A REPERCUSSÃO DOS ATENTADOS DE 11 DE SETEMBRO SOBRE A LIBERDADE DE EXPRESSÃO NA INTERNET

Demócrito Reinaldo Filho

A liberdade de informação e de expressão é um princípio basilar de todas as democracias modernas, por meio do qual é assegurado a qualquer pessoa expressar livremente seus pensamentos e idéias, sem restrições de conteúdo. Sua aplicação não se limita a praças e locais públicos, mas alcança também os próprios veículos de comunicação utilizados para a transmissão da informação, como a mídia escrita (jornais, livros e revistas), o rádio, a televisão e, mais recentemente, a Internet. A privacidade também é um princípio fundamental, que resguarda a intimidade da vida privada da pessoa humana.

Desde a última metade da década de 90, é bem verdade, foram sentidas as primeiras tentativas de restringir a liberdade de expressão na Internet, através de leis editadas com o objetivo de combater a disseminação da pornografia e a prática de crimes de preconceito contra determinadas raças e minorias étnicas. Contudo, somente após os ataques de 11 de setembro é que a liberdade de expressão e a confidencialidade das comunicações na Internet sofreram um impacto realmente preocupante. Como conseqüência da campanha contra o terrorismo e em prol de mais segurança, as liberdades civis podem estar definitivamente ameaçadas.

Os países tradicionalmente acusados de relegar os direitos humanos, como a China, o Vietnã, Arábia Saudita e Tunísia, têm habilmente aproveitado a onda contra o terrorismo para reforçar a vigilância na Internet e perseguir dissidentes políticos. Na China, cerca de 14 mil "cybercafes" foram fechados num período de poucas semanas, durante o último verão. Em agosto, 30 usuários de Internet estavam aprisionados e um dissidente recebeu a pena recorde de 11 anos de prisão. O governo chinês tem obrigado os provedores de acesso e grandes portais a assinarem acordos de monitoração de conteúdo informacional em seus sistemas.

Mas o problema pode estar não somente nos países historicamente hostis às liberdades civis. As democracias ocidentais estão dotando seus serviços de inteligência e segurança, através da aprovação de leis e outras medidas práticas, de um poder de acesso à informação sem precedentes. Estão praticamente transformando as companhias telefônicas e os provedores de Internet em potenciais instrumentos da polícia, que passou a ter alcance ao conteúdo dos e-mails enviados, aos registros de *sites* visitados e toda a movimentação dos usuários da Internet. Correspondências eletrônicas podem ser rotineiramente lidas por policiais e agentes dos serviços de inteligência, transformando qualquer cidadão em potencial suspeito. Isso está ocorrendo nos Estados Unidos, na Inglaterra, França, Alemanha, Espanha, Itália e Dinamarca, países (alguns destes) com

tradições democráticas seculares, onde os cidadãos tinham a garantia do sigilo de suas correspondências. A tendência no sentido do controle e fiscalização também conta com o apoio de corpos multinacionais, como a própria ONU, o Parlamento Europeu, o Conselho da Europa e o G-8 (o grupo dos países ricos). Essas medidas incluem a Resolução n. 1373 contra o terrorismo, aprovada pela ONU no dia 28 de setembro do ano passado; a emenda à Diretiva Européia sobre Proteção de Dados e Informações nas Telecomunicações, aprovada pelo Parlamento Europeu em 30 de maio deste ano; as recomendações do G-8 e várias medidas da Polícia Européia (a Europol).

Abaixo fazemos um resumo das medidas que foram ou estão sendo tomadas por cada um dos países, isoladamente, e as leis aprovadas pelos seus respectivos parlamentos, respeitante à vigilância da Internet:

Nos EUA

A descoberta de que os terroristas do 11 de setembro utilizaram a Internet para se comunicarem entre si e prepararem o ataque foi decisiva na determinação do governo de expandir as medidas de segurança na Internet. A campanha pelo controle das transmissões na rede começou poucas horas depois do ataque, quando agentes do FBI compareceram às sedes dos principais provedores com o objetivo de confiscar as mensagens de e-mails trocadas entre os terroristas. Nessa ocasião, tentaram instalar o programa "Carnivore" (hoje renomeado para DCS 1000), o primeiro e maior sistema de vigilância eletrônica usado por uma força policial nacional. Quando instalado no complexo informático de um provedor, possibilita a gravação e o armazenamento de todo o tráfico de mensagens dos usuários. Esse programa nunca antes tinha sido utilizado sem prévia autorização judicial, mas uma lei conhecida como "Combating Terrorism Act", aprovada com urgência apenas dois dias depois dos atentados (em 13 de setembro de 2002), permitiu sua utilização pelos serviços de inteligência sem esse tipo de exigência. Pouco tempo depois, em 24 de outubro daquele ano, a "House of Representatives" passou uma lei, o "USA Patriot Act" (depois designada apenas como "USA Act"), confirmando a autoridade antes conferida ao FBI para instalar o "Carnivore" nos sistemas dos provedores de Internet, com a exigência única de autorização de uma corte especial.

A questão da criptografia também passou a ser crucial nesse novo cenário. Muitos oficiais do governo começaram a combatê-la porque, através dela, um usuário da Internet pode manter suas mensagens de e-mail sigilosas. Por meio de qualquer programa de encriptação – um dos mais conhecidos é o PGP -, um remetente pode codificar sua mensagem, impedindo que outras pessoas tenham acesso ao seu conteúdo. No mesmo dia 13 de setembro, o senador republicano Judd Gregg, num discurso perante o Congresso, defendeu a proibição de todos os programas de encriptação cujos criadores não fornecerem o código fonte ou chave para as autoridades. Ele justificou sua proposição com o fato de o FBI ter levado dez meses para decodificar arquivos encontrados no computador dos terroristas responsáveis pelo primeiro atentado contra o *World Trade Center*, em 1993.

Enquanto essa medida legal não chega, o FBI tem tomado suas próprias iniciativas para lidar com os programas de criptografia. O "Magic Lantern", um programa tipo vírus enviado por e-mail para o computador de um usuário qualquer, permite registrar todas as letras e números teclados. Por esse meio, o programa torna possível ao

FBI desvendar o código teclado por um usuário de *software* de encriptação e, assim, abrir as mensagens escritas em seu computador.

Na França

O Governo do Primeiro-Ministro Lionel Jospin apresentou um pacote de medidas legais anti-terrorismo, em novembro do ano passado, as quais incluem uma lei (LSQ) que estende para um ano o período obrigatório para conservação do tráfico de informações nos sistemas dos provedores de Internet. A lei, que na verdade emenda uma outra lei já existente – a Lei na Sociedade da Informação (Loi sur la Société de l'Information) -, também dá poderes aos juízes para requerer às empresas, que desenvolvem *softwares* de encriptação, os códigos necessários para ler uma determinada mensagem encriptada. Essa lei (LSQ) foi aprovada em regime de urgência e à unanimidade no dia 15 de novembro, sem qualquer discussão. Defensores das liberdades civis argumentaram que se trata de uma ameaça à liberdade de expressão, além de exterminar os mecanismos de encriptação, configurando uma ameaça ao direito de sigilo nas correspondências.

Em julho deste ano, o gabinete do Primeiro-Ministro Jean-Pierre Raffarin apresentou outro pacote de medidas ao parlamento (a LOPSI), que também contêm dispositivos que levantaram preocupação no que diz respeito à liberdade de expressão e sigilo, principalmente os que atribuem à polícia o poder de fazer buscas remotas nos sistemas dos provedores. Essas disposições legais, aprovadas no dia 31 de julho, permitem que a polícia, mediante autorização judicial, tenha acesso direto aos registros do fluxo de informações enviadas e recebidas pelos usuários. Uma disposição central estabelece que a polícia tem permissão (desde que autorizada judicialmente) de "acesso direto a qualquer dado considerado necessário para a descoberta da verdade". Sua aprovação despertou a preocupação de várias entidades, inclusive a que congrega os juízes franceses (a IRIS), que temem que as buscas se transformem num ato discricionário da polícia, invadindo a privacidade dos usuários indistintamente.

Na Inglaterra

Se as medidas e leis aprovadas em outros países já foram suficientes para causar preocupação, o "Anti-Terrorism, Crime and Security Act", aprovado em dezembro do ano passado na Inglaterra supera os seus similares nesse ponto. A lei isenta a polícia em vários casos da obtenção prévia de autorização judicial para ter acesso ao fluxo de informações dos provedores de Internet; é suficiente uma ordem do Ministro do Interior ou de seus auxiliares imediatos[1]. A medida causou um alarido tão grande que muitos provedores ameaçaram transferir a sede de suas operações para outros países.

A polêmica não parou por aí. Em junho desse ano, o Ministro do Interior David Blunkett propôs emendas a uma controvertida lei aprovada em 2000, a "Regulation of Investigatory Powers Act" (RIPA), de forma a atribuir poderes a vários agentes governamentais, como auditores fiscais, servidores dos serviços de previdência e agentes municipais, para ter acesso aos dados e e-mails dos usuários da Internet. A proposta

[1] A Lei também aumenta para um ano o prazo que os provedores devem obrigatoriamente conservar os registros e informações de seus usuários.

sofreu tanta oposição das organizações de defesa das liberdades civis que sua discussão no parlamento foi adiada.

Na Índia

A Ordenação de Prevenção ao Terrorismo (POTO), aprovada logo após os ataques do 11 de setembro, permite ao governo monitorar todo tipo de comunicações, especialmente as trocas eletrônicas de informações por e-mail, sem necessidade de qualquer autorização oficial ou legal prévia. Os dados recolhidos dessa maneira, quando a ordem partir dos serviços de segurança, podem ser usados contra uma pessoa como prova em processo judicial.

Especialmente o trabalho dos jornalistas estava ameaçado por essa lei. O princípio universal que garante o sigilo da fonte já não era mais intocável, pois aqueles que se recusassem a fornecer às autoridades evidências que tinham obtido contra terroristas e suas organizações podiam ser presos por cinco anos, de acordo com os termos da lei. A lei terminou, no entanto, sendo emendada após forte oposição de organizações de defesa dos direitos humanos, e o dispositivo que obrigava os jornalistas a revelarem a fonte das informações ligadas a casos de terrorismo foi revogada.

Na Itália

Uma lei aprovada em dezembro do ano passado dá a várias autoridades poder para fiscalizar as atividades de pessoas suspeitas e interceptar suas mensagens de e-mail e todo o fluxo de suas informações, pela Internet e outros meios de telecomunicações. A peculiaridade dessa lei é que ela estende esses poderes oficiais a integrantes dos corpos policiais de escalão inferior. Além disso, a lei prevê que qualquer pessoa que revelar a atividades desses agentes policiais e os detalhes de como desempenham suas atividades de fiscalização podem ir para a prisão.

Na Espanha

No dia 27 de junho deste ano, foi aprovada em uma das casas legislativas a lei espanhola com objetivo de combater o terrorismo e *cybercrimes* – a LSSICE. A lei obriga os provedores de Internet a conservar os registros do tráfico de informações pelo prazo de um ano, além de conferir acesso policial a esses dados. Deputados da oposição já se organizam para aprovar emenda que proíbe a polícia e os serviços de inteligência de ter acesso sem prévia autorização judicial. Uma das provisões que despertam maiores reações é a que permite a derrubada de *sites* considerados de "valor prejudicial", até porque a lei não deixa claro que autoridades gozam desse poder. A liberdade de expressão é garantida na Constituição espanhola, cujo artigo 20 assegura o direito de "livremente enviar ou receber informação lícita através de qualquer meio de comunicação".

Na Alemanha

O “Otto-Katalog”, como tem sido chamado um pacote de medidas legislativas enviadas pelo Ministro do Interior da Alemanha, Otto Schily, e adotadas pelo parlamento no fim do ano passado, tem sido bastante criticado por organizações de defesa das liberdades civis. Uma das mais criticadas provisões é a que aboliu a distinção entre a polícia e os serviços de inteligência, conferindo a estes últimos amplo acesso às bases de dados dos órgãos policiais. As medidas também lhes conferem acesso aos registros das telecomunicações e informações constantes dos sistemas dos provedores.

No Canadá

A C-36, a lei canadense contra o terrorismo, aprovada em dezembro do ano passado, facilita a instalação de sistemas de escuta em telefones e computadores. Pela primeira vez na sua história, um órgão do Departamento de Defesa vai poder “grampear” tanto cidadãos canadenses quanto estrangeiros. O sigilo das correspondências eletrônicas ficou virtualmente extinto.

Na Dinamarca

O governo dinamarquês não criou uma lei específica, como fizeram outros governos, mas, com o propósito de combater o terrorismo, reformulou várias das leis existentes envolvendo a estrutura do Judiciário, a economia e tributação. Em especial a Internet e as novas tecnologias foram visadas, através da legalização da retenção dos registros de conexão e de chamadas telefônicas e o intercâmbio de mensagens eletrônicas, facilitando o acesso da polícia a essas informações. No dia 31 de maio deste ano, uma lei autorizou agentes do governo a manter esses dados em seu poder até o prazo de um ano. A lei foi mais além: permitiu a polícia consultar esses dados sem prévia autorização judicial. A polícia pode inclusive instalar, nos sistemas informáticos do provedor, programas ou tecnologia similar ao “Carnivore” usado pelo FBI americano.

No G-8

No último encontro desse grupo, que se realizou no Canadá, em junho deste ano, foi dito que a *network* formada entre instituições policiais de 26 países já é capaz de fornecer rápidas informações, quando são requeridas urgentes respostas pelas organizações policiais internacionais que combatem crimes *high tech*, incluindo a interceptação das mensagens entre terroristas e outros tipos de criminosos. Os especialistas presentes ao encontro disseram que as autoridades policiais desenvolveram mecanismos técnicos que podem determinar a origem, destino e rota de mensagens de terroristas e criminosos na Internet, além de reter evidências e meios de prova contra eles em meio eletrônico. Esse avanço no desenvolvimento desse sistema tem sido creditado em parte à insistência da Itália, que era o país que detinha a presidência do G-8 por ocasião dos atentados de 11 de setembro. Apenas 08 dias após os ataques, o governo italiano publicou uma declaração em que defendia a urgência da criação de uma polícia para combater *cybercrimes*.

Na União Européia

A União Européia sempre tinha se colocado contra qualquer tipo de medida de extrema fiscalização ou vigilância eletrônica. Essa posição, no entanto, começou a se alterar logos após os atentados de 11 de setembro. O Conselho Europeu vinha considerando a manutenção, na Diretiva sobre Proteção de Dados e Informações nas Telecomunicações, do princípio da "eliminação automática" dos registros de conexão à Internet. Pelo registro das conexões (*traffic logs*) que uma pessoa faz, ao telefone ou quando acessando a Internet, é possível se determinar para quem fez a ligação, o tempo de conexão, as mensagens recebidas, entre outros dados. Pela regra da "eliminação automática" (*automatic deletion*) dos registros de conexão (*logs*), os provedores e companhias telefônicas estariam obrigados a não registrar os *logs*. Mas o Presidente dos EUA, George Bush, em outubro do ano passado, exerceu influência sobre o Primeiro Ministro da Bélgica, Guy Verhofstadt, então Presidente da União Européia, para alterar a Diretiva tendo em consideração a luta contra o terrorismo e, assim, adotar a regra geral da retenção dos registros de telefones e dos dados da atividade na Internet. O Parlamento Europeu mudou sua posição em menos de um ano. No dia 30 de maio deste ano, aprovou uma emenda à Diretiva, estabelecendo, no seu art. 15.1, que todos os governos dos países membros que ainda não tenham adotado essa regra deverão, no prazo de 15 meses, editar leis obrigando os provedores de Internet e as companhias de telefone a reter todos os registros de e-mail e transmissões de informações na Internet, ou por meio de fax e chamadas de telefone, que transitem em seus sistemas, devendo, ainda, garantir à polícia, às autoridades judiciais e governamentais livre acesso a esse material.

Ainda no âmbito da União Européia, é de se destacar a Convenção sobre Cybercrimes, a primeira convenção internacional do gênero, assinada em Budapeste em novembro do último ano. A Convenção vinha sendo preparada há mais de 04 anos e se voltava inicialmente somente aos países europeus. Mas, depois dos atentados de 11 de setembro, foi assinada (dentre outros) pelos EUA, Canadá, Japão e África do Sul. Ela induz a centralização das evidências garimpadas em meio eletrônico de infrações e atividades relativas ao terrorismo e ao crime organizado, criando um sistema de vigilância generalizada, segundo seus críticos. A crítica se dirige especialmente a seus artigos 19, 20 e 21, que autorizam os serviços de segurança, no curso de suas investigações, a ter acesso aos registros mantidos pelos provedores, a estender as buscas a outros computadores (se necessário) e ter informações "real-time" sobre conexões e trânsito em *websites*.

É claro que várias dessas legislações que apresentamos acima em resumo poderão ser declaradas inconstitucionais, frente a disposições garantidoras de direitos humanos e das liberdades de expressão e cláusulas garantidoras da privacidade. Também oferece certa preocupação a questão da eliminação do sigilo permitido pelas técnicas de criptografia, que já foi usada em países governados por ditaduras por organizações de defesas de direitos humanos. É óbvio que essa tendência do reforço das leis de segurança atende à constatação de que o mundo realmente mudou. Os atentados serviram apenas para revelar a face mais aterradora do terrorismo e de seus adeptos. Os corpos policiais dos países têm que se adaptar à luta contra os *cybercrimes*, inclusive se organizando em entidades de cooperação internacional. Mas o que parece ameaçador é transformar os

sistemas de investigação em uma “larga e exploradora escala de vigilância eletrônica”. As medidas de investigação devem se adequar a alguns princípios já consagrados, como a autorização judicial prévia ou de autoridades competentes para casos excepcionais, e devem obedecer às diretrizes da limitação da duração, da proporcionalidade e da execução desenhada estritamente para atingir o interesse público em questão.

Recife, 11.09.02

Disponível em :< http://www.internetlegal.com.br/artigos/democrito7.zip>
Acesso: 18/07/06