DOI: 10.5433/2176-6665.2017.1V22N1P301

Crime, Polícia e Tecnologias da Informação

Police work and new technologies

Jaime Luiz Cunha Souza[1]

Resumo

Este artigo focaliza a percepção dos operadores dos sistemas de segurança pública acerca dos delitos praticados com a utilização de tecnologias de informação e comunicação (TIC) e seu impacto nas investigações policiais. A metodologia utilizada para a realização da pesquisa foi a qualitativa, com aplicação de questionários semiestruturados aos policiais da Delegacia de Repressão a Crimes Cibernéticos (DRCT), da Polícia Civil do Estado do Pará. Os resultados indicam que os policiais apresentam sérias limitações técnicas e operacionais relacionadas aos meios de comunicação e informação, e que tais dificuldades restringem sua capacidade de atuação.

Palavras-chave: Trabalho policial. Tecnologias. Informação. Investigação. Cibercrime.

Abstract

The article focuses on the perception of public safety systems operators about the crimes committed with the use of information and communication technologies and their impact on police investigations. The methodology used to conduct the research was the qualitative, semi-structured questionnaires with the officers of the Repression the Cyber Crimes – ESKD, Civil Police of the State of Pará. The results indicate that the cops have serious technical and operational limitations related to media and information, and such difficulties restrict its ability to act.

Keywords: Work Officer. Information. Technology. Research. Cybercrime.

1 Professor do Programa de Pós-Graduação em Segurança Pública da Universidade Federal do Pará (UFPa), Brasil. Email: jaimecunha@ufpa.br

Recebido em 18/11/2015. Aceito em 10/11/2016.

1. Introdução

O desenvolvimento das tecnologias de comunicação e informação (TIC) provocou alterações profundas em amplas dimensões da vida social. A extensão de seus benefícios é inquestionável, mas a sua capacidade de produzir danos parece proporcional. Este trabalho focaliza o impacto no trabalho policial dessas alterações, que fizeram surgir novas formas de delinquência. Com efeito, a rápida capacidade de reorganização e de rearticulação da delinquência, tornada possível pelos avanços tecnológicos, dinamizaram as atividades criminosas tradicionais e viabilizaram a prática de novas modalidades de transgressão da lei.

Começamos a abordagem do tema com a realização de uma discussão sobre as experiências de algumas instituições policiais de várias partes do mundo, notadamente dos Estados Unidos da América (EUA) e de países da Europa, para, posteriormente, focalizarmos mais diretamente o caso específico da Delegacia de Repressão a Crimes Tecnológicos (DRCT), da Polícia Civil do Estado do Pará. Tomamos como objeto de nossa análise a percepção dos policiais que desenvolvem suas atividades nessa delegacia especializada. A abordagem foi, essencialmente, qualitativa, e a coleta de dados, feita por meio de entrevista semiestruturada.

Com base nos dados e nos argumentos apresentados, buscou-se discutir a expansão das TIC, as limitações da atividade policial tradicional ante as novas tecnologias, a defasagem na eficiência do trabalho policial, particularmente na persecução dos delinquentes que utilizam como meio a internet, e o impacto de todo esse processo nas atividades de investigação. Mostrou-se como as fragilidades das instituições policiais podem ser extremamente danosas para a segurança pública.

2. Problemas antigos em novas modalidades

Atualmente, uma das poucas certezas é a de que estamos imersos em um oceano de informações (LÉVY, 2007). Inevitavelmente, tal imersão projeta sobre as pessoas uma gama enorme de possibilidades tanto para construir novas formas de sociabilidade e explorar nichos de atividades econômicas nunca antes imaginados, como para desenvolver atividades desviantes ou criminosas. Essa expansão de horizontes compromete o desempenho das instituições públicas e privadas, que estão quase sempre às voltas com carências de recursos humanos e defasagens tecnológicas, colocando em xeque não apenas os limites dentro dos quais se devem manter as ações dos agentes públicos, como também o próprio Estado de Direito e a democracia.

Tal dinâmica afeta sobremaneira a sociedade brasileira e particularmente suas instituições policiais, tradicionalmente resistentes a mudanças, as quais, ao longo do tempo, cristalizaram práticas de esquadrinhamento, sistematização e manipulação de informações, cujo objetivo sempre visou mais a proteção dos ocasionais detentores do poder político e econômico, do que as ações voltadas para o bem comum. Essa lógica de funcionamento consolidou uma prática que guarda semelhanças com a descrita por Foucault (2007), que tem como característica a construção de saberes a respeito das pessoas e de seus comportamentos, bem como a vigilância sobre grupos específicos classificados de acordo com sua suposta "normalidade" ou grau de periculosidade.

Com graus variáveis de eficiência, a mencionada estratégia foi utilizada durante o século XIX e boa parte do século XX como forma de controle social em grande parte da Europa e daquilo que se convencionou chamar "mundo civilizado". No entanto, a partir das duas últimas décadas do século XX, a dinâmica das relações pessoais e institucionais experimentou profundas mudanças em decorrência

do vertiginoso desenvolvimento e, posteriormente, da popularização das TIC. A partir desse período, a produção, o acesso e até mesmo a manipulação de informações, que, em décadas anteriores, eram prerrogativa predominantemente das instituições de controle social formal, tornaram-se disponíveis ao público em geral em decorrência da expansão vertiginosa dos meios de comunicação, da simplificação da operação dos computadores e do barateamento dos custos desse tipo de equipamento e de seus acessórios. Essa mudança multiplicou as formas de acesso aos dados sistematizados por outros e fez de cada indivíduo um potencial participante ativo de uma espécie de inteligência coletiva (LÉVY, 2007).

Apesar de perceberem as transformações em curso, os sistemas de justiça criminal em várias partes do mundo sempre reagiram muito lentamente a esse fenômeno, e as tentativas de adaptação das instituições estatais ao novo momento foram freadas pelo extremo conservadorismo e pelo pouco investimento em aprimoramento técnico dos sistemas de justiça criminal, especialmente das instituições policiais (NAIM, 2006). Tal inércia – comenta Naim (2006) – levou essas instituições a uma profunda defasagem em sua capacidade de acompanhar os desconcertantes fluxos de informações trocadas entre pessoas e instituições, e de realizar o monitoramento e a persecução daqueles que se utilizam desse tipo de ferramenta tecnológica para praticar crimes. Embora observem os impactos no cotidiano das pessoas decorrentes das mudanças na dinâmica do crime, os agentes públicos continuam tentando alcançar os novos crimes e os novos delinquentes por meios tradicionalmente adotados pelo sistema de justiça criminal.

Essa discrepância minou a tradicional prerrogativa do Estado de produzir Poder por meio do Saber, na medida em que o desenvolvimento das TIC gerou acessos cada vez mais amplos às informações. Essas informações, por sua vez, passaram a ser veiculadas

de forma descontrolada nas redes de comunicação e informação, as quais, em grande parte, por sua natureza transnacional e global, ficam relativamente fora do controle das autoridades legalmente constituídas. Isso gerou, inclusive, novas concepções a respeito do crime e do criminoso, cujos comportamentos não podem mais ser compreendidos recorrendo-se somente aos modelos explicativos propostos pelos teóricos clássicos das Ciências Sociais (CASTELLS, 2003; NAIM, 2006).

A nova criminalidade que surge na esteira do desenvolvimento das TIC possui dinamismo próprio, o qual permite que se reorganize, se readapte e se diferencie sistemicamente a partir de suas próprias necessidades e dos *inputs* que seus elementos internos captam da sociedade, em uma operação semelhante à que, no constructo teórico de Niklas Luhmann (1998), recebe o nome de *autopoiesis*.

Ao tratar de maneira mais específica das mudanças decorrentes da introdução dessa nova dinâmica, Castells (1999, 2003) indica como sintomático o fato de as atividades criminosas e as organizações ao estilo da máfia, de todo o mundo, terem-se tornado globais e, com a ajuda dos meios informacionais, serem capazes de proporcionar, em qualquer parte do mundo, meios para viabilizar qualquer forma de negócio ilícito, desde armas sofisticadas até substâncias químicas ilegais, passando pelo comércio de favores sexuais e pelo tráfico de pessoas. O autor acrescenta que uma das redes mais poderosas da sociedade contemporânea – a produção e a distribuição de narcóticos –, juntamente com seu componente intrínseco – a lavagem de dinheiro –, construíram uma geografia específica, toda conectada em rede, a qual flui para a mãe de toda acumulação, que é a rede financeira global.

Nesse sentido, os indivíduos ditos criminosos ou delinquentes que se utilizam de tecnologias informacionais não podem ser considerados simples desviantes motivados por carências econômicas e pelo enfraquecimento do controle social informal. No caso específico

dos crimes praticados com utilização de TIC, o perfil dos incriminados (MISSE, 1999) foge totalmente ao estereótipo do criminoso pobre, morador de regiões periféricas, com pouca escolaridade e baixo poder aquisitivo, característica esta já analisada por Sutherland (1940) desde as primeiras décadas do século XX..Esses indivíduos não se limitam a transgredir a ordem, ou a rejeitar as analogias de sua cultura, ou os argumentos das suas instituições. Eles reagem a um grande número de influências de múltiplas formas, pois até mesmo as instituições nas quais poderiam encontrar referências éticas e morais estão profundamente afetadas pelos impactos dos avanços tecnológicos e pelas novas formas de sociabilidade que o desenvolvimento das TIC fez surgir ao subverter valores e alterar padrões de comportamento (LÉVY, 1994, 1999, 2007).

Os laços que ligam os referidos incriminados não são mais laços de pertencimento cultural, são laços frágeis, criados em comunidades escolhidas por eles mesmos, de existência efêmera. Longe de serem espectadores passivos de sua própria condição, tais indivíduos deformam ou reinterpretam os conceitos que receberam de sua comunidade de origem, de sua família, reordenando-os em conformidade com os seus próprios interesses e projetos pessoais, que se tornam muito mais amplos pelas inúmeras redes sociais nas quais estão inseridos, sem, no entanto, deixarem de se conectar com seu cotidiano local (GARLAND, 2008).

Um exemplo característico da nova dinâmica é a forma como os indivíduos e grupos envolvidos com as atividades ilícitas inventam processos de decisão ou novos ordenamentos do real para dominar, principalmente, os espaços nos quais o poder público está ausente. Quando essa ocupação do espaço vazio deixado pelo Estado acontece, tanto as comunidades quanto os grupos criminosos que lá se encontrem instalados, seja por carência, seja por ação ou omissão, reorganizam-se informalmente para a reconstrução do papel das

instituições. Assim, criam instâncias não institucionais de decisão, por exemplo, os denominados "tribunais do crime", nos quais grupos de "criminosos" tomam para si o poder de julgar e punir, tarefa essa que deveria ser exclusiva das instituições do Estado. Ou seja, mesmo organizados em rede e interligados de forma global, as lógicas particulares e especificidades locais não são eliminadas, porque os grupos criminosos, ao se reconfigurarem como redes metassociais com ramificações globais, também entram em simbiose com as comunidades locais e passam a compor novos ordenamentos comunitários, os quais em parte assimilam e em parte rejeitam os elementos sociais e institucionais formais com os quais estão conectados direta ou indiretamente (CASTELLS, 2003).

São justamente as velocidades e quantidades dos fluxos multidirecionais que desconcertam as instituições em geral, mas impactam principalmente as instituições de segurança pública. Estas, muito lenta e tardiamente, têm-se dado conta de que uma alteração técnica, como o desenvolvimento acelerado dos meios de comunicação e informação, implica a reestruturação dos coletivos sociais básicos e, em consequência, de sua forma de atuação profissional.

Um dos principais erros que têm inviabilizado a atuação eficiente das instituições de segurança pública é o cultivo de métodos convencionais e ultrapassados para resolver a questão da criminalidade nesse novo contexto social, cuja característica principal é a modificação constante. Tem sido sistematicamente negligenciado o fato de que, diante das transformações tecnológicas que se desenvolveram nos últimos 30 anos, princípios como o de lei e ordem não podem manter-se estáticos e imutáveis, pois nem mesmo sua significação permaneceu idêntica durante esse tempo.

3. Cibercrime: transformações na operação do delito

Com a popularização dos computadores e as facilidades de comunicação via internet, as fronteiras outrora relativamente definidas entre o legal e o ilegal tornaram-se cada vez menos precisas. Legislações e jurisdições cruzam-se sem que as demarcações geográficas lhes sirvam de referência definitiva.

Não somente os sistemas financeiros e administrativos ligados à economia formal apropriaram-se das possibilidades trazidas pelas TIC. Os "criminosos" das mais variadas vertentes passaram a explorá-las, desenvolvendo novas modalidades de crimes, que combinam as facilidades tecnológicas dos meios de comunicação e informação com a mobilidade de pessoas, mercadorias e serviços (NAIM, 2006). De acordo com Kirby e Penna (2011) e Bossler e Holt (2012), a combinação de tecnologia e aumento da mobilidade cria inúmeras oportunidades para o crime, organizado ou não, e torna-o ainda mais complexo para as instituições policiais, porque, apesar das preocupações no sentido de neutralizar as atividades ilegais no âmbito transnacional, os órgãos de segurança locais continuam como atores fundamentais no acompanhamento e no enfrentamento das diversas modalidades delitivas, inclusive dos chamados crimes virtuais. O efeito disso é extremamente perturbador para a atividade policial, porque as transgressões da lei passam a ocorrer em um ambiente estranho ao trabalho policial tradicional.

Em sua análise das repercussões das relações entre o trabalho policial e o mundo virtual, Deibert e Rohozinski (2010) avaliam que o ciberespaço representa uma dimensão de riscos ainda mais complexa no já conturbado palco de conflitos econômicos, políticos e sociais. Para os autores, o espaço virtual tem implicações cada vez mais poderosas nas dinâmicas que ocorrem nos ambientes terrestres, aéreos, marítimos e até espaciais, e isso expande e torna mais complexo

o trabalho policial. As análises de Davis (2011) a respeito dessa relação destacam que a tecnologia da informação, ao fazer do ciberespaço um indutor de novas sociabilidades, transformou rapidamente, e às vezes até radicalmente, a vida das pessoas e das instituições, criando novas formas de compartilhamento de informações e um intrincado fluxo de dados pessoais e institucionais utilizados em atividades de comércio eletrônico, lícito ou ilícito.

Concepções otimistas veem nos novos tempos a ampliação das possibilidades de inserção democrática (LÉVY, 1999, 2007). No entanto, também já se percebeu que essa ampliação é igualmente responsável pelo aumento do fosso entre gerações e pela criação de múltiplas formas de atividades ditas criminosas, na medida em que as possibilidades da rede mundial de computadores foram apropriadas por organizações criminosas[2] nacionais e transnacionais, locais e globais, grandes e pequenas que, ao explorarem a ausência de legislações nacionais harmonizadas na definição dos chamados crimes virtuais, oferecem ampla gama de oportunidades para ganhos ilícitos (AUGUST, 2002; ZHENG et al., 2006). Como exemplo, podemos citar o caso da "organização criminosa" identificada e presa no Brasil durante a Copa do Mundo de Futebol de 2014, desarticulada pela polícia brasileira, que coordenava um esquema de compra e venda ilegal de ingressos e mantinha vínculos com a Fifa[3], e ramificações na seleção brasileira de futebol. O grupo teria agido nas últimas quatro edições da

2 Para as finalidade deste texto adotamos a definição de "organização Criminosa" contida na Convenção das Nações Unidas de 15 de novembro de 2000, conhecida como Convenção de Palermo, que foi aprovada no Brasil pelo Decreto Legislativo 231, de 29 de maio de 2003 e promulgada por meio do Decreto 5.015, de 12 de março de 2004, que define a organização criminosa como um grupo estruturado de três ou mais pessoas, existente Há algum tempo e atuando em conjunto com o propósito de cometer infrações à Lei e obter direta ou indiretamente benefícios econômicos ou outro benefício material.

3 FIFA – Federation International Football Association, é a entidade que supervisiona diversas federações, confederações e associações relacionadas com o futebol ao redor do mundo. Tem sua sede em Zurique, na Suíça, e promove várias competições entre em diversos países, sendo a mais conhecida a Copa do Mundo de Futebol, realizada a cada quatro anos. Mais informações sobre esta instituição estão disponíveis em http://www.fifa.com/

Copa do Mundo e, segundo a polícia, tinha "potencial" para lucrar R$ 200 milhões somente com o Mundial do Brasil. A quadrilha conseguia os ingressos, inclusive de camarote, das mais variadas formas: com a própria Fifa, com delegações de seleções, comprando de torcedores e também de organizações não governamentais (ONG) que recebiam gratuitamente as entradas[4]. Toda a articulação que possibilitava a concretização da negociação ilícita de ingressos foi potencializada pela utilização estratégica da internet.

Outro aspecto importante relacionado às ilegalidades operacionalizadas através da rede mundial de computadores diz respeito à intensa utilização do ciberespaço e das redes sociais para a veiculação de publicidades ligadas ao comércio de favores sexuais e às transações relacionadas às drogas ilícitas (DAVIS, 2011). Bossler e Holt (2012) avaliam como extremamente graves as consequências emocionais e psicológicas associadas às vítimas do cibercrime, particularmente para as crianças afetadas pela pornografia e pela pedofilia. Do mesmo modo, esses autores salientam a intensa preocupação que existe por parte de governos de todo o mundo no que diz respeito à possibilidade de ataques, por computador, contra infraestruturas críticas, como redes de energia, fontes de abastecimento, hospitais e sistemas financeiros, porque esses sistemas estão interligados e têm dependência muito grande da tecnologia da informação. Tais preocupações também fazem parte das aflições diárias de gestores de instituições privadas, assim como dos cidadãos comuns, que, de um momento para outro, podem ter tanto suas empresas quanto suas vidas expostas a grandes prejuízos sociais e financeiros. Assim, no segundo semestre de 2014, em um ataque considerado sem precedentes, *hackers*[5]

4 Reportagem disponível em <http://especiais.ne10.uol.com.br/arenadasnacoes/noticia/policia-do-rio-desarticula-quadrilha-de-cambistas-da-copa-do-mundo-1792> Acesso em 25 set 2014.

5 Neste texto não fazemos distinção entre hackers e crackers por considerarmos que tecnicamente ambos dedicam uma grande quantidade de tempo basicamente às mesmas ações: navegar na internet à procura de sistemas vulneráveis, sendo que a diferença entre eles pode ser percebida apenas em termos

expuseram na internet o conteúdo de filmes inéditos armazenados nos computadores da empresa Sony Pictures. Esse ataque, um dos maiores já sofridos por uma megacorporação, foi realizado com a utilização de um vírus não detectável pelos programas antivírus mais comuns e levou o FBI[6] a lançar um alerta para organizações de todo o mundo. Os especialistas em cibersegurança inicialmente suspeitaram que os *hackers* responsáveis pelo ataque tivessem agido a partir da Coreia do Norte. Posteriormente, essa hipótese foi descartada pelo FBI, sabendo-se de concreto apenas que o ataque foi desfechado a partir de um hotel de luxo localizado na Tailândia. O prejuízo causado foi estimado em, aproximadamente, 100 milhões de dólares[7].

Se, por um lado, existe uma crescente dimensão transnacional dos crimes virtuais, por outro lado, como mostram Bossler e Holt (2012), em um grande número de delitos praticados com utilização desses meios, há uma proximidade muito maior entre os que praticam e os que sofrem cibercrimes do que se imagina em princípio. Como exemplo, os autores citam o chamado *cyberbullying*, por meio do qual comportamentos agressivos ou assédio de pessoas são assumidos por indivíduos conhecidos das vítimas no mundo real, que vivem na mesma cidade ou, pelo menos, no mesmo estado.

Embora as diversas modalidades de cibercrime causem significativos prejuízos a pessoas, instituições e governos, a inércia e a defasagem tecnológico-operacional das instituições encarregadas de coibi-lo contribuem para que esse tipo de delito esteja entre os mais fáceis de serem cometidos e os que mais conseguem escapar à ação da polícia e da justiça. As causas dessa impunidade podem ser

do uso que fazem das fragilidades encontradas.

6 FBI – Federal Bureau of Investigation é uma Unidade de polícia do Departamento de Justiça dos EUA e que assume funções tanto de polícia de investigação quanto serviço de inteligência interno, ou contra inteligência.

7 Reportagem completa disponível em: <http://www1.folha.uol.com.br/tec/2014/12/1562817-entenda-o-caso-da-invasao-hacker-a-sony-pictures.shtml> Acesso em 23 dez 2014.

identificadas em alguns pontos específicos: primeiramente, por esse tipo de delito adicionar ao crime comum uma dimensão tecnológica com a qual as estruturas mais tradicionais das instituições policiais não estão habituadas; segundo, por esse tipo de ocorrência apresentar nível de prioridade baixo no conjunto de objetivos da polícia e dos demais organismos de aplicação da lei (BUTTON, 2012; DAVIS, 2011).

Dessa forma, as instituições policiais são colocadas diante de um dilema cujo impacto no seu cotidiano profissional é significativo: de um lado, o cultivo dos valores tradicionais nos quais foram formadas e que lhes dá uma certa identidade profissional; de outro lado, a necessidade de promover investimentos maciços em reformas institucionais capazes de prepará-las para os novos desafios que precisam enfrentar. A maioria das instituições policiais permanece em um meio-termo que, aliás, é a pior posição de todas, pois é aquela em que fica mais fragilizada e com menos possibilidades de agir eficientemente no enfrentamento da criminalidade.

4. Impacto nas formas de conduzir as investigações

A dificuldade das instituições policiais em relação às TIC em parte decorre do fato de que mesmo os gestores dessas instituições têm pouca informação sobre o cibercrime e as formas adequadas de enfrentá-lo. Bossler e Holt (2012), ao pesquisarem policiais dos EUA, verificaram que os funcionários das polícias daquele país não acreditam que a polícia local deve ser a principal responsável pelos casos de crimes que envolvem dispositivos informacionais. Eles constataram que as agências policiais locais sentem-se incapazes de tratar adequadamente crimes cibernéticos, principalmente porque resistem em abandonar, ou mesmo em flexibilizar, a forma tradicional de conduzir as investigações, com a qual estão familiarizados. Para os policiais entrevistados, esse tipo de crime dispensa as formas

tradicionais de construção da prova, ao mesmo tempo que exige maior familiaridade com as tecnologias que não fazem parte das habilidades comuns à maioria dos policiais que recebem a queixa e fazem o primeiro atendimento. Para tentar preencher essa lacuna – comentam os autores –, um número significativo de agências policiais tem organizado programas de treinamento para fornecer conhecimentos básicos sobre criminalidade informática e orientações relacionadas à coleta de provas. Como parte desse processo de qualificação, vários manuais e uma espécie de "guia de primeiros socorros", destinados àqueles que recebem a queixa inicial, já foram elaborados com o objetivo de detalhar os procedimentos a serem adotados em uma cena de crime praticado por meios cibernéticos, mas isso não conseguiu remover completamente o estranhamento e a desconfiança em relação às TIC.

Ao tentar captar o cerne das dificuldades das polícias para produzir investigações eficientes relacionadas ao cibercrime, Davis (2011) identificou alguns pontos fundamentais: o primeiro deles é que a polícia, no início deste terceiro milênio, provavelmente, está lidando com gerações de "criminosos" que possuem conhecimentos cada vez mais consistentes de informática, o que reduz significativamente a probabilidade de que eles sejam alcançados pelos meios tradicionais de investigação; o segundo é a constatação de que "grupos criminosos" tradicionais beneficiam-se muito das TIC para transportar ao ambiente virtual o mercado de drogas, que costumava ocorrer ao ar livre, e a prostituição, que pode ser contratada em ambientes virtuais, o que torna um pouco mais complexa a investigação dessa modalidade de delito; em terceiro lugar, e de certa forma na mesma linha de raciocínio de Sutherland (1940) sobre os crimes de "colarinho branco" também pontua que os delitos ocorridos com a utilização de computador muitas vezes não causam a mesma indignação que costumam causar os crimes cometidos com métodos tradicionais; em quarto lugar, existe

a dificuldade de compartilhar os dados obtidos tanto pelas várias agências de um mesmo país, quanto com agências de outras nações, sem contar as questões de jurisdição que envolvem determinados delitos.

Além de ser difícil determinar a unidade de aplicação da lei que deve assumir a investigação de ramificações transnacionais que utilizam o ciberespaço para concretizar suas atividades criminosas, a investigação desse tipo de crime requer uma série de recursos e a cooperação entre agências de diferentes níveis, o que torna complicado definir onde começa e onde termina a responsabilidade de cada nível de agência policial (KIRBY; PENNA, 2011). De acordo com Kirby e Penna (2011), tal fato, em última instância, contribui para que não se tenha clareza quanto ao que se deve fazer e ao papel de cada setor policial na investigação, muito menos sobre qual o montante de recursos com o qual cada instituição deve contribuir e quem os fornecerá.

Deibert e Rohozinski (2010) chamam a atenção para as dificuldades enfrentadas pelas polícias locais e pelas instituições judiciais, quando confrontadas com a necessidade de atuação em relação a determinados delitos que podem não ser definidos ou considerados crimes em outras jurisdições. Segundo os autores, o próprio conceito de jurisdição é confuso no ciberespaço, pois investigar atos, na internet, que são legais no país em que foram iniciados, mas ilegais onde foram efetivamente concretizados, é, evidentemente, uma situação problemática. Para eles, a capacidade dos Estados-Nação para lidar com a complexidade da investigação dos crimes cibernéticos é muito diferente de um país para o outro, e isso colabora para que as organizações criminosas encontrem refúgio seguro em Estados corruptos, ou naqueles em que a execução legal é frouxa; nesses Estados pouca ou nenhuma quantidade de esforço e recursos é alocada para equipamentos, qualificação de policiais e desenvolvimento de investigações nessa área.

Ao comentar a questão sob ótica semelhante, Bossler e Holt (2012) indicam a falta de um padrão para a definição do crime cibernético como um dos fatores fundamentais que contribuem para que esse tipo de crime não cause grande comoção nem seja claramente percebido pelo público, nem pelos gestores das instituições, e por isso não desperte o devido empenho para conseguir meios necessários às investigações. Eles dizem que, em geral, os executivos da polícia julgam difícil justificar o uso de recursos, cronicamente limitados nesse tipo de crime, cujos resultados, mesmo quando bem-sucedidos, têm pouca visibilidade.

Todo o aparato tecnológico que pode ser utilizado para instruir processos criminais de uma grande quantidade de informações, somado à característica transnacional e interestadual dos crimes cibernéticos, quando confrontado com a intensa mobilidade de pessoas, informações e mercadorias, tem-se tornado fundamental na reconfiguração das formas de investigação policial. Embora os operadores da segurança pública já demonstrem alguma compreensão de que também estão inseridos, gostem ou não, no emaranhado de redes e fluxos sociais e de comunicações globais, eles raramente vivem essa experiência com a preparação adequada. Muitos ainda relutam em admitir que a questão da segurança pública dependente do heroísmo pessoal dos agentes da lei não funciona quando o perfil do criminoso e seu *modus operandi* nada têm a ver com os estereótipos tradicionais de delinquentes com os quais tiveram contato nas ruas ou estão habituados a lidar no cotidiano das delegacias. Os delitos aberta ou veladamente perpetrados através da internet e redes sociais, protegidos pela distância e pela *expertise* técnica de seus operadores, capazes de deslocar recursos financeiros de um paraíso fiscal a outro sem que as autoridades do fisco sequer suspeitem, exigem um novo tipo de interpretação do fenômeno da criminalidade contemporânea, um novo tipo de intervenção e, consequentemente, novas técnicas de

investigação, e isso obrigatoriamente leva à necessidade de se elaborar uma nova concepção de trabalho policial.

5. Novos crimes e velha polícia: nossa experiência local

As dificuldades encontradas em países de capitalismo desenvolvido relacionadas ao impacto das TIC na segurança pública afetam de maneira mais intensa governos e instituições policiais da América Latina (ALVA DE LA SELVA, 2013; EVREINOFF CATALDO, 2008; MARCELLA, 2013; SAID HUNG; ARCILA CALDERÓN, 2011). Entre os que abordam especificamente a questão no Brasil, são relevantes os trabalhos de Pinheiro (2008, 2009), Mandarino Junior (2010), Alencar, Queiroz A. e Queiroz R. (2013) e Medeiros e Bygrave (2015). Esses autores têm discutido a criação de mecanismos de segurança na rede e também estratégias de investigação e persecução de ciberdelinquentes. Porém, as dificuldades relativas ao enfrentamento desse problema tornam-se sobremaneira agravadas nos estados da região Norte do Brasil, cujas instituições policiais sofrem com maior intensidade e frequência as limitações experimentadas pelas polícias das maiores metrópoles do país. Os policiais do Estado do Pará, mas especificamente aqueles ligados à DRCT, padecem especialmente da pouca oferta de qualificação na região Norte, principalmente em temas como jurisdição e rastreamento de comunicações difundidas na internet. A esse respeito, comenta um dos policiais da DRCT:

> [...] em virtude de estarmos distante fisicamente dos principais centros urbanos do país, isto se torna um fator dificultador, pois a distância, muitas das vezes, torna-se um empecilho para acompanhar o desenvolvimento das tecnologias de informação e comunicação, pois na grande maioria das vezes, os cursos, seminários, congressos e debates ainda são presenciais[8].

8 Policial lotado na DRCT até 2014.

Os policiais comentam que as questões da segurança na rede e do anonimato têm sido apenas uma das muitas responsabilidades que a delegacia especializada na repressão de crimes tecnológicos assumiu. A tarefa de agir de forma preventiva, por meio da promoção de cursos e palestras destinados a pessoas que se utilizam de redes sociais, tem sido uma preocupação constante, tanto quanto as ações de natureza repressiva. Uma das maiores preocupações consiste em esclarecer aos usuários do ciberespaço que, tanto no mundo real como no mundo virtual, a persecução penal dar-se-á com o mesmo objetivo: levar o "delinquente" à justiça.

Embora a polícia tenha uma necessidade vital de adaptar-se rapidamente à nova dinâmica introduzida pelas TIC, nem sempre essa adaptação tem sido feita com a devida celeridade. O fato de crimes com utilização de tecnologias informacionais por vezes começarem localmente e se consumarem em outra cidade, em outros estados e até em outros países ou, inversamente, começarem em outros países e terminarem localmente torna-se um fator complicador para as instituições policiais e obriga a polícia local a construir parcerias, algumas vezes informais, com instituições policiais de outras unidades da Federação e até mesmo internacionais. Um exemplo disso são as tentativas levadas a efeito por intermédio da Comunidade de Polícias da América (AMERIPOL), criada com o objetivo principal de promover o fortalecimento da cooperação policial, a troca de informações entre os países do continente americano e, ao mesmo tempo, coordenar operações de investigação criminal, assistência judicial entre as polícias e outras instituições dos sistemas de justiça criminal (LINCE BETANCOURT, 2014). O monitoramento preventivo das atividades criminosas nas redes sociais é prejudicado porque, além de tal procedimento ser objeto de inúmeras controvérsias jurídicas, também existe o fato de a DRCT não possuir meios adequados para realizar esse tipo de acompanhamento. Um dos policiais da DRCT

comenta: "[...] até o presente momento, não possuímos nenhum *software* especializado para realizar o monitoramento preventivo nas redes sociais"[9]. Da mesma forma que em outras instituições policiais brasileiras, a polícia do Estado do Pará também sofre com a falta de qualificação dos policiais para trabalhar com esse tipo de equipamento e de investigação que envolva tecnologias de informação. O mesmo policial acrescenta: "[...] por incrível que pareça, a principal limitação para uma atuação mais eficiente contra o cibercrime é a qualificação dos policiais, somada à legislação escassa e à ausência de barreiras físicas, em virtude da globalização". Tais pontos nevrálgicos já haviam sido apontados por Naim (2006) e Lince Betancourt (2014) quando analisaram a razão dos fracassos das polícias no combate à criminalidade transnacional.

Os policiais da DRCT esclarecem que os atendimentos mais comuns referem-se a crimes contra a honra, por exemplo calúnia, difamação ou injúria, e também os denominados "negócios fraudulentos", entre os quais se encaixa o crime de estelionato, o que é confirmado pelo do número de procedimentos policiais instaurados nessa delegacia, conforme demonstrado na Tabela 01, abaixo:

Tabela 01 – Principais Tipos de Ocorrência Registrados na DRCT entre 2012 e 2015

	2012	2013	2014	2015
Ameaça	21	23	22	21
Calúnia	14	20	27	15
Difamação	60	29	84	81
Estelionato	366	272	295	241
Total	461	344	428	358

Fonte: Secretaria Adjunta de Inteligência e Análise Criminal – SIAC.

Uma das características mencionadas por Zheng et al. (2006) e Bossler e Holt (2012) também é relatada pelos policiais da DRCT: segundo os registros feitos na referida delegacia, em grande parte dos casos, tanto o criminoso quanto a vítima de cibercrime são conhecidos

9 Policial lotado na DRCT até 2014.

e estão na mesma cidade, principalmente nos crimes contra a honra. Essa constatação faz reservar um papel extremamente importante para a polícia local, a despeito da necessidade de fortalecer parcerias internacionais, conforme mencionam os policiais da DRCT:

> "No que tange aos crimes contra a honra, praticados através da internet, em grande parte dos casos as pessoas envolvidas estão na mesma cidade ou pelo menos no mesmo Estado; já para os demais crimes isto não ocorre, principalmente no estelionato, pois é mais uma forma de dificultar o trabalho da polícia e, consequentemente, maior probabilidade de impunidade. A estatística vem dos procedimentos instaurados em contrapartida ao local de residência dos presos"[10].

Os policiais entrevistados acreditam que parte do sucesso dos "cibercriminosos" deve-se à sua atuação não apenas nas falhas dos programas operacionais dos computadores, mas também nas deficiências e limitações da polícia. Uma das causas dessas limitações é o fato de o combate ao cibercrime não ser classificado como alto nível de prioridade entre as preocupações dos gestores públicos. Os policiais mencionam como exemplo uma investigação iniciada no Estado do Pará, cujo desfecho foi deflagrado na cidade de São Paulo com a prisão de mais de uma dezena de cibercriminosos, em uma operação conjunta que envolveu policiais paraenses e paulistas. Embora o resultado inicial tenha sido a prisão dos principais criminosos, a maioria deles foi posta em liberdade simplesmente porque os policiais paraenses não dispunham de recursos suficientes para transferi-los, por via aérea, de São Paulo para Belém. Eis um exemplo cabal da falta de apoio e da ausência de prioridade em combater esse tipo de crime.

É sintomático da pouca atenção dada ao cibercrime e aos policiais encarregados de reprimi-lo o fato de que não existe, na polícia do Estado do Pará, qualquer programa sistemático de qualificação

10 Ex-delegado da DRCT.

destinado aos policiais que trabalham nessa área. Da mesma forma que em polícias de outras partes do mundo, na polícia do Estado do Pará, também há resistências entre os segmentos mais conservadores, pois, "[...] na grande maioria das vezes, este segmento não possui o conhecimento de como deve-se combater este tipo de ilícito e, em virtude disso, acaba ficando em segundo plano no que tange à prioridade"[11].

Enfim, o trabalho policial, em tempos de computadores e de internet, passa por uma séria crise existencial. Com base nas palavras de Capra (2006), podemos dizer que essa situação decorre do fato de estarmos tentando aplicar os conceitos de uma visão de mundo obsoleta – a visão de mundo mecanicista da ciência cartesiana-newtoniana – a uma realidade que já não pode ser entendida em função desses pressupostos, pois, como esclarece Lince Betancourt (2014), as atividades criminosas que constituem desafios contemporâneos têm a característica de serem espacialmente fluidas e transnacionais, já que sua atuação não depende de latitudes geográficas específicas e sua alta capacidade de adaptação mediante suas múltiplas redes globais consegue facilmente escapar às ações da justiça, ao mesmo tempo que é gerada uma grande quantidade de problemas sociais, econômicos e políticos por sua ampla capacidade de penetração em todas as dimensões da vida social.

6. Considerações finais

Apesar das diferenças, no que diz respeito tanto ao acesso à tecnologia como à cultura organizacional, as instituições policiais, de modo geral, não costumam ter muita intimidade com as tecnologias de comunicação e informação. A não ser por alguns departamentos especializados diretamente envolvidos com esse tipo de tecnologia,

11 Ex-delegado da DRCT.

as TIC ainda são vistas com certa desconfiança por grande parte dos policiais de formação mais conservadora. Eles ainda compreendem o trabalho policial como manutenção da lei e da ordem e monopólio da violência legítima. A perenidade dessa percepção foi confirmada pelos depoimentos coletados junto aos policiais da DRCT, para os quais esse é um dos grandes desafios a superar. Isso nos leva a concluir que as dificuldades arcadas por eles fora ou dentro da polícia civil do Estado do Pará guardam bastantes semelhanças com as encaradas por policiais de outras unidades da federação e até de outros países. A maioria dos problemas enfrentados tem como causa a falta de compreensão dos novos desafios impostos às instituições policiais e da importância que as TIC passaram a ter para a prática de crimes e para o trabalho policial.

As tentativas de superar essas dificuldades passam, necessariamente, pela adoção de uma nova percepção do crime e de seu enfrentamento, que seja capaz de dar conta das transformações sociais e da reorganização das atividades criminosas possibilitadas pelos desenvolvimentos das TIC. Um dos primeiros e mais importantes passos nessa direção consiste em construir redes de interfaces que permitam à polícia uma rápida movimentação na dimensão macro das redes globais, dos mercados internacionais, dos fluxos transnacionais, mas também, e ao mesmo tempo, permitam uma movimentação no sentido inverso, construindo possibilidades de diálogo com redes de interfaces internas, comunitárias e locais, e sempre abertas à possibilidade de novas ramificações.

Essa estratégia de atuação nas interfaces exige uma capacidade de análise que, infelizmente, ainda não faz parte da formação da maioria dos policiais incumbidos da prevenção e do combate à criminalidade. É preciso que os policiais ganhem intimidade com as TIC para que consigam percebê-la como aliada e não como adversária de seu trabalho. Da mesma forma que no treinamento tradicional

são simuladas inúmeras situações que o policial poderá enfrentar no cotidiano de seu trabalho, acreditamos que também deva fazer parte de sua formação, desde a academia de polícia, o treinamento para o enfrentamento da criminalidade virtual. Tais medidas tornam-se necessárias, além de óbvias, porque nos parece impossível acompanhar o crescente desenvolvimento das diversas modalidades criminosas e apreender, de forma eficaz, as técnicas para reprimi-las, apenas instruindo os policiais no manejo de armas de fogo, na condução de viaturas e no uso da força. Essas técnicas, que durante muito tempo foram o fundamento dos processos de preparação dos policiais e da intervenção da polícia, mostram-se insuficientes diante da criminalidade construída com base na tecnologia de ponta, que é característica do ciberespaço.

Referências

ALENCAR, Gliner Dias; QUEIROZ, Anderson Apolonio Lira; QUEIROZ, Ruy José G. B. de. Insiders: análise e possibilidades de mitigação de ameaças internas. **Revista Eletrônica de Sistemas de Informação**, v. 12, n. 3, p. 1-38, set./dez. 2013.

ALVA DE LA SELVA, Alma Rosa. De las promesas de la Cumbre e la crisis global: la brecha digital en América Latina. Telos: Cuadernos de Comunicación e Innovación, n. 94, p. 24-30, 2013.

AUGUST, Ray. International cyber-jurisdiction: a comparative analysis. **American Business Law Journal**, v. 39, n. 4, p. 531-574, jun. 2002. Disponível em: <http://onlinelibrary.wiley.com/doi/10.1111/j.1744-1714.2002.tb00305> Acesso em: 3 maio 2014.

BOSSLER, Adam M.; HOLT, Thomas J. Patrol officers'perceived role in responding to cybercrime. **Policing:** An International Journal of Police Strategies & Management, v. 35, n. 1, p. 165-181, 2012. Disponível em: <www.emeraldinsight.com/1363-951X.htm>. Acesso em: 11 abr. 2014.

BUTTON, Mark. Cross-border fraud and the case for an "interfraud". **Policing:** An International Journal of Police Strategies & Management, v. 35, n. 2, p. 285-303,

2012. Disponível em: <www.emeraldinsight.com/1363-951X.htm>. Acesso em: 22 abr. 2014.

CAPRA, Fritjof. **O ponto de mutação**: a ciência, a sociedade e a cultura emergente. São Paulo: Cultrix, 2006.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

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

DAVIS, Justin T. Examining perceptions of local law enforcement in the fight against crimes with a cyber componente. **Policing:** An International Journal of Police Strategies & Management, v. 35, n. 2, p. 272-284, 2011. Disponível em: <www.emeraldinsight.com/1363-951X.htm>. Acesso em: 11 abr. 2014.

DEIBERT, Ronald J.; ROHOZINSKI, Rafal. Risking security: policies and paradoxes of cyberspace security. **International Political Sociology**, v. 4, n. 1, p. 15-32, mar. 2010. Disponível em: <http://onlinelibrary.wiley.com/doi/10.1111/j.1749-5687.2009.00088.x/full> Acesso em: 19 abr. 2014.

EVREINOFF CATALDO, Iván. **La desinformación política en la guerra de los medios**. In: Cuadernos pedagógicos. Universidad Católica Nuestra Señora de la Asunción. Facultad de Filosofía y Ciencias Humanas: Asunción, nov. 2008.

FOUCAULT, Michel. **Vigiar e punir**. Petrópolis, RJ: Vozes, 2007.

GARLAND, David. A cultura do controle: crime e ordem social na sociedade contemporânea. Rio de Janeiro: Revan, p. 422, 2008.

KIRBY, Stuart; PENNA, Sue. Policing mobile criminality: implications for police forces in the UK. **Policing:** An International Journal of Police Strategies & Management, v. 34, n. 2, p. 182-197, 2011. Disponível em: <www.emeraldinsight.com/1363-951X.htm> Acesso em: 17 abr. 2014.

LÉVY, Pierre. **As tecnologias do pensamento:** o futuro na era da informática. Lisboa: Instituto Piaget, 1994.

_____. **Cibercultura**. São Paulo: Ed. 34, 1999.

_____. **A inteligência coletiva**: por uma antropologia do ciberespaço. São Paulo: Loyola, 2007.

LINCE BETANCOURT, Lina Facio. Cooperación policial entre Colombia y Centroamérica y el Caribe: el crimen organizado y el accionar de Ameripol bajo el enfoque multidimensional de la seguridad hemisférica. **Memorias:** Revista Digital

de Historia y Arqueología desde el Caribe Colombiano, Barranquilla, ano 10, n. 23, p. 1-24, maio/ago. 2014.

LUHMANN, Niklas. **Sistemas sociales:** lineamientos para una teoria general. Rubi (Barcelona): Antropos, 1998.

MANDARINO JUNIOR, Raphael. **Segurança e defesa do espaço cibernético brasileiro**. Recife: Cubzac, 2010.

MARCELLA, Gabriel. The transformation of security in Latin America: a cause for common action. Journal of International Affairs, v. 66, n. 2, p. 67-83, Spring/Summer 2013.

MEDEIROS, Francis Augusto; BYGRAVE, Lee A. Brazil's Marco Civil da Internet: does it live up to the hype? **Computer Law & Security Review:** The International Journal of Technology Law and Practice, v. 31, n. 1, p. 120-130, fev. 2015.

NAIM, Moisés. **Ilícito**: o ataque da pirataria, da lavagem de dinheiro e do tráfico à economia global. Rio de Janeiro: Jorge Zahar, 2006.

PINHEIRO, Patrícia Peck. **Curso de fundamento em gestão de segurança da informação e comunicações:** boas práticas de direito digital na administração pública. São Paulo, 2008. Disponível em: <http//www.planalto4.gov.br>. Acesso em: 1 set. 2015.

_____. **Direito Digital**. São Paulo: Saraiva, 2009.

SAID HUNG, Elias; ARCILA CALDERÓN, Carlos. Los cibermedios en América Latina y la Web 2.0. **Comunicar:** Revista Científica Iberoamericana de Comunicación y Educación, Barranquilla, n. 37, p.125-131, 2011.

SUTHERLAND, Edwin H. White-collar criminality. **American sociological review**, v. 5, n. 1, p. 1-12, 1940.

ZHENG, Rong; LI, Jiexun; CHEN, Hsinchun; HUANG, Zan. A framework for authorship identification of online messages: writing-style features and classification techniques. **Journal of The American Society for Information Science and Technology**, v. 57, n. 3, p. 378-393, fev. 2006.