PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

Thallita Gabriele Lopes Lima

Punição e desresponsabilização na prevenção de possíveis futuros perigosos:

multitude de dados, algoritmos e a construção de perfis antecipados de "terroristas" na França

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo programa de Pós-graduação em Relações Internacionais do Instituto de Relações Internacionais da PUC-Rio.

Orientadora: Profa. Isabel Rocha de Siqueira
Co-orientadora: Profa. Manuela Trindade Viana

Rio de Janeiro
Fevereiro de 2020

PUC-Rio - Certificação Digital Nº 1812441/CA

PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

Thallita Gabriele Lopes Lima

Punição e desresponsabilização na prevenção de possíveis futuros perigosos: multitude de dados, algoritmos e a construção de perfis antecipados de "terroristas" na França

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre pelo Programa de Pós-graduação em Relações Internacionais da PUC-Rio. Aprovada pela Comissão Examinadora abaixo.

Profa. Isabel Rocha de Siqueira
Orientadora e Presidente
Instituto de Relações Internacionais – PUC-Rio

Profa. Manuela Trindade Viana
Co-orientadora
Instituto de Relações Internacionais – PUC-Rio

Prof. Bruno Magalhães
Instituto de Relações Internacionais – PUC-Rio

Prof. Bruno de Vasconcelos Cardoso
IFCS – UFRJ

Rio de Janeiro, 28 de fevereiro de 2020

PUC-Rio - Certificação Digital Nº 1812441/CA

Todos os direitos reservados. É proibida a reprodução total ou parcial do trabalho sem a autorização da universidade, da autora e da orientadora.

Thallita Gabriele Lopes Lima

Graduada em Relações Internacionais pela Universidade Federal Rural do Rio de janeiro (UFRRJ) em 2016 com a monografia sobre a relação entre a insegurança urbana francesa e as políticas de migração e integração. Tem experiência com pesquisas sobre segurança pública, relação entre dispositivos tecnológicos e segurança. Áreas de interesse incluem segurança internacional; governança algorítmica; práticas de classificação e quantificação na política internacional contemporânea.

Ficha Catalográfica

Lima, Thallita Gabriele Lopes

Punição e desresponsabilização na prevenção de possíveis futuros perigosos : multitude de dados, algoritmos e a construção de perfis antecipados de “terroristas” na França / Thallita Gabriele Lopes Lima ; orientadora: Isabel Rocha de Siqueira ; coorientadora: Manuela Trindade Viana. – 2020.

82 f.: il.; 30 cm

Dissertação (mestrado)–Pontifícia Universidade Católica do Rio de Janeiro, Instituto de Relações Internacionais, 2020.

Inclui bibliografia

1. Relações Internacionais – Teses. 2. Vigilância. 3. Algoritmo. 4. França. 5. Antiterrorismo. 6. Responsabilização. I. Siqueira, Isabel Rocha de. II. Viana, Manuela Trindade. III. Pontifícia Universidade Católica do Rio de Janeiro. Instituto de Relações Internacionais. IV. Título.

CDD: 327

PUC-Rio - Certificação Digital Nº 1812441/CA

PUC-Rio - Certificação Digital Nº 1812441/CA

Para José, Átila e Wesley pelo apoio incondicional de sempre, carinho e participação que significaram segurança e a certeza de que não estava e nunca estarei sozinha em minha caminhada. Dedico a vocês além desta conquista todo o meu amor.

Agradecimentos

Gostaria de começar agradecendo a Deus por ter me dado saúde, coragem, sabedoria e equilíbrio para conseguir chegar até aqui.

Aos meus pais, José e Átila, agradeço pelo carinho, incentivo, compreensão, ao serem privados em muitos momentos da minha companhia, e principalmente por terem apoiado as minhas escolhas.

Ao meu companheiro de vida, Wesley, por todo carinho e amor. Obrigada pela paciência infinita nos meus momentos de tensão, pela constante disposição em ajudar, por sempre se fazer presente e por compartilhar comigo todos os anseios, dúvidas, sonhos, inseguranças e vitórias. Você sempre me acalma, o que foi fundamental para que eu superasse as dificuldades pelo caminho. Obrigada por ser minha paz e porto seguro.

Ademais, gostaria de agradecer ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) por financiar minha pesquisa e meu mestrado em meio a um período de desmonte governamental da ciência e educação no Brasil. Assim como, expressar toda a minha gratidão e afeto aos professores e funcionários do Instituto de Relações Internacionais da PUC-Rio.

Um agradecimento especial para duas pessoas que me inspiraram como pesquisadoras, professores e seres-humanos, além de partilharam a caminho que tornou esta pesquisa possível. Primeiramente, a minha orientadora Isabel, seus comentários, conversas, conselhos e sua atenção e carinho foram essenciais para este trabalho e para além dele. Também gostaria de agradecer a Manuela pela disponibilidade em ser minha co-orientadora, mas para além disso a disponibilidade que sempre tem em me ouvir. Obrigada pelas conversas e comentários. Posso afirmar com segurança que sua participação foi central para esse trabalho e, sem você minhas reflexões não seriam as mesmas. Meu agradecimento a vocês não cabe em palavras.

Aos meus colegas da turma de 2018 do mestrado um obrigada mais que especial, vocês são incríveis. Não poderia deixar de destacar aqui os companheiros de GT e tantas histórias: Ana Lacerda, Maria Alice e Mariana. Obrigada pelo apoio, conversas e risadas.

PUC-Rio - Certificação Digital Nº 1812441/CA

Resumo

Lima, Thallita Gabriele Lopes; Rocha de Siqueira, Isabel (Orientadora); Viana, Manuela Trindade (Co-orientadora). **Punição e desresponsabilização na prevenção de possíveis futuros perigosos: multitude de dados, algoritmos e a construção de perfis antecipados de "terroristas" na França.** Rio de Janeiro, 2020. 82 p. Dissertação de Mestrado – Instituto de Relações Internacionais, Pontifícia Universidade Católica do Rio de Janeiro.

Desde 2015, a França tem empreendido um processo de normalização de práticas anunciadas quando do estado de emergência, por meio da promulgação do Pacote de Lei sobre a Vigilância e a Lei Antiterrorista de 2017. Tais instrumentos propunham o fortalecimento da segurança interna e o combate ao terrorismo sob uma lógica de antecipação do risco, com técnicas de vigilância e controle informadas por dados e metadados. Este trabalho investiga os efeitos do crescente uso de tecnologias computacionais em práticas voltadas à prevenção de possíveis futuros perigosos, buscando explorar, mais precisamente, como afetam processos de responsabilização. O artigo se divide em três movimentos analíticos principais. Primeiro, analisarei a consubstanciação de uma arquitetura institucional e normativa que consolida o monopólio da supervisão em benefício dos serviços de inteligência; e como a prática de construção de "perfis suspeitos" através dos algoritmos veio a ser afirmada como uma necessidade para lidar com as contingências e incertezas na França face à ameaça do terrorismo e da radicalização. Em seguida, discutirei as condições de possibilidade do uso de algoritmos na produção de conhecimento de inteligência, em particular na produção de "evidências" que informam as medidas individuais de controle e vigilância. A proposta é analisar as conexões entre, de um lado, práticas de mensuração do perigo em um discurso técnico ancorado no imperativo da eficiência das práticas de vigilância; de outro, os efeitos de controle sobre os indivíduos com a flexibilização de salvaguardas processuais e garantias de direitos. O terceiro movimento terá seu ponto de gravidade nas camadas de práticas humanas e não humanas presentes nas medidas de controle e vigilância para entender seus efeitos sobre processos de responsabilização. Para tal, analisarei a relação entre a produção de conhecimento e a promulgação do não-conhecimento, através do sigilo e incerteza, nos processos de contestação das medidas individuais de controle e vigilância na França. O

PUC-Rio - Certificação Digital Nº 1812441/CA

objetivo geral aqui é analisar como dispositivos de controle administrativo, como a aplicação das medidas administrativas de controle e vigilância ("MICA" semelhante a prisão domiciliar), no contexto do combate ao terrorismo na França, exemplifica um sistema de validação de autoridade e dispersão dos processos de responsabilização. O trabalho argumenta que tais processos implicam uma ativa desresponsabilização dos profissionais de segurança através da dispersão de responsabilidade entre humanos e não humanos e também favorecem a promulgação do não-conhecimento, em especial através do sigilo.

Palavras-chave

Vigilância; algoritmo; França; antiterrorismo; responsabilização

PUC-Rio - Certificação Digital Nº 1812441/CA

Abstract

Lima, Thallita Gabriele Lopes; Rocha de Siqueira, Isabel (Advisor); Viana, Manuela Trindade (Co-advisor). **Punishment and desresponsibility in preventing possible dangerous futures: multitude of data, algorithms and the construction of anticipated profiles of "terrorists" in France**. Rio de Janeiro, 2020. 82 p. Dissertação de Mestrado – Instituto de Relações Internacionais, Pontifícia Universidade Católica do Rio de Janeiro.

Since 2015, France has undertaken a process of normalizing practices announced during the state of emergency, through the promulgation of the Surveillance and Anti-Terrorism Law Package of 2017. Such instruments proposed the strengthening of internal security and the fight against terrorism under a logic of risk anticipation, with surveillance and control techniques informed by data and metadata. This work investigates the effects of the increasing use of computer technologies in practices aimed at preventing possible dangerous futures, seeking to explore, more precisely, how they affect responsabilization processes. The article is divided into three main analytical movements. First, I will analyze the consolidation of an institutional and normative architecture that consolidates the monopoly of supervision for the benefit of intelligence services. In addition, how the practice of building "suspicious profiles" through the algorithms came to be affirmed as a necessity to deal with the contingencies and uncertainties in France in the face of the threat of terrorism and radicalization. Then, I will discuss the conditions for the possibility of using algorithms in the production of intelligence knowledge, in particular, in the production of "evidence" that inform individual control and surveillance measures. The proposal is to analyze the connections between, on the one hand, hazard measurement practices in a technical discourse anchored on the imperative of efficiency in surveillance practices; on the other hand, the effects of control over individuals with the easing of procedural safeguards and guarantees of rights. The third movement will have its point of gravity in the layers of human and non-human practices present in control and surveillance measures to understand its effects on accountability processes. To this end, I will analyze the relationship between the production of knowledge and the enactment of non-knowledge, through secrecy and uncertainty, in the processes of contesting individual control and surveillance measures in France. The general objective here is to analyze how administrative control devices, such as the

PUC-Rio - Certificação Digital Nº 1812441/CA

application of administrative control and surveillance measures ("MICA" similar to house arrest), in the context of combating terrorism in France, exemplify a system of validation of authority and dispersion responsabilization processes. The paper argues that such processes imply an active desresponsabilization of security professionals through the dispersion of responsibility between humans and non-humans and favor the promulgation of non-knowledge, especially through secrecy.

Keywords

Surveillance; algorithm; France; anti-terrorism; responsibilization.

PUC-Rio - Certificação Digital Nº 1812441/CA

Sumário

1. **Introdução** 13
2. **Arquitetura vigilante: novos meios técnicos e tecnológicos nas práticas de inteligência** 20
   - **2.1. A Lei de Inteligência e a emergência de uma comunidade de vigilância na França** 22
   - **2.2. Metadados, dados, algoritmos e a construção de perfis antecipados de "terroristas" na França** 32
3. **A individualização do controle da possibilidade: o caso das MICAs** 44
   - **3.1. Evidências baseadas em "notas brancas": a Lei SILT e a transformação das práticas judiciais** 46
   - **3.2. Medidas Individuais de Controle Administrativo (MICA): critérios e aplicações** 50
4. **Borrando a responsabilidade: tecnologias de vigilância algorítmica como um campo de práticas de desresponsabilização** 57
5. **Conclusão** 68
6. **Referências bibliográficas** 71

PUC-Rio - Certificação Digital Nº 1812441/CA

Lista de figuras

Figura 1. Análise de rede social..... 41

Figura 2. Esquema do processo de autorização das operações de inteligência à aplicação da MICA..... 51

PUC-Rio - Certificação Digital Nº 1812441/CA

PUC-Rio - Certificação Digital Nº 1812441/CA

Versos do Prisioneiro

Você
tem que aprender
a respeitar a vida humana, disse o juiz.

Parecia justo.

Mas o juiz
não sabia que, para muitos,
a vida não é humana.

O prisioneiro retorquiu:
Há muito me demiti de ser pessoa.

E proferiu, por fim:
um dia,
a nossa vida será, enfim,
viva e nossa.

COUTO, Mia. Poemas escolhidos/ Mia Couto. Apresentação José Castello – 1º ed. – São Paulo: Companhia das Letras, 2016, p. 50.

A certeza de ser punido é o que deve desviar o homem do crime e não mais o abominável teatro; a mecânica exemplar da punição muda as engrenagens. Por essa razão, a justiça não mais assume publicamente a parte da violência que está ligada a seu exercício.

FOUCAULT, Michel. Vigiar e Punir. 40 ed. Petrópolis: Vozes, 2012, p.14

1.
Introdução

Nos últimos anos, a França tem sido palco recorrente de atentados terroristas. Segundo a base de dados sobre terrorismo global da Universidade de Maryland, entre 2006 e 2016 o número de incidentes registrados foi de 289[1]. Em 30 anos, o país aprovou mais de 20 legislações antiterrorismo (CHOUZENOUX, 2016, p.11). Após os atentados à revista *Charlie Hebdo*, em janeiro de 2015, e os ataques em novembro do mesmo ano em Paris, as medidas anunciadas no contexto da declaração do estado de emergência foram posteriormente incorporadas ao Estado de Direito através do "Pacote de Lei sobre a Vigilância" e da "Lei Antiterrorista" de 2017. Tais instrumentos propunham o fortalecimento da segurança interna e o combate ao terrorismo sob uma lógica de antecipação do risco, com técnicas de vigilância e controle informadas por dados e metadados. Nesse processo, novos e amplos poderes foram concedidos à inteligência e a polícia, o que se tornou um "novo normal"[2].

Diante desse quadro, este artigo busca compreender os efeitos do crescente uso de tecnologias computacionais – notadamente, algoritmos – em medidas antiterrorismo na França. A análise explora uma dimensão específica dessa dinâmica, o impacto de tais medidas sobre processos de responsabilização. Com efeito, a prevenção ao terrorismo passou a autorizar o acesso discricionário dos serviços de inteligência e das forças policiais da França a computadores, cookies e metadados, enfraquecendo o escrutínio judicial sobre como esses recursos são usados[3].

PUC-Rio - Certificação Digital Nº 1812441/CA

[1] University of Maryland. *Global Terrorism Database: France.* June 2017. Disponível em: http://www.start.umd.edu/gtd/search/Results.aspx?search=France&sa.x=0&sa.y=0&sa=Search. Acesso: 09 de junho de 2019.

[2] Human Right Watch. France abuses under state of emergency (2016). Disponível em :https://www.hrw.org/news/2016/02/03/france-abuses-under-state-emergency. Acesso 05 de maio de 2019.

[3] Anistia Internacional (2018). "Punished without trial: the use of administrative control measures in the context of counter-terrorism in France". Disponível em: https://www.amnesty.org/download/Documents/EUR2193492018ENGLISH.PDF. Acesso em: 09 de julho de 2019.

Um exemplo desse movimento é a autorização de medidas administrativas individuais de controle e vigilância sem a necessidade de um mandado judicial[4]. O motivo para autorizar e legitimar essas medidas é amplo e vago: baseia-se na alegação de que os profissionais de segurança possuem "razões para acreditar" que uma pessoa ou um grupo está envolvido em uma atividade terrorista. Por sua vez, a legitimação de tais práticas está discursivamente ancorada em dados e evidências dos serviços de inteligência[5] que possuem caráter sigiloso. O Tribunal Europeu de Direitos do Homem (CEDH) alertou repetidamente o governo francês sobre o controle de suas técnicas de vigilância, consideradas como não responsivas à proteção dos direitos individuais[6].

Os processos de normalização de práticas emergenciais foram acompanhados da ampliação do investimento, por parte do governo francês, em novas tecnologias de processamento de dados para a vigilância e o policiamento dos perfis entendidos como um risco à segurança do país (KUBLER, 2017). A "Startup Nation"[7] – termo defendido pelo presidente francês – busca remodelar as burocracias e processos de tomadas de decisão em torno da necessidade de produzir grandes volumes de dados, além de torná-los acessíveis e utilizáveis, mantendo sua integridade e os acompanhando de potentes ferramentas de processamento de dados.

A política de segurança é uma política de conhecimento, ou seja, uma forma de instituir um regime de verdade ao determinar o que temer (HUYSMANS, 2006), e, nas práticas contemporâneas, a utilização de tecnologias computacionais tem sido uma fonte de autoridade e objetividade técnica (MARTIN, 2018). Em meio a uma ampla difusão da análise de dados e da triagem automatizada em contextos de segurança, a questão de como as decisões são tomadas na interface entre humanos

PUC-Rio - Certificação Digital Nº 1812441/CA

[4] As prisões domiciliares podem ser acompanhadas da obrigação de se apresentar uma vez por dia às unidades policiais ou gendarmaries e podem ser renovadas por três meses, se forem apresentadas informações novas ou adicionais (dentro de um limite de 12 meses). A pessoa pode estar isenta desta obrigação diária de relatar se concordar em ser colocada sob vigilância eletrônica.

[5] Como aponta Bonelli e Bigo (2019, p.103), o valor simbólico dos dados de inteligência depende menos de seu conteúdo do que de quem produziu, em que contexto e por quais razões.

[6] La Qradrature du Net (2016). Legal action against the French Surveillance Law. Disponível em: https://www.laquadrature.net/en/2016/05/11/surveillance-law-before-french-council-of-state/. Acesso 20 de dezembro de 2019.

[7] The New York Times (2018). Macron Vowed to Make France a 'Start-Up Nation.' Is It Getting There? Disponível em: https://www.nytimes.com/2018/05/23/business/emmanuel-macron-france-technology.html. Acesso 27 de dezembro de 2019.

e processos algorítmicos[8] se torna premente. O caráter antecipatório do saber algorítmico é notável em seus efeitos de poder. A evidência "supostamente revelada pela análise e correlação[9] de dados não tem pretensão de ser uma prova *ex post facto*, mas um meio de legitimação para agir antes do fato (BRUNO, 2016, p.34). Assim, diferente de medidas preventivas, a lógica pré-crime opera por meio de medidas que ligam a ação do Estado à suspeita sem a necessidade de acusação ou condenação (MCCULLOCH; PICKERING, 2009, p.2-3). Estabelece-se uma lógica punitiva *a priori*. Nesse contexto, o que significa pleitear o cálculo da segurança em uma lógica punitiva antecipatória e no espaço de futuros incertos e incalculáveis? A mensuração do risco e o policiamento através dos dados – uma forma de "proteger com algoritmos" (AMOORE, 2009) – seriam modos de reorientar a relação com a certeza, pois estão ancorados na credibilidade da produção de evidências através de métodos computacionais.

A questão que guia este artigo é: como o uso crescente dos algoritmos para a produção de conhecimento de segurança na França desafia processos de responsabilização? O objetivo aqui é analisar o que está em jogo na mobilização de dispositivos de controle administrativo em termos de processos de validação de autoridade e dispersão dos processos de responsabilização. Para tal, recorrerei ao caso específico das medidas administrativas de controle e vigilância (MICA, sigla em francês), no contexto do combate ao terrorismo na França. Apesar da pesquisa olhar para o uso de tecnologias em práticas de segurança na França, esse não é um fenômeno específico francês. Isso porque o uso de dados e tecnologias nas práticas de segurança têm se ampliado ao redor do mundo, justificado pela necessidade urgente de antecipar ataques terroristas e possíveis ameaças a ordem. Portanto, a proposta é contribuir com insights e ferramentas analíticas para análise das dinâmicas de responsabilização em práticas de segurança mediadas por tecnologias.

PUC-Rio - Certificação Digital Nº 1812441/CA

[8] Segundo a definição formal de Hill (2015, p.47), um algoritmo é uma construção matemática com "uma estrutura de controle composta finita, abstrata e eficaz, dada imperativamente, cumprindo um propósito determinado sob determinadas disposições". Entretanto, nossa investigação não se limitará a algoritmos como construções matemáticas. Como sugerido pela inclusão de "propósito" e "provisões" na definição de Hill, os algoritmos devem ser implementados e executados para que possam agir e ter efeitos. Assim, eles possuem forma ontológica própria de visualizar, mensurar, conhecer, ou calcular ações e fenômenos futuros (entendido como uma soma de várias incertezas).

[9] A correlação indica a interdependência entre duas ou mais variáveis. É importante pontuar que uma correlação não implica que x "causa" y, ou seja, uma correlação não implica causalidade.

Por isso, pretendo investigar o que as "soluções tecnológicas" para a governança da segurança tornam possíveis.

Essa empreitada mobiliza uma reflexão sobre a responsabilização no entrelaçamento de humanos e algoritmos nas práticas de antecipação de perfis "terroristas" na França. O termo responsabilização é utilizado nos estudos de governamentalidade[10] para refletir sobre os processos de atribuição de responsabilidade aos indivíduos por uma ação que anteriormente teria sido dever de outrem – geralmente uma agência estatal (MATZNER, 2016, p.277). Há aí uma demarcação dos limites da escolha individual "responsável", através de uma produção de conhecimento sobre técnicas e mentalidades adequadas para o gerenciamento de risco (DEAN, 1999, p.191). Esse processo reforça a responsabilidade dos indivíduos pelo risco que sua ação pode produzir. Aqui, entenderei "responsabilização" através da observação das camadas de processos e práticas, olhando para "quando" a ação se tornou possível, e não apenas para a imputação da responsabilidade de maneira individualizada. Nesse sentido, a atribuição da responsabilidade a coisas (como algoritmos), desenvolvida pela narrativa específica da visão através dos dados como uma prática sócio-epistêmica (RUPPERT et. al., 2017), desafia as atribuições tradicionais (individualizadoras) de responsabilidade. Dito de outro modo, o recurso a tais tecnologias computacionais difunde a responsabilidade em camadas de processos e práticas para além dos espaços convencionais do humano e dificulta a rastreabilidade desses processos.

Para engajar com as inquietações que constituem esta pesquisa, opto por uma abordagem sociológica que combina o método de Ian Hacking de *estilos de pensar e fazer*[11] e a lógica da prática de inspiração bourdieusiana[12]. Aqui, daremos centralidade às práticas e como elas estão inseridas em um raciocínio mais amplo

[10] Os estudos de governamentalidade, inspirados pelos cursos de Foucault intitulados "Segurança, Território e População" (1977-1978) e o "Nascimento da Biopolítica" (1978-1979), chamam a atenção para as complexas relações entre pensamento e o modo de governar (LARNER; WALTERS, 2004).

[11] O estilo de pensar e fazer que Hacking resgata de Crombie é historicamente enraizado em práticas dos séculos XVI e XVII quando começaram as tentativas de mensuração estatística dos sujeitos (HACKING, 2006), mas é possível, segundo Rocha de Siqueira (2014), problematizar como o pensamento estatístico vai se reinventar através das novas técnicas e tecnologias.

[12] Essa junção de métodos foi inspirada pela contribuição metodológica da professora Isabel Rocha de Siqueira em sua tese de doutorado: *"Measuring and Mananging 'fragile states': quantification and power"* (2014).

PUC-Rio - Certificação Digital Nº 1812441/CA

de estilo de *pensar e fazer,* o próprio meio pelos quais o aparato burocrático se torna uma realidade política. As práticas são generativas, criam significados, entidades e relações de poder (LEANDER, 2011, p.18). Assim, a busca pela prevenção da "desordem" por meio da mensuração, classificação e criação de "perfis perigosos" não será interpretada meramente como um conjunto de técnicas: tais práticas respondem a uma racionalidade entendida como "eficiente" do pensar estatístico na gestão da insegurança. Segundo Hacking (2012, p.601-5), os *estilos* são utilizados de maneira que se tornam padrões por uma "boa razão" – porque funcionam, não porque são "bons".

O trabalho está dividido em três movimentos analíticos centrais. Primeiro, analisarei a consubstanciação de uma arquitetura institucional e normativa que consolida o monopólio da supervisão em benefício dos serviços de inteligência. Como veremos, o aumento da regulação das práticas de inteligência coincide com a expansão das margens de excesso nas práticas desses serviços, como a coleta indiscriminada de metadados. Analisarei como a prática de construção de "perfis suspeitos" através dos algoritmos veio a ser afirmada como uma necessidade para lidar com as contingências e incertezas na França face à ameaça do terrorismo e da radicalização. Isso porque a criação dos perfis terroristas se baseia em critérios de risco que priorizam a probabilidade, em detrimento da especificidade.

Em seguida, discutirei as condições de possibilidade do uso de algoritmos na produção de conhecimento de inteligência, em particular na produção de "evidências" que informam as medidas individuais de controle e vigilância. A proposta é analisar as conexões entre, de um lado, práticas de mensuração do perigo em um discurso técnico ancorado no imperativo da eficiência das práticas de vigilância; de outro, os efeitos de controle sobre os indivíduos com a flexibilização de salvaguardas processuais e garantias de direitos.

O terceiro movimento terá seu ponto de gravidade nas camadas de práticas humanas e não humanas presentes nas medidas de controle e vigilância para entender seus efeitos sobre processos de responsabilização. Para tal, analisarei a relação entre a produção de conhecimento e a promulgação do não-conhecimento, através do sigilo e incerteza, nos processos de contestação das medidas individuais de controle e vigilância na França. O enquadramento dos algoritmos como

PUC-Rio - Certificação Digital Nº 1812441/CA

otimizadores das práticas de inteligência (MARTIN, 2018) adquire, nesse contexto, indiscutível relevância. Todavia, esse aumento de eficiência, "objetividade" e regulação coincide com as margens para excessos das práticas de inteligência.

Reforço a argumentação de uma ampla gama de autores críticos de que os algoritmos não são expressões neutras e imparciais de conhecimento: seu trabalho não é impassível e apolítico (DIAKOPOULOS, 2013; SEAVER, 2013; AMOORE, 2009, 2011; KITCHIN; DOGGE, 2011, ARADAU; BLAKE, 2015, BRUNO, 2016; ROUVROY; BERNS, 2018). Os algoritmos pesquisam, agrupam, classificam, combinam, analisam, perfilam, modelam, simulam, visualizam e regulam pessoas, processos e espaços. Eles moldam a forma como entendemos o mundo e eles mesmos produzem o mundo através de sua execução como software, com profundas consequências (KICHIN; DODGE, 2011). Os próprios modos de visualização algorítmica operam sintetizando a multiplicidade de caminhos em uma única saída que é acionável ao analista de segurança. Os algoritmos funcionam como um meio de direcionar e, de certo modo, disciplinar a atenção, concentrando-se em pontos particulares que produzem um conjunto reconhecível. Se os dados de um indivíduo são entendidos com probabilidade de pertencer a um terrorista ou radicalizado, por exemplo, só pela probabilidade ele já é visto como tal. O processo de classificar tipos de pessoas é um processo, no entanto de produzir/ inventar pessoas ("making up people") (HACKING, 2006), e a escolha do "rótulo" tem consequências. Quem é rotulado por quem, e a maneira como as classificações são aplicadas têm poderosas repercussões sociais.

Diante desse quadro, o trabalho visa contribuir com os debates dos estudos críticos sobre dados (KITCHIN, 2014) e as abordagens críticas de segurança e vigilância. Em especial, sobre a governança da segurança a partir da produção de conhecimento algorítmico, entendendo o algoritmo como uma peça em um quebra-cabeça mais amplo das práticas de gestão do "perigo". Além de oferecer uma análise crítica sobre as transformações tecnológica das práticas de profissionais de segurança. Proponho levar a sério as múltiplas facetas das transformações sociais e políticas que implicam a proliferação e o aumento do uso de dados nas práticas de

PUC-Rio - Certificação Digital Nº 1812441/CA

segurança. Segundo o relatório da International Data Corporate (IDC) de 2018[13], há uma estimativa de aumento exponencial dos dados em 2020 (44 vezes maior que o ano anterior), atingindo 35 zetabytes[14], e em 2025 de 175 zetabytes de dados novos serão criados em todo o mundo. Essa dinâmica tem implicações de longo alcance para a privacidade e a proteção de dados, assim como, com as liberdades civis e os direitos humanos (BAUMAN et al., 2015).

PUC-Rio - Certificação Digital Nº 1812441/CA

[13] IDC (2018). Data Age 2025. The Digitalization of the World: From de Edge to Core. Disponível em: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf. Acesso 10 de fevereiro de 2020.

[14] O zettabyte é um múltiplo de byte que é a unidade para informações digitais. O prefixo zetta indica multiplicação pela sétima potência de 1000 no Sistema Internacional de Unidades. Essa unidade é utilizada para mensuração da capacidade tecnológica de armazenagem de dados a nível mundial.

2.
Arquitetura vigilante: novos meios técnicos e tecnológicos nas práticas de inteligência

> Na luta contra o terrorismo, só pode haver uma escola: a de vigilância constante, a de rigor constante, a de melhoria contínua. Como a ameaça é difusa e móvel, nosso sistema de detecção, obstrução, repressão e proteção deve confiar em todos os serviços, desde o topo de nosso aparato de inteligência até a polícia e os gendarmes do setor. Eles têm que usar todas as ferramentas, as mais modernas técnicas de inteligência, os métodos de criação de perfil mais sistemáticos, mas também a vigilância de cada um. Em face da ameaça terrorista, todo o poder do Estado deve ser mobilizado. Nada deve ser deixado de fora[15]. (Discurso de Edwar Philip, Primeiro Ministro da França na apresentação do plano de ação contra o terrorismo em 13 de julho de 2018).

Na luta contra a contingência e incerteza na "guerra ao terror", lidando com a imprevisibilidade de eventos de baixa probabilidade, mas de alto impacto – como ataques terroristas (ARADAU; VAN MUNSTER, 2007, p.93) –, as agências de segurança se esforçam cada vez mais para detectar um possível futuro, a fim de mitigar probabilidades da ocorrência de novos ataques. O monitoramento de atividades futuras se tornou prática rotineira de diversas agências de inteligência, cujo o papel é antecipar determinados comportamentos considerados nocivos, ilegais, indesejáveis ou simplesmente indesejados.

Como argumentam Aradau e Van Munster (2007), o enquadramento do terrorismo como um desconhecido radical, como um risco que não pode ser antecipado racionalmente, tornou obsoleto o cálculo racional do seguro de risco e justificou medidas excepcionais e vigilância generalizada em nome do princípio da precaução, caracterizado por uma preocupação com risco zero. Essa mudança, segundo esses autores, culminou em dois efeitos principais nas práticas de conhecimento. Primeiro, através da implantação das práticas de pior cenário, nas quais o uso da especulação foi incentivado como complemento da modalidade de

[15] "Dans la lutte contre le terrorisme, il ne peut y avoir qu'une seule école: celle de la vigilance constante, celle de la rigueur constante, celle de l'amélioration continue. La menace étant diffuse et mobile, notre système de détection, d'obstruction, de répression et de protection doit s'appuyer sur tous les services, du sommet de notre appareil de renseignement à la police et aux gendarmes de l'industrie. Ils doivent utiliser tous les outils, les techniques de renseignement les plus modernes, les méthodes de profilage les plus systématiques, mais aussi la vigilance de chacun. Face à la menace terroriste, tout le pouvoir de l'Etat doit être mobilisé. Rien ne doit être laissé de côté" Discurso de Edwar Philip, Primeiro Ministro na apresentação do plano de ação contra o terrorismo em 13 de julho de 2018. Disponível em: https://www.gouvernement.fr/partage/10395-presentation-du-plan-d-action-contre-le-terrorisme-levallois-perret. Acesso: 24 de abril de 2019.

PUC-Rio - Certificação Digital Nº 1812441/CA

cálculo de antecipação (DE GOEDE, 2008), com a transferência do ônus da prova do Estado para suspeitos de terrorismo à luz de possíveis danos graves e irreversíveis (ARADAU; VAN MUNSTER, 2007, p.103). Segundo, o princípio da antecipação justificou o uso mais amplo possível das tecnologias de vigilância na coleta de dados de diferentes aspectos da vida cotidiana (Ibid., p. 91).

Essa transformação obscurece a linha entre as práticas de inteligência e a consubstanciação de evidência, ponto central para a análise aqui desenvolvida. Isso porque tem se tornado cada vez mais frequente a aceitação de dados de inteligência como evidências em tribunais e para uma ampla gama de práticas administrativas, que De Goede (2008, p.163) define como um campo extralegal de intervenção. Neste, os juízes perderam o monopólio para determinar a promulgação de medidas coercitivas de detenção, interrogatório, monitoramento e congelamento de bens: agora, compartilham essa autoridade com profissionais de segurança que são mantidos em um padrão muito mais flexível de prestação de contas (BIGO, 2006; BONELLI; RAGAZZI, 2014).

Nesta seção, analiso as práticas contraterroristas de produção de perfis através de dados como práticas sociais dos atores que os constituem. Hacking (2006) distinguiu seu conceito de *pensar e fazer* dos estilos de *raciocínio científico* de Crombie (1994), vinculando-o à questão da prática (ROCHA DE SIQUEIRA, 2014). O autor argumenta que a própria palavra *raciocínio* está relacionada ao pensamento e não "invoca suficientemente a mão manipuladora e o olhar atento" (HACKING, 2006, p.181). Os estilos de raciocínio expressos em estratégias públicas, documentos oficiais e memorandos não são suficientes para compreender as práticas burocráticas que os promulgam. Como apontou Bourdieu (1983), o raciocínio não existe fora do sentido prático dos atores: ele é modelado em sua prática e a modela. Nesse sentido, rejeito tanto a noção de determinismo tecnológico, quanto a proposição de que as tecnologias são externas aos processos e práticas sociais.

Para analisar *estilos de pensar e fazer,* é preciso entender como os agentes usam a tecnologia junto a outros recursos. Por isso, procurarei entender os processos e práticas no campo das agências francesas de inteligência que criaram condições de possibilidade tanto para a estruturação de uma arquitetura de

PUC-Rio - Certificação Digital Nº 1812441/CA

vigilância técnica e centralizada, quanto para a normalização das práticas de vigilância.

2.1.
A Lei de Inteligência e a emergência de uma comunidade de vigilância na França

Desde os ataques terroristas de 11 de setembro de 2001, há um contínuo processo de centralização e normalização das atividades de inteligência (BONELLI, 2008)[16]. Nesta seção, analisarei tais processos para compreender como se constitui uma arquitetura institucional e normativa de vigilância na França.

Desde 1984, a França apresenta um centro de coordenação e integração analítica de inteligência: a Unidade de Coordenação da Luta Anti-terrorista (UCLAT, sigla em francês). Segundo Shapiro e Susan (2003, p. 76-77), o objetivo da UCLAT tem sido estabelecer conexões entre todos os serviços de inteligência e policiais da França. No campo da inteligência, a UCLAT tinha a tarefa de lidar com o atrito entre a Direção Geral da Segurança Externa (DGSE), a Direção de Inteligência do Território (DST – sigla em francês), a Direção Central de Vigilância Geral (DCRG, sigla em francês), a Direção do Exército Militar (DRM, sigla em francês) e a Direção da Proteção e Segurança da Defesa (DPSD, sigla em francês). Nesse sentido, a inteligência francesa poderia ser caracterizada como uma "casa dividida" (CHOPIN, 2017, p. 12) – um campo de "luta de tribos desorganizadas" (BONELLI, 2008).

Em 2004, um órgão permanente das ações contraterrorismo foi instalado no DGSE para o trabalho coordenado interagências, uma cooperação entre agentes do DGSE, DST e DCRG. Aqui, já adquiria densidade a leitura de que as divisões entre segurança externa (objetivo do DGSE e DCRG) e interna (objetivo DST) impediam um desempenho eficaz da inteligência francesa. A natureza das atividades do órgão foi apresentada como "operacional", em contraste com as funções administrativas da UCLAT de garantir o compartilhamento de informações e integrar a análise de ameaças. Segundo Bonelli (2018), essa aparente duplicação da UCLAT foi vista com desconfiança, pois ampliaria a centralização do controle executivo sobre as

[16] Para uma discussão sobre um processo semelhante em países anglo-saxões, ver: Shapiro; Suzan, 2003.

PUC-Rio - Certificação Digital Nº 1812441/CA

atividades que tradicionalmente estavam sob a autoridade do Ministério do Interior – ou seja, sob a responsabilidade do parlamento. No mesmo ano, o Legislativo avançou em seus próprios esforços de centralização com a criação do Conselho de Inteligência Interior (CRI, sigla em francês). O CRI e o órgão operacional do DGSE foram reorganizados e fundidos, dando origem ao Conselho de Defesa e Segurança Nacional (CDSN, sigla em francês) em 2007. Assim, tanto os esforços de centralização da inteligência do Executivo quanto do Legislativo foram sintetizados. Sob autoridade presidencial, o CDSN foi criado para romper a divisão externa-doméstica em segurança (BONELLI, 2008). Em um ímpeto interinstitucional, o CDSN assumiu a responsabilidade pelas questões de segurança nacional, segurança pública e questões internacionais e de defesa da França.

Com a publicação do Livro Branco de Defesa Nacional (2008) durante o governo Sarkozy, há a primeira menção oficial a uma Comunidade de Inteligência Francesa (CIF)[17]. Esse processo de centralização institucional é também marcado pela normalização dos serviços de inteligência (BONELLI, 2008). Com efeito, o Livro Branco cuidou de declarar oficialmente o fornecimento de uma base legal para a realização de atividades de inteligência, sob aprovação do parlamento. Mais precisamente, indicou que "uma definição estatutária das missões dos serviços de inteligência será dada por lei" (HAYEZ, 2010, p.481) – o que posteriormente veio a ser consolidado pela Lei de Inteligência.

Os processos pelos quais ocorre uma centralização dos dados e uma ampliação da coleta e compilação destes também são centrais aqui, uma vez que os dados são estruturados e estruturantes de práticas nas quais diversos agentes e seus interesses produzem formas de interpretação e métodos que operam em circuitos de conhecimento de práticas de segurança. Segundo Ruppert et al. (2017), dados são um objeto investido de poderes particulares, influência e racionalidade. A "política de dados" pode ser compreendida como um campo de poder e conhecimento (RUPPERT et al., 2017, p.2). No caso da França, a ampliação dos bancos de dados

[17] THE FRENCH WHITE PAPER ON DEFENCE AND NATIONAL SECURITY (2008). Disponível em: http://www.mocr.army.cz/images/Bilakniha/ZSD/French%20White%20Paper%20on%20Defence%20and%20National%20Security%202008.pdf. Acesso 22 de dezembro de 2019.

PUC-Rio - Certificação Digital Nº 1812441/CA

desde a década de 1990[18] se deu em meio a uma série de disputas entre os agentes que mobilizam seus recursos. Em um relatório de 2018, publicado pelos deputados Didier Paris e Pierre Morel-A-L'Huissier, observa-se a multiplicação de arquivos de inteligência: atualmente, existem 106 arquivos "disponibilizados para os serviços de segurança" contra 58 em 2009. A interpretação desses arquivos e de dados coletados pelos mecanismos de vigilância informam a produção de perfis pelos algoritmos – que, por sua vez, apoiam a produção de listas de "sujeitos perigosos", tais como o Arquivo de Relatório de Terrorismo e Prevenção ao Terrorismo e os Arquivos S[19]. A produção de listas envolve o desenvolvimento de um "*conhecimento sistemático geral e preciso"* suficiente para prever comportamentos e possibilitar uma intervenção efetiva (HACKING, 1995, p.352, minha ênfase). O saber que emerge da compilação dos dados e através dela aparece como 'verdade real', imparcial e indubitável dos traços deixados pelos indivíduos.

Em 2016, o Decreto Nº 2016-1460 autorizou a centralização de dados da população francesa no arquivo chamado "Security Eletronic Titles" (TES) – um sistema de tratamento de dados pessoais[20]. A quantidade de dados fornecidos por grandes corporações de tecnologia à inteligência e a polícia francesa nos últimos anos também aumentou. Isso ocorreu tanto por meio da criação de um "grupo de contato" entre essas grandes corporações e o Ministério do Interior em 2015 (CASSINI, 2015) como pela Lei de Vigilância, que estipula obrigações de informações aos provedores de telecomunicações e hospedagem web não só em relação aos dados, mas também aos metadados. Na primeira metade de 2013, a Google recebeu 2.011 solicitações de autoridades francesas e cumpriu 49% delas; enquanto o Facebook recebeu 1.547 solicitações e cumpriu 39% destas. Já no primeiro semestre de 2017, a Google recebeu 5.661 solicitações, tendo atendido a

PUC-Rio - Certificação Digital Nº 1812441/CA

[18] Le Monde (2018). Des fichiers de police mal organisés et trop complexes. Disponível em: https://www.lemonde.fr/police-justice/article/2018/10/17/des-fichiers-de-police-mal-organises-et-trop-complexes_5370869_1653578.html. Acesso em 10 de junho de 2019.

[19] A lista remonta à década de 1960, durante a Guerra Fria, tornou possível acompanhar os movimentos dos diplomatas dos países orientais, mas também de sua comitiva. A maioria dos cartões S é produzida pela DGSI. Um plug S tem uma vida útil de um ano e pode ser renovado. É subdividido em diferentes níveis, criptografados de S1 a S16, mas eles não correspondem a níveis de periculosidade. Disponível em: France Culture (2018). https://www.franceculture.fr/droit-justice/les-fichiers-de-police-et-de-renseignement-sont-ils-trop-nombreux; Le Monde (2018) https://www.lemonde.fr/les-decodeurs/article/2015/11/17/attentats-du-13-novembre-qu-est-ce-qu-une-fiche-s_4811500_4355770.html. Acesso em 10 de junho de 2019.

[20] Trata-se da coleta de todos os dados necessários para estabelecer os documentos oficiais: sobrenome, nome, cor dos olhos, foto facial, dados biométricos e informações sobre a nacionalidade dos pais.

63%; e o Facebook, 4.700 solicitações, com 74% delas cumpridas (TRÉGUER, 2019, p.9). Para além dessas obrigações, os provedores de telecomunicações e prestadores de hospedagem que possuem serviços de criptografia devem fornecer dentro de 72 horas após a solicitações dos agentes autorizados as chaves que permitam descriptografar os dados (art. L. 871-1 do Código Francês de Segurança Interna). A criptografia pode ser entendida como um tipo de "obstrução", tornando os dados não legíveis aos mecanismos tecnológicos de análise, mas por outro lado pode ser uma garantia de privacidade dos dados[21].

No período sobre o qual estamos nos debruçando, a França ainda expandiu os poderes de vigilância de suas agências por meio de um novo aparato legislativo (TRÉGUER, 2019, p.9) e criou a Comissão Nacional para o Controle de Técnicas de Inteligência. Com isso, as operações de vigilância conduzidas por serviços de inteligência passam a ser submetidas a uma maior regulação e um maior controle. Principalmente desde a Lei Nº 86-1020 de 9 de setembro de 1986 – e em sua expansão em 1995 e 1996 –, o combate ao terrorismo na França por meio da atividade de inteligência foi marcado por um fenômeno de *judicialização*. Em outras palavras, desde a implementação dessa lei ao final do século XX, a missão de contraterrorismo da inteligência francesa esteve fortemente aliada ao sistema judiciário do país (BONELLI, 2008). Ao mesmo tempo, os serviços já estabelecidos de inteligência doméstica e estrangeira continuaram a exercer suas atividades em estreita cooperação com forças policiais (Ibid.).

Em julho de 2015, o Parlamento francês aprovou a Lei de Inteligência. Embora a tramitação do projeto de Lei ter sido acelerada após os ataques ao *Charlie Hebdo*, sua gestação data de 2013 (CHOPIN, 2016, p. 72). O objetivo da Lei é fornecer uma estrutura legal clara para os serviços de inteligência autorizados a usar certos meios técnicos de acesso às informações. A Lei cria novas seções no CFSI e amplia os âmbitos de propósitos de interesse público para os quais o uso de tecnologias de vigilância é autorizada. As práticas de vigilância só podem ser exercidas de acordo com os seguintes propósitos: (1) independência nacional, integridade territorial e defesa nacional; (2) interesse de política externa, execução de tratados com a União Europeia e prevenção de qualquer interferência externa;

[21] Disponível em: http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html?_r=1 . Acesso em 02 de outubro de 2019

PUC-Rio - Certificação Digital Nº 1812441/CA

(3) maior interesse econômico, industrial ou científico francês; (4) prevenção ao terrorismo; (5) prevenir ameaças à ordem pública; (6) prevenir o crime organizado; e (7) prevenção contra a proliferação de armas de destruição em massa[22]. Como podemos observar, os objetivos de vigilância da inteligência francesa incluem não apenas contraterrorismo, crime organizado e contraespionagem, mas também uma noção ampla e vaga de preservação da ordem pública.

Dada essa natureza abrangente das disposições contidas na Lei, a Federação Internacional dos Direitos Humanos (FIDH) alegou que o ataque a *Charlie Hebdo* "legitimou uma lei que certamente teria sido difícil de obter aprovação em outro contexto" (FIDH, 2016, p.27). Certamente, os discursos securitários após os ataques proporcionaram uma oportunidade para a introdução de uma legislação que servisse para legalizar – e ampliar – vigilância intrusiva que já estava sendo realizada "ilegalmente" por serviços de inteligência franceses (HAMILTON; BERLUSCONI, 2018). Lançado em 2008, o programa de vigilância em grande escala da França carecia de base jurídica válida (CHARDEL et al., 2016; TRÉGUER, 2017). Em seu parecer sobre a Lei, a Autoridade Francesa de Proteção de Dados (CNIL, sigla em francês) reconhece que as violações aos direitos de privacidade podem ser justificadas com respeito à legitimidade da meta e dos interesses em jogo e lembra que essas violações devem ser limitadas ao estritamente necessário, adequadas e proporcionais aos objetivos, ao mesmo tempo em que destaca que salvaguardas e controles apropriados devem estar em vigor[23].

A Lei de Inteligência reforça as condições para o uso e preservação dos dados coletados, assim como para a rastreabilidade e o monitoramento das medidas de vigilância. Para além disso, avança ainda mais na monopolização da supervisão de práticas de vigilância em benefício dos serviços de inteligência. Nesse sentido, a Lei confere aos serviços de inteligência uma investidura legal para a implantação autônoma de técnicas de vigilância que até então eram de competência exclusiva

[22] FRANCE. Law no 2015-912 of 24 July 2015 related to intelligence – Exposé des motifs. Disponível em: http://www.legifrance.gouv.fr/affichLoiPubliee.do;jsessionid=AC82D0703DA2374DEF16BEA404A88989.tpdila23v_3?idDocument=JORFDOLE000030375694&type=expose&typeLoi=&legislature=14. Acesso 10 de outubro de 2019.

[23] Opinion no2015-078 of 5 March 2015 on intelligence bill (Délibération no2015-078 du 5 mars 2015 portant avis sur un projet de loi relative au renseignement. Disponível em: http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/D2015-078-PJLRenseignement.pdf . Acesso em 3 de outubro de 2019.

PUC-Rio - Certificação Digital Nº 1812441/CA

do Judiciário (MÉGIE; PAWELLA, 2016). Esse processo foi justificado como uma regulação necessária das atividades de inteligência no Estado de Direito, em nome de uma maior eficiência desses serviços. Não surpreende, assim, que 22 Estados da União Europeia tenham reformado sua legislação-quadro de inteligência nos últimos anos.

Esse processo de regulação das atividades de inteligência ganhou relevo na França com a criação da Comissão Nacional para o Controle de Técnicas de Inteligência (CNCTR, sigla em francês)[24]. Isso porque, com a aprovação da Lei de Inteligência, as operações das agências de inteligência exigem uma autorização do Primeiro Ministro, que é entregue após parecer da CNCTR. As opiniões da Comissão não são vinculantes (Artigo L. 821-4 do CFSI), e a autorização é válida por um período máximo de quatro meses. Em casos de emergência e apenas para três finalidades limitadas (prevenção do terrorismo, salvaguarda da integridade do território nacional e prevenção de ameaças imediatas), o Primeiro Ministro pode emitir uma autorização sem opinião prévia da CNCTR. O pedido de autorização deve ser escrito e estabelecidos certos detalhes, incluindo as diferentes técnicas a serem adotadas, os objetivos da coleta de dados e a duração da autorização. A CNCTR, que é uma agência administrativa independente, pode emitir uma recomendação a qualquer momento para a inteligência, técnicas a serem interrompidas e os dados coletados destruídos. Também pode se referir ao Conselho de Estado como um último recurso (Artigo L. 833-8 do CFSI). Como essas disposições são consideradas dentro do escopo da administração, elas não exigem autorização prévia de um juiz judicial, mas os indivíduos têm direitos a interpor recurso *a posteriori*. É interessante pontuar que a CNCTR tem uma ação de controle contínuo, na qual emite uma opinião antes da autorização de uma técnica de inteligência, e possui um controle estendido *a posteriori* e poderes de monitoramento para verificar se nenhuma técnica de informação foi implementada ilegalmente (de acordo com os nove objetivos legais a que os serviços de inteligência devem se referir). O órgão garante a confidencialidade das solicitações feitas pelo poder executivo, enquanto exerce controle sobre sua eficácia e proporcionalidade.

[24] A CNCTR é composta por quatro magistrados, quatro parlamentares e um especialista em comunicações eletrônicas.

PUC-Rio - Certificação Digital Nº 1812441/CA

O escopo do controle da Comissão diz respeito às técnicas de inteligência destinadas *a monitorar o território nacional*, o que leva a conhecer o acesso administrativo aos dados de conexão (acesso aos dados da conexão em tempo real por algoritmo, por localização de pessoas objetos, pelos coletores IMSI[25]), interceptações de segurança, captura de fala e imagem em um local privado. De fato, a maior parte das licenças emitidas pela CNCTR está relacionada ao acesso aos dados da conexão em tempo diferido, ou seja, os dados relacionados à identificação dos números de inscrição ou conexão de uma pessoa designada ou à lista de números chamados, os metadados. Isso significa que uma parte principal do controle diz respeito ao acesso às técnicas de conexão à Internet (cujo nome está por trás desse número de telefone), mas não ao conteúdo. O controle da legalidade das solicitações (a CNCTR pode exercer tal técnica), como o controle da motivação, não precisa ser muito desenvolvido em relação às solicitações de acesso aos dados da conexão em tempo diferido. Portanto, a maior parte do controle é feita *a priori.* Nesse sentido, a CNCTR concentra-se em técnicas de vigilância cuja interferência na privacidade é enquadrada como fraca, pois essas provavelmente não são medidas que causam os maiores danos às liberdades individuais. Dito de outra forma, essa técnica seria menos invasiva por não olhar o conteúdo dos dados. Diante da consolidação de uma arquitetura antiterror na França que privilegia a atividade da inteligência, essas técnicas passam a ocupar, cada vez mais, a linha de frente das investigações[26] – enquadrando-as, de um lado, como eficientes, de outro, como menos nocivas à privacidade.

No contexto de luta contra o terrorismo há um aumento no volume dos pedidos de acesso a dados de conexão, interceptação de segurança e captura de dados, associada à urgência da ação. Isso leva ao ponto da adequação dos recursos humanos disponíveis à CNCTR e a capacidade de realizar um exame real da legalidade e da proporcionalidade da técnica de inteligência a implementar mediante ao incremento dos pedidos e a urgência a eles imputada. Uma questão é

[25] Um coletor IMSI é um dispositivo de escuta telefônica usado para interceptar o tráfego e acompanhar o movimento de usuários de telefones celulares. São torres de telefonia "falsas" que atuam entre o celular-alvo e as torres de celulares reais do provedor de serviços. Os coletores de IMSI capturam números internacionais do subscritor móvel (IMSI) e os números de série eletrônicos (ESM) dos telefones móveis desejados. Uma vez que o celular é conectado a esse sistema, ela pode interceptar chamadas e mensagens, além dos metadados.

[26] Em 2016, 20.356 pessoas foram submetidas a técnicas de vigilância, 45% das quais estavam associadas às medidas contra terroristas (CHOPIN, 2017).

PUC-Rio - Certificação Digital Nº 1812441/CA

que a CNCTR pode dar uma opinião favorável às práticas de vigilância não em relação aos elementos submetidos à sua apreciação (natureza da medida e sua proporcionalidade), mas nos objetivos 'urgentes' por trás da solicitação – a saber, a luta contra o terrorismo (CHARDEL et al., 2016).

Um ponto central é que os dados coletados pela inteligência internacional não estão totalmente integrados ao campo de regulação, que por si só já é limitado. À CNCTR, não compete autorizar a interceptação e exploração de comunicações internacionais: sua intervenção nessa área é limitada ao *controle a posteriori.* Assim, perde valor o controle de seu aspecto preventivo – ou seja, o parecer de legalidade e proporcionalidade antes da implementação da ação.

O controle da inteligência é ainda mais enfraquecido pela lei de programação militar, adotada em 13 de julho de 2018, que dá acesso à DGSI (Direção Geral de Inteligência Interior)[27] a dados internacionais capturados pela Defesa, em particular a DGSE, o que abre o caminho para uma exploração mais fácil de todos os dados. Esta lei permite fornecer aos investigadores antiterroristas as informações obtidas pelo DGSE fora das fronteiras nacionais. Desse modo, quando um indivíduo registrado como possível suspeito se comunica eletronicamente com o internacional, o DGSI poderá acessar essas trocas. Esses dados capturados no âmbito internacional passaram às estruturas internas e direcionaram práticas sem atravessar o controle *a priori* – mesmo que consultivo – da CNCTR. Essa isenção de ação é extremamente significativa e ainda mais surpreendente considerando a escala de compartilhamento de dados com parceiros estrangeiros sobre residentes franceses[28].

A legislação apresentada estabelece uma complexa relação entre segurança, liberdade, lei e tecnologia, e é o primeiro marco normativo de supervisão de práticas das agências de inteligência francesas (MÉGIE; PAWELLA, 2016, p.1-2). Contudo, o Tribunal Europeu de Direitos do Homem (CEDH) alertou

[27] Essa agência é fruto da fusão entre duas agências de inteligência doméstica, a DST e a DCRG.
[28] Em agosto de 2013, Le Monde publicou a seguinte citação de uma fonte da DGSI: "Nós intercambiamos o tempo todo com agências estrangeiras, inclusive com interlocutores da DGSE como a NSA americana do GCHQ britânico. Grande parte de nossa inteligência inclui elementos pertencentes aos nossos parceiros; escusado será dizer que não vamos deixar ninguém pousar as mãos". Disponível em: https://www.lemonde.fr/societe/article/2013/08/22/le-renforcement-du-controle-se-heurte-a-la-cooperation-internationale-entre-services_3464714_3224.html . Acesso 05 de janeiro de 2020.

PUC-Rio - Certificação Digital Nº 1812441/CA

repetidamente o governo francês sobre o controle de suas técnicas de vigilância, consideradas como não responsivas à proteção dos direitos individuais. Em setembro de 2018, a La Quadrature du Net, French Data Network, Federation of Associated Internet Access Providers e Igwan.net levaram ao Tribunal de Justiça da União Europeia (TJUE), um processo contra a Lei de Inteligência de 2015. Em especial, o documento apresentado aponta a preservação dos dados de conexão e metadados como pilar da inteligência. A preocupação dessas organizações de defesa da privacidade e agências de telecomunicações é que a lei francesa exige que as operadoras mantenham todas as informações sobre os usuários em cada comunicação. Desde 2015, os ativistas de direitos à privacidade digital, como La Quadrature du Net, têm pedido a manutenção e reafirmação da jurisprudência atual do TJUE que proíbe inequivocamente a retenção generalizada de metadados.

Para as organizações requerentes do pedido à TJUE, não existe um mecanismo para compensar eficaz e suficientemente a ausência de qualquer notificação *ex post*. Os artigos L. 833-4 e L. 841-1 do CFSI preveem que qualquer pessoa possa recorrer à CNCTR ou ao Conselho de Estado para fins de verificar se ele/ ela foi objeto de uma investigação ilegal da inteligência. Contudo, este mecanismo não pode ser considerado para solicitar e obter informações sobre interceptações das autoridades na jurisprudência do Tribunal Europeu dos Direitos do Homem Direitos (TJUE, Tribunal Geral, 4 de dezembro de 2015, Zakharov vs. Rússia, n. 47143/06, § 298).

De fato, a CNCTR, na melhor das hipóteses[29], apenas informa ao requerente a existência ou inexistência de uma ação ilegal no contexto das medidas de inteligência a ele/ ela aplicadas, sem dar acesso a qualquer elemento factual para o exercício do recurso efetivo do reclamante, nem detalhes sobre os dados coletados. Outrossim, no contexto de processos *ex post*, o sigilo da segurança nacional muitas vezes impede uma audiência aberta no Conselho de Estado. O artigo R.773-24, parágrafo 1, do Código de Justiça Administrativa estabelece que:

> Nos casos em que é provável que o processo envolva informações protegidas pelo sigilo da segurança nacional, ou confirme ou refute a implementação de uma medida de inteligência com relação ao reclamante, ou elementos reveladores contidos no processamento de dados,

[29] Em consonância com os artigos L. 773-6 e L. 773-7 do Código de Justiça Administrativa e a decisão do Conselho de Estado.

PUC-Rio - Certificação Digital Nº 1812441/CA

> ou se o reclamante não tiver afetado pela medida, o requerente é convidado a se retirar antes da declaração do parecer do relator público[30].

Essa exclusão pode ser ainda mais problemática tendo em vista que todas as políticas públicas devem contribuir para a segurança nacional, de acordo com o Artigo L. 1111-1 do Código de Defesa francês. Destarte, de acordo com o Decreto de 30 de novembro de 2011 que aprova Instrução Interministerial Geral Nº. 1300 sobre Proteção da Defesa Nacional do Sigilo, *"a proteção do sigilo diz respeito a todos os campos de atividade relacionados à defesa e segurança nacional: política, militar, diplomática, científica, econômica, industrial"*[31]. Nos termos do artigo R. 2311-6 do Código de Defesa, todos os elementos sujeitos a uma medida de classificação são considerados confidenciais por razões de defesa nacional, conforme decidido pelas próprias autoridades administrativas e ministeriais. Isso resulta na possibilidade de que a autoridade pública, ela mesma, exclua completamente certas informações de uma audiência aberta apenas colocando-a sob o selo secreto da segurança nacional.

Um exemplo, disto é que a maioria dos indivíduos entrevistados pela Anistia Internacional (2018) que estão sob medidas individuais de vigilância e controle (MICA) mencionou acreditar que estão no banco de dados dos "Arquivo S". Eles não têm acesso ao banco de dados onde os perfis dos arquivos S são armazenados, e esses indivíduos não têm provas tangíveis de que o Estado mantenha esse arquivo deles. O arquivo S faz parte do principal banco de dados de indivíduos suspeitos de ser uma ameaça potencial à segurança nacional. A presença de um indivíduo neste arquivo permite que as autoridades possuam informações específicas (incluindo motivos para o arquivo S, fotografias, rastreamento de movimentos, entre outros) e que as forças policiais da França e/ ou da UE possam realizar buscas baseadas no fato de que a pessoa está nesta lista. Segundo o Ministério do Interior, havia 25.000 pessoas classificadas no subgrupo da ficha S no final de 2017; 9.700 dos quais estavam lá devido à suspeita de "radicalização" (FRANÇA, 2017). Um indivíduo

[30] "Lorsque le processus est susceptible d'impliquer des informations protégées par le secret de la sécurité nationale, ou de confirmer ou de réfuter la mise en œuvre d'une mesure de renseignement à l'égard du plaignant, ou de révéler des éléments contenus dans le traitement des données, ou si le plaignant n'a pas affecté dans cette mesure, le demandeur est invité à se retirer avant que l'avis du rapporteur public n'ait été déclaré (...)".

[31] "La protection du secret concerne tous les domaines d'activité liés à la défense et à la sécurité nationales: politique, militaire, diplomatique, scientifique, économique, industriel".

PUC-Rio - Certificação Digital Nº 1812441/CA

não é notificado quando está listado neste banco de dados, tendo em vista o selo de sigilo por se tratar de assunto de defesa nacional. Normalmente, apreende-se que eles estão no banco de dados durante uma ação policial, aplicação de uma medida administrativa ou ao tentar viajar para outro país.

É nesse cenário de centralização institucional de dados e das agências de inteligência na França, que são geradas as condições de possibilidade para que as novas tecnologias utilizadas pela inteligência passem a agregar e correlacionar de forma mais "eficiente" diversas informações, culminando na criação de perfis antecipados de terroristas que ancoram as práticas administrativas, como as medidas administrativas de controle e vigilância. Os serviços franceses podem acessar computadores, ler conversas ou solicitar cookies, acessar os metadados e outras medidas, e por razões tão vagas que, potencialmente, abrangem qualquer ação perturbadora para o Estado: são colocadas no mesmo nível a prevenção do terrorismo e a defesa dos "principais interesses econômicos, industriais e científicos da França" ou "ataques à forma republicana de instituições". Assim, a Lei de Inteligência hoje coloca sob vigilância também os movimentos sociais, como as manifestações dos coletes amarelos ou de reivindicações ecológicas.

PUC-Rio - Certificação Digital Nº 1812441/CA

2.2. Metadados, dados, algoritmos e a construção de perfis antecipados de "terroristas" na França

À medida que o policiamento e a inteligência se tornam cada vez mais orientados a dados, baseados em tecnologia e automatizados, os algoritmos desempenham um papel crucial nos meios e métodos de aplicação das leis e da inteligência. Os algoritmos oferecem a promessa de abordar investigações que envolvem processamento de dados complexos, bem como a análise e acumulação de grandes quantidades de dados de fontes heterogêneas e, em particular, a prática de automação e criação de perfis a partir desses dados.

A Lei de Inteligência possibilita que os serviços de inteligência franceses usem novas técnicas de inteligência. Em termos de capacidade, a Lei visa de certa forma monitorar e regular a gama de ferramentas que as agências de inteligência

podem utilizar. Essas ferramentas incluem escutas telefônicas, dados abertos de Internet (como redes sociais, fóruns e etc.), registros de acesso à Internet e metadados, identificação geográfica, bem como a exploração de computadores (apreensão em buscas domiciliares ou o uso de métodos hacking), e a utilização de "caixas pretas" – algoritmos – para análise automatizada de dados (TRÉGUER, 2017, p. 7).

Além disso, a Lei prevê a análise automática de metadados para identificar o comportamento característico de um indivíduo "radicalizado" na Internet. A coleta de metadados é feita em tempo real pelos agentes de inteligência através da utilização de algoritmo de análise de big data. É o uso do sistema algorítmico do artigo L. 851-3 do Código da Segurança Interna que torna possível localizar "suspeitos" a partir dos metadados. Estes não incluem o conteúdo das comunicações; contudo, há a possibilidade de suspender, se necessário, o anonimato dos dados – o que sugere que estes são identificáveis (artigo L. 851-4 alínea 2 das notas de rodapé 3 e 48 do CFSI).

Cabe entender que o objetivo dos metadados é explicar o processo de produção de conjuntos de dados para seus usuários. Idealmente, os metadados devem incluir todas as descrições adicionais necessárias para entender os dados (SCHEEL; USTEK-SPILDA, 2019); eles estão recentemente no centro de controvérsias sobre práticas de segurança (ARADAU; BLANKE, 2015). Como argumenta Ruppert et al. (2013) há uma virada para os metadados nas práticas de governança e segurança que precisa ser compreendida no contexto de uma economia de produção de *big data*, em que as fontes digitais criam dados como subprodutos. Uma leitura dos metadados feita pelas agências de inteligência é que eles são menos nocivos por excluírem a análise de conteúdo e por serem analisados de maneira primária por algoritmos. Todavia, esse discurso tem sido desafiado por análises críticas que apontam que os metadados *são* dados sobre conteúdo e que carregam tanto conhecimento quanto os dados (AMOORE, 2011; SCHEEL; USTEK-SPILDA, 2019).

Como argumenta Louise Amoore (2011), os derivados de dados estão no centro da vigilância baseada em dados. Para a autora, as relações contidas nos agregados de dados, os rastros deixados pelos sujeitos, ajudam a estabelecer correlações. Esses tipos de tecnologias não são apenas um desafio para conceitos

PUC-Rio - Certificação Digital Nº 1812441/CA

individuais de privacidade e proteção de dados, mas também interrompem o compartilhamento de normas de privacidade em contextos sociais mais amplos. Os dados em si são um objeto epistêmico complexo, e as distinções entre tipos de dados são produzidas dependendo de como os dados são acionáveis por dispositivos. Os aplicativos de computador, os dispositivos móveis e quaisquer outros sistemas computadorizados que estão conectados à internet estão coletando metadados. Estes, quando agregados, podem fazer referência não somente a suas atividades na internet, mas a atividades cotidianas, bem como a suas relações com outras pessoas. Um exemplo, é que mesmo que um sujeito possa ter total consciência e transparência sobre as implicações do acesso a determinado conteúdo, ele decide de acordo com as regras contextuais de privacidade (cada provedor de serviços web explica quais as informações são coletadas e por quê, como as usa e analisa), mas os metadados por ele produzidos ainda podem ser usados para capturar dados e mesmo violar a privacidade de outrem. Isso pode ser ilustrado através da extração de metadados de uma conta de e-mail: é possível averiguar relações com outras pessoas, como locais de envio do e-mail, horário e assim estabelecer correlações. Assim, os metadados transbordam seus significados, o que implica entender quão problemático é seu deslocamento e sua separação do conteúdo.

Nas práticas de serviços de inteligência franceses, os metadados são utilizados para identificar novos perfis de prováveis terroristas. Para sua identificação, a lei prevê a extensão da vigilância de todos aqueles que entraram em contato com pessoas suspeitas, extraindo dados, analisando seu conteúdo, seus contatos, sua frequência e os modos de comunicação. A análise dos metadados estabelece uma conexão entre o caráter antecipatório do combate ao terrorismo, a ampliação do escopo das agências de inteligência e as práticas de *pensar e fazer* a antecipação do perfil terrorista na França de forma eficiente. Esse modo de criar perfis com base em dados promulga uma abordagem antecipatória, que, como argumenta Leese (2014, p. 499), se afasta do conhecimento factível e da experiência de profissionais e abraça a probabilidade ancorada em uma análise de dados em grande escala. A classificação de risco através de algoritmos veio a ser afirmada como modo de diminuir as contingências do futuro através de uma perspectiva preditiva. Assim, a probabilidade pode ser entendida como árbitro de uma racionalidade prática, entendendo que o raciocínio probabilístico significa que cada

PUC-Rio - Certificação Digital Nº 1812441/CA

propriedade de uma entidade formal é enquadrada como um indicador de correlações dentro de um conjunto de categorias (HACKING, 2006).

Em seu Plano de Ação Contra o Terrorismo publicado em julho de 2018, o governo francês aponta para a centralidade da produção de conhecimento sobre técnicas de criação de perfis e o uso de ferramentas tecnológicas nas atividades de inteligência. O documento propõe a criação de uma unidade de interserviços para a realização de pesquisas de padrões de comportamento e características que produzam um critério *objetivo* para medir a periculosidade de indivíduos radicalizados e que ajude a esclarecer os processos pelos quais recorrem a atos terroristas. Esse plano também indica uma abordagem que visa ao uso mais amplo de tecnologias de segurança envolvendo inteligência artificial e a adaptação da estrutura legal que as envolve[32].

Em meio a uma ampla difusão da análise de dados e da triagem automatizada em contextos de segurança, é fundamental questionar como as decisões são tomadas na interface entre humanos e processos algorítmicos. Essa forma de vigiar "toda a população" revela a tradução de métodos amparados em cálculos matemáticos e inferências indutivas do domínio digital para o não-digital (MITELSTADT et. al., 2016). Aqui, a indução passa a operar com um método não linear: perfis pré-existentes não são usados para identificar os alvos da intervenção de segurança, mas as correlações de informações nos dados produzem indutivamente novos perfis terroristas através de padrões de comportamento (LEESE, 2014). Ou seja, o perfil não mais orienta a implantação da vigilância; são os dados agora que orientam a produção do perfil.

A operacionalização do perfil terrorista ou sujeito propenso à radicalização em termos de metadados analisados algoritmicamente reenquadra as representações do que somos em termos de dados, como aponta Cheney-Lippold (2017, p.58). Embora a construção de perfis de "potenciais terroristas" através dos dados tenha como centralidade os métodos inferenciais, tais perfis ainda carregam características similares àquilo que foi historicamente representado como terrorista

[32] O Coordenador Ministerial de Inteligência Artificial, Cédric Villani foi encarregado de analisar e fazer propostas sobre mudanças relacionadas à transformação digital no campo da segurança interna. A própria existência do cargo já nos diz algo sobre a centralidade que as tecnologias digitais têm assumido nas práticas de governança.

PUC-Rio - Certificação Digital Nº 1812441/CA

(Ibid, p. 59). É importante pontuar que as classificações podem operar em um cruzamento entre o laço sequencial dos cálculos dos algoritmos e dos cálculos pessoais dos burocratas baseados em conhecimentos conjecturais e ambientes institucionais (BONELLI; RAGAZZI, 2014). Como afirma Amoore (2009), a imagem visualizada de um "perfil terrorista" nos dados processados por algoritmos requer algumas lacunas e invisibilidades que são simplesmente preenchidas pelo observador.

Se é verdade que o uso da tecnologia modifica o *modus operandi* dos serviços de inteligência, essa racionalidade computacional não está descolada da coleta de informação e processamento tradicional, encontrada nos modos de registro policiais, por exemplo. A acumulação de informação tanto qualitativa quanto quantitativa opera como fonte que fixa e atualiza cotidianamente os perfis suspeitos, assim como produz listas de indivíduos e grupos a serem monitorados, o que está para além da preocupação com o terrorismo, perpassando outras formas de representação de perigo, como visto na seção anterior.

As "caixas pretas" da coleta de dados e metadados, previstas na Lei de Inteligência e operacionalizadas desde finais de 2017, detectam sinais de um comportamento suspeito e enviam um alerta para os serviços de inteligência francês. Os dados podem ser cruzados com outros dados dos bancos de dados da inteligência, através da utilização de softwares de visualização e dataminig[33]. Portanto, trata-se de uma produção de conhecimento estatístico composto de correlações simples que se baseia em dados e metadados de fontes diversas. O conhecimento produzido através da criação de perfis não está amplamente disponível aos indivíduos, mas é investido sobre eles de maneira a inferir conhecimento e previsões probabilísticas a respeito de suas preferências, intenções e propensões que, de outra forma, não seria evidente (VAN OLTERLOO, 2013).

Como observa Gillespie (2014), os algoritmos não apenas processam os dados e metadados: eles produzem, afirmam e certificam o conhecimento por meio de uma lógica que opera com suposições particulares. O código não é puramente abstrato e matemático: possui dimensões sociais, políticas e estéticas significativas

[33] O datamining é o processamento automatizado de vasto volumes de dados para identificar correlações sutis entre eles.

PUC-Rio - Certificação Digital Nº 1812441/CA

(MONTFORT et. al., 2013, p.3), sendo produtos de assemblagens[34] sociotécnicas complexas, inerentemente enquadradas e moldadas por todos os tipos de decisões, políticas e ideologias. Embora os programadores possam procurar manter um alto grau de objetividade mecânica no processo de tradução de uma tarefa ou processo ou cálculo em um algoritmo, não conseguem escapar do conhecimento e contexto locais deles (CHENEY-LIPPOLD, 2017, p.10).

Da mesma forma, é difícil escapar de fatores intrínsecos aos processos algorítmicos como recursos disponíveis e a escolha e qualidade dos dados de treinamento; requisitos relacionados a normas, protocolos e lei; e escolhas e condicionalidades relacionadas a hardware, plataformas, largura de banda e idiomas (KITCHIN; DOGGE, 2011; DIAKOPOULOS, 2013). Uma grande quantidade de conhecimento, julgamento, escolha e restrições é então exercida na produção de algoritmos. Os algoritmos não são caixinhas separadas de processos sociais (SEAVER, 2013, p.10), tampouco funcionam isoladamente: fazem parte de um todo tecnológico mais amplo, que inclui infraestrutura, hardware, plataforma de códigos, dados e interfaces. Por isso, é importante compreender que os algoritmos são realizações contextuais e frágeis (GILLESPIE, 2014): o resultado de um conjunto de atores heterogêneos, instituições, tecnologias, práticas, infraestruturas, modos de governar e de produzir conhecimento.

Como observado, a Lei de Inteligência autorizou medidas intrusivas, como o uso de ferramentas de vigilância que captam ligações e a utilização dos algoritmos "caixa preta" em provedores de serviços de internet que coletam e analisam dados pessoais de uma ampla faixa de usuários franceses. Desse modo, as agências de inteligência chegam a acessar diretamente as redes para filtrar os "desvios" identificados na forma de sinais fracos através de algoritmos. Se o dispositivo revelar uma ameaça, o Ministro do Interior (ou um de seus delegados) pode então decidir renunciar ao anonimato nos dados, informações e documentos relacionados[35]. Contudo, a legibilidade dessas correlações depende de softwares de visualização.

PUC-Rio - Certificação Digital Nº 1812441/CA

[34] O uso de assemblagem aqui é no sentido proposto por Paul Rabinow (2003, p. 56) de uma "matriz experimental de elementos, técnicas e conceitos heterogêneos.

[35] Disponível em: https://www.i-resilience.fr/2015/04/surveillance-la-legalite-douteuse-des-boites-noires/. Acesso em 10 de junho de 2019.

Em 2005, a França comprou o IBM i2 Analyst Notebook (i2AN) em conjunto com programas de análise criminal, que passaram a operar nesse mesmo período. A iniciativa fez parte de um plano mais amplo voltado a trazer os dados do governo on-line de forma centralizada e com formato facilmente compartilhável. O governo francês definiu o período dentro do qual a polícia poderia manter informações pessoais sobre suspeitos e vítimas em arquivos, bem como nos bancos de dados unificados criados para armazenar estas informações (Kubler, 2017). Segundo a IBM (2017),

> [o] IBM i2 Analyst Notebook fornece recursos avançados de análise visual que podem ajudar a transformar rapidamente conjuntos complexos de informações díspares em inteligência acionável e de alta qualidade. Isso ajuda os analistas e outros envolvidos na análise de inteligência a identificar, prever e evitar atividades criminosas, terroristas e fraudulentas.[36]

Ou seja, o software da IBM agrega informações, organiza e visualiza os dados. Ele oferece uma ferramenta que pode classificar grandes quantidades de dados em um curto espaço de tempo e apresentar a visualização de correlações (IBM, 2017). O i2AN é um descendente direto dos algoritmos de árvore de decisão, e sua principal função é traduzir associações prováveis entre pessoas ou objetos em decisões de segurança acionáveis (KUBLER, 2017). Tanto o processo da datamining quanto da visualização destes é de natureza correlativa (BOYDE; CRAWFORD, 2012). Uma das funções mais importantes do i2AN é importar dados de vários conjuntos de bancos de dados e produzir visualizações que ajudarão a revelar conexões que não seriam feitas de outra forma. Esse tipo de software permite que as forças policiais acessem grandes quantidades de dados públicos, economizando recursos e tempo (KENNEDY et al., 2015). O papel do i2AN para a inteligência francesa é explicado pela revista policial National Gendarme Review:

> A análise da rede de inteligência é uma etapa essencial na adoção de ação e um pré-requisito para a tomada de decisão. O i2 Analyst's Notebook permite que os analistas classifiquem, analisem e visualizem rapidamente dados de várias fontes. Reduz o tempo necessário para reconhecer as informações necessárias para criar uma rede sólida e oportuna que permita a identificação, previsão, prevenção e

[36] "IBM i2 Analyst's Notebook provides rich visual analysis capabilities that can help to quickly turn complex sets of disparate information into high-quality, actionable intelligence. This helps analysts and others involved in intelligence analysis identify, predict, and avoid criminal, terrorist and fraudulent activities". IBM Corporation (2017). IBM i2 Analyst's Notebook: Discover and deliver actionable intelligence. Disponível em: https://www.ibm.com/downloads/cas/QNGO6RNA. Acesso: 13 de junho de 2019.

PUC-Rio - Certificação Digital Nº 1812441/CA

> interrupção de atividades terroristas, criminais e fraudulentas (CURRIEU; SAJHAU, 2014, p. 50)[37].

O uso do visual não apenas permite uma visualização exclusiva dos dados, mas também representa a velocidade e a capacidade de processamento do algoritmo. Os padrões miméticos gerados por algoritmos estão refazendo o observador dentro do sistema de visualização, direcionando a atenção em pontos específicos. O protocolo do i2AN é um caminho de dados que traça os limites de possibilidade do sistema. Ele opera criando um conglomerado de pontos sobre o indivíduo e tenta conectá-lo com outras redes de outros sujeitos possíveis suspeitos. Os softwares como o i2AN, podem assumir a forma de um algoritmo de produção de listas, as quais servem como pano de fundo para o cálculo do algoritmo. Johns (2016, p. 128) rastreia esse problema com o protocolo de produção de lista de algoritmo como o i2AN: para a autora, os softwares dissimulam tanto quanto revelam, perturbam tanto quanto estimulam.

Além da mineração de bancos de dados, as informações ainda podem ser extraídas por meio de medidas mais vigorosas, como uma operação na qual os telefones celulares e discos rígidos são confiscados – a exemplo das buscas domiciliares institucionalizadas através da Lei SILT. A ampliação das práticas administrativas, como as prisões e buscas domiciliares, também é objetivada pela extração de dados e pela "locabilidade" dos sujeitos (limitação de mobilidade, assim possibilitando o rastreio) (KUBLER, 2017). Essas práticas administrativas fornecem à polícia francesa uma quantidade enorme de informações sobre uma parte da população entendida como provável ameaça à ordem. Como Matzner (2013) sugere, esses sistemas que supostamente auxiliam os operadores humanos (tais como o i2AN) são baseados em relatos informativos do mundo que são inacessíveis para os seres humanos (análise em larga escala) e, portanto, exigem um certo nível de "confiança" no cálculo algorítmico. Nesse sentido, o processo de conformação de evidências, baseado nos dados policiais de vigilância e inteligência, permitem que correlações sejam feitas, pontos sejam conectados e as

[37] "Intelligence network analysis is an essential step in taking action and a prerequisite for decision making. I2 Analyst's Notebook enables analysts to quickly sort, analyze and view data from multiple sources. Reduces the time required to recognize the information needed to create a solid and timely network that enables the identification, prediction, prevention, and disruption of terrorist, criminal, and fraudulent activities".

PUC-Rio - Certificação Digital Nº 1812441/CA

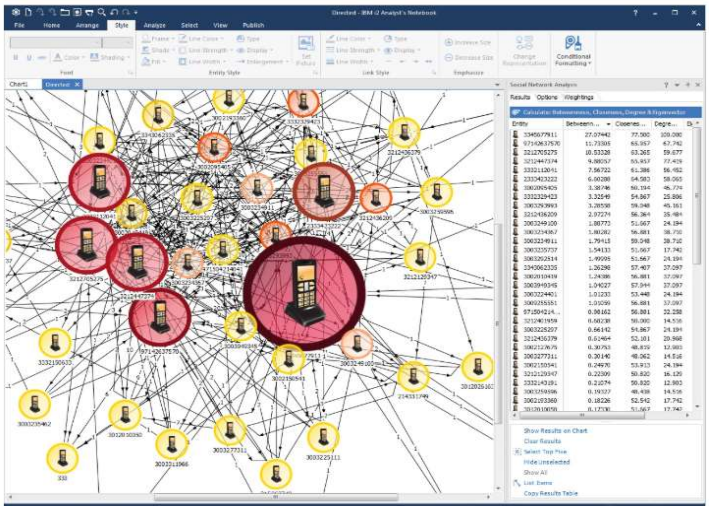
conclusões se tornem suficientes para justificar uma medida administrativa que amplie o controle e restrinja direitos.

Segundo Amoore (2009), as decisões baseadas na conjunção de "linhas de visão" humanas e as codificadas pelas tecnologias computacionais tornam o "terrorista" conhecível antes mesmo de praticar tal ato, através dos rastros desagregados de bits e bytes de um modo de vida. Assim, o algoritmo produz uma visualização rastreada de suspeição na qual outros sujeitos são mensurados, vigiados, policiados e até mesmo sofrem medidas punitivas (como veremos na seção 3).

Como podemos observar na Figura 1, o i2AN usa os gráficos de nós e links para visualizar a análise de redes sociais. Tais gráficos não são conhecidos por gerarem uma boa visualização para detecção de ameaça terrorista (HALL et al., 2015). Para que essas visualizações representem adequadamente os relacionamentos entre os nós, é necessário haver uma distinção clara de identidade entre os usuários internos e externos de uma rede. Comentando as visualizações de nós e links, Hall et al. (2015, p. 95) observam que "a visualização pressupõe tipos de comportamento fixos: os insiders são leais e os outsiders maliciosos. Essa distinção está de acordo com as abordagens militaristas do passado, mas na computação em nuvem não é fácil fazer a distinção entre insiders e outsiders". Ou seja, esse software mostra nós de correlações através de dados que produzem modulações de relações formando redes mais amplas e tornando mais flexíveis as separações entre quem está dentro e quem está fora dessa rede de sociabilidade.

PUC-Rio - Certificação Digital Nº 1812441/CA

Figura 1: Análise de rede social



Fonte: IBM i2 Analyst's Notebook. Disponível em: https://www.ibm.com/br-pt/marketplace/analysts-notebook.

Há uma dificuldade em encontrar padrões de comportamentos terroristas estruturantes de redes de relações sociais e, por esse motivo, a orientação da produção do "perfil terrorista" pela correlação de dados pode gerar uma gama de falsos positivos. Tanto nas pesquisas acadêmicas quanto discursos de autoridades de segurança apontam que não existe um perfil padronizado de "terrorista" ou "pré-terrorista" (PELZER, 2018, p.170). Isso porque o terrorismo é um comportamento não usual e a própria configuração do que é uma atividade terrorista é objeto de diversas definições não estabilizadas (BONELLI, 2014). Embora descritores de identidade como nome, raça e sexo possam ser conhecidos, o significado dessa identidade, em termos de sua ameaça ou anomalia, pode não o ser. O entendimento do dinamismo dos processos de radicalização violenta na criação dos perfis terroristas se baseia em critérios de risco não específicos e, portanto, prioriza a sensibilidade[38] e a probabilidade em detrimento da especificidade. A aplicação desses critérios não específicos permite identificar a probabilidade, ou melhor, a disposição do sujeito de se envolver em uma atividade terrorista. Não obstante, não dizem nada sobre as condições sob as quais essa disposição ganharia materialidade (PELZER, 2018).

[38] A sensibilidade refere-se à capacidade de uma ferramenta identificar com precisão aqueles com altos risco de serem uma ameaça. (PELZER, 2018, p.160).

PUC-Rio - Certificação Digital Nº 1812441/CA

A ideia de que localizar regularidades e padrões em uma quantidade vasta e heterogênea de dados pode levar ao estabelecimento de correlações entre pessoas aparentemente "suspeitas" parece possibilitar a conversão de evidências *ex post facto* na luta contra o terrorismo em um julgamento feito antes do evento. Assim, da visualização do sujeito em um emaranhado de dados e metadados é derivada a possibilidade de agir sobre ele. Os sujeitos suspeitos, neste caso, são reconstruídos por meio de um mapeamento imaginativo de suas tendências e potencialidades (AMOORE, 2011, p.28). Como Deleuze argumentou, as sociedades de controle, nas quais estamos agora imersos, produzem o "dividual" - um sujeito fracionado, composto de pontos de dados desagregados (DELEUZE, 1992, p.5; AMOORE, 2013, p. 92). A construção desse sujeito, como vimos, é altamente contingente e instável.

O uso das tecnologias para a criação de perfis a serem policiados baseia-se em parte no discurso de eficiência e de decisão sem vieses e preconceitos. Uma fé na objetividade, eficácia e operacionalidade das provisões algorítmicas, como observa Rouvroy (2016, p.13), substitui o processo de avaliação crítica daquilo que é apresentado como uma visualização ou decisão automatizada. Há uma questão política importante: somos confrontados com práticas e técnicas de governar que promovem certa aparência ética e, de certa maneira, responsável de segurança (AMOORE, 2009; ARADAU; O'NEIL, 2017; FERGUNSON, 2017), mas que borra formas de prestar atenção e rastrear os processos que levam à insegurança de sujeitos e comunidades. Nesse cenário, os processos de triagem e categorização incorretos, os chamados "falsos positivos", tornam-se partes essenciais de um horizonte desigual de direitos (NYERS, 2006).

Os procedimentos de operações de inteligência, como as práticas de coleta de dados, de mobilização de suspeitas através de correlações algorítmicas (que podem ou não ter confiabilidade empírica) e a visualização digital produzem evidências que dão apoio a processos de controle e eventualmente punição. Por isso, uma abordagem crítica implica levar a sério a produção e interpretação algorítmica de dados como uma prática epistêmica e política desigual. Por isso é necessário refletir sobre as formas de responsabilização nessas dinâmicas nas quais se entrelaçam humanos e algoritmos nas práticas de segurança. Tendo em vista que se trata de um desafio epistemológico, ontológico é ético que é profundamente

PUC-Rio - Certificação Digital Nº 1812441/CA

desigual e ao mesmo tempo inacessível, e de forma fulcral está hoje amplamente difundido como um *estilo de pensar e fazer*.

PUC-Rio - Certificação Digital Nº 1812441/CA

3.
A individualização do controle da possibilidade: o caso das MICAs

K. é um homem que reside da região metropolitana de Paris, sujeito a uma ordem de prisão domiciliar em 15 de novembro de 2015 no arcabouço de práticas da implantação do estado de emergência e que, no ano de 2016, foi submetido a uma medida de controle administrativo (MICA) – medida semelhante à prisão domiciliar no estado de emergência. Essa medida determina a restrição da circulação de uma pessoa a um perímetro geográfico específico por um período de três meses renovável e torna compulsória a prestação de contas periódica à polícia, declarando seu local de residência, sob punição de sanções penais. No documento de notificação da MICA, as autoridades alegaram que ele era um "radical islâmico" que mantinha contato com militantes pró-jihadistas e que planejava uma viagem a Síria. Em depoimento à Anistia Internacional, K. alega:

> Eu não entendi o que eles queriam dizer por "islâmicos radicais", então li a nota regida pelo serviço de inteligência e apresentado ao tribunal. Incluía uma lista de pessoas em que pensavam que eu estava mantendo contato. Eu conhecia três delas, não conhecia os outros. Eu tenho uma loja e esses três eram meus clientes. Como eu deveria saber que eles estavam em contato com radicais islâmicos? Isso não implica nada. Eles não encontraram algo que indicasse que eu queria viajar para a Síria, nem mesmo uma mensagem de texto. (ANISTIA INTERNACIONAL, 2018, p. 26)[39].

O cidadão francês K. não teve acesso à informação completa dos serviços de inteligência francesa e só conseguiu receber mais informações sobre o que a notificação queria dizer sobre "radical islâmico" porque apelou contra a medida que lhe foi imposta. Os advogados de K. apenas receberem as declarações do caso preparadas pelo Ministério do Interior pouco antes da audiência, limitando assim sua preparação. O conteúdo dessas declarações é baseado nas "notas brancas" fornecidas pelos serviços de inteligência (ANISTIA INTERNACIONAL, 2018).

[39] "I didn't understand what they mean by "radical Islamists", so I read a note governed by the intelligence service and presented to the court. Include a list of people who thought I was keeping in touch. I knew three of them, I didn't know the others. I have a store and these three were my customers. How should I know they were in touch with Islamic radicals? This does not imply anything. They didn't find anything to indicate that I wanted to travel to Syria, not even a text message" K. em entrevista à Anistia Internacional em julho de 2018. Para defesa da identidade dos entrevistados será utilizada apenas uma letra.

PUC-Rio - Certificação Digital Nº 1812441/CA

Essas notas podem fazer referência a supostas conexões ou reuniões entre uma pessoa designada a estar sob controle e outras pessoas que alegadamente constituem uma ameaça à ordem ou segurança pública, sem esclarecer a natureza da conexão ou as datas ou circunstâncias específicas das reuniões. Os tribunais administrativos e o Conselho de Estado raramente contestam as informações incluídas nessas notas ou exigem que o Ministério do Interior produza informações mais específicas – o que é prejudicial para a eficácia dos recursos disponíveis para aqueles sujeitos a medidas administrativas que restringem direitos através de evidências que são vagas e ao mesmo tempo eficientes, porque são autoautenticáveis. Nesse sentido, as MICAs podem ser interpretadas como um *estilo de pensar e fazer* que decreta seus próprios critérios de legitimidade e objetividade (HACKING, 2002, p.191) no âmbito em que está circunscrito.

Em 10 de dezembro de 2017, Y., foi designado a residir em uma cidade nos arredores de Paris por uma MICA. Essa foi justificada com base em suas supostas conexões com "islamitas radicais" e com jovens franceses que viajaram para Síria ou Iraque para ingressar no Estado Islâmico. A justificativa também mencionava que ele frequentemente visitava o que eles descreveram como "mesquita radical" nos arredores de Paris, a 24 km de onde residia. Em entrevista à Anistia Internacional, Y. afirmou (2018, p. 14):

> Não sou eu: eles estão procurando por outra pessoa. A data e o local de nascimento no primeiro documento que recebi sobre a residência designada estavam completamente errados. Por exemplo, eles indicaram que eu nasci na Tunísia, o que não é verdade. Eu nasci na França. Em qualquer caso, o que poderia acabar com todas as suspeitas contra mim? As pessoas que eu conheço ao meu redor têm mudado suas atitudes em relação a mim, e alguns fazem piadas[40].

Y. contestou a MICA que lhe foi atribuída no tribunal administrativo. Em juízo, o representante do Ministério do Interior justificou a medida com base em uma nota de inteligência, datada de 14 de novembro. A fim de proteger suas fontes e não comprometer seu trabalho, o Ministério do Interior alegou que apenas poderia disponibilizar ao tribunal algumas das informações coletadas pelos serviços de

[40] It's not me: they are looking for someone else. The date and place of birth in the first document I received about the designated residence was completely wrong. For example, they indicated that I was born in Tunisia, which is not true. I was born in France. In any case, what could end all suspicions against me? The people I know around me have changed their attitudes toward me, and some make jokes.

PUC-Rio - Certificação Digital Nº 1812441/CA

inteligência. O juiz não contestou tal argumento e, em 8 de janeiro, rejeitou o recurso de Y. (ANISTIA INTERNACIONAL, 2018).

À luz de tais casos, esta seção busca analisar as conexões entre, de um lado, práticas de mensuração do perigo em um discurso técnico ancorado no imperativo da eficiência das práticas de vigilância e, de outro, os efeitos de controle e a flexibilização de salvaguardas processuais e garantias de direitos.

3.1.
Evidências baseadas em "notas brancas": a Lei SILT e a transformação das práticas judiciais

A lei de 30 de outubro de 2017 ("Lei SILT"), que reforça a segurança interna e a luta contra o terrorismo, entrou em vigor em 1 de novembro de 2017, com o objetivo de estabelecer uma legislação comum para medidas administrativas policiais para fins de luta contra o terrorismo. A lei procura enquadrar, em condições mais estritas, as principais medidas implementadas no estado de emergência: a criação de perímetros de proteção, fechamento de locais de culto, medidas individuais de controle e supervisão administrativa, visitas domiciliares e apreensões. A Lei também fortalece os poderes dos serviços de inteligência na coleta e processamento de dados, bem como nos controles de fronteira.

Os membros da rede Antiterrorisme, Droits et Libertés, que inclui ONGs, sindicatos profissionais, advogados e acadêmicos, levantaram inúmeras queixas quanto à incompatibilidade da Lei SILT com os direitos fundamentais[41]. As reservas quanto à compatibilidade da Lei SILT com o Direito Internacional dos Direitos Humanos foram expressas por vários órgãos internacionais, como o Comissário para Direitos Humanos do Conselho da Europa e o Relator Especial para Direitos Humanos, por ocasião de sua visita à França em maio de 2018. Diversas recomendações foram feitas pelas Nações Unidas nesse contexto, com destaque para a necessidade de respeito aos direitos humanos na implementação da legislação antiterrorista e garantir as salvaguardas do devido processo legal. Na ocasião da visita, foi entregue à Relatora Especial da ONU, Fionnuala Ni Aolain, o

[41] Disponível: https://antiterrorisme-droits-libertes.org/spip.php?article53. Acesso em 13 de outubro de 2019

PUC-Rio - Certificação Digital Nº 1812441/CA

relatório "Terror in Courts – French conter-terrorism: Administrative and Penal Avenues"[42] (2018). O relatório indica uma clara normalização das medidas promulgadas com base na declaração do estado de emergência em 2015 e a "radicalização da Lei Administrativa".

Em geral, a Lei SILT é criticada por estabelecer um estado de emergência permanente, conferindo à administração poderes estendidos a longo prazo que são particularmente prejudiciais aos direitos e liberdades. Além disso, permite a implementação de medidas coercitivas de limitada verificação prévia de uma autoridade judicial com base em suspeitas, na ausência de qualquer evidência de participação na prática de um crime e por razões excessivamente vagas, desconsiderando o princípio da legalidade e da garantia das salvaguardas processuais.

Nesse sentido, a lei do SILT gera litígios regulares, principalmente na forma de questões prioritárias de constitucionalidade. O Conselho Constitucional validou a maioria das disposições; no entanto, censurou certas disposições relativas aos procedimentos para o exercício de recursos contra as MICAs, bem como à apreensão de documentos ou objetos durante as visitas domiciliares[43]. Em relação às MICAs, o Conselho Constitucional estabeleceu duas reservas de interpretação: (1) a medida não deve exceder um período cumulativo de 12 meses; e (2) a proibição de encontrar com determinados indivíduos não deve afetar desproporcionalmente o direito à vida familiar. A resistência do Conselho diz respeito à disposição de que o juiz administrativo deve decidir sobre recursos por discricionariedade e arbitrariedade de poder dirigido contra essas medidas dentro de 4 meses. Para o Conselho, o direito a um recurso judicial efetivo exige que seja decidido dentro de um curto período de tempo – 2 meses[44].

PUC-Rio - Certificação Digital Nº 1812441/CA

[42] WEIL. S. Terror in Courts – French conter-terrorism: Administrative and Penal Avenues. Report for the official visit of the Un Special Rapporteur on Counter-Terrorism and Humans Rights. Disponível: https://www.sciencespo.fr/psia/sites/sciencespo.fr.psia/files/Terror%20in%20Courts_2.pdf. Acesso 25 de agosto de 2019.

[43] FRANCE. Rapport du Gouvernement au Parlament. Mise en œuvre de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme. Novembre 2018. Disponível em: http://www2.assemblee-nationale.fr/content/download/75798/778106/version/1/file/Loi+SILT+-+Rapport+au+Parlement+2018.pdf. Acesso em 12 de outubro de 2019.

[44] LIGUE DES DROITS DE L'HOME (2018). Le Conseil Constitutionnel se Prononce sur les quatre Nouvelles Mesures de Police Administrative créées par la loi du 30 octobre 2017. Disponível em:

Ainda, a Lei prevê um mecanismo de supervisão parlamentar, confiada aos deputados e senadores membros das comissões das leis da Assembleia Nacional e do Senado. Os dados estatísticos sobre a implementação da Lei SILT são publicados mensalmente, com base nas informações fornecidas pelo Ministério do Interior. Embora esse mecanismo de supervisão busque definir limites a possíveis discricionariedades por parte dos serviços de inteligência e das forças policiais, esse quadro coexiste com a proliferação de prerrogativas administrativas que conferem mais poder às autoridades executivas para limitar as liberdades individuais, além de transferir a competência de revisão judicial ao juiz administrativo.

Os tribunais administrativos não operam com juízes comuns. Os juízes administrativos não precisam ser graduados na Escola Nacional de Magistrados, mas precisam ser graduados em Administração (WEIL, 2018, p. 10-11). Em relação ao Conselho de Estado, a mais alta jurisdição administrativa, o governo nacional nomeia uma parcela significativa de seus juízes-administradores – o que estimula uma cultura de proximidade entre o governo e os juízes administrativos e aumenta as chances de sintonia entre a avaliação dos juízes, de um lado, e de instituições como o Ministério do Interior, de outro, no que diz respeito à legalidade de uma medida (LATOUR, 2004)[45].

Os tribunais administrativos diferem consideravelmente dos tribunais comuns quando se trata de regras processuais. Talvez uma das principais diferenças seja o uso de "*notes blanches*" (notas brancas) como evidência, documentos elaborados com base em informações dos serviços de inteligência. As "*notes blanches*" podem conter detalhes sobre comportamentos ou ações suspeitas, incluindo associação com outras pessoas suspeitas, mas não fornecem informações sobre a fontes dessas informações e não contêm data ou assinatura. Enquanto as notas brancas não podem ser apresentadas com valor de prova perante os tribunais

PUC-Rio - Certificação Digital Nº 1812441/CA

https://www.ldh-france.org/le-conseil-constitutionnel-se-prononce-sur-les-quatre-nouvelles-mesures-de-police-administrative-creees-par-la-loi-du-30-octobre-2017-renforcant-la-securite-interieure-et-la-lutte-contre-le-terrorism/ Acesso: 11 de outubro de 2019.

[45] Há um estudo socio-legal fascinante sobre o Conselho de Estado realizado por Bruno Latour, La fabrique du droit: Une ethnographie du Conseil d'État, Collection Sciences Humaines et Sociales, Éditions La Découverte Poche, Paris, 2004.

comuns, seu uso é legitimado em tribunais administrativos por jurisprudência e prática administrativa[46].

O tratamento das notas brancas pelos tribunais administrativos é sustentado por uma presunção de verdade, como pode ser visto em inúmeras decisões que citam uma nota branca como a única evidência na qual uma decisão se baseia[47]. Segundo o presidente da seção de litígios do Conselho de Estado francês, *"*partimos do princípio de que os serviços de inteligência trabalhem honestamente e não exageram o conteúdo das notas brancas"[48]. Segundo o juiz administrativo Guillaume Odinet, a "revisão judicial não é fácil de fazer, tem que se determinar a periculosidade de uma pessoa de acordo com uma incerteza de base factual, baseada em medos, em várias suposições. A decisão da polícia administrativa é prospectiva"[49]. Há uma tendência a confiar nas notas brancas em jurisdições administrativas e aceitá-las sem mais provas, transferindo assim o ônus da prova ao acusado, que deve convencer o tribunal de que não é perigoso – uma tarefa desconfortável à luz de uma hostilidade e preconceito gerais contra a aparência e práticas religiosas, o que tem sido muito reforçado em discursos antiterroristas. Como refutar "suspeitas" diante de uma acusação com base em correlações realizadas por uma complexa relação entre metadados e dados dispersos analisados por algoritmos? Como sustentam Vauchez e Slama (2017, p. 287-288), "[o] valor decisivo dessas notas brancas e o peso que elas assumem na maioria dos casos

PUC-Rio - Certificação Digital Nº 1812441/CA

[46] A legalidade das notas brancas foi aprovada pela primeira vez pelo Conselho de Estado em 1991 e 2003
(Council of State, Ministre de l'Intérieur c. Diouri, Case No. 128128, 11 October 1991; Council of State, Ministre de l'Intérieur c. Rakhimov, Case No. 238662, 3 March 2003). A legalidade foi confirmado novamente pelo Conselho de Estado no Processo nº 394991, de 11 de dezembro de 2015, em que o Conselho confirmou que não há disposição legislativa ou princípio que impede o juiz administrativo de considerar os fatos fornecidos pelas "notas brancas" se foram submetidos a um processo contraditório e não foram seriamente contestados pelo requerente.

[47] Como exemplo do caso de K (Nº 14 de fevereiro de 2018). Tribunal Administratif D'Amiens. Disponível em: http://amiens.tribunal-administratif.fr/A-savoir/Communiques/L-AFFAIRE-DU-MOIS-N-14-Fevrier-2018. Acesso em 19 de outubro de 2019.

[48] Bernard Stirn, President of the State Council's litigation section, Report No. 3784, National Assembly, 25
May 2016. Disponível em: www.assembleenationale.fr/14/rapports/r3784.asp Acesso: 15 de outubro de 2019.

[49] Guillaume Odinet, "Le rôle du juge administratif dans le contrôle de l'état d'urgence", Les Cahiers de la Justice, Dalloz, 2017, p. 278. Para contextualizar ver em: Pierre Alonso, "Notes blanches: Les corbeaux de la place Beauvau", Libération, 15 Febr. 2016. Disponível em: https://www.liberation.fr/france/2016/02/15/notes-blanches-les-corbeaux-de-la-place-beauvau_1433587. Acesso 15 de outubro de 2019.

constituem um dos elementos mais significativos do excepcionalismo do processo na justiça administrativa"[50].

Nestas circunstâncias, os sujeitos visados têm dificuldade em contestar alegações que não são claramente expostas a eles, enquanto juízes não podem avaliar adequadamente o valor conclusivo da prova apresentada a eles em notas brancas (ANISTIA INTERNACIONAL, 2018, p.15-17). A maioria das pessoas não tem acesso à informação que o Estado detém e, portanto, os indivíduos podem não ter ideia de por que exatamente estão no radar das medidas de controle do governo[51].

Esse superinvestimento de evidência resulta de um desejo, por um lado, de confiar fortemente na suposta precisão dos termos de evidência e, por outro lado, coletar o máximo de evidências para condenar indivíduos afiliados a organizações difíceis de identificar. Sob o efeito dessas linhas de força, o equilíbrio entre verdade, eficiência e legitimidade – que é a base do conceito de evidência – pode estar mudando. Assim, às vezes a eficiência parece prevalecer sobre a imparcialidade em termos de respeito pela presunção de inocência e princípio do contraditório, por exemplo, mas também de respeito ao próprio direito à privacidade.

PUC-Rio - Certificação Digital Nº 1812441/CA

3.2.
Medidas Individuais de Controle Administrativo (MICA): critérios e aplicações

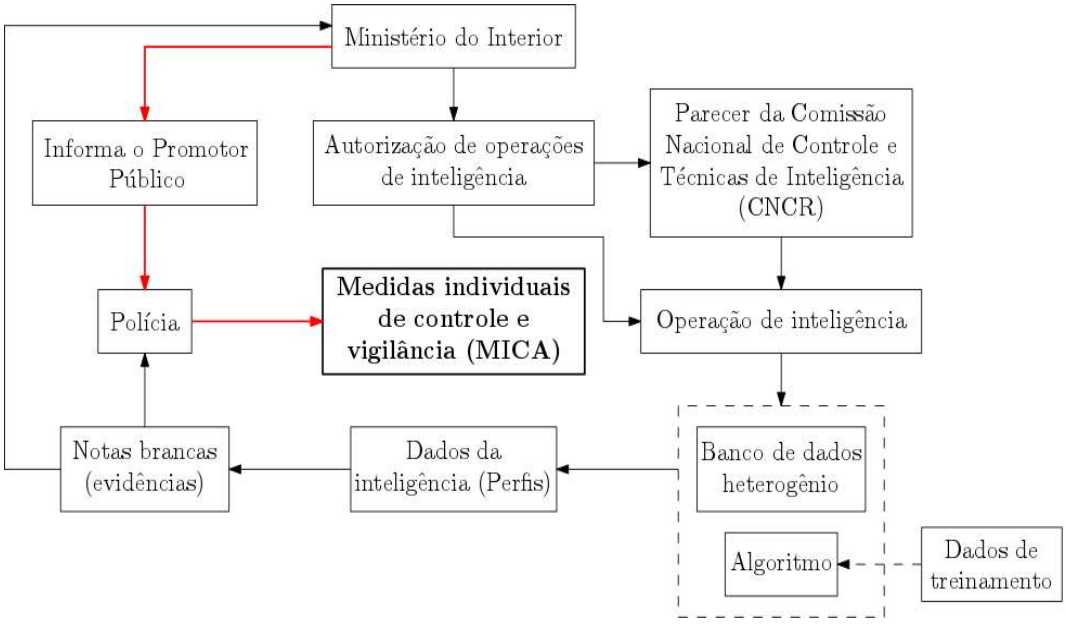
Como a análise das seções anteriores revela, a MICA atua como uma medida de mitigação de riscos futuros porque é imposta a uma pessoa antes que ela seja razoavelmente suspeita (o que é padrão criminal exigido) de ter cometido qualquer infração ao abrigo do Código Penal francês ou tendo dado qualquer passo afirmativo em relação a tal ofensa. As medidas possuem como foco padrões de comportamento de indivíduos e não ação concreta. As MICAs têm a função

[50] "La valeur déterminante de ces notes blanches et le poids qu'elles assument dans la plupart des affaires constituent l'un des éléments les plus significatifs de l'exceptionnalisme du processus en matière de justice administrative. Et, sauf dans de rares cas où le plaignant remercie souvent de bons procureurs, il peut «démonter» la version de la police, le juge administratif approuvant généralement les éléments de fait rapportés dans les notes vierges".

[51] Veja em: Official data in Bilan statistique de l'état d'urgence, 14 November 2015. Disponível em: www2.assembleenationale.fr/static/15/lois/bilan_contentieux.pdf. Acesso: 10 de outubro de 2019.

antecipatória destinada a impedir ou controlar o movimento de indivíduos que os serviços de segurança classificam como suspeitos. O Ministro do Interior decide exclusivamente emitir uma ordem de controle administrativo depois de informar o promotor público. Como observado anteriormente, nenhuma autorização judicial prévia é necessária e sua justificativa baseia-se nas informações oferecidas pelos serviços de inteligência – as notas brancas.

Figura 2. Esquema do processo de autorização das operações de inteligência à aplicação da MICA



Fonte: Elaboração própria.

As medidas individuais de controle e vigilância obrigam que o indivíduo a ela vinculadas, de acordo com o art. 65: (1) não se desloque para fora de uma área geográfica específica, que não pode ser inferior ao território do município; (2) informar periodicamente à polícia ou às unidades da gendarmarie, dentro do limite de uma vez ao dia; (3) declarar seu local de residência e qualquer mudança de local de residência. Além destas, o Ministro do Interior pode propor à pessoa sujeita à medida colocá-la sob vigilância eletrônica móvel, após ter informado o Ministério Público da República de Paris e o Ministério Público territorialmente competente. Esta colocação está sujeita ao consentimento por escrito da pessoa em questão, isso porque é um procedimento usado em medidas de prisão domiciliar. Nesse caso, o perímetro geográfico imposto sob o mesmo não pode ser menor que o território do

PUC-Rio - Certificação Digital Nº 1812441/CA

departamento[52]. Isto posto, podemos observar que essa medida provavelmente viola a liberdade de ir e vir das pessoas; todavia, foi considerada como constitucional. O Conselho Constitucional francês considerou que o legislador perseguiu o objetivo de combater ao terrorismo, que faz parte do objetivo de valor constitucional da prevenção de violações da ordem pública e definiu "precisamente" as condições para o uso da medida e limitou seu alcance a pessoas suspeitas de uma ameaça particularmente séria à ordem pública.

Aqui é importante então entender os critérios "precisos" sob os quais as MICAS são aplicadas. Há dois critérios pelos quais o sujeito estará sujeito à MICA: o primeiro é obrigatório e o segundo, alternativo[53]. Primeiro, o comportamento do indivíduo deve constituir uma ameaça grave à segurança e à ordem pública. Segundo, o indivíduo deve possuir um relacionamento habitual com pessoas ou organizações que incitam, facilitam ou participam de atos de terrorismo e/ou divulgar ou aderir a filosofias que incitam à prática de atos de terrorismo ou o justificam[54], sendo os dois últimos critérios cumulativos. O primeiro critério (o obrigatório) nos leva a interrogar: o que constitui um comportamento ameaçador? Quais são as características desse perfil comportamental? Como analisado na seção 2.2, há uma dificuldade de padronizar um perfil terrorista ou de um sujeito propenso ao terrorismo radical. Alguns dos principais motivos de aplicação da MICA recorrentes mobilizados pela autoridade administrativa e confirmados pela jurisprudência de acordo com o Relatório Parlamentar de 2018 sobre a Lei SILT podem nos ajudar não a responder as questões postas, mas a oferecer pistas de um "perfil comportamental" que ancora as práticas administrativas francesas no combate ao terrorismo.

Um comportamento que constitui uma grave ameaça à ordem pode englobar, de acordo com o Relatório Parlamentar (2018, p. 45) (1) praticar delitos

PUC-Rio - Certificação Digital Nº 1812441/CA

[52] France. LOI n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme. Disponível em: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000035932811&categorieLien=id. Acesso em 11 de outubro de 2019.

[53] Ibid.

[54] A justificativa do terrorismo e a provocação direta ao terrorismo são crimes. A justificativa do terrorismo consiste em apresentar ou comentar favoravelmente sobre atos terroristas. A provocação direta ao terrorismo é a incitação a cometer atos terroristas. Todos podem denunciar as declarações das forças de segurança que constituem uma dessas ofensas realizadas na Internet. A polícia pode ordenar o bloqueio do acesso aos sites nos quais essas declarações são publicadas. Disponível em: https://www.service-public.fr/particuliers/vosdroits/F32512. Acesso em: 10 de outubro de 2019.

no direito comum, revelado comportamento violento tendo dado origem a uma condenação e, em particular pena de reclusão; (2) ameaçar de morte ou violência uma pessoa, em especial quando é depositário da autoridade pública; (3) proferir comentários promovendo a morte como mártir; (4) apresentar comportamento violento relacionado a distúrbios psiquiátricos, mais frequentemente em quebra de tratamento; (5) permanecer em simulações de operações e treinamento militar ou à participação em combate; a prática de esportes de combate; a posse de armas declaradas ou não declaradas; a difusão de mensagens ou imagens violentas; (6) ter relação usual com pessoas que facilitam ou incitam atos de terrorismo ou conspiração criminosa como pessoas condenadas pela justificação do terrorismo ou crime organizado, pessoas que pertencem a grupos terroristas e/ ou criminosos, e pessoas pertencentes a um movimento radical ou que frequentam regularmente um local de culto fechado durante o estado de emergência (base no artigo L. 227-1 do CFSI), e ter relacionamento com presos radicalizados; e/ou (7) admitir que apoia ou difunde teses que incentivem a realização de atos de terrorismo ou a defesa de tais atos através de publicações nas redes sociais, documentos, objetos ou dados relacionados a radicalização descobertos durante uma busca domiciliar como observações apologéticas ou posse de imagens que valorizem um líder ou uma organização.

Os critérios utilizados para desencadear a MICA são amplos e imprecisos, o que pode deixar um substancial espaço para que a polícia interprete as informações produzidas pela inteligência – como as correlações e visualizações produzidas pelos algoritmos (UNHR, 2018; Collectif contre l'islamophobie en France, 2017). Ao invés de ter elementos substantivos concretos que poderiam desencadear essa ação estatal coercitiva, "razões sérias para acreditar" foi a fórmula escolhida: é o comportamento geral, e não a ação concreta do indivíduo, que é alvo. Além disso, uma "ameaça particularmente séria à ordem pública" não está claramente definida – apesar de termos visto algumas de suas características.

Com relação às demais condições que poderiam desencadear as medidas, a noção de "relação habitual" pode ser considerada problemática, pois não há indicação de como seria interpretado e poderia impactar desproporcionalmente os conhecidos do indivíduo. O fato de a "relação habitual" ser suficiente, sem evidência de participação concreta ou facilitação de um ato de terrorismo – mesmo

PUC-Rio - Certificação Digital Nº 1812441/CA

um ato preparatório – pode gerar uma ampliação nos casos de falsos positivos (como observamos na seção 2.3 e no caso de K. e Y.). O vínculo entre os atos direcionados e a ação terrorista está cada vez mais distante, pois o apoio ou a adesão à chamada "tese" terrorista pode ser baseada nas opiniões ou crenças de um indivíduo. Além disso, essas teses podem ser promulgadas na esfera privada e não na pública, o que suscita dúvidas em termos de como o juiz administrativo poderá controlá-las (REBETZ; WOUDE, 2018).

Apesar de a MICA não estar vinculada ao direito penal francês, há sanções penais, como o encarceramento, impostas no caso de violação dessas obrigações administrativas (PONCELA, 2016), e algumas das medidas podem ser difíceis de cumprir para os indivíduos (CAHN, 2016). Podemos exemplificar com a trajetória de M. (entrevistado pela Anistia Internacional, 2018, p. 38). M. todos dias quebra as condições de restrição de movimento impostas para que possa chegar ao seu local de trabalho, apesar de correr o risco de um ano de prisão por violar a MICA. Ele disse a Anistia Internacional (2018):

> Eu tenho filhos pequenos e minha esposa não trabalha. Dirijo meus negócios por conta própria. Como vou ganhar a vida se não trabalho? Eu tenho que ir trabalhar todos os dias e estou apavorado. Eu costumo andar de bicicleta porque é menos provável que seja interpelado pela polícia.

Além disto, a ausência de controle judiciário associado a essas medidas administrativas amplas e imprecisas que restringem a liberdade de um indivíduo pode ter um objetivo oculto se as condições e obrigações forem violadas. Não apenas se controla, mas criminaliza e pune. No contexto francês, é difícil produzir estatísticas sobre a natureza potencialmente discriminatória dessas medidas e seu impacto em comunidades específicas. Isso porque a política de produção de dados francesa rejeita qualquer referência a minorias raciais, étnicas, religiosas ou linguísticas[55]. Esse modelo é baseado na ideia de que o Estado deve interagir apenas com o indivíduo, não com comunidades ou grupos, a fim de dar tratamento igual a todos. A quantificação das MICAs diz respeito apenas à quantidade de medidas decididas por um período de tempo.

[55] A lei de Lei 78-77, de 06 de janeiro de 1978 proíbe expressamente compilar ou tratar dados de caráter pessoal que deixem transparecer, de maneira direta ou indiretamente, as origens raciais ou étnicas, as opiniões políticas, filosóficas ou religiosas.

PUC-Rio - Certificação Digital Nº 1812441/CA

Segundo o Relatório Parlamentar publicado em 2018, os indivíduos mais afetados pela MICA – aqueles mensurados e classificados como risco potencial – são residentes de Ile-de-France, particularmente em Seine-Saint-Denis, Paris, Yvelinese no Val-de-Marne. Outros departamentos com mais de duas medidas são Bas-Rhin (4), Isère (3) e Seine-et-Marne (3). Ademais, 8 departamentos têm duas medidas, 23 têm apenas uma e quase dois terços dos departamentos (62 precisamente) não possuem. Podemos observar que as MICAs têm uma concentração nas zonas urbanas sensíveis (ZUS)[56] em que medidas de controle e vigilância policial já são rotineiras. Em relação às características individuas, temos apenas dados de que 60 medidas dizem respeito a homens (quase 85%), cuja idade média é de 31 anos e 11 mulheres mais jovens em média (22 anos)[57]. E posso afirmar, com base nos dados, que grande parte desses homens foram previamente sujeitos a prisão domiciliar sob o estado de emergência.

A avaliação das medidas administrativas antiterroristas em comunidades específicas, incluindo distinções e disparidades discriminatórias que surgem dessas, enfrenta desafios complexos relacionados a restrições na coleta de estatísticas nacionais sobre minorias ou grupos religiosos específicos. Apesar de esses obstáculos técnicos à publicação de dados desagregados, em pesquisas realizadas pela Anistia Internacional (2016; 2018) e no Relatório da ONU sobre essas medidas, as comunidades árabes e/ou muçulmanas francesas são aquelas que foram principalmente alvo das medidas excepcionais durante o estado de emergência e sob a lei SILT (UNHR, 2018)[58]. As MICAs também se ocupam cada vez mais com as pessoas que saem da prisão (perfis propensos à radicalização ou radicalizados): pelo menos 15 pessoas cumprindo suas penas de detenção foram sujeitas a tal medida, que entra em vigor na data de sua libertação.

PUC-Rio - Certificação Digital Nº 1812441/CA

[56] Esse é um conceito de classificação do Institut National de la stattistique et des études économiques (Insee) para territórios infra-urbanos definidos pelas autoridades como alvos prioritários da política urbana, de acordo com fatores locais relacionados às dificuldades que os habitantes desses territórios estão enfrentando tanto sociais como securitárias. Disponível em: https://www.insee.fr/en/metadonnees/definition/c1679 (Acesso em 05 de janeiro de 2020).

[57] FRANCE. Rapport du Gouvernement au Parlament. Mise en œuvre de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme. Novembre 2018, p. 47-49. Disponível em: http://www2.assemblee-nationale.fr/content/download/75798/778106/version/1/file/Loi+SILT+-+Rapport+au+Parlement+2018.pdf . Acesso em 12 de outubro de 2019

[58] Disponível em: https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=23128&LangID=F. Acesso 29 de dezembro de 2019.

A MICA baseada no artigo L. 228-2 do CFSI é a forma mais rigorosa de aplicação e a mais utilizada – 59 de 72 MICAs aplicadas. Cabe ressaltar, ainda, que 48 das 59 medidas desse tipo foram renovadas pelo menos uma vez[59]. Para a renovação da MICA não é necessário apresentar elementos novos ou adicionais por até seis meses. A análise dos decretos atesta uma dificuldade dos serviços em identificar fatos verdadeiramente novos, exceto um evento judicial (violação de obrigações, prisão, etc.). As renovações geralmente são baseadas em alguns elementos adicionais relacionados a fatos antigos já mencionados na decisão inicial – com base nas evidências de inteligência. Com base em sua jurisprudência estabelecida para prisão domiciliar em estado de emergência, o Conselho de Estado introduziu uma presunção de urgência na área de litígios, medidas de controle e supervisão administrativa, considerando que tal medida "deve, em princípio e por si mesma, salvar que a administração afirme circunstâncias particulares, um ataque sério e imediato à situação dessa pessoa, susceptíveis a criar uma *situação de emergência*" (CE, ord., 1 st dezembro 2017 No. 415750, p. 47, ênfase minha).

Apesar das diversas questões problemáticas analisadas sobre a Lei SILT e as medidas administrativas de controle e vigilância individuais que ela promulga, essa legislação é considerada por alguns analistas e pela opinião pública como um "equilíbrio" entre uma luta eficiente contra o terrorismo e o respeito às liberdades individuais pelos mecanismos de regulação e possibilidade de recurso (REBERZ; WOUDE, 2017). Entretanto, pude observar que esse equilíbrio é meramente ficcional: apesar da possibilidade de contestação, ela é tornada inoperável. Além disso, conforme afirmado anteriormente, na ausência sistemática de dados sobre os sujeitos afetados pelas medidas administrativas implementadas na lei SILT, é difícil observar de maneira ampla como as práticas de antecipação do perfil de terrorista impactam comunidades específicas. Contudo, com base nas informações obtidas durante a pesquisa, ainda que não dados mais amplos e substanciais, é seguro presumir que essas práticas são discriminatórias: embora toda a população francesa esteja sob uma arquitetura de vigilância e controle, nem todas as pessoas são submetidas às medidas de policiamento de igual maneira.

[59] Ibid. nota 53.

PUC-Rio - Certificação Digital Nº 1812441/CA

4.
Borrando a responsabilidade: tecnologias de vigilância algorítmica como um campo de práticas de desresponsabilização

Como vimos, a questão de como lidar com o risco e a incerteza do porvir tem assumido centralidade nos debates de segurança. Esse modo de governar voltado para o futuro está ancorado em técnicas e práticas especializadas de produção de conhecimento (AMOORE, 2014; ARADAU; VAN MUNSTER, 2011). Não obstante, quais são as implicações da orientação da segurança para o futuro – como forma de antecipação – para as práticas de responsabilização? Como argumenta Aradau (2017), essa orientação para o futuro das práticas de segurança desafia os modos de raciocínio das práticas jurídicas.

Esta seção analisa as camadas de práticas humanas e não humanas presentes nas medidas administrativas de controle e vigilância para entender seus efeitos nos processos de responsabilização. O debate sobre a produção de conhecimento e não-conhecimento também é central aqui, isso porque conjuga tanto as racionalidades probabilísticas de segurança, como as jurídicas. Podemos compreender a ampliação da coleta de dados e o uso dos algoritmos como parte de uma mudança na própria prática de segurança e também do direito; logo, numa mudança no que se entende como responsabilização.

A responsabilidade tem se tornado uma "peça-chave" nas práticas do que é entendido como uma "boa governança" (GODDARD, 2012). Autores como Burchell (1996) e Garland (1996) e outros que os seguiram (por exemplo, DEAN 1997; ROSE 1999; O'MALLEY 2004) utilizam o termo "responsabilização" como característica da "governamentalidade neoliberal". Segundo Foucault (2008), "governamentalidade" é uma forma de poder que consiste em várias tecnologias, mentalidades e racionalidades de governar os outros e a si mesmo. Esse processo de responsabilização neoliberal busca definir a gestão de riscos de maneira individualista – ou seja, o indivíduo é responsável pelo risco que produz. Assim, as instituições estatais (mas, não apenas) tentam demarcar os limites da escolha individual responsável, produzindo conhecimento sobre as técnicas e mentalidades adequadas para o gerenciamento de risco (MATZNER et al., 2016). Todavia, o

PUC-Rio - Certificação Digital Nº 1812441/CA

conceito de responsabilização é polissêmico: pode ser tanto um chamado para a ação, como uma interpelação que constrói e assume um tipo de agência ética e certas disposições para a agir com uma auto-gestão (LEMKE, 2001, p.201), ou mesmo um processo de imputação de responsabilidade por possíveis "falhas" e irregularidades.

Por isso, cabe aqui olhar para as nuances trazidas pelo uso de tecnologias computacionais nas práticas de responsabilização em que o algoritmo é apenas uma peça de um quebra-cabeça mais amplo. O caso das MICAS é exemplar tanto da produção de uma responsabilização que age como do meio de governar possíveis condutas de "risco", quanto de como os modos de responsabilização por "falhas" das práticas administrativas são desafiados. Como argumenta Delmas-Mathy (2017), o aumento do foco na prevenção nas práticas antecipatórias resulta na substituição da responsabilidade do indivíduo devido a sua periculosidade. Isso não apenas desconsidera a presunção de inocência, mas também alimenta um processo mais amplo de neutralização que exclui "ameaças em potencial".

Na última década, houve um crescente interesse não só sobre a produção do conhecimento, mas do não-conhecimento em Ciência Tecnologia e Sociedade (CTS) e no campo emergente dos "estudos da ignorância" (GROSS; MCGOEY, 2015). A literatura CTS concentrou-se exatamente na representação da ignorância e do não-conhecimento nas práticas de conhecimento científico, um modo de representar as "incógnitas desconhecidas" de um mundo complexo e imprevisível.

Aqui, a ferramenta analítica do não conhecimento nos ajuda a pensar como os modos de "ignorância" são adotados nas práticas de governança da segurança. Como aponta Aradau (2017), os vocabulários de não conhecimento (incerteza, ambiguidade, sigilo e erro) não excluem os vocabulários de conhecimento (como certeza); eles estão intimamente relacionados por uma noção probabilística. Como argumenta Hacking (1975, p.12), a probabilidade tem uma dupla natureza: estatística e epistemológica. A primeira é geralmente associada às técnicas de risco estatísticos na literatura de Relações Internacionais e a segunda é basilar na racionalidade jurídica, ao medir graus de razoabilidade em proposições desprovidas de antecedentes estatísticos (ARADAU, 2017). Assim, a linguagem das probabilidades e da razoabilidade permite que os profissionais de segurança

PUC-Rio - Certificação Digital Nº 1812441/CA

gerenciem a incerteza e calibrem os *graus de certeza* em sua própria produção de conhecimento. Em especial, a questão da justificação do sigilo das agências de inteligência estabelece a fronteira entre saber/ não saber que é essencial para a análise das evidências (como as cartas brancas) nas práticas administrativas francesas como eficientes.

O não-conhecimento é importante para compreender como as questões de conhecimento são mobilizadas como *centrais* ao se fazer reivindicações de responsabilidade através de práticas de divulgação, transparência e visibilidade. A transparência é amplamente defendida no plano político internacional, e há muito tempo entre os órgãos legais e analistas políticos de várias áreas, como parte de um processo moderno de busca de externalizar o poder político no campo visual da percepção comum. A transparência é invocada com frequência em relação a práticas de governança através dos algoritmos e sua perda é, para muitos analistas, o ponto principal dos problemas dos algoritmos (MUSIANI, 2013, p. 141). Na questão da ampliação de uma arquitetura de vigilância e controle com a promulgação das MICAs na França, é exemplar como o conhecimento sobre perfis de risco e o não-conhecimento são promulgados pela inteligência através das práticas de coleta de dados, dos algoritmos "caixa-preta", da opacidade dos processos computacionais, da visualização dos padrões de dados incertos e fluxos sigilosos. Essas práticas contribuem para a autolegitimação que fortalece o *estilo de pensar e fazer* a antecipação do perfil terrorista na França pela comunidade de inteligência como um padrão de eficiência na luta contra o terrorismo; e mesmo quando "falha" ainda é fonte de autoridade importante. A naturalização de tais práticas no campo da inteligência constitui o que Bourdieu chama de *doxa* (BIGO, 2011), um reconhecimento de autenticidade sem, contudo, haver o reconhecimento da arbitrariedade, gerando um compartilhamento espontâneo por um senso prático.

É interessante olhar que se de um lado, a opacidade dos processos algorítmicos reforça a prática discursiva de uma tecnicidade neutra, o que sugere uma abordagem apolítica, a-normativa e acrítica dos códigos (ROUVROY; BERNS, 2015, p. 42), de outro, esses dispositivos são inescapavelmente carregados de vieses (O'NEIL, 2017). Isso é mostrado, por exemplo, com perfis produzidos por algoritmos, que inadvertidamente discriminam populações marginalizadas (BAROCAS; SELBST, 2015; ANISTIA INTERNACIONAL, 2018). Os vieses,

PUC-Rio - Certificação Digital Nº 1812441/CA

aparentemente triviais na análise algorítmica de um volume heterogêneo de dados são importantes à medida que são incorporados nas práticas, aqui em especial nas que constituem a antecipação do perfil de terrorista na França. No entanto, a metáfora da abertura da "caixa-preta" para obter insights e a transparência sobre a topografia da tecnologia pode ser uma abordagem limitada (MATZNER, 2017, p. 44-45). Isso porque o foco exclusivo nos algoritmos e nas tecnologias de coleta de dados e metadados reduz um processo amplo de medidas e ações realizadas com base nas categorizações e avaliações que os dados permitem. Isso não significa que não faz sentido abrir a "caixa-preta"; todavia, seria ingênuo concluir que precisamos apenas de uma melhor compreensão do funcionamento do algoritmo a fim de construir um algoritmo mais justo e imparcial. A transparência é importante como forma de conhecimento para uma governança dos algoritmos; contudo, como argumenta Matzner (2017), esse conhecimento deve ser ancorado em um quadro social, institucional e técnico mais amplo. Segundo Ananny (2015, p.17), é preciso olhar o todo tanto quanto as partes e vê-lo tanto quanto se pode. Isso porque, por exemplo a publicação de códigos algorítmicos ou um conjunto de dados não deixa claro seus processos e práticas ou são consistentemente legíveis e inteligíveis (JOPPA et. al. 2013; STRESSER, 2014). A transparência pode ser um nome que damos à dificuldade de reescrever a separação e distinção entre sujeito e objeto que sentirmos estar ameaçadas. Como de maneira enfática aborda Cheney-Lippold (2011, p.177), as assemblagens sociotécnicas removem os mecanismos tradicionais de resistência e revisão.

Um sistema algorítmico não é apenas constituído pelo código e pelos dados, mas um conjunto de informações humanas e não-humanas. Eles agem nos códigos, práticas e normas institucionalmente, com o poder de criar, sustentar e significar relacionamentos entre pessoas e dados por meio de ação observável e semiautônoma (ANANNY, 2016, p.93). Isso requer ir além dos algoritmos como "objetos fetichizados" e levar em conta as cenas humanas em que os algoritmos, os códigos e as plataformas se cruzam (CRAWFORD, 2016, p.14). Por isso, não é uma questão de responsabilizar os criadores dos algoritmos ou os agentes da inteligência, mas observar a assemblagem desses na produção de conhecimento e promulgação do não-conhecimento. Responsabilizar um conjunto não requer apenas ver dentro de qualquer componente, mas entender como se articula esse sistema. Por isso, o objetivo aqui é analisar como a ampliação dos modos de

PUC-Rio - Certificação Digital Nº 1812441/CA

conhecimento sobre um futuro incognoscível e contingente, tornada possível pelo crescente uso de algoritmos, torna difusa a responsabilidade, fragmentando-a em camadas de práticas para além do humano.

Segundo Tréguer (2019), após 2015 e, com algumas exceções, a influência do campo de direitos humanos no debate global sobre a reforma da vigilância enfraqueceu em conjunto com a atenção da mídia às questões de vigilância do Estado. As práticas e os discursos securitizadores (BIGO, 2008) enquadraram a ameaça terrorista como central na agenda de segurança. Isso conduziu a demandas por parte do campo dos profissionais da segurança para limitar a criptografia, aumentar os recursos e instrumentos de vigilância. O arcabouço discursivo que justifica o aprofundamento do uso de tecnologias e recursos de big data para a governança da segurança ativa um modo de imaginar particular da relação entre o todo e as partes. O "palheiro", metáfora usado pelos profissionais de segurança não se refere mais ao tamanho da amostra, mas às análises de big data no qual "N = toda a população" (MAYER –SCHONBERGER; CUKIER, 2013). Isso não leva apenas a ter mais e mais dados, mas também motiva a confiar no raciocínio probabilístico como uma maneira de renderizar[60] matematicamente a incerteza (ARADAU; BLANKE, 2015).

As análises críticas têm lançado luz para as práticas de vigilância de massa e seus efeitos sobre os direitos e a democracia (BAUMAN et. al., 2015; ROUVROY; BERNS, 2015; ARADAU; BLAKE, 2015). Os profissionais de segurança legitimam essas práticas como não-intrusivas, enquadrando-as em um discurso técnico de que os algoritmos analisam os dados primeiro, enquanto a eles só é acessível o que é processado pelas máquinas (ARADAU; BLANKE, 2015). Nesse sentido, o enquadramento discursivo que justifica a ampliação da vigilância depende de uma distinção entre computadores e analistas de segurança. Essas justificativas não apenas desmontam as críticas à vigilância de massa, mas também são mobilizadas para inibir as reivindicações de pessoas sujeitas a essa prática perante a lei, como observamos nas seções anteriores.

[60] O processo de rederização é pelo qual se obtém o produto final de um processamento digital qualquer. Aqui no caso, a renderizar a incerteza é transformá-la através de processos digitais.

PUC-Rio - Certificação Digital Nº 1812441/CA

A justificativa de separação entre humanos e tecnologias computacionais não tem fácil sustentação se entendermos que a própria computação é envolvida por conjuntos sociotécnicos, uma assemblagem instável e contingente de elementos heterogêneos (LATOUR, 2005). Por isso, precisamos compreender a relacionalidade humana e não-humana, bem como o conteúdo que mantém essas relações. Como argumenta Aradau e Blanke (2015), na segurança através de big data, a assemblagem de humanos e computadores é tanto uma relação, quanto uma divisão de trabalho. Nesta divisão do trabalho há uma integração de um raciocínio humano e de máquina em etapas de processamento e aprendizagem de como classificar o que são informações significativas e o que não são. Eles se relacionam nas mesmas infraestruturas para processar os dados (ibid.). A própria inteligência artificial se desenvolveu como um tipo de "inteligência" que combina raciocínio humano e de máquina. Podemos assumir que mesmos as técnicas não supervisionadas de análise de aprendizado de máquina requererem a participação humana. Nesses modelos, os seres humanos não interagem com os dados apenas no final; estão envolvidos em todas as etapas por meio de avaliação, otimização, treinamento, confecção de bases de dados e outras. Segundo Socher e Manning (2013), o aprendizado de máquina pode ser entendido como uma otimização numérica de peso para representações e características projetadas por humanos. Deste modo, a ampliação do uso de tecnologias digitais não significa que as decisões sejam simplesmente transferidas dos humanos para os algoritmos.

Com podemos observar, tão importante quanto o uso de tecnologias algorítmicas é a enorme quantidade de dados de que essas tecnologias precisam. Os serviços de inteligência franceses justificaram essa necessidade de uma base de dados infinitamente em expansão a partir da ideia de que ter todos os dados pode, algoritmicamente, revelar melhor conhecimento sobre potenciais terroristas, o que tornaria possível a ação antecipatória eficiente. Todavia, o esforço para coletar mais e mais dados pode ser contraproducente para a adaptação dos algoritmos de aprendizado de máquina e para seus métodos, pois geralmente leva a muitos falsos positivos. Isso porque, como cientistas de dados argumentam, quanto maior o "palheiro", maior a probabilidade de que apenas eventos sem sentido sejam adicionados (JANERT, 2010, p. 424). Como observamos na seção 2.2, o terrorismo por ser um evento aleatório e de padrão não bem definido gerar uma gama de falsos

PUC-Rio - Certificação Digital Nº 1812441/CA

positivos tornando difícil distinguir suspeitos “reais” e “falsos”. De modo geral, isso não ajuda a encontrar a agulha no palheiro, mas sim a confirmar se há razão para supor que pode haver uma agulha, mesmo que essa suposição não se confirme.

Essas formas de avaliação e mensuração mediante a análise algorítmica removem os mecanismos de governança de segurança do visível (GANDY, 2010; LEESE, 2014, AMOORE, 2008), e isso representa grandes obstáculos para as ferramentas legais e garantias de direitos. É crucial enfatizar que a lógica preventiva e pré-criminal que foi elucidada nas recentes reformas legais não é nova nas práticas contraterroristas francesas. As práticas contraterroristas francesas estão historicamente enraizadas e validadas em mudanças legislativas que priorizam as medidas administrativas como base para antecipação. Essas práticas têm sido autenticadas através de um entendimento de que atendem aos padrões de eficiência e otimização dos serviços de segurança. A expansão tanto de uma arquitetura de vigilância, como a ampliação de instâncias judiciais que determinam responsabilidade punitiva a indivíduos por suposto vínculo ao terrorismo podem ser analisadas aqui como uma conjugação das racionalidades probabilísticas da segurança e do direito.

A proliferação de legislações antiterroristas criou o que Cahn (2016) descreve como um “dispositivo depreciativo repressivo permanente” integrado ao Direito Penal, mas ancorado em práticas administrativas. A distinção entre os sistemas administrativo e criminal ficou turva na França, isso resultou em violação de direitos (REBETZ; WOUDE, 2018; ANISTIA INTERNACIONAL, 2018; HRW, 2017; WEIL, 2019). O uso do sistema administrativo para impor medidas de controle sobre pessoas, baseadas em informações secretas, violam, além do direito a um processo justo, os direitos à vida privada e familiar, liberdade de circulação e direito ao trabalho (ANISTIA INTERNACIONAL, 2018, p.4). Representantes do Ministério do Interior em entrevista à Anistia Internacional apontam que o limiar de “razões para acreditar" não é insuficiente e que o processo administrativo possui as salvaguardas necessárias (ANISTIA INTERNACIONAL, 2018, p. 20-24). Isso demostra o poder de produção de conhecimento dos serviços de inteligência e a confiabilidade em sua técnica e eficiência, como um poder discricionário.

PUC-Rio - Certificação Digital Nº 1812441/CA

A questão é que os processos de consubstanciação das MICAs não são neutros, apesar da alegada "objetividade" dos discursos da inteligência. Há traços de arbitrariedade e discriminação, como aponta o relatório *Punished without trial: the use of administrative control measures in the context of counter-terrorism in France* da Anistia Internacional (2018), assim como o Collective Against Islamophobia na França (CCIF) e a Human Rights Watch (HRW). Essas organizações foram apoiadas pela Comissão Nacional Consultiva dos Direitos Humanos (CNCDH), órgão de controle dos direitos humanos do governo francês. Além disto, segundo a CCIF tem havido inúmeros relatos de má conduta policial na prática dessas medidas[61].

Outrossim, a organização de Ação dos Direitos dos Mulçumanos denuncia o caráter discriminatório dos "sinais fracos" identificado pela inteligência de uma suposta "radicalização" para a produção dos perfis antecipados de terroristas, que mescla com demasiada frequência com simples sinais de afiliação religiosa[62]. Como afirma a Relatora Especial da ONU, o uso de notas brancas dificulta os direitos da defesa[63]; ao mesmo tempo, este "direito administrativo penal"[64] não oferece as garantias de proteção do procedimento criminal que supostamente regula qualquer medida repressiva[65]. O direito penal tem interpretação estrita e requer que a acusação forneça provas dos atos alegados, o regime instituído pela lei reconhece uma discrição importante na administração e é responsabilidade do litigante, uma presunção de risco que lhe pertence contestar. Neste sentido, o contraditório,

PUC-Rio - Certificação Digital Nº 1812441/CA

[61] Disponível em: https://theconversation.com/inside-emmanuel-macrons-draconian-anti-terrorism-law-83834. Acesso: 11 de junho de 2019.
[62] ADM. "Avis sur le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme", 28 septembre 2017. Disponível em: http://adm1.unblog.fr/2017/09/28/adm-avis-sur-le-projet-de-loi-renforcant-la-securite-interieure-et-la-lutte-contre-le-terrorisme/. Acesso 10 de outubro de 2019.
[63] Rapporteure spéciale sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, "Conclusions préliminaires de la visite", 23 mai 2018. Disponível em: https://www.ohchr.org/FR/NewsEvents/Pages/DisplayNews.aspx?NewsID=23128&LangID=F. Acesso em 11 de outubro de 2019.
[64] LDH, "Avis sur le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme", juillet 2017. Disponível em: https://www.ldh-france.org/wp-content/uploads/2017/10/avis-d%C3%A9taill%C3%A9-sur-le-projet-loi-s%C3%A9curit%C3%A9-int%C3%A9rieure-et-lutte-contre-terrorisme-juillet-2017-envoy%C3%A9-aux-d%C3%A9put%C3%A9s-et-s%C3%A9nateurs.pdf. Acesso em 11 de outubro de 2019.
[65]CNCDH, « Avis sur le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme », 6 juillet 2017. Disponível em: https://www.cncdh.fr/sites/default/files/170706_avis_sur_le_pjl_securite_interieure_terrorisme.pdf . Acesso em 11 de outubro 2019.

garantia essencial de processo penal, está amplamente ausente das disposições da lei, que no privilégio do pré-requisito desfruta a administração[66].

O poder do não-conhecimento está entrelaçado com a produção de conhecedores confiáveis e críveis, bem como produz uma relação de dominação epistêmica. Essa dominação, isola o conhecimento do mundo dominante sobre um mundo que esse conhecimento promulga e reproduz injustiças epistêmicas e sujeitos epistemicamente desfavorecidos (MILLS, 1997 apud ARADAU, 2017). Um exemplo é o vocabulário de probabilidade utilizado pelos serviços de inteligência para caracterizar sua própria produção de conhecimento sobre perfis antecipados de terroristas na França. Quando os analistas da inteligência francesa são demandados pelo tribunal administrativo a mostrar o conteúdo das cartas brancas (mesmo que parcial), eles demostram que as suspeitas inferenciais são articuláveis e razoáveis e se baseiam em relatos de práticas especializadas de coleta e análise de dados.

Desse modo, a incerteza e a certeza não são mutuamente exclusivas no raciocínio jurídico, mas estão intimamente entrelaçadas no raciocínio probabilístico. Contudo, a relação entre incerteza e probabilidade não significa que a incerteza seja atribuída a uma zona de não-conhecimento. Como Hacking (1975, p. 86, tradução minha) aponta, a "probabilidade não é nova na lei". Como observado, os tribunais administrativos ao aceitar apenas as cartas brancas, tomam decisão com base em evidências ambíguas, cada vez menos "certas", no sentido de estarem ancoradas em processos probabilísticos. Todavia, essas evidências são produzidas como razoáveis. A ambiguidade cria um "*blur*" sobre as práticas de vigilância e deixa para os sujeitos sob essas medidas uma zona de não-conhecimento. Isso se aprofunda quando os serviços de inteligência invocam na justificativa de suas práticas o processamento de dados realizado por tecnologias computacionais, processos que são muitas vezes ininteligíveis aos analistas.

Ao mesmo tempo em que testemunhamos a desresponsabilização de possíveis "falhas" e vieses dos profissionais de segurança, cabe chamar atenção para a coexistência desse processo com seu contraste profundo na ponta daquele

[66] Disponível em: http://www.syndicat-magistrature.org/Projet-de-loi-renforcant-la.html. Acesso em 11 de outubro de 2019.

PUC-Rio - Certificação Digital Nº 1812441/CA

que é objeto dessa malha de práticas de vigilância. Trata-se, com efeito, da hiper-responsabilização dos "suspeitos" pelas suas ações potenciais: ao indivíduo perfilado como potencial "terrorista", é imputada uma série de restrições punitivas por algo que ele por ventura sequer cogitou realizar. É seu atravessamento pelas correlações delineadas a partir de um mar de dados que afirmam seu provável caráter perigoso como algo a ser controlado. Portanto, cabe a ele o ônus de provar que não o é, sem de fato ter acesso ou entender como ele foi enquadrado como tal.

Aqui vemos como há um traçar de linha entre modos de incerteza aceitáveis e legítimos e não aceitáveis. A distinção entre especulação e incerteza só é possível à medida que a linguagem probabilística da lei de uma "suspeita razoável" seja reformulada na linguagem de um método científico. Na aplicação das MICAs na França, as cartas brancas demarcam em certa medida tanto zonas de conhecimento – produzidas a partir de um entendimento de conhecimento credível da inteligência –; como de não-conhecimento, porque por serem amplas e não específicas há ausências que tornam o acesso limitado pelos demandantes, advogados e ONGS ativistas dos direitos humanos e civis.

Como analisei, a comunidade de inteligência produz conhecimento sobre o que é entendido como perfil terrorista na França. Há uma ampla noção que as suas práticas e informações devem ser sigilosas tendo em vista o objetivo de resguardar a segurança nacional. Esse argumento de sigilo em razão da segurança foi adotado em larga medida como resposta aos processos administrativos de contestação de MICAs (ANISTIA INTERNACIONAL, 2018). Segundo Balmer (2006, p. 696), o sigilo tanto fratura quando perturba a topografia do conhecimento, isso porque oferece relatos restritos e particulares do mundo. Desse modo, o sigilo não apenas estabelece uma noção de campo da inteligência, aqueles que são conhecedores e produtores credíveis de conhecimento sobre a ameaça terrorista, bem como deslegitima aqueles que não fazem parte deste campo.

As práticas de conhecimento e não-conhecimento têm implicações políticas importantes (ARADAU, 2017) para intervenções individuais, públicas e acadêmicas que contestam o *estilo de pensar e fazer* perfis antecipados de terroristas através dos dados. Como analisei, apesar dos mecanismos de apelação e revisão, as medidas da Lei SILT e da revisão das próprias práticas de vigilância (através da Lei de Inteligência de 2015), esse processo é limitado: a própria

PUC-Rio - Certificação Digital Nº 1812441/CA

instituição cujo objetivo é regular a vigilância – a CNTR – não tem poderes vinculantes; é apenas consultiva. O pequeno número de recursos interpostos em relação ao número de MICAs revela a racionalidade com que opera esse sistema preventivo de possíveis futuros perigosos (REBETZ; WOUDE, 2018). A título ilustrativo, em outubro de 2018, a Comissão de Direito do Senado foi encarregada da supervisão da implementação da lei SILT e, nesse momento, observaram que 70 MICAS foram adotadas e, dentre elas, 68 foram renovadas (DECOEUR; SULZER, 2018).

PUC-Rio - Certificação Digital Nº 1812441/CA

5.
Conclusão

As análises críticas de segurança têm se concentrado na produção de conhecimento, técnicas e dispositivos que visam domesticar as incertezas à medida que tornam os problemas sociais legíveis. Na demanda por segurança e ordem, o futuro torna-se necessariamente acionável, trazendo-o de volta ao presente. Como observamos, a luta contra o terrorismo na França é caracterizada pela interação de lógicas e formas de produção de conhecimento, como também na promulgação do não-conhecimento, em especial na relação entre segurança e lei. As tendências em direção a respostas técnicas, gerenciais e tecnológicas aos desafios à segurança têm assumido centralidade há algum tempo (ABRAHAMSEN; WILLIAMS; BONELLI, 2010). As ferramentas técnicas e tecnológicas – como os algoritmos – se torna parte da "máquina de governo" (AGAR, 2003) na tentativa de domesticar as incógnitas através de práticas de antecipação.

Na discussão proposta, analisei como o argumento de que a otimização dos recursos técnicos e tecnológicos da inteligência é tanto fulcral para a alegada eficiência de seus serviços, como para um discurso de mitigação de abusos através de um controle institucional. A consubstanciação de uma arquitetura técnica centralizada com base normativa dos serviços de inteligência, criou condições de possibilidade para que as práticas de vigilância fossem ampliadas. A aparelhagem técnico-legal da vigilância se tornou ubíqua na rotina dos profissionais de segurança e ancorou medidas administrativas. É importante pontuar que o aumento do uso de medidas administrativas no contexto do combate ao terrorismo (DE GOEDE, 2016) vai além da França e tem visto um aumento alarmante nos últimos anos. O que indica um declínio gradual das salvaguardas processuais e de direitos para a proteção da ordem e segurança.

Portanto, a proposta aqui foi, ao invés de privilegiar um tipo de responsabilidade que precisa examinar o "dentro" dos sistemas tecnológicos, olhar para uma responsabilização que permita examinar através deles, entendendo-os como práticas sociotécnicas que performam a complexidade pela relação e

PUC-Rio - Certificação Digital Nº 1812441/CA

intervenção de humanos e não-humanos. Neste ponto, muitas perguntas sobre possíveis atribuições de responsabilidade permanecem em aberto. Contudo, observamos que apenas as reivindicações de responsabilidade através da afirmação da inevitabilidade tecnodeterminista gerada pela "visão" (transparência e opacidade) pode ser uma forma limitada e desresponsabilizadora. As tentativas de intervenção que olhem apenas os algoritmos podem criar o risco de negligenciarmos as relações sociotécnicas, a difusão das instituições e tecnologias no *estilo de pensar e fazer* prático dos serviços de inteligência, ou seja, a extensão e o reforço desse estilo de pensar e fazer. O risco é a busca por correções em apenas uma parte para tentar conter os aspectos mais perturbadores das práticas de segurança baseadas em dados.

Como observamos, a discricionariedade das práticas de controle sancionadas pela MICA é autorizada e legitimada dentro de um modo particular de produção de conhecimento e promulgação do não conhecimento. Aqui podemos observar como o poder de escrita dos serviços de inteligência aparece como um poder discricionário, que por vezes é negligenciado pela discussão crítica sobre o terrorismo, tecnologia e antecipação (BONELLI; RAGAZZI, 2014). A promulgação do não conhecimento através do sigilo e da ambiguidade das notas brancas nos ajuda a pensar como o *estilo de pensar e fazer* a antecipação do perfil terrorista na França sustenta a si mesmo por meio da produção de conhecimento considerado válido, oportuno e relevante, mas também por meio da opacidade. Isso abre três avenidas para pesquisas futuras. A primeira delas diz respeito a dissecar as condições de emergência dos sujeitos de conhecimento na construção de perfis de risco na França. A segunda veia analítica envolve analisar um ponto chave na arquitetura contraterrorismo na França: a relação entre os serviços de inteligência e os profissionais de segurança; e entre estes e os profissionais do direito nos tribunais. Por fim, cabe aprofundar uma das direções apontadas nesta pesquisa, qual seja, compreender as engrenagens que resultam em um "mathwashing"[67] de ações discriminatórias das práticas antiterror na França.

[67] Trata-se do uso de termos matemáticos, como o algoritmo, para encobrir uma realidade mais subjetiva. O termo foi cunhado pelo cientista de dados Fred Benenson analogamente ao termo whitewashing, para desmistificar uma crença geral de que como a matemática está envolvida, algoritmos são automaticamente neutros (JOH, 2017).

PUC-Rio - Certificação Digital Nº 1812441/CA

Em uma política global cada vez mais marcada pelo conservadorismo, o governo francês reivindica uma postura liberal com discursos de ética, controle e responsabilidade nos processos de inteligência. Contudo, a França aqui é vista ela mesma como caso exemplar de como as práticas iliberais de controle estão imiscuídas e normalizadas nos governos liberais.

PUC-Rio - Certificação Digital Nº 1812441/CA

6.
Referências bibliográficas

AAS, K. F. From narrative to database: Technological change and penal culture. Punishment & Society, 6(4), 379-393, 2004.

AMOORE, L. Algorithmic war: Everyday geographies of the War on Terror. Antipode, 41(1), 49-69, 2009.

AMOORE, L. Data derivatives: On the emergence of a security risk calculus for our times. Theory, Culture & Society, 28(6), 24-43. 2011.

AMOORE, L. Security and the claim to privacy. International Political Sociology, 8(1), 108-112, 2014.

AMOORE, Louise; HALL, Alexandra. Taking people apart: Digitised dissection and the body at the border. Environment and Planning D: Society and Space, v. 27, n. 3, p. 444-464, 2009.

AMOORE, Louise; PIOTUKH, Volha. Life beyond big data: Governing with little analytics. Economy and Society, v. 44, n. 3, p. 341-366, 2015

ANANNY, Mike. Toward an ethics of algorithms: Convening, observation, probability, and timeliness. Science, Technology, & Human Values, v. 41, n. 1, p. 93-117, 2016.

ARADAU, C; VAN MUNSTER, R. (2007) Governing terrorism through risk: Taking precautions, (un)knowing the future. European journal of international relations, v. 13, n. 1, p. 89-115.

ARADAU, Claudia et al. (Ed.). Critical security methods: New frameworks for analysis. Routledge, 2014.

ARADAU, Claudia; BLANKE, Tobias. Politics of prediction: Security and the time/space of governmentality in the age of big data. European Journal of Social Theory, v. 20, n. 3, p. 373-391, 2017.

ARADAU, Claudia; BLANKE, Tobias. The (Big) Data-security assemblage: Knowledge and critique. Big Data & Society, v. 2, n. 2, p. 2053951715609066, 2015.

ARADAU, Claudia; VAN MUNSTER, Rens. The time/space of preparedness: Anticipating the “next terrorist attack”. Space and Culture, v. 15, n. 2, p. 98-109, 2012.

ARADAU, Claudia. Assembling (non) knowledge: Security, law, and surveillance in a digital world. International Political Sociology, v. 11, n. 4, p. 327-342, 2017.

PUC-Rio - Certificação Digital Nº 1812441/CA

BAUMAN, Z. Vigilância líquida: Diálogos com David Lyon. Rio de Janeiro: Zahar, 2013.

BAUMAN, Z., BIGO, D., ESTEVES, P., GUILD, E., JABRI, V., LYON, D., & WALKER, R. B. J. Após Snowden: repensando o impacto da vigilância. Revista Eco-Pós, 18(2), 8-35, 2015.

BERLING, Trine Villumsen. The International Political Sociology of Security: Rethinking Theory and Practice.

BEST, Jacqueline. Ambiguity, uncertainty, and risk: rethinking indeterminacy. International Political Sociology, v. 2, n. 4, p. 355-374, 2008.Routledge, 2015.

BIGO, Didier; ISIN, Engin; RUPPERT, Evelyn (Ed.). Data Politics: Worlds, Subjects, Rights. Routledge, 2019.

BIGO, D. et al. The EU and its Counter-Terrorism Policies after the Paris Attacks. Liberty and Security in Europe No. 84, 27 November 2015.

BIGO, D. Globalized (in) security: the field and the ban-opticon. In Terror, insecurity and liberty Routledge. 20-58, 2014.

BIGO, D. International Political Sociology. In: WILLIAMS, P. (Org.). Security Studies: An Introduction. Londres: Routledge. 116-129, 2008.

BIGO, D. Sécurité et immigration: vers une governementalité por l' inquietude? Cultures & Conflits, 1998.

BIGO, D. Security and immigration: Toward a critique of the governmentality of unease. Alternatives, 27, 63-92, 2002.

BIGO, D. Vigilancia electrónica a gran escala y listas de alerta:¿ productos de una política paranoica?. REMHU-Revista Interdisciplinar da Mobilidade Humana, v. 23, n. 45, 2015.

BIGO, D.; TSOUKALA, A. (Ed.). Terror, insecurity and liberty: Illiberal practices of liberal regimes after 9/11. Routledge, 2008.

BIGO, Didier; WALKER, R.B.J. "Global Counter-Terrorism: From war to the widespread surveillance". In; FERNÁNDEZ, Gabriela Rodríguez et al (Eds.). Warlike Outlines of the Securitarian State: Life Control and the Exclusion of People. CHALLENGE Project: liberty & Security, 2009.

BONELLI, L. La France a peur: Une histoire sociale de" l'insécurité". La Découverte, 2010.

BONELLI, L., & RAGAZZI, F. Low-tech security: Files, notes, and memos as technologies of anticipation. Security Dialogue, 45(5), 476-493, 2014.

BONELLI, Laurent. 'Hidden in plain sight': intelligence, exception and suspicion after 11 september 2001. In: BIGO, D; TSOUKALA, A. (Eds.). Terror, Insecurity

PUC-Rio - Certificação Digital Nº 1812441/CA

and Liberty: Illiberal practices of liberal regimes after 9/11. Londres: Routledge, 2008, p. 100-120, 2008.

BONELLI. L. The control of the Enemy Within? Police Intelligence in the French suburbs (banlieues) and its relevance for globalization. In: Bigo, D. and Elspeth G. (Ed.). Controlling Frontiers. Free Movement into and within Europe. Hants and Burlington, Ashgate, 2005.

BOURDIEU, P. Esboço de uma teoria da prática. In: ORTIZ, Renato (org.). Pierre Bourdieu: Sociologia. Trad. de Paula Montero e Alícia Auzmendi. São Paulo: Ática, 1983 a, p. 46-81.

BOURDIEU, P. A economia das trocas simbólicas (5a ed.). São Paulo: Perspectiva., 2007.

BOURDIEU, P. O Poder Simbólico. Rio de Janeiro: Bertrand Brasil, 2001. 322p.

BOURDIEU, P. The Logic of Practice. Stanford: Stanford University Press, 1990.

BOURDIEU, P; WACQUANT, L. An Invitation to Reflexive Sociology. Chicago: Chicago University Press, 1992. 339p.

BROWNE, Simone. Dark matters: On the surveillance of blackness. Duke University Press, 2015.

BRUNO, Fernanda. Rastrear, classificar, performar. Ciência e Cultura, v. 68, n. 1, p. 34-38, 2016.

BRUNO, Fernanda. Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013

BUERGER, C. “Making Things Known: Epistemic Practices, the United Nations, and the Translation of Piracy.” International Political Sociology 9 (1): 1–18. 2015.

CAHN, O. Cet ennemi intérieur, nous devons le combattre. Le dispositif antiterroriste français, une manifestation du droit pénal de l’ennemi." Archives de politique criminelle 1 (2016): 89-121

CETTINA, Nathalie. Les controles du renseignement: em quoi est-il fragilisé? Centre Française de Recherche sur le Renseignement. Note de Réflexion nº25/ Août 2018. Disponível em: https://www.printfriendly.com/p/g/2FbbvD .

CF2R. État-Major Opérationnel de Prévention du Terrorisme (EMOPT). Centre Français de Recherche sur le Renseignement, 2017. Disponível em: https://www.cf2r.org/wp-content/uploads/2017/05/EMOPT.pdf . Acesso em 11 de outubro de 2019.

CHAMAYOU, Grégoire. Teoria do drone. Trad. Célia Euvaldo. São Paulo: Cosac Naify, 2015.

PUC-Rio - Certificação Digital Nº 1812441/CA

CHAN, Janet; BENNETT MOSES, Lyria. Is big data challenging criminology?. Theoretical criminology, v. 20, n. 1, p. 21-39, 2016.

CHANDLER, D. Conflict knowledge, Big Data and the emergence of emergence. In: LEANDER, A.; WÆVER, O. (Ed.). Assembling exclusive expertise: knowledge, ignorance and conflict resolution in the global South. Routledge, 2018.

CHENEY-LIPOLD, Jerry. A new algorithmic identity: soft biopolitics and the modulation of control. Theory, culture & society, v.28, n.6, 2011, p.164-181.

CHOPIN, O., Une loi polysémique et ambivalente". Les Cahiers français, n° 388, 2016, p. 70-74.

CHOUZENOUX, M. From the "exception" to the" rule": the case of the state of emergency in France following the November Paris attacks. 2016. (Tese de Doutorado).

CNIL (2014) ANACRIM: Logiciels de rapprochement judiciaire à des fins d'analyse criminelle. Disponível em: https://www.cnil.fr/fr/anacrim-logiciels-de-rapprochement-judiciaire-des-fins-danalyse-criminelle. Acesso em 11 de outubro de 2019.

Collectif contre l'islamophobie en France. 2017. "Quand L'urgence Devient La Règle." CCIF, November 2. https://www.islamophobie.net/articles/2017/11/02/quand-lurgence-devient-la-regle/ . Acesso 06 de janeiro de 2020.

CORRIEU, J-M, SAJHAU, P. Sécurité et protection des citoyens: Accroître la prévention et l'action grâce au numérique. Revue de la Gendarmerie 249: 45–49., 2014.

COTTERET. Jean-Marie. Les Fichiers de Police et de renseignement em France. Centre Française de Recherche sur le Renseignement. Rapport de recherche #21. Octobre 2017.

CRAWFORD, K. Can an algorithm be agonistic? Ten scenes from life in calculated publics. Science, Technology & Human Values, 41, 77–92.

CRAWFORD, A; Hutchinson, S. Mapping the contours of 'everyday security': time, space and emotion, British Journal of Criminology. 2015

CRENSHAW, M. Counterterrorism Policy and the Political Process. Studies in Conflict & Terrorism, v. 24, n. 5, p. 329-337, 2001.

CROISSANT, Jennifer L. Agnotology: Ignorance and absence or towards a sociology of things that aren't there. Social Epistemology, v. 28, n. 1, p. 4-25, 2014.

PUC-Rio - Certificação Digital Nº 1812441/CA

DANAHER, John et al. Algorithmic governance: Developing a research agenda through the power of collective intelligence. Big Data & Society, v. 4, n. 2, p. 2053951717726554, 2017.

DEAN, Mitchell. Governamentality: Power and Rule in modern society. London: Sage, 1999.

DE GOEDE, Marieke. The politics of privacy in the age of preemptive security: Introduction. International Political Sociology, v. 8, n. 1, p. 100-104, 2014.

DE GOEDE, Marieke; SIMON, Stephanie; HOIJTINK, Marijn. Performing preemption. Security Dialogue, v. 45, n. 5, p. 411-422, 2014.

DÉLÉGATION PARLEMENTAIRE AU RESEIGNEMENT (2017). Rapport relatif à l'activité de la delegation parlamentaire au renseignement pour l'année 2017. Disponível em: http://www.senat.fr/rap/r17-424/r17-4241.pdf . Acesso em 02 de outubro de 2019.

DELEUZE, G. Post-Scriptum sobre as Sociedades do Controle. In Deleuze, G. Conversações (1972-1990) (p. 219-226). Rio de Janeiro: Editora 34., 1992.

DENÉCÉ, Eric. The intelligence services' historical and cultural context. Handbook of European Intelligence Cultures, p. 135-146, 2016.

DESROSIÈRES, Alain. Statistics and social critique. Partecipazione e conflitto, v. 7, n. 2, p. 348-359, 2014.

DONEDA, D.; ALMEIDA, V. O que é governança de algoritmos? In: BRUNO et al. (org.). Tecnopolíticas da Vigilância: perspectivas da margem. 1. Ed. São Paulo: Boitempo, 2018.

FERGUSON, Andrew Guthrie. Big Data Distortions: Exploring the Limits of the ABA LEATPR Standards. Okla. L. Rev., v. 66, p. 831, 2013.

FERGUSON, Andrew Guthrie. Illuminating Black Data Policing. Ohio St. J. Crim. L., v. 15, p. 503, 2017.

FERGUSON, Andrew Guthrie. The rise of big data policing: Surveillance, race, and the future of law enforcement. NYU Press, 2017.

FOUCAULT, M. Em defesa da sociedade (Curso no Collège de France, 1975-1976) (p.285-315). São Paulo: Martins Fontes, 2005.

FOUCAULT, M. Microfísica do poder. São Paulo: Graal, 2013.

FRANCE. Comprendre la Loi sur le reiseigment. Disponível em: http://www.stop-djihadisme.gouv.fr/lutte-contre-terrorisme-radicalisation/mesures-lutter-contre-terrorisme/comprendre-loi-renseignement. Acesso em 15 de outubro de 2019.

FRANCE. Coordonnateur national du renseignement et lutte contre le terrorisme. Conseil des Ministres, 2017. Disponpivel em:

PUC-Rio - Certificação Digital Nº 1812441/CA

<http://www.gouvernement.fr/conseil-des-ministres/2017-06-14/coordonnateur-national-du-renseignement-et-lutte-contre-le-t>. Acesso em: 15 de outubro de 2019.

FRANCE. La communauté française du renseignement. Paris: Académie du renseignement, 2014.

FRANCE. Law no 2015-912 of 24 July 2015 related to intelligence – Exposé des motifs. Disponível em: http://www.legifrance.gouv.fr/affichLoiPubliee.do;jsessionid=AC82D0703DA2374DEF16BEA404A88989.tpdila23v_3?idDocument=JORFDOLE000030375694&type=expose&typeLoi=&legislature=14. Acesso 10 de outubro de 2019

FRANCE. Trente ans de législation antiterroriste. Vie Publique, 2016. Disponível em: http://www.vie-publique.fr/chronologie/chronos-thematiques/trente-ans-legislation-antiterroriste.html . Acesso em 14 de outubro de 2019.

GARAPON, A. Is there a French advantage in the fight against terrorism? Analisis del Real Instituto, n. 110, 2005

GIUDICELLI-DELAGE. Les transformations de l'administra- tion de la preuve pénale. Perspectives comparées: Allemagne, Belgique, Canada, Espagne, États-Unis, France, Italie, Portugal, Royaume-Uni. Archives de politique criminelle, n° 26, 2004, p. 139-188.

GOFFMAN, E. Stigma and social identity. In: Deviance and Liberty. Routledge. p. 24-31, 2018.

GROSS, Matthias. Risk and ignorance. Burgess, Adam; Alemanno, Alberto; Zinn, Jens (Hg.): Routledge Handbook of Risk Studies. London: Routledge, p. 310-317, 2016.

GROSS, Matthias. Risk as zombie category: Ulrich Beck's unfinished project of the 'non-knowledge'society. Security Dialogue, v. 47, n. 5, p. 386-402, 2016.

HACKING, I. Making up people. In: Biagioli M (ed.) The Science Studies Reader. New York: Routledge, pp. 161—171, 1999.

HACKING, I. Rewriting the soul: multiple personality and the sciences of memory. Princeton: Princeton University Press, 1995.

HACKING, I. The emergence of probability: A philosophical study of early ideas about probability, induction and statistical inference. Cambridge University Press, 2006.

HACKING, Ian, Historical Ontology. (London: Harper University Press, 2002.

HACKING, Ian, The Social Construction of What. (Cambridge, Massachusetts and London, England: Harvard University Press, 1999).

PUC-Rio - Certificação Digital Nº 1812441/CA

HACKING, I. 'On not being a pragmatist : eight reasons and a cause', in C.J. Misak. (eds) New Pragmatists (Oxford: Clarendon Press, 2007), 2, 32-49.

HACKING, Ian. Between Michel Foucault and Erving Goffman: between discourse in the abstract and face-to-face interaction. Economy and society, v. 33, n. 3, p. 277-302, 2004.

HALL, P; HEATH C; COLES-KEMP, L (2015) Critical visualization: A case for rethinking how we visualize risk and security. Journal of Cybersecurity 1(1): 93–108.

HARAWAY, Donna. The actors are cyborg, nature is coyote, and the geography is elsewhere: postscript to 'cyborgs at large'. Technoculture, v. 3, p. 183-202, 1991

HARDING, Sandra. Two influential theories of ignorance and philosophy's interests in ignoring them. Hypatia, v. 21, n. 3, p. 20-36, 2006.

HUYMANS. J. The Politics of Insecurity: Fear, migration and asylum in the EU. New York: Rutledge, 2006.

HUYSMANS, J. The Jargon of Exception: On Schmitt, Agamben and the Absence of Political Society. International Political Sociology, v. 2, n. 2, p. 165–183, 2008

HUYSMANS, Jef. What's in an act? On security speech acts and little security nothings. Security dialogue, v. 42, n. 4-5, p. 371-383, 2011.

IBM – Data analysis – i2 Analyst's Notebook (2016) CT253. Disponível em: http://www-03.ibm.com/software/products/en/analysts-notebook. Acesso em 08 de julho de 2019.

JOBARD, F., LÉVY, R., LAMBERTH, J., & NÉVANEN, S. Mesurer les discriminations selon l'apparence: une analyse des contrôles d'identité à Paris. Population, 67(3), 423-451, 2012.

JOHNS, F. Global governance through the pairing of list and algorithm. Environment and Planning D: Society and Space 34(1): 126–149. 2016.

JOHNS, Fleur. Global governance through the pairing of list and algorithm. Environment and Planning D: Society and Space, v. 34, n. 1, p. 126-149, 2016.

JOHNSON, JA. Technology and pragmatism: From value neutrality to value criticality, SSRN Scholarly Paper, Rochester, NY: Social Science Research. 2006.

JOURNAL DU DROIT ADMINISTRATIF. "Les Moyens De Preuve De La Nécessité Des Mesures De Police Durant L'état D'urgence". JDA (Dossier 1), 2016. http://www.journal-du-droit-administratif.fr/?p=231

KARPPI, T. "The Computer Said So": On the Ethics, Effectiveness, and Cultural Techniques of Predictive Policing. Social Media+ Society, 4(2), 2056305118768296, 2018.

PUC-Rio - Certificação Digital Nº 1812441/CA

KENNEDY, H; MOSS, G; BIRCHALL, C. Balancing the potential and problems of digital methods through action research: Methodological reflections. Information, Communication and Society 18(2): 172–186. 2015.

KITCHIN, R. Thinking critically about and researching algorithms. Information, Communication and Society 20(1): 14–29. 2017.

KLAUSSER. Nicolas. Conformité à la Constitution des mesures individuelles de contrôle administratif et de surveillance". La Revue des droits de l'homme, Actualités Droits-Libertés, mis en ligne le 04 mars 2018. Disponível em: http://journals.openedition.org/revdh/3786. Acesso em 02 de outubro de 2019.

KNUDSEN, Morten. From evidence-based management to management of non-knowledge. Emergence: Complexity and Organization, v. 19, n. 2, 2017.

KRAEMER, Felicitas; VAN OVERVELD, Kees; PETERSON, Martin. Is there an ethics of algorithms?. Ethics and Information Technology, v. 13, n. 3, p. 251-260, 2011.

KUBLER, K. State of urgency: Surveillance, power, and algorithms in France's state of emergency. Big Data & Society, 4(2), 2053951717736338, 2017.

LA QUADRATURE DU NET (2018). Recours contre le Reiseignement. Disponível em: https://www.laquadrature.net/2019/10/11/recours-contre-le-renseignement-compte-rendu-de-notre-audience-devant-la-cour-de-justice-de-lunion-europeenne/ . Acesso 08 de outubro de 2019.

LARNER, Wendy; WALTERS, William (Ed.). Global governmentality. London: Routledge, 2004.

LE MONDE (2018). Des fichiers de police mal organisés et trop complexes. Disponível em: https://www.lemonde.fr/police-justice/article/2018/10/17/des-fichiers-de-police-mal-organises-et-trop-complexes_5370869_1653578.html . Acesso em 10 de junho de 2019.

LATOUR. B. La fabrique du droit: Une ethnographie du Conseil d'État, Collection Sciences Humaines et Sociales, Éditions La Découverte Poche, Paris, 2004.

LATOUR, Bruno. An introduction to actor-network-theory. Reassembling the Social, 2005.

LEANDER, A. 'The Promises, Problems, and Potentials of a Bourdieu-Inspired Staging of International Relations', International Political Sociology 5: 3 (2011), 294-313.

LEESE, Matthias. The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. Security Dialogue, v. 45, n. 5, p. 494-511, 2014.

PUC-Rio - Certificação Digital Nº 1812441/CA

LYON, D. Surveillance society: Monitoring everyday life. Buckingham: Open University Press, 2001.

MALLARD, Grégoire; MCGOEY, Linsey. Strategic ignorance and global governance. 2018.

MAYER-SCHONBERG, V., & CUKIER, K. Big Data: a revolution that will transform how we live, work, and think (p. 73-97). Hoghton Mifflin Harcourt: New York. 2013.

MCCULLOCH, Jude; PICKERING, Sharon. Pre-Crime and Counter-TerrorismImagining Future Crime in the 'War on Terror'. The British Journal of Criminology, v. 49, n. 5, p. 628-645, 2009.

MCGOEY, Linsey (Ed.). An introduction to the sociology of ignorance: essays on the limits of knowing. Routledge, 2016.

MÉGIE, A. De la définition d'un cadre légal à la légitimation d'un nouveau régime de surveillance », Les Cahiers Français, n° 388, 2016, p. 63-69.

MENNICKEN, Andrea; MILLER, Peter. Accounting, territorialization and power. Foucault Studies, n. 13, p. 4-24, 2012.

MITTELSTADT, Brent Daniel et al. The ethics of algorithms: Mapping the debate. Big Data & Society, v. 3, n. 2, p. 2053951716679679, 2016.

MOL, A. Política Ontológica (pp. 63-77). In: Nunes, J. A. & Roque, R. (orgs.). Objectos Impuros. Porto: Afrontamento, 2008.

MORAN, M. Opposing Exclusion: The Political Significance of the Riots in French Suburbs (2005–2007), 19 MODERN &CONTEMP. FR. 297, 303, 2011.

MUCCHIELLI, L. Introduction to the debate: "A state of emergency, what consequences for public policies?". Sociologie, v. 8, n. 4, p. 429-432, 2017.

MUCCHIELLI, L. L'invention de la violence: des peurs, des chiffres, des faits. Paris: Fayar, pp.340, 2011.

MUELLER, Jennifer C. Producing colorblindness: Everyday mechanisms of white ignorance. Social Problems, v. 64, n. 2, p. 219-238, 2017.

MUSIANI, Francesca. Governance by algorithms. Internet Policy Review, v. 2, n. 3, 2013.

MUTLU, Can E. Of Algorithms, Data and Ethics: A Response to Andrew Bennett. Millennium, v. 43, n. 3, p. 998-1002, 2015.

NAKAMURA, L. Cybertypes: Race, Ethnicity, and Identity on the Internet, New York: Routledge. 2013.

PUC-Rio - Certificação Digital Nº 1812441/CA

NEOCLEOS, M. The Problem with Normality: Taking Exception to “Permanent Emergency”. Alternatives 31 (2): 191–213. 2006.

NIELSEN, Kristian H.; SØRENSEN, Mads P. How to take non-knowledge seriously, or “the unexpected virtue of ignorance”. Public Understanding of Science, v. 26, n. 3, p. 385-392, 2017.

NYERS, Peter. The accidental citizen: acts of sovereignty and (un)making citizenship. Economy and society, v. 35, n. 1, p. 22-41, 2006.

O’NEIL, C. The era of blind faith in big data must end. TIW Spreading (ed.), 2017a

O'NEIL, C. Weapons of math destruction: How big data increases inequality and threatens democracy. Broadway Books. 2017b.

OROZCO, Alex Mulattieri Suarez et al. Balanceamento entre segurança e desempenho na comunicação entre os planos de controle e dados em redes definidas por software. 2018.

PASQUALE, Frank. The black box society. Harvard University Press, 2015.

PAYE, Jean-Claude. Monthly Review; New York. Vol 67. Ed. February 2016. 1-12.

PERRY, Walt L. Predictive policing: The role of crime forecasting in law enforcement operations. Rand Corporation, 2013.

PROCTOR, Robert N.; SCHIEBINGER, Londa. Agnotology: The making and unmaking of ignorance. 2008.

RABINOW, P. Anthropos Today. Reflections on Modern Equipment. Princeton: Princeton University Press. 2003.

ROSE, Nikolas. Governing by numbers: Figuring out democracy. Accounting, organizations and society, v. 16, n. 7, p. 673-692, 1991.

ROUVROY, Antoinette; BERNS, Thomas. Le nouveau pouvoir statistique. Multitudes, n. 1, p. 88-103, 2010.

ROUVROY, A.; BERNS, T. Governamentalidade algorítmica e perspectivas de emancipação: o díspar como condição de individuação pela relação? In: BRUNO et al. (org.). Tecnopolíticas da Vigilância: perspectivas da margem. 1. Ed. São Paulo: Boitempo, 2018.

RUPPERT, Evelyn; ISIN, Engin; BIGO, D. (2017). Data politics. Big Data & Society, v. 4, n. 2, p. 2053951717717749.

SARMA. K. M. Risk assessment and the prevention of radicalization from nonviolence into terrorism. Am Psychol 72(3):278–288, 2017.

PUC-Rio - Certificação Digital Nº 1812441/CA

SALTER, Mark B. When securitization fails:The hard case of counter-terrorism programs. In: Securitization Theory. Routledge, 2010. p. 130-146.

SCHERRER, A., BIGO, D. Will the democratic debate over counterrorism gain the edge in battle?. Open Democracy, v. 11, 2015.

SOCHER, R.; MANNING, C. Deep learning for natural language processing (without magic). In: Keynote at the 2013 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (NAACL 2013). 2013.

STAVRIANAKIS, Anna. Requiem for risk: non-knowledge and domination in the governance of weapons circulation. International Political Sociology, 2019.

TRÉGUER, Félix. SEEING LIKE BIG TECH. Data Politics: Worlds, Subjects, Rights, 2019.

TRÉGUER, Félix. Intelligence reform and the Snowden paradox: The case of France. 2017.

TRÉGUER, Félix. From deep state illegality to law of the land: The case of internet surveillance in France. In: 7th Biennial Surveillance & Society Conference (SSN 2016):" Power, performance and trust". 2016a.

TRÉGUER, Félix. French Constitutional Council Strikes Down" Blank Check" Provision in the 2015 Intelligence Act. 2016b.

TSOUKALA, A.; CEYHAN, A. Contrôle de l'immigration: mythes et réalités. Cultures & Conflits, 1997.

TSOUKALA, Anastassia. Risk-focused security policies and human rights: The impossible symbiosis. In: Mapping Transatlantic Security Relations. Routledge, 2010. p. 55-73.

VAN MUNSTER, R; ARADAU, C. Politics of catastrophe: genealogies of the unknown. Routledge, 2011.

VILLANI, C.; LONGUET, G. Rapport de MM. Cédric VILLANI, député et Gérard LONGUET, sénateur, fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiquesn° 305 (2017-2018). Disponível em: https://www.senat.fr/rap/r17-305/r17-305.html. Acesso em 11 de outubro de 2019.

VOUCHEZ, S.; SLAMA, S. Harry Potter au Palais Royal? La lutte contre le terrorisme comme cape d'invisibilité de l'état d'urgence et la transformation de l'office du juge administrative. Les Cahiers de la Justice, Dalloz, 2017, pp. 287, 288.

WACQUANT, L. Seguindo Pierre Bourdieu no campo. Revista de Sociologia e Política, 26, 13-29, 2006.

PUC-Rio - Certificação Digital Nº 1812441/CA

WANG, Jackie. Carceral capitalism. MIT Press, 2018.

WARE, L. Color-blind racism in France: Bias against ethnic minority immigrants. Wash. UJL & Pol'y, 46, 184-244, 2015.

WEIL. S. Terror in Courts – French conter-terrorism: Administrative and Penal Avenues. Report for the official visit of the Un Special Rapporteur on Counter-Terrorism and Humans Rights. May 2018. Disponível: https://www.sciencespo.fr/psia/sites/sciencespo.fr.psia/files/Terror%20in%20Courts_2.pdf. Acesso 25 de agosto de 2019.

WILCOX, Lauren B. Bodies of violence: Theorizing embodied subjects in international relations. Oxford University Press, USA, 2015.

ZEDNER, Lucia. Pre-crime and post-criminology?. Theoretical criminology, v. 11, n. 2, p. 261-281, 2007.

ZIEWITZ, M. Governing algorithms: Myth, mess, and methods. Science, Technology & Human Values, 41, 3–16. 2016.

ZOUAVE, E. T.; MARQUENIE, T. An Inconvenient Truth: Algorithmic Transparency & Accountability in Criminal Intelligence Profiling. 2017 European Intelligence and Security Informatics Conference (EISIC), 2017.

PUC-Rio - Certificação Digital Nº 1812441/CA