Poder das armas matemáticas de investigação criminal em massa

Se você chegar em sua casa e a porta estiver trancada, abrindo-a com as suas chaves, poderá verificar que as janelas estão íntegras ao lançar rapidamente um olhar, terá a "sensação analógica de segurança", ainda que seus dispositivos eletrônicos-digitais tenham sido objeto de "penetração digital". É que a "sensação de segurança" ainda está vinculada aos referenciais "analógicos", pelos quais, sem suporte material da "invasão", acredita-se seguro. Essa é uma das faces da ingenuidade digital e das novas bases

As "Estratégias de Guerra", amplamente utilizadas e incorporadas no ambiente da investigação criminal, sempre foram ensinadas no contexto analógico. Ainda são utilizadas em situações de enfrentamento, cada vez mais raras, salvo nas ações de captura em território hostil. De qualquer forma, as práticas de investigação autorizam a utilização de medidas cautelares probatórias analógicas e arriscadas, especialmente a busca e apreensão, o agente infiltrado, a escuta ambiental, dentre outras. Mas a tática da "Emboscada Analógica" contava com planos em que o terreno deveria ser propício ao evento, isto é, as condições de tempo e espaço precisavam ser planejadas, coordenadas e contar com recursos humanos treinados para colocação em prática da "atividade de campo". O estereótipo construído pelos filmes e reproduzidos nas ações policiais, em geral, assumem o *script* dos filmes de Hollywood e/ou do "Tropa de Elite", com "heróis da guerra", fortes, destemidos e brutais.

Atualmente, os protagonistas da "guerra digital" são "nerds", "hackers" e "crackers" de "óculos", "magrelos" e desprovidos de explosão física, cujo exemplo típico é Edward Snowden (aqui). A guerra de baixas calorias não depende de armas bélicas e sim de teclados, inteligência, ausência ou ambiguidade de regras, vinculadas ao discurso do medo.

O Brasil está licitando a banda 5G que, associada ao poder de processamento das máquinas inteligentes, ao agigantamento dos sensores produtores de dados no cotidiano, principalmente por meio da "Internet das Coisas" (OiT) e "Cidades Inteligentes" (*Smart Cities* — confira o evento do Conpedi sobre o tema aqui dias 9-12 de novembro de 2021), promoverá a ampliação das oportunidades de "vasculhamento digital" no contexto da "computação ubíqua". Os casos das investigações com o uso de "Geo-fencing" (aqui), aquisição de dados apagados dos dispositivos com o software "Cellebrite" (Caso Henry — aqui) ou ainda as penetrações com "click zero" proporcionadas pelo software "Pegasus" (aqui e aqui), constituem apenas a "ponta do iceberg". As oportunidades digitais no campo da *Open Search Intelligence* (Osint), por exemplo, com custo baixo e curva de aprendizagem reduzida, conferem condições para facilmente localizar alvos. Por exemplo, pode-se identificar perfis falsos das redes sociais, foragidos ou mesmo os comentaristas *fakes* dos artigos publicados na **ConJur** (confira o OSINTFramework aqui).

A Emboscada Digital encontra menor resistência porque os alvos sequer sabem da "penetração silenciosa". É que a "penetração digital" captura os dispositivos de modo discreto, sem que existam os riscos associados à invasão territorial. O predomínio de ações ostensivas ou de investigações analógicas, por meio de investigadores em campo, agentes infiltrados, medidas cautelares probatórias, passa a ser o segundo estágio das investigações. O primeiro estágio é o da apuração digital sem fricção, desprovida de controles públicos, em que o *draw* digital é estruturado. Posteriormente, definidos os alvos, os agentes da investigação analógica são acionados para materializar e confirmar o que "já se sabia". As etapas da investigação são invertidas, com o prévio vasculhamento de evidências, longe da claridade do Devido Processo Legal.

Se a missão é a de obter os dados e as informações necessárias, eventual excesso dos meios acaba sendo contabilizado pela ambiguidade legislativa, situando-se entre as fronteiras de conteúdo variado entre as Agências ou Centros de Inteligências e as Agências de Controle Social. A dissimulação digital camufla-se em nome da "Doutrina da Inteligência" ou de "Estratégias Nacionais" para, à sorrelfa, poder manejar impunemente o potencial das ferramentas digitais. Configuram a "Doutrina do Poderio Digital". Os meios de obtenção de provas digitais são muito mais precisos e acurados, com danos humanos zero, além de poderem ser operados de longa distância. A violação dos Direitos Fundamentais é considerada apenas como um dano colateral, adequado e necessário à obtenção do resultado pretendido. Talvez seja o caso de se assumir o "Estado de Exceção Digital" para, então, poder-se indicar mecanismos de resistência (aqui). A noção de público e privado cedeu espaço para novas fronteiras sem marcos de ultrapassagem fixos, a saber, em nome de interesses maiores de Segurança Pública, a superioridade tecnológica do Estado, especialmente as inescrutáveis "Unidades de Inteligência" que operam à margem dos controles do processo penal, autoriza-se, sem mais, a penetrar no antigo regime privado. Por mais paradoxal que possa parecer, vivencia-se o regime da privacidade aberta (*Open Privacity*)

O Direito Fundamental à Privacidade passa a ser gerenciado por diversas normativas que potencializam a "desregulamentação", submetendo a eficácia ao preenchimento de diversos requisitos, termos e condições. Por mais que a preocupação com a Proteção de Dados (pessoais e/ou sensíveis) apresente-se no discurso manifesto, o discurso latente tolera as reiteradas violações por meio de distinções sobre a finalidade da aquisição. Tanto assim que a LGPD exclui da proteção os dados necessários à investigação criminal, a segurança pública, sem que a lei específica tenha sido votada. No contexto da aplicação normativa, prevalece o jargão intuitivo e, também, manipulador, da inexistência de Direitos Fundamentais Absolutos. Ainda que se possa acolher, em potência, a ausência de Direitos Fundamentais Absolutos, a flexibilização deixa de ser analisada *a priori*, vinculando-se às ponderações oportunistas *a posteriori*. Com isso, as violações aos Direitos Fundamentais passam a ser meros "danos colaterais" em nome de um bem maior, a Segurança.

Se todos passam a ser alvo de monitoramento, diante dos riscos sistêmicos, a quantidade de dados produzidos exige que as máquinas realizem o processamento, a partir da correlação de variáveis (entidades, relacionamento, instâncias etc.), previamente selecionadas pelos agentes de segurança, por meio de algoritmos de classificação e de agrupamento. A exigência de significância estatística depende dos pesos atribuídos e quando o padrão de risco reduz a significância, correlações espúrias tendem a gerar falsos positivos. É que a máquina ainda encontra dificuldades para estabelecer o contexto das inferências. A ambiguidade das palavras, no campo da pragmática, promove a ocorrência de falsos positivos (Erro Tipo I).

Foi o que aconteceu em 2008 com uma família de *Long Island*, em Nova York, quando as “máquinas de monitoramento” do navegador usado, a partir dos dados relacionados ao IP (*Internet Protocol*) identificaram pesquisas cruzadas com os termos “panela de pressão” e “mochila”, artefatos utilizados para produção de bombas e atentados terroristas. A família de Michele Catalano foi "visitada" por agentes do FBI. Segundo o site G1 "*Michele conta que seu marido estava na sala de casa com os cães da família, por volta das 9h da manhã, quando notou que três carros SUVs fecharam as entradas da casa. Seis agentes armados saíram das viaturas e cercaram a propriedade — dois se dirigiram à porta principal. 'Ele (o marido) saiu e os homens imediatamente mostraram as credenciais', escreve ela. Em seguida, o grupo de investigadores pediu para revistar a casa — o que, de acordo com a jornalista, foi feito superficialmente — e fez perguntas como 'Onde o senhor nasceu?', 'Onde nasceram seus pais?', 'Você tem alguma bomba?' e 'O senhor tem uma panela de pressão?'. O marido respondeu 'não' às perguntas finais, e acrescentou que apenas possuía uma panela de fazer arroz. 'Você poderia fazer uma bomba com ela?', teria perguntado um dos policiais. 'Não. Mas minha mulher a usa para fazer quinoa', respondeu o marido, despertando a curiosidade dos agentes. "Que m… é essa, quinoa?", perguntou um dos agentes. Após mais revistas no quintal da casa, a pergunta final: "O senhor já pesquisou (na internet) sobre como construir uma bomba com uma panela de pressão?" Segundo Michele, o marido respondeu também com uma questão: 'Nenhum dos senhores jamais ficou curioso sobre como alguém pode construir uma bomba com uma panela de pressão?' Dois agentes teriam respondido que sim. "Naquele momento, eles perceberam que não estavam lidando com terroristas", escreveu Michele. Os agentes teriam dito ainda que visitas como esta, que durou 45 minutos, ocorrem cem vezes por semana, sendo que em apenas 1% dos casos as suspeitas tem algum tipo de desdobramento. Mais tarde, o departamento de polícia do condado de Suffolk admitiu ter realizado a operação após as buscas que a família fez na internet. Michele prometeu nunca mais tentar comprar uma panela de pressão em sites de vendas online"* (aqui).

O aparelhamento das polícias (Civil e Militar) e dos Ministérios Públicos contracena com a desaparelhamento das Defensorias Públicas e com o modelo de Advocacia Criminal fragmentado. A manutenção da exclusão digital defensiva confere alarmante vantagem competitivo do Estado (Polícia e Ministério Público). Associada à mentalidade autoritária legada no campo do Processo Penal, renovam-se as estratégias de proibição e/ou de limitação de acesso à defesa das mesmas ferramentas. O esforço defensivo, no campo tecnológico, depende de iniciativas isoladas de profissionais liberais que investem em tecnologia. A diferença de máquinas e de acesso aos dados à defesa (pública e privada) amplia a “disparidade de armas tecnológicas”, justamente porque os profissionais e/ou Instituições que investem em tecnologia acabam obtendo melhores resultados, ainda mais quando adotam práticas oportunistas.

O dever de investigação fomenta práticas de "*Fishing Expedition Digital"*[1] por meio do qual "vasculham-se" a vida, o patrimônio, violando-se Direitos Fundamentais, "p*ara ver o que se acha"* . Depois, promove-se algum mecanismo de "esquentamento". Do ponto de vista da “estrutura de incentivos”, diante da reduzida (ainda) possibilidade de descoberta e punição, o comportamento oportunista digital truculento se potencializa, ainda mais no contexto de *Lawfare*. O lema dos oportunistas é o de “quem não deve não teme”, embora quem enuncie defenda, depois, a ilicitude das provas obtidas por crackers, ou seja, adota o garantismo seletivo e/ou conveniente de ocasião.

Diante da algo suspeito, surge o dever de investigar, em que os limites éticos são suspensos, em nome da estratégia assumida da “Doutrina da Segurança”. O *standard* probatório do suporte fático resta rebaixado, validando-se intuições, expertises, estereótipos, preconceitos, das mais variadas formas. O "Procedimento Operacional Padrão – POP" acopla fatores de risco em que a prévia exigência de "causa provável" resta flexibilizada em nome do resultado. Os abusos estão previamente justificados diante da "democratização da truculência", afinal, estão “apurando crimes”. A cadeia de comando, por sua vez, diante da dinâmica, velocidade e ambiente digital, transfere-se ao nível operacional, isto é, não se trata mais do cumprimento de Planos de Ação definidos e determinados. A Nova Ordem de Segurança Digital aposta na distribuição mais homogênea do que Scott Shapiro denominou de Economia da Confiança. A rapidez da ação sempre foi essencial no campo das batalhas, no meio digital ele depende de "um click".

A tolerância do Poder Judiciário associa-se ao modelo em nome dos resultados. Garantias processuais são rebaixadas em nome dos interesses coletivos. O duplo do discurso configura-se pelo rebaixamento dos Direitos Fundamentais em nome dos Direitos Fundamentais, por meio da estratégia de que não existem Direitos Absolutos e pela adoção de uma metodologia *ad-hoc* de ponderação, desde antes acolhida pelas Agências de Controle Social.

Se o "inimigo" está entre nós, além da suspeita universal, o desafio é separar o "sinal" do "ruído" (aqui), em que as táticas englobantes justificam práticas digitais hostis contra potenciais adversários, mesmo sem “causa provável”. A estratégia rompe as barreiras analógicas, exigindo a decisão urgente da inclusão digital, ou seja, de se dar o passo tecnológico, na linha do que defendem, por exemplo, Richard Susskind (No Brasil: Fabiano Hartmann, Isabela Ferrari, Dierle Nunes, Juarez Freitas, Barbara Guasque, Roberta Zumblick da Silva, Fausto Morais, Marcella Nardeli, Spencer Sydow, Elias Jacob, José Bolzan de Morais, Flaviane Barros, Juarez Freitas, Sabrina Leles, Bernardo de Azevedo, dentre outros — não deu para citarmos todos).

Por isso, a invocação do livro de Cath O’Neil (aqui) como título, porque as coordenadas de realidade se modificaram e, quando você estiver lendo o texto, em casa ou no escritório, mesmo sem sinais de violação, pode estar sendo "vasculhado digitalmente". E não adianta perguntar: Alexa, alguém está me vigiando? O "Calcanhar de Aquiles" da Investigação Estatal Digital oportunista são os "rastros digitais". A ofensiva contra a Cadeia de Custódia Digital e a prevalência da Regra de *Brady* na versão Digital decorrem do problema da preservação de evidências ilícitas. As táticas de "cobertura" são, em geral, a alegação de interesses nacionais, de sigilo dos documentos, em que as normas de transparência e de *accountability* (vertical e horizontal) são invocadas para o fim de evitar a descoberta dos comportamentos oportunistas. Além disso, o discurso prevalecente vale-se dos resultados obtidos, da manipulação ideológicas, do desconhecimento dos membros do Poder Judiciário e da mentalidade autoritária. A conjugação destes fatores é, ainda, suficiente ao bloqueio dos atos ilegais eventualmente praticados. Mas os "rastros" tendem a permanecer e, com os meios certos, mais dia, menos dia, acabam sendo descobertos.

[1] SILVA, Viviani Ghizoni a; MELO E SILVA, Philipe Benoni; MORAIS DA ROSA, Alexandre. ***Fishng Expeditions*** **e Encontro Fortuiro na Busca e Apreensão**: um dilema oculto do Processo Penal. Florianópolis: EMais, 2022.

Date Created

05/11/2021