Internet e Jurisdição, Acesso Transfronteiríço a Dados e o Caso Irlanda Microsoft

Internet and Jurisdiction, Crossborder Access to data and the Case Microsoft Ireland

MELISSA GARCIA BLAGITZ DE ABREU E SILVA
Procuradora da República em São Paulo, membro do Grupo de Combate a Crimes Cibernéticos da Procuradoria da República em São Paulo e do Grupo de Trabalho sobre Crimes Cibernéticos da 2a. Câmara de Coordenação e Revisão do Ministério Público Federal. Mestre em Direito pela Universidade de Chicago.

Resumo: A Internet trouxe uma revolução na forma como a sociedade pensa, age e interage. Ela também trouxe uma revolução na forma como documentos eletrônicos são acessados e guardados. Num mundo de computação nas nuvens, o uso do princípio territorial para definição de jurisdição tornou-se obsoleto e inadequado. Países europeus, signatários ou não da Convenção de Budapeste, estão modificando o critério para definição de jurisdição e a forma como prova eletrônica é coletada e acessada. O novo critério é controle e não território – aqueles que têm controle sobre os dados precisam fornecê-los, independentemente do local em que estão fisicamente armazenados. A legislação brasileira também adotou o critério controle e a discussão sobre seus reflexos finalmente chegou às Corte Norte-americanas com o Caso Microsoft Irlanda. O novo critério, controle, é hoje o único caminho possível. O único caminho que respeita soberania e as peculiaridades da prova eletrônica.

Palavras-chave: Internet, Jurisdição, Acesso Transfronteiriço.

Abstract: The Internet brought a revolution on the way society thinks, acts and interacts. It also brought a revolution on how documents are kept an accessed. In a world of cloud computing, the use of the territorial principle to determine jurisdiction became obsolete and inadequate. European countries, members of the Budapest Convention or not, have been slowly changing the paradigm to define Internet Jurisdiction and the way electronic evidence is reached and collected. The new test is control, not location – those who have control over the data must provide it, no matter where it is physically located. The Brazilian legislation has also adopted the same principle and the discussion about its implications has finally reached the US Courts with the Microsoft Ireland Case. The new paradigm is today the only feasible way forward. The only way that respects sovereignty and the peculiarities of electronic evidence.

Keywords: Jurisdiction; Crossborder Access; Internet

1. Introdução

A Internet produziu uma revolução. A rede mudou a forma como a sociedade pensa, age e interage. Ela permitiu ampla e irrestrita comunicação e trocas de dados, ignorando fronteiras físicas. A nova realidade modificou profundamente como dados e documentos eletrônicos são armazenados e acessados. Nesse novo quadro, o conceito puramente territorial de jurisdição tornou-se inadequado e obsoleto, e o desenvolvimento de novos critérios um tema urgente.

Enquanto o mundo lida há mais de uma década com os problemas relacionados ao acesso transfronteiriço a provas eletrônicas, isto é, o acesso direto a provas eletrônicas fora das fronteiras do Estado requisitante, o problema apenas despertou maior atenção e interesse nas cortes norte-americanas com o caso Microsoft Irlanda[1]. O longo debate entre Departamento de Justiça e Microsoft nesse caso, embora aparentemente limitado a preceitos da legislação norte-americana, em realidade refletiu a necessidade de novos parâmetros para a definição de jurisdição em um mundo de computadores e nuvens.

Este artigo propõe-se ao breve exame dos principais argumentos apresentados pelo governo norte-americano e a Microsoft e de como esses argumentos, embora aparentemente limitados à realidade local, espelham questões mais amplas que vêm sendo discutidas em outros países e possuem reflexos na legislação brasileira.

2. O Caso Microsoft Irlanda

Resumidamente, o caso Microsoft Irlanda refere-se a um pedido e posterior expedição de mandado de busca e apreensão para coletar informações e conteúdo de uma conta de e-mail mantida e controlada pela empresa Microsoft. A base legal para a decisão inicial, emitida por um magistrado do Circuito de Nova Iorque, é a seção 18 U.S.C. § 2703(a)[2], que impõe a

[1] In the Matter of a Warrant to Search a Certain E-mail Account Controlled And Maintained By Microsoft Corporation, United States Court of Appeals for the Second Circuit, Docket No. 14-2985, julgado em 14 de julho de 2016.

[2] 18 U.S.C. § 2703(a) determina, em tradução livre: "CONTEÚDO DE COMUNICAÇÃO ELETRÔNICA ARMAZENADA – Um órgão do governo pode requisitar que um serviço provedor de comunicação eletrônica apresente o conteúdo de comunicação eletrônica guarda em sistema de comunicação eletrônica por menos de cento e oitenta dias apenas mediante de mandado expedido pela corte competente através do procedimento descrito nas Normas de Processo Penal Federal (ou no caso de cortes estaduais, conforme as normas processuais estaduais).
No original: "CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE. – A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire of electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction"

necessidade de mandado de busca e apreensão para a obtenção de conteúdo de e-mails com menos de 180 dias[3]. Houve resistência da empresa na entrega dos dados ao argumento de que eles, apesar de controlados pela Microsoft nos Estados Unidos, estavam armazenados em servidores mantidos pela empresa na República da Irlanda o que, na visão da companhia, demandaria pedido formal de cooperação internacional, sem a possibilidade de acesso direto.

Assim, a principal questão em debate nos sucessivos recursos que se seguiram após a autorização inicial se resume a como definir a obtenção de dados guardados fisicamente em um país, mas controlados por empresa que presta serviços no território local. Discute-se se haveria apenas uma questão interna, de acesso a dados controlados por empresa local, independente de onde estão fisicamente armazenados, ou uma questão internacional a demandar envolvimento de autoridades estrangeiras e pedido formal de cooperação.

Em suas objeções ao mandado expedido, Microsoft apresentou, essencialmente, quatro argumentos: a) a seção 2703(a) exige a expedição de mandado de busca e apreensão, que somente pode ser cumprido no território sob jurisdição do Juízo expedidor; b) há presunção contra a aplicação extraterritorial de preceitos da legislação norte-americana, presunção esta que somente pode ser deixada de lado se há a clara intenção da norma legal, expressa em sua linguagem[4], de ser cumprida fora do território norte-americano e nada na lei que autoriza a busca e nem nas regras de procedimento que devem ser seguidas para sua execução contém essa indicação; c) o mandado expedido autoriza a busca e apreensão no território de outro país; e d) ainda que fosse possível a aplicação extraterritorial da norma, razões diplomáticas a desaconselhariam, pois o Direito Internacional não reconhece o acesso transfronteiriço a dados.

O governo norte-americano, de sua parte, argumentou que: a) o mandado expedido nos termos da seção 2703(a) é executado como uma requisição e não uma busca e apreensão: é uma ordem para o fornecimento de dados ("compelled disclosure") e não autorização para entrada forçada e apreensão; e b) como tal, o critério a ser empregado é quem controla os documentos ou dados e não o local onde eles estão fisicamente mantidos (control, not location).

Na última decisão proferida no caso, datada de 14 de julho de 2016[5], a Corte de Apelações do Segundo Circuito concordou com os argumentos da Microsoft e considerou o caso apenas uma questão de extraterritorialidade de norma, aplicando a ele a presunção contra extraterritorialidade acima mencionada. Embora reconhecendo que a questão representa um problema novo que precisa ser analisado com urgência pelo Legislador, a corte concluiu que

[3] É importante observar que a distinção feita pela legislação norte-americana entre e-mails armazenados por mais ou menos de cento e oitenta dias foi modificada por diversas decisões de Cortes Federais aplicando a Quarta Emenda constitucional e o conceito de "expectativa de privacidade" definido em Katz v. United States (Suprema Corte, 1967, 389 U.S. 347). Hoje, no sistema legal norte-americano, qualquer conteúdo de comunicação eletrônica somente pode ser obtido mediante mandado de busca e apreensão expedido pela autoridade judiciária competente.

[4] No caso Morrison v. National Australia Bank Ltd. (130 S.CT. 2869), a Suprema Corte norte-americana decidiu que a legislação local, salvo se houver clara demonstração do contrário pela redação ou intenção declarada do Legislador, somente deve ser aplicada no território sob jurisdição dos Estados Unidos e que tal princípio deve ser observado em todos os casos em que as partes buscam efeitos extraterritoriais na aplicação da lei norte-americana.

[5] A íntegra da decisão pode ser acessada em: http://www.ca2.uscourts.gov/decisions/isysquery/605fa83c-ff94-4bcf-b99f-6cb020f12608/6/doc/14-2985_complete_opn.pdf#xml=http://www.ca2.uscourts.gov/decisions/isysquery/605fa83c-ff94-4bcf-b99f-6cb020f12608/6/hilite/

nem a seção 2703(a), nem a regra 41 do Processo Penal Federal, que disciplina a expedição e o cumprimento de mandados de busca e apreensão, traziam indicativos que permitissem a aplicação extraterritorial, e como o mandado deveria ser cumprido em território irlandês, onde armazenados os dados, sem a extraterritorialidade o Juízo não poderia expedir ordem a ser cumprida fora de sua jurisdição.

Sem adentrar em análise mais profunda da legislação estadunidense, é certo que o argumento utilizado pelo governo norte-americano, de controle ao invés de localização, para definir a jurisdição sobre a prova eletrônica tem respaldo no Direito Internacional, na Convenção de Budapeste sobre Cibercriminalidade, e legislações de diversos países, inclusive o Brasil. Ele também representa uma mudança de paradigma que reflete as peculiaridades da prova eletrônica e as necessidades do mundo conectado nas nuvens.

3. A Convenção de Budapeste sobre Cibercriminalidade e o Acesso à Prova Eletrônica

A Convenção de Budapeste sobre Cibercriminalidade do Conselho da Europa (CETS no. 185) foi um dos primeiros e até o momento é um dos únicos instrumentos internacionais sobre crimes cibernéticos e prova eletrônica. Originalmente gestada o Conselho da Europa, foi assinada por 54 países, incluindo 9 não europeus, e está em pleno vigor para 48 deles[6].

A Convenção regula detalhadamente crimes cibernéticos e prova eletrônica[7]. Seu principal objetivo é harmonizar a legislação mundial sobre crimes cibernéticos, permitindo melhor uso de mecanismos de cooperação internacional e extradição. Ela contém dispositivos de direito material, descrevendo ofensas criminais, e também dispositivos processuais, incluindo ferramentas de investigação, preservação de dados, requisições de provas, busca e apreensão, e jurisdição internacional e cooperação.

3.1 O Princípio Territorial, Prova Eletrônica e Crimes Cibernéticos

O princípio territorial é a regra mais básica para definição de jurisdição. Todo Estado é soberano em seu território e consequência necessária da soberania é a habilidade de legislar, julgar e executar seus julgamentos dentro de seu território. Ele é baseado no fato de que um Estado tem controle sobre as ações, pessoas e coisas dentro de suas fronteiras. Como consequência, um documento ou prova armazenada no território de um Estado e necessária para um procedimento em outro Estado deve ser objeto de um pedido de cooperação internacional em matéria judicial.

O princípio territorial funciona sem maiores problemas em investigações convencionais. Normalmente, crimes são cometidos em um território, por uma pessoa dentro desse território, tendo como vítimas pessoas no território. O mesmo Estado que tem jurisdição territorial para legislar, terá jurisdição territorial para julgar o caso e executar a pena eventualmente imposta.

---

[6] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=VsTdZN6J

[7] O texto completo em português pode ser encontrado em https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa428

Quando mais de um Estado está envolvido, usualmente há uma ligação territorial que torna fácil identificar qual deles tem jurisdição sobre o caso – o local onde estão as vítimas geralmente está relacionado com o local da prova, ainda que o autor do fato esteja em outro lugar, e essas questões são resolvidas com regras sedimentadas. Crimes tradicionais não representam grandes desafios ao princípio.

O princípio territorial puro, no entanto, simplesmente não funciona para provas eletrônicas e crimes cibernéticos internacionais[8].

Primeiro, porque crimes cibernéticos, em regra, atingem vítimas por todo o mundo, usando equipamentos espalhados globalmente, com autores conectados na rede a partir de diferentes países. Provas eletrônicas, ainda que relacionadas a crimes tradicionais locais, são normalmente armazenadas em diferentes lugares, por diferentes empresas, de diferentes países, com base em critérios puramente coorporativos – o que funciona melhor para a operação da empresa responsável pela armazenagem.

Segundo, porque provas eletrônicas podem ser acessadas de qualquer lugar. Independentemente do local onde esteja mantido fisicamente o servidor que armazena os dados, desde que conectado em qualquer tipo de rede, eles poderão ser acessados de qualquer ponto do mundo.

Essa afirmativa um tanto quanto óbvia é crucial e pode levar a resultados desconcertantes quando o princípio territorial é aplicado sem qualquer restrição a crimes com provas eletrônicas. De acordo com o princípio em seu conceito mais básico, se um órgão de investigação possui um mandado de busca e apreensão legalmente expedido para apreender um computador e o encontra ligado, exibindo o acesso a uma conta de e-mail mantida em servidores localizados em outro país, os agentes não poderão acessar, coletar ou mesmo ler os e-mails. Os e-mails, nesse exemplo, mesmo nas vistas dos investigadores e acessíveis às pontas dos seus dedos, são na verdade documentos internacionais, sob a jurisdição de outro país, e somente poderão ser lidos ou acessados mediante autorização desse país, após demorado e laborioso pedido de cooperação internacional.

A conclusão aqui é simples: o princípio territorial em sua forma tradicional não atende às peculiaridades das provas eletrônicas e dos crimes cibernéticos, e a necessidade de novos instrumentos funcionais tem sido objeto de constantes debates entre órgãos de investigação e a academia. A Convenção de Budapeste deu um primeiro passo para solucionar esse dilema.

3.2 A Convenção de Budapeste

A Convenção de Budapeste tem dois artigos que precisam ser analisados em conjunto quando se pretende entender o novo parâmetro internacional para acesso a provas eletrônicas, que substitui o critério de localização por controle, sem perder de vista da jurisdição territorial.

O primeiro artigo expressamente admite o que é referido como "acesso transfronteiriço a dados informáticos armazenados". Em outras palavras, o dispositivo reconhece que a prova eletrônica é acessível de qualquer lugar do mundo e estabelece, ex ante, que os Estados signatários da Convenção poderão, atendidas determinadas circunstâncias, acessar arquivos e documentos que estão fisicamente localizados em outros Estados signatários, mas que podem ser acessados através da rede. *In verbis*, o artigo 32 estabelece que:

[8] A expressão "crimes cibernéticos internacionais" é até certo ponto um paradoxo porque todos os crimes cibernéticos hoje têm um componente internacional, em maior ou menor grau.

> Uma Parte pode, sem autorização de outra Parte:
> a) Aceder a dados informáticos armazenados acessíveis ao público (fonte aberta), seja qual for a localização geográfica desses dados; ou
> b) aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados situados no território de outra Parte, se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados, através deste sistema informático.

A alínea (b) disciplina o exemplo mencionado acima e também estabelece o critério controle para a determinação da jurisdição. Nos termos da Convenção, os Estados signatários autorizam previamente que os outros Estados signatários acessem diretamente dados armazenados em seus territórios se a pessoa legalmente autorizada a fornecer esses dados consentir voluntariamente. Isto é, se a pessoa que controla a informação consentir, órgãos de investigação poderão acessar a informação, mesmo que armazenada no exterior.

Esse dispositivo, entretanto, tem limitações. A primeira é que ele não pode ser aplicado a dados armazenados em países que não são signatários da Convenção. Isso limita o escopo do dispositivo, ainda que a Convenção tenha sido assinada por países que representam grande parte do fluxo de dados via Internet.

A segunda limitação traduz-se na impossibilidade de a informação ser obtida sem o consentimento da pessoa que a controla, o que é agravado pelo fato de, na maioria dos países, os provedores de serviço e de aplicativos não poderem legalmente consentir e ceder informações de seus usuários. O dispositivo, assim, é limitado à pessoa que legalmente controla e detém a informação e consente em auxiliar. Ele não prevê a possibilidade de requisição, mesmo judicial ("compelled disclosure"), e nem de extensão da autorização a terceiros que controlam a informação porque prestam serviços, ausente autorização específica do usuário[9].

Apesar desses problemas, o dispositivo representa avanço notável, especialmente quando considerado que foi escrito no início dos anos 2000.

O segundo dispositivo está no artigo 18 da Convenção e a legislação doméstica editada para implementá-lo está criando novos dispositivos de Direito Internacional costumeiro e modificando a forma como é definida a jurisdição sobre a prova eletrônica.

O artigo 18 determina que cada Estado signatário "adotará" as medidas legislativas necessárias para "habilitar as suas autoridades competentes" para ordenar a uma pessoa em seu território que forneça "dados informáticos específicos, na sua posse ou sob o seu controle e armazenados num sistema informático ou um outro suporte de armazenamento de dados informáticos" (destaque nosso)[10].

---

[9] Diversas discussões estão correndo dentro do Conselho da Europa visando aprimorar o acesso transfronteiríço a dados. Relatórios das discussões em inglês podem ser acessados em http://www.coe.int/en/web/cybercrime/t-cy-reports.

[10] In verbis:

"Artigo 18º. – Injunção

1. Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para ordenar::

a. A uma pessoa que se encontre no seu território que comunique os dados informáticos específicos, na sua posse ou sob o seu controle e armazenados num sistema informático ou num outro suporte de armazenamento de dados informáticos; e

O artigo não menciona onde a informação deve estar armazenada, se fora ou dentro do território do requisitante, mencionando apenas que a pessoa requisitada deve ter controle sobre os dados, mas o entendimento no momento da assinatura da Convenção era de que o dispositivo limitava-se a documentos e arquivos armazenados no território do Estado requisitante[11]. Entretanto, o critério controle é expressamente reconhecido pela Convenção e as legislações domésticas que a implementaram foram além.

Na realidade, as legislações domésticas dos países signatários estão dando força plena ao critério controle, estabelecendo que um Estado, ainda segundo o princípio territorial, tem plena jurisdição sobre empresas localizadas ou prestando serviços em seu território, e pode requisitar delas quaisquer informações por elas controladas, independentemente do local em que estão fisicamente armazenadas. Em verdade, no mundo da computação nas nuvens, o local físico de armazenamento torna-se cada vez mais irrelevante, pois pode mudar em questão de minutos ou ser completamente desconhecido, tornando-se essencial quem controla as informações e onde esse controlador presta serviços.

3.3 A Legislação Doméstica[12] e a Jurisprudência de Países Europeus

Como mencionado, na esteira dos dispositivos da Convenção de Budapeste, diversos Estados europeus, signatários ou não da Convenção, elaboraram legislações adotando e expandindo o acesso transfronteiriço a dados e o critério controle.

Apesar da inicial vocação local, os Estados utilizam o artigo 18 para requisitar que empresas prestadoras de serviço em seus territórios forneçam dados eletrônicos necessários a investigações[13]. Austrália, Espanha e Canadá permitem que órgãos de investigação requisitem

b. A um fornecedor de serviços que preste serviços no território da Parte, que comunique os dados na sua posse ou sob o seu controle, relativos aos assinantes e respeitantes a esses serviços.

2. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º. e 15º.

3. Para os fins do presente artigo, a expressão "dados relativos aos assinantes" designa qualquer informação, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida por um fornecedor de serviços e que diga respeito aos assinantes dos seus serviços, diferentes dos dados relativos ao tráfego ou ao conteúdo e que permitam determinar:

a. O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esses respeito e o período de serviço;

b. A identidade, a morada postal ou geográfica e o número de telefone do assinante e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços;

c. Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

[11] O parágrafo 173 das Notas Explicativas sobre a Convenção esclarece que o termo "posse ou controle" refere-se à posse física no território do país requisitante e a situações em que a pessoa requisitada pode produzir livremente o documento no território do país requisitante (o texto completo em inglês pode ser acessado em https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b).

[12] Extraído de "Transborder access and jurisdiction: What are the options", relatório do Subgrupo em Jurisdição e Acesso Transfronteiríço a Dados do Comitê T-CY da Convenção de Budapeste, adotado em dezembro de 2012 (http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf).

[13] Maxwell, Winston/Wolf, Christopher (2012): A Global Reality: Governmental Access to Data in the Cloud (Hogan Lovells White Paper, 23 May 2012), mencionado pelo relatório do T-CY. O documento original, em inglês, está em https://www.hoganlovells.com/en/publications/hogan-lovells-white-paper-government-access-to-data-in-the-cloud.

de empresas localizadas em seu território informações, independentemente do local de armazenamento. Dinamarca, França e Reino Unido trazem dispositivos semelhantes, com um requisito a mais, permitindo a requisição e o acesso direto quando os dados estão sobre o controle de empresa local e podem ser acessados de seus territórios.

Ironicamente, no caso Microsoft Irlanda, o próprio governo irlandês apresentou petição como amicus informando à Corte de Apelação que, apesar das preocupações da empresa ré com questões diplomáticas que pudessem advir do acesso direto aos dados armazenados no exterior, a legislação irlandesa também autoriza o acesso direto, mediante o critério de controle. O documento, citando decisão da Suprema Corte irlandesa no caso Walsh v. Irish National Bank, afirma que a legislação local permite o acesso a dados controlados por empresa irlandesa, independentemente do local em que estão fisicamente armazenados[14]. Importante salientar que a Irlanda assinou, mas não ratificou a Convenção de Budapeste.

Em todos os casos citados, as legislações locais reconhecem que o que determina a possibilidade de acesso direto a provas eletrônicas não é o local de armazenamento destas, mas o local em que estabelecida, de qualquer forma, ou prestando serviços a empresa que controla esses dados. Órgãos de investigação desses países podem requisitar dados controlados por empresas que prestam serviços em seus territórios independentemente do local onde os dados estão fisicamente armazenados.

O uso do critério controle também tem sido reconhecido pela Jurisprudência dos países europeus.

No caso Licra – Ligue Contre le Racisme et l'Antisémitisme et Union des Édutiants Juifs de France v. Yahoo! Inc. et Société Yahoo! France, o Tribunal de Grande Instance expediu uma ordem determinando que a empresa Yahoo! tomasse todas as medidas necessárias a dissuadir e "tornar impossível" a visualização e venda de artigos nazistas na França[15]. O caso prosseguiu em litígio nos Estados Unidos, onde a Corte do Nono Circuito decidiu que Yahoo! não poderia utilizar a Primeira Emenda à Constituição Norte-Americana, que trata da liberdade de expressão, para descumprir a legislação francesa[16]. Em outras palavras, ambas as cortes reconheceram que uma empresa prestando serviços em um determinado país precisa obedecer à legislação desse país, mesmo que sua operação e seus servidores estejam localizados ou sediados em outro país.

Em outro caso envolvendo o Yahoo!, a Suprema Corte da Bélgica confirmou que se uma empresa presta serviços em território belga, ela precisa obedecer à lei local fornecendo todos os dados e documentos controlados por ela[17]. Interessante notar que a decisão não exigiu que a empresa tivesse sede ou subsidiária na Bélgica, mas apenas que ali prestasse serviços (à época, Yahoo! não possuía representantes na Bélgica e foi citada por e-mail).

Mais recentemente, a Corte Europeia de Justiça decidiu que um provedor estabelecido em um Estado Membro deve obedecer às diretrizes europeias, independentemente do local

[14] O original afirma que: "[h]owever on the central point whether it had power to order production of documents by an Irish registered company by on of its branches situated in a foreign country, the Supreme Court found that it did. The Supreme Court found that the Taxes Consolidation Act empowers the Irish taxation authorities to seek an order that an Irish bank produce records of accounts held by its customers wherever the information is situated" (grifo nosso). O texto, em inglês, pode ser acessado em http://digitalconstitution.com/wp-content/uploads/2014/09/Ireland-AmicusBrief.pdf.

[15] https://fr.wikipedia.org/wiki/LICRA_contre_Yahoo!

[16] Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisémitisme (433 F.3ed 1199).

[17] https://gavclaw.com/2015/12/07/its-true-belgian-supreme-court-confirms-order-for-yahoo-to-hand-over-ip-addresses/

físico de seus equipamentos ou do local em que sua operação é mantida[18][19]. Em 14 de abril de 2016, a União Europeia aprovou como lei um pacote de Proteção de Dados que segue os mesmos critérios, estabelecendo a jurisdição dos Estados membros sobre empresas que prestam serviços em seus territórios[20].

Em resumo, países europeus, há mais de uma década, reconhecem o critério controle para a obtenção direta de provas eletrônicas, adotando-o em suas legislações e em decisões judiciais. Se uma empresa presta serviços ou está localizada em determinado país, ela precisa atender às requisições de documentos eletrônicos apresentadas legalmente pelos órgãos de investigação desse país, não importando onde esses documentos estão fisicamente armazenados, se no próprio Estado requisitante ou em outro local. Esse mesmo critério foi adotado pelo Marco Civil da Internet.

3.4 A Legislação Brasileira

O artigo 11 da Lei no. 12.965/2014, Marco Civil da Internet, estabelece que:

> Artigo 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e dos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Análise superficial do dispositivo pode levar à conclusão de que ele apenas reproduz o princípio territorial puro. Se a empresa presta serviços no Brasil, deve adequar-se à legislação brasileira, à legislação local, o que em si não contém nenhuma inovação.

Essa conclusão, porém, é equivocada, pois o dispositivo tem alcance muito maior do que a simples aplicação do princípio territorial.

Em verdade, o artigo reflete posicionamento jurisprudencial, inclusive das cortes superiores, de que a empresa que presta serviços no país precisa cumprir a legislação nacional. A norma apenas deixa tal obrigação mais clara, determinando em seu § 2o., que a lei brasileira será aplicada "mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil". Assim, ainda que a operação da empresa ocorra toda no exterior, e ali sejam tomadas as decisões corporativas e mantidos os servidores que coletam e armazenam os dados necessários para a prestação dos serviços, deverá ser observada a legislação brasileira para os dados coletados no Brasil, inclusive quanto às requisições judicias descritas no artigo 10.

Nesse contexto, as sucessivas negativas de provedores constituídos sob as leis brasileiras, mas com sede de operação em outros países em fornecer dados diretamente às autoridades brasileiras carecem de completo fundamento, quer na legislação nacional, quer na legislação internacional. Cada vez mais é irrelevante onde os dados são armazenados, restando apenas a questão de quem controla esses dados e onde o serviço é prestado.

---

[18] http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf.
[19] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf
[20] http://www.whitecase.com/publications/article/european-parliament-approves-new-eu-data-protection-law

Imperioso concluir, dessa forma, que a legislação brasileira, ainda que preservando certos aspectos do princípio territorial, também adotou o critério controle e nisso está em absoluta harmonia com a legislação europeia, com a nova interpretação legal que se busca nos Estados Unidos, e com o Direito Internacional. Terá jurisdição para requisitar dados diretamente o Estado em que a empresa que controla os dados presta serviços, independente do local físico em que mantidos seus equipamentos e armazenados os documentos. A regra é controle, não localização.

4. Conclusão - O Futuro do Acesso a Dados

O problema do acesso direto a dados e à prova eletrônica é urgente e afeta não apenas os crimes propriamente considerados cibernéticos, como a persecução penal de crimes comuns, mas com provas armazenadas em sistemas informáticos. O critério controle não é a única solução para esse problema, mas tem sido a mais adotado por legislações em todo o mundo.

Existem duas razões principais para a adoção do critério controle. A primeira delas é a realidade da prova eletrônica.

Dados e documentos eletrônicos são, por essência, móveis. Eles podem ser armazenados em qualquer lugar e também podem ser movimentados para qualquer lugar, a qualquer tempo, em questão de minutos, com um único clique. Eles podem ser movidos para o território de um Estado observador de obrigações internacionais, para Sealand[21] ou para o alto mar[22]. Com frequência, é impossível determinar onde os dados estão fisicamente localizados (servidores que utilizam redes de anonimato como TOR 2 e i2p, por exemplo), ou mesmo autenticar a localização declarada (nem todos os servidores de internet são transparentes quanto ao local de sua operação). A lei não pode ignorar a realizada e o único critério disponível hoje é controle.

Em segundo lugar, o critério controle preserva a territorialidade e a soberania dos Estados. Uma empresa não pode ser constituída, manter escritórios ou subsidiárias, ou prestar serviços em um país, dirigidos especificamente a seus residentes, sem se submeter à lei local. Do contrário, empresas não apenas poderiam escolher a jurisdição, como também a lei que as regula, escolhendo aquela que mais lhes favorece, não necessariamente aquela que melhor protege seus consumidores e usuários. Se é inconcebível que uma empresa possa prestar qualquer tipo de serviço físico sem obedecer à lei local, o mesmo é válido para empresas de internet. O modelo de negócios possui peculiaridades, mas não demanda tratamento preferencial.

O atual quadro da legislação internacional apresenta desafios e o critério controle pode gerar distorções. Entretanto, ele é hoje o principal instrumento aceito internacionalmente e que, na prática, se mostra mais adequado às peculiaridades da prova eletrônica. Os argumentos apresentados no caso Microsoft Irlanda pelo governo norte-americano reforçam que também naquele país, sede da maior parte das empresas que ainda se recusa a atender

[21] https://en.wikipedia.org/wiki/Principality_of_Sealand
[22] http://www.extremetech.com/extreme/222251-under-the-sea-microsoft-testing-underwater-data-centers

requisições diretas, o critério controle passou a ser reconhecido como a única solução prática viável num mundo de computadores e nuvens.