PERSPECTIVA PARA NOVOS MODELOS DE "INVESTIGAÇÃO TECNOLÓGICA" E PROTEÇÃO DE DIREITOS FUNDAMENTAIS NA ERA DA INTERNET

4

O chamado "ciberterrorismo" como um primordial exemplo, em conjunto a problemas de definição e a luta contra terrorismo e os crimes cibernéticos

Perspective for new types of "technological investigation" and protection of fundamental rights in the Era of Internet The so-called "cyberterrorism" as a prime example, between problems of definition and the fight against terrorism and cybercrime

ROBERTO FLOR

Professor de Direito Penal da Tecnologia da Informação e Direito Penal Internacional e Professor Assistente (*ricercatore*) de Direito Penal na Universidade de Verona (Itália). Investigador científico em centros universitários nos E.U.A, Reino Unido e Alemanha.

Traduzido por

MARCELO ALMEIDA RUIVO

Doutorando em Ciências Jurídico-Criminais na Faculdade de Direito da Universidade de Coimbra.

CÁSSIO CHECHI DE ASSIS

Mestrando em Ciências Jurídico-Criminais na Faculdade de Direito da Universidade de Coimbra.

ÁREA DO DIREITO: Penal

RESUMO: A ameaça do "ciberterrorismo" e o uso da Internet voltado ao terrorismo são particularmente alarmantes, principalmente em função da forte dependência da ordem social, política e econômica na rede global. Duas suposições basilares devem ser consideradas: 1) o papel que a Internet e as novas tecnologias podem desempenhar na preparação ou cometimento de crimes; 2) o papel que a Internet e as novas tecnologias podem desempenhar no combate aos crimes. O objetivo do presente trabalho é identificar critérios elevados para proporcionar uma regulação específica para novos tipos de investigação, garantindo respeito aos direitos fundamentais, a partir de um primordial exemplo: a luta contra o "ciberterrorismo". Tais critérios serão extraídos de diversas decisões significativas das Cortes Constitucionais europeias, especialmente aquelas acerca de normas que regulem retenção de dados e pesquisa on-line.

PALAVRAS-CHAVE: Terrorismo internacional - Ciberterrorismo - Crimes cibernéticos - "Investigações tecnológicas" e retenção de dados - Direito penal - Limites constitucionais - Proteção de direitos fundamentais.

ABSTRACT: The threat of "cyber-terrorism" and the use of Internet for terrorist purposes are particularly alarming, primarily because of the strong dependence of the current social, economic and political order on the global network. Two main assumptions should be considered: 1) the role that Internet and the new technologies can play in preparing or committing crimes; 2) the role of Internet and the new technologies can play in the fight against crimes. The objective of this paper is to identify some high standards to provide a specific regulation for new types of investigation, ensuring respect for fundamental rights, starting from a prime example: the fight against "cyberterrorism". These standards may be drawn from several important decisions of the Constitutional Courts in Europe, especially those decisions regarding regulations governing data retention and on-line search.

KEYWORDS: International terrorism - Cyberterrorism - Cybercrime - "Technological investigations" & data retention - Criminal law - Constitutional limits - Protection of fundamental rights.

1. INTRODUÇÃO

Após[1] os ataques de 11.09.2011, em Nova Iorque e Washingon; de 11.03.2004, em Madrid; de 7 e 21.07.2005, em Londres; bem como o de

1. Paper escrito para II Congreso Internacional de Jóvenes Investigadores en Ciencias Penales. 2. ed., Salamanca, 2011.

30.06.2007 em Glasgow, a ameaça terrorista assumiu um caráter peculiar que, nas ciências criminais, resultou no debate da persecução penal do "inimigo" (*diritto penale del nemico* – Enemy Criminal Law – *Feindstrafrecht*) e no combate contra o inimigo penal ("IHL" ou "o *jus in bello* penal").[2]

A segurança interna do Estado individual deve agora considerar a necessidade de um direito penal diverso do "tradicional" – relacionado ao "simples" delito. Tal é necessário para enfrentar – senão prevenir – o fenômeno criminal transnacional, que objetiva desafiar ou erradicar um sistema político, social ou econômico, baseado num grupo comum de valores geralmente compartilhados.

Considerando a distinção entre "terrorismo em tempos de paz" e "terrorismo em tempos de guerra" – que, mesmo dentro do direito internacional humanitário, resultou na diferenciação entre modelo tradicional e modelo novo, projetado para o combatente tratado como criminoso (inimigo)[3] – é evidente que a definição de terrorismo pode ser não só ampla, mas igualmente não reconhecida universalmente.[4]

---

2. Ver JAKOBS, Kriminalisierung im Vorfeld einer Rechtsgutverletzung, *ZStW*, 1985, 751. Entre os mais recentes trabalhos desse autor ver JAKOBS, Terroristen als Personen im Recht?, *ZGS*, 2005, 839; JAKOBS, Bürgerstrafrecht und Feindstrafrecht, *HRRS*, 3/2004, 88; JAKOBS, Feindstrafrecht? – Eine Untersuchung zu den Bedingungen von Rechtlichkeit, *HRRS*, 8-9/2006, 290. Para crítica, ver, recentemente, VORMBAUM (Hrsg), *Kritik des Feindstrafrechts*, Berlin, 2009; MORGUET, *Feindstrafrecht, eine kritische Analyse*, Berlin, 2009. Ver também FERRAJOLI, "Il diritto penale del nemico" e la dissoluzione del diritto penale, *Quest. giust.*, 2006, 797; DONINI, Diritto penale di lotta. Ciò che il dibattito sul diritto penale del nemico non deve limitarsi ad esorcizzare, *Studi sulla questione criminale*, 2007, 55; DONINI, Il diritto penale di fronte al "nemico", *Cass. pen.*, 2006, 735; para o debate internacional ver AA.VV., *Diritto penale del nemico. Un dibattito internazionale*, Milano, 2007; AA.VV., *Delitto politico e diritto penale del nemico*, Bologna, 2007; BARTOLI, *Lotta al terrorismo internazionale. Tra diritto penale del nemico, ius in bello del criminale e annientamento del nemico assoluto*, Torino, 2008. Ver também VIGANÒ, Lucha contra el terrorismo y protección de los derechos fundamentales. In: ARROYO ZAPATERO, *Piratas, mercenarios, soldados, jueces y policías: nuevos desafíos del Derecho penal europeo e internacional*, Ediciones de la Universidad de Castilla-La Mancha, Cuenca, 2010, 77-85 (com mais referências); VIGANÒ, Terrorism and the Rule of Law: an Italian View. In: SERRANO-PIEDECASAS; CRESPO (ed.), *Terrorismo y Estado de Derecho*, Iustel Madrid, 2010, 515-539.

3. Ver CASSESE, The multifaceted Criminal Notion of Terrorism in International Law, *JICJ*, 2006, 950. Ver também AA.VV., *Terrorismo internazionale e diritto penale*, Padova, 2007.

4. Sobre a definição de terrorismo ver GOLDER; WILLIAMS, What is terrorism?, *Un. New South. Wales Law Journ*, 27, 2004, 270, e o relatório Tomuschat (Codexter – Council of Europe Committee of Experts on Terrorism – Conselho de Europa Comitê de es-

O chamado "ciberterrorismo" se insere nesse contexto, e num mundo globalizado. Esse fenômeno ainda não resta bem definido, mas, por um lado, representa uma função que o desenvolvimento tecnológico tem exercido e atualmente exerce em planejar e/ou executar ataques terroristas. Por outro lado, a qualificação de "ciber" pode representar que os alvos dos ataques sejam os sistemas informáticos do Estado, os dados ou informações lá armazenados ou o sistema de comunicações baseado em estruturas lógicas e redes de computadores.

A Internet e outras novas tecnologias desempenham significativo papel na atual sociedade global da informação. São elas agora essenciais em cada setor da vivência humana e podem ser usadas para a preparação e consumação de graves delitos contra significativos bens jurídicos.

A ameaça do "ciberterrorismo" e o uso da Internet voltado ao terrorismo são particularmente alarmantes, principalmente em função da forte dependência da ordem social, política e econômica na informatização e na rede global.

Se tal ameaça é superestimada em certos casos, especialmente em termos de percepção pelo público, não pode ser subestimada, ou, pior, ignorada pelos legisladores.

Duas suposições basilares devem ser consideradas: 1) o papel que a Internet e as novas tecnologias podem desempenhar na preparação ou cometimento de

---

pecialistas sobre terrorismo). Sobre a convenção internacional ver: Convenção para a Repressão da Captura Ilícita de Aeronaves, 16.12.1970; Convenção para a Repressão dos Actos Ilegais contra a Segurança da Aviação Civil, Montreal 23.09.1971; Convenção sobre a Prevenção e Repressão de Crimes contra Pessoas Gozando de Protecção Internacional, incluindo os Agentes Diplomáticos, Nova Iorque 14.12.1973; Convenção Internacional contra a Tomada de Reféns, Nova Iorque, 17.12.1979; Convenção sobre a Protecção Física dos Materiais Nucleares, Viena 3.03.1980; Protocolo para a Repressão de Actos Ilícitos de Violência nos Aeroportos ao Serviço da Aviação Civil Internacional, Montreal, 24.02.1988; Convenção para a Supressão de Actos Ilícitos contra a Segurança da Navegação Marítima, Roma 10.03.1988; Protocolo para a Supressão de Actos Ilícitos contra a Segurança das Plataformas Fixas Localizadas na Plataforma Continental, Roma 10.03.1988; Convenção para a Repressão dos Atentados Terroristas à Bomba, Nova Iorque 15.12.1997; Convenção Internacional para a Supressão do Financiamento do Terrorismo, Nova Iorque 09.12.1999; Convenção Internacional para a Repressão dos Actos de Terrorismo Nuclear, Nova Iorque, 13.04.2005 (Alteração ao apêndice, 09.11.2008, entrou em vigor em 13.09.2009). Sobre a definição de terrorismo em consideração ao direito penal italiano, ver VIGANÒ, La nozione di 'terrorismo' ai sensi del diritto penale. In: SALERNO (ed.). *Sanzioni "individuali" del Consiglio di Sicurezza e garanzie processuali fondamentali*, Cedam (Padova), 2010, 193-220.

crimes, inclusive terrorismo e "ciberterrorismo"; 2) o papel que a Internet e as novas tecnologias podem desempenhar no combate ao crime, incluindo terrorismo e "ciberterrorismo", especialmente no que concerne às investigações possuírem certo "caráter tecnológico".

O objetivo do presente trabalho é identificar critérios elevados para guiar o desenvolvimento de uma regulação específica para novos tipos de investigação, garantindo respeito aos direitos fundamentais, a partir de um primordial exemplo: a luta contra o "ciberterrorismo". Esses critérios serão extraídos de certas decisões significativas das Cortes Constitucionais europeias, especialmente em se tratando de normas que regulem retenção de dados e pesquisa on-line, algumas das quais deram força à luta contra terrorismo internacional.

2. CIBERTERRORISMO: MITO OU REALIDADE?

Definir o termo "terrorismo" não é uma simples tarefa.[5] Contudo, definir o termo "ciberterrorismo" é ainda mais complicado, em função dos diferentes significados que a palavra invoca, variando de realidade a mito. A complexidade em encontrar uma definição consensual é considerada um dos obstáculos em criar um mecanismo internacional para combatê-lo.[6]

---

5. A amplamente aceita definição de terrorismo a nível internacional é encontrada no art. 2, Seção 1 (b), da Convenção Internacional das Nações Unidas para a Supressão do Financiamento do Terrorismo de 1999. Esta definição foi reafirmada em outros instrumentos internacionais (i.e., Res. 1.566 do Conselho de Segurança da ONU): "Qualquer outro ato destinado a causar a morte ou lesões corporais graves a um civil ou a qualquer outra pessoa não tomar parte ativa nas hostilidades numa situação de conflito armado, quando o propósito de tal ato, por sua natureza ou contexto, é intimidar uma população ou obrigar um governo ou uma organização internacional a agir ou abster-se de praticar qualquer ato". Ver YOUNG, Defining terrorism: the evolution of terrorism as legal concept in international law and its influence on definitions in domestic legislation, 29 *B.C. Int'l &Comp. L. Rev.* 23, 2006, 53; STEPHENS, International Criminal law and the response to international terrorism, 27(2) *U. New South Wales L.J.* 454, 2004, 461-462-463.

6. Ver TAUB, Terrorism in the International Law, *International Law*, 2003, 476; KURTH CRONIN, Behind the curve: globalization and international terrorism, 27(3) *Int'l Sec.* 30, 2002, 32. Ver, também, com referência ao "Digital Pearl Harbor" (após essa experiência, o governo dos EUA começou uma campanha de melhoria – também em nível legislativo – da prontidão para o ciberterrorismo), MYTHRI RAGHAVAN, In fear of cyberterrorism: an analysis of the congressional response, *J.L. Tech. & Pol'y*, 2003, 297-312. Quanto a outras iniciativas nacionais (ou seja, o Centro Nacional de Assistência Técnica no Reino Unido) ver WALKER, Cyberterrorism: Legal principle

O ciberterrorismo deve ser mantido à parte da assim chamada "ciberguerra"[7] e deve ser visto num contexto do fenômeno mais amplo "terrorismo". Aparenta ser apropriado aceitar aqui um conceito lato deste,[8] incluindo o uso ou ameaça

---

and law in the United Kingdom, *110(3) Penn St. L. Rev.*, 2006, 625-665. Para mais referências, ver, também, A. COHEN, Cyberterrorism: are we legally ready?, *Journal of Int. Business & Law,* 2010; PRICHARD; MACDONALD, Cyber terrorism: a study of the extent of coverage in computer security textbooks, 3 *J. Info. Tech. Edu.*, 2004, 279, 281; BRENNER; GOODMAN, In defense of cyberterrorism: an argument for anticipating cyber-attacks, *J.L. Tech.& Pol'y* , 2002, 12; BRENNER, Cybercrime, cyberterrorism and cyberwarfare, *Rev. int. droit pénal.*, 3, 77, 2006, 453-471.

7. Ver Clarke; Knake, *Cyber war*: the next threat to national security and what to do about it, HarperCollins Pub., 2010; LIBICKI, *Cyberdeterrence and cyberwar*, Rand Corp., 2009; MEHAN, *Cyberwar, cyberterror, cybercrime,* IT Governance Pub., 2008. BALDI; GELBSTEIN; KURBALIJA, *Hacktivism, cyber-terrorism and cyberwar: the activities of the uncivil society in cyberspace*, DiploFoundation, 2003.

8. Ver já, SCHMID; JONGMAN et al, *Political terrorism: A new guide to actors, authors, concepts, data bases, theories, and literature*, New Brunswick, NJ, Transaction Books, 1988, 5. Em nível europeu, ver a Decisão-Quadro de 13.06.2002 sobre o combate ao terrorismo, em particular no art. 1, que determina: todo Estado-membro deve tomar as medidas necessárias para assegurar que os atos intencionais previstos nas alíneas (a) à (i), definidos como crimes sob a lei nacional, o que, dada a sua natureza ou contexto, pode danificar seriamente um país ou uma organização internacional, quando cometido com o intuito de: – intimidar gravemente a população, ou – obrigar indevidamente um governo ou organização internacional a praticar ou se abster-se de praticar qualquer ato ou – desestabilizar gravemente ou destruir as estruturas políticas, constitucionais, económicas ou sociais de um país ou de uma organização internacional, deve ser considerado como infrações terroristas: (a) ataques contra a vida de uma pessoa que pode causar a morte, (b) os ataques à integridade física de uma pessoa, (c) sequestro ou tomada de reféns; (d) causação de extensa destruição de instalação do governo ou pública, sistema de transporte, infraestrutura, incluindo sistema de informação, plataformas fixas situadas na plataforma continental, locais públicos ou em propriedades privadas suscetíveis de pôr em perigo a vida humana ou resultar em grande perda econômica; (e) a apreensão de aeronaves, navios e outros meios de transporte público ou de mercadorias; (f) a fabricação, posse, aquisição, transporte, fornecimento ou uso de armas, explosivos ou de armas nucleares, biológicas ou químicas, bem como a investigação e desenvolvimento de armas biológicas e químicas; (g) a liberação de substâncias perigosas, ou a provocação de incêndios, inundações ou explosões cujo efeito é o de colocar em risco a vida humana, (h) interferência ou interrupção o fornecimento de água, energia ou qualquer outro recurso natural fundamental cujo efeito põe em perigo a vida humana; (i) a ameaça de cometer qualquer dos atos referidos do (a) ao (h). O art. 2 estabelece: entende-se por "grupo terrorista": um grupo estruturado de mais de duas pessoas, que ao longo de um período de tempo e atuando em conjunto para cometer de infrações terroristas; por "grupo estruturado", um grupo que não é

de uso ilegal de força ou violência, caracterizado por finalidades políticas, ideológicas ou religiosas, contra indivíduos ou bens para intimidar ou coagir certo governo ou população civil. Essa intimidação ou coerção inclui um plano "psicológico", que pode se constituir no aumento do medo ou na percepção deste.

Tal definição tem sua origem nos fenômenos que, pelas suas naturezas ou contextos, podem causar sérios danos a certo país ou organização interna-

---

aleatoriamente formado para a prática imediata de uma infracção e que não precisa ter formalmente papéis definidos para os seus membros, continuidade na sua composição ou uma estrutura desenvolvida. Ver também Decisão-Quadro 2008/919/JHA de 28.11.2008 que altera Decisão-Quadro 2002/475/JHA relativa ao combate ao terrorismo, que diz que a ameaça "terrorista cresceu e evoluiu rapidamente nos últimos anos, com mudanças no *modus operandi* de ativistas e apoiantes do terrorismo, incluindo a substituição de grupos estruturados e hierarquizados por células semiautônomas frouxamente amarradas umas as outras. Essas células interligam-se a redes internacionais e dependem, cada vez mais, do uso de novas tecnologias, em particular a Internet. A internet é utilizada para inspirar e mobilizar redes terroristas locais e indivíduos na Europa e também serve como uma fonte de informação sobre os meios e métodos terroristas, funcionando, portanto, como um 'campo de treino virtual'. As atividades de incitamento público à prática de infrações terroristas, recrutamento para o terrorismo e treinamento para o terrorismo têm-se multiplicado a um custo muito baixo e risco" (enquanto 3 e 4). O "novo" art. 3 da decisão determina: as infrações relacionadas com atividades terroristas: (a) "incitamento público à prática de infrações terroristas", a distribuição, ou qualquer outra forma de disponibilização, de uma mensagem para o público, com a intenção de incitar a prática de um dos crimes referidos no art. 1 (1) (a) a (h), no qual tal conduta ou não diretamente defendendo a prática de infrações terroristas, cause o perigo que uma ou mais dessas infrações possa ser cometida; (b) "recrutamento para terrorismo", a solicitação a outra pessoa para cometer um dos crimes referidos no art. 1 (1) (a) a (h) ou no art. 2(2); (c) por "treino para terrorismo" se entende o fornecimento de instrução para a confeção ou utilização de explosivos, armas de fogo ou outras armas e substâncias nocivas ou perigosas ou sobre outros métodos e técnicas específicos, com o propósito de cometer um dos crimes enumerados no art. 1 (1) (a) a (h), sabendo que os conhecimentos ministrados destinam-se a serem usados para essa finalidade. 2. Cada estado-membro deve tomar as medidas necessárias para garantir que as infrações relacionadas com atividades terroristas incluem os seguintes atos intencionais: (a) o incitamento público à prática de infrações terroristas, (b) o recrutamento para terrorismo; (c) treino para terrorismo, (d) furto qualificado com vista à prática das infrações previstas no art. 1 (1), (e) chantagem com vista para a prática de uma das infrações previstas no art. 1 (1); (f) a elaboração de documentos administrativos falsos com vista à prática de um dos crimes referidos no art. 1 (1) (a) a (h) e no art. 2 (2) (b). Na Itália, por exemplo, a Lei 155/2005, introduzido no Código Penal três novos crimes: art. 270-quater (Recrutamento para fins terroristas), art. 270-quinquies (treino para terrorismo) e arte. 270-sexies (crimes com fins de terrorismo).

cional, e são planejados com escopo de intimidar uma população; forçar um governo ou uma organização internacional a executar – ou deixar de executar – determinada ato; ou desestabilizar ou destruir as estruturas políticas, constitucionais, econômicas e sociais de determinado país ou organização internacional. O "ciberterrorismo" pode englobar pelo menos três fenômenos:[9]

9. Essa definição é, em parte, semelhante a descrita por SIEBER; BRUNST, *Cyberterrorism: the use of the Internet for terrorist purposes*, Council of Europe Publishing, 2007, 14. Os Autores especificam definições de classes de ciberterrorismo desde o uso comum da internet por terroristas até casos criminais reais envolvendo tanto as perdas virtuais quanto físicas. Ver também SIEBER. In: SPINELLIS (ed.), *Computer crimes, cyber-terrorism, child pornography and financial crimes. Reports presented to the Preparatory Colloquium for the Round Table II of the 17th International Congress of Penal Law* (Beijing, 2004), Athens 2004, 11-50. O argumento central de Sieber é que a emergente sociedade da informação e sua vulnerabilidade apresenta novos riscos, como uma questão de fato, e novos desafios para o sistema de justiça criminal, como uma questão de direito. Outros autores tomaram o chamado "ciberterrorismo" como um exemplo primordial. Em 2007, Vogel apresentou um artigo para a Conferência Mundial de Direito Penal. Direito Penal no século XXI (Guadalajara, México, 18 a 23.11.2007). O título é *Towards a Global Convention against Cybercrime* (também em: [www.penal.org]), no qual o autor relatou que ciberterrorismo pode ser um "ataque em grande escala contra um sistema de informação" (por exemplo, se os terroristas atacassem sistemas de informação essenciais para os mercados de capitais internacionais de modo que esses mercados viessem a quebrar), um crime de informática (por exemplo, se terrorista assumissem o controle de mais de um sistema de gestão da informação de uma instalação nuclear e disparassem um colapso nuclear) ou crime relacionado ao conteúdo (por exemplo, se o terrorista difundisse propaganda ou projetos para bombas por meio da Internet), mas dificilmente poderia ser descrito como uma categoria separada ou crime". Brenner escreveu que "ciberterrorismo essencialmente consiste na utilização de tecnologia computacional para se engajar no terrorismo. Desde que 'crime' e 'terrorismo' são semelhantes em certos aspectos e desde que ambos têm como alvo habilidade das sociedades para manter a ordem interna, temos de começar por diferenciar os dois. Basicamente, o crime é 'pessoal', enquanto o terrorismo é 'político'. Crimes são cometidos por motivos pessoais, individuais, o mais importante dos quais é o ganho pessoal e o desejo (necessidade) de prejudicar os outros psicologicamente e/ou fisicamente. Terrorismo, muitas vezes, resulta na imposição de 'danos' indistintos daqueles causados pelo crime (por exemplo, a morte, danos pessoais, destruição de propriedade), mas os 'danos' são infligidos por razões muito diferentes. Um estatuto dos EUA, por exemplo, define o 'terrorismo' como (a) a cometer atos que constituem 'crimes' sob a lei de qualquer país (b) para intimidar ou coagir uma população civil, para influenciar a política do governo por intimidação ou coerção ou afetar a conduta do governo pela destruição em massa de assassinato ou sequestro". O autor especificou: "Para entender o que ciberterrorismo pode – e vai – ser, temos de examinar como os terroristas podem usar a tecnologia de computador para intimidar ou coagir uma

1) ataques executados através de uma rede de computadores e que podem causar danos irreparáveis a sistemas informáticos "confidenciais", a dados "confidenciais" – ou "secretos" – lá armazenados ou processados, a sistemas de comunicação, ou à infraestrutura do Estado – ou de entes públicos – essencial para a própria vida humana;[10]

2) a disseminação de conteúdo ilegal na rede, com objetivo não só de fornecer informação na preparação de um ataque terrorista, mas também de incitar, anunciar, disseminar ideias ou opiniões, recrutar militantes e coletar fundos para guerras ideológicas ou disseminar material de cunho racista ou xenofóbico;[11]

3) o uso da Internet, ou de redes, como meios de comunicação entre terroristas, os quais podem usufruir do anonimato ao utilizar sistemas para terceirizar o fluxo de dados, e ao separar o momento das comunicações, também possível por intermédio de procedimentos automatizados – e programáveis *ex ante*.

---

população civil e, assim, minar a capacidade de uma sociedade para sustentar a ordem interna. Conceitualmente, a sua utilização para esse fim se divide em três categorias: (a) arma de destruição em massa, (b) arma de distração em massa, e (c) arma de transtorno em massa". Ver BRENNER, *Cibercrime* cit., 457-458.

Para uma ampla definição de terrorismo ver HOFFMAN, Defining terrorism. In: HOWARD; SAWYER (eds.), *Terrorism and counterterrorism: understanding the new security environment*, Guilford, CT, McGraw-Hill/Dushkin, 2003, 22; BYMAN, "*Scoring the war on terrorism*," *the national interest*, Summer 2003, 79 e ss. Ver também o relatório do Reino Unido sobre *The definition of terrorism*, apresentado ao Parlamento pelo secretário de Estado para o Departamento de assuntos domésticos, sob o comando de Sua Majestade, 2007.

10. Serviços públicos, desde hospitais em rede até serviços de água e elétrica, são agora altamente dependentes de redes e sistemas informáticos. Excelente exemplo dessa dependência foi o ataque cibernético contra a Estônia em 2007. Ver o Relatório do CRS (Congressional Research Service — Serviço de Pesquisa Parlamentar) para o Congresso intitulado *Botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for congress*, U.S. Department of State, 2008.

11. A diferença básica do ativismo "pacífico" é que esse tem como objetivo a visibilidade e publicidade destinadas ao "constrangimento" o alvo. O ciberterrorismo, ao contrário, tem como finalidade a propaganda, recrutamento, pesquisa de fundos ou de financiamento e utilização de novas tecnologias como meio de difusão/comunicação. Ver BALDI; GELBSTEIN; KURBALIJA, *Hacktivism* cit., 18. cfr. REITAN, *Global activism*, New York, 2007, MEIKLE, *Media activism and the Internet*, London, 2002. Ver também B. R. DAVIS, *Ending the cyber jihad: combating terrorist exploitation of the Internet with the rule of law and improved tools for cyber governance*, 15 *Commlaw Conspectus*, 2006, 119-186; in general WEIMANN, *Terror on the Internet: the new arena, the new challenges*, Washington DC, 2006. Sobre o racismo na internet ver AKDENIZ, *Racism on the Internet*, Council of Europe, 2009.

É outrossim possível propor uma classificação adicional baseada no "papel" desempenhado pela tecnologia e pela Internet, distinguindo entre casos nos quais:

1) ferramentas de computador, incluindo infraestrutura e rede, são os únicos meios para perpetrar um ataque terrorista, na sua fase preparatória e/ou consumativa (por exemplo, a busca *online* de informações de como construir um aparato explosivo ou do alvo físico a ser atingido);

2) ferramentas de computador, incluindo infraestruturas e redes, são essenciais para a preparação ou execução de um ataque terrorista (por exemplo, para a distribuição de programas maliciosos) ou constituem o objeto ou finalidade de tal atividade. Nestes casos, os alvos podem ser vários, tais quais: transpassar medidas de seguranças para acessar sistemas computacionais; sabotar a integridade, confidencialidade ou segredo de sistemas computacionais e dados; tornar os sistemas inutilizáveis ou inoperantes, incluindo websites; alterar ou falsificar dados e informações lá armazenados; interferir com infraestrutura "confidencial", comumente relacionada com outras infraestruturas para o suprimento de energia, água, serviços de transporte, defesa nacional, saúde ou política públicas.[12]

Em termos de direito penal material, "ciberterrorismo", considerado como um fenômeno englobado pelo "terrorismo" mais amplo, é caracterizado por um número de componentes estruturais comuns tanto ao crime cibernético quanto ao terrorismo.

Os métodos de realização do ataque, entretanto, podem ser diversos e utilizar dos meios tecnológicos mais sofisticados ou as mais "simples" ou "tradicionais" estratégias e modos de execução" (i.e., a destruição física de um prédio que abriga os servidores que armazenam bancos de dados contendo informações "confidenciais", "estratégicas" ou "de utilidade pública").[13]

---

12. Alguns autores distinguem entre diferentes tipos de redes que podem ser sujeitas a ataques ciberterroristas: redes militares e de defesa civil; outras redes governamentais; redes privadas ou públicas usadas para controlar os serviços públicos e outros sistemas de prestação de serviços de infra-estrutura, redes públicas utilizadas por consumidores individuais e empresas de comunicação e educação. Ver, por exemplo, TRACHTMAN, *Global cyberterrorism, jurisdiction, and international organization*, 2004 (WP).

13. Estas considerações são confirmadas pelos modelos existentes de proteção contra o terrorismo, que se baseiam principalmente em: 1) a qualidade da vítima – considerada sob o ponto de vista criminológico – que é independente e externa aos objectivos visados pelo ataque terrorista; 2) a finalidade subjetiva ou a atitude psicológica do agente ou agentes, quem, muitas vezes, persegue ou prosseguem propósitos ideoló-

3. CIBERTERRORISMO E CRIMES CIBERNÉTICOS: ATAQUES GLOBAIS, RESPOSTAS GLOBAIS

No ciberespaço, o paralelo com os componentes do fenômeno do "terrorismo" pode ser válido, e, de acordo com a função atribuída à tecnologia e à rede, pode haver uma conexão próxima com o crime cibernético.[14]

No nível de fontes legislativas supranacionais e suas aplicações na Europa, a Convenção sobre o Crime Cibernético do Conselho da Europa é o instrumento internacional mais importante no combate ao crime cibernético. Aberta à assinatura em Budapeste em novembro de 2011, tem sido ratificada até a presente data por trinta Estados, enquanto outros países usam suas disposições como diretrizes para introduzir aos seus ordenamentos jurídicos instrumentos apropriados no combate ao crime cibernético.[15]

Tal tratado deu sequência à Res. 1, adotada pelos Ministros da Justiça do Conselho da Europa durante a XXI Conferência (em Praga, 10 e 11.06.1997),

---

gico, político ou religioso; 3) a qualidade da vítima e a atitude psicológica do agente ou agentes (tipo de modelo híbrido ou misto).

14. Em outras palavras, podemos colocar sistematicamente atos criminosos entre cibercrime "no seu sentido próprio", quando os meios típicos da comissão pertencem à tecnologia informática ou telemática ou o objeto passivo tem um "caráter tecnológico-computacional" ou, ainda, podemos os colocar entre os crimes cibernéticos "no seu sentido impróprio", quando eles são crimes comuns, que só pode ser eventualmente cometidos por meio do uso da tecnologia. Ver PICOTTI, La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee, *Riv. trim. dir. pen. ec.*, 4, 2011, 827 e ss.; PICOTTI, Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati. In _____ (cur.), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, 21, PICOTTI, Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione Internazionale. *Dir. Internet*, 2005, 189; PICOTTI, La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale, *Dir. pen. proc.*, 2008, 700. Ver também FLOR, *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet*, Padova, 2010, 195; FLOR; J. OH JANG, Cyber-criminality: finding a balance between freedom and security. An introduction, *Cyber-criminality: finding a balance between freedom and security*, S. MANACORDA (ed.), R. FLOR; J. OH JANG (coords.), Milano, ISPAC, 2012; BRENNER, Defining cybercrime: a review of federal and State Law. In: CLIFFORD (ed.), *Cybercrime*, III Ed., Carolina Academic Press, 2011, 15-104, 17.

15. Ver "Octopus Interface 2008 – *Cooperation against Cybercrime*", "Octopus Interface 2009 – *Cooperation against Cybercrime*" e "Octopus Interface 2010 – *Cooperation against Cybercrime*", in: [www.coe.int]. Ver GERCKE, National, regional and international legal approaches in the fight against cybercrime, *CRi*, 1, 2008, 7.

que expressava a vontade do Comitê de Ministros em apoiar o trabalho feito *in subjecta materia* pelo Comitê Europeu para os Problemas Criminais (CDPC), a fim de aproximar leis nacionais de diferentes países e permitir o uso de sistemas práticos na investigação de crimes telemáticos. A convenção também deu sequência à Res. 3, adotada na XXIII Conferência dos Ministros Europeus da Justiça (em Londres, 08 e 09.06.2000), a qual encorajou as partes a continuar seus esforços na busca de soluções apropriadas para permitir a participação do maior número possível de países na convenção.

Em termos de direito penal material, o tratado dispõe que cada parte tome as medidas necessárias para criminalizar certas condutas, como o acesso ilícito a sistema de informática ou telecomunicação (art. 2.º), interceptação ilícita (art. 3.º), ataque à integridade de dados (art. 4.º), o ataque à integridade de sistemas informáticos (art. 5.º), a utilização indevida de dispositivos (art. 6.º), a falsificação de dados (art. 7.º), a fraude informática (art. 8.º), infrações relativas à pornografia infantil (art. 9.º), bem como infrações relativas a direito do autor e direitos conexos. Ademais, o art. 12 também dispõe que tais infrações estão sujeitas à responsabilização penal da pessoa jurídica.

Em termos de direito processual, há, outrossim, provisões específicas no que tange à retenção de tráfico de dados e comunicação (arts. 16 e 17), medidas para a busca e apreensão de dados informáticos – inclusive acesso a sistemas informáticos que armazenam dados e informações – (art. 19), a coleta em tempo real de dados (art. 20) e a interceptação do conteúdo dos dados (art. 21).

Finalmente, após a Convenção sobre o Crime Cibernético, foi outrossim aberto à assinatura o Protocolo adicional relativo à Criminalização de atos de natureza racista e xenofóbica praticados através de sistemas informáticos.

De jure condito, assim, em adição às convenções de combate ao terrorismo,[16] há outro grupo de normas que podem ser aplicadas em ordenamentos nacionais e podem ser aplicáveis ao fenômeno do chamado ciberterrorismo, nos três sentidos supracitados.[17]

---

16. Acima, nota 3.

17. Com referências sobre a luta contra o ciberterrorismo ver BRUNST, Terrorism and the Internet. In: WADE; MALJEVIC (eds.), *A war on terror? The European stance on a new threat, changing laws and human rights implications*, New York, 2009, 51; BRUNST, Legal aspects of cyber terrorism, in centre of excellence – Defence against terrorism (ed.), *Legal aspects of combating terrorism*, Amsterdam, NATO, *Science for peace and security series*, 2008, 63; NATO, Use of the Internet by terrorists – A threat analysis. In: CENTRE OF EXCELLENCE – DEFENCE AGAINST TERRORISM (ed.), *Responses to cyber terrorism*, Amsterdam, IOS Press, NATO, Science for peace and security series, 2008, 34.

No nível procedimental ou puramente investigativo, em casos de ataques executados via uma rede informática ou por seu intermédio, de distribuição de conteúdo ilícito, ou de uso de rede informática como meio de comunicação entre terroristas, seria irrealista confiar unicamente nos meios tradicionais de investigação. Pelo contrário: o uso de novas tecnologias é essencial na busca e colheita de provas, na identificação da fonte do ataque ou do receptor das comunicações, ou a fim de prevenir a consumação de graves infrações contra importantes bens jurídicos coletivos.

Devemos acrescentar à necessidade de um amplo e articulado debate na adoção de novas ferramentas "tecnológicas" possuidoras, também, de funções preventivas a demanda pelo reconhecimento de funções públicas a corpos privados (como os provedores de serviço de Internet – ISP, em inglês), que desempenham um papel crucial na sociedade atual.

A experiência de certos países europeus – particularmente a Alemanha, Romênia e República Tcheca – indica um momento peculiar na história, no qual, mesmo no combate ao terrorismo (e ciberterrorismo), o uso de investigações "baseadas em computadores" e o acesso a dados informáticos e informações, devem se ajustar com a necessidade de avaliação e colheita de provas e o respeito aos direitos fundamentais. Contudo, não se deve confundir "limites constitucionais" da lei com possíveis limites ontológicos das medidas "tecnológicas" ou da retenção de dados. Em outras palavras, esses precedentes declararam inconstitucionais *as leis estabelecendo tais medidas*.

4. A EXPERIÊNCIA ALEMÃ

Nesse contexto, os julgados do Tribunal Constitucional Alemão (*Bundesverfassungsgericht)* de 27.02.2009, acerca da investigação on-line (*Online Durchsuchung)* e de 02.03.2010, acerca da *retenção de dados*, são, indubitavelmente, dois precedentes momentosos.[18]

Na sua primeira decisão, a Corte Constitucional Alemã declarou inconstitucional o § 5 co. 2, n. 11, da Lei de Proteção da Constituição da Renânia

18. BVerfG 370/07 –595/07, 27.02.2008, *CR*, 2008, 306 and 1 BvR 256/08, 1 BvR 263/08, 1 *BvR* 586/08, in [www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html]. Ver FLOR, Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung. *Riv. trim. dir. pen. ec.*, 3 , 2009 , 695; FLOR, Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht: la decisione del 27 febbraio 2008 sulla Online Durchsuchung e la sua portata alla luce della sentenza del 2 marzo 2010 sul data retention, *Ciberspazio e diritto*, 11, 2 , 2010 , 359, com mais referências.

do Norte-Vestfália (*Gesetz über den Verfassungsschutz in Nordrhein-Westfalen – VSG* – como emendada em 20.12.2006), no que tange à colheita e processamento de dados pessoais de usuários, particularmente de sistemas informáticos e da Internet.

Com a segunda decisão, todavia, o *Bundesverfassungsgericht* declarou inconstitucionais os §§ 113a e 113b da *Telekommunikationsgesetz* (TKG, como alterada pelo art. 6, n. 6, da reforma da lei do setor de telecomunicações, promulgando a Diretiva 2006/24/EC, alterando a Diretiva 2002/58/EC) e § 100g, co. 1, primeira parte, StPO, em função de sua inconsistência com o art. 10, co. 1, do *Grundgesetz* (GG). Tal caso dizia respeito às normas igualmente adotadas para enfrentar as ameaças de terrorismo internacional (BGBl I S. 3083, 25.12.2008), que dispunha da retenção de dados por um período de seis meses, independentemente de condições fáticas relacionadas à preparação ou cometimento de tais crimes.

4.1 A decisão do Bundesverfassungsgericht *acerca do* Online *Durchsuchung*

§ 5 co. 2, n. 11VSG, que constituía o embasamento legal para definir o *Online Durchsuchung*,[19] autorizava uma "agência de inteligência para proteger a Constituição" (*Verfassungsschutzbehörde*), a executar dois tipos de ações investigativas: primeiro, monitoramento e reconhecimento secreto da Internet ("alternativa 1"); e, segundo, o acesso secreto à sistemas de tecnologia da informação usando infiltrações técnicas e/ou acesso ("alternativa 2").

A Corte Constitucional Alemã sustentou que as normas regulando o uso de sistemas de "vigilância" ou "monitoramento" de atividades de usuários devem respeitar os direitos fundamentais dos indivíduos delineados no art. 1.º, § 1.º, da Constituição alemã (*Grundgesetz*-GG) (a dignidade humana é inviolável; é dever das autoridades estatais respeitá-la e protegê-la); no art. 2, co. 1, GG (qualquer um tem o direito do livre desenvolvimento de sua personalidade, enquanto não viole o direito de outros, a ordem constitucional e a lei moral); e, enquanto manifestações do direito comum de personalidade (*allgemeine Persönlichkeitsrecht*), no art. 10 da GG (*Das Briefgeheimnis sowie das Post – und Fernmeldegeheimnis unverletzlich*), e no art. 13 (*Die Wohnung ist unverletzlich*).

Nesse caso, a corte sustentou que dois direitos fundamentais são relevantes: 1) o "direito à autodeterminação informativa" – que vai além da proteção da

19. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung* cit.; FLOR, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht* cit.

privacidade e não é limitado a dados confidenciais por natureza. Isso fornece ao indivíduo, em princípio, o poder de determinar por si a disseminação e uso de dados pessoais, mesmo que caracterizados por um conteúdo mínimo, assim estendendo a proteção à liberdade de privacidade em termos de direitos fundamentais;[20] 2) o *direito fundamental de garantir o sigilo e integridade aos sistemas informáticos*, como sistemas informáticos sob investigação podem conter dados pessoais que, pela sua quantidade e caráter, podem facilitar o conhecimento de partes significativas de informações privadas, econômicas, e/ou profissionais de um indivíduo.[21]

Contudo, a Corte Constitucional reconheceu que tais direitos são limitados. As restrições justificam-se tanto pelo propósito de prevenção quando pelo de persecução de tais infrações penais, desde que haja embasamento constitucional.

Em suma, a Corte declarou inconstitucional a lei da *Gesetz über den Verfassungsschutz in Nordrhein-Westfalen*, por causa do conflito com os princípios da clareza (precisão) e determinação (cujas bases estão previstas nos arts. 20 e 28, co. 1, da GG) e no princípio da proporcionalidade. O princípio da proporcionalidade requer que a compressão de direitos fundamentais deve almejar uma finalidade legítima e ser adequada, necessária e apropriada enquanto meio para atingi-la. A Corte admitiu (fazendo explícita referência ao combate ao terrorismo) que a proteção (enquanto o Estado tenha o poder para garantir a paz e a ordem constitucional) e a segurança pública contra ameaças à vida, proteção física e liberdade são valores possuidores de *status* constitucional, os quais devem ser sopesados e avaliados quando são confrontados por valores igualmente altos e interesses contrários.

Resta claro que a compreensão de direitos fundamentais no contexto de um *alvo de prevenção* atende o requisito da adequação somente quando certos fatos, em certo caso, ameaça um interesse jurídico prevalecente, embora não possa ser apurado no momento – e, assim, não pode ser determinado com certeza – que o risco tornar-se-á real no futuro próximo.

Acesso secreto é, portanto, constitucionalmente permitido somente quando é essencial para a tutela destes interesses jurídicos *importantes e prevalecentes*, como a vida, a integridade física e a liberdade individual, ou dos interesses de

20. Sobre direito à própria determinação *Recht auf informationelle Selbstbestimmung*, ver também *BVerfGE 65, 1 <43>; 84, 192 <194>*.

21. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung* cit., FLOR, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht* cit.

determinada comunidade (*Güter der Allgemeinheit*), quando a ameaça a estes atinge as fundações do Estado, sua manutenção, ou as bases da existência humana, inclusive a operação de serviços essenciais. Por óbvio, as investigações devem ser conduzidas de acordo com precauções procedimentais apropriadas estabelecidas por ordem judicial exarada após determinado controle preventivo, com a função de "compensação de representação" (*kompensatorischen Repräsentation*) dos interesses dos indivíduos envolvidos no procedimento.

4.2 A decisão do Bundesverfassungsgericht *acerca da retenção de dados*

A recente decisão da Corte Constitucional Alemã[22] acerca da retenção de dados considerou a questão da constitucionalidade dos §§ 113a e 113b do *Telekommunikationsgesetzes* (*TKG*) e do § 100g, co. 1, primeira parte, do StPO.

A Corte sustentou que os §§ 113a e 113b da *TKG*, conforme alteração do art. 2.°, n. 6, da lei de reforma do setor de telecomunicações (*Gesetzes zur Neuregelung Telekommunikationsüberwachung und der anderer verdeckter Ermittlungsmaßnahmen*) e a implementação da Diretiva 2006/24/EC, de 21.12.2007 (*Bundesgesetzblatt Teil I Seite 3198*), são inconstitucionais por inconformidade com o art. 10, § 1.°, da GG.

Ademais, o § 100g, co. 1, primeira parte, conforme alterado pelo art. 1.°, n. 11, da lei de reforma do setor de telecomunicações e das outras medidas investigativas sigilosas (*Gesetzes zur Neuregelung Telekommunikationsüberwachung und der anderer verdeckter Ermittlungsmaßnahmen*), e a implementação da Diretiva 2006/24/EC, foram considerados, por conexão com a aquisição de tráfico de dados telemáticos, conforme determinado no art. 113 da *TKG*, incongruentes com os arts. 1.° e 2.° da GG, bem como com o art. 10, co. 1, do mesmo diploma.

Destarte, os dados armazenados com base em tais provisões devem ser cancelados e não poderão serem transmitidos para as autoridades solicitadoras.[23]

---

22. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, in: [www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html]. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung* cit., FLOR, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht* cit.; FLOR, Data retention e limiti al potere coercitivo dello Stato in materia penale: le sentenze del Bundesverfassungsgericht e della Curtea Constituţională, *Cass. pen.*, 5 , 2011, 1952-1969, com mais referências.

23. Mais especificamente, o desafio de demanda constitucional § § 113a, 113b da Lei das Telecomunicações (*Telekommunikationsgesetz* – TKG) e § 100g do Código de

Embora a maioria dos provedores de serviços públicos de comunicação eletrônica sejam partes privadas, estão engajados em atividades de importância pública em cooperação com as autoridades estatais e, por meio de legítimos

---

Processo Penal (*Strafprozessordnung* – StPO), na medida em que este último permite a recolha de dados armazenados nos termos do § TKG 113a. O § 113a TKG prevê que os provedores de serviços de telecomunicações acessíveis ao público têm o dever de guardar praticamente todos os dados de tráfego de serviços de telefone (rede fixa, comunicações móveis, fax, SMS, MMS), serviços de e-mail e serviços de Internet sem ocasião, a título de precaução. O dever de armazenamento essencial estende a toda a informação que é necessário a fim de reconstruir quem comunicou ou tentou se comunicar, quando, por quanto tempo, para quem e a partir de onde. Em contraste, o conteúdo da comunicação e, consequentemente, os detalhes de quais páginas da Internet foram visitadas pelos utilizadores, não são para ser armazenadas. Depois dos seis meses em que existir o serviço de armazenamento, os dados serão eliminados dentro de um mês. O § 113b TKG regula os efeitos possíveis para o qual esses dados poderem ser utilizados. Essa disposição é uma disposição de referência: ela própria não contém uma autorização de recuperação de dados, mas apenas amplamente designa utilizações previstas que são possíveis em geral, que são para ser colocadas em termos concretos, por disposições de ramos específicos da lei aprovada pelo Governo Federal e os estados. Na frase 1, primeira parte, os efeitos possíveis da utilização direta dos dados são listados: a repressão de infracções penais, a afastar dos perigos significativos para a segurança pública e do desempenho de tarefas de inteligência. A segunda parte permite, além disso, o uso indireto dos dados de informação nos termos do § TKG 113,1 na forma de uma reivindicação de informações dos prestadores de serviços, a fim de identificar os endereços IP. Esse prevê que se as autoridades já sabem um endereço IP – por exemplo, de uma queixa-crime ou de suas próprias investigações – podem exigir informações sobre o usuário a quem esse endereço foi alocado. O legislador permite isso para os efeitos da repressão de infracções penais e contra-ordenações e afastar do perigo, independentemente de definições mais específicas; neste contexto, não há nem uma exigência de autoridade judicial, nem um direito de notificação. O § 100g StPO colocando § sentença 113b 1 primeira parte, 1 número 1 TKG em termos específicos rege o uso direto para o processo criminal dos dados armazenados por precaução. Mas, tomado como um todo, a prestação é mais ampla e governa todo o acesso aos dados de tráfego de telecomunicações que seja. Isso, portanto, permite – e originalmente apenas permitiu – o acesso a dados de conexão que são armazenados pelos prestadores de serviços por outras razões (por exemplo, a fim de realizar transações comerciais). Ele permite, até mesmo, os dados acumulados serem usados de forma independente duma lista exaustiva de infrações penais de peso substancial e, para além disso, de acordo com um exame da proporcionalidade com base no caso individual, também serem usados geralmente para processar delitos que são cometidos por meios de telecomunicações. Anteriormente, deve haver uma decisão do juiz e o Código de Processo Penal também prevê deveres de notificação judicial e, subsequentemente, medidas judicias a esse respeito.

atos destas, representam a manifestação do poder coercitivo estatal *in subiecta materia*.

As previsões acerca do armazenamento de informação por um período de 6 meses são compatíveis com o art. 10 da GG em termos absolutos e o armazenamento de tais dados por provedores de serviços não está impedido *ab origine* se tais disposições estão integradas em uma estrutura legal "apropriada", i.e., uma estrutura apta a satisfazer o princípio da proporcionalidade. As expressões de inconstitucionalidade, assim, versam principalmente acerca da função do armazenamento de dados, que não é afetada por condições específicas, diz respeito a todos os usuários e á adequada, indiscriminadamente, a qualquer dado.

Tais operações, embora não envolvam o conteúdo das comunicações, afetam a esfera íntima de indivíduos, e são potencialmente aptas a captar informações confidenciais (como preferências e inclinações políticas ou pessoais), resultando no registro e a elaboração de "perfis" de usuários.

Em outras palavras, tal atividade envolve o risco, por um lado, de iniciar ou aprofundar investigação sobre um indivíduo ou mais, sem que lhes seja dado motivo e, por outro, de abuso por tais autoridades.

Na opinião dos magistrados, é essencial não só a previsão de condições, mas também a adoção de medidas de segurança proporcionais, aptas a garantir um critério elevado, cuja avaliação e implementação não pode ser deixada à apreciação pessoal do provedor ou ser dependente de meros critérios econômicos. Quando apropriado, deverá ser fornecido um órgão *ad hoc* para a regulação de critérios técnicos.

O legislador deve explicitamente expor os pressupostos, tipo, natureza e nível das medidas segurança e os limites no uso de dados.

A Corte decidiu que um prévio requisito para legitimar a limitação em direitos fundamentais é a existência de um perigo real para a vida ou a liberdade pessoal dos indivíduos ou, ainda, para a segurança da Federação ou do território.

Em conjunto com a obrigação de reter dados, o legislador deve proporcionar, assim, uma exaustiva lista de infrações relacionadas aos bens específicos e relevantes a serem protegidos.

O uso e transmissão dos dados armazenados devem ser sujeitos ao controle da autoridade judicial. Ainda, no contexto da discricionariedade legislativa, a lei pode requerer que certa informação seja fornecida independentemente dos limites fornecidos ou impostos por crimes específicos ou por uma lista de atos ilícitos ou de interesses jurídicos, com base em autorizações comuns fornecidas por disposições legais específicas.

Com respeito ao limite de interferência, de acordo com os magistrados deve ser garantido que a informação não é coletada ao acaso, mas somente o que diz respeito com o objetivo dado ou um perigo real, com base nos fatos do caso concreto.

Em relação ao uso indireto de endereços de IP, contudo, as cortes tem especificado que não é nem necessário fornecer critérios rigorosos para tais informações, nem rigorosa requisição judicial do pedido. Em qualquer caso, os indivíduos envolvidos devem ser informados quando esses dados são processados e/ou coletados.[24]

De especial importância é o voto dissidente do Juiz Schluckebier, que sustenta que a obrigação de reter os dados por um período de 6 meses não é inconsistente com o direito fundamental tutelado pelo art. 10, § 1.º, da GG. Por razões técnicas, o tráfico de dados permanece na "região" do ISP, dentro de seus servidores, e usuários confiam, com base na relação contratual, que os dados são protegidos e tratados com estrito sigilo. Uma vez que sejam adotadas medidas de segurança atualizadas, não há fundamento objetivo para arguir que o usuário possa sofrer restrições relevantes a direitos fundamentais, considerando, também, que o armazenamento não se estenda ao conteúdo das comunicações.

Em essência, as disposições contestadas não seriam inapropriadas, pois razoáveis e proporcionais.

A partir de tal voto dissidente, podemos inferir que na relação conflitante entre a obrigação do Estado em proteger interesses jurídicos e o interesse indi-

24. Mais especificamente, no entanto, a criação de direitos oficiais à informação, a fim de identificar os endereços de IP é também de importância considerável. Ao fazer isso, o legislador influencia as condições de comunicação na Internet e limita o seu anonimato. Nesta base, em conjunto com o armazenamento sistemático de dados de acesso à Internet para endereços IP previamente definidos, é possível, em grande medida, para determinar a identidade dos utilizadores da Internet. Dentro do critério legislativo tem, nesse contexto, o legislador também pode permitir que essa informação seja dada, mesmo independentemente dos limites impostos por delitos específicos ou por listas de interesses jurídicos, para a repressão de infracções penais, para o afastar do perigo e para o desempenho de funções dos serviços de inteligência, com base em autorizações gerais para invadir prestados por ramos específicos do direito. É certo que, no que respeita ao limite de interferência, é necessário assegurar que a informação não é obtida de forma aleatória, mas apenas a partir de uma suspeita suficiente inicial ou de um perigo com base em fatos relacionados ao caso individual. Para esse tipo de informação, não é necessário prever uma exigência da autoridade judicial, no entanto, as pessoas afetadas devem ser informadas quando tal informação é obtida.

vidual em proteger os direitos garantidos pela Constituição, cabe ao legislador garantir o equilíbrio em tal conflito. Deve-se, outrossim, considerar a eficaz e constitucional administração da Justiça à luz das mudanças provocadas por novas tecnologias e novas formas de comunicação.

Em conclusão, embora a importância dos interesses a serem protegidos é, *per se*, suficiente para justificar a compressão de direitos fundamentais, os princípios constitucionais exigem que a restrição a tais direitos seja cumprida por intermédio de uma regra que exige elevado padrão de clareza e é obrigatória por sua natureza. O objetivo deve almejar um fim legítimo e ser adequado, necessário e apropriado como meio para atingi-lo, enquanto respeitando o princípio da proporcionalidade.

5. A EXPERIÊNCIA ROMENA

A decisão da *Curtea Constituțională* romena de 08.10.2009[25] tratou com questões similares àquelas que foram objetos da recente decisão do *Bundesverfassungsgericht* envolvendo retenção de dados.

Ambas as Leis 398/2008 aplicando a Diretiva 2002/58/EC (que altera a Diretiva 2002/58/EC), e 506/2004 incluíram a obrigação dos provedores de serviços públicos de comunicação eletrônica de armazenar dados gerados ou processados durante suas atividades, com o objetivo de torná-los disponíveis às autoridades competentes na eventualidade de investigações e procedimentos contra infrações graves.

Os Juízes invocaram o reconhecimento internacional do direito à privacidade e vida familiar, protegido pelo art. 26 da Constituição da Romênia, como disposto no art. 12 da Declaração Universal dos Direitos Humanos, no art. 17 do Pacto Internacional sobre Direitos Civis e Políticos, e no art. 8.º da Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais.

Contudo, tais direitos, incluindo a liberdade de expressão, com expressão no art. 30 da Constituição da Romênia e no art. 10 da Convenção, não são absolutos. Nesse contexto, nem a Convenção para a Proteção dos Direitos do Homem e das liberdades fundamentais nem a Constituição nacional proíbem decisões legislativas limitando direitos fundamentais. Tais limites, contudo,

25. Ver *Decizia* 1258 del 8 ottobre 2009, in *Monitorul Oficial* n. 798 – 23 novembre 2009. Ver RINCEANU, Das Urteil des rumänischen Verfassungsgerichtshofs zur Verfassungswidrigkeit der Vorratsdatenspeicherung, *Jahrbuch für Ostrecht*, 2011, 52/1, 49; FLOR, *Data retention e limiti* cit.

são legítimos caso atendam requisitos específicos, em estrita conformidade com o art. 8.º da Convenção e o art. 53 da Constituição da Romênia, e somente no caso da ação legislativa ser voltada à proteção de importantes interesses, os quais podem ser segurança nacional, saúde pública, proteção da ordem pública ou prevenção de crimes. A ação legislativa deve ser necessária, proporcional à situação que a determinou, aplicada de modo não discriminatório e não deve debilitar a existência do direito ou da liberdade fundamental.

A Corte também apontou que a implementação de Diretrizes da União Europeia implica obrigações quanto aos objetivos, mas não em relação aos meios para os alcançar, depositando, destarte, certa discricionariedade nas mãos dos Estados membros.

A Lei 298/2008 reguladora da obrigação, dos provedores de serviços de comunicação eletrônica acessíveis ao público ou de redes públicas de comunicação, de armazenar dados por um período de 6 meses, expressou a vontade do legislador de restringir o exercício destes direitos fundamentais.

A disposição foi declarada inconstitucional por três motivos: 1) fracassou em respeitar o princípio da precisão em determinar o âmbito dos dados necessários para identificar usuários, possibilitando, assim, possíveis abusos na atividade da conservação, tratamento e uso da informação armazenada por provedores de serviços de comunicação eletrônica acessíveis ao público ou de redes públicas de comunicação. As limitações aos direitos fundamentais da confidencialidade, sigilo da correspondência e liberdade de expressão devem, de fato, serem dispostas de um modo claro e inequívoco, a fim de se evitar qualquer avaliação arbitrária pelas autoridades. Os sujeitos afetados pela legislação são membros da sociedade civil e devem estar aptos a compreender as leis aplicáveis a fim de ajustarem suas condutas e estarem cientes das consequências; 2) o legislador não reconheceu o significado da passagem "para a prevenção e diferenciação de ameaças à segurança nacional, instituições estatais (...) pode acessar, sob condições que regulam a atividade da segurança nacional, os dados armazenados por provedores de serviços de comunicação eletrônica acessíveis ao público ou de redes públicas de comunicação"; 3) a Lei 298/2008 estabeleceu, em geral, a regra da retenção de dados por um período de 6 meses, e a obrigação do provedor tem um caráter inerentemente contínuo, onde a Diretiva 2002/58/EC, Lei 677/2001 que dispõe da proteção de dados pessoais e a Lei 506/2004 permitiam limites excepcionais ao direito à privacidade sob as condições específicas dispostas na Constituição e na lei internacional aplicável no caso. Em essência, a Lei 298 "transformou" a exceção em "regra", requerendo armazenamento de dados por um período de 6 meses; tais dados podem ser usados mediante decisão fundamentada da corte "para o

passado e não para o futuro". Ao contrário, a Lei 298/2008, não considera a necessidade de interrupção da limitação e, na opinião dos juízes constitucionais, a instrução no livre exercício dos direitos fundamentais envolvidos toma lugar numa "maneira independente e contínua a partir da ocorrência de um evento que possa justificá-la, a partir de uma causa determinante e somente para a proteção e detecção, após o cometimento de crime grave".

A Corte concordou com o legislador na urgência em garantir proteção adequada e eficaz compatível com o contínuo processo de modernização e de atualização tecnológica do meio. Contudo, ela também notou que as soluções legislativas devem respeitar os direitos dos indivíduos, que podem ser legalmente limitados ou "objetos de restrições" somente em relação à proteção de interesses ou direitos importantes, como os direitos coletivos ou interesses relacionados à segurança pública nacional, ordem pública e prevenção de crimes.

6. A RECENTE EXPERIÊNCIA DA REPÚBLICA TCHECA E A DECISÃO ACERCA DA RETENÇÃO DE DADOS

Em 31.03.2011, a Corte Constitucional da República Tcheca decidiu – nos termos da seção 70, subseção 1 da Lei da Corte Constitucional – afastar as disposições da seção 97, subseções 3 e 4 da Lei das comunicações eletrônicas e alteração de certas leis relacionadas (Lei de Comunicações Eletrônicas), 127/2005, Coll., conforme alterada, e contestou o Dec. 485/2005 Coll. na extensão de tráfico e dados de localização, o tempo de rentenção disso e a forma e método da transmissão de tanto a corpos autorizados a utilizar tais dados.[26]

O art. 1.°, § 1.°, da Constituição da República Tcheca, incorpora o princípio normativo do Estado cumpridor da lei democrática. O respeito a direitos fundamentais e liberdades individuais é o atributo fundamental deste conceito constitucional de estado cumpridor da lei e requisito prévio de seu funcionamento, o qual é explicitamente especificado como um atributo de tal ordem constitucional escolhida na disposição supracitada. A Corte asseverou que tal disposição constitucional forma a base para o conceito material de estato jurídico, o qual é caracerizado pela autoridade pública respeitando a livre (autônoma) esfera dos indivíduos, definida por direitos fundamentais e liberdades. Por uma questão principiológica, a autoridade pública não intervém nessa esfera, ou, mais precisamente, somente em casos onde tal intervenção é justificada pelo conflito com outros direitos fundamentais, que é em interesse público, o

26. Para maiores referências ver FLOR, *Data retention e limiti* cit.

qual está em conformidade com a Constituição, o qual é inequivocamente definido por lei que dispõe que a intervenção, desde que a intervenção prevista em lei respeite o princípio da proporcionalidade e a finalidade não seja tão extensa quanto a redução do direito ou liberdade.

Os juízes, em complemento, asseveraram que o direito à vida privada incorpora, também, a garantia de autodeterminação em termos de decisões cruciais sendo feitas pelo indivíduo. Em outras palavras, o direito à privacidade também garante o direito de um individuo de decidir, pela sua própria discricionariedade, até qual extensão, de quais modos e sob quais circunstâncias fatos pessoais e privados devem ser divulgados a outras entidades. Esse é um aspecto do direito à privacidade em forma do direito à autodeterminação informativa. Dada a sua natureza e importância, a Corte estabeleceu que o direito à autodeterminação informativa enquadra-se na categoria direitos fundamentais e liberdades. Uma vez junto com a liberdade pessoal, liberdade em termos de dimensões espaciais (lar), liberdade de comunicação e certamente outros direitos fundamentais garantidos ela constituição, cria-se a esfera pessoal de um indivíduo, cuja integridade individual há de ser respeitada e consistentemente tutelada enquanto fundamento necessário para a existência digna e desenvolvimento da vida humana enquanto tal. Portanto, é certamente justificado garantir respeito e proteção por ordem constitucional a esta esfera, pois, olhando tal questão de um ponto de vista levemente diferente, ela representa a manifestação do respeito aos direitos e liberdades de humanos e cidadãos.[27]

27. O Tribunal constatou que no seu julgamento relacionado com o direito ao respeito pela vida privada nos termos do art. 8 da Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais, o Tribunal Europeu de Direitos Humanos descreveu ações como dados, conteúdos de controle de e-mail e escutas telefônicas como violação de privacidade de um indivíduo [cf. decisão Klass e outros v. Alemanha (5.029/1971) de 06.09.1978, Leander v. Suécia (9.248/1981) de 26.03.1987, Kruslin v. França (11.801/1985) de 24.04.1990 ou decisão Kopp v. Suíça (23.224/1994) de 25.03.1998], detectação de números de telefone de pessoas no aparelho telefônico [cf. decisão P.G. e J.H. v. Reino Unido (44.787/1998) de 25.09.2001], detectação de dados relativos à ligação telefônica (cf. acima mencionada decisão Amã v. Suíça) ou retenção de dados em bancos de dados de DNA de indivíduos acusados de um delito [cf. S. decisão Marper v. Reino Unido (30.562/2004 e 30.566/2004) de 04.12.2008]. Na decisão Rotaru v. Roménia (28.341/1995) de 04.05.2000, o Tribunal Europeu de Direitos Humanos deduziu a obrigação positiva do Estado para descartar dados relativos à esfera privada de um indivíduo, que foram coletadas e processadas pelo estado, a partir do direito à vida privada manifesta por meio do direito de autodeterminação informativa.

Os juízes tem feito expressa referência às decisões da Corte Constitucional, ou Suprema Cortes, da Alemanha,[28] Romênia, Bulgária e Chipre.[29]

A partir do ponto de vista da Corte, o propósito primário da regulação legal da universal e preventiva coleta e retenção de tráfico e dados de localização em comunicações eletrônicas é a proteção contra ameaças à segurança e a necessidade de assegurar a disponibilidade de tais dados para propósitos de precaução, detecção, investigação e persecução de crimes graves, conduzidas pelas autoridades públicas. A persecução de crimes e a punição justificada de infratores é um interesse público aprovado pela Constituição, cuja essência é a delegação de responsabilidade a pessoas físicas e entes estatais, da incumbência de responsabilizar agentes por infrações substanciais a direitos fundamentais e a liberdades. Se o direito penal deve permitir a condução do interesse público na persecução da criminalidade por intermédio de instrumentos robustos, o uso dos quais resulta em sérias violações da integridade pessoal e direitos fundamentais e liberdades de um indivíduo, então o limite constitucional legal deve ser respeitando enquanto tal execução acontece. Violações de integridade ou privacidade pessoais (i.e., ausência de respeito por estas) podem, assim, ocorrer somente em circunstâncias extremamente excepcionais pela parte da autoridade pública. Isso deverá ser inevitável numa sociedade democrática no caso do propósito do interesse público não possa ser atingido por qualquer outro modo, e deverá ser aceitável somente de

28. "Abordagem semelhante é fácil de encontrar também no juízo dos tribunais constitucionais de outros países. Por exemplo, o acima mencionado Tribunal Constitucional Federal da Alemanha garante – por meio do direito à autodeterminação informativa – a proteção não só do conteúdo da informação transmitida, mas também das circunstâncias externas na qual a comunicação ocorreu – ou seja, lugar, tempo, participantes, tipo e forma de comunicação – uma vez que tais informações sobre as circunstâncias de uma dada comunicação podem, combinadas com outros dados, indicar os conteúdos transmitidos como tais; ao inspecionar e analisar esses dados, é possível criar perfis individuais dos participantes envolvidos na comunicação [cf. decisão de 27.07.2005, BVerfGE 113, 348 (*Vorbeugende Telekommunikationsüberwachung*) ou 27.02.2008, BVerfGE 120, 274 (*Grundrecht auf Computerschutz*)".

29. "O Tribunal Constitucional romeno chegou a conclusões semelhantes no seu acórdão de 08.10.2009 (1.258), que considera inconstitucional a local regulamentação legal, uma vez que não define a finalidade da utilização de tal medida suficientemente, seu texto é muito vago e não define, em mais detalhes, os poderes e deveres dos intitulados autoridades públicas e concede aos indivíduos afetados, devido à ausência de controle judicial, garantias suficientes contra a utilização indevida (...), mais adiante, o Supremo Tribunal Administrativo búlgaro no julgamento de 11.12.2008 (...), bem como o Supremo Tribunal chiprense no jul de 01.02.2011 (...)".

acordo com a existência legal e observância das efetivas e especificas garantias contra arbitrariedades.

As disposições contestadas da Lei das comunicações eletrônicas, seção 97, subseção 3, sentença 3, vagamente especificam a obrigação de pessoas jurídicas ou físicas que retêm tráfico e dados de localização na extensão supracitada, para "tornar tais dados disponíveis sob requisição dos órgãos intitulados a requisitá-los com fulcro em regulação jurídica especial" sem qualquer atraso. Na opinião da Corte Constitucional, não resta claro na redação das disposições da Lei de comunicações eletrônicas, nem em sua exposição de motivos, quais órgãos intitulados e qual regulação jurídica especial são especificamente compreendidos.

Ademais, o propósito de transmitir tráfico e dados de localização a órgãos intitulados não é clara e precisamente definido, o que torna impossível determinar até qual extensão as disposições contestadas são realmente necessárias.

Em relação à finalidade de tornar tais dados "disponíveis para o propósito de investigação, detecção e persecução de crimes graves" (mesmo que não se define tais crimes com maiores detalhes), nem as disposições contestadas, nem as citadas do Código Penal (seção 88a, subseção 1 – regulando condições do uso de dados retidos para o propósito de persecução criminal) cercam tais limitações. Nos termos desta norma, o legislador não condiciona a opção de usar dados retidos em procedimentos criminais por justo receio que um crime grave tenha se consumado. Ao mesmo tempo, não há regulação acerca da obrigação das autoridades envolvidas em procedimentos criminais de informarem o indivíduo (monitorado) acerca disso, nem sequer *ex-post*, o que não se enquadra nos requisitos resultantes do segundo passo do exame de proporcionalidade (i.e., a necessidade dos meios, desde que resta claro pelo suprarreferido que o meio mais respeitoso ao direito fundamental à autodeterminação informativa não fora utilizado).

A Corte Constitucional também considerou que as normas jurídicas contestadas pelos peticionantes não definem suficientemente regras claras e detalhadas contendo requisitos mínimos para a segurança dos dados retidos (especialmente quanto à prevenção do acesso por terceiros, definição de procedimentos resultantes na proteção da integridade e confidencialidade dos dados e um procedimento para descartar os dados.[30]

30. Sobre o período de retenção, a mera definição de "não inferior a seis meses e não mais que 12 meses", dado o lapso indicado nesse prazo, influencia a obrigação de descartar os dados, pode ser considerada ambígua e, com respeito ao âmbito e à natureza con-

Em conclusão, meramente na forma de *obiter dicta*, a Corte Constitucional declarou que o desenvolvimento de tecnologia da informação moderna e meios de comunicação andam de mãos dados com novas e mais sofisticadas modalidades de atividades criminosas com as quais temos que lidar. Contudo, a Corte Constitucional duvida que o instrumento de tráfico e retenção de dados universal e preventivo em quase toda comunicação eletrônica seja, sozinho, um instrumento necessário e apropriado, em decorrência do nível de violação à privacidade que envolve um enorme número de indivíduos em comunicações eletrônicas.[31]

---

fidencial dos dados retidos, totalmente insuficiente. Nenhuma das obrigações mencionadas faz descrever as regras ou os métodos de encontra-las com mais detalhes, não há uma definição rigorosa dos requisitos em matéria de segurança dos dados conservados, não é totalmente rastreável como os dados são manipulados nem por parte de pessoas jurídicas ou pessoas naturais de retenção de tráfego e dados de localização, nem as entituladas autoridades públicas depois de solicitar os dados, nem o caminho do descartamento de tais dados é definido. Mais adiante, não há uma definição de responsabilidade e respectivas sanções em caso de violação de tais obrigações, incluisive faltando a criação da maneira como os indivíduos afetados podem buscar proteção eficaz contra possível uso indevido arbitrariedade ou não cumprimento das obrigações definidas.

31. Dentro da área da Europa, tal opinião é, de longe, não isolada a partir do momento em que a Directiva de Retenção de Dados, em si, tem sido muito criticada desde o início de sua existência por parte dos Estados-membros (por exemplo, os governos da Irlanda, Países Baixos, Áustria e Suécia hesitaram muito tempo ou ainda estão hesitando a sua implementação, a exemplo dos últimos dois países mencionados acima, apesar de uma ameaça anunciada em público pela Comissão Europeia de inciar processo perante o Tribunal Europeu de Justiça), bem como legisladores no Parlamento Europeu, a Autoridade Europeia para a Protecção de Dados (3 December, 2010 [www.dataretention2010.net/docs.jsp]) ou o Partido Protecção de Dados, criado nos termos do art. 29 da Diretiva 95/46/EC ou organizações não governamentais (Statewatch, European Digital Rights ou Arbeitskreis Vorratsdatenspeicherung – AK Vorrat entre outros). Ao contrário, ao menos em parte, o relatório de avaliação sobre a Directiva relativa à conservação de dados (Directiva 2006/24/CE) – Bruxelas, 2011/04/18 COM (2011) 225 final. O relatório específico demonstrou que a retenção de dados é uma ferramenta valiosa para os sistemas de justiça criminal e para aplicação da lei na União Europeia. A contribuição da diretiva para a harmonização de retenção de dados tem sido restringida em termos de, por exemplo, limitação da finalidade e dos períodos de retenção, assim como também na área de reembolso de custos incorridos pelos operadores, que está fora de seu escopo. Dadas as implicações e riscos para o mercado interno e para o respeito ao direito à privacidade e à protecção de dados pessoais, a UE deve continuar por meio de regras comuns a assegurar que os padrões elevados para o armazenamento, recuperação e uso de tráfego e dados

7. CONCLUSÕES: RUMO A UMA NOVA PERSPECTIVA EUROPEIA?

A partir dos fundamentos do julgamento das Cortes Constitucionais da Alemanha, da Romênia e da República Tcheca ganhamos alguns importantes critérios que podem ser úteis no tratamento com as novas ferramentas de investigação tecnológica para combater ou prevenir atos de ciberterrorismo.

De qualquer modo, devemos primeiro indicar alguns elementos notórios no fundamento das decisões:

1) o explícito ou implícito reconhecimento do papel essencial dos provedores de serviço de Internet, que podem também realizar atividades de importância pública.[32] Portanto, os limites e proteções conectadas com a conduta dessa operação não podem ser deixadas a suas apreciações subjetivas, mas elas devem ser impostas pelo legislador;

2) a intenção preventiva de instrumentos novos de investigação e a utilidade prática – em processos ou investigações criminais – do armazenamento de dados dos usuários. Essas medidas são válidas para os sistemas de justiça criminal e para a execução legal na União Europeia;

3) As Cortes endereçaram a questão da legitimidade em consideração ao significado de investigação, armazenamento e controle do tráfico eletrônico

---

de localização são consistentemente mantido. À luz destas conclusões, a Comissão pretende propor alterações à directiva com base em uma avaliação de impacto.Ver também, FLOR, The de jure condendo perspectives of the s.c. data retention in the Cloud Scenario: ontological limits, constitutional limits and protection of fundamental rights, *Conventional and Constitutional Limits of the "European Criminal Law" after the Treaty of Lisbon - The Debate in Germany and in Italy* (international conference), Verona, 17.09.2011. Um exemplo determinante, neste contexto global e tecnológico, é também o uso das redes sociais para fins investigativos ou vigilância: ver NIETO; MAROTO, Redes sociales en internet y "data mining" en la prospección e investigación de comportamientos delictivos, paper, *UCLM* [www3.uclm.es], 2010; SEMITSU, From facebook to mug shot: how the dearth of social networking privacy rights revolutionized online government surveillance, 31 *Pace L. Rev.*, 2011, 291; O'FLOINN; ORMEROD, Social networking sites, ripa and criminal investigations, *Crim. Law Rev.*, 10, 2011, 766-789.

32. Sobre a importância dos ISPs e do equilíbrio com os direitos fundamentais ver também as diretrizes de direitos humanos para provedores de serviços de Internet do Conselho da Europa em cooperação com a Comissão Europeia Internet Services Providers Association – (EuroISPA), ver FLOR, *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet. Un'indagine comparata in prospettiva europea ed internazionale*, Padova, 2010, 418.

em respeito à proteção dos direitos humanos fundamentais, concluindo que não há proibição absoluta em soluções legislativas limitando essas restrições de direitos;

4) a qualificação de intervenções públicas na área dos direitos individuais não deve ser apenas estabelecida pelo direito, mas a restrição não deve exceder o limite da estrita necessidade em relação com os propósitos essenciais para a vida da sociedade democrática, entre os quais se inclui a identificação e punição dos autores de crimes graves.

Em conclusão, ações legislativas que podem restringir os direitos fundamentais devem ser consideradas apenas legítimas em casos nos quais elas são proporcionais e voltadas a proteger importantes e dominantes interesses jurídicos. O legislador deve balancear os interesses em conflito e adotar uma clara, precisa e inteligível regra, ou seja, uma regra que respeite altos critérios de certeza, precisão e transparência. A regra deve estabelecer de uma forma rigorosa as condições para a restrição dos direitos fundamentais envolvidos, a avaliação da qual deve ser cominada num corpo independente.[33]

A legitimidade da luta contra o terrorismo, o ciberterrorismo e os crimes cibernéticos não pode, todavia, ignorar a regra da excepcionalidade. Em outras palavras, a evolução do direito penal não pode se mover em direção a tendências autoritárias, mas deve sempre garantir a aplicação dos princípios fundamentais, como *ultima ratio*, proporcionalidade e respeito dos direitos humanos e das liberdades fundamentais. [34]

Em âmbito europeu, em 24.02.2005, com referência à luta contra os crimes cibernéticos, foi aprovada a Decisão-Quadro 2005/222/JAI relativa a ataques contra sistemas de informação. Considerando o n. 5, lê-se: "As consideráveis lacunas e diferenças entre as legislações dos Estados-Membros neste domínio podem entravar a luta contra o crime organizado e o terrorismo, e pode complicar a efetividade da cooperação policial e judiciária em matéria de ataques contra sistemas de informação". Segundo o Conselho, "o carácter transnacional dos modernos sistemas de informação", ressalta "a necessidade urgente de novas medidas de aproximação das legislações penais neste domínio".

---

33. Esta perspetiva tem sido objeto da resolução "especiais medidas processuais para proteger os direitos humanos fundamentais", aprovada pelo IAPL-AIDP durante o XVIII Congresso Internacional em Istambul (20 a 27.09.2009), que forneceu recomendações específicas sobre a questão das inestigações investigações "proativas" com vista à prevenção da preparação e da prática de infrações terroristas.

34. Ver também o art. 21 da Convenção sobre os Crimes Cibernéticos.

Considerando que n. 8 afirma que a "o direito penal, na área de ataques contra sistemas de informação, deve ser aproximado de forma a assegurar a melhor possibilidade de cooperação policial e judicial em matéria de crimes relacionados a ataques contra sistemas de informação e contribuir para a luta contra o crime organizado e terrorismo".

A entrada em vigor do Tratado de Lisboa, em 01.12.2009, abriu subsequentemente novos horizontes para o "direito penal europeu". Uma das principais inovações foi a superação da distinção entre o primeiro pilar e o terceiro pilar. O espaço de liberdade, segurança e justiça, para qual o Título V do Tratado – sobre o "Funcionamento da União Europeia" – é dedicado, foi incluído entre as matérias reguladas por atos típicos de direito comunitário (diretivas).

O novo art. 83 do Tratado sobre o Funcionamento da União Europeia estabelece que "O Parlamento Europeu e o Conselho da Europa, por meio de diretivas adotadas de acordo com o processo legislativo ordinário, podem estabelecer regras mínimas relativas à definição das infrações penais e das sanções em domínios de criminalidade particularmente graves com dimensão transfronteiriça resultante da natureza ou do impacto de tais infracções, ou a partir de uma necessidade especial para os combater em uma base comum". Entre essas áreas de criminalidade, criminalidade cibernética, terrorismo, e o crime organizado estão expressamente incluídas.[35]

Ciberterrorismo, portanto, nos significados que examinamos até agora, pode muito bem se enquadrar entre estas formas de criminalidade transnacional grave ou, pelo menos, nas áreas de "crime cibernético" e "terrorismo".

O Tratado de Lisboa prevê, junto com um reconhecimento expresso de competências da União em matéria penal por meio do uso de diretivas, um certo número de disposições de "natureza processual", como fortalecimento do papel da Eurojust e da Europol. Ele também oferece a possibilidade de criação de um Ministério Público Europeu e os instrumentos de cooperação policial, com o objetivo de estabelecer medidas em relação à recolha, armazenamento e processamento de dados e informações, e técnicas compartilhadas de investigação para identificar as formas graves de criminalidade organizada.

Neste contexto, a Comissão Europeia apresentou duas novas medidas contra os ataques a importantes sistemas de informação: uma proposta de diretiva

35. Depois do Tratado de Lisboa ver GERCKE, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU. The redefined role of EU and the change in approach from patchwork to comprehensiveness, *Cri*, 3/2010, 75; GERCKE, Die Entwicklung des Internetstrafrechts 2009/2010, *ZUM*, 2010, 633.

relativa a ataques contra sistemas de informação, que revoga a Decisão-Quadro de 2005 acima mencionada[36] e uma proposta de regulamento para fortalecer e modernizar a Agência Europeia para a Segurança da Informação (Enisa). As duas iniciativas têm sua base na Agenda Digital Europeia[37] e no Programa de Estocolmo para aumentar a confiança e segurança de rede.[38]

A proposta de diretiva, em particular, mantém as disposições da Decisão-Quadro relativa a criminalizar o acesso ilegal a sistemas informáticos e a interferência de sistema e dados ilegais (corrupção de dados, informações, programas ou sistemas), acrescentando, em termos de direito penal material, a criminalização de ferramentas destinadas a cometer um crime, a interceptação ilegal de dados e informações e, em termos de cooperação internacional, as regras para melhorar a justiça criminal e cooperação entre os Estados.

Prima facie essas disposições estão em linha com as previsões da Convenção sobre o cibercrime, já ratificadas pela maior parte dos países europeus.

Portanto, após a aplicação do Tratado de Lisboa, as bases para a criação de uma harmonização racional e orgânica em matéria penal e de prevenir e combater a criminalidade grave – como o terrorismo, ciberterrorismo e crimes cibernéticos – foram estabelecidas.

Um papel importante é desempenhado pela investigação "tecnológica".

Na estrutura atual da sociedade da informação e Internet, de fato, não podemos pensar enfrentar os desafios colocados pelas novas tecnologias, quando são utilizados para a prática desses crimes graves, apenas com os meios tradicionais de investigação. Temos que levar em conta a necessidade de uma discussão ampla e variada sobre a adoção de novas ferramentas, que também têm uma função preventiva, evocando o caráter absoluto dos direitos fundamentais.

A questão diz respeito aos limites dentro dos quais o legislador (nacional e europeu) pode operar em prejuízo dos direitos fundamentais e na luta contra o terrorismo, ciberterrorismo e crimes cibernéticos.

Em termos estruturais, toda a liberdade é um elemento essencial da ordem fundamental constitucional e qualquer direito fundamental sofre limitações em matéria de proteção dos direitos de outros de igual importância, que fazem parte, por sua vez, da regulamentação. Consequentemente, um núcleo invio-

36. Ver a proposta de diretiva relativa a ataques contra sistemas de informação, Memo/10/463 (2010/09/30).

37. Com 2010/245/def.

38. Programa de Estocolmo (2010/C 115/01).

lável deve ser identificado à luz desta relação entre direitos e liberdades fundamentais, nomeadamente na restrição da última possibilitando a realização de outros valores constitucionais.[39]

A este respeito, o art. 52 da Carta dos Direitos Fundamentais da União Europeia,[40] considerando o equilíbrio entre direitos, identifica no princípio da proporcionalidade a diretriz fundamental, tanto em termos de interpretação e escolhas político-normativo do legislador, destacando a área de discricionariedade.

Os desafios colocados pelos novos fenômenos criminais – como ciberterrorismo e crimes cibernéticos – exigem um processo de escolhas políticas em matéria penal, que não pode ser comparado com a viagem de Raphael Hythlodaeus para a ilha de Utopia, uma *societas perfecta*.[41]

A inata natureza transnacional do terrorismo, ciberterrorismo e dos crimes cibernéticos implica a necessidade de uma resposta abrangente e oportuna, que deve começar a partir da convicção de que a tecnologia é o resultado da atividade humana criativa, é neutra na sua natureza, assim como destinada a evoluir.[42]

---

39. DENNINGER, Zum Begriff des Wesensgehaltes in der Rechtsprechung (art. 19, co. 1 GG), *Die öffentliche Verwaltung*, 13, 1960, p. 812 e ss. Vedi anche EPPING, *Grundrechte*, 3. Auf., Springer, 2007. HÄBERLE, *Le libertà fondamentali nello Stato costituzionale*, Carocci, 2005.

40. Ver art. 6, par. 2 e 3, TUE. Sobre o Tratado de Lisboa e Direito Penal ver HERLIN KARNELL, The Lisbon Treaty. A critical analysis of Its Impact on EU Criminal Law, *Eucrim*, 2010, 59; HERLIN KARNELL, The Lisbon Treaty and the area of criminal law and justice, *EPA*, 2008, 1; CERIZZA, *Solutions offered by the Lisbon Treaty*, *Eucrim*, 2010, 65; MITSILEGAS, The third wave of third pillar law: Which direction for EU Criminal Justice?, *ELR*, 2009, 523; LANDENBURGER, Police and criminal law in the Treaty of Lisbon. A new Dimension for the Community Method, *ECLR*, 2008, 20. See also PEERS, Eu Criminal Law and the Treaty of Lisbon, 33 *ELR*, 2008, 507; BERNARDI, All'indomani di Lisbona: note sul principio europeo di legalità penale, *Quad. cost.*, 2009, 37; SIEBER, Rechtliche Ordnung in einer globalen Welt, *Rechtstheorie Bd. 41, Heft 2*, 2010, 151; SIEBER, Die Zukunft des Europäischen Strafrechts – Ein neuer Ansatz zu den Zielen und Modellen des europäischen Strafrechtssystems, *ZStW*, 2009, 1. Mais recentemente GRASSO, Il Trattato di Lisbona e le nuove competenze penali dell'Unione Europea, *Studi in Onore di Mario Romano*, Napoli, 2011, 2307-2350 e, em geral, GRASSO; PICOTTI; SICURELLA (eds.), *L'evoluzione del diritto penale nei settori di interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011.

41. Ver MORO, *Libellus vere aureus, nec minus salutaris quam festivus de optimo rei publicae statu, deque nova insula Utopia*, 1516.

42. KRANZBERG, Technology and history: Kranzberg Laws, *Tech.&Cult.*, 27, 3, 1986, 544.

Seria utópico acreditar que os criminosos do novo milênio não exploraram as oportunidades oferecidas pela revolução tecnológica. Seria igualmente irrealista acreditar que a luta contra esses criminosos pode ser realizada sem recorrer às mesmas oportunidades.[43]

PESQUISAS DO EDITORIAL

Veja também Doutrina

- O direito internacional e o direito brasileiro em face do terrorismo, de Antônio Paulo Cachapuz de Medeiros – *RCP* 15/335;
- O terrorismo no direito brasileiro: análise à luz da obrigação internacional de repressão do crime de terrorismo, de Leandro Moll – *RDCI* 80/376; e
- Terrorismo: reflexões a partir da criminologia crítica, de Maurício Stegemann Dieter – *RBCCrim* 75/295.

- A Era do Controle – Introdução crítica ao direito penal cibernético, de Túlio Lima Vianna, *Doutrinas Essenciais de Direito Penal*, organizada por Alberto Silva Franco e Guilherme de Souza Nucci, São Paulo, Ed. RT, 2010, vol. 8, p. 1039; e
- Entre a civilização e a barbárie, de Adauto Alonso S. Suannes, de *Doutrinas Essenciais de Direito Penal*, organizada por Alberto Silva Franco e Guilherme de Souza Nucci, São Paulo, Ed. RT, 2010, vol. 7, p. 475.

---

43. A conclusão do trabalho de Brenner de 2006 é emblemática: "Meu ponto é que, para lidar de forma eficaz com ameaças cibernéticas, não só precisamos de leis que nos permitem prender e processar os criminosos e cibeterroristas. Temos também de criar e implementar procedimentos que permitam que a polícia e outros agentes do governo analisem com precisão ameaças cibernéticas 'rotineiras' (crimes cibernéticos) e ameaças cibernéticas 'não rotineiras' (ciberterrorismo e ciberguerra)". Ver BRENNER, *Cybercrime* cit., 471.