camara-e.net
Câmara Brasileira da Economia Digital

PL 8045/2010: RISCO DE VIGILÂNCIA EM MASSA

A Câmara Brasileira da Economia Digital ("Câmara-e.net"), representante do ecossistema da economia digital, manifesta preocupação com o PL 8045/2010, que estabelece o novo Código de Processo Penal.

Ainda que traga importantes avanços, alguns ajustes são necessários de modo a assegurar um **grau satisfatório de segurança jurídica** e adequar a proposta à legislação específica vigente, em especial ao Marco Civil da Internet (MCI), que já estabeleceu os parâmetros e diretrizes para o uso da internet no país e para a atuação dos provedores de aplicações de internet.

Entre os pontos de atenção, destacam-se **previsões genéricas** e **excessivas** sobre acesso e guarda de prova digital, que subvertem garantias previstas no MCI e podem incentivar a vigilância em massa.

DESTACAMOS 08 PONTOS DO PL 8045/2010

1 Subverte o Racional Consagrado no MCI, que Exige Ordem Judicial para Acessar Dados de Terceiros

O PL - sem considerar que cabe ao delegado de polícia conduzir a investigação criminal - permite que peritos solicitem "documentos, dados e informações" diretamente às entidades públicas e privadas.

Essa previsão não leva em conta a exigência - consagrada no MCI - de **ordem judicial para acessar qualquer dado de terceiro**, cuja exceção é apenas o acesso aos dados cadastrais nas hipóteses previstas legalmente. Esse arranjo não foi eleito pelo legislador à toa, ele garante a **privacidade** e **segurança** dos usuários, assim como a **liberdade de expressão** online, evitando censura e vigilância em massa.

2 Incentiva o Armazenamento Excessivo de Dados e Esvazia o Direito à Privacidade

Ao prever que o acesso e a guarda de dados alcançam qualquer “prova digital”, o PL exige que os provedores armazenem dados **além do limite previsto no Marco Civil da Internet**, que impõe o dever de guarda apenas aos registros de conexão e de acesso. Igualmente, o Decreto regulamentador do MCI (n. 8.771/2014) obriga os provedores a **reterem a menor quantidade possível de dados pessoais**, comunicações privadas e registros de conexão e acesso a aplicações.

Além disso, a previsão de guarda de registros de "dados pessoais, necessários e suficientes" para a individualização dos usuários por 1 ano ***(i)*** gera forte **insegurança jurídica** ao não especificar quais seriam esses dados; e ***(ii)*** contraria o MCI que prevê a guarda de registros de conexão por 1 ano e de acesso por 6 meses, assim como a guarda cautelar por prazo superior a pedido de autoridade.

Quanto ao acesso a esses dados, ainda que tenha previsto requisitos de necessidade, adequação e proporcionalidade, o texto é genérico e não trata das condições mínimas e necessárias para guiar o fornecimento desses dados (individualização do objeto da ordem, indivíduos impactados, período, justificativa motivada, etc.), terminando por incentivar **violações à privacidade dos usuários**.

3 Risco ao Sigilo das Comunicações

Ao disciplinar a interceptação telefônica, a proposta precisa considerar a severidade da medida, que impõe uma grande **limitação à privacidade**, sob pena de **violar o direito dos brasileiros ao sigilo de suas comunicações**. Por isso, a proposta deve ***(i)*** restringir seu uso aos crimes de maior gravidade; e ***(ii)*** vedar pedidos coletivos e genéricos.

Em relação à disposição de meios para a interceptação, é importante destacar que é responsabilidade das concessionárias e operadoras de serviço de telecomunicações, tal como previsto na Lei n. 9.296/1996, que precisam dispor de um prazo razoável para o cumprimento da ordem, na medida de suas capacidades técnicas.

4 Transfere Indevidamente Obrigações do Poder Público aos Particulares

O PL criou a “requisição itinerante”, transferindo indevidamente aos particulares o dever de entregar uma ordem judicial recebida erroneamente em razão de equívoco da autoridade quanto à determinação do responsável por atender à solicitação. Os provedores não possuem meios para identificar o real destinatário da requisição e correm o risco de também errarem ao encaminhá-la, podendo levar à **quebra indevida do sigilo da informação.**

5 Viola o Princípio da Legalidade e Promove a Vigilância em Massa

A proposta viola o princípio da legalidade e pode gerar discordâncias, ilegalidades e **vigilância em massa** ao não definir o que seria “acesso forçado”, “métodos de segurança ofensiva” e “qualquer outra forma que possibilite a exploração, isolamento ou tomada de controle". Na prática, abre espaço para quebra de medidas de segurança do dispositivo eletrônico do investigado (senhas/criptografia) e para busca e apreensão em domicílios de terceiros, inclusive de provedores que teriam acesso aos dados, **desconsiderando eventuais limites técnicos/jurídicos** para sua disponibilização.

6 Prevê Prazos Inadequados

Os prazos previstos pelo PL – ***(i)*** 60 dias para a interceptação, permitidas prorrogações por igual período; e ***(ii)*** 1 ano para guarda da prova digital em razão de requisição do MP ou da "polícia investigativa"- **não são razoáveis**.

Atualmente, a Lei nº 9296/1996 prevê o prazo de interceptação de 15 dias, renováveis por iguais períodos, que é mais razoável e se mostra suficiente, sobretudo considerando que há jurisprudência consolidada possibilitando a renovação por quantas vezes forem necessárias, desde que haja fundamentação. Além disso, o prazo de 1 ano para guarda da prova digital é excessivo, sendo mais razoável sua redução para 15 dias, prazo suficiente para o juiz decidir sobre a pertinência da medida.

7 Risco à Neutralidade da Rede

Tendo em vista os postulados da necessidade e adequação da medida cautelar alternativa à prisão, o investigado precisa ter a oportunidade de remover o conteúdo pessoalmente. Contudo, a proposta ***(i)*** transfere esse dever de remoção para o provedor de aplicações; e ***(ii)*** viola a **neutralidade da rede** e **cria risco de bloqueio das aplicações** ao possibilitar o direcionamento da ordem aos provedores de conexão, podendo **prejudicar milhões de usuários que utilizam os serviços digitais diariamente**.

8 Ajustes na Técnica Legislativa

São necessários alguns ajustes na técnica legislativa de maneira a adequar o texto à legislação vigente: ***(i)*** substituir o termo “polícia investigativa” por “delegado de polícia”, inclusive para evitar abusos de autoridades que não possuem poder para conduzir a investigação criminal; e ***(ii)*** trocar “legítimos interessados” para “partes interessadas”, expressão menos ampla, que harmoniza com demais dispositivos previstos pelo próprio PL.

SUBSTITUTIVO AO PL 8045/2010	SUGESTÃO DE ALTERAÇÃO
Art. 237. O perito oficial possui autonomia técnica e científica, devendo utilizar todos os meios e recursos tecnológicos necessários à realização da perícia, bem como pesquisar vestígios que visem a instruir o laudo pericial, e ainda solicitar: I - à autoridade competente, pessoas e entidades públicas ou privadas, os documentos, dados e informações necessários à realização dos exames periciais.	Art. 237. O**s** perito**s** ~~oficial possui~~ **exercerão suas atividades com** autonomia técnica, ~~e~~ científica **e funcional, podendo** ~~devendo~~ utilizar todos os meios e recursos tecnológicos necessários à realização da perícia, bem como pesquisar vestígios que visem a instruir o laudo pericial, e ainda ~~solicitar~~: I – **requerer** à autoridade competente, ~~pessoas e entidades públicas ou privadas~~, os documentos, dados e informações necessários à realização dos exames periciais.
	Art. 283 (...) **§... Não será admitida a interceptação se o fato investigado constituir infração penal punida, no máximo, com pena de detenção.** **§... São vedados os pedidos coletivos que sejam genéricos ou inespecíficos.**
Art. 288. A prestadora de serviços de telecomunicações deverá disponibilizar, gratuitamente, os recursos e os meios tecnológicos necessários à interceptação, indicando ao juiz o nome do profissional que prestará tal colaboração. § 1º A ordem judicial deverá ser cumprida no prazo máximo de vinte e quatro horas, sob pena de multa diária até o efetivo cumprimento da diligência, sem prejuízo das demais medidas coercitivas e sanções cabíveis. § 2º No caso de ocorrência de qualquer fato que possa colocar em risco a continuidade da interceptação, incluindo as solicitações do usuário quanto à portabilidade ou alteração do código de acesso, suspensão ou cancelamento do serviço e transferência da titularidade do contrato de prestação de serviço, a prestadora deve informar ao juiz no prazo máximo de vinte e quatro horas contado da ciência do fato, sob pena de multa diária, sem prejuízo das demais medidas coercitivas e sanções cabíveis.	Art. 288. ~~A prestadora~~ **As concessionárias/operadoras** de serviços de telecomunicações dever**ão** disponibilizar, gratuitamente, os recursos e os meios tecnológicos necessários à interceptação, indicando ao juiz o nome do profissional que prestará tal colaboração. § 1º A ordem judicial deverá ser cumprida **pelos destinatários no prazo de 48 (quarenta e oito) horas, na medida de sua capacidade técnica.** ~~no prazo máximo de vinte e quatro horas, sob pena de multa diária até o efetivo cumprimento da diligência, sem prejuízo das demais medidas coercitivas e sanções cabíveis.~~ **§ 2º Exclusão**
Art. 301. Poderão os legítimos interessados, para o fim da investigação ou instrução processual, requerer ordem judicial para guarda e acesso à prova digital sob controle de terceiros, observados os requisitos de necessidade, adequação, finalidade e proporcionalidade. § 1º O requerimento deve individualizar usuários, provedores, dispositivos eletrônicos ou sistemas informáticos, temporalidades, redes de dados e protocolos de rede próprios ao contexto do legítimo interesse manifestado, não podendo ter caráter genérico. § 2º Os dados transmitidos ou encaminhados em suporte físico, pelos controladores ou provedores em cumprimento de ordem judicial ou, sendo dados cadastrais, por requisição da autoridade policial e do Ministério Público, devem estar em formato interoperável e com garantia de autenticidade e integridade.	Art. 301. Poderão ~~os legítimos~~ **as partes** interessadas, para o fim da investigação ou instrução processual, requerer ordem judicial para guarda e acesso à prova digital sob controle de terceiros, observad**a a legislação específica e atendidos** os requisitos de necessidade, adequação e proporcionalidade. **§ 1º Sem prejuízo dos demais requisitos legais, o requerimento e a ordem judicial correspondente devem:** a) individualizar usuários; **b) individualizar os dados buscados;** **c) especificar o período de datas para as quais se referem os dados buscados;** **d) especificar os provedores de conexão ou aplicações, dispositivos eletrônicos ou sistemas informáticos, redes de dados e protocolos de rede próprios ao contexto do legítimo interesse manifestado, considerando os controladores dos dados;** **e) apresentar justificativa motivada para acesso à prova digital.** **§ 2º São vedados pedidos coletivos que sejam genéricos ou inespecíficos.**

	§ 3º Os dados transmitidos ou encaminhados em suporte físico, pelos controladores **dos dados** ~~ou provedores emcumprimento de ordem judicial, ou, sendo dados cadastrais, por requisição da autoridade policial e do Ministério Público,~~ devem estar em formato interoperável e com garantia de autenticidade e integridade, **nos limites de sua capacidade técnica.** **§ ... Nas hipóteses do caput, o juiz, respeitado o contraditório, decidirá acerca da realização da diligência ou solicitação.**
Art. 302. Os provedores de conexão e aplicação deverão manter, além das informações de guarda legal previstas em lei, os registros de dados pessoais necessários e suficientes para a individualização inequívoca dos usuários de seus serviços pelo prazo de um ano.	**Art. 302. Exclusão integral**
Art. 303. Se houver receio de que a prova digital possa perder-se, alterar-se ou deixar de estar disponível, poderá o juiz, a requerimento do legítimo interessado, ordenar a quem tenha disponibilidade, controle ou opere os dados, que os guarde pelo prazo de até um ano, podendo este prazo ser renovado, observadas a necessidade, adequação e proporcionalidade.	Art. 303. Se houver receio de que a prova digital possa perder-se, alterar-se ou deixar de estar disponível, poderá o juiz, a requerimento **da parte interessada** ~~do legítimo interessado,~~ ordenar a quem tenha disponibilidade, controle ou opere os dados, que os guarde pelo prazo de até **seis meses** ~~um ano,~~ podendo este prazo ser renovado, observadas a necessidade, adequação e proporcionalidade. **§1º São vedados os pedidos coletivos que sejam genéricos ou inespecíficos.** **§2º Nas hipóteses do caput, o juiz, respeitado o contraditório, decidirá acerca da realização da diligência ou solicitação.** **§3º Poderá o juiz decidir, fundamentadamente, sem a manifestação da parte contrária nas hipóteses em que seu conhecimento possa frustrar a medida.**
Art. 306. O provedor de estrutura, de conexão ou de aplicação em face da qual tenha sido expedida a diligência, constatando que a medida deve ser cumprida por outro provedor, remeterá a requisição a este em caráter itinerante, a fim de se praticar o ato, independentemente de nova ordem, comunicando-se à autoridade judicial ou ao órgão de investigação em vinte e quatro horas. § 1º No mandado constará que o redirecionamento se reveste de obrigatoriedade, independentemente de nova ordem. § 2º Os provedores em face da qual tenha sido ordenada a diligência indicarão à autoridade judiciária e ao órgão de investigação, em vinte e quatro horas, os outros provedores através dos quais tenha tido conhecimento da ocorrência de tráfego de dados pertinentes ao alvo da interceptação, com o fim de identificar todos os provedores envolvidos.	**Art. 306: Exclusão integral**
Art. 307. A coleta por acesso forçado a dispositivo eletrônico, sistema informático ou redes de dados, ocorrerá somente após prévia desobediência de ordem judicial determinando a entrega da prova pretendida ou quando impossível identificar o controlador ou provedor em território nacional, e compreenderá os métodos de segurança ofensiva ou qualquer outra forma que possibilite a exploração, isolamento e tomada de controle. Parágrafo único. Em caso de dispositivo, sistema informático ou redes de dados que se encontrem em território estrangeiro, somente se procederá por via da cooperação internacional.	**Art. 307: Exclusão integral**

Art. 308, § 1º Em caso de monitoramento do fluxo de dados, o prazo da medida não poderá exceder a sessenta dias, permitidas prorrogações por igual período, desde que continuem presentes os pressupostos autorizadores da diligência, até o máximo de trezentos e sessenta dias, salvo quando se tratar de crime permanente, enquanto não cessar a permanência.
(...)

§ 3º A polícia investigativa ou o Ministério Público poderá requisitar a guarda da prova digital sem acesso ao conteúdo pelo prazo de um ano, independentemente de autorização judicial, quando houver perigo na demora, devendo comunicar a medida ao juiz competente em até vinte e quatro horas, para validação da medida.

Art. 668. Em caso de crimes praticados por meio da internet, o juiz poderá determinar ao provedor de aplicação que torne e mantenha indisponível, nos limites técnicos do seu serviço, conteúdo de localização específica e inequivocamente utilizado para a execução de infrações penais.

Parágrafo único. Caso o provedor de aplicação não possua estabelecimento no País, o juiz poderá determinar a indisponibilidade do conteúdo de que trata o caput a provedores de conexão à internet.

Art. 308, § 1º **A ordem de que trata o caput deve especificar os indivíduos cujos dados estão sendo requeridos, sendo vedados pedidos coletivos que sejam genéricos ou inespecíficos.**

§ 2º Em caso de **interceptação** ~~monitoramento do fluxo de dados,~~ o prazo da medida não poderá exceder a **quinze dias** ~~sessenta dias,~~ permitidas prorrogações por igual período, desde que continuem presentes os pressupostos autorizadores da diligência, até o máximo de ~~trezentos e sessenta dias~~ **180 (cento e oitenta dias)**, salvo quando se tratar de caso em que **exista risco iminente à vida ou integridade física de indivíduos específicos** ~~crime permanente, enquanto não cessar a permanência.~~
(...)
§ **4º O delegado de polícia** ~~polícia investigativa~~ ou o Ministério Público poderá requisitar a guarda da prova digital sem acesso ao conteúdo pelo prazo **de quinze dias** ~~de um ano,~~ independentemente de autorização judicial, quando houver perigo na demora, devendo comunicar a medida ao juiz competente em até vinte e quatro horas, para validação da medida, **quando o juiz poderá determinar, conforme a regra geral, a guarda dos dados obtidos.**

Art. 668. Em caso de crimes praticados por meio da internet, o juiz poderá determinar ao **investigado que promova o bloqueio de conta de aplicação de internet utilizada para execução de infrações penais ou do conteúdo apontado como infringente veiculado na rede mundial de computadores** ~~provedor de aplicação que torne e mantenha indisponível, nos limites técnicos do seu serviço, conteúdo de localização específica e inequivocamente utilizado para a execução de infrações penais.~~
~~Parágrafo único. Caso o provedor de aplicação não possua estabelecimento no País, o juiz poderá determinar a indisponibilidade do conteúdo de que trata o caput a provedores de conexão à internet.~~
§1º Em caso de descumprimento, o juiz poderá proferir ordem judicial direcionada aos provedores de aplicações de internet, para que, no âmbito e nos limites técnicos de seus serviços, bloqueiem a conta de aplicação de internet utilizada para a execução de infrações penais ou o conteúdo apontado como infringente.
§2º A ordem judicial de que trata o parágrafo anterior deve, sob pena de nulidade, conter elementos que permitam a identificação clara, específica e inequívoca do conteúdo a ser indisponibilizado, mediante endereço completo de URL e, no caso de conta de aplicação de internet, identificador válido junto ao provedor de aplicação, que permita a identificação da conta, de forma inequívoca.