SEGURANÇA PREDITIVA? A INCORPORAÇÃO DE TÉCNICAS DE MINERAÇÃO DE DADOS E PERFILIZAÇÃO EM CONFLITOS INTERNACIONAIS COM DRONES PELOS EUA E EM PRÁTICAS DE VIGILÂNCIA PELA POLICIA MILITAR DO ESTADO DE SÃO PAULO

Resumo: Com o desenvolvimento de novas tecnologias de comunicação, processamento e gerenciamento de dados, cada vez mais o acesso privilegiado à informação torna-se central para as estratégias de segurança pública e internacional. Um exemplo disso são os Drones, cuja capacidade de coleta massiva de dados, e associação à técnicas de perfilização geográfica, tem autorizado assassinatos extrajudiciais no exterior. De modo semelhante, o governo do estado de São Paulo tem implementado um sistema de vigilância que potencialmente permite prisões e autuações antecipativas. Nosso objetivo apresentar a ascensão desse novo tipo de paradigma militar e de segurança pública, que provisoriamente podemos definir como "segurança preditiva". Debateremos algumas hipóteses de problematização desse dispositivo forma de governamentalidade, à luz dos Estudos de Vigilância, dos Estudos sociais da Ciência e da Tecnologia e em certa medida da Sociologia da Punição. Assim, a tônica geral da nossa problematização é que esse dispositivo de "segurança" se orienta a legitimar práticas excessivas em ambientes de guerra, e em contextos urbanos da guerra global ao terror. No entanto, como concluiremos, um estudo mais detalhado exigirá a compreensão de como se estruturam os algoritmos que sustentam esse dispositivo e práticas.

Palavras Chave: big data, vigilância, drones, detecta, segurança preditiva

ALCIDES EDUARDO DOS REIS PERON[^ ^](#SDFOOTNOTE1SYM)

Seguridad Predictiva? La incorporacion tecnicas de Minería de datos y Perfilizacion em Conflictos Internacionales com Drones por los EE.UU. y em practicas de Vigilancia por la Policia Militar de São Paulo

Resumen: Con el desarrollo de nuevas tecnologías de la comunicación, procesamiento y gestión de datos, cada vez más el acceso privilegiado a la información es central para las estrategias de seguridad pública e internacionales. Un ejemplo son los aviones no tripulados (drones), cuya capacidad de recogida de datos en masa, asociado a técnicas de perfilizacion geográfica, ha autorizado a las ejecuciones extrajudiciales. Del mismo modo, el gobierno del estado de Sao Paulo se ha implementado un sistema de vigilancia que potencialmente permite a las detenciones y multas a futuro, el Detecta. Nuestro objetivo es presentar el surgimiento de este nuevo tipo de paradigma de seguridad militar y pública, al cual podemos definir provisionalmente como "seguridad predictiva." Vamos a discutir algunas hipótesis que cuestionan esta forma el dispositivo de gubernamentalidad, a la luz de los estudios de vigilancia, estudios sociales de la ciencia y la tecnología, y en cierta medida, la sociología del castigo. De este modo, el tono general de nuestra problemática es que este dispositivo "seguridad" está orientada a legitimar prácticas excesivas en los entornos de guerra, y los contextos urbanos de la guerra global contra el terrorismo. Sin embargo, como vamos concluir, un estudio más detallado requerirá una comprensión de cómo se estructuran los algoritmos que apoyan este dispositivo y prácticas.

Palabras Clave: big data, vigilancia, drones, detecta, seguridad preditiva.

Predictive Security? The incorporation of Data Minning and Profiling techniques in International Conflicts with Drones by the U.S. and Surveillance Practices by São Paulo's Military Police

Abstract: From the development of new communication, process and data management Technologies, the privileged access to information increasingly becomes central to the public and international security strategies. One example is the Drone warfare, whose massive data collection, and association to profiling techniques, is "legitimizing" extrajudicial killings overseas. Similarly, the government of São Paulo is implementing a surveillance system that potentially allows anticipative imprisonments. Our objective then is to present the ascension on this new military and public security paradigm, which provisionally we could name as "Predictive security". We will debate, then, some hypothesis of this dispositive and new form of governmentality through the Surveillance Studies, Social Studies of Science and Technology and in certain way, Sociology of the Punishment. The general tone of our problematics is the idea that this dispositive of security seeks to legitimize excessive practices in war and urban global war on terrorism environments. However, as we will conclude, a more detailed study will demand th comprehension of the development and controversies around the algorithms that sustains this practices.

Key-Words: big data, surveillance, drones, detecta, predictive security

INTRODUÇÃO

Com o desenvolvimento de novas tecnologias de comunicação, processamento e gerenciamento de dados, cada vez mais o acesso privilegiado à informação torna-se central para as estratégias de segurança pública e internacional. Um exemplo disso é o emprego de Drones Militares armados, como peça chave para a estratégia estadunidense de combate ao terrorismo no Oriente Médio. De modo semelhante, o governo do estado de São Paulo contratou da empresa*Microsoft* um sistema de vigilância que permite o processamento de imagens através das câmeras de monitoramento, recolhendo dados e informações que podem substanciar prisões e autuações antes mesmo que se consubstancie um crime.

Em ambos os casos, observamos a constituição de um novo conceito, que provisoriamente podemos nomear como de "Segurança Preditiva", apoiada em dispositivos de vigilância associados à técnicas de automatização do processamento de dados. Assim, nosso objetivo aqui é apresentar

uma proposta de trabalho que explore a identidade entre uma ascendente prática militar e de segurança pública. Buscaremos, assim, apresentar algumas hipóteses de problematização à luz dos Estudos de Vigilância, dos Estudos sociais da Ciência e da Tecnologia, e em certa medida da Sociologia da Punição. A tônica geral da nossa problematização é que essa forma de "segurança" se orienta a legitimar práticas excessivas em ambientes de guerra, e em contextos urbanos de guerra ao terror, no entanto, como observaremos, paulatinamente elas estariam fundamentando no campo da segurança pública, algo que suscitará algumas hipóteses.

DRONES, *TOTAL INFORMATIONAL AWARENES*, E ASSASSINATOS EXTRAJUDICIAIS

Desde 2004 a Força Aérea estadunidense (USAF) e a Agência Central de Inteligência (CIA) vem conduzindo operações de Assassinatos Extrajudiciais com Drones armados, como ações de contra insurgência em países como Paquistão, Iêmen e Somália. Por si só, esses atos já se caracterizam ilegais, uma vez que atentam contra a soberania de países não implicados formalmente em nenhum conflito, atuando contra pessoas não diretamente engajadas em conflitos armados, como explica Alston (2010).

Priorizando esse tipo de tecnologia, o*DoD* então orquestra a transição dos antigos sistemas de comando e controle em sistemas de Comando, Controle, Computação, Comunicação, Informação, Vigilância e Reconhecimento, denominado C4IRS. Os conflitos agora se centrariam na obtenção de informações e reconhecimento das posições inimigas, através de uma sorte de instrumentos conectados em rede – tudo isso realizado à distância, denominando-se como *Network Centric Warfare* (Cebrowsky, 2000) – permitindo a partir de várias unidades agindo em rede, ações cirúrgicas e rápidas – base da doutrina de *Shock and Awe* (rapidez e reconhecimento) (Albert e Hayes, 2003).

Nesse contexto, a RAM ao introduzir as TICs como uma nova base tecnológica dos armamentos dá a possibilidade para o surgimento, por um lado, de uma nova doutrina de operações militares na qual o acesso a informação passa ser a determinante para o seu sucesso, mas por outro lado, também cria uma nova dimensão de atuação das Forças Armadas em que o controle a disseminação e a destruição da informação tornam-se a dinâmica própria das operações. Emerge então uma nova modalidade de conflito, a "guerra informacional". Bellamy (2001:61) faz uso de uma definição ampla para compreender a Guerra Centrada em Rede: dividida em três partes distintas, a guerra informacional é uma "administração da percepção", quando a informação é a mensagem; ela é destruição de sistemas, quando a informação é um meio; e por fim, ela é exploração da informação, quando esta é o alvo.

Assim, em um determinado momento, como expõe Bellamy (2001), caracterizado por uma Guerra de Comando e Controle (C^2 Warfare) a intenção é o desenvolvimento de operações militares no contexto de C4ISR, capazes de destruir a infra-estrutura de C^2 do inimigo por meio de equipamentos eletrônicos, garantindo a primazia no combate. Por sua vez a*Software Warfare* seria um combate travado no campo de fluxo de dados computacionais com o objetivo de atingir

as capacidades inimigas, neutralizando-as e assim alcançando uma supremacia no combate físico.

A informação, então, torna-se o meio e o fim de grande parte das operações militares, seja pelo seu controle, seja pela posse de informações privilegiadas para elaborar o reconhecimento do território, antevendo-se aos ataques inimigos, e tornando mais precisos.

Sabemos que os Assassinatos Extrajudiciais realizados com Drones se organizam de duas formas. Em primeiro lugar, através de Assassinatos Seletivos (*Targeted Killing*), em que as operações estariam orientadas para eliminar alvos muito específicos, e fariam uso de oficiais de inteligência em campo, bem como de dados coletados a partir da triagem de imagens realizadas pelos Drones, obtidos com rastreamento de celulares, dentre outros. Nesse caso, sabe-se o nome e a localização dos sujeitos, e como descreve O'Connel (2009) existem advogados e especialistas em direito internacional e de guerra presentes durante a autorização dos ataques, que julgam se as provas existentes seriam suficientes para realizar ataques que culminem na eliminação de suspeitos.

Um outro método seria o de Assassinatos por Assinatura de Calor (*Signature Killing*). Nesse caso, como expõe Chamayou (2013), a visualização de "alvos" através das câmeras infravermelho, identificando os corpos enquanto sinais de calor, formam arquivos de imagens, que cruzadas com informações sobre geolocalização, dados telefônicos a partir do rastreamento de "chips", constroem o que é chamado de padrões de vida, ou de comportamento. Essas são informações que podem ser cruzadas para compor os padrões considerados "suspeitos", e com isso legitimar o assassinato de alvos à distância. Segundo Chamayou (2013: 72-73), a análise dos padrões de vida ocorre a partir de uma fusão entre a análise de conexões e geoespacial, uma cartografia conjunta do social, em um local e num espaço temporal. Nesse sentido, assim que um alvo potencial é designado, se inicia uma investigação sobre ele. Recolhem-se dados telefônicos e de outras ordens, que passam a ser associados ao o movimento registrado pela leitura de calor das câmeras do *VANT*. Criam-se, assim, pontos nodulares destinados a construir um diagrama que compõe um arquivo sobre o seu padrão de vida e sua estrutura de relacionamentos.

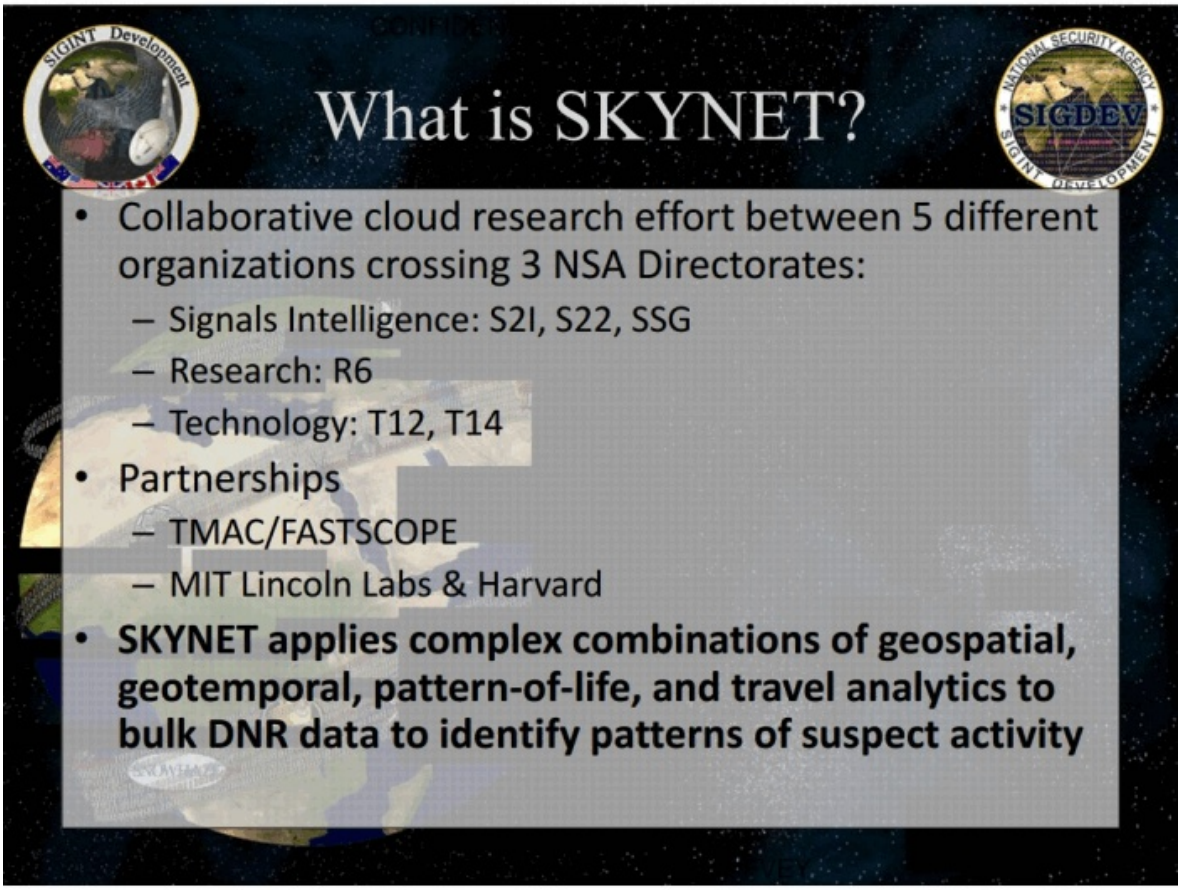
Nesse mesmo período, a*National Security Agency* (NSA), passa a incorporar novos dispositivos de vigilância massiva de dados, tornando-se um dispositivo fundamental de inteligência para a realização de operações militares "encobertas". A atividade central da NSA seria coletar informações de indivíduos de forma massiva, possibilitando aos líderes militares, políticos, e tomadores de decisão, o reconhecimento dos potenciais inimigos e ameaças, suas ações e planos, de forma a tomarem decisões preventivas adequadas (NSA, 2016).

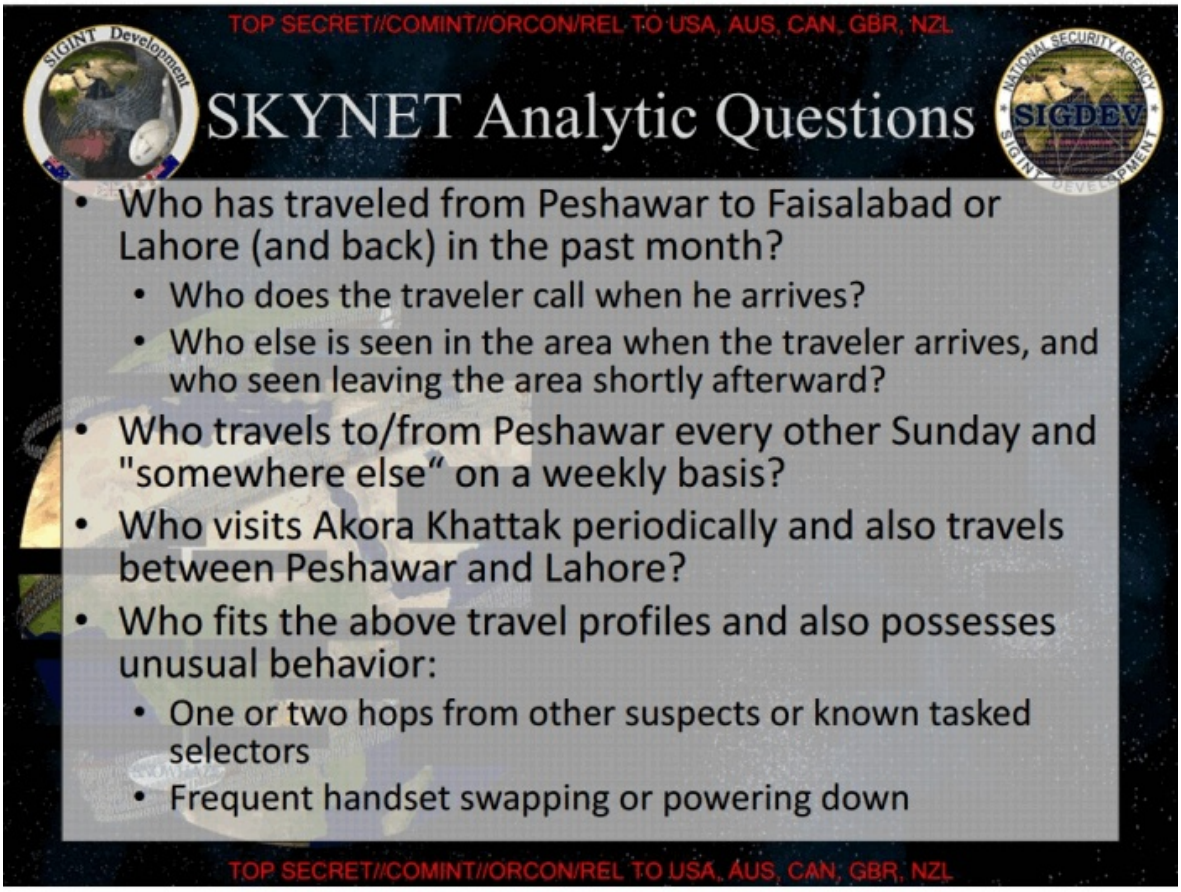
É nesse espírito que se desenvolve o*Total Information Awarness Program* (Mack, Beeb & Wenzel, 2002), pela DARPA, que visa a construção de arquitetura, processos e tecnologias com vias a permitir a coleta e triagem massiva de informações e dados. Não tarda para que militares a agentes de inteligência desenvolvam técnicas e conceitos que permitam o uso desses dados para a operacionalização de suas missões. Com a coleta massiva de dados, e triagem algorítmica, um exemplo pode ser o conceito operacional que Força Aérea dos EUA desenvolve a partir de então, é o *Predictive Battlespace Awereness* , que pode ser entendido como "(...) o conhecimento

do ambiente operacional que permite o comandante e seu pessoal antecipar corretamente condições futuras, acessar condições em mudança, estabelecer prioridades, e explorar oportunidades emergentes enquanto mitiga o impacto de ações adversárias não esperadas" (Piccerillo & Brumaugh, 2004)

Em um recente "vazamento" de informações sobre como se operam esses Assassinatos por Assinatura, a agência de jornalismo investigativo*The Intercept* (2015) revelou que um sistema desenvolvido para o cruzamento de dados obtidos pelos Drones, *Skynet* , é capaz de angariar dados para a construção de padrões de vida a partir de dados produzidos por redes sociais. Essas informações seriam cruzadas tanto com as imagens, como com os padrões de movimento dos alvos, construindo assim padrões aparentemente suspeitos. As imagens abaixo, extraída de documentos oficiais da Agência de Segurança Nacional (*NSA*), revelam brevemente as intenções desse sistema, e as dinâmicas mapeadas.

FIGURA 1:
Slides explicativos dos métodos do sistema Skynet





Fonte: The Intercept (2015)

Assim, os Drones que foram desenvolvidos exclusivamente para vigilância e monitoramento para a USAF e CIA, no momento que são armados, se integram a uma extensa cadeia de comunicação, constituída por pessoas, instrumentos e instituições. Nesse âmbito, são desenvolvidos sistemas capazes de coletar e cruzar dados massivos sobre o comportamento das pessoas observadas. A despeito do caráter panóptico dos drones, monitorando de forma constante e persistente regiões do globo, disciplinando o corpo social a funcionar de maneira ordenada e útil, a adoção de técnicas de mineração de dados (*data minning*) e perfilização (*profiling*), permitem uma nova forma de visualizar os alvos, não apenas mirando o indivíduo, mas como atesta Kanashiro (2016), olha para o fluxo de dados e metadados produzidos por eles. De certa forma, esses metadados, aliados a uma forma de visualização, monitoramento e eliminação, têm potencial de autorizar e manifestar ações preditivas, assumindo o status de evidências de comportamentos suspeitos, até mesmo culpados.

Não seria exagero afirmar, assim, que se inaugura uma prática de segurança, que tem em um saber estatístico-punitivo, o principal pilar para fundamentar ataques e Assassinatos Extrajudiciais. A essa prática, fundamentada por uma sorte de conceitos operacionais maturados da RAM,

podemos denominar como "dispositivo de segurança preditiva", o qual se caracterizaria por um conjunto heterogêneo de práticas, instrumentos e saberes orientados a detectar comportamentos discrepantes e "nocivos", e perfilá-los de forma a atualizar o risco potencial do sujeito, possivelmente autorizando (ou ao menos legitimando) sanções preemptivas. O elemento central dessa prática, ao nosso ver, está na relação temporal e estruturante com as ideias de prevenção e preempção. Enquanto no primeiro caso, o ato se dá como uma precaução diante de uma hipótese de ação de uma outra parte, o segundo se organiza em torno de provas, evidencias "sólidas" que sustentem uma ação antecipatória – legal e prevista na normativa internacional, em alguns casos. No entanto, em ambas as situações, a produção de justificativas para a realização dos atos se organiza a partir do olhar sobre as experiências passadas, evidencias estáticas e opacas, como discursos, movimentos táticos e políticos: O olhar sobre o passado se torna a justificativa presente para os ataques. De modo distinto, o saber estatístico-punitivo olha para o passado e para presente para a conformação das hipóteses de futuro, transformando riscos hipotéticos em "sólidas" evidencias que sustentam os ataques antecipativos: É o olhar assertivo para um futuro certo que condiciona as ações presentes.

Não à toa, o saber preditivo está em perfeita consonância com as ações supostamente "preemptivas" estadunidenses no imediato pós 11 de setembro, contra Estados e organizações inimigas, ampliando descomunalmente o seu escopo de projeção de poder.

O DETECA E O DISPOSITIVO DE POLICIAMENTO PREDITIVO

Em um outro contexto, em setembro de 2014, aparentemente apartado da dimensão internacional e de guerra, o governador de São Paulo, Geraldo Alkmin, anuncia uma parceria com a*Microsoft* e a cidade de Nova Iorque para contratação de um sistema de monitoramento e análise de dados para auxílio das operações policiais do Estado de São Paulo. Denominado Detecta, o sistema é uma adaptação do *Domain Awareness System,* da polícia de Nova Iorque, profundamente imerso em um discurso de emprego de alta tecnologia para combate aos problemas de segurança pública da cidade e do estado (Geraldo, 2014). Segundo a PRODESP, o Detecta seria um sistema baseado em um "complexo algoritmo de processamento e em regras de negócios parametrizáveis" que permitiria "uma correlação das bases de dados com as informações dos sensores e assim emitir alertas" (Beraldo, 2015: 34).

Via de regra, o Detecta possui tanto as funcionalidades de sistemas de leitura imagética algorítimica que permitem a produção de dois tipos de alertas, os "Inteligentes" e os "Analíticos", bem como a funcionalidade coleta massiva de dados, construindo bases de dados de geo-referenciamento para o policiamento preditivo. Aqui, nos interessam os "Alertas analíticos", os quais baseiam-se em perfis de comportamentos "suspeitos" desenvolvidos pela Polícia Militar em parceria com a PRODESP, para o reconhecimento de condutas através das câmeras. De acordo com a Secretaria de Segurança Pública, a intenção é ampliar o leque de perfis compreendidos como suspeitos para além de atividades relacionadas ao transito, cruzando informações de bancos de dados de outras instituições, como o Fotocrim (Secretaria, 2015a).

No que tange a segunda funcionalidade desse sistema, observa-se a sua capacidade de produzir estatísticas e modelos sobre ocorrências e grupos de indivíduos, a partir de sistemas de mineração de dados e perfilização geográfica (*geo-profiling*). Nesse sentido, a intenção do governo paulista é que o sistema passe a munir a PM paulista com dados e informações para o estímulo do que entendem por "Consciência Situacional". Ao cruzar os dados do Registro Digital de Ocorrência (RDO), Detram, Chamados 190 e Fotocrim, a ideia é que isso permita a construção de estatísticas sobre ocorrências, bem como a perfilização de condutas criminosas em regiões específicas capaz de subsidiar uma prática de policiamento preditivo na PM paulista (Secretaria 2015b).

Essa é uma prerrogativa inédita para as práticas policiais, antecipar as autuações e prisões com base em mineração de dados e perfilização de condutas criminosas, legitimando ações preditivas de contenção de manifestações, e de prisão de "perfis" considerados perigosos para determinadas regiões. Ao depositar fé em um sistema que reproduz perfis de periculosidade, travestindo-o enquanto automatizado, ainda que haja um esperado aumento da eficiência policial, abre-se margem para a desenho de uma espécie de saber-poder, que subsidia e garante maior capacidade de controle e gestão sobre grandes fluxos, e fluxos específicos de indivíduos nos ambientes urbanos.

Todavia, conforme um relatório desenvolvido pelo Tribunal de Contas do Estado (TCE), que almejava verificar se de fato o Detecta cumpria a sua função (automatizar o processo de vídeo monitoramento dos espaços públicos, se garante a confiabilidade e a segurança das informações, resultados nas atividades de planejamento, prevenção e investigação policial) conclui que, todas as capacidades previstas, alertas, sistemas estatísticos, não são e nem estão operacionais, por inúmeros motivos (Beraldo, 2015). Mais adiante, exprime também que, devido a uma série de problemas de ordem técnica, com o Detecta "corre-se o risco de que as informações disponibilizadas no banco de dados possam ser utilizadas para outros fins que não o de segurança pública" (Beraldo, 2015: 74). Ou seja, a rigor, o Detecta mantém apenas o sistema de coleta de*feeds* , e seu compartilhamento destes com o *DAS* .

Desse modo, é fundamental que compreendamos que os discursos sobre policiamento e segurança preditiva, os algorítimos para a triagem dos dados, que embasam o Detecta, são desenvolvidos e gestados em países como os EUA e Inglaterra, tanto por autoridades policiais, como por empresas como*Microsoft* e *Cisco* , que provem essa capacidade. Sobre isso, o chefe do Departamento de Polícia de Lincoln, Nebraska, Tom Casady, em sua reflexão sobre sistemas informacionais, afirma que ao se associarem uma série de informações que vão desde histórico de crimes, idade, raça, status de imigração, habitação, renda, à sistemas mapas, há uma melhor e mais clara visualização da relação entre pobreza, renda e criminalidade, antes legada unicamente à uma "literatura criminal" (Casady, 2011).

Conforme os departamentos de polícia adotam sistemas de gestão massiva de dados e registros, a sua capacidade de agrupar e analisar dados sobre crime e desordem se amplia muito. Ainda que esse movimento possa ser entendido como uma mera forma de "mapeamento", muito comum em investigações criminais ao longo dos últimos anos, a sua particularidade reside na

possibilidade de construir modelos estatísticos e de geo-referenciamento, a partir de análise massiva de dados públicos, e seu cruzamento com plataformas de dados criminais, capazes de classificar grupos de indivíduos, e apontar padrões de criminalidade futura. Nesse sentido, essa nova forma de olhar e gerir a criminalidade ganha uma nova notação, Policiamento Preditivo (*predictive policing*), cuja definição tem sido objeto de debate entre departamentos de polícia, e de empresas transnacionais de gestão de infra-estruturas de informação e comunicação.

Ainda que o conceito de policiamento preditivo esteja em disputa, é possível que identifiquemos várias nuances nas definições já apresentadas. Os departamentos de polícia estadunidenses, em parceria com o*National Institute of Justice* compreenderam de forma ampla esse procedimento, o definindo como uma "estratégica policial que usa a coleta de dados de diferentes fontes, e análises avançadas, usando os resultados para informar-se, antecipar-se, prever e responder de maneira mais efetiva ao crime futuro" (Pearsall, 2010). Da mesma forma, a *RAND Corporation* define a prática como: "Aplicação de técnicas analíticas para identificar potenciais alvos para a intervenção policial e prevenção de crimes, ou solução de crimes passados a partir de predições estatísticas" (Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Holywood, J. S., 2013).

Na esteira dessas definições, empresas que provêm os serviços de*cloud based analysis* , como a *Microsoft* , integrando infra-estruturas de monitoramento à sistemas de mineração algorítimica de dados, e perfilização geográfica a partir de plataformas de dados criminais, também buscam imprimir a uma visão positiva dessa nova forma de policiamento. Responsável pelo desenvolvimento do *Domain Awarenes System* (*DAS*) para cidade de Nova Iorque, a *Microsoft* defende que o policiamento preditivo deriva de um novo arranjo possibilitado pelas novas tecnologias de análise e armazenamento em nuvem, considerando, evidentemente, a perspectiva de redução de custos em conjunto com uma maior eficiência das ações policiais no "combate ao crime" (Arthur, 2015). De maneira objetiva, a *Microsoft* explica que, os sistemas de computação em nuvem conectariam todos os departamentos de inteligência policial, para a construção de padrões históricos de criminalidade, e com isso projetar tendências futuras de criminalidade por região (Bhandari, 2016).

A rigor, as plataformas computacionais que substanciam esse tipo de prática, se caracterizam por sistemas complexos de coleta massiva de dados, orientados por algorítimos de busca, classificação, seleção, agrupamento e cruzamento de informações. Em geral o processo pode ser descrito em duas fases: a de mineração e cruzamento de dados (*data minning*), e de perfilização geográfica (*geographical profilling*). Em um primeiro momento são triadas informações geralmente públicas, como números de identidade, imagens e fotos, placas de carro, residência, formação, cor, idade, dentre outros, e a depender do sistema e do contexto, invocam-se dados privados, como dados telefônicos, bancários, ficha criminal, etc. Os sistemas são abastecidos, ainda, com informações e dados criminais geo-referenciados, permitindo a criação dos chamados mapas de densidade, que permitem aos agentes de segurança visualizarem incidentes ocorridos no passado, bem como fluxos e espaços de circulação dos cidadãos e "criminosos". No momento em que os algorítimos desenvolvidos para essa prática estabelecem a classificação desses dados

e o "nexo" possível entre eles, é possível o início de um processo de análise geoespacial que "(...) caracteriza as localizações associadas com os eventos passados e cria um modelo que incorpora fatores ambientais associados estatisticamente com incidentes passados (...) que pode ser usado para identificar localizações similares aonde incidentes futuros podem ocorrer" (McCue, 2011: 04).

É nesse último momento que se verifica a prática de perfilização geográfica, que com base em algoritmos, permite priorizar indivíduos em longas listas de suspeitos. Nessa técnica, modelos computacionais articulados por uma série de algoritmos que analisam uma determinada localização geográfica, padrões de comportamento de "delinquentes", ou grupos de pessoas, considerando informações como data, horário, características estéticas, de comportamento, para verificar a probabilidade voltar a agir ou circular no local.

Em países marcados tanto por atentados terroristas, bem como atos violentos cometidos por indivíduos portando armas pesadas, as formas de policiamento preditivo caem como uma luva para os agentes de segurança pública. O*DAS* , nesse sentido, é declaradamente um dispositivo de contraterrorismo, elaborado mediante a um discurso emergencial, orienta-se a prever e deter a preparação e ataques terroristas, sendo sumariamente aproveitado para conter manifestações, e crimes menores (NYPD, 2009:02). Desse modo, gestado em comum por empresas de telecomunicações e departamentos policiais estadunidenses, e alinhado a uma promessa de maior eficiência em prover segurança à redução de custos oriunda de parcerias público-privadas, o *DAS* e as técnicas de policiamento preditivo, curiosamente, encontram ressonância nos discursos que conformam os sistemas de gestão e controle da segurança pública no Brasil, o que, *a priori* , nos leva a elaborar algumas problematizações.

Nesse sentido, o Detecta, bem como o*DAS* e o *Pred Pol,* tal como os dispositivos preconizados por Foucault (1996), se organizam a partir de um conjunto heterogêneo de saberes e elementos discursivos e materiais, orientados para responder a uma urgência, nesse caso, a necessidade de punições antecipativas. Assim, o saber que nos referimos aqui, que confere autoridade a essa prática é o que se manifesta na perfilização de condutas normais ou anormais, desejáveis ou indesejáveis, a partir de critérios quantitativos, permitindo a classificação de grandes massas de indivíduos como suspeitos, ou propensos ao crime a partir de indícios estatísticos. De certa forma, esses saberes e dispositivos sustentam uma forma de governamentalidade, no mesmo sentido proposto por Foucault (2008), que tem na possibilidade de punição antecipatória – similar a dos ataques preemptivos – uma nova forma de gerir a segurança pública.

A esse respeito, a partir do discurso proclamado por instituições militares estadunidenses, pelas empresas de telecomunicações, departamentos de polícia e segurança pública, é possível apresentar uma problematização acerca do modo como as "predições" assumem o estatuto de verdade futura no momento de elaboração das operações, transformando aquilo que seria um risco potencial, em um risco real, diante das "abordagens preditivas" (Bruno, 2016). Em outras palavras, diante desse estatuto de verdade que as estatísticas preditivas assumem, definindo

níveis de periculosidade em condutas desviantes, como Lianos e Gouglas (2000) irão sustentar, é o risco que se configura como o registro cultural central das práticas punitivas, e não o crime.

Em uma perspectiva mais centrada nos algorítmos, que aprofunda a problematização acima, Josh Scannel (2016: 03), discorrendo sobre o*DAS* irá afirmar que "os softwares de predição de crimes, não tem nada a ver com prevenção de crime". Ao invés disso, os algoritmos que baseiam esses sistemas apenas "matematizam" uma estética policial discriminatória, organizando a cidade em torno de percepções irreais, ou uma "reorganização da ontologia na computação" (Scannel, 2016: 03). O algoritmo seria, portanto, um objeto político, uma junção de forças que se imprimem no social como uma espécie de "governança algorítmica". O autor defende que esses algorítimos preditivos, ao pretenderem reduzir a "bagunça do contexto social em uma computação enxuta" (Scannel, 2016: 08) em uma decisão estética e simplista, acabam por eliminar o social da sociabilidade. Como resultado, produzem uma "fantasia refinada da cidade", a *smart city* , que mascara um Estado carcerário, cuja agência humana na tomada de decisão sobre a "culpabilidade" dos sujeitos, é suprimida por uma governança algorítimica.

Autores como Keith Guzik (2009), Sara Degli Espositi (2014) e José van Dijck (2014), ao contentrarem-se naquilo que chamam Datavigilância, discutem o papel das novas técnicas de processamento de dados em nuvem, como mineração de dados (*Data Minning*) e perfilização algorítmica (*Profiling*)[1], enquanto intensificadores do processo de controle social e discriminação. Por sua vez, Henrique Parra (2016), Fernanda Bruno (2016), Marta Kanashiro (2016), dentre outros, tem buscado, discutir o a relação entre instrumentos de "Big Data" no incremento e intensificação dos sistemas contemporâneos de vigilância e governamentalidade no Brasil. Inaugura-se uma prática, que tem na técnica de processamento algorítimico, o principal pilar para erigir uma nova forma de governamentalidade.

Sobre isso, Antoinette Rouvroy e Thomas Berns (2010), descrevem essas técnicas como um novo saber-poder estatístico, que originados em um fenômeno contemporâneo de registros sistemáticos e "digitalização da vida própria", e apoiadas em dispositivos de detecção, classificação e avaliação antecipatória dos comportamentos humanos, consagram uma forma específica de governamentalidade algorítmica. Ela se caracteriza pela capacidade em interpretar os dados registrados, a partir de critérios de normalidade ou anormalidade, interesse ou indiferença, prevendo, orientando e prevenindo certos tipos de comportamentos. Em geral, seria "um poder que reside nos algoritmos de correlação estatística, articulado para um "controle" ou mais ainda, uma antecipação de um novo tipo" (Rouvroy et Berns, 2010: 88-89).

Portanto, a segurança preditiva, em contexto de gestão de conflitos e da segurança pública em ambientes urbanos, possui uma profunda identidade com os processos que caracterizariam uma "governamentalidade algorítmica", o que lança luzes para um debate mais aprofundado, seja a partir de uma aproximação com a Sociologia da Punição, ou dos Estudos Críticos de segurança Internacional.

CONCLUSÕES PRELIMINARES

Ao observarmos práticas tão semelhantes, em contextos tão distintos, organizadas pelos mesmos pilares, torna-se elementar traçar não apenas um conceito que as exprima em um bojo comum, mas fundamentalmente, um paralelo histórico entre elas. Nesse sentido, o trabalho de Stephen Graham (2006) nos esclarece que diversas tecnologias, projetos, técnicas e doutrinas desenvolvidas no âmbito da RAM tinham por objetivo não apenas uma maior eficiência e capacidade de camuflagem dos armamentos e das operações militares, mas em grande medida, também, o desenvolvimento de dispositivos de vigilância, rastreamento e monitoramento para a gestão da segurança pública. Esses dispositivos e técnicas seriam fundamentais para o projeto estadunidense de "império global" (Graham, 2006: 263), organizando as operações militares também em ambientes urbanos complexos, sejam nos grandes centros urbanos dos países centrais, ou periféricos.

No entanto, ainda que as novas dimensões estadunidenses do militarismo respondam pelo ímpeto de aplicação dessas novas técnicas e produção desse novo saber, é fundamental destacar o discurso privado em seu entorno. É fulcral o papel da*Microsoft* na profusão de um discurso de maior eficiência das ações policiais, pois ele entra em consonância com o discurso de autoridades, respaldando a introdução e aplicação desses sistemas de vigilância em ambientes urbanos. Algumas de nossas primeiras observações a esse respeito, com algumas entrevistas realizadas, é que boa parte dos gestores e responsáveis pelo Detecta enxergam as práticas, os saberes produzidos apenas como um tipo de negócio, abstrato, neutro e imparcial, reforçando a ideia de uma racionalidade econômica, técnica e não política governando a implementação desse sistema.

De acordo com Alvarez (2002: 693), essa busca por centrar o indivíduo, em sua composição biológica e mental, enquanto sujeito do crime, excluindo quaisquer determinações sócio-culturais, teve uma ampla e positiva recepção no Brasil no início do século XX, e permanecem até hoje como característica estruturante do pensamento criminológico brasileiro. De acordo com o autor, o pensamento jurídico daquele período compreendeu as novas teorias criminológicas a partir do seu potencial de controle social, mas principalmente, como estabelecer formas diferenciadas de tratamento jurídico-penal para determinados segmentos da população, o que garante um "tratamento desigual para os desiguais" (Alvarez, 2002: 696).

Em ambos os casos, os "dispositivos de segurança/policiamento preditivo" potencialmente autorizariam ações preemptivas das autoridades, conformando uma governança centrada nos algoritmos, esquadrinhando e classificando aqueles que potencialmente podem ou não circular, ou podem ou não viver. A problemática no caso dos Drones é que os estudos apresentados tanto pela*New American Foundation* , *Bureau of Investigative Journalism* , demonstram a falha dessas técnicas, uma vez que elas tem sido responsáveis por uma descomunal desproporcionalidade nas mortes de civis e "contrainsurgentes". Considerando que o relatório do TCE demonstra a ineficácia "*a priori"* do Detecta, nos parece que um dispositivo gerido em um contexto de "guerra

global ao terror", reforçará o uso arbitrário de violência, legitimando e aprofundando práticas punitivas excludentes. Assim, uma compreensão devidamente crítica dos dispositivos e formas de governança da segurança preditiva, requer uma aproximação que compreenda, problematize a trajetória política dos algoritmos que fundamentam o seu saber elementar. Talvez uma aproximação entre os Estudos Sociais da Ciência e da Tecnologia, os Estudos de Segurança Crítica Internacional e Sociologia da Punição consigam revelar os elementos políticos, sociais e controvérsias no processo de desenvolvimento dos algoritmos e consequentemente da segurança preditiva.

NOTAS

* Doutor em Política Científica e Tecnológica pela Unicamp, e Pesquisador do GAPI (Grupo de análise de Políticas de Inovação)

1. A mineração de dados pode ser entendida como, a aplicação de tecnologias e técnicas de bancos de dados (como de analise estatística e modelização) a fim de descobrir estruturas ocultas e sutis relações entre dados, e inferir regras que permitem a previsão de resultados futuros. Por sua vez, perfilização algorítimica é entendida como a inferência de presença de características observáveis num dado indivíduo, ou de características não observáveis , atuais ou futuras (Rouvroy et Berns, 2010: 91-92).

REFERÊNCIAS

ALBERTS, D. S; HAYES, R. E. (2003) Power to the Edge: Comand... Control... in the Information Age. Washington, D.C.: DoD Command and Control Research Program, 2003.

Alston, Philip (2010) Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions. United Nations Human Rights Council. Disponível em:http://www.refworld.org/docid/4c07635c2.html. Acesso em 02/07/2014.

Alvarez, M. C. (2002). A Criminologia no Brasil ou como Tratar Desigualmente os Desiguais.*Dados, Revista de Ciências Sociais* , 45(4), 677-704.

Arthur, K. (2015) Supporting Law enforcement resources with predictive policing.*Microsoft Government* . Disponível em: https://enterprise.microsoft.com/en-us/industries/government/supporting-law-enforcement-resources-with-predictive-policing/.

Bellamy, C. (2001). What is information warfare? In R. Matthews & J. Treddenick (orgs.)*Managing the revolution in military affairs* , (pp. 56-75). New York: Palgrave.

Beraldo, S. E. (2015). Relatório de Fiscalização de Natureza Operacional Solução de Consciência Situacional – DAS "Detecta".*Tribunal de Contas da União* . Processo n. 17.941/026/2015.

Bhandari, P. (2016) Predictive Policing: The future of law enforcement.*Microsoft State and Local Government* . Disponível em https://enterprise.microsoft.com/en-

us/industries/government/predictive-policing-the-future-of-law-enforcement/.

Bruno, F. (2016). Rastrear, Classificar, Performar.*Ciência e Cultura* . 68(1), 34-38.

Casady, T. (2011). Police Legitimacy and Predictive Policing.*Geography Public Safety* . 2(4). 01-03.

Cebrowsky, A. K. (2000). Military responses to the informational age.*The RUSI Journal,* 145(5), 25-29.

Chamayou, G. (2013).*Théorie du drone* . Paris: La Fabrique.

Dicjk, J. V. (2014). Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology.*Surveillance & Society* , 2(12), 197-208.

Espositi, S. D. (2014). When Big Data Meets Dataveillance: The hidden side of analytics.*Surveillance & Society* , 2(12), 209-225.

Foucault, M. (2008) Segurança, Território e População: Curso no Collège de France (1977-1978). São Paulo: Martins Fontes.

Geraldo 45. (2014) Detecta: Tecnologia Contra o Crime.*Youtube* . Disponível em: https://www.youtube.com/watch?v=KcUH7_-usTs. Acessado em 09/07/2016.

Graham, S. (2006). Surveillance, Urbanization and the "US Revolution in Military Affairs". In D. Lyon (Org.)*Theorizing Surveillance: The Panopticon and Beyond* (247-269). Portland: Willian Publishing.

Guzik, K. (2009). Discrimination by Design: predictive data mining as security practice in the United States' 'war on terrorism'.*Surveillance & Society* . 1(7), 1-17.

Kanashiro, M. (2016) Apresentação: Vigiar e Resistir: a constituição de práticas e saberes em torno da informação.*Ciência e Cultura* . 68(1), 20-24.

Lianos, M; Goulas, M. (2000) Dangerization and the End of Deviance: The institutional Environment. In: British Journal of Criminology. N. 40. Pp. 261-278.

Mack, G; Beeb, B & Wenzel G. (2002). Total Information Awerness Program (TIA), System Description Document (SDD).*Darpa: Information Awerness Office* .

McCue, C. (2011). Proactive Policing: Using Geographic Analysis to Fight Crime.*Geography Public Safety* . 2(4). 03-05.

National security Agency (2016) What We do. Disponível em:https://www.nsa.gov/what-we-do/.

NYPD (2009) DAS: Public Security Privacy Guidelines. Disponível em:http://www.nyc.gov/html/nypd/html/crime_prevention/counterterrorism.shtml

O'Connel, M. E. (2009) Unlawful Killing with Combat Drones: A case Study of Pakistan 2004-2009.*Legal Studies Research Paper* . 6 de Novembro. 09-43.

Parra, H. (2016) Abertura e Controle na governamentalidade algorítimica.*Ciência e Cultura* . 68(1). 39-42.

Pearsall, B. (2010) Predictive Policing: The Future of Law Enforcement?*NIJ Journal* . N. 266. 16-19.

Perry, W.L., McInnis, B., Price, C.C., Smith, S.C., & Holywood, J.S. (2013) Predictive Policing: The Role of

Crime Forecasting in Law Enforcement Operations.*Rand Corporation Safety and Justice Program* .

Piccerillo, R. A. & Brumbaugh, D. A. (2004). Predictive Battlespace Awareness: Linking Intelligence, Surveillance and Recoinassance Operations to Effects Based Operations.*2004 Command and Control Research and Technology Symposium: The Power of Information Age Concepts and Technologies* . The Pentagon: Recoinassance Directorate Air and Space Operations.

Rouvroy, A. et Berns, T. (2010). Le nouveau Pouvoir Statistique: ou quand le controle s'exerce sur un réel normé, docile et sans événement car constitué de corps “numériques”...*Multitudes* , 40, 88-103.

Scannel, J. (2016). What Can an Algorithm Do?*DIS Magazine* . 1-9.

Secretaria de Segurança Pública de São Paulo. (2015a) Alexandre de Moraes Explica o Funcionamento do Detecta.*Notícias* . Disponível em: http://www.ssp.sp.gov.br/noticia/lenoticia.aspx?id=36199. Acessado em: 10/02/2016.

Secretaria de Segurança Pública de São Paulo. (2015b). Secretaría lança cinturão eletrônico de monitoramento do Detecta em todo litoral de SP.*Notícias* . Disponível em: http://www.ssp.sp.gov.br/noticia/lenoticia.aspx?id=36669.

The Intercept. Skynet: Applying Advanced Cloud-based Behaviour Analytics. (2015)*Documents* . Disponível em: https://theintercept.com/document/2015/05/08/skynet-applying-advanced-cloud-based-behavior-analytics/.