O DEMÔNIO DE LAPLACE É DIGITAL E DISCRIMINADOR: O USO (QUASE) EXCLUSIVO DE BANCOS DE DADOS CRIMINAIS EM SURVEILLANCE COMO FERRAMENTA ESTIGMATIZANTE.

Marcos Rafael Lucca Machado[1]

1 INTRODUÇÃO

No presente trabalho serão abordadas as tecnologias de Big Data e Surveillance, bem como o porquê dessas tecnologias estarem sendo cada vez mais aplicadas nos mais variados campos, especialmente no da segurança pública, tendo por exemplo a implantação, cada dia maior, de programas com o DETECTA e DAS pelos estados nacionais, citando a obra de Pierre-Simon Laplace.

Por fim, dentro da teoria da prevenção secundária ou situacional abordar-se-á o policiamento preditivo local e pessoal e a implementação dos programas de surveillance, buscando verificar uma possível ocorrência de discriminação e caso ocorra, quais os motivos para tal e qual a forma de resolução da referida problemática.

2 METODOLOGIA

Para o desenvolvimento do trabalho há de se abordar os métodos utilizados para a confecção do atual projeto de pesquisa, dito isto, temos que a presente pesquisa tem propósito exploratório, com vias a verificar a incidência ou não de parâmetros discriminatórios para o indivíduo fazendo uso do método de abordagem dedutivo, tendo-se em vista que partirá de análise das teorias criminológicas bem como das tecnologias de processamento de dados, pondo ênfase na doutrina majoritária e artigos científicos para desenvolvimento da pesquisa bibliográfica.

3 DESENVOLVIMENTO

Não é algo novo ao cotidiano o uso demasiado da internet, principalmente pelas atuais gerações. Redes sociais como Facebook, Instagram e LinkedIn são companheiras

1 Acadêmico do Curso de Direito da Faculdade Metodista Centenário - FMC. Endereço eletrônico: xxxxxx

diárias de quase todos na atualidade, tecnologias de armazenamento em nuvem como o Google Drive, Onedrive da Microsoft e o Dropbox se tornaram a salvaguarda daqueles que temem por perder seus documentos se deixá-los em uma mídia física e, por fim, os próprios smartphones, computadores de bolso os quais são capazes de desempenhar quase todas as tarefas que o usuário necessite, tornando-se quase que onipresentes no cotidiano mundial.

Inexoravelmente, todos estes, geram terabytes de dados a todo o momento, nesse sentido, segundo Bernard Marr (2016, pg. 2) “Nós criamos mais dados nos últimos dois anos do que em toda a história da humanidade. Prevê-se que em 2020, 1.7 megabytes de novos dados serão criados a cada segundo, por cada ser humano no planeta”.

E como toda essa quantidade de dados é utilizada? Neste momento surge a tecnologia de big data, a qual faz uso de toda a imensidão de dados produzidos pelos mais diferentes tipos de sensores de modo a agrupar e dar sentido a estes dados, em um plano maior. Segundo Fernanda Tasinaffo, em artigo publicado em 2018 para o portal jurídico “Ciências Criminais”, “De forma geral, o Big Data permite a identificação de comportamentos e tendências, não sendo utilizado somente como uma estratégia de marketing, mas sim para a melhoria de serviços, produtos, etc.”, mas como isso de fato ocorre?

As tecnologias de Big Data são formadas a partir de um conjunto de fatores declarados, mais comumente, como os 5 V’s do big data, quais sejam, Volume, Velocidade, Variedade, Veracidade e Valor.

Sendo o Volume como a quantidade de dados à serem analisados pelos programas de big data. A Velocidade como o tempo hábil o qual o big data necessita para analisar todos os dados, devendo este ser o menor possível, a Variedade diz respeito à diversidade dos dados utilizados, ou a quantidade de bancos de dados empregados em fornecer matéria para tratamento pelas tecnologias de Big Data. O fator da Veracidade e do Valor, acrescidos posteriormente, tratam do quanto um dado ou um conjunto de dados é confiável no sentido da veracidade e o quanto cada conjunto de dados vale para a análise a que se destinam, caso este do valor.

Nesse sentido, entra em voga Pierre-Simon Laplace, astrônomo, físico e matemático francês que viveu entre 1749 e 1827, que, dentre suas diversas contribuições intelectuais, em 1814 deu origem a um ensaio que posteriormente viria a ser denominado de “O Demônio de Laplace”, no qual Laplace descreve uma entidade com intelecto tão vasto que, tendo todas as informações, seria capaz de antever o futuro, seu ensaio, muito se assemelha a atual

tecnologia de Big Data e como ela vem sendo tratada atualmente por seus utilizadores, independente da área de atuação, com efeitos nos mais diversos campos, nesse sentido colaciona-se o ensaio para que se possa auxiliar numa melhor visualização, vejamos:

> "Devemos considerar o estado presente do universo como efeito dos seus estados passados e como causa dos que se vão seguir. Suponha-se uma inteligência que pudesse conhecer todas as forças pelas quais a natureza é animada e o estado em um instante de todos os objetos - uma inteligência suficientemente grande que pudesse submeter todos esses dados à análise - ela englobaria na mesma fórmula os movimentos dos maiores corpos do universo e também dos menores átomos: nada lhe seria incerto e o futuro, assim como o passado, estaria presente ante os seus olhos" (Laplace. 1990, p. 326)

Assim, tem se inferido que a partir do uso dos programas de big data é possível traçar padrões comportamentais e preditivos, se munidos da quantidade necessária de informação.

Nesse ínterim, adentra-se ao tópico da surveillance propriamente dita, conceituada primorosamente por David Lyon como:

> (...) qualquer atenção sistemática e rotineira aos detalhes pessoais, específicos ou agregados, para um propósito definido. Esse propósito, a intenção da prática de surveillance, pode ser proteger, entender, cuidar, assegurar direitos, controlar, administrar ou influenciar indivíduos ou grupos." (lyon, 2015, p 2-3)

Interessante se faz frisar que na surveillance, não há a necessidade de haver alguém ou algum governo "do outro lado" espiando por trás das telas dos computadores. A bem da verdade, à parte os programas de Big Data, não há mais ninguém fiscalizando todos esses dados de maneira contínua, tal qual ocorre na vigilância ou na espionagem.

Segundo Rafaela Bolson Dalla Favera (2018, pg. 13), o que caracteriza e diferencia a surveillance da tradicional vigilância é o fato de que "a surveillance vai além da observação de suspeitos, criminosos ou de ambientes propícios para o cometimentos de delitos." Sendo que atualmente a surveillance se aplica a "qualquer sistema social, seja governamental, empresarial, pessoal..." de modo que, pode-se inferir que a Surveillance está presente em qualquer aspecto do cotidiano haja vista a imersão tecnológica em que toda a sociedade se encontra.

Os programas de surveillance tratados no presente trabalho, são focados no que é atualmente denominado policiamento preditivo, o qual, de acordo com a organização sem fins lucrativos "Brennan Center for Justice" se subdivide em duas facetas, o policiamento preditivo local e o policiamento preditivo pessoal.

No policiamento preditivo local tem-se a análise dos bancos de dados à disposição com o fim de se descobrir os locais e horários em que os cidadãos estão mais propensos a serem vítimas de algum ilícito (roubos, furtos e até mesmo assassinatos), os comumente conhecidos como "hot spots - pontos quentes em tradução literal" de forma a fornecer às

forças policiais informações acerca da necessidade de alocação de patrulhas, intensificação da fiscalização, bem como o contrário.

Já o policiamento preditivo pessoal baseia-se no indivíduo em si, de forma que, segundo a organização Brennan Center for Justice, “analisa bancos de dados de forma a gerar listas de indivíduos que o algoritmo julga serem propensos a cometer delitos”, nesse sentido Panucci (2015, pg. 67) assevera que “o sistema se porta de forma tão evoluída tecnologicamente que atua com a finalidade não somente de “adivinhar” um delito a ser cometido, mas também com o intuito de prever quem poderá praticar uma infração penal.”

Tal sistema vem sendo amplamente implementado nos Estados Unidos, como se vê nos primeiros 15 (quinze) minutos do documentário alemão “Pre-crime” de 2017, em que a polícia de Chicago, Estados Unidos da América, tem abordado cidadãos devido ao fato dos mesmos terem sido colocados em uma “heat list - lista quente em tradução literal” avisando-os das possíveis consequências da permanência destes na senda delitiva, mesmo que estes jamais tenham cometido ilícito algum.

Mas como isto é feito de fato? No caso do CRUSH e do DAS, ainda segundo a literatura de Predictive Policing (pg. 10-12) são quatro vetores a serem analisados, que são prever o crime de forma propriamente dita, prever quem são os criminosos, prever a identidade desses criminosos e por fim prever quem são as vítimas desses crimes.

O aspecto chave do presente trabalho insere-se na previsão de quem são os possíveis criminosos, consistente, em uma visão macro, na identificação de possíveis conflitos entre gangues, disputas de território para o comércio de drogas, dentre outros, que dá-se através de modelos de análise sobre os recentes embates e, em uma escala micro, tem-se a identificação de indivíduos que possam vir a se tornar infratores através de modelos de regressão e classificação com base em fatores de risco.

No entanto, não se tem notícia de quais são esses fatores de risco que são utilizados, sabe-se que são levados em consideração indicativos como os presentes no instituto da dosimetria da pena do Direito Penal, citando por exemplo os motivos do crime, bem como os meios empregados, ocorre que, como se vê em reportagem publicada pelo jornal The Guardian em 25 de julho de 2010 os parâmetros de classificação vem se tornando cada vez mais subjetivos, como se vê no seguinte trecho.

> O Ministério da Justiça começou a utilizar análises preditivas para calcular os dados disponíveis em seu Sistema de Avaliação de Ofensores com vistas a ajudar a prever quais prisioneiros que devem ser libertados estariam mais propensos a reincidir baseado em circunstâncias como acomodação, educação, relacionamentos, gestão

> financeira e de renda, estilo de vida, associações, uso indevido de álcool e drogas, bem-estar emocional, comportamento e atitudes. (THE GUARDIAN, 2010, s.p.)

Nesse ínterim, cabe ao devido processo científico observar como, de fato são "alimentados" diferentes programas de surveillance ao redor do globo, como o "Detecta", "Domain Awareness System - DAS", assim,tem-se que estes, funcionam de maneira ligeiramente igual, visto que o programa DETECTA é uma versão do programa DAS, ambos comercializados pela empresa Microsoft, com o intuito de ajudar na atualização e melhoria da Segurança Pública.

Em reportagem redigida por Annie Mcdonough, veiculada em 29 de abril de 2019, o jornal Novaiorquino "CIty and State" cita o "Domain Awareness System" como sendo um programa:

> "Lançado em 2012, como uma parceria entre o Departamento de Polícia de Nova York e a Microsoft, o "Domain Awareness System - DAS" é uma central de comando que o departamento possui, "é uma das maiores conexões de câmeras de monitoramento, leitores de placas de veículos, e sensores radiológicos do mundo, designados a detectar e prevenir atos terroristas, mas com grande valor nas investigações criminais".O sistema inclui câmeras de CFTV públicas em tempo real e aquelas pertencentes e operadas por entidades privadas que deram ao departamento acesso a seus servidores. Estimativas colocam o número de câmeras em funcionamento no sistema em torno de 9.000 (nove mil), porém, Daniel Schwarz, estrategista de privacidade e tecnologia da União das Liberdades Civis de Nova York, disse que o número pode ser maior. (City And State Journal, 2019, s.p.)

Não há diferenciação entre os dois programas citados, senão com relação ao aparato tecnológico que os suplementam, de modo que resta ao presente trabalho focar nos bancos de dados utilizados pelo programas listados, nesse sentido, tem-se que majoritariamente esses programas usam bancos de dados históricos, como as bases de dados de criminosos do estado ou mesmo de todo o pais, quando integrados ao sistema.

Mas no que consistem tais bancos de dados? Tem-se dentre outros o "Infocrim", que é um banco de dados criminal, parcialmente acessível ao público, onde são concentradas estatísticas de taxas de homicídios, registros de óbitos, Boletins de Ocorrência dos mais variados delitos, dentre outros ilícitos, ainda, pode ser utilizado o atual Banco Nacional de Perfis Genéticos, em que pese ainda ser um tema bastante controvertido, tem-se também a aplicação do banco de dados de presos, o "Infopen" sem contar o próprio banco de dados das polícias civis e militares, estaduais ou federais.

Nesse sentido tem-se a problemática do presente trabalho visto estes bancos de dados citados guardarem informações sobre os ditos infratores, nota-se que esses bancos de dados acabam por remeter a apenas uma parcela da população pátria, como se vê pelo divulgado

pelo portal eletrônico da Câmara dos Deputados 26 evidenciando quem são aqueles que gerarão o maior índice de alertas nos sistemas de surveillance atualmente utilizados:

> Além da precariedade do sistema carcerário, as políticas de encarceramento e aumento de pena se voltam, via de regra, contra a população negra e pobre. Entre os presos, 61,7% são pretos ou pardos. Vale lembrar que 53,63% da população brasileira têm essa característica. Os brancos, inversamente, são 37,22% dos presos, enquanto são 45,48% na população em geral. E, ainda, de acordo com o Departamento Penitenciário Nacional (Depen), em 2014, 75% dos encarcerados têm até o ensino fundamental completo, um indicador de baixa renda. (Câmarados Deputados, 2018, s.p.)

Tendo como base o exemplo acima, nota-se que bancos de dados como este, quando analisados, classificados e aplicados ao policiamento preditivo pessoal tendem a direcionar os programas de surveillance à pessoa do negro, do pobre de modo que viria a chancelar um policiamento policial (MORAIS, 2018, p. 886), focado no que parece, uma higienização social, fato que de forma alguma deve ser aceito na sociedade moderna.

4 RESULTADOS E CONCLUSÕES

Perante todo o exposto, chega-se à conclusão de que os algoritmos usados nos diversos programas de surveillance, por si só, não são causadores de grandes danos, visto sua reconhecida aplicabilidade nos mais diversos campos.

No entanto, no que tange ao policiamento preditivo pessoal, a aplicabilidade de tais tecnologias é impensável, visto que, se de um lado não se pode continuar utilizando os sistemas de surveillance com o atual nível de acesso à informação, haja vista, essa falta de informação complementar, ser elemento constitutivo de um sistema que claramente direcionam as forças de segurança em uma única direção, servindo de chancela para possíveis violências policiais focadas em segmentos da sociedade, como a população afrodescendente ou periférica.

Por outro lado, a única forma de fazer com que os algoritmos empregados nos programas de surveillance não acabem por demonstrar resultados enviesados e consequentemente estigmatizante, é alimentando esses algoritmos com todos os dados possíveis, situação esta impossível sem que haja a total violação de direitos e garantias fundamentais, como a garantia constitucional à privacidade.

REFERÊNCIAS

BAUMAN, ZYGMUNT; LYON, DAVID. Vigilância Líquida. 1. ed. São Paulo: Zahar 2013.

BRASIL. Câmara dos Deputados. **Sistema carcerário brasileiro: negros e pobres na prisão.** Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cdhm/noticias/sistema-carcerario-brasileiro-negros-e-pobres-na-prisao>. Acesso em: abril de 2020.

BRASIL. Secretaria de Segurança Pública do Estado de São Paulo. **Infocrim.** Disponível em: < http://catalogo.governoaberto.sp.gov.br/dataset/45-infocrim-informacoes-criminais >. Acessado em: 13 de fevereiro de 2020.

Crime software may help police predict violent offences. The Guardian, 25 de julho de 2010. Disponível em: <https://www.theguardian.com/uk/2010/jul/25/police-software-crime-prediction>. Acesso em: 17 de agosto de 2018.

Díaz, Ángel. **New York City Police Department Surveillance Technology**, BRENNAN CENTER FOR JUSTICE. Nova York, 4 de outubro de 2019.

FAVERA, Rafaela Bolson Dalla; **Surveillance e Direitos Humanos.** 1. ed. [S. l.]: Editora Juris, 2018. 13 p.

GIOVANELLA, THIAGO. **Os 5 Vs do Big Data.** 2017. Disponível em: <http://www.tgiovanella.com.br/2017/05/os-5-vs-do-big-data/>. Acesso em: 9 set. 2019.

How New York city is watching you. City and State, Nova York, 29 de abril de 2019. Disponível em: < https://www.cityandstateny.com/articles/policy/technology/how-new-york-city-is-watching-you.html >. Acesso em: 09 de set. de 2019.

LAPLACE, P. S. M. D. **Essai philosophique sur les probabilités.** 6. ed. Paris: Bachelier, 1840. 274 p.

MARR, BERNARD. **Big Data in Practice.** 1. ed. United Kingdon: Wiley, 2012.

MOMBELLI, Elisa. **Uso do big data na segurança pública é bem-vindo.** Consultor Jurídico, 02, julho de 2014. Disponível em: < https://www.conjur.com.br/2014-jul-01/elisa-mombelli-uso-big-data-seguranca-publica-bem-vindo >. Acesso em: 20 de março de 2020.

MORAIS, José luis bolzan de. **O Estado de Direito "confrontado" pela "revolução da internet"!** Revista Eletrônica do Curso de Direito da UFSM, v. 13, n. 3, p. 876-903, 2018.

PERRY, Walter L. et al. **Predictive Policing: The Rule of Crime Forecasting in Law Enforcement Operation.** 1 ed. Rand Corporation, 2013.

TASSINAFO, FERNANDA. **A utilização do Big Data para prevenção de crimes.** 2018. Disponível em: <https://canalcienciascriminais.com.br/big-data-prevencao-crimes/>. Acesso em: 9 set. 2019.