Gilles Deleuze, a sociedade passou por uma transformação transpassando de uma sociedade de disciplina para uma sociedade de controle, de acordo com o filósofo[33]. "Controle" é o nome que Burroughs propõe para designar o novo monstro, e que Foucault reconhece como nosso futuro próximo. Paul Virilio também analisa sem parar as formas ultrarápidas de controle ao ar livre, que substituem as antigas disciplinas que operavam na duração de um sistema fechado". O pensador entende que as sociedades operam por meio de máquinas próprias daquele determinado tempo, assim:

> É fácil fazer corresponder a cada sociedade certos tipos de máquina, não porque as máquinas sejam determinantes, mas porque elas exprimem as formas sociais capazes de lhes darem nascimento e utilizá-las. As antigas sociedades de soberania manejavam máquinas simples, alavancas, roldanas, relógios; mas as sociedades disciplinares recentes tinham por equipamento máquinas energéticas, com o perigo passivo da entropia e o perigo ativo da sabotagem; as sociedades de controle operam por máquinas de uma terceira espécie, máquinas de informática e computadores, cujo perigo passivo é a interferência, e, o ativo, a pirataria e a introdução de vírus.[34]

---

[30] BRUNO, Fernanda. **Mapas de crime: vigilância distribuída e participação na cibercultura**. E-Compós (Brasília), v. 12, p. 1-16, 2009, p. 2.
[31] Idem, p. 3.
[32] Idem, p. 3.
[33] DELEUZE, Gilles. **Post-Scriptum sobre as Sociedades do Controle**. Rio de Janeiro: Ed. 34, 1992, p. 220.
[34] DELEUZE, Gilles. Post-**Scriptum sobre as Sociedades do Controle**. Rio de Janeiro: Ed. 34, 1992, p. 223..

Destarte, Deleuze esclarece que essa mudança trata da transformação do próprio sistema capitalista. Conforme o autor leciona, o capitalismo do século XIX era de concentração, visado para a produção e a propriedade, entretanto, o capitalismo vigente é de "sobre-produção", orientado especificamente para o produto em si e sua venda, e "por isso ele é essencialmente dispersivo, e a fábrica cedeu lugar à empresa.[35]

Nesse rumo, antes de adentrarmos na análise acerca das tecnologias de vigilância – e posteriormente, o tema central deste estudo, qual seja o policiamento preditivo –, é imperioso discorrer brevemente sobre o sistema vigente no qual elas estão inseridas: o capitalismo de vigilância. De acordo com Foucault "a vigilância se torna um operador econômico decisivo, na medida em que é ao mesmo tempo uma peça interna no aparelho de produção e uma engrenagem específica do poder disciplinar"[36]. À vista disso, os próximos parágrafos serão dedicados a abordar sinteticamente o sistema capitalista de vigilância, a partir do pensamento de Shoshana Zuboff.[37]

Zuboff explica que o esse modelo econômico emergiu a partir da crise no capitalismo ocidental, promovendo uma alteração na relação entre os indivíduos e as empresas. Isso porque, na conjuntura anterior, os empregados produziam e consumiam os itens que eles próprios produziam. Contudo, atualmente, o contexto alterou-se no sentido de que não há mais essa reciprocidade, visto que há um novo personagem intermediando essa relação: os capitalistas de vigilância, que "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".[38]

Em continuidade, a autora conceitua o capitalismo de vigilância como sendo aquele que demanda para si a "experiência humana", a fim de utilizá-la como matéria prima gratuita e com o objetivo de traduzir essa informação em dados comportamentais. Em suas palavras:

---

[35] Idem, p. 224.
[36] MICHEL, Foucault. **Vigiar e Punir: nascimento da prisão**; tradução de Raquel Ramalhete. 42. Ed. Petrópolis, RJ: Vozes, 2014, p. 172.
[37] Shoshana Zuboff é professora emérita na *Harvard Business School*, possui PH.D. em psicologia social na Universidade de Harvard.
[38] ZUBOFF apud LEMES em LEMES, Marcelle Martins. **Inteligência artificial, algoritmos e policiamento preditivo no poder público federal brasileiro**. Monografia. Faculdade de Direito, Universidade de Brasília. Brasília, 2019, p. 44.

> Embora alguns desses dados sejam aplicados para o aprimoramento de produtos e serviços, o restante é declarado como superávit comportamental do proprietário, alimentando avançados processos de fabricação conhecidos como "inteligência de máquina" e manufaturado em produtos de predição que antecipam o que um determinado indivíduo faria agora, daqui a pouco e mais tarde. Por m, esses produtos de predições são comercializados num novo tipo de mercado para predições comportamentais que chamo de mercados de comportamentos futuros. Os capitalistas de vigilância têm acumulado uma riqueza enorme a partir dessas operações comerciais, uma vez que muitas companhias estão ávidas para apostar no nosso comportamento futuro.[39]

Desse modo, tendo em vista a concorrência exacerbada entre os capitalistas de vigilância, novas fontes visando o aquecimento do mercado foram procuradas. Dessa forma, a essência dos indivíduos, suas personalidades, vozes e emoções passaram a ser uma valiosa matéria prima. Explica a professora que:

> Os capitalistas de vigilância descobriram que os dados comportamentais mais preditivos provêm da intervenção no jogo de modo a incentivar, persuadir, sintonizar e arrebanhar comportamento em busca de resultados lucrativos. Pressões de natureza competitiva provocaram a mudança, na qual processos de máquina automatizados não só conhecem nosso comportamento, como também moldam nosso comportamento em escala. Com tal reorientação transformando conhecimento em poder, não basta mais automatizar o fluxo de informação sobre nós; a meta agora é *nos automatizar*. Nessa fase da evolução do capitalismo de vigilância, os meios de produção estão subordinados a "meios de modicação comportamental" cada vez mais complexos e abrangentes. Dessa maneira, o capitalismo de vigilância gera uma nova espécie de poder que chamo de *instrumentarismo*[40]

À vista disso, de acordo com Zuboff[41] entende-se por *instrumentarismo* como sendo um poder que modula o comportamento humano em benefício dos interesses de terceiros (capitalistas de vigilância). Assim, ao invés de se utilizarem de exércitos e do poder bélico, a sua vontade é exercida pela via automatizada, uma estrutura computacional onisciente, com seus espaços inteligentes conectados numa rede. Isto é:

---

[39] ZUBOFF, Soshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**; tradução de George Schlesinger - 1. Ed. – Rio de Janeiro, RJ: Intrínseca, 2020, p. 19.
[40] Ibid., p. 19.
[41] Idem, p. 19.

> A conexão digital é agora um meio para fins comerciais de terceiros. Em sua essência, o capitalismo de vigilância é parasítico e autorreferente. Ele revive a velha imagem que Karl Marx desenhou do capitalismo como um vampiro que se alimenta do trabalho, mas agora com uma reviravolta. Em vez do trabalho, o capitalismo de vigilância se alimenta de todo aspecto de toda a experiência humana[42]

Sob essa lógica, elucida a autora que o capitalismo de vigilância não está mais vinculado a grandes empresas do ramo da internet, em que o produto-comportamento somente era encarado como um produto pelo mercado de publicidade online, agora esse modelo é tido como basilar para qualquer segmento de negócios que tenha a internet como base. Nesse sentido, os produtos de predição são negociados para serem utilizados não mais somente no setor publicitário, mas também no de seguros, lojas de varejo, finanças, bens e serviços e tantos outros. E a partir dessa dinâmica nova, Zuboff explica pagamos para sermos dominados.". Nas exatas palavras da professora:

> (...) Nós somos as fontes do superávit crucial do capitalismo de vigilância: os objetos de uma operação de extração de matéria-prima tecnologicamente avançada e da qual é cada vez mais impossível escapar. Os verdadeiros clientes do capitalismo de vigilância são as empresas que negociam nos mercados de comportamento futuro. Essa lógica transforma a vida comum na renovação diária de um pacto faustiano do século XXI. "Faustiano" porque é quase impossível livrar-se dele, apesar do fato de que aquilo que precisamos dar em troca destruirá a vida tal qual a conhecemos. Considere que a internet se tornou essencial para a participação na sociedade, que a internet se encontra agora saturada de comércio e que este está agora subordinado ao capitalismo de vigilância. Nossa dependência está no cerne do projeto de vigilância comercial, no qual as necessidades que sentimos por uma vida eficaz lutam contra a inclinação de resistir às audazes incursões do sistema.[43]

Ademais, outra questão relevante trazida pela autora diz respeito às operações que ela denomina como "renderização" *(rendition)*, isto é, o processo de transmutação das experiências pessoais em dados. Desse modo, a renderização "descreve as práticas operacionais concretas por meio das quais a despossessão é realizada, com a experiência humana sendo reivindicada como matéria-prima para a dataficação e tudo que se segue, de fabricação a

---

[42] Ibid., p. 20.

[43] ZUBOFF, Soshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**; tradução de George Schlesinger - 1. Ed. – Rio de Janeiro, RJ: Intrínseca, 2020, p. 22.

vendas”[44]. A professora ainda explica que o capitalismo de vigilância funciona como uma equação: de um lado, se têm as tecnologias que são programadas para transformar a experiência humana em dados – operação que, geralmente, ocorre sem o consentimento do usuário, e por outro lado, sempre que o indivíduo utiliza uma “interface digital” ele torna sua experiência datificável, servindo de matéria prima para o o sistema capitalista de vigilância. Assim, afirma Zuboff que “não pode haver capitalismo de vigilância sem renderização”.[45]

Sob essa ótica, é possível observar um movimento de reformulação dos produtos pelo mercado, tendo em vista que agora o objetivo é incorporar a renderização nos novos artefatos. Assim, surge então a nova lógica de produtos “inteligentes”, desenhados para proporcionar a renderização, com objetivo de assegurar o processo de “dataficação”, e por isso, “inteligente é um eufemismo para renderização” conforme elucida Zuboff.[46] Em suas palavras:

> O objeto inteligente é um tipo de marionete; apesar de toda sua “inteligência”, continua sendo uma infeliz marionete dançando conforme os imperativos econômicos ocultos do titereiro. Produtos, serviços e aplicativos marcham ao som do inevitabilismo rumo à promessa de receitas da vigilância extraídas dos espaços ainda inexplorados que chamamos de “minha realidade”, “minha casa”, “minha vida” e “meu corpo”. Todo produto inteligente repete as nossas perguntas essenciais: o que um produto inteligente sabe, e para quem ele conta*? Quem sabe? Quem decide? Quem decide quem decide?*[47]

Nota-se, portanto, como o capitalismo de vigilância alterou as dinâmicas de mercado, acarretando na modificação da estrutura dos produtos desenvolvidos, constituindo a nova geração de produtos inteligentes e preditivos, cujo intuito se traduz no desejo de introduzir-se na vivência do ser humano de forma imperceptível e invasiva, a fim de transformar a sua experiência pessoal em matéria-prima.

Assim, considerando o que foi elucidado, a seguir iremos discorrermos sobre as tecnologias de vigilância, principalmente o *big data* e, por fim, introduziremos o debate acerca da dessas tecnologias de vigilância no contexto da segurança.

---

[44] Idem, p. 269.
[45] Idem, p. 270
[46] Idem, p. 274
[47] Ibid., p. 276.

2.3 Tecnologias de vigilância: o fenômeno do *Big Data* como propulsor da vigilância

Com a disseminação do acesso à internet, juntamente dos avanços científicos na área da tecnologia e da engenharia computacional, concatenado ao surgimento da nova etapa do sistema capitalista – e seu objetivo primal de mercantilizar o comportamento humano – novas tecnologias de vigilância foram surgindo ao longo do tempo.

O intuito dessas tecnologias é o de possibilitar a coleta, monitoramento e análise dos indivíduos na sociedade, promovendo o controle já apresentado anteriormente.

Preliminarmente, é interessante tratarmos do conceito de tecnologia de vigilância digital desenvolvido por Fernanda Bruno. Para a autora, um dispositivo de vigilância digital possui características elementares, sendo estas o "monitoramento de ações, informações e comunicações dos indivíduos no ciberespaço, a montagem de bancos de dados e a elaboração de perfis computacionais"[48]. Além disso, ela também enfatiza que para uma melhor compreensão destes dispositivos, é preciso levar em conta seus processos de constituição. Bruno explica que são quatro processos: (i) mecanismos de coleta, monitoramento e arquivo de informação; (ii) sistemas de classificação e conhecimento de dados; (iii) os procedimentos de individualização e produção de identidades; e (iv) as formas de controle sobre as ações e escolhas dos indivíduos.[49]

Em continuidade, a autora ainda explica que com o passar dos anos a capacidade de se monitorar e coletar dados dos indivíduos cresceu em inúmeros setores, como por exemplo o da segurança, saúde, trabalho, vida social etc. Dessa forma, a partir disso novas tecnologias foram surgindo já com a habilidade de coletar dados embutido em seu maquinário, a exemplo os "cartões de crédito, sistemas de geolocalização por satélite, navegações e buscas on-line".[50]

Outrossim, de acordo com Bruno, insta destacar duas características relevantes sobre o surgimento desses maquinários de vigilância. A primeira diz respeito a quem ou quais

---

[48] BRUNO, Fernanda. **Monitoramento, classificação e controle nos dispositivos de vigilância digital**. Revista FAMECOS, v. 15, n. 36, p. 10-16, 20 nov. 2008, p. 11.
[49] BRUNO, Fernanda. **Monitoramento, classificação e controle nos dispositivos de vigilância digital**. Revista FAMECOS, v. 15, n. 36, p. 10-16, 20 nov. 2008
[50] BRUNO, Fernanda. **Monitoramento, classificação e controle nos dispositivos de vigilância digital**. Revista FAMECOS, v. 15, n. 36, p. 10-16, 20 nov. 2008, p. 11.

agentes são "capacitadas e/ou autorizadas" a coletar dados individuais, a resposta se consolida no sentido de que tanto o setor privado quanto o público poderiam realizar essa atividade, desde que "respeitando regras mínimas de proteção a "privacidade"[5152]. Já a segunda característica versa sobre o tipo de dado coletado, podendo ser dividido em dois tipos: o primeiro tipo denominado de "relativamente estáveis", visto que apresentam "pouca ou nenhuma variação ao longo do tempo", como por exemplo "dados biométricos, geodemográficos, relativos a gênero", e o segundo denominado de "móveis ou circunstanciais", nos quais se inserem os dados comportamentais, transacionais, sociais etc.[53]

Sobre esses dados móveis, Bruno esclarece que é nesse tipo que se localizam os dados próprios da vigilância digital. Isso se dá porque a coleta desses dados só foi possível por conta da agregação das tecnologias informacionais no dia a dia do indivíduo. Em suas palavras:

> Estas [tecnologias informacionais] permitiram uma coleta à distância e automatizada, capaz de capturar os dados em tempo real ou in the wild, sem as tradicionais mediações de entrevistadores e questionários. Além dessa facilitação, há um deslocamento do foco de interesse, que se volta menos para os atributos estáveis do que para os móveis e circunstanciais, cada vez mais particularizados.[54]

Em seu artigo a autora trata também da questão da classificação e conhecimento acerca dos dados coletados, visto que um grupamento de dados só ganha uma significação a partir da sua análise e classificação com o fim de proporcionar um entendimento sobre indivíduos ou acerca da realidade ao qual estão inseridos. Desse modo, Bruno explica que os bancos de dados "ordenam os dados provenientes de indivíduos em categorias infraindividuais, podendo estas serem ou não atreladas a identificadores pessoais (como nome, endereço, número de CPF)". À vista disso, essas categorias infra individuais podem ser geradas a partir de um molde *"top-dow"*, isto é, "utilizando classes pré-estabelecidas – idade, gênero, profissão" ou a

---

[51] Idem, p. 12

[52] Sobre a temática referente à proteção de dados dos indivíduos, insta destacar que já existem algumas regulações legislativas sobre o tema ao redor do mundo e no Brasil. Por exemplo: na Europa, tem-se a *Gerenal Data Protection Regulation* (GDPR), aprovado em 2016 e cujo objetivo é garantir a proteção de dados dos cidadãos europeus da União Europeia e Espaço Econômico Europeu. Recentemente, no Brasil também foi sancionada a Lei Geral de Proteção de Dados (LGPD), sancionada em 2020, e tem como finalidade proteger os direitos fundamentais de liberdade e de privacidade dos indivíduos, bem como regular as atividades de tratamento desses dados. Além disso, em 10 de fevereiro de 2022 foi promulgada a Emenda Constitucional 115/2022 que elenca a proteção de dados como uma garantia fundamental.

[53] Idem, p. 12.

[54] BRUNO, Fernanda. **Monitoramento, classificação e controle nos dispositivos de vigilância digital**. Revista FAMECOS, v. 15, n. 36, p. 10-16, 20 nov. 2008, p. 12.

partir do modelo *"bottom-up"*, ou seja, "gerando classes a partir da análise dos dados" como por exemplo "frequentadores do site Y que clicam nos links de tipo X". Com essa categorização pronta, submete-se o resultado a um tratamento secundário, cujo procedimento é realizado a partir da técnica de mineração de dados *(data mining)* e a produção de perfis computacionais *(profiling)*[55]. Sobre isso, a autora utiliza os argumentos de Bennet e explica:

> Tais padrões são constituídos a partir de mecanismos de geração de regras, sendo mais comuns as de tipo associativo (similaridade, vizinhança, afinidade) entre pelo menos dois elementos, que depois diferenciam tipos de indivíduos ou grupos. Esses tipos correspondem a perfis computacionais gerados pelo mecanismo designado *profiling*. A geração de perfis segue uma lógica indutiva que visa "determinar indicadores de características e/ou padrões de comportamento que são relacionados à ocorrência de certos comportamentos" (BENNET apud BRUNO)

> Os padrões e regularidades daí extraídos permitem visualizar domínios com certa homogeneidade interna e
> fronteiras externas – de interesses, comportamentos, traços psicológicos – que de outro modo ficariam indefinidos ou fora do nosso campo de atenção. Assumem assim um formato mais dócil, calculável, legitimando e orientando intervenções diversas. Perfis de criminosos, consumidores, profissionais, doentes físicos ou mentais, tipos psicológicos ou comportamentais apresentam-se como padrões que ao mesmo tempo ordenam e objetivam a multiplicidade humana, legitimando formas de governá-la.[56]

A autora defende ainda que esses perfis são "micro-regularidades" dos grupos analisados e que tais regularidades são "tendências" e não uma lei, assim:

> A taxonomia e o conhecimento não revelam aí um conjunto de características intrínsecas aos indivíduos, mas padrões de conduta e escolha na presença de fatores que constituem uma circunstância. Deste modo, a inadequação ao perfil não representa um desvio, mas uma contingência, uma particularidade a ser, não corrigida, mas incorporada ao próprio cálculo de determinação do perfil.[57]

Como exemplo do exposto, Bruno cita a utilização do método de *profiling* para explicar comportamentos criminosos, em suas palavras:

---

[55] Idem, p. 13.
[56] BRUNO, Fernanda. **Monitoramento, classificação e controle nos dispositivos de vigilância digital**. Revista FAMECOS, v. 15, n. 36, p. 10-16, 20 nov. 2008, p.13.
[57] Idem, p. 13.

> Teorias que utilizam o profiling para explicar a ocorrência de comportamentos criminosos, por exemplo, concebem o crime não mais como o resultado de uma patologia individual ou uma disfunção social, mas como um evento em que se articulam padrões motivacionais e "situações criminogênicas" (Garland, 2002). As teorias do criminoso ou da criminalidade cedem lugar à produção de perfis de ocorrência do evento criminal, o qual deve ser evitado por um controle das circunstâncias e oportunidades.[58]

Dessa forma, perpassado este esclarecimento acerca do conceito de tecnologia de vigilância digital, passaremos ao estudo do *Big Data*. Apesar de ter inúmeras definições, traremos no trabalho as definições técnicas, mas principalmente aquela formada e debatida por Cathy O'Neil[59] em seu famoso livro "Algoritmos de Destruição em Massa: Como o Big Data aumenta a desigualdade e ameaça a democracia". Assim, de acordo com a IBM *(International Business Machines Corporation)*, o *Big Data* pode ser definido como:

> Conjunto de dados cujo tamanho ou tipo está além da habilidade de captura, gerenciamento e processamento dos dados dos tradicionais bancos de dados. As características do big data incluem alto volume, alta velocidade e alta variedade de dados. As fontes de dados estão se torando mais complexas do que as de dados tradicionais, visto que estão sendo impulsionadas por inteligência artificial (IA), dispositivos móveis, mídias sociais e Internet das Coisas (IoT). Por exemplo, os diferentes tipos de dados se originam de sensores, dispositivos, vídeo/áudio, redes, arquivos de log, aplicativos transacionais, web e mídia social – muitos deles sendo gerados em tempo real e em grande escala. (tradução minha)[60]

Outra definição, em mesmo sentido, de acordo com Pimenta:

> Ele [*big data*] representa grosso modo o grande volume de dados, base para a produção de informações não estruturadas e estruturadas, produzidos de maneira

[58] Idem, p. 13
[59] Cathy O'Neil é Ph.D em matemática pela Universidade de Harvard e pós-doutora pelo MIT (Massachusetts Institute of Technoloy).
[60] No original: "It can be defined as data sets whose size or type is beyond the ability of traditional relational databases to capture, manage and process the data with low latency. Characteristics of big data include high volume, high velocity and high variety. Sources of data are becoming more complex than those for traditional data because they are being driven by artificial intelligence (AI), mobile devices, social media and the Internet of Things (IoT). For example, the different types of data originate from sensors, devices, video/audio, networks, log files, transactional applications, web and social media — much of it generated in real time and at a very large scale."

> exponencial na contemporaneidade. Mais do que seu volume, sua articulação em rede, sua velocidade e diversidade possibilitaram a produção de mais dados, a partir dos dados já existentes, sobre indivíduos, grupos ou sobre a própria informação, quaisquer que seja ela, disponível. (BOYD; CRAWFORD, 2011).[61]

Ademais, ainda na tentativa de definir o que é *Big Data*, segundo Chan e Bennett[62]:

> É possível definir o Big Data a partir do tamanho e tipo de conjunto de dados que estão sendo utilizados, a capacidade de armazenamento desse conjunto e o processamento e/ou análise sistémica analítica (...) A razão para a diversidade de definições se dá pela variedade de tecnologias utilizadas, plataformas e sistemas envolvidos e pelos objetivos a serem alcançados. Essa rotulação única diz mais sobre captura uma tendência ampliada na maneira em como os dados são capturados, armazenados e utilizados e não tenta rotular, especificamente, um produto ou processo. (tradução minha)[63]

Igualmente, ainda de acordo com as autoras Chan e Bennet, uma definição popular de *Big Data* envolve um conceito determinado pelos três "Vs", ou seja, "Volume (a grande quantidade de dados), Velocidade (a velocidade com a qual um dado é adicionado ao conjunto e processado) e a Variedade (os dados podem ser extraídos de diferentes fontes, a partir de diversos formatos e estruturas)".[64]

Já consoante a concepção de Cathy O'Neil, o *Big Data* estrutura um modelo que ela denomina como "armas de destruição em massa (ADMs)". A autora explica que com o avanço da matemática, novas técnicas foram se expandindo "*petabytes* de dados eram processados 24 horas por dia, 7 dias por semana, muitos deles raspados de redes sociais ou sites

---

[61] PIMENTA, R. M. **Big data e controle da informação na era digital: tecnogênese de uma memória a serviço do mercado e do estado**. 2013, p. 2.
[62] CHAN, Janet; BENNETT MOSES, Lyria**, Is Big Data Challenging Criminology?.** UNSW Law Research Paper No. 20-81, 2015, p. 4.
[63] Tradução minha. No original: "It is possible to define Big Data by reference to the size and type of data sets being employed, the capabilities of a data storage, processing and/or analytic system (...) The reason for the diversity of definitions is the variety of technologies employed, platforms and systems potentially involved and purposes to be achieved. The single label captures a broad trend in how data is captured, stored and used rather than to identifying a particular product or process."
[64] No original: "A popular definition of Big Data is that it involves (at least) three V's—Volume (the amount of data), Velocity (the speed at which data is being added and processed) and Variety (the fact that data may come from multiple sources using different formats and structures)."

de e-commerce. E cada vez mais o foco não era nos movimentos financeiros globais, mas nos seres humanos", formando a partir disso uma economia do *Big Data.*[65]

A autora explica que esses modelos eram apresentados e vendidos como imparciais e objetivos, sem a influência do senso humano. Contudo, ela chama atenção para o fato de que tais modelos matemáticos eram formulados a partir de escolhas feitas por seres humanos e, ainda que não tivessem a intenção, tais modelos exprimiam o que quer que seus criadores desejam. Assim, ela define ADMs a partir da seguinte narrativa:

> (...) muitos desses modelos programavam preconceitos, equívocos e vieses humanos nos sistemas de software que cada vez mais geriam nossas vidas. Como deuses, esses modelos matemáticos eram opacos, seus mecanismos invisíveis a todos exceto os altos sacerdotes de seus domínios: os matemáticos e cientistas da computação. Suas decisões, mesmo quando erradas ou danosas, estavam para de qualquer contestação. E elas tendiam a punir os pobres e oprimidos da sociedade enquanto enriquecia ainda mais os ricos.[66]

Em continuidade, a matemática explica simplificadamente o que seria um modelo. Assim, um modelo pode ser definido como uma representação abstrata de qualquer processo, como por exemplo um jogo de beisebol, ações de um governo estrangeiro, o público de um cinema etc, e tal modelo reúne as informações sobre o objeto de pesquisa e as usa para prever respostas em diferentes situações. Entretanto, é importante pontuar que um modelo sempre é passível de erros, visto que se tratam de simplificações e nenhum modelo é capaz "de incluir toda a complexidade do mundo real ou as nuances da comunicação humana"[67]. O' Neil explica que:

> Para criar um modelo, então, fazemos escolhas sobre o que é importante o bastante para ser incluído, simplificando o mundo numa versão de brinquedo que possa ser facilmente entendida, e a partir da qual possamos inferir fatos e ações importantes. Esperamos que o modelo lide com apenas um trabalho e aceitamos que irá ocasionalmente agir como uma máquina ignorante com enormes pontos cegos.[68]

---

[65] O'NEIL, Cathy. **Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia** / Cathy O'Neil; tradução Rafael Abraham. 1 ed. Santo André, SP; Editora Rua do Sabão, 2020, p. 7.
[66] Ibid. p. 8.
[67] Ibid., p. 30-33.
[68] Ibid., p. 33-34.

Sobre esses pontos cegos, a autora frisa que eles refletem o "julgamento e as prioridades" dos indivíduos que criaram o modelo. Por isso, ainda que os modelos sejam vistos como sendo imparciais, eles acabam refletindo os valores de seus criadores, dessa forma "modelos são opiniões embutidas em matemática".[69]

Ao longo de seu livro, O'Neil expõe algumas características que fazem do *Big Data* uma ameaça, como por exemplo a falta de transparência e a existência de vieses presentes nos modelos, oriundos dos valores e princípios defendidos por seus criadores. A autora também analisa diversos casos concretos nos quais o *Big Data* foi utilizado de forma prejudicial no campo da publicidade, economia, segurança pública[70], vida privada, entre outros. Resumindo:

> (...) Prometendo eficiência e justiça, elas distorcem o ensino superior, aumentam as dívidas, estimulam o encarceramento em massa, esmagam os pobres em quase todos os momentos, e minam a democracia. Pode parecer que a resposta lógica seria desarmar essas armas, uma por uma.
>
> O problema é que elas alimentam-se umas das outras. Pessoas pobres são mais propensas a ter pouco crédito e viver em bairros com maior incidência de crimes, cercadas por outras pessoas pobres. Uma vez que o universo sombrio das ADMs digere esses dados, ele inunda essas pessoas com anúncios predatórios de empréstimos imobiliários de alto risco ou universidades com fins lucrativos. Envia mais policiamento para prendê-las, e quando são condenadas as sentencia com penas mais duras. Esses dados alimentam outras ADMs, que marcam as mesmas pessoas como de alto risco ou alvos fáceis e prosseguem a bloqueá-las de empregos, enquanto aumentam seus juros para empréstimos imobiliários, de carros e todo e qualquer plano de seguro imaginável. Isso derruba ainda mais sua classificação de crédito, criando nada menos que uma espiral mortal de modelagem. Ser pobre em um mundo de ADMs está se tornando cada vez mais perigoso e custoso.
>
> As mesmas ADMs que abusam dos pobres também posicionam as classes abastadas da sociedade em lugares protegidos e confortáveis. As enviam para férias em Aruba e para estudar na escola de negócios Wharton. Para muitos deles, pode parecer que o mundo está ficando mais fácil e inteligente. Os modelos destacam pechinchas no prosciutto e chianti, recomendam um ótimo filme no Amazon Prime, ou os conduzem passo a passo até um café num bairro que costumava ser "suspeito". A natureza silenciosa e personalizada desse targeting impede que os vencedores sociais vejam

[69] Idem, p. 35.
[70] Este ponto será analisado mais a frente.

> como esses mesmos modelos estão destruindo vidas, às vezes apenas a algumas quadras de distância.[71]

Sob essa ótica, ultrapassada a exposição da definição e algumas problemáticas que circundam o tema, é primordial analisarmos brevemente também o *Big Data* inserido no contexto do capitalismo de vigilância. Partindo da premissa de que, nos dias atuais, ter o controle da informação e da produção de conhecimento é uma forma de produção de riqueza (LOPES apud PIMENTA, 2013, p. 6) Para tanto, revisitaremos as observações de Soshana Zuboff em seu artigo "Big Other: Capitalismo de Vigilância e Perspectivas para uma civilização de informação". A autora estudará o *Big Data* não como uma tecnologia ou processo autônomo, mas como um evento social, sob a nova lógica de acumulação (capitalismo de vigilância) a partir do modus operandi do Google, visto que é considerada como a empresa pioneira do *Big Data* – e que tem servido de modelo para demais empresas e startups.

Assim, Zuboff trata inicialmente do trabalho basilar quando se aborda o *Big Data*: os dados, a extração e a análise. No caso dos dados, a autora afirma que os dados oriundos de transações econômicas mediadas por computadores ocupam em larga escala uma proporção do *Big Data*. Porém, existem outras fontes que devem ser levadas em consideração, são cinco ao todo. Dessa forma, uma segunda fonte que provem dados para o fenômeno em comento é a internet das coisas (IoT)[72]. Outra fonte de dados também relevante advém dos bancos de dados governamentais e corporativos[73]. A quarta fonte de dados que compõe o *Big Data* deriva das câmeras de vigilância pública e privadas, "desde *smarthpones* até satélites, do Google Street

---

[71] O'NEIL, Cathy. **Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia**. 2020, p. 8.p. 307-308.

[72]Internet das coisas (IoT) pode ser entendido como: "É toda e qualquer tecnologia que possibilita que os mais diferentes objetos se conectem à internet e interajam com ela. É o que você já vê no seu computador, celular, relógio ou *SmartTV* sendo aplicado em sua geladeira, micro-ondas, ar condicionado ou até no seu carro.". Dessa forma, Zuboff afirma que: "Os novos investimentos da Google em *machine learning**, *drones*, dispositivos vestíveis, carros automatizados, nanopartículas que patrulham o corpo procurando por sinais de doenças e dispositivos inteligentes para o monitoramento do lar são componentes essenciais dessa cada vez maior rede de sensores inteligentes e dispositivos conectados à internet destinados a formar uma nova infraestrutura inteligente para corpos e objetos" ZUBOFF, Soshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**; tradução de George Schlesinger - 1. Ed. – Rio de Janeiro, RJ: Intrínseca, 2020, p. 27.

[73]Sobre essa terceira fonte, Zuboff comenta que tais dados incluem: "aqueles associados aos bancos, a intermediação de pagamentos eletrônicos, as agências de avaliaçao de crédito, as companhias aéreas, aos registros censitários e fiscais, as operações de planos de saúde, aos cartões de crédito, aos seguros, as empresas farmacêuticas e de comunicações, e outros mais. Muitos desses dados, juntamente com os fluxos das transações comerciais, são adquiridos, agregados, analisados, acondicionados e por fim vendidos por *data brokers* que operam (pelo menos nos Estados Unidos) de forma sigilosa, ao largo dos estatutos de proteção do consumidor e sem seu consentimento e conhecimento, ignorando seus direitos a privacidade e aos devidos procedimentos legais. Idem, p. 28.

View ao Google Earth"[74]. Por fim, a quinta e última fonte seriam as "formas não mercantis de "produção social", isto é, a expressão individual de cada ser humano.[75]

Acerca da extração dos dados, de acordo com Zuboff, é um processo "unidirecional", no qual se toma algo, uma informação, o dado, não existe uma relação de reciprocidade, trata-se de um elo unilateral. Isso porque "os processos extrativos que tornam o *big data* possível normalmente ocorrem na ausência de diálogo ou de consentimento, apesar de indicarem tanto fatos quanto subjetividades de vidas individuais."[76]. Dessa forma, a autora acredita que é a subjetividade que agrega valor aos dados extraídos. Em suas palavras:

> Na verdade, é o status de tais dados como sinais de subjetividades que os tornam mais valiosos para os anunciantes. Para a Google e outros agregadores de big data, no entanto, os dados são apenas bits. As subjetividades são convertidas em objetos que reorientam o subjetivo para a mercantilização.[77]

Já sobre a análise dos dados, observa-se que para efetuar este procedimento de análise se faz necessário cientistas de dados que dominem certos métodos capazes de realizar "análises preditivas, mineração de realidade, análise de padrões de vida e assim por diante", e além dessa necessidade de conhecimento, há uma demanda material, isto é, a "hiperescala" – servidores virtuais cuja capacidade de computação pode ser expandida, sem que seja necessário expandir o espaço físico ou investir em máquinas de resfriamento de computadores ou ainda o consumo de energia elétrica. Outrossim, a autora explica a lógica de acumulação concatenada ao *Big Data* e liderada pelo Google, declarado que as receitas decorrem de ativos de vigilância,

---

[74] Sobre o Google Street View a autora apresenta a problemática concernente a falta de autorização para a execução do dispositivo, ela explica: "O Street View sofreu restrições em muitos países e continua a enfrentar processos litigiosos em torno do que os reclamantes caracterizam como táticas "secretas", "ilícitas" e "ilegais" de coleta de dados nos Estados Unidos, na Europa e em outras regiões. Com o Street View, a Google desenvolveu um método declarativo que foi utilizado em outros empreendimentos relativos a dados. O *modus operandi* consiste em fazer incursões em territórios privados não protegidos até que alguma resistência seja encontrada. Como um observador dos direitos do consumidor resumiu para o *The New York Times*, "a Google coloca a inovação a frente de tudo e resiste a pedir permissao"29. A empresa não pergunta se pode fotografar casas para seus bancos de dados, ela simplesmente pega o que quer. A Google, então, esgota seus adversários no tribunal ou eventualmente concorda em pagar multas que representam um investimento negligenciável para um retorno significativo". Idem, p. 29-30.

[75] Zuboff elucida de que essa quinta fonte, qual sejam as formas de produção social são denominadas de "cotidianidade". Essas fontes seriam: "As necessidades individuais de autoexpressão, voz, influencia, informação, aprendizagem, empoderamento e conexão reuniram em poucos anos uma ampla gama de novas capacidades: pesquisas do Google, música do iPod, páginas do Facebook, vídeos do YouTube, *blogs*, redes, comunidades de amigos, estranhos e colegas, todos ultrapassando as antigas fronteiras institucionais e geográficas em uma espécie de exultação de caça, coleta e compartilhamento de informações para todos os propósitos, ou mesmo para nenhum.". Idem, p. 31.

[76] Idem, p. 34.

[77] Idem, p. 34.

ou seja, operações automatizadas que se apropriam de dados, podendo tais ativos serem caracterizados como contrabando "na medida em que foram tomados, em vez de fornecidos"[78]

Destarte, Zuboff também apresenta um novo personagem inserido no contexto do dessa nova lógica capitalista e do *Big Data*: o *Big Other*, um novo poder soberano. Em suas palavras:

> Essa nova arquitetura configura-se como um ubíquo regime institucional em rede que registra, modifica e mercantiliza a experiencia cotidiana, desde o uso de um eletrodoméstico até seus próprios corpos, da comunicação ao pensamento, tudo com vista a estabelecer novos caminhos para a monetização e o lucro. O Big Other é o poder soberano de um futuro próximo que aniquila a liberdade alcançada pelo Estado de direito. É um novo regime de fatos independentes e independentemente controlados que suplanta a necessidade de contratos, de governança e o dinamismo de uma democracia de mercado. O Big Other é a encarnação, no século XXI, do texto eletrônico que aspira abranger e revelar os amplos fatos imanentes de comportamentos econômicos, sociais, físicos e biológicos.[79]

Por conseguinte, com a instituição deste novo poder, a autora afirma que não há escapatória, uma vez que o corpo do ser humano – por dentro e por fora – estão impregnados de dados e viabilizam o monitoramento sobre si mesmo, dando margem para a instituição de um comportamento que já fora antecipado. Zuboff elucida:

> Nesse mundo do qual não existe fuga, os efeitos arrepiantes da conformidade antecipatória cedem a medida que a agencia mental e o autodomínio da antecipação são gradualmente submersos em um novo tipo de automatização. A conformidade antecipatória assume um ponto de origem na consciência a partir do qual é feita a escolha de se conformar, com o objetivo de evitar sanções e de camuflagem social. Isso também implica uma diferença, ou pelo menos a possibilidade de uma diferença, entre o comportamento que se deveria ter performado e o comportamento que se escolhe performar como uma solução instrumental contra o poder invasivo.[80]

E sob essa lógica, essa conformidade antecipatória não aprisiona o indivíduo a tomar uma certa atitude, no entanto, qualquer caminho que ele escolha já foi antecipado e "moldado pelos interesses financeiros e/ou ideológicos, que incubem o *Big Other* e invadem

[78] Idem, p. 39.
[79] Idem, p. 44.
[80] Idem, p. 45.

todos os aspectos da "vida privada" de cada um". Sendo assim, esse poder agora é voltado para a "propriedade dos meios de modificação comportamental"[81]. Outrossim, sob essa perspectiva da ubiquidade deste novo poder soberano, o trabalho da vigilância nestes termos não seria o de suprimir os direitos de privacidade, mas sim redistribuí-los. Nas palavras de Zuboff:

> Os capitalistas de vigilância exploraram de forma hábil um lapso na evolução social, uma vez que o rápido desenvolvimento de suas habilidades de vigiar para o lucro em muito suplantou a compreensão pública e o eventual desenvolvimento de leis e regulamentações legais. Como resultado, os direitos a privacidade, uma vez acumulados e afirmados, podem então ser invocados como legitimação para manter a obscuridade das operações de vigilância.
>
> (...)
>
> Esses argumentos sugerem que a lógica da acumulação que sustenta o capitalismo de vigilância não é totalmente capturada pelo campo institucional convencional da empresa privada. Acumulam-se não apenas capital e ativos de vigilância, mas também direitos. Isso ocorre mediante um agenciamento único de processos de negócios, que opera fora dos auspícios de mecanismos democráticos legítimos ou das tradicionais pressões do mercado, de reciprocidade e escolha do consumidor. Essa acumulação é obtida por meio de uma declaração unilateral que se parece mais com as relações sociais de uma autoridade absolutista pré-moderna. No contexto dessa nova forma de mercado que eu chamo de capitalismo de vigilância, a hiperescala se torna uma ameaça profundamente antidemocrática.[82]

À vista do exposto, torna-se evidente que compreende como a utilização desses dados e a crescente expansão do *Big Data* em inúmeras searas da vida humana está sendo desempenhada, tendo em vista as diversas consequências que afetam a sociedade. Por esse motivo, analisar o impacto do *Big Data* no âmbito da segurança pública é fundamental, posto que aqui se está lidando com os direitos e liberdades dos indivíduos. Assim sendo, passaremos a rápida análise deste fenômeno no contexto da segurança pública, introduzindo o tema central deste trabalho (e que será examinado no segundo capítulo), o policiamento preditivo.

2.4 *Big Data* e segurança pública: uma introdução ao policiamento preditivo

[81] Idem, p. 45.
[82] Idem, p. 47-49.

Consoante o entendimento de Chan e Bennett, o *Big Data* pode ser utilizado principalmente em duas frentes dentro do contexto da criminologia: primeiramente, como fonte de pesquisa para estudiosos da área das ciências criminais, que passaram a utilizar os dados oriundos das redes sociais para complementar ou substituir pesquisas decorrentes de entrevistas, inquéritos etc; segundamente, o *Big Data* também é utilizado como ferramenta para computadores gerarem modelos algorítmicos de predição, visando guiar estratégias de policiamento e demais decisões quando se trata de justiça penal.[83]

Dessa forma, focaremos nesta segunda aplicação do *Big Data*, qual seja como instrumento de predição, cujo objetivo é orientar táticas de policiamento. De acordo com as pesquisadoras:

> A utilização do policiamento preditivo vai além da análise de *hotspots* – policiamento orientado para mapeamento de crimes, a partir do uso e análise de dados, com o fim de prever onde e quando o próximo crime ou séries de crimes ocorrerão. Tais previsões se debruçam sobre um lugar e tempo específicos, com alta probabilidade de ocorrência de crimes, sobre indivíduos que, futuramente, possam estar em situação de risco, criando também perfis precisos sobre prováveis infratores que já tenham cometido crimes específicos no passado, bem como identificando grupos ou indivíduos que correm o risco de se tornarem vítimas de crimes. [84]

As autoras esclarecem que a análise preditiva "não se desvia dos métodos de pesquisa comumente utilizado na criminologia quantitativa"[85]. Isso porque o próprio policiamento preditivo é estabelecido por meio de conceitos e teorias já assentadas na criminologia, como por exemplo o policiamento orientado para problemas e a teoria da vitimização repetida.

---

[83] CHAN, Janet; BENNETT MOSES, Lyria**. Is Big Data Challenging Criminology?.** UNSW Law Research Paper No. 20-81, 2015. p. 5.

[84] Tradução minha. No original: "The rise of 'predictive policing' goes beyond hotspot analysis, problem-oriented policing and crime mapping to use data and analytics to 'forecast where and when the next crime or series of crimes will take place' (Uchida, 2013: 3871). These predictions can be about 'places and times with an increased risk of crime', 'individuals at risk of offending in the future', creating 'profiles that accurately match likely offenders with specific past crimes' or identifying groups or individuals at risk of becoming victims of crime" Idem, p. 7

[85] Tradução minha. No original: "The predictive analytics presented thus far does not deviate substantially from normal research methods used in quantitative criminology. The use of predictive policing, for example, is very much informed by established concepts and theories such as situational crime prevention, problem-oriented policing and repeat victimization theory (Uchida, 2013)." Idem, p. 8.

Outra definição, desta vez trazida pela pesquisadora e pós-doutoranda pela USP, Letícia Gomes Simões, resume o policiamento preditivo como:

> O policiamento preditivo pode ser definido como uma "aplicação da modelagem por computadores a dados criminais passados para predizer atividade criminal futura" (BACHNER, apud JOH, 2014, p. 42, tradução livre), ou seja, "Policiamento preditivo é a fusão da 'tecnologia da informação…, teoria criminológica, [e] algoritmos preditivos'. Em outras palavras, é o 'uso de dados e análises para predizer o crime'" (SELBST, 2017, p. 114, tradução livre, notas omitidas). O uso de análises estatísticas e projeções para o trabalho policial tampouco é novidade. O que muda, aqui, é a expansão dessa lógica para uma situação com mais dados disponíveis e mais poder para analisá-los, o que tornaria tais policiamentos mais precisos, neutros e confiáveis.[86]

Retomando as lições de Cathy O'Neil, a autora também trata do policiamento preditivo em seu livro sobre *Big Data*. Para exemplificar esse método de policiamento, a autora utiliza o caso da cidade de Reading, na Pensilvânia, Estados Unidos. Ela conta que em 2013 a polícia da cidade investiu em um *software* de previsão de crimes criado uma startup da Califórnia, a PredPol[87]. O objetivo do programa era processar dados de histórico criminal e calcular onde a taxa de ocorrência de crimes seria mais alta, assim "os policiais de Reading podiam ver as conclusões do programa como uma série de quadrantes, cada um com quase o tamanho de dois campos de futebol".[88]

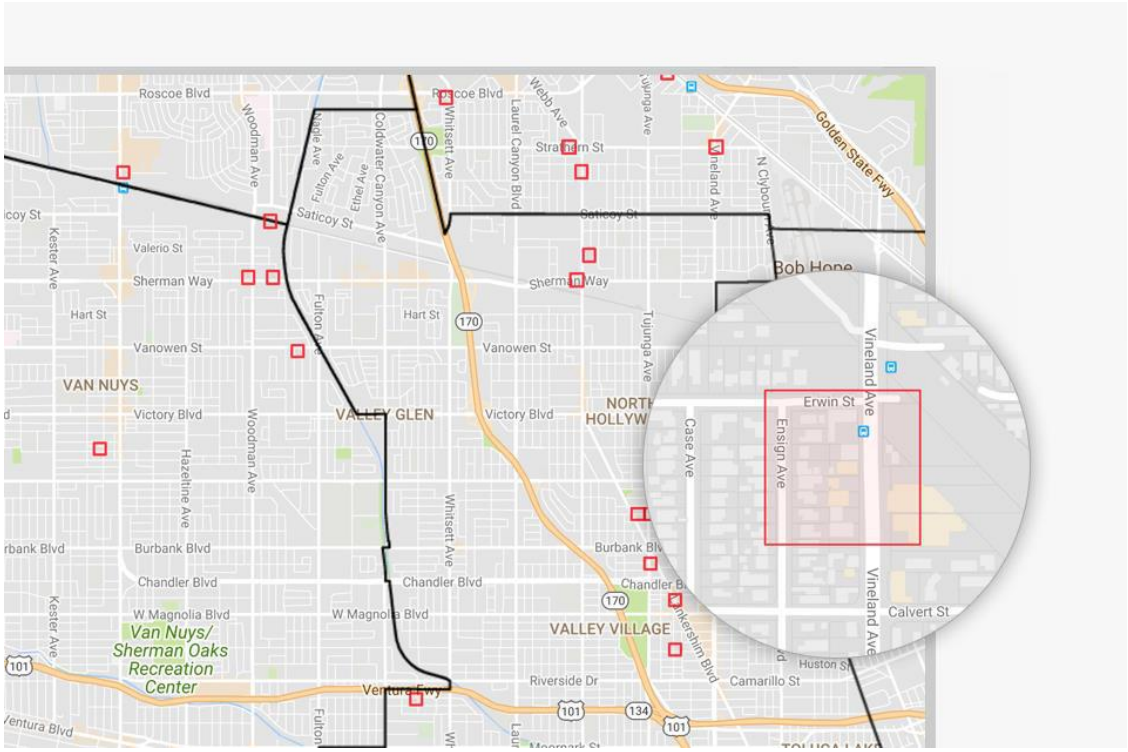
O'Neil então correlaciona esse tipo de modelo de predição sobre quais locais são mais perigosos com modelos de deslocamento de defesa num jogo de beisebol – e consequentemente, necessitam de mais policiamento. Ela explica que:

> Aqueles sistemas olham para o histórico de rebatidas de cada jogador e então posicionam os defensores no lugar onde é mais provável conseguir pegar a bola. Softwares de previsão de crimes realizam análises parecidas, posicionando policiais em locais onde crimes parecem ser mais prováveis de ocorrer. Ambos os tipos de

[86] GOMES, Letícia Simões. **Policiamento preditivo, controle social e desigualdades raciais**. Anais do 43º Encontro Anual da ANPOCS, Caxambu-MG, 2019.
[87] A startup agora chama-se Geolitica, de acordo com as informações em seu *website* (https://www.predpol.com/)
[88] O'NEIL, Cathy. **Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia** / Cathy O'Neil; tradução Rafael Abraham. 1 ed. Santo André, SP; Editora Rua do Sabão, 2020, p. 134.

modelo otimizam recursos. Mas vários dos modelos de previsão de crimes são mais sofisticados, porque preveem progressões que podem levar a ondas de crimes. O PredPol, por exemplo, é baseado em software sísmico: ele vê um crime numa área, o incorpora em padrões de histórico, e faz a previsão de onde e quando pode ocorrer novamente. (Uma correlação simples que ele encontrou: se assaltantes baterem na casa do vizinho, prepare-se para o pior).[89]

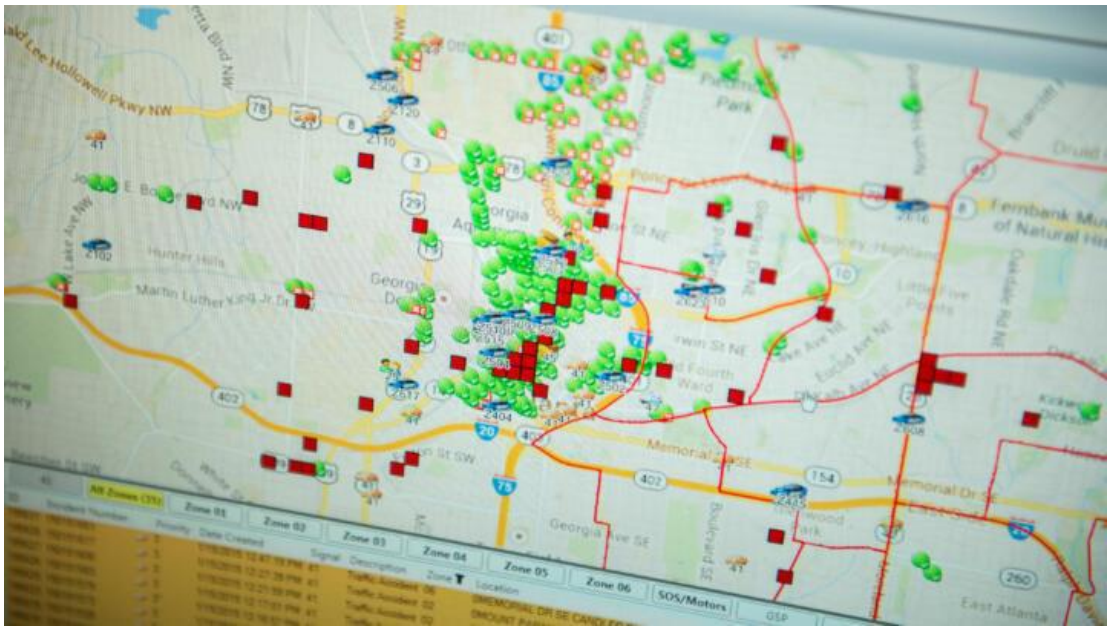
Figura 3 - Mapa gerado pelo PredPol



Fonte: website do Prepol (https://www.predpol.com)

[89] O'NEIL, Cathy. **Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia**. 2020, p. 135.

Figura 4 - Mapa da cidade de Atlanta, Géorgia (EUA), gerado pelo PredPol



Fonte: The Markup

Todavia, ainda que esse tipo de software de modelo de previsão de crime seja, de fato, uma inovação na esfera pública e tenha como fim cooperar com as forças policiais, com o objetivo de garantir maior segurança a população, apresentando vantagens como a eficiência do trabalho policial e a redução de custos, ainda há algumas questões controvertidas que circundam esses modelos de predição, como por exemplo a incidência de vieses (que ensejam na discriminação de pobres e negros), questões sobre a privacidade dos indivíduos, a opacidade incorporada a tal modelo, entre tantas outras questões que serão abordadas no próximo capítulo deste trabalho.

3 *BIG DATA* COMO A NOVA BOLA DE CRISTAL DA POLÍCIA: O POLICIAMENTO PREDITIVO

Dando continuidade ao tema, ainda de acordo com o exposto por O'Neil[90] acerca do *software* desenvolvido pela PredPol, ela esclarece que o modelo não tem como foco principal o indivíduo, mas sim a localização geográfica:

[90] Importante relembrar que O'Neil é norte-americana e sua obra leva em consideração as especificidades de seu país.

> Os inputs principais são o tipo e local de cada crime e quando ocorreram. Parece justo o bastante. E se os policiais passarem mais tempo em áreas de alto risco, repelindo ladrões e assaltantes de carro, há boas razões para crer que a comunidade se sairá beneficiada.[91]

Entretanto, a autora narra um problema grave que rodeia esse tipo de modelo, ela explica que:

> Quando a polícia configura seu sistema PredPol, ela tem uma escolha. Podem concentrar-se exclusivamente nos chamados crimes Parte 1. São os crimes violentos, incluindo homicídio, agressão e incêndio criminoso. Mas podem também ampliar o foco ao incluir crimes Parte 2, incluindo vadiagem, mendicância mais agressiva, bem como consumo e venda de pequenas quantias de drogas. Muitos desses crimes de "perturbação" não seriam registrados se um policial não estivesse lá para vê-los.[92]

Neste viés, essa complicação acaba acarretando num "ciclo nocivo de feedback", visto que "a própria polícia gera novos dados, o que justifica mais policiamento"[93], colocando em foco a questão da discriminação decorrente deste tipo de configuração:

> Esses crimes de perturbação são endêmicos em muitos bairros empobrecidos (...). Infelizmente, incluí-los no modelo ameaça distorcer a análise. Uma vez que os dados de perturbação fluam para dentro de um modelo de previsão, mais policiais são atraídos para aqueles bairros, onde é mais provável que prendam mais pessoas. Afinal, mesmo que o objetivo seja impedir assaltos, assassinatos e estupros, sempre haverá períodos calmos. É da natureza do patrulhamento. E se um policial em patrulha vê alguns jovens que não parecem ter mais de dezesseis anos bebendo algo de uma garrafa escondida, ele os para. Esses tipos de crimes de menor grau povoam os modelos com mais e mais pontos, e os modelos enviam os policiais de volta aos mesmos bairros.[94]

Nesse sentido, é possível culpabilizar a ocorrência desses resultados enviesados haja vista a possível presença dos ditos "laços de reforço". Eduardo Bertassi[95] clarifica que "Em

---

[91] O'NEIL, Cathy. **Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia**. 2020, p 136.
[92] Idem, p. 136.
[93] Idem, p. 137.
[94] Ibid., p. 137.
[95] Engenheiro e mestrando em engenharia da computação pela Escola Politécnica da Universidade de São Paulo e pesquisador do CEST-USP.

engenharia de sistemas, um laço de reforço (do inglês *reinforcing loops*) é aquele em que uma ação produz um resultado que influencia mais da mesma ação, resultando em taxas de crescimento ou redução. Os laços podem ser dos tipos positivo ou negativo"[96]. Dessa forma, o engenheiro explica que o temor acerca desses *reinforcing loops* consiste na probabilidade do algoritmo apontar regularmente "os mesmos criminosos, ou as mesmas regiões da cidade, devido à quantidade de ocorrências passadas e recentes registradas"[97], corroborando, portanto, com o que foi destacado por O'Neil.

Seguindo nesta linha, é relevante abordamos mais exemplos da utilização do policiamento preditivo antes de iniciarmos sua análise detalhadamente. Além da cidade de Reading, na Pensilvânia (EUA), o *software* da PredPol também já foi utilizado em Los Angeles, na Califórnia (EUA) – inclusive, o departamento de polícia de Los Angeles é conhecido por ser pioneiro no uso de programas que utilizam dados e *softwares* para prever crimes. Entretanto, após o compartilhamento de documentos acerca do *modus operandi* do modelo – que confirmaram a existência de padrões de policiamento, acarretando no reforço do patrulhamento em determinados bairros mais pobres e em comunidades negras –, juntamente da ostensiva pressão popular, o departamento da polícia de LA (LAPD) encerrou seu contrato com a empresa em abril 2020[98].

Ademais, ainda se tratando do território norte-americano, outro exemplo famoso do uso de modelos de predição para prever crimes era aquele empregado pelo Departamento de Polícia da cidade Chicago, em Illinois. O programa era denominado de "Heat List" ou "Strategic Subjects List" (SSL) e ensejou na criação de uma lista, gerada por um algoritmo, cujo objetivo era identificar pessoas com maior probabilidade de se envolverem em um incidente com arma de fogo, fosse como infrator ou como vítima e, assim, tais indivíduos eram

[96]O autor apresenta exemplos sobre esses laços de reforço: "Um exemplo de laço de reforço positivo é o do crescimento populacional: quanto maior for a população de um país, maior será o aumento de nascimentos e quanto maior for o número de nascimentos, maior será a população de um país. Um exemplo de laço de reforço negativo é o da relação de predação: quanto maior for o número de predadores em uma área, menor será o número de presas e quanto menor for o número de presas, menor será o número de predadores; porém, quando o número de predadores diminuir, o número de presas voltará a aumentar (caso elas não tenham sido extintas), e o número de predadores também aumentará (caso eles não tenham morrido por inanição). Por simplificação, os fatores externos que influenciam as taxas de crescimento ou redução foram desconsiderados." In: BERTASSI, Eduardo. **Considerações sobre *softwares* de policiamento preditivo**. Boletim – Volume 3, Número 11, Dezembro/2018, São Paulo/SP, p. 3.

[97] Idem, p. 3.

[98] Para ter mais detalhes sobre o tema, recomenda-se a leitura da matéria do The Guardian "*LAPD ended predictive policing programs amid public outcry. A new effort shares many of their flaws.*

submetidos a intervenções policiais, como por exemplo: visita domiciliar, aumento de vigilância e convite para reuniões comunitárias. Contudo, após uma extensa análise do programa constatou-se a sua ineficácia, tendo em vista a elevada dependência de dados oriundos de registros de prisão, o que tornava a ferramenta pouco confiável. Assim, em janeiro de 2020 o programa foi arquivado definitivamente.[99]

Insta ressaltar que esse tipo de tecnologia não vem sendo empregado somente nos Estados Unidos. Na Europa já existem relatos do emprego de sistemas de policiamento preditivo, é o caso do "*Gang Matrix"* em Londres, capital da Inglaterra, e do "*X-law"*[100] em Nápoles, na Itália. No exemplo londrino, a ferramenta foi lançada em 2012 e trata-se de uma base de dados que reúne informações sobre indivíduos suspeitos com maiores chances de se envolverem em incidentes executados por gangues. De acordo com uma pesquisa realizada pela Anistia Internacional, em outubro de 2017, 3.806 pessoas estavam inseridas no sistema, e destas 78% eram negras – um valor incompatível, visto que de acordo com dados do próprio departamento de polícia londrino apenas 27% dos jovens infratores responsáveis por crimes violentos são negros[101].

No continente asiático também já se verifica a utilização de tecnologias que visam predizer o crime. Em Kanagawa, no Japão, a força policial japonesa inaugurou um *software* de policiamento preditivo que faz uso de inteligência artificial (IA). No caso japonês, foram feitos testes com a utilização de IA para auxiliar nas investigações de crimes de lavagem de dinheiro, no qual a ferramenta avaliava o risco e apontava quais casos deveriam ser priorizados. Em outro teste realizado pela polícia japonesa, a inteligência artificial foi empregada nos casos envolvendo violência doméstica e tinha como objetivo indicar o nível de risco que a vítima estaria correndo, a partir da análise detalhada de sua queixa combinada com a sua relação com o acusado. Já na China, na região de Xinjiang, autoridades chinesas foram acusadas de estarem utilizando um sistema de policiamento preditivo para deter arbitrariamente membros da minoria

---

[99] Para saber mais sobre o assunto, recomenda-se a leitura da matéria do *Brennan Center for Justice "Predictive Policing Explained: Attempts to forecast crime with algorithmic techniques could reinforce existing racial biases in the criminal justice system"*

[100] Para entender melhor o programa utilizado pela polícia italiana acesse a matéria da BBC: **Polícia usa algoritmo que prevê crimes para prender ladrão na Iália.** BBC. 19 de novembro 2018, Disponível em: https://www.bbc.com/portuguese/internacional-46198655#:~:text=Um%20agente%20policial%20de%20N%C3%A1poles,prestes%20a%20realizar%20um%20roubo.

[101]A pesquisa completa realizada pela Anistia internacional pode ser encontrada: https://www.amnesty.org.uk/london-trident-gangs-matrix-metropolitan-police

Uigures. De acordo com a ONG Human Rights Watch, a Plataforma de Operações Conjunta[102] utiliza dados visando monitorar ameaças em potencial, levando em conta informações categóricas como por exemplo se o ano de nascimento do sujeito é anterior a 1980".[103]

Por fim, já no território latino-americano, programas de policiamento preditivo também já foram utilizados. No Brasil[104], verifica-se o uso desse tipo de tecnologia nos estados de São Paulo, Rio de Janeiro[105] e Ceará, por exemplo.

Na região paulista, podemos citar o sistema "Detecta"[106], implantando pelo Governo do Estado de São Paulo em 2014 e vigente até os dias atuais, o sistema é composto por "3.144 câmeras em 1.497 pontos de todo o Estado de São Paulo", além disso o sistema contém o "maior banco de dados de informações policiais da América Latina"[107]. De acordo com uma pesquisa realizada pelo Estado de São Paulo, entre abril de 2014 e abril de 2017:

---

[102] *Integrated Joint Operations Platform (IJOP)*

[103] Sobre este caso, recomenda-se a leitura da matéria Masha Borak: **China's big data policing platform 'arbitrarily' targets Uygurs in Xinjiang based on age, family relations, HRW says**. South China Morning Post. 10 de dezembro de 2020. Disponível em: https://www.scmp.com/tech/policy/article/3113208/chinas-big-data-policing-platform-arbitrarily-targets-uygurs-xinjiang

[104] Ademais, visando trazer ainda mais informações sobre o tema no cenário brasileiro, insta citar o recente (2020) concurso de Inovação em Segurança Pública (Inovapol), cuja finalidade é "estimular iniciativas tecnológicas com objetivo de resolver desafios no combate ao crime no Distrito Federal". É promovido por uma instituição privada e conta, por exemplo, com apoio da Polícia Civil do Distrito Federal, bem como entidades sindicais e associações representativas de delegados e peritos. No Edital do concurso é possível observar a apresentação dos desafios tecnológicos, como por exemplo a mineração de dados *(data mining)*. Para maiores informações acesse https://inovapol.com.br/ e o edital https://inovapol.com.br/wp-content/uploads/2021/03/EDITAL_02-INOVAPOL-2020.pdf.

[105]No caso carioca, em 2016, o Instituto Igarapé, em parceria com uma empresa de análise de dados, desenvolveu uma plataforma chamada "CrimeRadar" que utiliza a técnica de aprendizagem de máquina, cujo objetivo era prever as taxas de crimes nos bairros cariocas em horários específicos. Atualmente, os dados encontram-se desatualizados e não se tem informações o emprego do aplicativo pela força policial carioca. Outrossim, de acordo com um relatório do Instituto Igarapé, em 2018 foi realizada uma parceria com o Polícia Militar do Estado de Santa Catarina, visando desenvolver uma versão do CrimeRadar para o estado. Para maiores informações, acesse o website https://igarape.org.br/apps/crimeradar/ e recomenda-se a leitura do relatório "Future Crime: Assessing twenty first century crime prediction", disponível em: https://igarape.org.br/inteligencia-artificial-pode-melhorar-policiamento/.

[106] Para mais detalhes acerca do sistema Detecta, recomenda-se a leitura do artigo elaborado pela pesquisadora Letícia Simões Gomes: Policiamento preditivo, controle social e desigualdades raciais. Anais do 43º Encontro Anual da ANPOCS, Caxambu-MG, 2019.

[107] De acordo com a matéria do Governo do Estado de São Paulo: "Além do monitoramento das câmeras, o Detecta reúne o maior banco de dados de informações policiais da América Latina. Estão integrados ao sistema os bancos de dados das polícias civil e militar, do Registro Digital de Ocorrências (RDO), Instituto de Identificação (IIRGD), Sistema Operacional da Polícia Militar (SIOPM-190), Sistema de Fotos Criminais (Fotocrim), além de dados de veículos e de Carteira Nacional de Habilitação (CNH) do Detran. Os dados reúnem informações e fotos de criminosos procurados, cadastro de pessoas desaparecidas, dados sobre a situação de veículos, se estão com os documentos em ordem, de foram furtados, roubados ou clonados. Também são utilizadas nas operações policiais, as imagens de câmeras particulares, que são analisadas e triadas pelos funcionários das empresas. As imagens relacionadas com ocorrências policiais são enviadas para o banco de dados na forma de alertas. Elas são gravadas e armazenadas onde foram registradas e podem ser requisitadas em caso de ação policial ou militar." In: Portal do Governo de São Paulo. Detecta monitora o Estado de SP com mais de três mil câmeras de vídeo. 2017.

> As imagens captadas contribuíram para a prisão de 4.731 pessoas em flagrante delito; interceptação de 3.320 veículos, apreensão de 276 armas de fogo e leitura de 20 bilhões de placas de automóveis. Na capital, durante o mesmo período, 2.942 pessoas foram detidas, 2.172 veículos interceptados e apreendidas 162 armas de fogo.[108]

Já no Estado do Ceará, em fevereiro de 2021 foi lançado o "Sistema Tecnológico para Acompanhamento de Unidades de Segurança" (Status), um *software* com a finalidade de combater a criminalidade em áreas específicas, a partir da geração de estatísticas de georreferenciamento. O s*oftware* é alimentado, por exemplo, com dados de atendimentos, ocorrências e estatísticas de segurança pública. A partir disso o programa "predefine processos, gera estatísticas georreferenciadas consistentes"[109]. Franklin Torres, estatístico e coordenador da Gerência de Estatística e Geoprocessamento (Geesp/Supesp) explica que esse georreferenciamento:

> É feito através dos boletins de ocorrência (BOs) e inquéritos policiais que são nossa própria fonte de informação, gerados a partir da Polícia Civil. Mas também pegamos dados georreferenciados a partir de cada atendimento que é feito quando alguém liga pro 190, por exemplo, é gerado um ponto no mapa. Ou seja, a partir do endereço fornecido na ocorrência é feita uma marcação no mapa", observa Franklin. "Se alguém liga de um telefone público nós conseguimos identificar a localização desse telefone e lançamos no mapa. Assim também fazemos quando a Perícia (Forense) vai ao local de um crime"[110]

À vista do exposto, considerando avanço e desenvolvimento de novas tecnologias, é notória a ascensão de ferramentas analíticas empregadas no campo da segurança pública, com o propósito de contribuir com a atividade policial e torná-la ainda mais eficiente. Todavia, conforme explicitado em alguns exemplos apresentados, o policiamento preditivo apresenta desafios que devem ser analisados.

---

[108] Idem.

[109] Franklin Torres acrescenta que: "As principais funcionalidades do Status consistem no uso de estatísticas qualitativas das ocorrências importadas por semana, mês e ano; uso de cenários a partir de cadastros de indicadores criminais; apresentação visual do ambiente por meio da realização das análises de mapas; análise de estatísticas por principais tipos criminais, entre outros (...) o próprio Status apresenta os locais, dias e horários em que mais acontecem as ocorrências. Com isso, é possível reforçar o policiamento naquela área. As Delegacias conseguem identificar claramente as suas áreas, assim como o perfil do crime, e enviam viaturas para patrulhar as áreas que concentram maior mancha de calor". In: Portal do Governo do Ceará. Sigo e Status: ferramentas inéditas de tecnologia são usadas no combate a crimes e controle de sinistros. 2021.

[110] Idem.

Dessa forma, daremos continuidade a este capítulo com o objetivo de detalhar o policiamento preditivo, apresentando uma definição pormenorizada, bem como os métodos empregados, e os desafios que circundam o tema.

3.1 Definição e métodos

Conforme já abordado anteriormente, com o desenvolvimento das tecnologias de extração, análise, organização e manipulação dos dados, o *Big Data* tornou-se uma valiosa ferramenta. Desse modo, a quantidade vultuosa adquira se torna processável tendo em vista a capacidade de processamento de dados de super computadores e seus algoritmos (processos matemáticos cujo objetivo é resolver um certo problema), inclusive algoritmos de aprendizagem por máquina *(machine learning)*. Nesse sentido, no contexto das políticas de segurança pública, o uso destes instrumentos matemáticos possibilita e facilita a vigilância exercida pela polícia, a partir da criação e uso de modelos de preditivos no seu cotidiano, com intuito de torna a atividade policial mais eficiente.

Dessa forma, de acordo com uma pesquisa realizada pela RAND Corporation (PERRY, a*t al.*,), o policiamento preditivo pode ser definido como:

> A aplicação de técnicas analíticas, principalmente as técnicas quantitativas, cujo objetivo é identificar prováveis alvos para que sofram uma intervenção policial, prevenir crimes ou resolver crimes passados, a partir de previsões estatísticas. A utilização dessas técnicas estatísticas e geoespacias existem há décadas. Contudo, nos últimos anos, aumentou-se o interesse em ferramentas analíticas que se baseiam em um grande conjunto de dados que visam realizar previsões, a fim de apoiar a prevenção do crime. Esse tipo de instrumento aumenta consideravelmente a confiança da polícia em se debruçar sobre tais tecnologias de informação (TI) para recolher, manter e analisar esse grupamento de dados.
>
> (...)
>
> Agências policiais usam análise informática de informação sobre crimes passados, sobre o ambiente local, e outro tipo de inteligência para prever e prevenir crimes. A ideia é aprimorar o discernimento da situação a nível tático e estratégico, bem como desenvolver estratégias que promovam um policiamento mais eficiente e eficaz. Com essa consciência situacional e antecipação do comportamento humano, a polícia pode identificar e desenvolver estratégias para prevenir atividades criminosas executada

> por infratores reincidentes contra possíveis vítimas. Tais métodos também permitem que os departamentos policiais trabalhem mais proativamente com recursos limitados. [111]

Segundo Moses e Chan, o policiamento preditivo é um termo que deve ser compreendido como um conjunto de ferramentas analíticas e práticas empregadas no cenário policial a fim de garantir o cumprimento da lei. Dessa forma, o policiamento preditivo se dá com o uso dessa série de instrumentos, a partir do qual seria possível prever onde e quando o próximo crime, ou séries de crimes, poderiam ocorrer, auxiliando na tomada de decisão da força policial. Além disso, o elemento essencial neste contexto é o analítico, isto é, o emprego de *softwares* que "analisa históricos de dados sobre crimes (e por vezes, outros dados como por exemplo dados provenientes de meios de comunicação, tempo e inadimplência hipotecária)" com o objetivo de "prever onde, mas também a quem" o crime ocorrerá. Outrossim, essa técnica vai além de somente prever crimes, mas também "envolve a tomada de ação com objetivo de alterar os resultados, por meio da identificação de táticas/estratégias de prevenção do crime" (texto original no rodapé).[112]. Nas palavras das autoras:

> Como um fenômeno, o policiamento preditivo é mais do que um conjunto de ferramentas. O policiamento preditivo é também uma premissa de que é possível utilizar a tecnologia para prever crimes antes mesmo dele ocorrer, que os instrumentos de previsão podem realizar tal previsão com precisão, e que a polícia utilizará este conhecimento eficazmente para reduzir a criminalidade[113].

---

[111] Tradução minha. No original: "Predictive policing is the application of analytical techniques—particularly quantitative techniques—to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions. The use of statistical and geospatial analyses to forecast crime levels has been around for decades. In recent years, however, there has been a surge of interest in analytical tools that draw on very large data sets to make predictions in support of crime prevention. These tools greatly increase police departments' reliance on information technology (IT) to collect, maintain, and analyze those data sets, however (...) Police agencies use computer analysis of information about past crimes, the local environment, and other pertinent intelligence to "predict" and prevent crime. The idea is to improve situational awareness at the tactical and strategic levels and to develop strategies that foster more efficient and effective policing. With situational awareness and anticipation of human behavior, police can identify and develop strategies to prevent criminal activity by repeat offenders against repeat victims. These methods also allow police departments to work more proactively with limited resources." In: PERRY**,** Walter L., *et al*.,.**Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations**. Santa Monica, CA: Rand Corporation. 2013, p. 2.

[112] Tradução minha. No original: "As practised, mostly within the US but also elsewhere, the analytic element typically involves an off-the-shelf or adapted software tool that analyses historic crime data (and sometimes other data such as social media, weather, and mortgage defaults) to predict most commonly where, but sometimes by whom or to whom, crime will take place." CHAN, Janet; MOSES, Bennett. **Lyria Algorithmic prediction in policing: assumptions, evaluation, and accountability, Policing and Society.** 28:7, 806-822, 2018, p. 806

[113] Tradução minha. No original: "As a phenomenon, predictive policing is more than a set of tools. Predictive policing is also premised on the assumptions that it is possible to use technology to predict crime before it happens (van Brakel and De Hert 2011), that forecasting tools can predict accurately, and that police will use this knowledge

Em continuidade, pode-se dizer que o policiamento preditivo possui três objetivos principais: prever potenciais infratores; prever possíveis vítimas; e, por fim, prever quando e onde há um alto risco de haver novas ocorrências de crime. Assim, Hardyns e Rummens explicam que:

> A primeira categoria consiste, por exemplo, em prever uma possível reincidência ou a identificação de possíveis infratores com base nos seus antecedentes criminais, levando em consideração também características do crime. Nestes casos, a análise preditiva complementa outros métodos, como por exemplo perfis geográficos. A segunda categoria destina-se, por exemplo, a prever quais sujeitos possuem risco de se tornarem vítimas de um dado crime, baseado nos dados das vítimas já conhecidas, ou no crescente risco de violência doméstica ou ainda com base dos dados sobre gangues. Já o objetivo da terceira categoria refere-se a prever crimes futuros da forma mais precisa possível no tempo e espaço, a fim de utilizar essa informação para orientar proativamente as rotas de patrulhamento policial ou os locais que carecem do controle policial.
>
> Embora o termo "policiamento preditivo" seja por vezes utilizado para se referir a todas as três categorias, é cada vez mais utilizado para se referir a última categoria. Nesse sentido, o policiamento preditivo pode ser definido: "A utilização de dados históricos para criar uma previsão espaço-temporal de áreas de criminalidade ou *hot sposts* de criminalidade que servirão de base para a tomada de decisões sobre o emprego dos recursos policiais, com a expectativa de que a presença de oficiais no local e hora específicos dissuadirá ou detectará a atividade criminosa"[114]

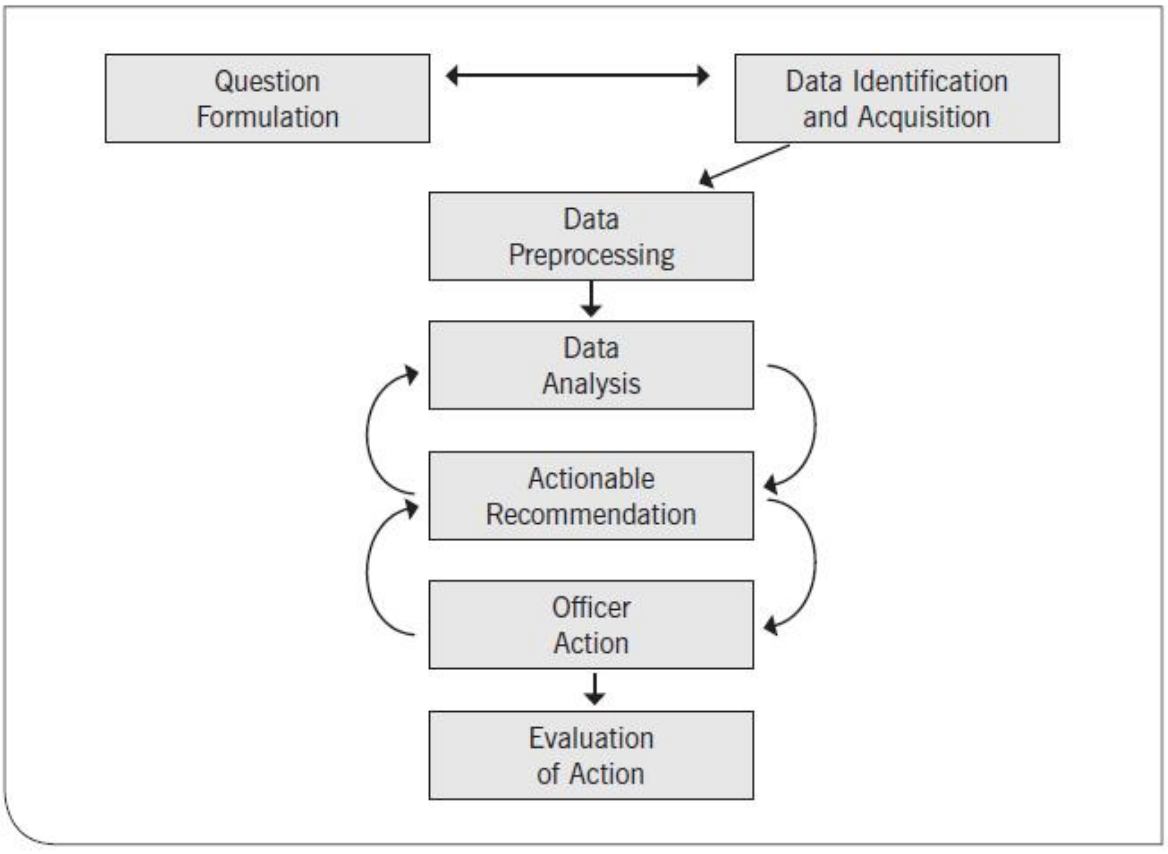
effectively to reduce crime". CHAN, Janet; MOSES, Bennett. **Lyria Algorithmic prediction in policing: assumptions, evaluation, and accountability, Policing and Society.** 28:7, 806-822, 2018, p. 807.

[114] Tradução minha. No original: "The first category consists of, for example, the prediction of recidivism (Berk et al. 2009) or the identification of possible perpetrators based on their background and the characteristics of certain crimes. In these cases, predictive analysis complements other methods such as (geographic) profiling. The second category is aimed at, for example, predicting which people are at risk of becoming a victim of a certain crime based on the known victims' data or the risk of the escalating of domestic or gang violence (Ratcliffe and Rengert 2008). The objective of the third category is to predict future crimes as precise as possible in time and space and use that information to proactively guide police patrol routes or the locations of police controls. Although the term 'predictive policing' is sometimes used to refer to all three categories, it is increasingly used to denote specifically the latter category. In that sense, predictive policing can be defined as: Bthe use of historical data to create a spatiotemporal forecast of areas of criminality or crime hot spots that will be the basis for police resource allocation decisions with the expectation that having officers at the proposed place and time will deter or detect criminal activity (Ratcliffe 2014, p. 4)." In: HARDYNS, Wim, RUMMENS, Aneeleen. **Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges. European Jornal on Criminal Policy Research**, 24, 201–218. 2018, p. 3.

Os autores ainda argumentam, resumidamente, que o objetivo primal do policiamento preditivo é conceber previsões de crime, com o fim de antever certas tendências de criminalidade e utilizar a informação estruturada para formular estratégias de prevenção à criminalidade. Além disso, a longo prazo, a finalidade do policiamento preditivo é ser empregado no âmbito do policiamento conduzido pelos departamentos de inteligência, cujo intuito é aplicar os dados coletados para análise, e como consequência, orientar as operações policiais.[115]

Neste viés, é fundamental analisarmos como se dá um modelo de análise de crime e seu passo-a-passo. A figura abaixo resume bem os componentes deste processo, na concepção de Bachner[116]:

Figura 5 - Modelo de Análise de Crime



Fonte: BACHNER (2013, p. 11)

[115] RATICLIFFE apud HARDYNS e RUMMENS, 2018, p. 3.
[116] BACHNER, Jennifer. **Predictive Policing: Preventing Crime with Data and Analytics.** IBM Center for The Business of Government. 2013, p. 12.

Explicando o esquema acima, o processo de análise de crime se divide em sete etapas: **(1)** a primeira é a formulação de uma pergunta por um agente policial, podendo ser tática, como por exemplo "a previsão da provável localização de roubos de automóveis durante um turno" ou estratégica, por exemplo "a previsão das necessidades policiais pelos próximos dez anos"; **(2)** posteriormente à elaboração da pergunta, um analista criminal irá determinar se a organização tem os dados[117] essenciais para fornecer uma resposta; **(3)** após o levantamento os dados serão processados; **(4)** em seguida, tais dados serão analisados e durante essa fase eles poderão ser remanejados, como por exemplo "com a recodificação de variáveis", "introdução de dados novos" e "validação de dados". Durante esse estágio o analista de dados poderá empregar técnicas como o *clustering*[118]; **(5)** nesta fase, a finalidade da análise é fornecer subsídios para as investigações e gerar possíveis recomendações; **(6)** após a análise e formulação das recomendações, as orientações que forem relevantes serão comunicadas aos oficiais de polícia e utilizadas para auxiliar na tomada de decisão; e **(7)** por fim, após tomada as medidas cabíveis serão realizadas avaliações para determinar de o processo empregado acarretou num resultado favorável.[119]

Sob essa lógica, levando em consideração o modelo de análise de crime descrito, a autora elenca ainda cinco desafios no que diz respeito a implementação deste procedimento. Os desafios regem[120]:

1. **Sobre a coleta e gerenciamento de grandes volumes de dados:** dados utilizados pela polícia advém de diversas fontes, incluindo do próprio governo e de instituições privadas. Assim, a administração desse aglomerado de dados requer um alto investimento de tempo e recursos;

2. **Sobre o conhecimento técnico dos analistas de dados:** é fundamental que os analistas de dados tenham a expertise não só para

[117] Sobre a variedade de dados que podem ser utilizados no Policiamento Preditivo consultar Anexo I.
[118] A técnica de *Clustering* consiste na: "categorização e agrupamento de dados de um conjunto. Ele é feito automaticamente por algoritmos de *machine learning*, que identificam padrões e características em comum entre as informações de maneira autônoma. Isso facilita a análise de dados.". In: COUTINHO, Thiago**. O que é Clustering? Veja como funciona essa análise!** Voitto. 2021.
[119] BACHNER, Jennifer. **Predictive Policing: Preventing Crime with Data and Analytics.** IBM Center for The Business of Government. 2013, p. 11-13.
[120] Idem, p. 13.

> analisar os dados, mas também para traduzir e esclarecer a informação dentro do contexto criminológico. Se este não for o caso, a recomendação do analista de nada servirá para a tomada de decisão da polícia;
>
> 3. **Sobre manter adequadamente os recursos analíticos:** com o rápido avanço da tecnologia, é necessário que as agências policiais proporcionem aos analistas de dados a formação necessária e a tecnologia adequada, como *softwares*, bases de dados e sistemas de informação geográfica;
>
> 4. **Sobre favorecer a comunicação eficaz entre analistas e oficiais da polícia:** a comunicação entre os analistas de dados e os oficiais deve ser clara e compreensiva, tendo em vista que a análise dos dados e a elaboração da recomendação pelos analistas serão utilizadas para auxiliar o trabalho policial na prática;
>
> 5. **Sobre garantir que os oficiais irão considerar as recomendações:** as agências policiais devem estabelecer instruções precisas sobre a forma como as recomendações dos analistas deverão ser utilizadas para embasar a tomada de decisão sobre as estratégias policiais.

Corroborando com o que já foi demonstrado acima, outro modelo de policiamento preditivo nos ajuda a compreender melhor este fenômeno é formulado por Perry, *et al*., em seu relatório de pesquisa para a Rand Corporation. Neste ínterim, insta elucidar que em cada fase do ciclo de policiamento preditivo "são feitas escolhas relativas, como por exemplo os tipos de dados que serão coletados, a duração e frequência da coleta e atualização dos dados", além disso "os tipos de ferramentas analíticas que serão utilizadas, as variáveis que serão focadas, os tipos de operações policiais que serão empregadas, como e quando avaliar o sucesso das intervenções" e, finalmente, "quais modificações devem ser implementadas nessas intervenções durante a avaliação de sucesso". Desse modo, "estas escolhas podem ser tomadas e

implementadas de maneira variada, sob uma série de condições organizacionais, incluindo a nível de caráter pessoal, de recursos, de apoio institucional e de conhecimento técnico".[121]

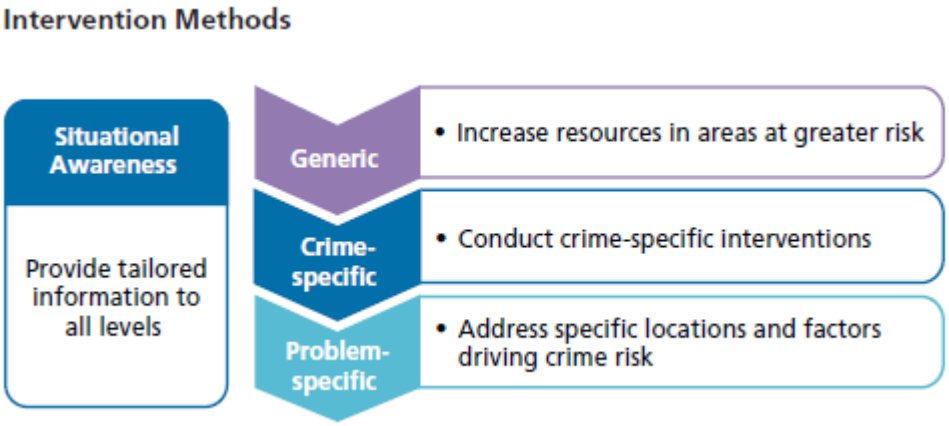
Figura 6 - Processo Comercial de Policiamento com base em Previsões

Fonte: PERRY, *et al.* (2013, p. 12)

Ainda sob essa perspectiva, é necessário abordar também o tipo de intervenção que será escolhido pela força policial. Nesse sentido, Perry, *et al.*, elucida que a intervenção escolhida vai variar de acordo com a situação e com o departamento responsável. Neste viés, os autores elencam os tipos de intervenção, dá mais genérica para a mais específica:

[121] PERRY, *et al*., apud MOSES e CHAN, 2016, p. 807.

Figura 7 - Métodos de Intervenção



Fonte: PERRY, *et al.* (2013, p. 14)

a) Intervenções genérica: diz respeito à alocação de mais recursos, visando responder o aumento do risco. Por exemplo: em *hot spots*, podem ser enviados mais oficiais para o local;

b) Intervenções específicas ao crime: diz respeito à atribuição de recursos adaptáveis ao tipo de crime já previsto. Por exemplo: os recursos podem se concentrar sobre um determinado sujeito que está em vias de cometer uma infração;

c) Intervenções orientadas para um problema específico: diz respeito à identificação e resolução do crime, a nível local, populacional ou envolvendo indivíduos específicos.

Ademais, os autores também fornecem uma "taxonomia dos métodos[122] de policiamento preditivo". Ao todo, são quatro métodos: (1) de predição de crimes, isto é, pretendendo prever locais com alto risco de se ocorrer um crime; (2) de predição de infratores, com objetivo de identificar sujeitos com risco de cometerem uma infração futura; (3) de predição da identidade de ofensores, isto é, criação de perfis que combinam com as

[122] Para visualizar as tabelas referentes a cada método acesse o Anexo II.

características de sujeitos que já possuem antecedentes criminais; e (4) de predição de vítimas, cuja finalidade é identificar indivíduos ou grupos de pessoas com maior probabilidade de se tornarem vítimas de crimes (similar ao método de predição de infratores ou de locais onde possam ocorrer crimes, por exemplo)[123].

Além das definições já expostas, cabe ainda tratarmos das três modalidades de policiamento preditivo de acordo com Selbst: *place-based predictive policing, person-based predictive policing* e *suspect-based predictive policing*. A primeira modalidade é a mais popular e baseia-se na localização, como por exemplo o software da Predpol. Esse modelo de predição "é focado, principalmente, no reconhecimento de *hot spots* e é utilizado para gestão de recursos" e assim "a polícia quer colocar mais agentes onde há ocorrências de crime. Ocasionalmente, havendo um padrão específico, há uma possibilidade da polícia prever uma próxima onda de crime"; A **segunda modalidade** se apoia na predição sobre o sujeito, como por exemplo o *software* da Beware, que permite que a polícia "verifique a pontuação de ameaça de uma pessoa ou de um endereço, logo que chega uma ligação do 911, atribuindo então um rótulo verde, amarelo, ou vermelho" a partir da análise de dados públicos disponíveis. Outro exemplo que cabe aqui seria a *Chicago Heat List*, "capaz de encontrar indivíduos sujeitos a estarem envolvidos numa ação criminosa não especificada futuramente"; Finalmente, a **terceira modalidade** é baseada em suspeitas, ou seja, os sistemas fundamentados em suspeitas são "sistemas digitais proveniente do profilamento de infratores para a criação de um modelo que será utilizado para localizar suspeitos".[124]

---

[123] A respeito dos métodos de predição de crime e predição de vítimas os autores ainda especificam as técnicas analíticas utilizadas, cada qual com seu objetivo específico. Ao todo, eles dividem tais técnicas em quatro classes (conferir a tabela no Anexo III):
1 - "*Classical statistical techniques*: This class includes standard statistical processes, such as most forms of regression, data mining, time-series analysis, and seasonality adjustments;"
2 - "*Simple methods*: Simple methods do not require much in the way of sophisticated computing or large amounts of data. Most heuristic methods, for example, are simple methods—relying more on checklists and indexes than on the analysis of large data sets."
3 - "*Complex applications*: These applications include new and innovative methods or methods that require considerable amounts of data in addition to sophisticated computing tools. Many newer data mining methods and some near-repeat methods fall into this class."
4 - "*Tailored methods*: In several cases examined here, existing techniques were adapted to support predictive policing. For example, classical statistical methods can be used to produce heat maps, which are simple, color-coded grids depicting the intensity of crime activity in a given area." In: PERRY**,** Walter L., *et al*.,. **Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations**. Santa Monica, CA: Rand Corporation. 2013, p. 18.

[124] SELBST, Andrew D. **Disparate impact in Big Data policing**. Georgia Law Review, v. 52, 2017, p. 21-31.

3.2 Mitos

Ultrapassada a análise sobre a definição e esclarecimento dos métodos de policiamento preditivo, é importante revisitarmos brevemente a pesquisa de Perry, *et al.*, para desvendar alguns mitos a respeito desta técnica de predição policial.

Nesse sentido, os autores elencam quatro mitos que circundam o tema[125]*:*

> **1) Sobre a capacidade do computador saber o que vai acontecer no futuro**: os algoritmos de predição empregado no policiamento preditivo não capazes de prever, de fato, os eventos que irão acontecer no futuro, mas sim o seu possível risco de ocorrer. Além disso, de fato, a busca por um padrão é uma tarefa simples para um computador, contudo é importante lembrar que a qualidade das previsões serão diretamente proporcionais com a qualidade dos dados utilizados;
>
> **2) Sobre o computador fazer tudo sozinho**: mesmo com os *softwares* mais avançados, o trabalho humano ainda é fundamental para encontrar dados relevantes, realizar sua análise e interpretar os resultados, a fim de tomar a melhor ação e avaliar o impacto das intervenções;
>
> **3) Sobre a necessidade um modelo caro e de última geração:** na prática, poucos departamentos policiais tem acessos aos melhores computadores para rodarem *softwares* avançados de predição. Em muitos estudos de caso, a simples racionalidade (heurística) funciona tão bem quanto um programa de computador em executar atividades de policiamento preditivo;
>
> **4) Sobre a predição automaticamente reduzir drasticamente a criminalidade:** predições são simplesmente previsões e isso não

[125] PERRY, Walter L., *et al*.,. **Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations**. Santa Monica, CA: Rand Corporation. 2013, p. 115-118.

> significa que irá reduzir a atividade criminosa. Para tanto, é preciso tomar medidas com base nas predições.

Ainda neste viés, é necessário esclarecer que para que os métodos de policiamento preditivo possam ser utilizados como um componente de prevenção de crimes, é preciso evitar cair num lugar comum, em certas armadilhas. Os autores também listam algumas, mas as principais – e que também serão trabalhadas a seguir – dizem respeito à qualidade do dado utilizado e desrespeito aos direitos de privacidade[126].

3.3 Vulnerabilidades

A aplicação do *Big Data* como instrumento para o desenvolvimento de modelos algorítmicos de predição que visam direcionar as táticas de agentes policiais é, de fato, uma inovação profícua e que, até certo ponto, deve ser prestigiada. Contudo, apesar das vantagens fornecidas por esse tipo de tecnologia – por exemplo, a eficiência, melhor alocação de recursos e o apoio na tomada de decisão pelos oficiais –, as consequências da utilização desse modelo de predição devem ser apontadas e debatidas.

---

[126] Ao todo, eles enumeram cinco armadilhas que devem ser observadas durante a aplicação do método de policiamento preditivo:

- "*Focusing on accuracy instead of utility.* It may be accurate to characterize an entire city as a crime hot spot, but such a large area is not "actionable" when it comes to planning police interventions with limited resources. To identify hot spots that are small enough for police to realistically take action, analysts must accept some limits on accuracy as measured by the proportion of overall crime captured by the data;
- *Relying on poor-quality data*. Three typical deficiencies in data quality are data censoring, or omitting data on incidents of interest in particular places or at particular times; systematic bias, which may result from how data are collected; and irrelevant data, or data that are notuseful for the specific problem being addressed;
- *Misunderstanding the factors behind the prediction.* When applying techniques like regression or data mining, analysts should use common sense in selecting factors for analysis to avoid acting on spurious relationships;
- *Underemphasizing assessment and evaluation.* During interviews with practitioners, RAND researchers found that very few respondents had evaluated the effectiveness of their departments' predictions. Measuring effectiveness is key to identifying areas for improvement and allocating resources efficiently;
- *Overlooking civil and privacy rights*. Designating certain areas or individuals as meriting law enforcement action raises civil and privacy rights concerns. The U.S. Supreme Court has ruled that standards for reasonable suspicion are relaxed in "high-crime areas," but what constitutes such an area and what measures may be taken are open questions." In: PERRY**,** Walter L., *et al*.,. **Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations**. Santa Monica, CA: Rand Corporation. 2013, p. 118-125.

Neste viés, passaremos agora à análise de algumas inconsistências que os modelos de policiamento preditivo apresentam, com base nos estudos de Fergunson e Selbst. Neste trabalho não nos debruçaremos sobre todas as complicações que circundam o tema, mas tão somente as mais relevantes. Dessa forma, abordaremos as seguintes problemáticas: discriminação racial (vieses), os dados de natureza ruim (*bad data*), a falta de transparência e a prestação de contas (*accountability*).

a) Discriminação racial

De acordo com Simões-Gomes[127]:

> O conceito de filtragem racial, tanto na literatura norte-americana quanto na brasileira, está localizada no campo do policiamento direto, no contato do agente de segurança pública com o cidadão. Sucede, porém, que o desenvolvimento das próprias políticas de segurança pública em uma sociedade racialmente desigual – mesmo que cegas à raça (*colourblind*) e visando à redução da discricionariedade de onde se imagina provir o tratamento discriminatório – tem reproduzido viés racial ao concretizar-se[128]

É possível afirmar que a polícia, durante sua tomada de decisão, atua de maneira discriminatória, a agência policial "escolhe para onde deseja focar sua atenção, quem prender e quando usar a força" e a partir da análise dessas tomadas de decisão, vislumbra-se que a atuação policial "impacta de maneira desproporcional os sujeitos pobres e negros"[129]. Segundo o autor:

> This is the result of bias built into policing as na institution, as well as unconscious biases of individual police officers. Thus, where police use predictive policing technology, the purpose is not only to detect hidden patterns, but also to inject a "neutral," data-driven tool into the process to prevent unconscious police biases from entering the equation.

---

[127] GOMES, Letícia Simões. **Policiamento preditivo, controle social e desigualdades raciais.** Anais do 43º Encontro Anual da ANPOCS, Caxambu-MG, 2019, p. 3.
[128] SELBST, 2017; FERGUSON; 2015 apud SIMÕES-GOMES, 2019, p. 4
[129] Tradução minha. No original: "Police act with incredible discretion. They choose where to focus their attention, who to arrest, and when to use force. They make many choices every day regarding who is a suspect and who appears to be a criminal. Examined in the aggregate, all of those choices exhibit disproportionate impacts on poor people and people of color." SELBST, Andrew D. **Disparate impact in Big Data policing**. Georgia Law Review, v. 52, 2017, p. 119.

> Predictive policing promises both to provide auditable methods that will prevent invidious intentional discrimination and to mitigate the unconscious biases attending police officers' daily choices. But at the moment, such a promise amounts to little more than a useful sales tactic. Data mining is likely to introduce new discrimination or to reproduce and exacerbate the existing discrimination in society due to various design choices that are necessary to any data mining system.[130]

Nesse sentido, observa-se que o policiamento preditivo, apesar de se apoiar no argumento de que é uma ferramenta neutra – tendo em vista tratar-se de um algoritmo, uma fórmula matemática que está por detrás da tecnologia empregada –, é fundamental deixarmos claro que mesmo a tecnologia pode contar vieses (*bias*) racistas.

Sob essa lógica, cabe aqui uma breve explicação sobre o que é *data mining*, ou seja, "mineração de dados". Essa técnica consiste na utilização de algoritmos de *machine learning* para um grande volume de dados, com intuito de encontrar um dado padrão, relacionando diversas variáveis para então identificar um novo conjunto de dados. Segundo Selbst, funciona da seguinte maneira: "um grande conjunto de casos é exposto ao algoritmo. Então o computador constrói um modelo preditivo, um conjunto de correlações que determinam alguns atributos [oriundos da análise daqueles dados]" assim, uma vez que esses atributos são descobertos "o computador compara novos traços dos sujeitos em estudo, comparando com os atributos já correlacionados, para então fazer uma previsão sobre um resultado ainda inobservável"[131]. Ainda assim, apesar do processo ser realizado por um computador, há chances da própria máquina ser imbuída de vieses, de forma consciente ou inconsciente. Complementando, o argumento do autor:

> By definition, data mining is always a form of statistical (and therefore seemingly rational) discrimination. Indeed, the very point of data mining is to provide a rational basis upon which to distinguish between individuals and to reliably confer to the individual the qualities possessed by those who seem statistically similar. Nevertheless, data mining holds the potential to unduly discount members of legally protected classes and to place them at systematic relative disadvantage. Unlike more

[130] SELBST, Andrew D. **Disparate impact in Big Data policing**. Georgia Law Review, v. 52, 2017, p. 119-120.
[131] Tradução minha. No original: "It works by exposing a machine learning algorithm to examples of cases of interest with known outcomes.85 The computer then builds a predictive model— a set of correlations that determine which related attributes can serve as useful proxies for an otherwise unobservable outcome." SELBST, Andrew D. **Disparate impact in Big Data policing**. Georgia Law Review, v. 52, 2017, p. 127.

> subjective forms of decision making, data mining's ill effects are often not traceable to human bias, conscious or unconscious.[132]

Dessa forma, Simões-Gomes resume bem e elenca alguns pontos em que podem ocorrer uma falta de neutralidade, que acarreta na reprodução de discriminação:

> Dentre eles [níveis], elencam-se: a) a discricionariedade do programador no desenvolvimento do software (o grau de precisão e generalização das variáveis, as conexões causais e exemplos dados à máquina no processo de *machine learning*); b) a confiabilidade dos dados (dado que muitos vêm de *data brokers*, i.e., terceiros que compilam e comercializam informações, outros vêm de bancos de dados do governo); c) a natureza dos dados (como o banco sobre antecedentes criminais estão dentre os mais frequentes, assim como o de ocorrências); d) a manipulação dos dados (em quais categorias crimes são agrupados e qual a sua priorização; e) a inserção dessas técnicas no processo de policiamento (se serve para alocação de recursos, para a formação de "listas de ameaças ("threat lists"), para investigação de suspeitos pré-identificados, etc.)[133]

No policiamento preditivo, a "mineração" dos dados utilizados para alimentar as máquinas de predição derivam de fontes diferenciadas, como por exemplo "dados sobre atividades criminosas passadas, como locais de crime e registros de prisão", em outros casos, as empresas desenvolvedoras desse tipo de *software* "incorporam outros tipos de dados (...) como os dados de redes sociais como o Facebook e Twiter"[134] que são obtidos através da compra de "ferramentas que são desenvolvidas, principalmente, para o mundo dos negócios".[135]

---

[132] SELBST, Andre D., BAROCAS, Salon. **Big Data's Disparate Impact.** California Law Review 671. 2016, p. 677.

[133] GOMES, Letícia Simões. **Policiamento preditivo, controle social e desigualdades raciais.** Anais do 43º Encontro Anual da ANPOCS, Caxambu-MG, 2019, p. 5.

[134] Neste ponto, vê-se aqui um ótimo exemplo da tese de Zuboff acerca dos capitalistas de vigilância e a nova lógica econômica. Isso porque os dados de comunicação oriundos de redes sociais como Facebook e Twitter tornaram-se um produto utilizado para viabilizar uma hipervigilância sobre os indivíduos.

[135] Tradução minha. No original: "In predictive policing, the observed attributes come from data that the police mine from various sources. There are several different approaches to predictive policing. Some primarily use data about past criminal activity, such as crime locations and arrest records, but others incorporate many other types of data. These companies sometimes purchase tools "largely developed by and for the commercial world,"as well as data from social networks such as Facebook and Twitter.88 The unobservable cases of interest are the location and time of future crimes, the likely perpetrators or victims of future crimes, and likely suspects in past crimes." SELBST, Andrew D. **Disparate impact in Big Data policing**. Georgia Law Review, v. 52, 2017, p. 128.

Não obstante, é possível retomar aqui o que já foi elucidado por Cathy O'Neil a respeito do "ciclo nocivo de feedback" que, por conseguinte, reforçam ainda mais o aspecto discriminatório do policiamento preditivo. Simões-Gomes também alerta sobre esse problema:

> Além disso, é interessante notar que a maior parte dessas tecnologias usa como base crimes patrimoniais e/ou ligados ao tráfico de entorpecentes, coincidentemente os tipos mais presentes nas bases de dados criminais. Outras tipologias, como estupro, tortura, crime de ódio, violência doméstica, não entram nesta contabilização. Nesse sentido, Joh (2014) apontou que esses sistemas não estão preparados para alguns tipos de ocorrência, pois muitos deles não obedecem a padrões territoriais. A natureza dos dados, então, é essencial: ao ensinar ao software o que é crime, recorre-se a uma gama duplamente restrita de dados: primeiro, ao ser um banco de dados de justiça criminal, filtra-se pelo sistema de registro oficial (há aqui um viés do que foi notificado enquanto tal, não correspondendo a uma amostra representativa nem universal dos delitos, cf. RATTON JR, 1996; ADORNO, 1993), que consolida vieses historicamente construídos na atividade policial. Segundo, recorta-se tal banco de dados para aqueles que são enquadráveis na construção de uma modelagem específica de *software*, focalizando ainda mais em crimes patrimoniais e/ou relacionados ao tráfico. O sistema, então, tende a reproduzir padrões encontrados nessa seleção.[136]

Revisitando os modelos de policiamento preditivo apresentados por Selbst, quais sejam, *place-based predictive policing, person-based predictive policing* e *suspect-based predictive policing,* insta esclarecer que cada um possui um modus operandi que está longe de serem neutros. Exploraremos resumidamente cada um a seguir.

Primeiramente, acerca do ***place-based predictive policing***, método mais comum quando se fala em policiamento preditivo. Mais uma vez, comprava-se o argumento de O'Neil. O autor explica que primeiro o "*data miner"* deve traduzir a pergunta central de forma que a máquina consiga entender, então um policial não pode simples perguntar "como posso prevenir o crime?", mas sim apresentar uma questão que possa ser traduzida de modo a se obter uma resposta que tenha por base "a valoração de variáveis sobre um determinado alvo". Selbst diz:

> But the categories are not always obvious. If the system is designed to detect crimes within a particular square on a map, it should separate out types of crime. Should "type of crime" be broken down into violent and nonviolent? Should property crimes or

[136] GOMES, Letícia Simões. **Policiamento preditivo, controle social e desigualdades raciais.** Anais do 43º Encontro Anual da ANPOCS, Caxambu-MG, 2019, p. 5-6.

> nuisance crimes be counted separately? Should nuisance crimes then be further broken down? Deciding how to parse the problem can have severe consequences for the ultimate outcome. For example, if the nuance between robberies and burglaries is missing because both are placed in the "property crime" bucket, the algorithm may not detect the difference between an area with high amounts of robberies and an area with a high number of burglaries, though the two crimes might be perpetrated by different people with different victims.[137]

A próxima maneira de enviesar o modelo é através do treinamento do dado. Isso porque o "dado é o único contato que o algoritmo tem com o mundo exterior". Desse modo, é fundamental categorizar corretamente os exemplos que estão sendo utilizados para treinar a máquina. Neste caso, o dado mais utilizado comumente é o derivado de informações sobre crimes passados, geralmente coletado pelos próprios policiais. Dentro deste contexto, rotular esses exemplos significa pontuar se aquele dado "é ou não um crime, e se é, qual tipo de crime".

O problema disso tudo é que dados provenientes de crime "raramente são precisos". E isso se dá visto que, na maioria dos casos, o contato dos departamentos policiais com os infratores é no momento da prisão – e os dados coletados nesta etapa raramente são atualizados. Para piorar, é de conhecimento comum que a polícia prende muito mais pessoas negras. Portanto, ao se considerar dados oriundos dessas detenções como a melhor base de dados, claramente se demonstra o enviesamento racial que será imbuído no algoritmo, assim "resultando numa rotulagem incorreta do tipo de crime, além do modelo aprender que pessoas negras cometem crimes em maior porcentagem".[138]

Outra fonte de dados utilizada pela polícia ou por empresas de tecnologia, capaz de ampliar as taxas de erro e reproduzir vieses, provém da compra de conjunto de dados de "*data brokers"* (corretores de dados). De certa forma, não se pode averiguar a veracidade desses dados que, inclusive, são "otimizados para uso comercial e não para o trabalho policial". Além disso, não existe nenhuma garantia de que esses *data brokers* não iram correlacionar uma dada informação a pessoa errada. Dessa forma, essa "granularidade" dos recursos pode afetar os resultados, visto que pode acarretar numa generalização injusta e, assim, "a decisão mais precisa pode não levar ao resultado mais justo".[139]

---

[137] SELBST, Andrew D. **Disparate impact in Big Data policing**. Georgia Law Review, v. 52, 2017, p. 132.
[138] Ibid., p. 135-136, tradução minha, notas omitidas.
[139] Ibid., p. 136- 137, tradução minha, notas omitidas.

Passando para o segundo método, ***person-based predictive policing***, a consequência relacionada ao viés discriminatório reside na possibilidade do sistema hiper monitorar um indivíduo e, assim que ocorre um crime, os agentes irão averiguar eles primeiro. Ou então, "no caso da polícia responder a uma ocorrência erroneamente classificada como "vermelha" eles podem proceder com uma abordagem com o emprego desnecessário da força "*with an itchy trigger finger*". O autor usa como exemplo o caso da polícia de Los Angeles:

> As sociologist Sarah Brayne has documented, the Los Angeles Police Department's person-based predictive policing uses a simple points-based system, where more points means a person is a greater threat. To find "the worst of the worst," the LAPD adds one point per police contact, leading to the very same type of feedback loops that exist in place-based policing. Over time, the erroneous appearance of greater threat levels in minority neighborhoods could also exacerbate an already adversarial relationship with police and endanger lives as a result. Just like mislabeled instances of crime in place-based systems, the embedding of historically biased policing will teach the algorithm that being a person of color makes one more likely to be a criminal.
>
> (...)
>
> Feature selection is also more complicated with respect to people rather than places. Representations of people in data are necessarily reductive. As Toon Calders and Indre Žliobaite have noted, "[i]t is often impossible to collect all the attributes of a subject or take all the environmental factors into account with a model."Police may be tempted to use certain types of data—for example, race, gender, neighborhood, or age—because it is easily accessible. Choice of features would ideally not be made based on cost or accessibility. Features that do not adequately capture the relevant distinctions between people or locations will make the predictions less accurate. But cost and convenience are common factors in these decisions, and both can lead to discriminatory outcomes[140]

Por fim, quanto ao ***suspect-based predictive policing***, o autor o classifica como o mais problemático dos três modelos. Aqui o perigo discriminatório reside na probabilidade de o resultado fornecido pelo algoritmo apresentar, em maior escala, um grau de suspeita tendo por base a raça de um suspeito.

---

[140] Ibid., p. 138-139.

Comprovando a gravidade do que foi exposto, após o assassinato de George Floyd nos EUA (2020), as empresas IBM, Amazon e Microsoft anunciaram a suspensão da oferta de tecnologia de reconhecimento facial para o uso de forças policiais dos Estados Unidos. Especificamente, as duas primeiras decidiram abandonar o desenvolvimento das tecnologias de vigilância e pausaram as pesquisas. Já o presidente da Microsoft se pronunciou afirmando que a empresa não venderia tecnologia de reconhecimento facial para a polícia estadunidense até que entrasse em vigor uma lei nacional regulando o uso dessas tecnologias.

No cenário brasileiro, alguns exemplos dessas inconsistências presentes no policiamento preditivo também podem ser observados. Foi o caso de Tiago Vianna Gomes, negro, 28 anos, e Luiz Carlos da Costa Justino, negro, 23 anos, ambos em situações diferentes, mas com tantas nuances em comum. Em 2016, Tiago teve sua foto tirada e foi fichado 52ª Delegacia de Polícia de Nova Iguaçu após ter sido acusado pelo crime de receptação, cujo processo respondeu em liberdade. No entanto, sem qualquer explicação, sua foto foi registrada num álbum de suspeito da 57ª Delegacia de Polícia de Nilópolis. Depois disso, o primeiro mandado de prisão resultou em sua prisão durante oito meses; em entrevista para a Folha de São Paulo ele contou que foi “levado para cadeia e perguntava 'fui preso por quê?'. Até que minha mãe, na visita três dias depois, disse que eu estava respondendo por 157”. Desde então, Tiago foi alvo de inúmeras denúncias e todas pelo reconhecimento da mesma foto tirada em 2016.[141]

Em 2020, Luiz Carlos da Costa Justino foi preso por ter sido acusado de um roubo que ocorreu três anos antes e que ele não cometeu. O músico da Orquestra de Cordas da Grota narrou para a Revista Piauí os cinco dias que ficou preso e deu detalhes do caso. No caso do Luiz, o mandado de prisão apresenta inconsistências inequívocas, a primeira era a de que no momento do crime, o músico estava tocando numa padaria, de acordo com a gravação de vídeos no local e; segundo, a vítima do roubo o acusou com base em uma foto dele incluída no banco de dados da Polícia Civil do Rio de Janeiro (PCRJ), o que não faz sentido, uma vez que Luiz não possuía antecedentes criminais.[142]

---

[141] PAULUZE, Thaiza. **Foto em delegacia faz jovem negro ser acusado 9 vezes e preso duas por roubos que não cometeu**. Folha de São Paulo. 2021. Disponível em: https://www1.folha.uol.com.br/cotidiano/2021/01/foto-em-delegacia-faz-jovem-negro-ser-acusado-9-vezes-e-preso-duas-por-roubos-que-nao-cometeu.shtml.

[142] JUSTINO, Luiz Carlos da Costa. **Qual facção, vagabundo?**. Revista Piauí. 2020. Disponível em: https://piaui.folha.uol.com.br/materia/qual-faccao-vagabundo/.

Mais recentemente, em janeiro deste ano, uma imagem do ator norte-americano Michael B. Jordan, famoso por interpretar um personagem no filme *Pantera Negra*, foi utilizada num catálogo (Termo de Reconhecimento Fotográfico) da Polícia Civil do Cerará (PCCE) para reconhecimento de suspeitos que participaram de uma chacina.[143]

Por todo o exposto, resta evidente que a técnica de policiamento preditivo, apesar de ser amplamente difundida sob a égide da neutralidade, por muitas vezes, ostentou um caráter manifestamente enviesado.

Reproduzindo, portanto, uma visão discriminatória e racista, marcada pela super vigilância (e violência) empreendida pelo aparato policial contra indivíduos negros e pobres. E culminando, por conseguinte, na restrição de liberdade desses sujeitos e, em casos piores, em suas mortes.

b) Bad Data

Sem dúvidas, o elemento basilar de qualquer tecnologia de predição são os dados. A dificuldade envolvendo a coleta de dados utilizáveis e precisos para integrarem um sistema de predição expõe a vulnerabilidade deste processo.

Bad Data refere-se a "falhas, fragmentações e uma pressão interna e externa para coletar enormes quantidades de informações constantemente, de maneira instantânea, e ainda sem os recursos financeiros necessários para garantir sua precisão", segundo Ferguson.[144]

Em primeiro lugar, dados precisam ser coletados, e muito dessa informação coletada é realizada por humanos, capazes de cometer erros e isso pode influenciar na limpidez do dado. Além disso, dados também podem ser fragmentados, o autor explica que em crimes como assassinato tendem a serem reportados às autoridades, enquanto outros crimes como

[143] **Foto de astro de cinema Michael B. Jordan aparece em lista de procurados pela Polícia do Cerará.** G1. 2022. Disponível em: https://g1.globo.com/ce/ceara/noticia/2022/01/07/astro-do-cinema-michael-b-jordan-aparece-em-lista-de-procurados-pela-policia-do-ceara.ghtml.
[144] FERGUSON, Andrew Guthrie. **Policing Predictive Policing.** Washington University Law Rewiew, V. 94. Issue 5. 2017, p. 1145.

violência doméstica apresentam uma tendência contrária. Dados também podem conter vieses, conforme já analisado anteriormente, promovendo aquele ciclo nocivo de feedback. De acordo com o autor:

> Some scholars have even argued that such a predictive focus merely increases arrests rather than decreases crime. Finally, explicit bias has also been a factor in the collection of data on suspects, potentially undermining the basis of the predictive technologies. Sadly, racial and class-based bias remain a problem.
>
> (...)
>
> As civil liberties advocate, Hanni Fakhoury, has warned:
>
> It ends up being a self-fulfilling prophecy. . . . The algorithm is telling you exactly what you programmed it to tell you. "Young black kids in the south side of Chicago are more likely to commit crimes," and the algorithm lets the police launder this belief. It's not racism, They can say. They are making the decision based on what the algorithm is, even though the algorithm is going to spit back what you put into it. And if the data is biased to begin with and based on human judgment, then the results the algorithm is going to spit out will reflect those biases.[145]

c) Transparência

Neste ponto, se compara o policiamento preditivo a uma *black-box* (caixa preta). Desse modo, aponta o autor que "a falta de transparência existe em todos os níveis de policiamento preditivo", inclusive "dados simples como estatísticas criminais, que em muitos casos estão disponíveis para o público, são alvo de grande preocupação acerca de sua precisão e completude".[146]

Não obstante, a própria natureza do algoritmo é um fator que intensifica a falta de transparência. Isso porque, com exceção talvez dos próprios desenvolvedores, a agência policial recebe tão somente os resultados, mas não sabe e/ou não entende como o modelo funciona e

[145] FERGUSON, Andrew Guthrie. **Policing Predictive Policing.** Washington University Law Rewiew, V. 94. Issue 5. 2017, p. 1149.
[146] Tradução minha. No original: "As currently implemented, a lack of transparency exists at all levels of predictive policing. Even something as simple as crime statistics, which in many cases are publicly available, remain rife with concerns about accuracy and completeness." Idem, p. 1165.

quais variantes leva em consideração. Dificultando, então, afirmar a "precisão, eficácia e a imparcialidade do programa"[147]. Nas palavras do autor:

> True, police can see if the system works, but police cannot see how the system works. This lack of transparency is not simply the result of new technology, but also the influence of the proprietary nature of the software. The companies involved in these real-world tests are in a multimillion-dollar race to convince police departments to adopt their particular products. The companies have financial interests and proprietary secrets to protect, and every incentive to report positive outcomes.[148]

Sobre essa problemática, Ferguson sugere que deve ser estabelecido um sistema de auditoria independente sobre coleta, análise e manutenção dos dados. Ademais, um sistema transparente deve ser capaz de mostrar como o policiamento preditivo funciona, para isso ele sugere que a publicização das métricas. Por fim, devem ser criados programas de treinamento dentro das agências de polícia, com objetivo de garantir que o trabalho de processamento dos dados esteja sendo realizado corretamente.[149]

d) Accountability

Ferguson afirma que quanto maior a transparência, maior a responsabilização. Dessa forma, accountability se refere "a uma obrigação ética dos indivíduos (neste caso, funcionários do governo) de responder pelas suas ações, possíveis falhas e irregularidades" (2017, p. 1168, tradução minha, notas omitidas). Ele também elucida de que transparência é diferente de responsabilização, mas que é através da transparência do policiamento preditivo que surge a possibilidade de responsabilizar os agentes por seus atos.

Finalmente, o autor esclarece que ausência de responsabilização deriva da própria imaturidade da tecnologia, uma vez que o policiamento preditivo abrange técnicas ainda incipientes e experimentais, concatenado ao rápido avanço tecnológico[150].

---

[147] Tradução minha. No original: "Thus, predictive policing runs into the same problems as other automated predictive technologies: the technical complexity of the design makes it nearly impossible for outsiders to determine the accuracy, effectiveness, or fairness of the program". Idem, p. 1166.
[148] Idem, p. 1166.
[149] Idem, p. 1168.
[150] Idem, p.1169-1171.

Assim, ele apresenta algumas alternativas:

> At a theoretical level, the world of data-driven police accountability is just being imagined. While beyond the scope of this article, scholars have proposed a host of data-driven tactics to hold police accountable to the community. Technologies that can track and record police activity hav been proposed. Consumer technologies that "police the police" have bee developed. Administrative procedures have been suggested. New lega oversight structures that involve both federal intervention and communit accountability have been envisioned. What these suggestions share in common is a belief that a focus on police data might provide a two-way street of accountability—reducing crime and reducing police misconduct[151]

3.4 Regulação

Sob essa lógica, considerando as questões levantadas sobre a responsabilização e o processo embrionário do policiamento preditivo, concatenado aos seus métodos e consequências apresentadas, nota-se que a necessidade da criação de uma regulamentação robusta e singular sobre o tema.

No território dos Estados Unidos, apesar do caloroso debate sobre o tema e pressão da população, até o presente momento não foi emitido nenhum regulamento concernente ao emprego do policiamento preditivo.

Já no cenário europeu, em outubro de 2021, o Parlamento Europeu adotou uma resolução relativa ao uso de inteligência artificial (IA) no âmbito do direito penal e sua aplicação pela polícia e autoridades judiciais em matéria criminal. Os deputados europeus entenderam ser necessária uma supervisão humana específica orientada para a aplicação de determinadas operações, com objetivo de "evitar a fuga de dados, violações de segurança de dados, e acesso não autorizado a dados pessoais e outras informações". Ficou assentado que as autoridades policiais e judiciais só poderão utilizar a*rtificial intelligence* em operações que garantam o princípio da privacidade e proteção de dados.[152]

---

[151] Idem, p. 1171.
[152] PINGEN, Anna. **EP Resolution on AI in Criminal Law and Policing.** Eucrim. 2021.

Além disso, a resolução também proibiu de maneira permanente o uso de análise e reconhecimento automático de características humanas em espaços públicos, demonstrando também preocupação quanto ao uso de base de dados privadas utilizadas em tecnologias de reconhecimento facial. Em suma, os deputados consentiram que o emprego dessa modalidade de tecnologia representa uma perda de autonomia e um perigo para o princípio da não discriminação e direitos fundamentais.

No Brasil, o modelo adotado para a Lei Geral de Proteção de Dados (LGPD) assemelha-se ao europeu. Ou seja, a legislação é aplicada de maneira abrangente em inúmeros âmbitos da sociedade. Em igual sentido, assim como a *General Data Protection Regulation* (GDPR) se omitiu sobre a proteção de dados na esfera criminal, a LGPD seguiu pelo mesmo caminho e não trouxe um regulamento sobre o tratamento de dados no âmbito da segurança pública.

No entanto, com a publicação da LGPD em 2018, nota-se que o debate sobre a proteção de dados em diversos níveis se expandiu. Desse modo, no ano de 2019 a Câmara dos Deputados criou uma Comissão de Juristas com intuito de elaborar um Anteprojeto de lei sobre a temática do tratamento de dados na seara penal, ou seja, no contexto da segurança pública e persecução penal.

O Anteprojeto, apelidado de LGPD penal, apresenta como fundamentação a:

> necessidade prática de que os órgãos responsáveis por atividades de segurança pública e de investigação/repressão criminais detenham segurança jurídica para exercer suas funções com maior eficiência e eficácia – como pela participação em mecanismos de cooperação internacional –, porém sempre de forma compatível com as garantias processuais e os direitos fundamentais dos titulares de dados envolvidos. Trata-se, portanto, de projeto que oferece balizas e parâmetros para operações de tratamento de dados pessoais no âmbito de atividades de segurança pública e de persecução criminal, equilibrando tanto a proteção do titular contra mau uso e abusos como acesso de autoridades a todo potencial de ferramentas e plataformas modernas para segurança pública e investigações[153]

[153] **Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal**. Câmara dos Deputados. 2020.

Até agora com 68 artigos, o Anteprojeto estabelece balizas principiológicas que irão orientar o tratamento dos dados no âmbito criminal. Alguns foram retirados da própria LGPD, enquanto outros foram introduzidos especialmente considerando o contexto penal, como por exemplo o princípio da licitude e da legalidade estrita.

O Anteprojeto também possui um capítulo inteiro destinado à regulação das tecnologias de monitoramento, apresentando um conceito e definindo diretrizes para o seu emprego pelas autoridades competentes, decretando que seu uso deve ser limitado aos casos com autorização judicial. Conforme se observa em alguns artigos, a título de exemplo:

> Art. 42. A utilização de tecnologias de monitoramento ou o tratamento de dados pessoais que representem elevado risco para direitos, liberdades e garantias dos titulares dos dados por autoridades competentes dependerá de previsão legal específica, que estabeleça garantias aos direitos dos titulares e seja precedida de relatório de impacto de vigilância.
>
> Art. 43. No âmbito de atividades de segurança pública, é vedada a utilização de tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial.

No momento atual, o projeto está na Câmara dos Deputados aguardando um parlamentar para apresenta-lo formalmente, para então, torna-se um Projeto de Lei. Neste viés, tendo em vista que o poder legislativo brasileiro se inspirou fortemente na regulamentação europeia sobre a questão da proteção de dados, é possível estimar que tão logo Brasil contará com uma Lei regulamentando a proteção de dados com aplicação direcionada para a segurança pública e investigação criminal.

4 CONCLUSÃO

No decorrer da presente pesquisa, pretendemos analisar como o desenvolvimento da internet culminou na formação da sociedade informacional, que por sua vez proporcionou a vida em rede e o surgimento de novas tecnologias capazes de exercer uma atividade de hiper vigilância, em especial o *Big Data*.

Neste panorama, as inovações tecnológicas, com múltiplos processes de aprendizagem, tornaram-se capazes de oferecer melhorias na esfera social. A introdução de novas tecnologias na seara da segurança política é um exemplo da promissora aplicação do *Big Data* no dia a dia, haja vista a sua elevada capacidade de antecipar crimes.

Contudo, insta ressaltar que antes da aplicação desse método na prática, algumas reflexões devem ser levantadas sobre a hiper vigilância exercida por meio dessas tecnologias. A associação entre vigilância, capitalismo de vigilância e o surgimento de novas tecnologias deve ser ponderada com precaução, tendo em vista a possibilidade de se infringir direitos e garantias fundamentais.

Em que pese a metodologia do policiamento preditivo basear-se na análise e processamento de dados realizados por um algoritmo, não se pode afirmar que essa operação é completamente neutra e livre de vieses. Conforme comprovado, por vezes, dados podem estar contaminados por vieses racistas, caso em que os computadores irão reproduzir essa sistemática (ciclo nocivo de feedback), culminando na punição de sujeitos pobre e negros, em sua maioria, cujo nível irá depender da modalidade policiamento empregada (*place-based, person-based* ou *suspect-based*), cada qual com sua especificidade.

Neste sentido, ressalta-se que ainda que o surgimento e desenvolvimento de tecnologias tenha como objetivo facilitar a vida do ser humano de tantas formas, inclusive dentro do direito e do âmbito das políticas públicas, é essencial ratificar que o policiamento preditivo não deve ser percebido como uma “bola de cristal” pelas agências policiais, ou seja, como a solução de todos os problemas relacionados à criminalidade e justiça penal – especialmente aqueles concernentes à previsão do crime.

À vista de todo o exposto, salienta-se que diante da reconhecida incipiência e da lacuna regulatória sobre o tema, é de extrema urgência que o debate sobre o policiamento preditivo seja difundido nos diversos âmbitos sociais, com intuito de informar os cidadãos acerca da discricionaridade empregada pelas agências policiais por meio do uso de tecnologias, bem como para pressionar as instâncias legislativas a editar normas regulatórias que direcionem e delimitem o uso do policiamento preditivo, na tentativa de reduzir a assimetria de poder entre o Estado (na forma de seus agentes policiais) e o cidadão. Garantindo, portanto, seus direitos, liberdades e garantias fundamentais.

REFERÊNCIAS

AGUIRRE, Katherine; BADRAN, Emile; MUGGAH, Robert. **Future Crime: Assessing twenty first century crime prediction.** 2019. Igarapé Institute. Disponível em: < https://igarape.org.br/inteligencia-artificial-pode-melhorar-policiamento/>. Acesso em: 18 de fev. 2022.

Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Disponível em em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf>. Acesso em 26 de fev. 2022.

AZEVEDO, Rodrigo Ghiringhelli de**. A Era da Informação: Economia, Sociedade e Cultura Vol. 1 - O Poder da Identidade.** São Paulo, Ed. Paz e Terra, 1999. Disponível em: <https://seer.ufrgs.br/sociologias/article/view/6935/4209>. Acesso em: 07 de fev. 2022.

BACHNER, Jennifer. **Predictive Policing: Preventing Crime with Data and Analytics.** IBM Center for The Business of Government. 2013. Disponível em: <https://www.businessofgovernment.org/sites/default/files/Predictive%20Policing.pdf> Acesso em: 24 de fev. 2022.

BARRICHELLO, Eugenia Maria Mariano da Rocha; MOREIRA, Elizabeth Huber**. A análise da vigilância de Foucault e sua aplicação na sociedade contemporânea: estudo de aspectos da vigilância e sua relação com as novas tecnologias de comunicação.** Intexto, Porto Alegre, UFRGS, n. 33, p. 64-75, maio/ago. 2015. Disponível em: < https://seer.ufrgs.br/index.php/intexto/article/view/50075>. Acesso em: 08 de fev. 2022.

BERTASSI, Eduardo. **Considerações sobre *softwares* de policiamento preditivo**. Boletim – Volume 3, Número 11, Dezembro/2018, São Paulo/SP. Disponível em: http://www.cest.poli.usp.br/pt/boletins/>. Acesso em: 20 de fev. 2022.

BHUIYAN, Johana . **LAPD ended predictive policing programs amid public outcry. A new effort shares many of their flaws.** 2021. THE GUARDIAN. Disponível em: <https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform>. Acesso em 20 de fev. 2022.

BORAK, Masha. **China's big data policing platform 'arbitrarily' targets Uygurs in Xinjiang based on age, family relations, HRW says**. 2020. South China Morning Post. Disponível em: <https://www.scmp.com/tech/policy/article/3113208/chinas-big-data-policing-platform-arbitrarily-targets-uygurs-xinjiang>. Acesso em: 21 de fev. 2022.

BRANDÃO, Lucas. **A Sociedade da informação aos olhos de Manuel Castells**. Comunidade Cultura e Arte. Online. Disponível em: <https://comunidadeculturaearte.com/a-sociedade-da-informacao-em-rede-aos-olhos-de-manuel-castells/>. Acesso em: 01 de fev. 2022.

BRUNO, Fernanda**. Mapas de crime: vigilância distribuída e participação na cibercultura**. E-Compós (Brasília), v. 12, p. 1-16, 2009. Disponível em: <https://www.e-compos.org.br/e-compos/article/view/409/352>. Acesso em: 12 de fev. 2022.

BRUNO, Fernanda. **Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade** / Fernanda Bruno. – Porto Alegre: Sulina, 2013. 190 p.; (Coleção Cibercultura).

BRUNO, Fernanda**. Monitoramento, classificação e controle nos dispositivos de vigilância digital.** Revista FAMECOS, v. 15, n. 36, p. 10-16, 20 nov. 2008. Disponível em: < https://revistaseletronicas.pucrs.br/ojs/index.php/revistafamecos/article/view/4410>. Acesso em: 08 de fev. 2022.

CASTELLS, Manuel. ***A galáxia da Internet:* reflexões sobre a Internet, os negócios e a sociedade.** Trad. Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar, 2003.

CHAN, Janet; BENNETT MOSES, Lyria**. Is Big Data Challenging Criminology?.** UNSW Law Research Paper No. 20-81, 2015. Disponível em: <https://ssrn.com/abstract=3742536>. Acesso em: 18 de fev. 2022.

CHAN, Janet; MOSES, Bennett. Lyria **Algorithmic prediction in policing: assumptions, evaluation, and accountability, Policing and Society**. 28:7, 806-822, 2018. Disponivel em: <https://doi.org/10.1080/10439463.2016.1253695>. Acesso em: 18 de fev. 2022.

CODED BIAS. Documentário. Direção: Shalini Kantayya. 2020. NETFLIX.

COSTA, Eduardo; REIS, Carolina**. Histórico da LGPD penal: o que foi feito até aqui e quais são os próximos passos?.** 2021. LAPIN. Disponível em: < https://lapin.org.br/2021/04/16/lgpd-penal-o-que-foi-feito-ate-aqui-e-quais-sao-os-proximos-passos/>. Acesso em 23 de fev. 2022.

COUTINHO, Thiago**. O que é Clustering? Veja como funciona essa análise!** Voitto. 2021. Disponível em: < https://www.voitto.com.br/blog/artigo/clustering>. Acesso em: 25 de fev. 2022.

CrimeRadar. Instituto Igarapé. Disponível em: <https://igarape.org.br/apps/crimeradar/>. Acesso em: 24 de fev. 2022.

DA COSTA, Camila Mattos**. "We are watching you": policiamento preditivo, controle, disciplina e vigilância.** Anais do 8º Encontro Internacional de Política Social, 15º Encontro Nacional de Política Social. v. 1 n. 1 (2020): "Questão social, violência e segurança pública:

desafios e perspectivas. Vitória, ES. 2020. Disponível em: < https://periodicos.ufes.br/einps/article/view/33282>. Acesso em: 08 de fev. 2022.

DELEUZE, Gilles. **Post-Scriptum sobre as Sociedades do Controle**. Rio de Janeiro: Ed. 34, 1992, p. 219-226.

DELOITTE. **Surveillance and Predictive Policing Through AI.** Deloitte. 2021. Disponível em: <https://www2.deloitte.com/global/en/pages/public-sector/articles/urban-future-with-a-purpose/surveillance-and-predictive-policing-through-ai.html>. Acesso em: 20 de fev. 2022.

Detecta monitora o Estado de SP com mais de três mil câmeras de vídeo. Portal do Governo de São Paulo. 2017. Disponível em: <https://www.saopaulo.sp.gov.br/spnoticias/detecta-monitora-o-estado-de-sao-paulo-com-3-mil-cameras-de-video/>. Acesso em: 21 de fev. 2022.

DIAS, G. A., & VIEIRA, A. A. N. (2015). **Big data: questões éticas e legais emergentes. Ciência Da Informação**, 42(2). Disponível em: http://revista.ibict.br/ciinf/article/view/1380>. Acesso em: 16 de fev. 2022.

FERGUSON, Andrew Guthrie. **Policing Predictive Policing.** Washington University Law Rewiew, V. 94. Issue 5. 2017. Disponível em: <https://openscholarship.wustl.edu/law_lawreview/vol94/iss5/5>. Acesso em: 23 de fev. 2022.

FERGUSON, Andrew Guthrie. **The Police Are Using Computer Algorithms to Tell If You're a Threat**. 2017. Disponível em: <https://time.com/4966125/police-departments-algorithms-chicago/>. Acesso em 21 de fev. 2022.

FERGUSON, Andrew Guthrie. **The rise of Big Data policing: Surveillance, Race, and the Future of Law Enforcement**. New York University Press, New York, 2017.

FOODY, Kathleen. **Chicago police end effort to predict gun offenders, victims.** AP News. Disponível em: <https://apnews.com/article/41f75b783d796b80815609e737211cc6>. Acesso em: 20 de fev. 2022.

Foto de astro de cinema Michael B. Jordan aparece em lista de procurados pela Polícia do Cerará. G1. 2022. Disponível em: < https://g1.globo.com/ce/ceara/noticia/2022/01/07/astro-do-cinema-michael-b-jordan-aparece-em-lista-de-procurados-pela-policia-do-ceara.ghtml>. Acesso em: 26 de fev. 2022.

FOUCAULT, Michel. **Vigiar e Punir: nascimento da prisão**; tradução de Raquel Ramalhete. 42. Ed. Petrópolis, RJ: Vozes, 2014.

GLESS, Sabine. **Policiamento preditivo: em defesa dos "verdadeiros-positivos**". Tradução de Heloisa Estellita e Miguel Lima Carneiro. Revista Direito GV, v. 16, n. 1, jan./abr. 2020. Disponível em: <https://direitosp.fgv.br/publicacoes/revista/artigo/policiamento-preditivo-defesa-verdadeiros-positivos>. Acesso em 23 de fev. 2022.

GOMES, Letícia Simões. **Policiamento preditivo, controle social e desigualdades raciais.** Anais do 43º Encontro Anual da ANPOCS, Caxambu-MG, 2019. Disponível em: < https://anpocs.com/index.php/encontros/papers/43-encontro-anual-da-anpocs/spg-6/spg32-1/12010-policiamento-preditivo-controle-social-e-desigualdades-raciais?path=43-encontro-anual-da-anpocs/spg-6/spg32-1>. Acesso em: 18 de fev. 2022.

HARDYNS, Wim, RUMMENS, Aneeleen. **Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges. European Jornal on Criminal Policy Research**, 24, 201–218. 2018. Disponível em:<https://doi.org/10.1007/s10610-017-9361-2>. Acesso em: 23 de fev. 2022.

HOLLOWAY, Thomas H. Polícia no **Rio de Janeiro: repressão e resistência numa cidade do século XIX**. Tradução de Francisco de Castro Azevedo. Rio de Janeiro: FGV, 1997.
IBM. **Big Data Analytics.** Disponível em: <https://www.ibm.com/analytics/big-data-analytics#:~:text=What%20is%20big%20data%20exactly,high%20velocity%20and%20high%20variety.>. Acesso em: 18 de fev. 2022.

Internet das Coisas: um passeio pelo futuro que já é realidade no dia a dia das pessoas. Portal do Governo Federal. 2021. Disponível em: <https://www.gov.br/mcom/pt-br/noticias/2021/marco/internet-das-coisas-um-passeio-pelo-futuro-que-ja-e-real-no-dia-a-dia-das-pessoas>. Acesso em: 18 de fev. 2022.

JUSTINO, Luiz Carlos da Costa. **Qual facção, vagabundo?**. Revista Piauí. 2020. Disponível em: < https://piaui.folha.uol.com.br/materia/qual-faccao-vagabundo/>. Acesso em: 26 de fev. 2022.

LAU, Tim. **Predictive Policing Explained: Attempts to forecast crime with algorithmic techniques could reinforce existing racial biases in the criminal justice system**. 2020. Brennan Center For Justice. Disponível em: <https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained>. Acesso em 20 de fev. 2022.

LEMES, Marcelle Martins. **Inteligência artificial, algoritmos e policiamento preditivo no poder público federal brasileiro**. Monografia. Faculdade de Direito, Universidade de Brasília. Brasília, 2019.

O'NEIL, Cathy. **Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia** / Cathy O'Neil; tradução Rafael Abraham. 1 ed. Santo André, SP; Editora Rua do Sabão, 2020.

PAULUZE, Thaiza. **Foto em delegacia faz jovem negro ser acusado 9 vezes e preso duas por roubos que não cometeu**. Folha de São Paulo. 2021. Disponível em: < https://www1.folha.uol.com.br/cotidiano/2021/01/foto-em-delegacia-faz-jovem-negro-ser-acusado-9-vezes-e-preso-duas-por-roubos-que-nao-cometeu.shtml> Acesso em: 26 de fev. 2022.

PEDRO, Rosa Maria Leite Ribeiro; SZAPIRO, Ana Maria; RHEINGANTZ, Paulo Afonso. **Dispositivos de vigilância e as cidades: tecnologia, política e vida cotidiana**. Rev. Polis Psique, Porto Alegre , v. 5, n. 3, p. 26-44, dez. 2015. Disponível em: <http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S2238-152X2015000200003&lng=pt&nrm=iso>. Acesso em: 15 de fev. 2022.

PERRY, Walter L., *et al*.,. **Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations**. Santa Monica, CA: Rand Corporation. 2013. Disponível em: < https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf>. Acesso em: 23 de fev. 2022.

PIMENTA, R. M. **Big data e controle da informação na era digital: tecnogênese de uma memória a serviço do mercado e do estado**. Tendências da Pesquisa Brasileira em Ciência da Informação, v. 6, n. 2, 2013. Disponível em: <http://hdl.handle.net/20.500.11959/brapci/119514>. Acesso em: 18 fev. 2022.

PINGEN, Anna. EP Resolution on AI in Criminal Law and Policing. Eucrim. 2021. Disponível em: <https://eucrim.eu/news/ep-resolution-on-ai-in-criminal-law-and-policing/#:~:text=On%206%20October%202021%2C%20the,248%20votes%20with%2062%20abstentions.> Acesso em: 25 de fev. 2022.

PredPol. Disponível em: <https://www.predpol.com/>. Acesso em: 24 de fev. 2022.

RATCLIFFE, Jerry. **Intelligence-led policing.** Londres/NY: Ed. Routledge, 2016.

SELBST, Andrew D. **Disparate impact in Big Data policing**. Georgia Law Review, v. 52, 2017. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2819182>. Acesso em: 23 de fev. 2022.

SELBST, Andre D., BAROCAS, Salon. **Big Data's Disparate Impact.** California Law Review 671. 2016. Disponível em: <https://ssrn.com/abstract=2477899 >. Acesso em 25 de fev. 2022.

Sigo e Status: ferramentas inéditas de tecnologia são usadas no combate a crimes e controle de sinistros. Portal do Governo do Ceará. 2021. Disponível: < https://www.ceara.gov.br/2021/12/28/sigo-e-status-ferramentas-ineditas-de-tecnologia-sao-usadas-no-combate-a-crimes-e-controle-de-sinistros/>. Acesso em: 21 de fev. 2022.

SOUSA, Reginaldo Canuto de.; MORAIS, M. S. A.. **POLÍCIA E SOCIEDADE: uma análise da história da Segurança Pública brasileira**. 2011. (Apresentação de Trabalho/Comunicação).
Wha tis the Gangs Matrix?. Anistia Internacional. 2020. Disponível em: < https://www.amnesty.org.uk/london-trident-gangs-matrix-metropolitan-police>. Acesso em 21 de fev. 2022.

STRAZZA, Pedro. Nos passos da IBM e Amazon, Microsoft passa a barrar venda de tecnologias de reconhecimento facial à polícia. 2020. B9. Disponível em: < https://www.b9.com.br/127447/nos-passos-da-ibm-e-amazon-microsoft-passa-a-barrar-venda-de-tecnologias-de-reconhecimento-facial-a-policia/>. Acesso em: 25 de fev. 2022.

YOSHIDA, Shinpachi. **Japan's police to increasingly partner up with AI to fight crime.** 2021. Disponível em: < https://www.asahi.com/ajw/articles/14421414>. Acesso em 21 de fev. 2022.

ZUBOFF, Soshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**; tradução de George Schlesinger - 1. Ed. – Rio de Janeiro, RJ: Intrínseca, 2020.

ZUBOFF, Soshana. **Big Other: Capitalismo de Vigilância e Perspectivas para uma civilização de informação**. In: Tecnopolíticas da vigilância: perspectivas da margem / organização Fernanda Bruno ... [et al.]; [tradução Heloísa Cardoso Mourão ... [et al.]]. - 1. ed. – São Paulo: Boitempo, 2018.

ANEXOS

Anexo I – Exemplos de variáveis que podem ser utilizadas pelo Policiamento Preditivo

Spatial Variables	Temppral Variables	Social Network Variables
Indicators of Areas with Potential Victims/Targets • Shopping malls • Property values • Hotels • Area demographics • Population density • Residential instability **Indicators of Escape Routes** • Highways • Bridges • Tunnels • Public transportation • Railways • Dense foliage **Indicators of Criminal Residences** • Bars and liquor stores • Adult retail stores • Fast food restaurants • Bus stops • Public health information • Areas with physical decay	• Payday schedules • Time of day • Weekend vs. weekday • Seasonal weather (e.g., hot versus cold weather) • Weather disasters • Moon phases • Traffic patterns • Sporting and entertainment events	• Kinship • Friendship • Affiliation with an organization • Financial transaction • Offender/victim

Fonte: BACHNER (2013, p. 16)

Anexo II – Tabela resumindo os métodos e tecnologias utilizadas para cada tipo de predição (de crimes, de infratores, de identidades de infratores e de vítimas)

Law Enforcement Use of Predictive Technologies: Predicting Crimes

Problem	Conventional Crime Analysis (low to moderate data demand and complexity)	Predictive Analytics (large data demand and high complexity)
Identify areas at increased risk		
Using historical crime data	Crime mapping (hot spot identification)	Advanced hot spot identification models; risk terrain analysis
Using a range of additional data (e.g., 911 calls, economics)	Basic regression models created in a spreadsheet program	Regression, classification, and clustering models
Accounting for increased risk from a recent crime	Assumption of increased risk in areas immediately surrounding a recent crime	Near-repeat modeling
Determine *when* areas will be most at risk of crime	Graphing/mapping the frequency of crimes in a given area by time/date (or specific events)	Spatiotemporal analysis methods
Identify geographic features that increase the risk of crime	Finding locations with the greatest frequency of crime incidents and drawing inferences	Risk terrain analysis

Fonte: PERRY, *et al.* (2013, p. 10)

Law Enforcement Use of Predictive Technologies: Predicting Offenders

Problem	Conventional Crime Analysis (low to moderate data demand and complexity)	Predictive Analytics (large data demand and high complexity)
Find a high risk of a violent outbreak between criminal groups	Manual review of incoming gang/ criminal intelligence reports	Near-repeat modeling (on recent intergroup violence)
Identify individuals who may become offenders:	Clinical instruments that summarize known risk factors	Regression and classification models using the risk factors
Probationers and parolees at greatest risk of reoffending		
Domestic violence cases with a high risk of injury or death		
Mental health patients at greatest risk of future criminal behavior or violence		

Fonte: PERRY, *et al.* (2013, p. 10)

Law Enforcement Use of Predictive Technologies: Predicting Perpetrator Identities

Problem	Conventional Crime Analysis (low to moderate data demand and complexity)	Predictive Analytics (large data demand and high complexity)
Identify suspects using a victim's criminal history or other partial data (e.g., plate number)	Manually reviewing criminal intelligence reports and drawing inferences	Computer-assisted queries and analysis of intelligence and other databases
Determine which crimes are part of a series (i.e., most likely committed by the same perpetrator)	Crime linking (use a table to compare the attributes of crimes known to be in a series with other crimes)	Statistical modeling to perform crime linking
Find a perpetrator's most likely anchor point	Locating areas both near and between crimes in a series	Geographic profiling tools (to statistically infer most likely points)
Find suspects using sensor information around a crime scene (GPS tracking, license plate reader)	Manual requests and review of sensor data	Computer-assisted queries and analysis of sensor databases

Fonte: PERRY, *et al.* (2013, p.11)

Law Enforcement Use of Predictive Technologies: Predicting Crime Victims

Problem	Conventional Crime Analysis (low to moderate data demand and complexity)	Predictive Analytics (large data demand and high complexity)
Identify groups likely to be victims of various types of crime (vulnerable populations)	Crime mapping (identifying crime type hot spots)	Advanced models to identify crime types by hot spot; risk terrain analysis
Identify people directly affected by at-risk locations	Manually graphing or mapping most frequent crime sites and identifying people most likely to be at these locations	Advanced crime-mapping tools to generate crime locations and identify workers, residents, and others who frequent these locations
Identify people at risk for victimization (e.g., people engaged in high-risk criminal behavior)	Review of criminal records of individuals known to be engaged in repeated criminal activity	Advanced data mining techniques used on local and other accessible crime databases to identify repeat offenders at risk
Identify people at risk of domestic violence	Manual review of domestic disturbance incidents; people involved in such incidents are, by definition, at risk	Computer-assisted database queries of multiple databases to identify domestic and other disturbances involving local residents when in other jurisdictions

Fonte: PERRY, *et al.* (2013, p. 12)

Anexo III – Tabela que correlaciona as técnicas analíticas utilizadas para prever crimes com as quatro classes apresentadas

Classes of Predictive Techniques

Analytic Category and Primary Application	Predictive Technique	Class			
		Classical	Simple	Complex	Tailored
Hot spot analysis (*where*, using crime data only)	Grid mapping	X			X
	Covering ellipses	X			
	Kernel density	X			
	Heuristics		X		X
Regression methods (*where*, using a range of data)	Linear	X	X		
	Stepwise	X		X	
	Splines			X	X
	Leading indicators	X			X
Data mining (*where*, using a range of data)	Clustering	X		X	
	Classification	X		X	
Near-repeat (*where*, over next few days, using crime data only)	Self-exciting point process			X	
	ProMap			X	
	Heuristic		X		
Spatiotemporal analysis (*when*, using crime and temporal data)	Heat maps	X	X		X
	Additive model			X	
	Seasonality	X			
Risk terrain analysis (*where*, using geography associated with risk)	Geospatial predictive analysis			X	X
	Risk terrain modeling		X		X

Fonte: PERRY, *et al.* (2013, p. 19)