RASTREAR E ELIMINAR: OS NOVOS INSTRUMENTOS DE CONFLITO E VIGILANCIA E O MILITARISMO URBANO

Alcides Eduardo dos Reis Peron

Universidade Anhembi-Morumbi

"Trabalho preparado para sua apresentação no 9º Congresso Latinoamericano de Ciência Política, organizado pela Associação Latino-americana de Ciência Política (ALACIP). Montevideu, 26 ao 28 de julho de 2017"

VIGIAR, PERFORMAR E ELIMINAR: OS NOVOS INSTRUMENTOS DE CONFLITO E VIGILÂNCIA E O MILITARISMO URBANO

Alcides Eduardo dos Reis Peron

Resumo

Nos últimos 20 anos, diante dos progressos tecnológicos observados durante a "Revolução" nos Assuntos Militares estadunidense, e em decorrência do endurecimento das políticas de combate ao terrorismo, verificamos uma miríade de dispositivos cibernéticos de vigilância e controle fundamentando e estruturando as práticas de segurança e de projeção de poder internacionais. Dos Drones armados, aos novos sistemas de policiamento preditivo urbano – como o "Domain Awareness System" em Nova Iorque e o Detecta em São Paulo – a coleta massiva de dados vem estruturando novas formas cercear e eliminar "insurgentes", imigrantes ou criminosos, e aproximando as práticas e táticas de guerra ao ambiente urbano, como observam Bigo (2016), Aradau (2015) e Graham (2016). Nesse sentido, o objetivo desse trabalho é, por um lado, entender como esses novos dispositivos cibernéticos vem intensificando e legitimando práticas excessivas de segurança, tanto internacional quanto urbanas. Por outro lado, buscamos debater de que forma as abordagens, metodologias e categorias analíticas levadas a cabo pelos Estudos Críticos da segurança Internacional e pelos Estudos Sociais da Ciência e da Tecnologia, contribuem para compreender mais enfaticamente os limites e tensões oriundas da adoção desses novos dispositivos.

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.

Essa pesquisa irá explorar as possibilidades teóricas da aproximação entre os Estudos Críticos de Segurança Internacional (ECSI), os Estudos de Vigilância e os Estudos Sociais da Ciência e da Tecnologia (ESCT), principalmente no que tange o desenvolvimento de abordagens para compreender como a reprodução de determinados discursos e práticas securitizadoras é amparada e intensificada pelo desenvolvimento e emprego de novas tecnologias, meios informacionais e técnicas comunicacionais. Nesse sentido, a partir dos ECSI, e apoiados no referencial metodológico dos ESCT, que debate a tecnologia enquanto um lócus de política e autoridade, e nos Estudos de Vigilância, compreendendo a complexidade da relação entre vigilância, segurança e democracia, acreditamos que é possível desenvolvermos um programa de pesquisas que compreenda a problemática da tecnologia para os Estudos de Segurança Internacional.

Assim, nossa hipótese é que os complexos sistemas de armamentos, vigilância, e comunicação, dentre outros, ainda que intensifiquem a capacidade do Estado e demais agentes em agir sobre determinados grupos, eles são também responsáveis por produzir constrangimentos e visíveis formas de controle e arbitrariedade militar e policial. Faz-se urgente, portando, que nos debrucemos sobre o desenvolvimento e aplicação dessas tecnologias, a fim de que compreendamos mais a fundo os processos autoritários que as conformam e são "naturalizados" por elas.

Segurança e tecnologia: Possíveis debates

Nos últimos 30 anos temos verificado uma aceleração do processo de desenvolvimento de novas tecnologias de informação, 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. Em uma sociedade

profundamente marcada pela profusão de uma forma de comunicação ubíqua, dispositivos informacionais onipresentes, é fundamental que o pensamento em Segurança Internacional incorporasse uma dimensão analítica desses objetos, processos e práticas resultantes da sua incorporação em conflitos e em políticas de segurança e defesa.

Durante o período conhecido como "Revolução nos Assuntos Militares", essas tecnologias fundamentaram o desenvolvimento de novos instrumentos de comunicação e vigilância, armamentos sofisticados (smart bombs), bem como de uma complexa infra-estrutura comunicacional capaz de agenciar conflitos remotamente, como no caso do emprego de drones armados pelos EUA no oriente médio. Essas tecnologias também tem permitindo o aprimoramento de técnicas de monitoramento, como é o caso dos instrumentos de coleta massiva de dados, e perfilização geográfica (Big Data), que estruturando práticas de espionagem internacional levadas a cabo pela National surveillance Agency (NSA).

Nesse mesmo contexto, o uso de ferramentas computacionais através da internet tem sido um dos elementos que vem conformando os denominados conflitos "cibernéticos", ou como os colégios militares estadunidenses os definem "conflitos centrados em rede" (CEBROWSKY, 2000). Exemplos desse tipo de conflito envolvem práticas de espionagem, vigilância, sabotagem, crimes que ocorrem no âmbito do ciberespaço, bem como a manipulação do fluxo informacional global, produzindo narrativas favoráveis à processos de securitização e de engajamento em conflitos (BELLAMY, 2011).

Essas infra-estruturas comunicacionais garantem às grandes empresas de comunicação e jornalismo um enorme protagonismo no cenário internacional, a tal ponto de autores como James Der Derian (2009a) considerá-las atores estruturantes do sistema internacional, ao construírem narrativas que agem sobre a percepção social acerca de noções de ameaças, práticas militares e conflitos. Por outro lado, essa intricada rede comunicacional, em um contexto de profusão de práticas terroristas e assimétricas, e conflitos irregulares, tem sido um profícuo instrumento de propagação e narrativas e ideologias, como o "Estado Islâmico" vem fazendo em suas intervenções fílmicas através da internet.

Em comum nesses diversos processos, é possível identificarmos sistemas tecnológicos reconfigurando práticas de segurança, reforçando discursos securitizadores

ou de extremistas. Assim, por um lado, o emprego de novas tecnologias informacionais permite ampliar as capacidades do Estado e de grupos adjacentes em identificar e "construir" ameaças. Por outro lado, permitem ainda diversificar as formas de se agir sobre as ameaças, inaugurando novos tipos de conflitos – cibernéticos, operados remotamente, informacionais, dentre outros. Cada vez mais o desenvolvimento e emprego dessas tecnologias tem suscitado debates nos Estudos Estratégicos e de Segurança Internacional, impondo a necessidade destes campos em se expandirem, e incorporarem novas metodologias e abordagens para a compreensão desses novos fenômenos.

Desde meados dos anos 1980, por exemplo, diversos autores como Barry Buzan, Ole Weaver e Richard Ullman (1983) vem discutindo a ampliação e a organização dos Estudos de Segurança Internacional (ESI), no entanto, pouco esforço tem sido destinado no período atual para compreender os novos desafios impostos pela adoção dessas novas tecnologias. Ainda que no âmbito da Escola de Copenhague Helen Nissenbaum e Lene Hansen (2009: 1167) tentem atribuir certo valor tanto para as ciberespaço como para as novas tecnologias informacionais e de vigilância nos ESI, as autoras esbarram em um elemento que denominam "Tecnificação", em que os ambientes e processos permeados por essas tecnologias produze discursos técnicos e especializados. Nesse sentido, as autoras irão afirmar a dificuldade em compreender esses sistemas como uma barreira para a "politização" desses temas na agenda dos ESI.

As recentes intersecções entre os Estudos Críticos de Segurança (KRAUSE, 1998; WYN JONES, 1999; e DER DERIAN, 2009), os Estudos de Vigilância (BIGO, 2006; e LYON, 2006), bem como os Estudos Sociais da Ciência e da Tecnologia (WINNER, 1983, MCKENZIE, 2012), tem apresentado possibilidades interessantes para o debate e apreensão desses temas, e toda a sua implicação para os ECSI. Desse modo nos parece que tem havido uma necessidade de desenvolver abordagens que vão além de um simples processo de ampliação do conceito e dos Estudos de Segurança, mas principalmente, deem conta de compreender a complexidade relativa a adoção de novas tecnologias comunicacionais e informacionais para os processos securitizadores, provocando profundas alterações no modo como a Segurança e as políticas de Segurança Internacional são pensadas, debatidas e exercidas.

Durante os conturbados anos da Guerra Fria, o conceito de Segurança, era concebido de modo extremamente negativo, como a mera ausência de ameaças. Não

obstante, essa concepção de Segurança se caracterizava por um profundo estreitamento daquilo que se consideravam ameaças externas, e dos meios e agentes para combatê-las, respectivamente, o Estado, e os meios militares. Nesse contexto, era comum que a segurança se configurasse enquanto uma construção em que as categorias de ameaças, problemas e possibilidades de estudos eram percebidas e definidas por instituições militares, *think-tanks* alinhados a essa visão estado-centrica, territorialista e limitada.

Problemas de ordem ambiental, econômica, social e política não eram tidos como relevantes pelo campo de estudos em segurança, a menos que de alguma forma viessem a afetar diretamente a estrutura e organização do Estado. Algumas teorias nesse momento, principalmente as teorias Feministas, Críticas e Construtivistas, partindo da premissa de, de que "a teoria é sempre para alguém e por algum propósito" (COX, 1986: 207), irão argumentar que não apenas os estudos de segurança seriam inadequados, mas sim que ela refletia uma espécie de exercício de autoridade, uma forma dos grupos dominantes imporem uma interpretação particular da realidade (SHEEHAN, 2005: 45).

Nesse período, os processos globalizadores dão margem para o surgimento e diversificação de diversos tipos de fenômenos e problemas, que atentariam ferozmente não apenas contra o Estado, mas contra a sociedade, a economia, o meio ambiente e às estruturas políticas, com igual ou pior capacidade de destruição e fragilização que as chamadas "ameaças tradicionais". Diante desse cenário, com o destaque de novos atores, como as empresas transnacionais, empresas de comunicação, ONGs, bem como novas práticas de violência, como atentados terroristas, guerras irregulares, dentre outras, Barry Buzan (1983) irá propor que a noção de Segurança deveria ampliar-se em até dois sentidos. Em primeiro lugar, o conceito deveria apartar-se da sua relação exclusiva com o militarismo, e transbordar para outros setores, como economia e sociedade, em seguida, o objeto referente da segurança, aquele que deveria ser segurado, não deveria ser conceitualizado apenas em termos do Estado, mas envolver o indivíduo e o sistema.

A ampliação do espectro e conceito de segurança – a securitização – via de regra, significaria conferir aos objetos securitizados, problemas e ameaças, o status de uma ameaça existencial, e portanto, garantindo a ele a devida prioridade, urgência, atenção e governamental. Dada a excepcionalidade do objeto, devido ao seu potencial caráter emergencial, ele seria postado em uma escala superior de valor diante dos demais, haveria um maior comprometimento com a alocação de recursos para a solução dos problemas. (BUZAN, 1991: 432-4333)

Dentre as novas possibilidades conceituais de segurança de coletividades humanas, Buzan (1991a: 19-20) apontará cinco setores: Segurança Militar, que envolve a preocupação com as capacidades de ofensiva e defensiva armada, e a percepção dos Estados sobre as intenções de cada um; Segurança Política, que envolve os debates sobre estabilidade organizacional dos Estados, sistemas, governos e ideologias que os legitimam; Segurança Econômica: que envolve o acesso a recursos, finanças e mercados necessários para sustentar níveis aceitáveis de bem estar e poder do Estado; Segurança Social, que se concentra na sustentabilidade dos padrões de linguagem, cultura, religioso e de identidade e costumes nacionais; Segurança Ambiental, focada na manutenção da biosfera local e planetária, diante da necessidade humana.

De acordo com Buzan, Waeaver e De Wilde (1998:08), ainda que esses cinco setores definam um ponto focal para análise e discussão, eles estão profundamente relacionados, manifestando-se enquanto uma totalidade complexa, dificilmente compreendida em separado. Assim, ao longo da década de 1980 e 1990, Buzan e Hansen (2012) e outros expoentes da chamada Escola de Copenhague, buscam organizar e conferir forma e substância ao campo de estudos de Segurança Internacional. Nesse processo, identificariam três vertentes teóricas, ou paradigmas que caracterizam os ESI, a perspectiva tradicionalista, a abrangente e a crítica. No primeiro momento, fundamentada em perspectivas realistas e neo-realistas, verifica-se que há uma restrição da problemática de segurança ao escopo militar, tendo o Estado como o principal referencial e analítico. Em seguida, há a perspectiva abrangente, aonde se concentrariam os esforços da Escola de Copenhague, que enxerga a necessidade de incorporação das ameaças militares, políticas, econômicas, dentre outras no escopo dos ESI, pois entende que as ameaças são geradas em múltiplos campos e esferas de existência. Nesse sentido, ao debruçar-se sobre o processo de construção da excepcionalidade dos objetos securitizados, autores como Ole Weaver (1993) irão debater os "atos de fala" e o desenvolvimento de discursos como sendo fundamentais para o processo de securitização – englobando um estudo sobre o agente securitizador, o objeto securitizado e a audiência que legitimaria esse processo. Por fim, Buzan e Hansen (2012) identificam a emergência de uma escola crítica dos ESI, que em trabalhos de autores como Richard Wyn Jones (1999), Ken Booth (1997), Keith Krause (1998), dentre outros, que irão se concentrar em questões como auto-determinação coletiva e emancipação ou esclarecimento individual em face de práticas opressivas e injustas, como sendo objeto dos Estudos de Segurança.

Para nossos propósitos nesse trabalho, pretendemos nos concentrar em específico nessa última vertente teórica, que conformará os denominados Estudos Críticos da Segurança Internacional (ECSI). Isso porque, acreditamos, como fará Wyn Jones (1999), que esses estudos críticos nos permitiriam construir uma sólida aproximação com os Estudos Sociais da Ciência e da Tecnologia (ESCT), assim como dos Estudos de Vigilância, debatendo a tecnologia como elemento central nos discursos autoritários de segurança, bem como na construção de formas sofisticadas de controle e repressão. Nesse âmbito, como comenta Sheehan (2005: 152), os ECSI evoluem diretamente dos trabalhos da Teoria Crítica, tanto no que concerne os Trabalhos de Robert Cox, como dos pensadores da Escola de Frankfurt, propondo "uma coerente preocupação acerca de como determinadas estruturas e práticas contribuem para a manutenção da opressão, a partir de então provendo uma visão alternativa que os oprimidos podem compreender, engajar e possivelmente implementar".

Nesse ponto, os ECSI seguem as premissas da Teoria Crítica, pressupondo uma conexão entre conhecimento e poder. Nesse sentido, a Teoria Crítica é pensada enquanto uma oposição ao que Horkheimer nomeia como "Teoria Tradicional" que, guardando inúmeras referências com o positivismo, entende o mundo como uma série de fatos que esperam ser descobertos e enquadrados em determinados campos de conhecimento. Essas teorias, ao concentrarem-se na premissa metodológica de que os fatos podem ser descobertos e trabalhados independentemente da estrutura social em que ocorre a percepção, faz com que Robert Cox a compreenda como uma forma de reprodução do status quo, ou exercício de autoridade, fazendo parecer natural a distribuição de poder existente. Nesse sentido, elas teriam o potencial de privilegiar e normalizar um entendimento particular do que constitui o conhecimento, temas e problemas relevantes, menosprezando os clamores por verdade daqueles que se opõem à ordem existente.

A Teoria Crítica, portanto, entenderia que os fatos são produto de estruturas e interações sociais e históricas, o que os permite identificar como as teorias e narrativas contribuem para os interesses de determinados grupos. Assim, ciente das suas bases contextuais e históricas, a Teoria Crítica irá entender a sociedade e buscar mudá-la, ao demonstrar a natureza mutável e contingente das formas de dominação e opressão (SHEEHAN, 2005: 154).

A recepção da Teoria Crítica pelos Estudos de Segurança é realizada por autores como Ken Booth (1991), o qual irá explicitar que Segurança não é a mera ausência de

ameaças físicas a integridade do ser humano ou do Estado, mas sim um estado no qual há a ausência de insegurança em um sentido amplo; diversos elementos são capazes de produzir um estado de insegurança, a um indivíduo e a um coletivo, dentre eles, destacam-se a precarização, a pobreza como determinantes. Para Booth, essa insegurança induziria os indivíduos a tomarem decisões equivocadas, portanto, sendo necessário prover os oprimidos com um ferramental capaz de torná-los conscientes e empoderá-los. Exatamente esse processo de empoderamento, e liberdade diante formas de "violência estrutural" que o autor definirá como um processo de emancipação, algo elementar para as políticas de segurança e segurança internacional, capaz de imbuir os atores de certa autonomia (BOOTH, 1991: 31).

Assim, o comprometimento em explorar ao máximo as potencialidades da emancipação humana, a crítica ao positivismo, o foco no questionamento dos discursos e práticas de segurança que produziriam efeitos opressivos e constrangedores, a investigação sobre o processo de construção das ameaças pelos agentes securitizadores, dentre outros, seriam elementos que caracterizariam os objetos e as metodologias dos Estudos Críticos de Segurança. No entanto, os ECSI vão além do processo de ampliação dos Estudos de Segurança Internacional, não apenas oferecendo uma nova epistemologia e ontologia, mas trazendo novos objetivos, referentes e problemas.

Desse modo, buscando apresentar os elementos que sintetizam o programa de pesquisas dos Estudos Críticos de Segurança Internacional, Keith Krause (1998: 317) irá apontar algumas premissas que os autores desse campo irão assumir: 1) Os principais atores da política mundial são constructos sociais, e produtos de complexos processos históricos que incluem diversas dimensões sociais, políticas, materiais e ideacionais; 2) Esses sujeitos são constituídos por práticas políticas que criam entendimentos sociais compartilhados; 3) Sendo assim a política mundial não é estática, dado que são constructos sociais; 4) Nosso conhecimento sobre os sujeitos, estruturas e práticas não são objetivos, posto que a organização e descrição dos fatos é coletiva, e não prevê a separação entre "observador" e atores sociais; 5) Métodos interpretativos que investigam os entendimentos dos atores sobre a organização de seu mundo social, e sua relação com as estruturas sociais e práticas são um foco central para a pesquisa; 6) O propósito da teoria não seria necessariamente a explicação e a predição em uma estrutura trans-histórica e generalizada, mas um entendimento contextual e um conhecimento prático.

Com base nessas premissas, Richard Wyn Jones (1999) irá desenvolver uma noção de Estratégia – contrapondo a perspectiva extremamente limitada exposta por Buzan – que estivesse em consonância com a dimensão analítica dos ECS, ou seja, que previsse a possibilidade de emancipação e afirmação. Wyn Jones percebe que para Buzan, estratégia é algo que ignora os fins, os resultados humanos, do uso de força. Consequentemente, para ele, a tecnologia seria um fenômeno eminentemente neutro, desprovido de dimensões políticas, cuja única funcionalidade seria apresentar um leque de opções para a ação estratégica. Assim, a tecnologia condicionaria a ação estratégica, ainda que os resultados do seu emprego fossem desastrosos. Desse modo, a estratégia seria uma forma de racionalidade instrumental que engessaria a possibilidade de mudança, principalmente por conta da sua perspectiva neutra e rasa em relação à tecnologia.

Para superar essa perspectiva, incorporando à noção de estratégia e segurança a possibilidade de mudança, Wyn Jones acredita uma abordagem crítica acerca das tecnologias permitiria compreender a tecnologia enquanto resultado de construção social e política. Se a tecnologia, elemento que engessa a possibilidade de mudança e emancipação é, na verdade um constructo social, discursivo e político passível de agenciamentos e debates, Wyn Jones (1999) entenderá que também a noção de Estratégia. O autor irá então se concentrar em autores como Arthur Feenberg (1991), Donald Mackenzie (2012), e Langdon Winner (2012), questionando os pressupostos neo-realistas acerca da neutralidade da tecnologia e de ruptura entre "meios e fins". Consequentemente, dado que os fins políticos e a estruturação da estratégia estariam contidos na constituição, adoção e uso da tecnologia, é possível que os fins e cursos de ação da estratégia se alterem, a partir da interferência, questionamento e debate acerca das tecnologias.

Tanto Winner (1980) como Feenberg (1991) irão propor uma perspectiva "crítica" da tecnologia, entendendo que os artefatos em si, e não apenas o no contexto em que foram elaborados, seriam portadores de política, que se manifesta em seu design, seu uso ou sua aplicação. Considerando política, nesse sentido, como a totalidade de arranjos de poder e autoridade nas associações humanas, eles defendem que a tecnologia é um fenômeno político não apenas pela sua construção social, mas por considerar que existem disputas de cunho político-sociais nesse processo que se manifestam no desenho final dos artefatos, e que consequentemente serão perpetuadas e reproduzidas em seu uso. Logo, no momento em que as tecnologias são criadas e postas em uso, Winner (1986:06)

acredita que elas promoverão "significantes alterações nos padrões de atividade humana e suas instituições". Winner irá defender que uma vez que as decisões humanas sobre o desenvolvimento da tecnologia estão constantemente mascaradas, encaixotadas de modo a permanecerem obscuras à sociedade, a tecnologia parece operar além do controle humano, e operar o resultado de um processo automático inevitável.

O filósofo francês, Gregoire Chamayou (2013), defende a necessidade de uma teoria crítica dos armamentos, a qual nos permitiria compreender de que forma os meios constrangem os modos de ação (em outras palavras, constrangem a própria política de segurança), e provocam efeitos muito específicos sobre os usuários, sobre aqueles alvejados por essas armas, e sobre aqueles que decidem politicamente pelo seu uso. Buscando descrever como a natureza da guerra é tumultuada pela adoção dos drones armados, Chamayou (2013:41) entende que essa tecnologia permitiria a promoção de campanhas que, diferentemente de guerras formais, teriam o único objetivo: de vigiar e aniquilar alvos considerados suspeitos. De acordo com o autor, a única forma para se derrubar o "mecanismo da luta militar" seria a partir de uma teoria crítica dos armamentos, que através de uma análise tanto técnica, quanto política, permita revelar os padrões ocultos de poder e autoridade nessa tecnologia, bem como o seu impacto social: "A ideia seria que os meios são constrangedores, e que a cada tipo de meio são associados a uma sorte de restrições específicas (...) Ao invés de indagar se o fim justificaria os meios, torna-se mais importante indagar o que a escolha desses meios, por si só, tende a impor" (2015: 24).

No mesmo caminho, James Der Derian (2009a) se concentrará em entender os conflitos conduzidos pelos EUA nos últimos 30 anos, à luz dos impactos das novas tecnologias cibernéticas e comunicacionais descrevendo o que chama de "Guerra Virtuosa" (do inglês *Virtuous War*, ao mesmo tempo virtual, e imbuída de virtudes). Em seus estudos, baseados na teoria crítica e no construtivismo, o autor irá debater a forma pela qual os meios de comunicação, organizados sob a forma de uma "Rede Militar-Industrial de Entretenimento", promovendo narrativas acerca dos conflitos, das ameaças internacionais, em paralelo ao constante emprego de tecnologias de controle remoto e mediação do conflito (*drones*, mísseis transcontinentais, radares, satélites, dentre outros) contribuem para a perpetuação do conflito, e de um estado de constante insegurança. Essa perpetuação ocorreria, de acordo com o autor, a partir da difusão de uma perspectiva "sanitarizada", "cirúrgica" e branda acerca dos conflitos e dos instrumentos empregados.

Não diferente, Didier Bigo (2006) e David Lyon (2006) entendem que os Estudos Críticos de Segurança I tem uma imensa proximidade dos Estudos de Vigilância. Isso porque, assim como a os ECS, os Estudos de Vigilância têm buscado compreender os discursos e práticas que perpassam pelo desenvolvimento e emprego de tecnologias que fundamentam práticas de Segurança. No caso específico dos Estudos de Vigilância, as tecnologias referem-se aquelas capazes de uma captura contínua e rotineira de dados, processamento cruzamento, apropriação e gerenciamento de informações, e que incluem também o controle de acesso, a vigilância, o monitoramento e a identificação de pessoas, a construção de bancos de dados e perfis sobre a população (KANASHIRO, 2016).

Desse modo, não se trata simplesmente de desenvolver aqui um programa de pesquisa que contribuísse para a incorporação da tecnologia pelo processo de securitização, apresentando as características de uma eventual "Segurança Cibernética" ou " Informacional", mas fundamentalmente, de aprofundar a compreensão sobre como a tecnologia é fruto de uma construção social e política, assim como objeto para intensificação e amplificação dos discursos securitizadores. Nesse sentido, identificar os constructos de poder e autoridade nos instrumentos informacionais e de vigilância, analisando o modo como eles reproduzem essas formas e valores sobre seus usuários, e sobre seus "alvos", nos parece, uma tarefa crucial para os Estudos Críticos de Segurança.

Desse modo, os ESCI ampliam o leque metodológico e analítico dos Estudos de Segurança, pois com isso se torna possível descrever as complexas redes de poder que se estruturam através das políticas de segurança dos países, bem como seus efeitos mais diversos. Essas políticas que, no caso dos EUA, tem se desenvolvido e sustentado no entorno de novas tecnologias informacionais e de outras naturezas que, como veremos a seguir, por um lado permitem um uso indiscriminado de violência militar, por outro, se espalham enquanto doutrinas e técnicas de policiamento, produzindo um efeito similar sobre as políticas de segurança pública.

Para tanto, não apenas o recuso aos ESCTS é suficiente, pois determinadas redes e arranjos tecnológicos podem ser tão amplas e complexas, que as controvérsias e problemáticas que nos interessam podem nos escapar. Assim, os ESCI nos permitem também uma reflexão complementar, a partir de categorias analíticas dos Estudos de Vigilância, que recuperam a terminologia foucaultiana de governamentalidade, dispositivos e saber-poder.

Drones, *Total Informational Awareness*: A Segurança Preditiva

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.

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.

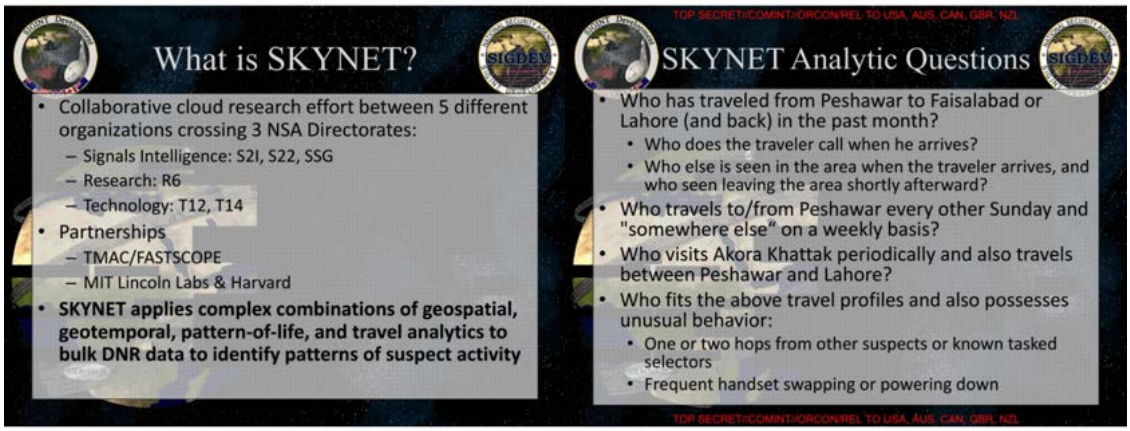
Um outro método seria o de Assassinatos por Assinatura de Calor (*Signature Killing*). Nesse caso, como expõe Chamayou (2013), a visualização de "alvos" através das câmeras infravermelho, identificando os corpos enquanto sinais de calor, formam arquivos de imagens, que cruzadas com informações sobre 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.

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).

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*), enquanto intensificadores do processo de controle social e discriminação. 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). 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).

Conclusão: Controle e Militarismo Urbano

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.

Essas tecnologias caracterizam-se pela dualidade de emprego, subsidiando técnicas e práticas policiais em complexos contextos urbanos – exemplos disso vão de carros fortificados de uso exclusivo militar, até mesmo dispositivos sonoros de dispersão de pessoas, helicópteros especiais, etc. De acordo com Granham (2015), elas tem se espalhado para os países periféricos em concomitante com a profusão da racionalidade neoliberal, que irá imperar sobre as políticas econômicas nesses países. Isso porque, conforme as políticas neoliberais reforçam as desigualdades sociais a partir da reprodução ampliada do capital nesses territórios, produzindo revoltas populares, formas de comércio informal, práticas ilícitas, cada vez mais técnicas de policiamento tendem a se sofisticar – adotando instrumentos e práticas antes testadas em campos de batalha e contextos militarizados.

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.

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.

Aradau, C. (2014) Security that Matters: Critical Infrastructure and Objects of Protection. In: Security Dialogue. Vol 4. n. 05. Pp. 491-514.

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/>.

Bigo, D. (2006) Security, Exception, Ban and Surveillance. In: Lyon, David Theorizing Surveillance: The Panopticon and Beyond. Portland: Willian Publishing.

Booth, K. (1991) Security and Emancipation. In: Review of International Studies, 17, 317-326.

Bourne, M; Johson, H; Lisle, D. (2015) Laboratizing the border: The production, translation and anticipation of security technologies. In: Security Dialogue, Vol. 46. N. 4. Pp. 307-325.

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.

Der Derian, J. (2009a) Critical Practices in International Theory: Selected Essays. Nova Iorque: Routledge.

_____. (2009b) Virtuous War: Mapping the Military-Industrial Media Entertainment Network. 2ª edição. Nova Iorque: Routledge.

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.

Feenberg, A. (2010) A Tecnologia pode incorporar valores? A Resposta de Marcuse para a questão da época. In: Neder, Ricardo. A teoria crítica de Andrew Feenberg: Racionalização democrática, poder e tecnologia. Brasília: Observatório do movimento pela tecnologia social na América Latina.

Foucault, M. (2005) Em defesa da Sociedade: Curso no Collège de France (1975-1976). São Paulo: Martins Fontes.

_____. (2014) Microfísica do Poder. São Paulo: Paz e Terra.

_____. (2008a) O Nascimento da Biopolítica: Curso dado no Collège de France (1978-1979) São Paulo: Martins Fontes.

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

_____. (2014) Vigiar e Punir: Nascimento da Prisão. Petrópolis: Vozes.

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.

Krause, K. (1998) Critical Theory and Security Studies: The Research Programme of "Critical Security Studies". In: Cooperation and Conflict, N. 3, Vol. 33. Pp: 298-333.

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/>.

Winner, L. (1980) "Do Artifacts Have Politics?" In: Deadalus, V. 109, n. 1, 121-136.

Wyn Jones, R. (1999) Security, Strategy, and Critical Theory. Colorado: Lynne Rienner.