SIMPÓSIO MERCADOS DE PROTEÇÃO E GOVERNANÇA DA SEGURANÇA

UNIVERSIDADE ESTADUAL DE LONDRINA

12 a 14 de junho de 2019

GT GOVERNANÇA MULTICÊNTRICA DA SEGURANÇA

Policiamento em rede: um levantamento das instituições e atores que atuam na segurança da Internet no Brasil

Marcelo da Luz Batalha
Professor no Instituto Federal Goiano-Ceres; mestre em Ciência Política (Unicamp); doutorando em Sociologia (Unicamp).

Policiamento em rede: um levantamento das instituições e atores que atuam na segurança da Internet no Brasil

Marcelo da Luz Batalha[1]

Resumo
O cibercrime tem ganhado visibilidade e interesse público no Brasil nos anos últimos anos, seja por eventos que causam pânico moral na sociedade ou eventos que envolvam celebridades que são vítimas de algum crime virtual decorrente de exposição na Internet. Contudo, o fenômeno do cibercrime e suas vítimas têm sido mais reais e comuns. Para combater e reprimir o cibercrime, foram criadas delegacias especializadas ligadas às polícias civis dos Estados. Este trabalho é fruto de pesquisa para o doutorado em Sociologia, que tem como método de pesquisa a etnografia de delegacias e eventos sobre o tema do cibercrime e cibersegurança no Brasil. O objetivo é apontar os desafios ao policiamento na Internet, especialmente pelas delegacias especializadas que atendem o grande público, e apresentar que o modelo de policiamento na rede deveria seguir o modelo nodal, com a participação de vários atores. A pesquisa identificou alguns atores que atuam no policiamento contra os crimes cometidos pela rede mundial de computadores no Brasil. Porém, ainda existe uma distância entre esses atores com a instituição policial. Como um fenômeno que ainda não é visto como um problema a ser enfrentado pela segurança pública, o cibercrime e a cibersegurança tem sido tratado principalmente pelos atores privados.

Palavras-chave: Segurança; Policiamento; Internet, Cibercrime.

Introdução.

Historicamente o policiamento esteve ligado à territorialidade e a necessidade de controle e segurança de espaços definidos fisicamente. Com o avanço tecnológico, a diversificação do consumo e usos das tecnologias da informação e comunicação – computadores, celulares – a mentalidade sobre o território a ser policiado e monitorado transformou-se. Os riscos e crimes ainda estão circunscritos nas ruas, onde se exige um policiamento ostensivo de viaturas policiais, para o controle e a prisão de criminosos e suspeitos, mas existem riscos e crimes cometidos na supervia da informação (*information superhighway)*, termo popular usado nos anos 90 para se referir aos sistemas de comunicação digital e à rede de telecomunicações da Internet (CASTELLS, 2003).

1 Professor de Sociologia no Instituto Federal Goiano-Ceres; mestre em Ciência Política (Unicamp); doutorando em Sociologia (Unicamp). E-mail: mabatalha@gmail.com.

O resultado manifesta-se na nossa própria compreensão do que é o mundo "real" e propõe desafios às instituições sociais. A Internet alterou extensivamente a economia, a política e a cultura nas mais diversas sociedades. A participação política e a democracia, hoje impactada pelas novas tecnologias, nos faz enfrentar as notícias falsas (*fake news)*. Crianças, jovens e adultos ressignificam suas sociabilidades através de comunidades, culturas e subculturas baseadas na Internet, da educação às formas de relacionamento amoroso. Os problemas perpassam todas as esferas e instituições sociais até então tidas como sólidas.

No mais recente episódio que envolveu educação, sociabilidades, comportamentos juvenis e Internet, o ataque à escola de Suzano, trouxe novamente para o debate público os desafios para a resolução dos problemas da violência na nossa sociedade, agora potencializadas pela Internet e suas camadas, revelando a rede profunda e escura (*deep* e *dark web*).

Há tempos a Internet vem sendo objeto e campo de estudos das Ciências Sociais. Os seus usos políticos, as transformações e impactos culturais e econômicas mais diversos. Após ter estudado, no mestrado[2], uma rede mundial de ativistas que (re)elaborava repertórios e estruturas para a manifestação política na rede mundial, permeada pela discussão da privacidade, anonimato e contra-vigilância, tendo acompanhado o processo de discussão pública e da elaboração das leis civil e penal para a Internet no Brasil – o Marco Civil da Internet e a Lei 12.737 de delitos informáticos – voltei-me para o problema dos crimes cibernéticos, mais especificamente para as delegacias especializadas e os atores envolvidos na governança da segurança (GARRIOTT, 2018), no que diz repeito à Internet.

A caracterização sociológica e criminológica do problema e a pesquisa são sustentadas por bibliografias internacionais sobre cibercrime (WALL, 2007; LEMAN-LANGLOIS, 2008; YAR, 2006), pois as referências biográficas nacionais sobre o tema ainda estão produzidas por especialistas da área da computação e da segurança da informação, por policiais ativos, quase sempre lançando manuais práticos de resolução de investigação na seara do cibercrime.

A proposta de trabalho está pautada na ideia do policiamento em rede e em nós, na intersecção de atores públicos e privados no combate e resolução de cibercrimes, apresentada pelos pesquisadores Johnny Nhan e Laura Huey (2008) e

2 BATALHA, Marcelo da Luz. **Novas fronteiras para a comunicação ativista em rede: um olhar sobre o centro de mídia independente**. 2010. Dissertação (Mestrado em Ciência Política). Instituto de Filosofia e Ciências Humanas, Universidade Estadual de Campinas, Campinas.

Wall (2010) para pensar os atores envolvidos no ecossistema de policiamento da Internet no Brasil.

O impacto da Internet na operação do crime.

A Internet foi desenvolvida e introduzida no mundo acadêmico dos Estados Unidos nos anos 50, mas a sua exploração comercial global data de fins da década de 80. A Internet revolucionou a maneira como vemos, agimos no mundo e nos definimos. O seu impacto foi extensivo, modificando desde os comportamentos primários de socialização e sociabilidade, a educação, a política, a economia, alterando e embaralhando as fronteiras territoriais e de jurisdições.

Apesar de existir muitos pontos positivos sobre os impactos da Internet, a rede mundial de computadores provoca novos e velhos desafios para a sociedade, como no campo dos crimes e da segurança. Os crimes cometidos pelos meios eletrônicos ou digitais, comumente chamados de cibercrimes, são crimes novos que merecem uma nova teoria sobre o crime?

Ao mesmo tempo em que a Internet é massivamente apropriada pela população mundial, através de políticas públicas de inclusão digital ou inclusão induzida por grandes empresas de tecnologia, como Google e Facebook, seu uso social é desigual e diverso.

Esta desigualdade de acesso e apropriação das novas tecnologias de comunicação e informação espelha as desigualdades econômicas, culturais e políticas do mundo real. Culturalmente, vemos reproduzir na Internet comportamentos e crimes do cotidiano, como crimes de racismo, discurso de ódio, difamação e algumas novas variações de crimes contra grupos sociais vitimizados: mulheres, LGBT's e negros. O caso das mulheres é exemplar, pois foi o maior público vitimizado que recorria às delegacias especializadas, durante a pesquisa de campo, dado que corrobora com o crescimento de 1.640%, no ano de 2018 em relação ao ano de 2017, de denúncias de violência contra as mulheres na Internet, no Brasil[3].

O aspecto econômico também espelha as desigualdades reproduzidas no cotidiano, principalmente a divisão econômica regional existente no mundo e no

3 SUPERIOR TRIBUNAL DE JUSTIÇA. *Crimes sexuais pela internet:* a violência contra a mulher entre o real e o virtual. Disponível em http://www.stj.jus.br/sites/STJ/default/pt_BR/Comunicação/noticias/Not%C3%Adcias/Crimes-sexuais-pela-internet:-a-violência-contra-a-mulher-entre-o-real-e-o-virtual. Acesso em 24 mai. 2019.

Brasil. Segundo Nir Kshetri (2013), que realizou pesquisa extensiva sobre os crimes financeiros em países como Brasil, Índia, países da África e da antiga União Soviética, o cibercrime colocou novos desafios às relações econômicas internacionais, apresentando um padrão representativo da divisão econômica mundial: os ataques e fraudes têm origem nos países do sul global tendo como vítimas indivíduos e instituições financeiras dos países desenvolvidos (KSHERTRI, 2013, p. 4).

Este padrão representa uma divisão e desigualdade social econômica, que é compensada pela prática do crime financeiro cometido pela Internet. Tal fenômeno se reproduz no Brasil, quando as vítimas alvo concentram-se nas regiões sudeste e sul, e as origens dos ataques concentram-se nas regiões centro-oeste e norte do país. É o que Misha Glenny (2011) revela com a sua investigação junto a esquemas de cibercriminosos do leste europeu: é uma motivação *à la* Robin Hood, ou seja, a fraude, transferência e saque através de engenharia social ou vírus pela Internet, voltado para os cidadãos das regiões mais ricas representa a reapropriação da riqueza concentrada. Agora sem a necessidade de sequestros relâmpagos, assalto a bancos físicos, basta encontrar uma brecha na segurança dos bancos *online*, nos computadores dos usuários, a paciência dos atacantes até que as suas vítimas cliquem, motivados pela curiosidade ou ganância, sobre um *link* que lhe revelará imagens exclusivas ou lhe retornará alguma recompensa ou herança desconhecida.

A Internet impacta, assim, o campo da criminologia e da segurança, pois reproduz velhas e novas formas de crimes e motivação. As vítimas, também, não são diferentes, não são virtuais, como comumente relacionamos e qualificamos os fatos e objetos com a Internet, mas são vítimas reais.

Definição de cibercrime.

O termo “cibercrime” é um termo genérico usado como sinônimo de *crimes tecnológicos, crimes de alta tecnologia, crimes de Internet, crimes digitais, crimes eletrônicos, crimes cibernéticos.* As próprias delegacias especializadas neste tipo de crime não têm um nome padrão e utilizam os diversos significados descritos acima[4].

4 SAFERNET BRASIL. *Delegacias cibercrimes.* Disponível em https://new.safernet.org.br/content/delegacias-cibercrimes. Acesso em 24 mai. 2019.

A Lei 12.737/12[5], a lei brasileira de cibercrimes, intitula os crimes previstos como delitos informáticos.

A lei em questão tipifica como delitos informáticos a invasão de dispositivos eletrônicos conectados ou não à Internet sem autorização expressa ou tácita do titular, a instalação de vulnerabilidade (vírus) para obter vantagens e a interrupção de serviços de utilidade pública que dependam da conexão com a Internet.

Pela lei brasileira, o que se entende por cibercrime são atos envolvendo computadores com fins de tirar vantagens ou danos a pessoas e computadores. A bibliografia sobre o tema chama a atenção para o fato de que nem todos os atos que se enquadram como cibercrime devam ser considerados como crimes novos e que necessitam uma nova tipificação criminal. De fato, a característica do cibercrime é o uso de dispositivos eletrônicos e a conexão destes dispositivos com a Internet, alterando o meio e o alcance do crime. Mas atos considerados delitos genuinamente eletrônico ou digital são os que retirando os computadores de cena, deixariam, como a infecção por vírus e o impedimento de acesso a computadores e serviços através da negação por ataque ou criptografia.

Wall (2007; 2010) nos diz que o que se chama cibercrime são produtos da rede mundial de computadores, definidos nos termos na nova sociedade da informação e em rede, que altera o modo, as oportunidades, o alcance e os impactos do ato criminoso, agora tecnologizado e distribuído em rede.

Yar (2013) utiliza-se do conceito de compressão do tempo-espaço, que David Harvey utiliza para definir a globalização, para caracterizar e definir o cibercrime. Os potenciais criminosos com acesso a computadores e à Internet podem alcançar as suas vítimas sem qualquer necessidade de compartilhar o mesmo tempo e espaço, superando as barreiras geográficas, assim como podem alcançar um número incalculável de vítimas distribuídas geograficamente pelo mundo. Destaca ainda o potencial de manipulação e invenção de identidades e a possibilidade de manter o anonimato através de recursos informáticos e da Internet.

Portanto, o que nos interessa sobre o cibercrime não é somente a catalogação novos comportamentos e atos que as sociedades possam vir a enquadrar como crimes e que possam ser receber o prefixo *ciber*, mas também

---

5 BRASIL. Lei n. 12.737 de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 24 de mai. 2019.

como a Internet potencializou, alterou os modos de cometer crimes e os desafios para o controle, combate e policiamento na rede mundial de computadores.

O policiamento em rede.

O policiamento na era da Internet, principalmente para controlar e combater o crime mediado por computadores e outros artefatos eletrônicos, é visto pelos pesquisadores que se dedicaram a estudar o cibercrime pelo viés sociológico e do policiamento como um desafio ao modelo mesmo de policiamento.

Wall (2006) destaca que a polícia tem um grande desafio pela frente, pelo seu modelo tradicional que remonta ao paradigma *peeliano*. A polícia moderna surge como uma instituição estatal, burocrática, para lidar com as desordens e distúrbios sociais provocados pela revolução industrial nas cidades. Desde o seu surgimento, a polícia e seus agentes reclamam de recursos materiais e tecnológicos para a realização do trabalho policial, ou seja, para controlar o crime e capturar os criminosos. As demandas por recursos materiais não foram superadas, especialmente no Brasil, onde ainda faltam recursos básicos para o funcionamento de muitas delegacias de polícia, como viaturas, computadores e, até mesmo, a existência de locais próprios para o funcionamento de uma delegacia[6].

Além das limitações dos recursos materiais e tecnológicos, a polícia encontra obstáculos burocráticos e jurídicos na consecução do seu trabalho. Pode-se dizer que um dos detalhes que levou o fenômeno do cibercrime para o debate público foi o processo legislativo que visava a promoção de uma lei criminal para sustentar a operação das policias especializadas em cibercrime no Brasil. A Lei 12.737/12, que altera o código penal brasileiro, tipificando os delitos informáticos, é uma lei reduzida e oriunda de um projeto de lei que foi debatida por mais de uma década, o PL nº 84/99, também conhecida como Lei Azeredo.

6 A delegacia especializada em cibercrime da Polícia Civil de Minas Gerais funcionava no espaço compartilhado com outras tantas delegacias especializadas. Não era uma delegacia de polícia com um espaço próprio. Era uma repartição compartilhada com outras repartições. A estrutura era para um ou dois agentes policiais que realizavam a recepção e o boletim de ocorrência no mesmo espaço. Não tinha uma sala individual de para realizar a oitiva, coletar o depoimento ou denúncia. A delegacia especializada do Rio Grande do Sul também era um compartimento, sala/escritório em uma delegacia compartilhada com outras unidades policiais. A polícia com melhor estrutura, com uma unidade própria, foi a da Polícia Civil do Paraná. Adiante, veremos, através das falas dos delegados e policiais que a polícia tem as suas demandas, mas que são atendidas segundo os interesses políticos dos governadores. Ou seja, para mostrar para a população, ainda é muito mais importante investir recursos em delegacias que são mais procuradas e tradicionais. As delegacias de cibercrime ainda são uma novidade e somente em eventos de pânico moral público, quando um caso ganha notoriedade dos meios de comunicação é que se questionam o porquê as delegacias são tão deficitárias em recursos.

O PL 89/99 visava diminuir os entraves judiciais de acesso a dados pessoais e de navegação dos usuários de Internet no Brasil, tornando obrigatória a criação de um registro civil único para cada internauta, o armazenamento de dados de navegação e a entrega desses dados à polícia investigativa sem qualquer autorização judicial. Se pensada pelo viés do trabalho policial e o desafio que a polícia encontra na consecução das investigações, a proposta seria exitosa e ia ao encontro à demanda das polícias especializadas em cibercrime: a celeridade do judiciário em responder e autorizar o acesso aos dados cadastrais e pessoais de usuários nas investigações.

Mas houve uma reação da sociedade civil organizada, que trouxe o debate sobre as violações dos direitos individuais pela polícia brasileira e que colocou em xeque a possibilidade de uma vigilância sem controle sobre os internautas no Brasil, associando o PL 89/99 a um grande projeto legislativo que autorizava um panóptico *online*, onde todos os usuários teriam seus dados de navegação registrados e poderiam ser alvos de investigação, sem qualquer dever das autoridades de informarem o motivo para ter acesso às informações e históricos digitais dos internautas[7].

A polícia especializada em cibercrime enfrenta o desafio de superar a sua organização e modelo operação histórica, respondendo às demandas localizadas e obedecendo a um regramento burocrático judicial muitas vezes rígido, que não acompanha a celeridade necessária para obter os dados necessários para uma investigação e a resolução dos crimes. O cibercrime, como vimos, é um fenômeno intrinsecamente ligado às novas tecnologias em rede, que transpõe os limites físicos e temporais, ou seja, é um fenômeno em rede e que coloca os desafios às instituições tradicionais de polícia.

O desafio, portanto, para o policiamento na Internet está na adoção das características que seguem o modelo de rede ou nodal, com a colaboração de múltiplos atores, que não têm o papel tradicional da polícia, mas que podem com ela colaborar, como empresas privadas de segurança da informação, organizações da

7 O movimento reativo da sociedade civil brasileira deu origem a mobilização de setores da sociedade civil organizadas ligadas às questões de tecnologia e da acadêmia. Os repertórios de campanha foram os mais variados, desde aulas públicas e protestos de rua contra o PL 89/99, até o uso da própria Internet e serviços de redes sociais, com a utilização de *hashtags* para marcar dar visibilidade à crítica ao projeto, como o #MegaNão. Desse movimento da sociedade civil organizada surgiu a proposta de uma lei civil de direitos e deveres dos cidadãos no uso da Internet no Brasil, que culminou na Lei 12.965/14, conhecida como Marco Civil da Internet.

sociedade civil ou entidades de caráter público-privado voltado para a manutenção e controle de qualidade técnica da rede que conecta os computadores. É o que os pesquisadores têm apontado como modelo para o policiamento relacionado com o cibercrime no mundo (NHAN; HUEY, 2008; NHAN; HUEY; BROLL, 2012; WALL, 2010).

A segurança e o policiamento da Internet no Brasil.

A questão da segurança no uso da Internet, através de computadores ou outros artefatos tecnológicos, correlato com os crimes cometidos e sofridos pelos cidadãos, coloca um novo desafio à gestão da segurança. Como a própria rede mundial de computadores, a governança da segurança na Internet deve se basear em uma rede de atores complexa.

A segurança pública representada pelas polícias civis, que recebem as denúncias diariamente dos cidadãos comuns nas delegacias especializadas estaduais, que realizam as investigações e produções de provas para o inquérito e processo judicial, trabalham como em um modelo de polícia tradicional. Não existem delegacias do tipo *CSI Cyber*[8], como pode sugerir a ideia das delegacias especializadas em crimes cibernéticos ou eletrônicos.

O problema da segurança com relação à Internet é diferente da segurança dos cidadãos que andam pelas ruas. Não existe uma polícia controlando, monitorando e patrulhando o ciberespaço. Aos cidadãos recaí a responsabilidade de conhecer os caminhos permitidos e os proibidos para uma navegação segura, os *sites* e endereços que apresentam ameaças ou riscos. Caso algum crime aconteça, pode-se procurar a polícia, registrar o boletim de ocorrência como qualquer outro crime ou delito. Mas não tem como prender ou chegar ao acusado em tempo real ou

8 O imaginário *cyber* é rico e povoa a mente das pessoas. Assim como a construção do tipo ideal do *hacker* como um indivíduo do sexo masculino, com problemas e distúrbios psicológicos causados pelo isolamento ou dificuldades de sociabilidade, causado por um alto grau de inteligência e habilidade técnica. Tal imagem deve ser desconstruída, assim como a associação do hacker com o criminoso, pois o universo *hacker* é formado por pessoas de ambos os sexos, com culturas e subculturas, práticas de sociabilidades específicas relativas à formação de suas comunidades, e não apresentam distúrbios psicológicos nem são indivíduos com capacidades especiais. Hackers são pessoas com conhecimento e domínio em programação e que atuam na programação e reprogramação de *softwares*, alguns com grande interesse pela política e a segurança. Muitos hackers são donos de empresas de segurança ou trabalham em empresas de segurança. Durante a pesquisa de campo, frequentei alguns encontros de hackers e segurança, como o Silver Bullet, no qual os hackers dividiam suas apresentações e demonstrações de programas e habilidades com instituições de segurança pública, como a Polícia Federal e o próprio Exército brasileiro. Sobre a ética hacker, ver COLEMAN (2012), HIMANEN (2001).

acionar uma viatura com policiais para fazer rondas pelas ruas ou bater em uma porta atrás do suspeito real, fazer a prisão e conduzi-lo para a delegacia. Os crimes cometidos através de computadores conectados à Internet colocam desafios à investigação e à prisão dos autores ou suspeitos dos crimes, o que é próprio da rede mundial de computadores: a desconexão do tempo e espaço, a ausência física do suposto criminoso, o anonimato ou a facilidade de se tornar anônimo por um tempo, até que os rastros digitais, dados e metadados de navegação, guardados pelas empresas que oferecem acesso ou serviços na Internet, são entregues para a polícia realizar a investigação e chegar a um suspeito ou criminoso.

Se o crime é especializado, as delegacias de crimes cibernéticos, cibercrimes, crimes digitais, crimes eletrônicos – não há uma nomenclatura comum entre as delegacias especializadas –, são como toda e qualquer delegacia de polícia no Brasil. Se diferenciam pelo atendimento ao público vítima de algum crime sofrido por meios eletrônicos conectados à Internet. A investigação dá-se através da coleta de dados e informações que se encontram em serviços conectados à Internet, o que leva a depender de muitos parceiros para a investigação, como a liberação por parte do judiciário para o acesso a dados e informações dos provedores de Internet, as plataformas de acesso a serviços e conteúdos, como as gigantes da Internet, Google, Facebook, WhatsApp. Em níveis de infraestrutura são como as delegacias comuns, algumas não tendo muitos recursos, como foi dito, porque ainda estão no início e dependem do interesse político e de quão visibilidade dão nos jornais policiais.

O número de agentes policiais são poucos, os recursos também. Mas o número de cidadãos vítimas cresce a cada dia, ou como relataram os agentes “nos dias e semanas após as datas comemorativas que movimentam o comércio [eletrônico], a delegacia enche!”. Porque os crimes mais denunciados são os crimes financeiros, como fraudes em compras realizadas em sítios falsos da Internet, quando o cliente paga e não recebe o produto ou paga um boleto falsificado. Tem os crimes de extorsão, após a vítima entrar em uma sala de bate papo, se envolver com alguém, trocar fotos de nudismo e enviar para o outro. A partir daí, o mais comum, especialmente mulheres, é a vítima sofrer chantagem para não ser exposta na Internet[9].

9 Realizei pesquisa de campo nas delegacias especializadas de São Paulo, Minas Gerais, Paraná e Rio Grande do Sul. Acompanhei as vítimas nos seus depoimentos quando me era permitido. Quando a vítima era mulher e a denúncia envolvia crimes contra a intimidade, violência de gênero, não pude

Como foi tido, os agentes policiais não têm acesso a uma estrutura de computadores e máquinas inteligentes que os ajudam a revelar os crimes, como na série televisiva *CSY*, são policiais uniformizados, armados com armas e computadores de mesa (*desktop*), que preenchem um formulário e anexam os *prints* das provas[10], que as próprias vítimas são responsabilizadas por levar e apresentar no ato de lavrar o boletim de ocorrência. O número de peritos criminais que realizam perícias em computadores, HD's e aparelhos eletrônicos é mínimo. Fica por conta da vítima a responsabilidade por apresentar um laudo de perícia técnica especializada, se o caso exigir.

A dificuldade com recursos humanos e material é justificada por um delegado responsável por uma das delegacias especializadas: "Para criar e manter uma delegacia especializada, tem que ter interesse político. O interesse político ainda está em alocar recursos em viaturas e policiais na rua. As delegacias para ganhar recursos e se manterem, tem que produzir fatos que gerem atenção da mídia. Os governadores não têm interesse em comprar computadores, ferramentas de investigação e investir em perícia digital, mas, sim, comprar viaturas e armas para armar a polícia". Outro delegado me disse: "era preciso um equipamento para espelhar os HD's das vítimas para preservar as provas. Não tínhamos. Como eu lutei pela criação da especializada em crimes cibernéticos, eu mesmo comprei do meu bolso os equipamentos. Era da minha responsabilidade se quisesse fazer realmente alguma investigação e prestar o serviço à população. Chegou uma hora que não estávamos mais fazendo boletim de ocorrência, porque nossa capacidade estourou".

Tal falta de interesse político e de investimento recaí também sobre a má formação e treinamento dos agentes, a falta de especialidade dos policiais com a questão digital – o recrutamento não é feito pela área de formação, não existe o pré-requisito de ser formado em Ciência da Computação ou em alguma na área da

---

acompanhar, e os depoimentos eram todos reservados e feitos para uma policial. Mas quase sempre acompanhava as vítimas e depoimentos, pois eram denúncias de crimes e fraudes financeiras, estelionato, roubo de senhas, transferência não autorizada de valores entre contas bancárias, pedidos de resgate após ter computador criptografado por outra pessoa (*ramnsonware*), uma ou outra queixa de crimes contra a pessoa, como calúnia, difamação após discussões ou términos de namoro.

10 Os *prints* são impressões das imagens das telas dos computadores e celulares que provam e fundamentam a denúncia. É a partir desses dados que a polícia inicia a investigação. Se o suspeito é caracterizado por é um perfil que a vítima não conhece pessoalmente, como em um serviço de rede social, é a partir do nome que está impresso que a polícia pedirá uma autorização para que a empresa responsável pelo serviço envie os dados cadastrais para que se inicie a busca pela localização do indivíduo.

informática. O que se aprende sobre Internet, informática, investigação digital é no fazer cotidiano do trabalho policial. Nenhum policial entrevistado tinha formação na área de tecnologia da informação.

E como a fala de que delegacias enchem após uma data comemorativa ou *Black Friday*, indicando que é na realização do comércio eletrônico onde acontecem os principais crimes chamados digitais, é no comércio eletrônico que os atores públicos e privados da teia de segurança aparecem em cena, para alguns conscientemente, para outros negligenciados. Os cidadãos conscientes e educados dos riscos, perigos e das ameaças advindos do uso de computadores conectados na Internet se protegem com a contratação de serviços e pacotes de segurança privada. O mercado de segurança privada na Internet oferece desde pacotes de antivírus a empresas especializadas no monitoramento e bloqueio de ataques a sites de empresas que têm grandes banco de dados – verdadeiro *petróleo ou ouro digital* em guardados em servidores criptografados, monitorados e protegidos.

Os serviços de segurança privada é um nicho de mercado emergente e em crescimento no mundo e no Brasil. Médias e grandes empresas são orientadas, por consultores de segurança, a criar e manter uma equipe técnica específica, assim como um orçamento específico, para a segurança da informação, proteção e resolução de problemas e ataques à rede de computadores interna das empresas.

As empresas que atuam diretamente com o comércio eletrônico (*e-commerce)* são as mais interessadas em contratar *os vigilantes* particulares para monitorar e evitar a aproximação de potenciais assaltantes que, porventura, roubariam as credenciais, o dinheiro e as mercadorias dos seus clientes.

O comércio eletrônico cresce anualmente e ganha reputação com sítios que apresentam certificados e selos de segurança, de monitoramento e confiança nas suas transações. Como não há policiamento ostensivo na Internet, como há na 25 de Março, principalmente em épocas festivas, sempre reforçada por seguranças particulares contratados, às empresas que atuam na Internet resta disputarem e conquistarem seus clientes oferecendo os serviços de segurança privados para a realização de suas compras e navegação com o menor risco. Tal fato reforça o pressuposto das empresas de comércio eletrônico, especialmente instituições financeiras, preterirem a justiça ou polícia em prol da segurança privada na Internet: as empresas contratam a segurança particular contra fraudes, resolvem

internamente e não tornam público a sua vulnerabilidade e fraqueza (WALL, 2007; 2010)[11].

Isso também enfraquece o protagonismo da segurança pública, personificada nas delegacias especializadas, levantando a hipótese de que a segurança e a proteção no uso da Internet cabe exclusivamente aos indivíduos e empresas. Para ilustrar essa dupla vitimização, acompanhei um depoimento de um dono de uma pequena empresa que tivera seus computadores e máquinas paralisadas por um vírus. A vítima não sabia sequer que se tratava de um golpe bastante comum, o *ransomware*, que ataca um computador ou uma rede de computadores que posteriormente é inviabilizada por criptografia, que só poderá ser revertida mediante pagamento para um indivíduo ou grupo que possuía as chaves corretas para descriptografar. O agente que atendeu a vítima deu apenas orientações para que procurasse um serviço particular de segurança que pudesse resolver o problema dos maquinários parados e para que o evento não ocorresse novamente.

Os eventos sobre cibercrime e cibersegurança, quase sempre realizados com o apoio e organização da Federação do Comércio do Estado de São Paulo (Fecomércio-SP) e Federação Brasileira de Bancos (Febraban), acontecia anualmente com o nome de Congresso de Crimes Eletrônicos. O tom das palestras e eventos sobre segurança recaía sobre a promoção do conhecimento sobre os comportamentos dos usuários, principalmente do comércio eletrônico, e os riscos envolvidos nos negócios. A promoção de um ambiente saudável e seguro para as transações *online* ficava a cargo de empresas privadas de segurança, principalmente as de antivírus – Norton, Kasperky[12].

A rede mundial de computadores não é um *mundo* feito apenas de *bits*, códigos e dados que estão nas nuvens[13], sem qualquer tangibilidade ou

11 Vazamentos de dados de clientes e fraudes eletrônicas de instituições financeiras são eventos tratados no mundo da segurança da informação com grande especulação e pode ser utilizado para diminuir a credibilidade das instituições financeiras e empresas que atuam no comércio eletrônico ou atendimento via Internet. A própria Lei de Geral de Proteção de Dados Pessoais (LGPD), aprovada no ano de 2018 e para entrar em vigor no ano de 2020, visa reforçar, por força de lei, que as empresas adotem políticas de segurança e proteção de dados.

12 As empresas de antivírus de computador oferecem toda uma linha de produtos de segurança para usuários individuais e empresas. São as empresas de segurança que apontam, anualmente, nos seus relatórios, os principais riscos aos usuários na Internet. São as empresas de antivírus que atuam na linha de frente, nas estratégias de prevenção e reação aos diversos ataques.

13 A própria ideia de nuvem, estado gasoso, não sólido, em um estado etéreo, no uso corriqueiro da expressão “dados na nuvem”, dá às pessoas com menos conhecimento sobre a engenharia e funcionamento da Internet a sensação e a crença de que a Internet não é um estrutura física. A Internet, ao contrário, é uma estrutura física e robusta de cabos, fios, computadores e roteadores por onde trafegam os nossos dados. Nesta camada física é que opera a camada de programas. A

características físicas, a Internet é construída por cabos, fios e *hardwares* que apresentam ou oferecem vulnerabilidades e são permanentemente atacas por indivíduos ou programas automatizados, vírus ou códigos maliciosos, que buscam encontrar brechas nesta estrutra física. Assim como as rodovias são monitoradas para evitar acidentes, a infraestrutura da Internet é constantemente monitorada para identificar as ameaças e incidentes que possam comprometer a própria rede e o seu funcionamento, e alertar os seus usuários quanto aos riscos e ameaças de segurança. Esse monitoramento é realizado pelos Centros de Estudos, Resposta e Tratamento de Incidentes de Segurança (Cert, no Brasil Cert.br[14]) em várias regiões do mundo.

Esse monitoramento produz dados e informações sobre as principais ocorrências de incidentes e ameaças na rede – ataques de *spams*, servidores DNS maliciosos, que são servidores que reorientam o acesso de um site original para outro falso, geralmente de instituições financeiras ou de comércio eletrônico, dados que ficam abertos para todos, mas que exigem algum grau de conhecimento e de interesse nestas interpretar essas informações. É um tipo arranjo de interesse público e privado de patrulhamento das ameaças na Internet, que não tem nenhum poder de policiamento ou identificação de indivíduos ou grupos que cometeram crimes, portanto pouco contribuem com a atividade e prática policial de resolução de crimes na Internet. Apesar disto, o Cert.br é um dos principais atores na governança da segurança da Internet a produzir materiais didáticos de alta qualidade sobre o uso seguro da Internet e suas ameaças. É um ator que atua na promoção da informação e educação, na formação de consciência sobre riscos e na promoção da cultura de segurança para o grande público[15].

A segurança nodal da Internet também conta com grupos da sociedade civil, que buscam ocupar o vazio do poder público na segurança e dar respostas aos crimes cometidos pela da Internet. No caso investigado, uma organização não-

---

Internet por ser essa rede materializada de cabos e de pontos de troca de tráfego de dados vindo de todas as partes tem a sua geografia, até mesmo responde a uma geopolítica de interesses, como ficou evidente no escândalo de vigilância da Agência de Segurança dos Estados Unidos revelada pelo Edward Snowden, em que surgiram propostas políticas de um consórcio de países para cabeamento e criação de rotas de tráfego de dados independentes da infraestrutura dos EUA. Para mais informações sobre a estrutura física e a geopolítica da Internet, ver BLUM (2012).

14 Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança para a Internet no Brasil. https://cert.br.

15 O Cert.br produz uma cartilha e fascículos sobre segurança da Internet que é educativo para crianças, jovens e adultos. Esse material é distribuído para escolas de todo o país e utilizado em campanhas sobre segurança da Internet. Esse material está disponível em https://cartilha.cert.br.

governamental se encontra no centro da rede de policiamento na Internet no Brasil. A SaferNet Brasil é uma ONG que recebe denúncias, monitora perfis e suspeitos por crimes de pedofilia, racismo e de discurso de ódio no Brasil, contribuindo diretamente com os órgãos de polícia do Estado e instituições de Justiça.

Considerações finais.

A pesquisa identificou, a partir da investigação das delegacias especializadas em cibercrime, atores privados que atuam na segurança e repressão aos crimes cibernéticos. Contudo, o que fica evidente é que, em vez de ser uma rede de atores contribuindo com uns com os outros, há parcerias estabelecidas entre um e outro ator, sem uma articulação em rede entre de todos.

A SaferNet Brasil colabora com a Polícia Federal nos casos de pedofilia, repassando as denúncias, mas não há uma estrutura de compartilhamento de dados e ajuda mútua com as polícias civis.

O Cert.br realiza pesquisas e produz muitas informações pertinentes sobre segurança na Internet, mas não tem uma comunicação direta com as instituições policiais, como disse uma técnica do Cert.br: “nós não temos o interesse de fazer o papel de polícia, de identificar e prender criminosos na Internet. Nós somos responsáveis por monitorar e contribuir para um ecossistema sadio e seguro da Internet”. O trabalho do Cert.br, parece, é um trabalho muito técnico e longe das demandas das delegacias e dos problemas reais causados pelo cibercrime.

As empresas privadas de segurança, como as empresas de antivírus não contribuem diretamente com as instituições policiais. Como disse um delegado: “até hoje nenhuma empresa de antivírus nos procurou para oferecer ajuda, tecnologia e conhecimento. E eles têm as ferramentas, conhecimento que poderiam nos ajudar”.

A Polícia Federal tem parceria de colaboração com as grandes empresas da Internet, como Google e Microsoft, para o fornecimento de dados e incidentes que estejam sob investigação. Mas ainda falta, de acordo com os relatos, uma parceria mais efetiva entre as polícias e as empresas privadas de segurança e de serviços na Internet no Brasil.

A própria organização das polícias civis é desestruturada, segundo os relatos coletados dos delegados e agentes. Segundo eles, não existe uma plataforma ou banco de dados compartilhados entre as polícias estaduais. Se o crime é cometido com o uso da Internet, não existe uma ferramenta compartilhada na Internet para a

troca de informações e o trabalho conjunto entre as polícias. É como a velha demanda das polícias desde finais do século XIX: as polícias não têm acesso às tecnologias disponíveis e não fazem uso das estratégias que os criminosos fazem das tecnologias para cometer seus crimes. Enquanto indivíduos e grupos fazem o uso das tecnologias, quebrando as barreiras geográficas para atacar o seu alvo, as polícias ainda trabalham de modo analógico e obedecendo regras burocráticas enrijecidas[16].

Quando se compara o trabalho das polícias civis especializadas com o da Polícia Federal, que apresenta vantagens em relação a acordos de cooperação com empresas de tecnologia, material e treinamento, fica evidente, na fala de um agente da polícia civil, que precisa de uma maior parceria entre as polícias e atores envolvidos no policiamento e segurança na Internet: “A Polícia Federal é responsabilizada pela investigação de crimes cometidos contra a União ou crimes que envolvam cidadãos de outros países. A Polícia Federal tem mais recursos do que nós. Mas nós é que estamos na ponta do sistema de segurança, somos nós que recebemos a vítimas e denúncias. Ninguém bate à porta da Polícia Federal para reclamar ou fazer uma denúncia. E todos querem contribuir com a Polícia Federal, mas somos nós que atendemos diretamente o cidadão. Muitas investigações são iniciadas pela Polícia Civil e depois passadas para a Polícia Federal, e ao término nem sabemos o resultado ou sequer somos citados”.

Referências.

BLUM, Andrew. *Tubes: A journey to the center of the Internet*. New York: HarperCollins, 2012.

CASTELLS, Manuel. *A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade*. Rio de Janeiro: Zahar, 2003.

COLEMAN, Gabriella. *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton University Press, 2012.

16 A polícia responsável pela investigação de uma denúncia é a polícia de onde aconteceu o suposto crime. Como muitos crimes pela Internet são cometidos tendo como origem um Estado e alvo cidadãos de outro Estado, a vítima reporta à sua delegacia o ocorrido, se o suspeito for de outro Estado, é passada para a delegacia deste Estado de origem do suposto crime a denúncia para que ela realize a investigação. Esse é o grande problema, segundo os informantes das delegacias onde a pesquisa foi realizada, nas regiões sudeste e sul: as polícias dos outros Estados não têm condições de realizar investigações de crimes que os próprios cidadãos sofreram, sequer teriam para os cidadãos de outros Estados.

GARRIOT, Willian (org). *Policiamento e governança contemporânea – A antropologia da polícia na prática*. Campinas: Editora da Unicamp, 2018.

GLENNY, Misha. *Mercado sombrio: o cibercrime e você.* São Paulo: Companhia das Letras, 2011.

HIMANEN, Pekka. *A Ética dos Hackers e o Espírito da Era da Informação.* Rio de Janeiro, Campus, 2001.

KSGHETRI, Nir. *Cybercrime and Cybersecurity in the Global South.* New York: Palgrave Mcmillan, 2013.

LEMAN-LANGLOIS, Stéphane (org). *Technocrime: Technology, crime and social control*. Willian Publishing, 2008.

NHAN, Johnny; HUEY, Laura. Policing through nodes, clusters and bandwidth. In: LEMAN-LANGLOIS, Stéphane (org). *Technocrime: Technology, crime and social control*. Willian Publishing, 2008.

NHAN, Johnny; HUEY, Laura; BROLL, Ryan. 'Uppity civilians' and 'cyber-vigilantes': the role of the general public in policing cyber-crime. Criminology & Criminal Justice, 13 (1), 2012.

WALL, David. *Cybercime: The transformation of Crime in the Information Age*. Polity Press, 2007.
_____. Policing Cybercrimes: situating the public police in networks of security within cyberspace. *Police Practice & Research: An International Journal,* 8 (2), 2010.

YAR, Majid. *Cybercrime and Society*. SAGE Publications, 2013.