RESENHA

GOODMAN, Marc. "**Future Crimes:** Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It (1 ed. Nova Iorque: Doubleday, 2015)

Quando tudo está conectado e vulnerável ao crime, o que fazer?

MATEUS DE OLIVEIRA FORNASIER*

"**Future Crimes:** Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It" (1 ed. Nova Iorque: Doubleday, 2015), do jurista e autoridade em segurança digital estadunidense Marc Goodman, traz uma série de exemplos práticos e questões teórico-jurídicas relacionadas à segurança na internet (concernentes ao presente e às possibilidades futuras). Trata-se de uma obra extremamente atual, em que questões da nossa época (na qual, como o próprio subtítulo sugere, "tudo está conectado" e "todos estão vulneráveis") é um verdadeiro alerta contra o que estamos expondo sobre nossas vidas privadas, bem como o que pessoas mal-intencionadas poderiam fazer com esses dados que ingenuamente fornecemos em rede diuturnamente.

À primeira vista se poderia pensar: um especialista em segurança estadunidense (Goodman já foi funcionário do Departamento de Polícia de Los Angeles – o LAPD – antes de sua carreira acadêmica), tratando sobre possibilidades de explorar as vulnerabilidades tecnológicas do cidadão comum, provavelmente beira a paranoia em seu etnocentrismo, apresentando o mundo como estado constantemente ameaçado pelo terrorismo. E, de fato, é o que se encontra na obra: muitos casos de invasão de privacidade por criminosos (hackers que se apropriam de senhas na internet, de cartões de crédito, de perfis em comunidades virtuais, de localizações em GPS e outras situações já comuns em nossos cotidianos). Contudo, há de se dar um voto de confiança ao autor e seguir adiante na leitura, pois longe de ser etnocêntrica e paranoica, a obra é coerentemente alarmista.

Em sua obra, o autor expõe que, apesar de o mundo estar cada vez mais conectado à internet (e, consequentemente, dela mais dependente), pois desde os particulares até as empresas, passando-se pelos serviços de infraestrutura básicos (transportes públicos, polícia, energia elétrica, etc.), todos estão dependentes da rede – cuja segurança, contudo, conforme o autor busca expor, é ilusória. Em primeiro lugar, ilustrem-se os programas antivírus, com os quais grandes somas são gastas por empresas e particulares: com informações e dados consistentes, o autor busca provar sua cada vez menor eficácia em relação à sagacidade de hackers (que podem agir por simples diversão, a serviço do crime ou de governos). Seja qual for o método de segurança eletrônica nas comunicações feitas pela internet, é

questão de horas (ou minutos), para invasores, a intrusão em seus sistemas.

Agrava a situação a complexidade tecnológica do porvir que já se ensaia atualmente. As combinações e interpenetrações possíveis entre várias formas tecnológicas (e.g. biotecnologias, robótica, impressão 3D, internet das coisas, nanotecnologias) permitem pensar num cenário que beira o apocalíptico. Cenário este em que as já praticamente insuperáveis intrusões via internet se demonstram simplórias.

A tecnologia permite ao crime um crescimento exponencial nos seus resultados (e.g. frutos de crimes virtuais contra o patrimônio): quanto mais o mundo se torna dependente do computador, mais complexos se tornam os códigos-fonte dos softwares usados – o que significa que mais possibilidades de invasão sua (o que permite a inserção de malwares, aumento das possibilidades de invasão, etc.) se apresentam a criminosos. Aliás, tantos são os atores (hackers, ciberativistas, governos, organizações criminosas) quantas são as intenções destrutivas no que tange ao uso da internet. De outra banda, tanto é o aumento da complexidade das possibilidades de uso mal-intencionado da internet e da informática quanto o é o da dependência da tecnologia para a vida cotidiana – e as organizações cujo propósito é fornecer a segurança neste âmbito não têm capacidade de se desenvolver na mesma taxa exponencial.

As redes sociais são também delineadas por Goodman como sendo, na verdade, grandes depósitos de informações exploráveis pelas companhias das mais variadas naturezas. Num cenário assim, aquilo que o consumidor digita em fóruns relacionados à saúde, por exemplo, é organizado pelos mantenedores desses sítios da internet, classificado e vendido a outras empresas, que poderão se utilizar desses dados para os mais variados fins relacionados a seguros de saúde, grandes laboratórios farmacêuticos, etc. Isto porque nas letras miúdas dos contratos online a que o comunicador em um fórum ao dele participar, muitas vezes, estabelece o direito da companhia mantenedora do fórum a comercializar/repassar suas informações a terceiros. Aliás, nem ao menos o anonimato é resguardado em tais situações, tendo em vista que já há, no mercado, empresas fornecedoras de serviços de "engenharia reversa" de software, capazes de rastrear o uso de pseudônimos em sítios dessa natureza. Em outras palavras, o consumidor se torna também produto nas redes sociais, estando sua privacidade a ser comercializada.

Google e Facebook seriam exemplos de companhias cujas estratégias de captação, organização e oferecimento de dados e perfis pessoais são emblemáticos e desafiadores de qualquer estrutura política e jurídica – não apenas de modo hipotético, mas também em ocorrências fáticas. A gratuidade dos produtos e serviços ofertados atrai as pessoas e as companhias, mas subrepticiamente, na verdade, estão a captar cotidianos e características que, de modo organizado, irão disponibilizar aos seus investidores e patrocinadores. Isto já se revela na prática, com a quantidade de processos sendo ajuizados, ao redor do mundo, em face desses gigantes que ofendem a privacidade alheia e a tornam seu produto.

Juridicamente, a ferramenta permissionária do contrato eletrônico de "Termos e Serviços" – onipresente em comunidades virtuais e assemelhados, mas oniscientemente ignorados – torna

onipotentes as companhias que as controlam. Estas se tornam, fática e hipoteticamente, titulares de direitos sobre toda e qualquer informação (inclusive pessoal) que os usuários vierem a nelas postar. Ademais, a revolução dos aparelhos celulares permitiu a potencialização da intrusão na privacidade, dado que cada vez mais tecnologias de detecção dos contextos em que seus usuários se inserem são incorporadas a tais aparelhos: seus aplicativos, câmeras e sistemas de GPS abrem possibilidades infinitas, combinadas aos "Termos de Serviço" sub-reptícios.

Segundo nos traz o autor, quando somados os lucros anuais das empresas de monitoramento de dados dos consumidores na internet, encontra-se um montante três vezes maior do que o que dispõe anualmente a Agência Nacional de Segurança dos EUA – revelando-se que a maior parte da vigilância de dados está sob o domínio privado. Seu poder de invasão da privacidade dos consumidores é enorme – mas, apesar disso, ainda não há qualquer regulação (lei, norma administrativa, etc.) pelo governo dos Estados Unidos da América (país de Goodman) desta matéria. Há tentativas da parte de alguns Congressistas; porém, os enormes lucros (possíveis e efetivos) a partir da ligação entre as atividades dessas empresas e o lobby realizado no Legislativo estadunidense pelos representantes dos interessados são fortes indícios de que qualquer tentativa regulatória será desanimada e impedida de prosseguir.

A tecnologia de bancos de dados informatizados e ligados em rede, somada àquelas de GPS e telefonia celular, tornariam essas companhias capazes não apenas de saber onde as pessoas estiveram (ou estão): o cruzamento de dados com probabilidades de rotinas permite traçar vários tipos de perfil (religioso, político, de consumo, de opção sexual, etc.), o que já constitui grave ameaça às liberdades individuais em países onde a lei é mais liberal – mas imagine-se em outros, em que desvios do "normal" são considerados crimes (homossexualidade, diferença política, religiosa, etc.).

Ademais, o posicionamento jurídico dominante nos EUA, no que tange à matéria, segundo Goodman, é o do chamado *third-party doctrine*, segundo a qual as informações que os indivíduos compartilham na internet são considerados espaços de acesso público – e não os *private papers* que gozam de status de acesso privado de acordo com a Constituição estadunidense – o que, somado aos Termos de Serviço de qualquer comunidade virtual ou aplicativo de smartphone, deixa o consumidor não apenas desprotegido, mas reforça ainda mais a tese de que sua privacidade se converte em mercadoria. Aliás, estes dados estão também à disposição da polícia, da Justiça e de Agências de Serviço Secreto – bem como são alcance de todos aqueles que puderem pagar pelo acesso a eles. Isto pode vir a gerar possibilidades probatórias (e suas distorções) de modos surpreendentes em investigações e processos dois mais variados tipos - com uma eficiência com que até mesmo agentes de antigas polícias secretas sequer sonhariam. A vigilância quase absoluta foi atingida, e não há regulação jurídica plausível.

Este delineamento permite que o autor realize uma incursão num oceano de possibilidades futuras do crime tecnológico – no qual não apenas senhas na internet, cartões de crédito e perfis em comunidades virtuais são clonados:

passa-se a um novo estágio, em que se materializam: i) o roubo de identidades biométricas; ii) o uso de robôs, *drones* e inteligência artificial para se cometer crimes; iii) a materialização sem precedentes de crimes praticados com o uso de biotecnologia, nanotecnologia e física quântica. Entretanto, esse cenário apocalíptico é mitigado com propostas para o presente e para o futuro a fim de se evitar seu agravamento: desde atitudes simples como atualização frequente de senhas e descarregamento de arquivos apenas de sítios confiáveis, até questões relacionadas com uma repaginação total da política global de segurança na rede até o projeto de um grande conjunto de medidas tecnológicas combinadas chamadas de "higiene cibernética".

Analisando criticamente, nota-se que a obra não faz parte de uma matriz teórico-jurídica bem definida (talvez se possa falar de Realismo Jurídico ou de Estudos Jurídicos Críticos). Mas isto não constitui nenhum demérito à obra: trata-se de um texto de fácil compreensão, de grande riqueza de detalhes e de um contato permanente para com a realidade (sem se perder, em momento algum, em devaneios teóricos eruditos de pouca utilidade). Pode-se até mesmo caracterizar esta obra, talvez, como exemplo a ser seguido por teóricos das mais variadas áreas do Direito: a imaginação baseada em prognósticos e dados bem sopesados e relevantes é necessária em um campo de estudos tão viciado pela repetição daquilo que outros já fizeram como indício de uma falta de criatividade assombrosa.

Recebido em 2015-05-14
Publicado em 2015-07-09

* **MATEUS DE OLIVEIRA FORNASIER** é Doutor em Direito Público pela Universidade do Vale do Rio dos Sinos (UNISINOS, São Leopoldo/RS, Brasil). Professor do Mestrado em Direitos Humanos da Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UNIJUI, Ijuí/RS, Brasil)