TUTELA PENAL DA SEGURANÇA INFORMAÇÃO: POLÍTICA CRIMINAL NO AMBIENTE DE ALTA TECNOLOGIA

Leonardo Rezende Cecilio [1]

[1] Advogado criminalista (Brasil). Pós-Graduando em Direito Penal Econômico pela Faculdade de Direito da Universidade de Coimbra (Portugal). Pós-Graduando em Direito Público pela Universidade Cândido Mendes (Rio de Janeiro). Graduado em Direito pela Faculdade de Ciências Sociais Aplicadas Ibmec/RJ. Discente do Curso de Formação Perito em Análise Computacional Forense (CLAVIS). Membro da Assotiation Internationale de Droit Pénal (AIDP), do Instituto Brasileiro de Ciências Criminais (IBCCRIM) e do Instituto Brasileiro de Direito da Informática (IBDI).

RESUMO: Este trabalho é dedicado a debater a segurança da informação como novo bem jurídico-penal dotado de aptidão para instrumentalizar a incipiente política criminal no ciberespaço. Considerando os diferentes papéis que assume para as entidades da sociedade pós-industrial, a informação revela possuir uma peculiar identidade binária, sendo o interesse juridicamente violado em uma série de condutas hostis, as quais os outros campos do Direito não são capazes de inibir – mostrando-se ostensiva a necessidade de intervenção pela disciplina penal. Contudo, ante o risco de pulverização de dispositivos penais sem qualidade técnica, é primordial catalogar os variados tipos de condutas mal intencionadas e correlacioná-las com os respectivos bens jurídicos ameaçados para que, finalmente, seja possível apresentar um conceito de crime informático congruente com a subsidiariedade do Direito Penal.

PALAVRAS-CHAVE: Política Criminal. Segurança da Informação. Bem jurídico. Crime informático.

"In pessima republica plurimae legis."
(Tácito)

1. Intróito

No século XIX, Jules Henri Poincaré afirmou que o progresso científico é resultante da aproximação de ciências, observando-se a semelhança entre suas formas – apesar das diferenças entre suas matérias. Etimologicamente derivada do grego *kybernetes* (*timoneiro*; *piloto*), a expressão *cibernética* guarda original relação semântica com a atividade de controlar. Os tempos atuais testemunham a virtualização de conhecimentos e atividades, onde a aparente liberdade proposta pela internet não é despretensiosa – em verdade, inversamente proporcional à privacidade, homeopaticamente renunciada a cada clique. Nesse cenário, a falaciosa gratuidade dos serviços oferecidos na rede é paga com a informação – a moeda da nova *economia dos dados*, cujo controlador ainda não foi revelado.

Hoje, as relações sociais mantidas somente a partir (e através) da tecnologia da informação clamam com nitidez pela intervenção regulatória do Estado. A História coleciona episódios que deixaram evidente que a desregulação pode ser um sedutor veículo de desenvolvimento sem a inconveniência de controles políticos, mas também um prefácio de situações traumáticas. Exemplo autoexplicativo foi a crise mundial de 2008 – sequela do *laissez-faire, laissez*-passez norte-americano para o setor financeiro, iniciado na década de 1980. Por outro lado, a arquitetura peculiar do ambiente digital – autônoma, autorreguladora e evolucionista – inviabiliza a demarcação de fronteiras, e, com ela, o estabelecimento de jurisdições.

Embora enfrente certa reticência, existe o pensamento de que a informação deve ser alçada ao *status* de bem jurídico-penal, emergente das revoluções tecnológicas. Não há dúvidas de que se trata de um elemento que se tornou indispensável *para uma vida juridicamente segura* (ROXIN, 2011, p. 185), e um dos maiores desafios que o Direito Penal encontra para protegê-lo é diagnosticar sua natureza e traduzi-la para sua própria linguagem – condição elementar para que o sistema jurídico possa operar com tecnicidade, como ensina Knut Amelung.

Ocorre que nas sociedades pós-industriais é perceptível a existência de uma clara dilatação da disciplina penal na legislação de diversos países – condicionada por uma suposição (de escala global) de que se chega à pacificidade a partir da edição reiterada de tipos penais e do asseveramento das penas (SILVA SÁNCHEZ, 2011). Segundo o mestre espanhol Jesus María Silva Sánchez, catedrático de Direito Penal da Universidad del País Basco e da Universidad Pompeu Fabra, essa tendência acompanha o fenômeno da globalização, ampliando os espaços de riscos jurídico-penalmente relevantes, propondo a criação de novos tipos penais, flexibilizando regras de imputação e relativizando princípios político-criminais (*ibidem*, p. 05) – pelo que, a partir da última década, adquiriu inédita tônica a discussão sobre a necessidade de se reconduzir a intervenção punitiva do Estado a uma plataforma minimalista.

O Direito Penal é ramo jurídico protetor somente dos bens jurídicos mais relevantes. É isso que torna possível afirmar que a norma penal incriminadora não é o objeto legítimo da tutela penal, mas sim como a ferramenta adequada para a proteção pretendida de determinados bens individuais, sociais ou reais, que são, aliás, seu substrato validador. São os bens jurídicos impedem que o mero ato de desafiar um comando proibidor esgote o conceito de delito – razão pela qual uma ampla frente de defensores os concebem como instrumento de orientação crítica da política criminal. Nesse sentido, a expansão da disciplina penal parece obrigada a se submeter *à aparição de novos bens jurídicos – de novos interesses ou de novas valorações de interesses preexistentes* (SILVA SÁNCHEZ, 2011, p. 11).

De todo modo, não render-se o Estado a um já conhecido punitivismo simbólico não se confunde com subestimar transformações cosmovisionais e, consequentemente, negar novos contornos do *modus vivendi*. Todavia, a menos que se pretenda abandonar o caráter científico da atividade jurídica, o pensamento sistemático deve ser orientado a fim de se buscar a maneira mais justa de pacificar questões problemáticas (MUÑOZ CONDE, 1972, p. 17), pelo que é inadmissível permitir que a urgência subverta a produção do Direito (ÖST, 1999, p. 360) em pleno século XXI, sobretudo diante da coletânea de tragédias experimentadas por inúmeros Estados ao longo da História, resultado de manipulações e imprudências legislativas.

É criada, assim, uma tensão dialética entre a pungente de se proteger relações sociais mantidas somente a partir (e através) dos avanços tecnológicos e a irrenunciável índole de *ultima ratio* da disciplina penal, cuja abdicação implicaria, já de imediato, em uma pulverização de dispositivos jurídico-penais. Ganha relevo, pois, o indesviável debate acerca de como se conferir proteção jurídico-penal àquilo a que se tem apontado como um superestimado condutor de um mundo moldado pela tecnologia: a informação.

2. Intervenção penal no ciberespaço

2.1. A natureza binária da informação

Giambattista Vico sinalou que *os homens, sempre que das coisas remotas e desconhecidas não podem fazer nenhuma ideia, avaliam-nas a partir das coisas deles conhecidas e antevistas* (VICO, 1974). De variadas nacionalidades, existe a (limitada) leitura de que a delinquência informática é uma combinação de computação e delitos já previstos no ordenamento jurídico. Por outro lado, há quem acredite que todas as ofensivas relacionadas à informática estão descobertas pelo ordenamento jurídico. Ocorre que há eventos em que a informática é mais do que um mero instrumento para a prática de condutas já tipificadas, e ignorar lesões específicas, somente possíveis a partir do emprego da tecnologia da informação, sugere a negação de novas inteligências, subtraindo da sociedade da informação uma evolução com segura em tempos baseados no binômio *desenvolvimento-riscos* [1].

Como já afirmado, um dos maiores desafios à tutela jurídica da informação decorre da complexidade de se identificar sua natureza, permanecendo sua definição ainda incógnita, inclusive para os campos de pesquisa voltados

para o estudo crítico sobre sua estrutura conceitual e de seus princípios básicos (MATTOS, 2014). Isso porque, até hoje, nenhum bem jurídico recebeu diferentes valorações ao ser analisado em situações distintas. Por exemplo, a vida de uma ou de outra pessoa tem a mesma relevância para o Direito Penal, recebendo igual tutela, independentemente de quem seja seu titular. O mesmo ocorre com a liberdade, a dignidade e a propriedade. Por outro lado, considerada sua ubiquidade nas sociedades contemporâneas, a informação assume diferentes papéis frente à maquina pública, ao mercado e à sociedade civil, representando diferentes formas de valor já que, naturalmente, cada uma dessas entidades dela se vale de forma distinta. Sua vitalidade é inequívoca, mas subsumi-la no conceito de bem jurídico é, antes de tudo, um desafio de ordem semântica.

Apesar de sua indefinição conceitual, se analisarmos isoladamente o comportamento da informação para o Estado, para uma empresa e para o indivíduo, podemos identificar uma característica binária, inédita no universo dos bens jurídicos: uma dimensão econômico-patrimonial e uma dimensão individual. Duas identidades distintamente valoradas, reunidas em um mesmo princípio.

No campo privado, a informação se tornou o fundamento das organizações modernas (DRUCKER, 1992) – o que faz dela um capital estratégico, inclusive concebido no âmbito da inteligência empresarial. Moedas e notas – tecnologias outrora criadas para registrar proprietários e propriedades – cumpriram seu papel; hoje, *o ativo mais importante é o conhecimento; a manifestação de vontade é não presencial, as testemunhas são as máquinas e o documento original é o arquivo – o impresso é cópia* (PECK & SLEIMAN, 2006).

Principalmente na indústria e nas atividades financeiras de natureza especulativa, a disseminação seletiva de informações é uma inquietude constante – resultado da cultura do compartilhamento (SIANES, 2007) –, já que sua utilização assimétrica pode imprimir distorções no mercado privado ao dar superlatividade a um agente econômico que a possua. Na busca por vantagem competitiva, a inovação métodos, fórmulas, produtos e serviços é um fator interveniente na tomada de decisões e pode determinar lideranças – processo no qual a informação é afirmada como um insumo. Ou seja, diz-se respeito, aqui, à hegemonia comercial, e, particularmente nesta realidade, a subtração do capital intelectual tem se tornado uma atividade cada vez mais rentável e atraente, tangendo diretamente o direito à propriedade e a livre concorrência de mercado.

No tocante ao Estado, a informação também figura como um recurso estratégico, sob a forma de conhecimento sensível, desta vez, hábil a lançar seu proprietário a posições de destaque na comunidade internacional. Os conhecimentos sensíveis são aqueles de alto valor agregado e estratégico para um país, com potencial de gerar oportunidades de desenvolvimento econômico, tecnológico e científico (*ibidem*), e, na maioria dos países, a máquina pública tem confiado à informática a salvaguarda de dados, o planejamento, a execução e o controle dos serviços essenciais, pelo que protegê-los se tornou um dos maiores desafios do século XXI.

É natural que o interesse em tutelar a informação toque também à manutenção da soberania e assuntos estatais. Nos últimos anos, têm sido denunciadas distorções na agenda internacional de cibersegurança no que se refere à coleta massiva de dados de alvos de alto perfil – como chefes de Estado, representações diplomáticas e empresas de setores estratégicos –, o que, dissonante dos objetivos formalmente declarados, se confunde com espionagem política, econômico-financeira e industrial. Não obstante, isso confirma o referencial econômico-patrimonial da informação, na medida em que qualquer interesse na obtenção de conhecimentos estratégicos se refere a disputas por hegemonia (política ou econômica) – o que, por sua vez, retoma, direta ou indiretamente, a própria lógica de mercado.

Podemos observar que nessas duas hipóteses mencionadas, a informação não é um fim em si mesmo e não possui um valor intrínseco, devendo se considerar o valor que ela agrega enquanto elemento fundamental para o desenvolvimento do Estado e do mercado privado. Portanto, ela figura como um objeto singular, sujeito à

disponibilidade e à negociabilidade, submetida exclusivamente a critério de seu titular. Em semelhante sentido é bem-vinda a afirmação de Marco Antônio Zanellato de que *os bens jurídicos informáticos não valem pelo que são, mas pelo que agregam* (ZANELLATO, 2002, p. 167). Isso significa que (reiteramos, para esse plano), uma vez perdida a utilidade econômica de uma informação, já não subsiste razão para resguardá-la juridicamente.

A outra face da informação, por seu turno, gira em torno das relações humanas, estando fincada em uma plataforma antropocêntrica. Hoje, informação é no ciberespaço um projetor da vida privada – gênero que abarca desde o direito à privacidade até a inviolabilidade de comunicações e correspondências, o que é essencial para o exercício da liberdade de pensamento.

Segundo a Electronic Frontier Foundation (EFF), conhecidos não mais do que a data de nascimento, o código postal e o sexo (o que corresponde a uma quantidade de informação mensurada em, aproximadamente, 33 bits) é possível deduzir a identidade de alguém (EFF, 2010). Isso conota haver uma sociedade de controle [1] – a se considerar o fato de que, praticamente, já não há atividade isenta de registros por tecnologias informacionais (MORAES, 2013).

A atual dimensão planetária da internet *é como um organismo sem pele* (ASSANGE *et al*, 2013, p.82), onde tudo o que é feito é visto. Uma compilação de dados do usuário, baseada em seu histórico personalizado de navegação, vem sendo armazenada indistintamente em servidores distribuídos por todo o globo, submetida (quando muito) a escassa regulação jurídica. Isso ilustra uma evidente defasagem da autonomia individual e uma mitigação de todo o controle que o individuo tem sobre sua esfera mais íntima – agora condicionado à capacidade de governar a informação. Por isso, na faceta individual da informação não há que se falar em valor agregado, posto que ela se revela como um fim em si mesmo – inalienável, inviolável e, tampouco, passível de barganha ou acumulação. Aqui, a informação possui um valor intrínseco; sua própria essência é sua validade.

2.2. A segurança da informação como bem jurídico-penal

A ciência jurídica é intimamente ligada à práxis social. Embora deva ser construída e, a todo tempo, desconstruída com responsabilidade e comprometimento, precisa, igualmente, atender às condições pragmáticas da sociedade, sob pena de se tornar uma coleção de obviedades e silogismos divorciados do cotidiano humano. Nesse prisma, sobre a intervenção do Direito Penal, ensina afortunadamente Juarez Tavares que, em vez de ser tratado o bem jurídico como o objeto de proteção, *deve assumir a posição de objeto de referência necessário da incriminação* (TAVARES, 2009, p. 233) [2].

Discutir política criminal demanda um estudo sinérgico e uma coerente reflexão da Criminologia e da real função consagrada do Direito Penal [3], as *ferramentas conceituais*. Objetiva-se, pois, uma estratégia semântico-jurídica que torne idônea a incriminação de determinadas condutas, cumprindo, nessa oportunidade, investigar os princípios que norteiam a via da intervenção penal de modo a discutir tratar-se de um *bem jurídico-penal* – conceito que *continua a ser o ponto de partida da incriminação* (HENFENDEHL, 2011, p. 72).

Limitador do poder punitivo do Estado – e corolário dos princípios da intervenção mínima e da reserva legal –, é no princípio da subsidiariedade que a disciplina penal é resumida à tutela seletiva do bem jurídico (BITENCOURT, 2000, p. 12), limitando-se a proteger somente aqueles mais relevantes porque não contemplados de modo bastante pela proteção dos demais ramos do Direito. *Os princípios situam-se no plano deontológico*, ensina Humberto Ávila (2012, p. 87), estabelecendo a obrigatoriedade de se adotar as condutas que forem necessárias para a promoção de um estado de coisas. É assim questionável a partir de que momento um bem jurídico deve ser elevado à categoria de bem jurídico-penal, apto a reputar necessária a intervenção do Estado por tal via (PRADO, 2011, p.110 e

[1] Locución idealizada por Gilles Deleuze.

ss). Para Santiago Mir Puig e Luiz Regis Prado, a questão é sanada por um *juízo de suficiente importância social* capaz de justificar o valor do bem analisado para a sociedade, comprovando sê-lo merecedor daquele *status.* Para tanto, é preciso pautar-se na concepção de Estado de Direito, exercendo esse juízo de valor nos limites de suas funções dogmáticas (AMELUNG, 2011, p. 118).

Genericamente, a melhor doutrina acorda que a teoria da proteção de bens jurídicos exija que uma norma de comportamento penalmente sancionada deva sempre proteger um bem – assim impondo a recusa à legitimação de normas penais inúteis (HEFENDEHL, 2011, pp. 157-158). Nessa linha, Knut Amelung defende que a teoria dos bens jurídicos demanda que a norma tenha utilidade mais profunda e significativa do que a mera preocupação em manter sua vigência fática, cabendo ao legislador fixar essa utilidade – sabatinada por critérios constitucionais. No entanto, o autor assinala como exagero pretender que o objeto de toda norma penal apresente sempre uma referência específica à pessoa – que, para uns, é o bem jurídico matriz e superior (AMELUNG, 2011, p. 129).

Confrontando esse raciocínio, Winfried Hassemer filia-se a uma noção pessoal do bem jurídico (igualmente defendido por Marx e Hohmann), acompanhando o posicionamento de Franz Birnbaum (1834) no sentido de que tal conceito precisa estar vinculado concretamente a pessoas e coisas (BIRNBAUM *apud* HASSEMER, 2011. p.19). Para Claus Roxin, catedrático de Direito Penal da Universidade de Munique, e que também se aproxima daquele escólio, os bens jurídicos são *dados ou finalidades necessários para o livre desenvolvimento do indivíduo, para a realização de seus direitos fundamentais ou para o funcionamento estatal baseado nessas finalidades* (ROXIN, 2011, p. 186). Roxin considera que, além da vida, da liberdade, da propriedade, etc., também são bens jurídicos aqueles pertencentes à coletividade – como uma Justiça que funcione adequadamente, uma circulação idônea de moeda ou um meio ambiente saudável.

De um modo ou de outro, parece seguro afirmar que a introjeção da informação no campo do Direito sob a forma de bem jurídico-penal se mostra legítima a partir do momento em que a idoneidade dos dados confiados à tecnologia da informação se tornou também inexorável pressuposto para o desenvolvimento de *uma vida juridicamente segura* (ROXIN, 2011, p. 185) ante a vocação tecnológica da humanidade.

Além de a tutela da propriedade privada, da livre concorrência de mercado e dos interesses de Estado estar prevista na Carta Política, sobre a privacidade, é interessante destacar que a teoria constitucional assinala a pretensão de proteger o indivíduo contra dois ataques: *i)* a violação da intimidade e *ii)* a liberdade de se ter uma vida privada (SILVA 1998, 211). Hoje, o barateamento das tecnologias de armazenamento de dados é um dos catalisadores da chamada política de *interceptação estratégica*, entendida como o monitoramento massivo e indiscriminado dos cidadãos que vai desde seus hábitos consumeristas (através das operadoras de cartões de crédito) até suas comunicações privadas. Se antes um indivíduo era um potencial alvo de vigilância por razões profissionais ou evidências de envolvimentos criminosos, hoje a regra é monitorar e registrar randomicamente, para posterior refino das informações colecionadas (*ibid*, p 57) – embora o quê se fazer, exatamente com todo o conteúdo estocado permaneça a principal questão a ser respondida. De todo modo, o meio especializado reconhece que a internet – que deveria ser um espaço civil – tornou-se um ambiente militarizado (ASSANGE, 2013, p. 53).

O direito à privacidade é *erga omnes*. É ele que possui a faculdade de compelir as outras pessoas a respeitar determinadas situações da vida que dizem respeito somente a seu titular (FERRAZ JÚNIOR, 1993, p.77). No longínquo instante de promulgação da *Magna Charta Libertatum* (1215) já se reconhecia comumente a privacidade como um pilar indispensável para a coexistência pacífica entre cidadãos. O núcleo desse direito alude ao controle que o indivíduo possui sobre as que informações devam ou não vir a público, submetido única e discricionariamente à decisão daquele a quem pertencem (BRANCO, 2009, p. 422). Além disso, sublinhamos que a privacidade é um dos mais relevantes componentes de certas relações humanas – como o casamento (*ibidem*, p 421.). No campo dos

Direitos Humanos, já se afirmou que a locução *vida* privada inclui a proteção contra *ataques* à integridade física, e moral, à liberdade intelectual, contra o uso indevido do nome ou a imagem de alguém, contra a espionagem, *controle ou distúrbio da paz individual e contra a violação de atividades cobertas pelo segredo profissional* (ROLIN, 1973).

No epicentro do direito à privacidade habita a governança das informações que um indivíduo tem sobre si mesmo. A esse respeito anota Pierre Kayser que há dois ataques contra a informação: a divulgação e a investigação (KAYSER, 1984, p.11). Em linha parecida, nos Estados Unidos, William L. Prosser pontua que são quarto as formas de vilipendiar objetivamente a privacidade: i) intrusão na esfera do indivíduo; ii) a condução a público de fatos privados; iii) a exposição deturpada de alguém; e iv) a apropriação do nome ou imagem de alguém, principalmente com propósitos comerciais (PROSSER 1984, 107). A tese sobre a proteção da vida privada foi lançada em dezembro de 1890, através de um artigo veiculado na Harvard Law Review, no qual Brandeis e Warren defenderam que o indivíduo tem o direito de escapar do noticiário público para certas situações particulares. Mais tarde, a jurisprudência sucessivamente foi dilatando o escopo original do direito à privacidade até consagrá-lo como um instrumento de decisões subjetivas e um espaço de autonomia individual, livre da interferência inclusive de autoridades públicas (BRANCO, 2008).

Atualmente, seja no sistema *common law* seja no sistema *civil law*, o direito à privacidade é consagrado como um componente do determinante do círculo do indivíduo, e, ao lado do poder político e da lei, resulta na conexão entre o Estado, propriamente dito, e o sistema legal, formando o Estado de Direito (COSTA *et al*, 2006, p. 96).

3. Adequação semântico-dogmática de *crime informático*

A concepção de *crime informático* (ou *cibernético* ou, ainda, *digitais*), é genericamente abordada como *qualquer conduta ilegal, não ética ou não autorizada que envolva processamento automático de dados e/ou transmissão de dados* (OCDE). A doutrina é oscilante a esse respeito, em virtude de naquele conceito serem reunidas uma série de *condutas que em comum possuem apenas a circunstância de que são utilizados para sua prática sistemas de computador* (BOITEUX, 2010, pp. 953-954).

Na incipiente produção doutrinária dedicada ao tema, diversos autores compartilham da definição apresentada pela OCDE e pela da Convenção de Budapeste, admitindo como crime informático toda conduta criminosa associada ao uso de sistemas computadorizados. Nesse sentido, Luciana Boiteux leciona que a expressão *crimes informáticos* alude a todas as *condutas antissociais alçadas à condição de fatos típicos por decisão de política criminal, diante da constatação da sua gravidade e necessidade de interferência do direito penal* (BOITEUX, 2010, pp. 953-954). Para Ivette Senise Ferreira, trata-se de *toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão* (FERREIRA, 2000. p. 210). Na mesma linha segue Carla Rodrigues Araújo de Castro, para quem o crime de informática é aquele cometido através da internet, praticado contra sistema de informática ou através dele – compreendendo, pois, tanto os crimes praticados contra o computador e seus acessórios quanto aqueles cometidos através deste (*sic*) (CASTRO, 2003, pp. 9 e 31).

Também na plataforma defensora do crime informático como *aquele vinculado ao uso de computadores*, alguma doutrina afortunadamente propõe diferenciar as condutas que envolvam a informática como *meio* para a ação criminosa daquelas que nela têm seu próprio *fim*. Nessa linha militam Vicente Greco Filho (2000) e Marcelo Xavier de Freitas Crespo (2011) – que, inclusive, sugere uma categorização em *crimes digitais próprios* (meios eletrônicos como objeto protegido) e *crimes digitais impróprios* (meios eletrônicos como instrumento/meio para se lesionar outros bens jurídicos) (*idem, ibidem,* pp. 63 e ss). Em semelhante opinião caminha Augusto Eduardo de Souza Rossini, que aventa a divisão desses delitos em *puros* e *mistos* (ROSSINI, 2002) [4].

Marcelo Crespo chega a defender que, por exemplo, *a simples utilização de um computador para a perpetração de um delito como um estelionato não deveria ser (...) com precisão técnica, considerada um crime informático* (grifo nosso) (CRESPO, 2011, p. 63) – mas exclui de tal afirmação as hipóteses nas quais mecanismos são informaticamente criados com o fim de ludibriar a vítima e induzi-la a fornecer seus dados pessoais[5].

Respeitadas ao máximo todas as propostas acadêmicas dedicadas ao tema – e prefaciando qualquer manifestação dialética de nossa parte –, cabe salientar que *nem toda conduta maliciosa operada digitalmente representa um ataque à informação.* Em via oposta, que *nem toda afronta à informação ocorre pela via digital.*

É possível afirmar com segurança que, sobretudo em estudos não criminais, a expressão *crime* vem sendo utilizada de forma tecnicamente inócua. A primeira observação a ser feita é que chega-se ao ponto de indicar como *crime informático* (*cibernético* ou, ainda, *digitais*) condutas que sequer possuem tipificação no ordenamento jurídico. De igual maneira, é bastante evidente uma tendência de alcunhar como tais diversas condutas que não ameaçam a segurança da informação, enquanto bem jurídico.

Trata-se, em verdade, de *hostilidades informáticas* – expressão que não admite como sinônimo a locução *hostilidades digitais* ante a possibilidade de se atacar a informação por meios não lógicos, mas sim pela via física, como demonstraremos a seguir. Assim sendo, são espécies de hostilidades informáticas: i) *atividades maliciosas não incriminadas; ii) crimes informatizados* e; iii) *crimes informáticos.*

No Brasil, um exemplo da primeira categoria é o envio de *spams.* Embora definido em alguns países como crime, o envio em massa de mensagens não solicitadas permanece sem regulação no Direito Penal brasileiro – e, portanto, é evidente a atipicidade da conduta. No segundo grupo (crimes informatizados), inserimos o que são nada mais do que versões digitais de crimes já previstos, e que em momento algum são direcionadas contra a idoneidade da informação. É o que ocorre nos crimes contra a honra cometidos via internet – que, essencialmente, violam exatamente o mesmo bem jurídico: *a honra.* O bem jurídico da injúria praticada através de um computador é o mesmo daquele violado por uma injúria cometida presencialmente: a honra da vítima. O mesmo ocorre com os chamados *crimes de ódio*, consistentes em afirmações ou instigações a favor da discriminação étnica, religiosa, social ou em virtude da opção sexual. É jurídico-penalmente irrelevante, postar um comentário racista em um grupo de discussão ou colar um adesivo com o mesmo conteúdo em local de acesso público, razão pela qual não se trata de um crime informático, mas sim a versão digital de uma conduta já incriminada na maioria nos Estados democráticos contemporâneos. É estritamente uma questão de *modus operandi.*

Da mesma forma, alertamos que também a circulação de material pedopornográfico na rede, a rigor, não atinge a segurança da informação – a dizê-la como bem jurídico –, mas sim a incolumidade da criança e do adolescente – razão pela qual é combatida, no Brasil, pelo Estatuto da Criança e do Adolescente, diploma específico que internalizou a Convenção Internacional sobre os Direitos da Criança (1990). É, incontestavelmente, uma prática reprovável, que merece ser (e é) inibida e penalmente sancionada, mas que não caracteriza, com precisão técnica, um *crime informático*, sob pena de se esvaziar o princípio da lesividade e o princípio da proteção de bens jurídicos.

Por fim, as condutas substancialmente dignas de serem indicadas como crimes informáticos são aquelas direcionadas contra os princípios basilares da Segurança da Informação – ou seja, são aquelas que afrontam sua autenticidade, integridade, confidencialidade, disponibilidade e seu não repúdio. O princípio da autenticidade é o que assegura que os dados acessados sejam verídicos e de que o usuário seja legítimo. Já o princípio da integridade remete à proteção da informação contra modificações sem a permissão de seu titular. A confidencialidade, por sua vez, se traduz na garantia de que a informação não será acessada por pessoal não autorizado, enquanto a disponibilidade consiste na segurança de que a informação estará disponível quando for acessada. Por fim, o não repúdio da informação é o que garante a irretratabilidade sobre a autoria de uma atividade.

Nessa esteira, considerada a gama de peculiaridades inerentes a tão complexo tema, cremos que uma definição precisa de delito informático seja a *conduta legalmente definida como criminosa que atente física ou logicamente contra a integridade, a confidencialidade, a autenticidade, a disponibilidade ou o não repúdio da informação, ou, ainda, contra o correto funcionamento das ferramentas físicas ou lógicas* [6] *responsáveis pelo processamento, armazenamento e transmissão de dados.*

Naturalmente, não se exclui a possibilidade de uma tal conduta ser subsumida por mais de um tipo penal, afetando, ao mesmo tempo, a informática e outros bens jurídicos (conhecida hipótese do concurso formal de crimes) – posicionamento compartilhado por Carlos Romeo Casabona e Francisco Bueno Arús, na Espanha. Se, todavia, persiste a intenção de combater condutas que se limitam a atacar por meio da informática, uma alternativa ao aumento do catálogo incriminador que é aparentemente viável seria a criação de circunstâncias qualificadoras que tragam, no tipo penal correspondente, o elemento do emprego de alta tecnologia. Ou, ainda, considerada a extensa gama de possíveis delitos passíveis de cometimento com o uso da informática, poderia ser criada uma causa genérica de aumento de pena (no caso brasileiro, a ser inserida no artigo 61 da Parte Geral do Código Penal). Assim, o agente que viesse a cometer um crime contra a honra através da rede, teria sua pena aumentada em razão do emprego de alta tecnologia.

5. Considerações Finais

Malgrado a patente carência normativa no âmbito da tecnologia da informação – que hoje praticamente define os contornos da comunidade internacional –, a opção regulatória pela via da disciplina penal deve prestigiar seus princípios regentes a fim de que a tutela da segurança da informação não usurpe a noção da intervenção mínima, o que seria rasurar a identidade de *ultima ratio* do Direito Penal. Para isso, a identificação e a delimitação do quê, factualmente, se pretende proteger, é condição indispensável para o traçado de tipos penais precisos e congruentes com o Estado de Direito, permitindo à política criminal emergente no assunto adquirir aptidão para prover segurança ao desenvolvimento social-tecnológico com eficiência e credibilidade dogmática. A questão é, a todo momento, sabatinada em funis conceituais, pelo que é indispensável primar pela tecnicidade sistemática de modo que não se valha de forma leviana da expressão *crime* e não se corrompa toda a teoria do delito.

Por fim – e talvez ainda mais importante –, é também inevitável a conclusão de que a proteger a informação enquanto bem jurídico significa, além da pretensão de conter a criminalidade comum, projetar no ciberespaço a eficácia horizontal e vertical dos direitos e garantias fundamentais como modo de limitar a entrada do poder do Estado na esfera do infranqueável.

Referências

AMELUNG, Knut. O conceito de bem jurídico na teoria jurídico-penal na proteção de bens jurídicos. In: O Bem Jurídico como Limitação do Poder Estatal de Incriminar? Coord. GRECO, Luís; TÓRTIMA, Fernanda Lara. pp.117-158. Rio de Janeiro: Lumen Juris, 2011.

A Primer on Information Theory and Privacy. Por Peter Eckersley. Publicado em 26.01.2010. Disponível em: <https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy>. Acesso em: 22.08.2012.

BITENCOURT, Cezar Roberto. Manual de Direito Penal – Parte Geral. Vol.1. São Paulo: Saraiva, 2000.

BOITEUX, Luciana. Crimes Informáticos: Reflexões sobre Política Criminal. In: Doutrinas Especiais – Direito Penal. Coord. FRANCO, Alberto Silva; NUCCI, Guilherme de Souza. Vol. VIII. São Paulo: RT, 2010. pp. 953-954. Disponível também em: RBCCrim 47/2004. mar.abr./2004.

BRANDEIS, Louis D.; WARREN, Samuel D. The Right to Privacy. *In:* Harvard Law School. Vol. 04. Dec. 15. The Harvard Law Review Association: 1890.Disponível em: <http://www.jstor.org/stable/1321160 >. Acesso em: 01.03.2014.
CASABONA, Carlos María Romeo. La protección penal de los mensajes de correo electrónico. In: Doutrinas Especiais – Direito Penal. Coord. FRANCO, Alberto Silva; NUCCI, Guilherme de Souza. Vol. VIII. São Paulo: RT, 2010. Disponível também em: RBCCrim 55/2005. jul.ago/2005.
CASTRO, Carla Rodrigues Araújo de. Crimes de Informática e seus aspectos processuais. 2ª Ed. Rio de Janeiro: Lumen Juris, 2003. pp. 9 e 31.
CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. 2ª Ed. São Paulo: Saraiva, 2011.
DRUCKER, Peter. Administrando para o Futuro. 2ª Ed. São Paulo: Pioneira, 1992.
FERRAJOLI, Luigi. Por uma Teoria dos Direitos e dos Bens Fundamentais. Porto Alegre: Livraria do Advogado, 2011.
FERREIRA, Ivete Senise. Os crimes de informática. In: Estudos jurídicos em homenagem a Manoel Pedro Pimentel. BARRA, Rubens Prestes; ANDREUCCI, Ricardo Antunes. São Paulo: Revista dos Tribunais, 1992. n.9. p.139-162.
HASSEMER, Winfried. Linhas Gerais de uma Teoria do Bem Jurídico. In: O Bem Jurídico como Limitação do Poder Estatal de Incriminar? Coord. GRECO, Luís; TÓRTIMA, Fernanda Lara. pp.15-56. Rio de Janeiro: Lumen Juris, 2011.
HEFENDEHL, Roland. Linhas Gerais de uma Teoria do Bem Jurídico. In: O Bem Jurídico como Limitação do Poder Estatal de Incriminar? Coord. GRECO, Luís; TÓRTIMA, Fernanda Lara. pp. 57-75 Rio de Janeiro: Lumen Juris, 2011.
MORAES, João Antônio de. Cliques de Vigilância. In: Filosofia. Ano VI – Edição 81. Pp. 14-23. São Paulo: abr. 2013.
NETO, Mário Furlaneto; GUIMARÃES, José Augusto Chaves. Direito da Informática. Crimes na Internet: elementos para uma reflexão sobre a ética informacional. In: Revista CEJ, n. 20. pp. 67-73Brasília, jan.-mar. 2003. p. 69, apud BARROS, marcos de; GARBOSSA, Daniella; CONTE, Christiany. Crimes Informáticos e a Proposição Legislativa. In: Doutrinas Especiais - Direito Penal. pp. 981-1027. Coord. FRANCO, Alberto Silva; NUCCI, Guilherme de Souza. Vol. III. São Paulo: RT, 2010.
PECK, Patrícia; SLEIMAN, Cristina. Direito Digital: Gestão do Risco Eletrônico. USP. Disponível em:<http://www.security.usp.br/palestras/%7B91AB0DB1-D373-4167-A317-847267D6BDD%7D_USP__palestra_PPP_cms_V1_091106_final.pdf>. Acesso em: 03.10.2012.
PRADO, Luiz Regis. Bem jurídico penal e Constituição. São Paulo: Revista dos Tribunais, 1997
RODOTÀ, Stefano. La Vida y las Reglas: entre el derecho y el no derecho. Trad. Andrea Greppi. Prólogo de José Luís Píñas Mañas. Espanha: Editorial Trotta.
RODRÍGUEZ, Luiz Ramón Ruiz; AGUDELO, Gloria González. *El Factor Tecnologico em La Expansión Del Crimen Organizado.* Centro de Investigacíon Interdisciplinaria en Derecho Penal Económico. Disponível em: <http://www.ciidpe.com.ar/area3/FACTOR_TECONOLOGICO_EN_CRIMEN_ORGANIZADO._RUIZ_Y_GONZALEZ.pdf>. Acesso em: 19.11.2011.
ROSSINI, Augusto Eduardo de Souza. Condutas Ilícitas na Sociedade Digital. In: Caderno Jurídico: Escola Superior do Ministério Público de São Paulo. Imprensa Oficial do Estado de São Paulo, ano 2, jul. 2002, pp. 131-142.
ROLIN, Henry. Conclusions in Privacy and Human Rights. Manchester: 1973.
ROXIN, Claus. Sobre o Recente Debate em Torno do Bem Jurídico. In: O Bem Jurídico como Limitação do Poder Estatal de Incriminar? Coord. GRECO, Luís; TÓRTIMA, Fernanda Lara. pp.15-56. Rio de Janeiro: Lumen Juris, 2011.
_____. Política Criminal y Sistema del Derecho Penal. Traducción y Introducción de Francisco Muñoz Conde. 2ª Ed. Colección Claves del Derecho Penal. Vol. 2. Buenos Aires: Hammurabi, 2002.
SETZER, Valdemar W. Dado, Informação, Conhecimento e Competência. Disponível em: <http://www.ime.usp.br/~vwsetzer/dado-info-Folha.html>. Acesso em; 05.02.2013.
SIANES, Marta. Proteção do Conhecimento na Sociedade da Informação. VII Encontro Nacional de Estudos Estratégicos. Agência Brasileira de Inteligência. Disponível em: < https://sistema.planalto.gov.br/siseventos/viienee/exec/arquivos/ANAISVIIENEE_INTERNET/01SEGURANCAEDEFESA/MESA14SEGURANCANOVASDIMENSOES/MESA14APRESENTACOES/MartaSianesProtConhSocInformacao.pdf>. Acesso em: 02.jan.2013.
SILVA SÁNCHEZ, Jesús María. La expansión del Derecho Penal: Aspectos de la Política criminal en las sociedades postindustriales. Madrid: Edisofer, 2011.
SOLOVE, Daniel J.; ROTEMBERG, Marc; SCHWARTZ, Paul M.. Information privacy law. 2. Ed. Aspen Publishers: Nova York, 2006.
TAVARES, Juarez. Teoria do Crime Culposo. 3ª Ed. Prefácio ROXIN, Claus. Rio de Janeiro: Lúmen Júris, 2009.
VICO, Giambattista. *Os Pensadores. Seleção*, tradução e notas de Antônio Lázaro de Almeida Prado. São Paulo: Abril, 1974.
ZANELLATO, Marco Antônio. *Brevíssimas considerações sobre delitos informáticos. In:* Caderno Jurídico. São Paulo: Escola Superior do Ministério Público de São Paulo. pp. 164-228. Imprensa Oficial do Estado de São Paulo, ano 2, n.4, jul.2002. p. 167.

[1] Expressão emprestada de Marcelo Xavier de Freitas Crespo.

[2] Citando o grego Nicos Poulantzas (1975), Juarez assevera que a atividade humana é condensada no interesse – que, por sua vez, é dependente das estruturas social, econômica, política, ideológica e jurídica (TAVARES, 2009, p. 236). Ocorre que hoje, na vigência do modelo capitalista, muitas vezes essas estruturas estão desvinculadas umas das outras, fazendo com que seus respectivos interesses caminhem em descompasso (*ibidem*) – daí a importância de se entender o bem jurídico como um *instrumento adequado do processo de comunicação que se destina a determinar as zonas do lícito e do ilícito* (*ibidem*, p. 234).

[3] Nesse sentido, Claus Roxin, Alessandro Barata, Pavarini e Andrade.

[4] Há, ainda, o posicionamento de que haveria os chamados crimes informáticos *comuns*, entendidos como todos aqueles em que, embora não seja a informática o bem jurídico tutelado, a Internet é condição sem a qual a conduta criminosa não se efetiva. O exemplo dado é a transferência ilícita de valores em uma *home banking*, isto é, transações financeiras e bancárias efetuadas a partir da residência ou do escritório através da Internet (NETO & GUIMARÃES *apud* BARROS *et all*, 2010).

[5] Por exemplo, o que ocorre com emprego de *phishing* e *web spoofing* (páginas simuladas).

[6] Para *ferramentas físicas e lógicas*, nos referimos, respectivamente, a *hardwares* e *softwares.*