A questão penal no marco civil

Vladimir Aras[1]

Sumário: 1. Introdução. 2. Falsa dicotomia: lei penal versus marco civil. 3. A proteção do marco civil depende do regulamento penal. 3.1. A guarda e fornecimento de registros de conexão e de acesso. 4. A necessidade do tratamento conjunto e uniforme para os aspectos civis e penais das relações ciberespaciais. 5. Conclusão. Referências

Resumo: este artigo examina aspectos penais e processuais penais que derivam do Projeto de Lei 2126/2011, do Marco Civil da Internet no Brasil. O autor procura demonstrar que o melhor caminho para a regulamentação do ciberespaço no País é a adoção de legislação abrangente, que proteja os direitos dos usuários da Internet, especialmente a liberdade de expressão e a privacidade, e tipifique os crimes informáticos próprios, que pretendem tutelar os bens jurídicos fundamentais da sociedade da informação.

Palavras-chave: marco civil – ciberdireitos – cibercrimes – ciberespaço – legislação – Brasil

Introdução

Ninguém pode negar o esforço do Congresso Nacional para aprovar uma legislação sobre internet no Brasil. Os primeiros projetos de lei para tipificar crimes de informática, próprios e impróprios, remontam aos anos 1990. O mais importante deles, o projeto Piauhylino Filho (PL 84/1999), ainda está atravancado no Poder Legislativo federal[2], desde que suas inúmeras falhas foram reveladas por especialistas em ciberdireitos e em ciberciminalidade.

Embora a aprovação de uma legislação penal seja necessária, o PL 84/99 – agora apelidado de Lei Azeredo ou, exageradamente, de "AI-5 Digital" – precisa de muitas alterações para começar a ficar bom. Falei sobre isto neste artigo aqui[3] e apontei, item a item, os vários erros do projeto de lei dos cibercrimes.

Para estabelecer um contraponto ao projeto Azeredo, entidades da sociedade, ongs e ciberativistas passaram a insistir na necessidade de, primeiro, aprovar-se um "Marco Civil da Internet no Brasil". Seria algo com um Estatuto do Internauta, uma lei brasileira para regulamentar os ciberdireitos, os direitos da era da informação.

O Poder Executivo acaba de enviar ao Congresso Nacional o PL 2126/2011, que "*estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil*". O texto, muito bem trabalhado, positiva importantes princípios, como a proteção à privacidade e aos dados pessoais, à liberdade de expressão, comunicação e manifestação do pensamento. A iniciativa é fruto da cooperação entre a Secretaria de Assuntos Legislativos do Ministério da Justiça – SAL/MJ e o Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getúlio Vargas do Rio de Janeiro[4] e teve como base os "Princípios para a governança e uso da Internet"[5].

O PL 2126/20011 tem quatro eixos: cuida dos direitos dos usuários (entre eles a privacidade e a liberdade), da responsabilização pelo conteúdo disponibilizado; da guarda de dados de conexão e acesso e seu fornecimento; e do problema da neutralidade da Internet[6].

2. Falsa dicotomia: lei penal versus marco civil

Quero discutir os aspectos penais do marco civil, que se relacionam com três dos quatro eixos antes apontados, com a exceção do tema da neutralidade da rede. Embora se diga que o projeto não tem efeitos sobre as atividades de persecução penal, isto não é verdade. O debate em torno da regulamentação do ciberespaço no Brasil perdeu-se numa dicotomia ou falso choque entre temas penais e matéria cível, entre os "repressores" e os "libertários". Parece que voltamos ao alvorecer da Internet no Brasil quando se temia o Grande Irmão[7] e se dizia que o espaço virtual era uma terra sem leis[8].

Na verdade, já somos "grandinhos" e deixamos de acreditar em fantasmas. O Brasil é um Estado democrático de Direito; não é uma China e ninguém tolerará abusos do Estado contra as liberdades públicas na

---

1 Vladimir Aras, 40 anos, é mestre em Direito Público pela Universidade Federal de Pernambuco (UFPE), professor assistente de processo penal na Universidade Federal da Bahia (UFBA) e no Centro Universitário Jorge Amado (Unijorge), procurador da República na Bahia (MPF/BA), especializado em reforma processual penal latinoamericana pelo *Centro de Estudios de Justicia de las Americas* (CEJAS), associado ao Instituto Brasileiro de Ciências Criminais (IBCCrim), membro da *International Association of Prosecutors* (IAP), professor da Escola Superior do Ministério Público da União (ESMPU), instrutor do Programa Nacional de Capacitação em Combate à Lavagem de Dinheiro (PNLD/MJ), membro do Grupo de Trabalho em Lavagem de Ativos da Procuradoria Geral da República (GT-LD), é um dos representantes do MPF na Estratégia Nacional de Prevenção e Combate à Corrupção e à Lavagem de Ativos (ENCCLA), foi promotor de Justiça na Bahia (MP/BA) e edita o Blog do Vlad: www.blogdovladimir.wordpress.com. Email: vladimiraras@hotmail.com.

2 Foi aprovado na Câmara dos Deputados em novembro de 2003 e atualmente aguarda apreciação pelo Senado.

3 ARAS, Vladimir. O projeto de lei dos cibercrimes (PLS 76/2000): crítica ao substitutivo aprovado no Senado. Revista On-line ANPR, n. 8, Brasília, janeiro/junho de 2009. Disponível em: http://blogdovladimir.files.wordpress.com/2010/01/artigo_projeto-de-lei-dos-cibercrimes-pls-76-de-2000.pdf.

4 BRASIL. Ministério da Justiça. Marco civil da Internet: seus direitos e deveres em discussão. Disponível em: http://culturadigital.br/marcocivil/

5 Resolução CGI.br/RES/2009/003/P.

6 Para evitar o chamado *traffic shaping*, manipulação dos pacotes de dados, a critério dos provedores.

7 A referência é ao Big Brother, de George Orwell, do livro "1984".

8 ARAS, Vladimir. Crimes de informática: uma nova criminalidade. Jus Navigandi, Teresina, ano 5, n. 51, out. 2001. Disponível em: http://jus.uol.com.br/revista/texto/2250/crimes-de-informatica

Internet ou onde quer que seja! Eis aí a falsa dicotomia entre o suposto “mundo virtual” e o “mundo real” contaminando o debate. A liberdade que “do lado de fora” do ciberespaço já exercemos é a mesma liberdade que “do lado de dentro” também já temos. Se vez ou outra ocorre censura indevida a sites da Internet, há também repudiável censura a jornais impressos e até a filmes. Há uma só ambiência (e não duas) e uma ambivalência. “Real” e “virtual” se confundem numa coisa só. E todas as ferramentas deste mundo único são ambivalentes, como a própria Internet, onde coexistem usos legítimos e ilegítimos.

Onde o homem estiver, aí deve estar o Direito (*ubi societas ibi jus*). A inexistência de legislação penal clara ameaça os ciberdireitos, porque, não havendo normas específicas para a Internet, a Justiça criminal tende a lançar mão da legislação comum – “analógica” por assim dizer, pois dos anos 1940 –, em lugar de utilizar leis talhadas e pensadas para a era digital. Se o ciberespaço é um ambiente para produção e difusão do conhecimento, para o desenvolvimento científico, educacional e econômico e para a interação entre os povos, é também, por sua própria ambivalência, uma cena de crime.

Então, deixemos de lado qualquer discurso que pareça demagógico ou que seja, no mínimo, incoerente. A regulação dos direitos cibernéticos é essencial, mas não podemos prescindir dos ciberdeveres, das restrições a condutas indevidas, da prevenção e repúdio a esses usos ilegítimos que vulneram direitos fundamentais de outros usuários da Internet.

A Europa em peso, ao lado dos Estados Unidos, segue uma dupla via: prevê os direitos do ciberespaço, especialmente a liberdade e a privacidade, e procura estabelecer, também neste cenário de intereação humana, um ambiente de segurança e justiça. Não por outro motivo dezenas de democracias ratificaram a Convenção sobre Cibercriminalidade (Budapeste, 2001), já em vigor internacional[9].

A Convenção de Budapeste, também conhecida como CETS 185, estabelece para os Estados-Parte o dever de criminalizar certas condutas deletérias aos bens jurídicos da era da informação, procura proteger crianças e os direitos de autor na Internet e, no seu protocolo adicional, cuida da discriminação na Internet, por meio do racismo e da xenofobia. Além disso, estabelece a necessidade de regular os mecanismos probatórios e de preservação dos dados de conexão, para fins processuais penais.

3. A proteção do marco civil depende do regulamento penal

As questões cíveis e criminais em matéria de garantia de direitos e tutela de bens jurídicos são tão imbricadas que não foi possível, no projeto do Marco Civil da Internet, evitar dispositivos que têm claro interesse penal e processual penal. Para começar, o artigo 2º, inciso II, do PL 2126/2011 pretende tutelar os direitos humanos nos meios digitais, o que implica a necessidade de proteção de direitos constitucionais de vítimas de cibercrimes.

Ao prever no inciso V do artigo 3º como princípio fundante do estatuto a preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais, o projeto aponta alguns dos mais importantes bens jurídicos da sociedade da informação, o que reclama, queiramos ou não, a adoção de tipos penais informáticos (puros ou próprios, os chamados *computer crimes*) para assegurar estes propósitos de segurança, funcionalidade e estabilidade, diante, por exemplo, de ciberataques, distribuição de vírus ou destruição de infraestruturas de suporte da rede. Como garantir a segurança da rede com mera retórica e sem a função de intimidação da norma penal?

A ideia da prevenção e da punição por meio da lei penal é reforçada pelo inciso VI do mesmo artigo 3º do marco civil, que pretende assegurar a “*a responsabilização dos agentes de acordo com suas atividades, nos termos da lei*”. Não é possível neste contexto, por mais refratários que sejamos a controles estatais, prescindir de uma das espécies de responsabilização, a criminal. Lamentavelmente, como o PL do marco civil não se ocupou do tema, deixou a porta aberta para que o projeto Azeredo, tão criticado (justa e injustamente), continue sendo a única alternativa imediata para a regulamentação dos crimes propriamente informáticos (os “puros”).

Enunciar o “*direito de acesso à Internet a todos os cidadãos*” é uma válida preocupação do projeto. Mas, na minha visão, não se pode proteger devidamente esse direito se não houver tipos penais apropriados para fazer frente a ameaças digitais, que hoje são atípicas e, portanto, impuníveis. Muitos usos ilegítimos da rede são voltados exatamente para impedir ou dificultar o acesso à Internet e deveriam ser criminalizados, com sanções proporcionais. É o caso dos ataques de negação de serviço (*denial of service*) e da disseminação de vírus.

9 Em ago/2011, os Estados Unidos e 30 países europeus ratificaram a Convenção de Budapeste (CETS 185). O Canadá, a África do Sul e o Japão já assinaram o texto, mas ainda não o ratificaram. Argentina, Chile, Costa Rica, México e República Dominicana já manifestaram interesse oficial de tornarem-se partes do tratado (aqui). O Brasil resiste. O nó górdio está na questão da tutela penal dos direitos de autor.

Há outros vínculos entre a regulação civil e a persecução criminal na Internet. No artigo 7º do PL, assegura-se ao usuário de Internet a "*inviolabilidade e ao sigilo de suas comunicações pela Internet, salvo por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal*". Esta garantia deriva do artigo 5º, inciso XII, da Constituição Federal e não é nenhuma novidade, já que o tema é objeto da Lei 9.296/96, com a mesmíssima disciplina, que cuida da interceptação de comunicações telefônicas e telemáticas. Com isto, o projeto do marco civil age com acerto ao legitimar essa técnica especial de investigação criminal.

Uma falha normativa resulta do inciso II do artigo 7º do projeto, que prevê o direito à não suspensão da conexão à Internet, salvo por débito diretamente decorrente de sua utilização. Os autores do projeto não se esqueceram de tutelar os direitos patrimoniais dos provedores (na relação de consumo), mas olvidaram que, num contexto criminal, um juiz pode, legitimamente, para fins cautelares, determinar a suspensão de uma conexão à Internet[10] para evitar que uma determinada conduta ilícita prossiga. Cito como exemplo a previsão do artigo 20, §3º, da Lei 7.716/89[11], segundo o qual, nos crimes de racismo e apologia ao nazifascismo cometidos por intermédio dos meios de comunicação social, inclusive a Internet, o juiz pode determinar, a pedido do Ministério Público ou com sua oitiva, "*a interdição de páginas de informação na rede mundial de computadores*" ou "*interdição das mensagens*" (sic), o que pode ser interpretado como restrição de acesso àquelas e proibição do envio destas. Ademais, no exercício do seu poder geral de cautela, pode o juiz determinar a suspensão de qualquer conexão à rede. Porém, sem um regulamento criminal claro sobre o tema, corre-se o risco de abusos contra a liberdade de acesso à rede e de seu uso.

De igual modo, com a aprovação da Lei 12.403/2011, que alterou o Código de Processo Penal, agora são possíveis outras medidas cautelares relacionadas à Internet, como, por exemplo, as do artigo 319, incisos I e II, do CPP, de proibição de acesso ou frequência a determinados lugares quando, por circunstâncias relacionadas ao fato, deva o indiciado ou acusado permanecer distante desses locais para evitar o risco de novas infrações[12]; e de proibição de manter contato com pessoa determinada quando, por circunstâncias relacionadas ao fato, deva o indiciado ou acusado dela permanecer distante[13]. Nos crimes informáticos, próprios ou impróprios, e especialmente nos casos de ciberpedofilia, tais cautelares serão tão mais eficientes quanto mais se possa limitar judicialmente o acesso do agressor a dispositivos conectados ou conectáveis.

3.1. A guarda e fornecimento de registros de conexão e de acesso

Os registros de conexão à Internet e as anotações sobre acesso a aplicações de Internet são fundamentais para o rastreamento de atividades criminosas e para a determinação de autoria.

O inciso V do artigo 7º do projeto do marco civil veda o fornecimento a terceiros dos registros de conexão[14] e dos registros de acesso a aplicações de Internet[15], salvo mediante consentimento ou nas hipóteses previstas em lei. Os registros de conexão são o "*conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados*", ao passo que os "registros de acesso a aplicações de Internet" correspondem ao "*conjunto de informações referentes à data e hora de uso de uma determinada aplicação de Internet a partir de um determinado endereço IP*".

Embora tais registros de conexão à Internet não digam respeito diretamente ao conteúdo do tráfego ou da comunicação, o PL do marco civil os trata como se fossem dados sensíveis *tout court*. Mal comparando, tais informações técnicas, correspondem em geral, no que tange a telefones, aos registros de chamadas originadas e

---

10 Segundo o artigo 5º, inciso V, do PL 2126/2011, "conexão à Internet" é a "habilitação de um terminal para envio e recebimento de pacotes de dados pela Internet, mediante a atribuição ou autenticação de um endereço IP".

11 Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. Pena: reclusão de um a três anos e multa. §1º Fabricar, comercializar, distribuir ou veicular símbolos, emblemas, ornamentos, distintivos ou propaganda que utilizem a cruz suástica ou gamada, para fins de divulgação do nazismo. Pena: reclusão de dois a cinco anos e multa. §2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza: Pena: reclusão de dois a cinco anos e multa. §3º No caso do parágrafo anterior, o juiz poderá determinar, ouvido o Ministério Público ou a pedido deste, ainda antes do inquérito policial, sob pena de desobediência: I - o recolhimento imediato ou a busca e apreensão dos exemplares do material respectivo; II - a cessação das respectivas transmissões radiofônicas ou televisivas. III - a interdição das respectivas mensagens ou páginas de informação na rede mundial de computadores.

12 Por "lugares", pode-se entender uma lan house, um local que disponilize acesso wi-fi ou um centro informático.

13 Inclusive a proibição de manter contato, por meio da Internet, por emails ou comunicadores instantâneos.

14 Segundo o artigo 5º, inciso VI, do projeto do marco vivil, "registro de conexão" é o conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados".

15 Conforme o artigo 5º, inciso VII, do projeto "aplicações de Internet" correspondem ao conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet".

recebidas, à sua duração, data, horário e valor. Não se revela, com o fornecimento de tais dados, nenhuma informação sobre o diálogo em si mesmo (a "conversa").

Uns consideram essencial autorização judicial para o fornecimento de tais registros; outros crêem que a Polícia e o Ministério Público podem requisitar diretamente tais dados aos provedores, no curso de uma investigação criminal. Para o *Parquet*, há previsão expressa na Lei Complementar 75/93 sobre a requisição de informações, ainda que sigilosas, a órgãos públicos e entes privados[16]. O projeto optou claramente pela primeira solução, ao determinar que "*o provedor responsável pela guarda somente será obrigado a disponibilizar as informações que permitam a identificação do usuário mediante ordem judicial*" (artigo 10, §1º), o que abrange até mesmo singelos dados cadastrais, não incluídos na cláusula constitucional de reserva de jurisdição, prevista no artigo 5º, inciso XII, da CF.

Como se percebe, está em jogo o direito à privacidade, cuja garantia é objeto do artigo 8º do projeto, como condição para o pleno exercício do direito de acesso à Internet. Obviamente, nenhuma garantia é absoluta e a própria Constituição e as leis permitem sua flexibilização quando em jogo interesses sociais mais relevantes ou quando ameaçado ou lesado o interesse público. Esta tensão fica muito clara no exame das práticas pedófilas pela Internet, a exemplo do *grooming*. O pedófilo tem direito à sua privacidade, mas não pode valer-se dele para impedir a Polícia e o Ministério Público de obter seus dados pessoais, seus logs e até o conteúdo de emails e mensagens instantâneas, quando relacionadas à prática de um crime.

Mais adiante, ao cuidar do tráfego de dados, o PL novamente tangencia a questão processual penal, o que, como vimos, é inevitável. O parágrafo único do artigo 9º do projeto proíbe os responsáveis pelo tráfego de "*monitorar, analisar ou fiscalizar*" o conteúdo dos pacotes de dados, mas ressalva "*as hipóteses permitidas em lei*", entre as quais, evidentemente, está a investigação criminal, nos termos da Lei 9.296/96, que regulamenta a interceptação de comunicações telefônicas e telemáticas.

O tema da guarda de registros é ainda mais problemático. Corretamente, o projeto diferencia a guarda de registro de conexões (objeto do artigo 11) da guarda do registro de acesso a aplicações de Internet (objeto do artigo 12). Já nas discussões da Lei Azeredo, foram enormes as controvérsias sobre o período de manutenção dos *logs,* tarefa que é custosa para provedores e operadores da Internet, e vital para a investigação criminal. O artigo 11 do projeto diz que esse prazo será de um ano, o que pode ser insuficiente para a apuração de crimes graves, porque nem sempre a verificação policial se inicia imediatamente após a prática do delito. Felizmente, o §2º do artigo 11 do PL permite que a autoridade policial ou administrativa[17] "requeira cautelarmente" a guarda de registros de conexão por prazo superior a um ano.

A Polícia e o Ministério Público notificarão o mantenedor dos dados sobre a necessidade de sua preservação. Ao referir-se a "requerimento", o projeto parece indicar a necessidade de judicialização deste procedimento, o que de fato se confirma com a leitura do §3º do mesmo artigo. A Polícia e o Ministério Público poderão requisitar (a proposta utiliza o verbo "requerer") aos provedores a preservação pré-cautelar dos *logs*. A partir daí, esses órgãos de persecução terão 60 dias para requerer em juízo o acesso aos dados de conexão. Esgotado esse prazo sem que advenha alvará judicial autorizativo, o provedor guardião dos registros estará exonerado do dever de guarda.

Segundo o artigo 10 do projeto, a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet deve atender à preservação da intimidade, vida privada, honra e imagem das partes direta ou indiretamente envolvidas. Conforme o artigo 11, os registros de conexão deverão ser preservados em sigilo, em ambiente "controlado e de segurança". Trata-se de um dever de sigilo para os responsáveis pela operação e funcionamento da rede mundial. Curiosamente, o marco civil cedeu às contingências e no artigo 10, §3º, prevê a responsabilização administrativa, civil e criminal para os casos de violação de sigilo, o que revela o contrassenso que é tentar tratar dos direitos (civis) sem considerar os deveres de ação e abstenção, impostos pelas normas penais. Embora estabelece os deveres de sigilo, controle e segurança, paradoxalmente, o PL deixa sem punição aquele que violar a segurança dessas bases de dados ou destruí-las. É que, sem regras penais específicas, essas condutas continuarão atípicas.

---

16 Artigo 8º, incisos II e IV, c/c o §2º, da Lei Complementar 75/93 (LOMPU).

17 Em tema criminal, esta "autoridade administrativa" só pode ser o Ministério Público. Mas, por não dizê-lo expressamente, o projeto abre a porta para que outros entes, como a Receita Federal, a Fazenda Nacional, a Advocacia-Geral da União e órgãos correlatos façam pedidos de preservação para fins não penais.

Para o acesso aos dados, a parte interessada (o Ministério Público, a Defensoria ou um advogado constituído) fará petição ao juiz criminal ou cível competente, para que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de Internet. O pedido só será deferido se houver fundados indícios da ocorrência do ilícito, justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e a indicação do período ao qual se referem os registros. O processo poderá tramitar em sigilo judicial.

Quanto aos registros de acesso a aplicações de Internet[18], o projeto é compreensivelmente mais restritivo. A regra é proibir os *provedores de conexão* de guardar tais registros (artigo 12), porque esses *logs* podem revelar preferências pessoas, hábitos de consumo, atividades sócio-econômicas e culturais, opções e propensões individuais, relacionadas à vida privada.

Porém, os *provedores das próprias aplicações de Internet* poderão[19] manter arquivados os registros de acesso aos serviços que fornecem, consoante o artigo 13 do PL. Mas o projeto condiciona o acesso a esses dados a expressa autorização judicial, circunscrita às hipóteses de investigação criminal, na forma do artigo 7º, inciso I, do PL. Para isto, a proposta legislativa determina que os provedores das aplicações gravem os *logs* de acesso às aplicações on-line assim que receberem determinação do juiz criminal competente. O correto seria obrigar esses provedores de aplicações a registrar obrigatoriamente[20] os dados de acesso a essas funções, devido à importância de tais informações para certas investigações criminais.

A ordem judicial deverá indicar o prazo de guarda dos registros de acesso às aplicações de Internet, desde que se tratem de registros relativos a fatos específicos em período determinado, e apenas se houver justa causa, na forma do artigo 17 do projeto, que prevê o procedimento geral para flexibilização do sigilo de dados informáticos, inclusive para fins criminais.

Também foi prevista a tutela pré-cautelar do interesse persecutório, pois se permite a preservação dos registros de acesso às aplicações de Internet, mediante simples requisição da Polícia ou do Ministério Público, devendo os órgãos de persecução providenciar a decisão judicial confirmatória no prazo de 60 dias, consoante o disposto no artigo 11, §§3º e 4º, do projeto, para só então obterem os dados já preservados pelo provedor.

4. A necessidade do tratamento conjunto e uniforme para os aspectos civis e penais das relações ciberespaciais

Como vimos, o discurso que sustenta a importante iniciativa materializada no PL 2126/2011 aparentemente pretendeu excluir da discussão os temas da cibercriminalidade. Não logrou êxito neste propósito.

O texto do marco civil está entremeado de vários temas de direito penal e processual penal. É preciso cuidar das regulações civis e penais num só estatuto. Sinal disto está na própria justificativa do projeto do marco civil, que aponta riscos para o caso de "*aprovação desarticulada de propostas normativas especializadas, que gerem divergência e prejudiquem um tratamento harmônico da matéria*"[21]. Entretanto, é exatamente isto o que ocorrerá (ou continuará a ocorrer) se não houver a adoção concomitante de normas protetivas de direitos fundamentais (os ciberdireitos) e regras de direito penal para tipificação proporcional e responsável dos crimes de informática próprios (os ciberdeveres de ação e abstenção).

Sem dúvida, esta artificial dissociação de temáticas leva a outros dos riscos previstos na mesma exposição de motivos enviada à presidência da República, isto é, o risco de "*prejuízos judiciais sensíveis, até que a jurisprudência se adeque às realidades da sociedade da informação*", exatamente pela falta "*ou mesmo omissões nas políticas públicas"* (inclusive a política criminal); que pode levar à "*violação progressiva de direitos dos usuários*" da Internet nesta nação. Ora, isto ocorre desde meados anos 1990, quando a rede mundial se implantou comercialmente no Brasil e se expandiu pelo País. A verdade é o contrário disto: a omissão de uma política criminal clara tem aumentado o risco de violação progressiva de direitos dos internautas, exatamente porque não há normas penais e processuais adequadas à persecução de cibercrimes, cujos principais autores são os próprios internautas, e não o Estado.

Por isto, pode-se dizer que o item 16 da justificativa do projeto do marco civil promete o que não

18 Conforme o artigo 5º, inciso VII, do projeto "aplicações de Internet" correspondem ao conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet".

19 Diferentemente dos dados referentes às conexões à Internet, cuja guarda será obrigatória pelo prazo mínimo de um ano (artigo 11), os dados de acesso a aplicações de Internet apenas *podem* ser mantidos pelos provedores dessas aplicações, o que pode gerar dificuldades para a persecução criminal.

20 Neste sentido, ELIAS, Paulo Sá. Marco civil da Internet quer garantir que haja leis. Consultor Jurídico, 27 de agosto de 2011. Disponível em: http://www.conjur.com.br/2011-ago-27/marco-civil-internet-garantir-haja-leis-restringir-liberdades.

21 Nisto há uma crítica evidente ao PL 84/99 (projeto Azeredo).

pode cumprir. Assegura que "*A norma mira os usos legítimos, protegendo a privacidade dos usuários e a liberdade de expressão, adotando como pressuposto o princípio da presunção de inocência, tratando os abusos como eventos excepcionais*". Na verdade, a premissa é equivocada e deslocada no tempo. O projeto se preocupou apenas em proteger os usuários da Internet de ameaças às suas liberdades e vidas privadas, quando praticadas pelo Leviatã estatal, tão como se o Estado fosse (ainda ou somente) o inimigo número um das liberdades públicas.

Contudo, ao adotar esta concepção, o projeto deixa o caminho aberto para que esses mesmos bens jurídicos sejam atacados por autores privados, dedicados a usos não legítimos (um eufemismo para "crimes"), que hoje corriqueiramente infestam o ciberespaço, com práticas que vão desde a pedo-pornografia até o estelionato ou furto informático, passando pelo *phishing* e por outras práticas espúrias que vitimam os usuários legítimos que o PL 2126/2011 diz pretender proteger, mas que continuarão à mercê desses cibercriminosos. Se o Estado pode ser um tubarão ameaçador para as liberdades públicas na Internet, certas empresas privadas e *crackers* também fazem parte da fauna perniciosa do mar digital.

Os delitos contra a intimidade, o patrimônio, a fé pública, bem como condutas contra a integridade e a disponibilidade da informação trafegável e das conexões passam ao largo do projeto, como se os bens jurídicos surgidos com a sociedade da informação pudessem ser destacados da realidade e considerados de forma estanque. Não podemos fugir aos mandamentos constitucionais, que, ao lado da intimidade e das demais liberdades públicas, ordenam a tutela da honra, do patrimônio, da privacidade e da segurança; vela pelos direitos das crianças e adolescentes; e repudia o racismo. Tradicionalmente, estes bens jurídicos no "mundo concreto" sempre foram tutelados pela lei penal. Por que não o seriam também no "mundo virtual"?

Em suma, a proteção civil aos usuários da Internet pode ser suficiente para condutas menos danosas ou lesivas, de acordo com o princípio da intervenção mínima e em consonância com a subsidiariedade do direito penal. Mas, para aquelas condutas mais gravosas, as que lesam gravemente o patrimônio jurídico e a dignidade das pessoas e a segurança da sociedade, lamentavelmente ainda não é possível abrir mão do direito penal[22]. Aqui o marco civil, amplo, democrático e claro, e a tipificação penal, tópica, limitada e constitucionalmente coerente, devem dar-se às mãos em prol da cidadania na era digital.

5. Conclusão

Numa Internet globalizada, o Brasil não pode fugir do dever internacional de cooperação para a persecução criminal de delitos informáticos próprios (*cybercrimes* ou *computer-crimes*) e impróprios (*computer-facilitated crimes*). O artigo 2º, inciso I, do projeto do marco civil reconhece a "escala mundial da rede", o que significa que, como Estado soberano, devemos pensar em legislação harmônica com as das demais nações do globo. Nenhuma das democracias europeias se limitou a estabelecer um marco civil; buscou-se também a normatização penal e processual penal do ciberespaço. O direito penal não é somente um instrumento de violência controlada contra autores de crimes; é também um meio de proteção dos direitos fundamentais das vítimas destes.

Criminosos que atuam no ciberespaço não têm o menor respeito pelos direitos individuais dos usuários da Internet. Subtraem informações pessoais, fazem-se passar pelas vítimas, furtam valores, clonam cartões de crédito, cometem *grooming* contra crianças e adolescentes, distribuem vírus de computador, divulgam dados sigilosos (públicos e privados), realizam ataques de negação de serviço, destroem informações vitais para a sociedade ou tentam desestabilizar infraestruturas críticas, como sistemas de controle de tráfego aéreo ou de distribuição de energia elétrica. Infelizmente, a Internet não é um parque de diversões, um mundo idílico onde o mal não viceja.

As sociedades humanas dependem cada vez mais dos computadores, das redes informáticas, de sua interconexão, prontidão e instantaneidade e de suas características essenciais, que são a confidencialidade das comunicações, a integridade dos dados e a disponibilidade da informação e dos serviços relacionados à Internet, qualidades estas tão caras às relações interpessoais e ao desenvolvimento científico e econômico. Chega perto da puerilidade a repulsa automática ao PL 84/99, estigmatizado como AI-5 Digital. Como escrevi noutro artigo[23], o projeto Azeredo é sofrível, mas procurou seguir um caminho inevitável, o de tipificação de crimes informáticos essenciais para que a Internet no Brasil seja também um "espaço de segurança, justiça e liberdade" e que não nos

22 FOUCAULT, Michel. Vigiar e punir: nascimento da prisão. Vozes: Petrópolis, 1987. Mesmo sendo um feroz crítico do sistema penal, Foucault reconhece que a pena, inclusive a de prisão, é uma detestável solução da qual ainda não se pode abrir mão.

23 ARAS, Vladimir. O projeto de lei dos cibercrimes (PLS 76/2000): crítica ao substitutivo aprovado no Senado. Revista On-line ANPR, n. 8, Brasília, janeiro/junho de 2009. Disponível em: http://blogdovladimir.files.wordpress.com/2010/01/artigo_projeto-de-lei-dos-cibercrimes-pls-76-de-2000.pdf.

tornemos um “paraíso digital” um *data haven,* que sem dúvida será muito bem explorado por organizações criminosas e delinquentes comuns de vários matizes.

A pretendida dissociação entre o marco civil e a regulamentação penal/processual é inútil e ineficiente e contradiz o esforço de países desenvolvidos, democracias incontestáveis, que resolveram em 2001, há onze anos, estabelecer um “marco penal” para a Internet mundial, que veio a ser a Convenção de Budapeste.

Portanto, aplacadas as paixões de lado a lado, que venham as duas regulamentações, num texto coeso, coerente, uniforme e garantista, no melhor sentido da palavra, isto é, um estatuto que seja capaz de proteger as liberdades públicas dos cidadãos e não deixá-los à mercê de cibercriminosos.

É de se indagar aos que rejeitam de forma absoluta a regulamentação global (civil e criminal) do ciberespaço, o que diriam do Estatuto da Criança e do Adolescente (Lei 8.069/90), do Código de Defesa do Consumidor (Lei 8.078/90), do Estatuto do Idoso (Lei 10.741/03), do Estatuto do Torcedor (Lei 10.671/03), e da Lei Maria da Penha (Lei 11.340/06). Estas são apenas algumas das leis aprovadas no Brasil nos últimos 20 anos que contêm dispositivos civis e criminais. São diplomas incontestavelmente legítimos e coerentes com uma sociedade que respeita os direitos humanos. Crianças, idosos, mulheres, consumidores e torcedores, todos mereceram proteção civil e penal, dada a relevância dos bens jurídicos em jogo. Por que deveria ser diferente com a Internet e seus usuários? A opção por uma política legislativa geminada não nos levará à *Matrix;* tampouco nossas máquinas se converterão nas tele-telas do Grande Irmão.

Dito deste modo, percebe-se que o projeto do marco civil, excepcional nos seus aspectos principiológicos e de garantia e muitas vezes melhor tecnicamente do que o PL 84/99, ainda assim peca por não atender ao escopo a que se propôs, de ser uma lei que aborde “*de forma transversal a Internet,* [e] *viabilize ao Brasil o início imediato de um melhor diálogo entre o Direito e a Internet*”. Não adianta proteger direitos dos internautas apenas no papel, sem que seja possível tutelar com segurança e de forma dissuasiva esses mesmos bens jurídicos constitucionais do ciberespaço. Para melhor proteger os ciberdireitos, devem existir ciberdeveres. Sem isto, o limbo e a incerteza jurídica continuarão. Haverá um escudo, mas não uma espada.

Referências

ARAS, Vladimir. **Crimes de informática: uma nova criminalidade**. Jus Navigandi, Teresina, ano 5, n. 51, out. 2001. Disponível em: http://jus.uol.com.br/revista/texto/2250/crimes-de-informatica

ARAS, Vladimir. **O projeto de lei dos cibercrimes (PLS 76/2000):** crítica ao substitutivo aprovado no Senado. Revista On-line ANPR, n. 8, Brasília, janeiro/junho de 2009. Disponível em: http://blogdovladimir.files.wordpress.com/2010/01/artigo_projeto-de-lei-dos-cibercrimes-pls-76-de-2000.pdf.

BRASIL. Ministério da Justiça. **Marco civil da Internet:** seus direitos e deveres em discussão. Disponível em: http://culturadigital.br/marcocivil/

ELIAS, Paulo Sá. **Marco civil da Internet quer garantir que haja leis**. Consultor Jurídico, 27 de agosto de 2011. Disponível em: http://www.conjur.com.br/2011-ago-27/marco-civil-internet-garantir-haja-leis-restringir-liberdades.

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. Vozes: Petrópolis, 1987.