1. Introdução

"Marco Civil da Internet" é o nome pelo qual ficou conhecido a Lei Federal 12.965/2014, antigo Projeto de Lei nº 2.126/2011, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

O processo de construção do Marco Civil da Internet foi único: teve inspiração no Decálogo da Internet – dez princípios fundamentais, estabelecidos pelo Comitê Gestor da Internet no Brasil, para embasar as ações para o desenvolvimento da Internet em nosso país – e foi objeto de consulta pública online em duas fases: na primeira, indagou-se à comunidade de usuários, empresas, sociedade civil e ao público em geral quais temas deveriam fazer parte de um marco regulatório civil para a Internet no Brasil; na segunda, com apoio nas contribuições recebidas na fase anterior, um texto-base do projeto de lei foi apresentado à sociedade e submetido à consulta aberta, resultando em centenas de contribuições e manifestações – todas elas publicadas online no endereço <http://culturadigital.br/marcocivil/>.

No entanto, desde que a ideia de um Marco Civil para a Internet brasileira foi apresentada, questionava-se qual seria a efetiva necessidade de sua existência. A maioria dos críticos argumentava, por exemplo, que "regular a internet por lei é algo totalmente desnecessário, sem sentido e inócuo"[1], e que as leis existentes já seriam suficientes para proteger os direitos dos cidadãos no ambiente online.

Os críticos da proposta, porém, não haviam compreendido que o objetivo do Marco Civil da Internet era duplo: consagrar direitos dos usuários da Internet – notadamente privacidade, liberdade de expressão e neutralidade da rede – e estabelecer segurança jurídica para as atividades de plataformas digitais, redes sociais e dos demais serviços oferecidos online.

2. A importância das plataformas digitais e das redes sociais

Apesar de vivermos em um mundo cada vez mais conectado, nem sempre compreendemos todos os benefícios trazidos pelas plataformas digitais e pelas redes sociais. Diversos fatores econômicos, sociais e jurídicos evidenciam a importância de um tratamento jurídico equilibrado para as atividades desempenhadas por esses atores, pois do contrário haveria retração do uso de

1 Cf., por todos, SIQUEIRA, Ethevaldo. *Entenda o polêmico Marco Civil da Internet.* Texto publicado em 12/3/2014. Disponível em <http://www.telequest.com.br/portal/index.php/destaque/1182-para-entender-o-polemico-marco-civil-da-internet>.

ferramentas e de plataformas online, com prejuízos diretos aos usuários. Abaixo destacamos, sinteticamente, alguns desses fatores:

a) Ferramentas digitais têm uma importante função social. Serviços e plataformas online transformaram o cenário social e político, facilitando a comunicação e o acesso ao governo e criando novas possibilidades de interação, organização e mobilização social, na maioria dos casos por meio de serviços e plataformas gratuitos ou de baixo custo. As recentes reformas políticas e a queda de regimes totalitários em diversos países do mundo, parcialmente facilitadas pelo uso de ferramentas online, evidenciam o potencial democratizante da Internet.

b) A proteção das plataformas digitais promove a liberdade de expressão, o acesso à informação, à educação e à cultura. A Internet possibilita que pessoas expressem suas opiniões sem interferências, recebendo e compartilhando informações livremente, promovendo a integração regional, a inclusão social e o rompimento de barreiras socioeconômicas. O conteúdo gerado por usuários e disponibilizado por meio de serviços e plataformas oferecidas pelos provedores representa, hoje, uma das principais formas de expressão, fomentando o pensamento crítico e o estabelecimento de novas comunidades. Um ambiente de insegurança jurídica a respeito do tratamento legal desse conteúdo poderia forçar as plataformas digitais e as redes sociais a fechar os espaços ou a desativar as ferramentas que viabilizam essas formas de atividade, fazendo com que todo o potencial desses espaços e dessas ferramentas fosse desperdiçado. Não se pode inverter a lógica de que a Internet é uma das maiores conquistas tecnológicas da humanidade para presumir, perigosa e falsamente, que ela apenas serve para a prática de atos ilícitos.

c) Plataformas digitais e redes sociais exercem grande variedade de papéis econômicos. Além de gerar empregos e tributos por meio de novos modelos de negócio e de constante inovação, as ferramentas online fomentam o comércio de bens e serviços, ampliam o acesso de consumidores à informação e criam novos canais de interação com fornecedores. Os serviços gratuitos ou de baixo custo oferecidos pelos provedores inserem na economia digital microempresas, empreendedores e pessoas físicas, reduzindo tanto os custos para o empresário quanto os preços para o consumidor.

d) A segurança jurídica no ambiente online fomenta a inovação nacional. A próxima revolução online é apenas uma ideia neste momento. A inovação na Internet depende da existência de um sistema jurídico equilibrado que proteja provedores de responsabilidade pelos atos de seus usuários. A ausência

de salvaguardas aumenta tremendamente os custos para empreendedores, pequenas empresas e startups brasileiras, criando disparidades que inviabilizam a inovação nacional e afugentam investimentos estrangeiros. A insegurança jurídica sobre este tema sempre era apontada como um dos principais obstáculos ao desenvolvimento de serviços e plataformas nacionais na Internet por pequenos empresários e empreendedores brasileiros, pois salvaguardas se aplicam a todos os provedores – grandes, médios ou pequenos – e são essenciais para o oferecimento de novos serviços e plataformas online.

3. O combate a atos ilícitos online pré e pós Marco Civil da Internet

Pré-Marco Civil da Internet, o combate a atos ilícitos online era tarefa complexa, dificultada pela insegurança jurídica existente em decorrência de diversas lacunas no ordenamento jurídico brasileiro.

Entre as diversas incertezas sobre o tema, destacavam-se:

i) plataformas digitais e redes sociais deveriam ou não guardar dados a respeito de seus usuários? Seria melhor adotar um modelo de retenção ou de preservação de dados? Quais as consequências jurídicas decorrentes da guarda ou não-guarda desses dados?

ii) quais dados deveriam ser guardados? Como assegurar o sigilo desses dados? Quais medidas de segurança deveriam ser adotadas?

iii) por quanto tempo esses dados deveriam ser guardados?

iv) quem poderia ter acesso a esses dados? Qualquer pessoa, apenas a vítima, apenas autoridades, apenas o Poder Judiciário?

v) qual o procedimento correto para ter acesso a esses dados? Simples notificação? Requerimento de autoridade? Somente ordem judicial?

Até a Lei 12.965/2014 detalhar esse tema, era possível encontrar decisões judiciais em todos os sentidos, o que dificultava tanto as atividades das empresas que oferecem produtos e serviços online quanto as próprias investigações conduzidas por autoridades e por representantes dos interessados.

O Marco Civil da Internet tentou trazer respostas claras a essas indagações ao assegurar a privacidade do usuário da Internet tanto em relação ao tratamento de seus dados pessoais quanto em relação à inviolabilidade e sigilo de suas comunicações privadas. Boa parte dos debates sobre a proteção da

inviolabilidade e do sigilo das comunicações privadas do usuário da Internet está ligada ao combate a atos ilícitos online.

Com efeito, discute-se mundialmente, inclusive na doutrina e na jurisprudência, se provedores de serviços online devem ou não utilizar meios tecnológicos e equipamentos informáticos que possibilitem a identificação dos dados de conexão dos usuários, para que tais informações sejam disponibilizadas a quem de direito em caso de ato ilícito, pois nem sempre os dados cadastrais contendo os nomes, endereços e demais dados pessoais dos usuários estarão corretos ou atualizados.

Esclareça-se que os dados cadastrais consistem nas informações pessoais fornecidas pelo usuário ao provedor de serviços, tais como nome, endereço, números de documentos pessoais ou empresariais e demais informações necessárias à instalação, funcionamento e cobrança dos serviços.

Os dados de conexão consistem nos endereços IP utilizados durante o acesso à Internet, bem como em outras informações relativas ao uso da rede, tais como datas e horários de *login* e *logout*, nome de usuário utilizado e demais informações técnicas que tenham por objetivo identificar determinado usuário. Não englobam, portanto, o conteúdo das comunicações, nem as transmissões de dados realizadas pelo usuário, mas apenas os dados vinculados à sua identificação ao acessar um serviço online.

Os deveres de conhecer determinados dados dos usuários e de mantê-los por tempo determinado encontram-se previstos nos artigos 13[2] e 15[3] do Marco Civil da Internet.

---

2 Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. § 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros. § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no **caput**. § 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no **caput**. § 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º. § 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo. § 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

3 Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

Como se percebe, o Marco Civil da Internet impõe aos provedores que fornecem acesso à Internet o dever de guardar, por um ano, os registros de **conexão** – definidos no artigo 5º, inciso VI, como o *"conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados"*.

Da mesma forma, o Marco Civil da Internet impõe aos provedores de aplicações – conceito que engloba, nos termos da definição prevista no artigo 5º, inciso VII, o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet e abrange, portanto, provedores de correio eletrônico, de hospedagem e de conteúdo, entre diversos outros – o dever de guardar, por seis meses, os registros de **acesso a aplicações de Internet** – definidos no artigo 5º, inciso VIII, como o *"conjunto de informações referentes à data e hora de uso de uma determinada aplicação de Internet a partir de um determinado endereço IP"*.

Como se vê, o Marco Civil da Internet impôs um modelo de guarda obrigatória de dados para os provedores de aplicações, e não *facultativa*, como originalmente previsto. Adotou, assim, um modelo único de *retenção de dados* de forma indiscriminada, em oposição a um modelo de preservação dos dados efetivamente ligados a um ato ilícito praticado, o que implica tratar todos os usuários de Internet como suspeitos da prática de atos ilícitos, com sérias implicações para sua privacidade.

Como mencionado, em sua versão original o Marco Civil da Internet privilegiava o modelo de *preservação de dados*, impondo a provedores de conexão e de aplicações que recebem uma ordem judicial o dever de preservar, *a partir daquele momento*, dados específicos de usuários determinados, suspeitos de terem praticado crimes ou atos ilícitos por meio da Internet. Todos os demais usuários do provedor não seriam afetados.

§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no **caput** a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no **caput**, observado o disposto nos §§ 3º e 4º do art. 13.

§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Insista-se, portanto, que para a proteção da privacidade do usuário **o modelo de preservação de dados é mais adequado.** Isso porque, nesse modelo, a guarda de registros apenas é realizada a partir do momento em que há uma denúncia ou se constata uma suspeita da ocorrência de crime ou de prática de ato ilícito, iniciando-se então o processo de investigação somente contra os possíveis usuários envolvidos, sem implicações para os direitos dos demais usuários de um determinado serviço. Com isso, torna-se possível combater ilícitos e crimes online sem violar normas constitucionais nem afetar direitos fundamentais dos cidadãos, atendendo assim ao necessário sopesamento entre princípios e à regra da proporcionalidade.

Convém recordar que a Alemanha, a Romênia e a República Checa, primeiros países europeus a adotar normas de retenção de dados em obediência à Diretiva Europeia 2006/24/CE, acabaram por rejeitar esse modelo, entendendo a Corte Constitucional de cada um desses países que a retenção de dados de usuários, notadamente de registros de acesso a aplicações de Internet, viola a privacidade do cidadão e a regra da proporcionalidade.

Do mesmo modo, Peter Hustinx, Supervisor Europeu de Proteção de Dados, emitiu opinião concluindo pela inadequação da Diretiva Europeia 2006/24/CE, recordando que ela foi adotada no clamor dos atentados terroristas que ocorreram na Europa em 2004 (Madri) e 2005 (Londres), enfatizando que: a) a Diretiva não alcançou seus objetivos desde que foi criada; b) mecanismos de retenção de dados não são úteis, nem necessários para combater ilícitos online; c) leis nacionais europeias de retenção de dados, tais como implementadas, não obedecem as próprias normas europeias e internacionais de privacidade, violando os direitos fundamentais dos cidadãos.

Finalmente, em abril de 2014, a Corte Europeia de Justiça declarou inválida a **Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações** eletrónicas publicamente disponíveis ou de redes públicas de comunicações, por entender que *"ao adotar a Diretiva 2006/24, o legislador da União excedeu os limites impostos pelo respeito do princípio da proporcionalidade à luz dos artigos 7º, 8º e 52º, nº* **1, da Carta dos Direitos Fundamentais da União Europeia"**.[4]

4 Cf. Corte Europeia de Justiça, Digital Rights Ireland Ltd (C-293/12) contra Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of

Aliás, foi exatamente por este motivo – adoção de um modelo de retenção de dados de todos os usuários de forma indiscriminada, pelo prazo de três anos, ignorando a privacidade dos usuários – que o Projeto de Lei 84/99 ficou conhecido entre os membros da sociedade civil como "AI-5 Digital". Independentemente do eventual exagero de retórica, isso deixa claro que a população brasileira de usuários da Internet não aceita retenção de dados realizada de forma indiscriminada e por prazo tão longo, está preocupada com sua privacidade e alarmada pelo fato de ser vista como suspeita sem nada ter feito de errado, notadamente quando se recorda que uma parcela ínfima de usuários de Internet comete crimes ou ilícitos online.

Seja como for, os provedores de aplicações de Internet também têm o dever de manter em sigilo todos os dados cadastrais e de conexão de seus usuários, observando-se, apenas, as exceções previstas contratualmente e as outras que forem aplicáveis, na forma da lei.

Nesse ponto, o Marco Civil da Internet impõe aos provedores o dever geral de sigilo com relação aos registros de conexão e de acesso de seus usuários, estabelecendo inclusive punições em caso de violação do sigilo dessas informações:

> *Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.*
>
> *§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no* ***caput****, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.*
>
> *§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.*

the Garda Síochána, Irlanda, The Attorney General. Íntegra do acórdão disponível em <http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d51038ac09f7174cfd819eaa6ad22d753b.e34KaxiLc3eQc40LaxqMbN4OaNmNeo?text=&docid=150642&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=171877>.

> *§ 3º O disposto no* ***caput*** *não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.*
>
> *§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.*

Evidentemente, o sigilo dos dados cadastrais e de conexão de um usuário pode ser afastado quando este comete um ato ilícito por meio da Internet. Em tal situação, caso os provedores de serviços de Internet tenham armazenado tais dados, poderão informá-los à vítima, **sempre mediante ordem judicial específica.**

Isso porque fornecer dados de usuários da Internet, sem ordem judicial específica, representaria desobediência às normas impositivas da Constituição Federal que asseguram a privacidade e o sigilo de dados do indivíduo.

Além disso, a obtenção, *sem ordem judicial*, de dados de usuários supostamente envolvidos em atos ilícitos poderia ser prejudicial à própria investigação, já que provas obtidas em desobediência à Constituição Federal e fora do devido processo legal podem, eventualmente, ser consideradas inadmissíveis, ante o disposto no artigo 5º, inciso LVI da Constituição Federal, no artigo 332 do Código de Processo Civil, no artigo 157 do Código de Processo Penal e em outros dispositivos de legislação específica.

Por outro lado, importante destacar que a *quebra de sigilo* de dados cadastrais e de conexão é distinta da *interceptação* ou *monitoramento* de informações transmitidas através da Internet (esta última regulada pela Lei 9.296/96), pois os dados cadastrais e de conexão de um usuário não se confundem com o conteúdo das comunicações eletrônicas realizadas por ele. O sigilo dos dados cadastrais e de conexão é protegido pelo direito à privacidade, que não prevalece em face de ato ilícito cometido, pois, do contrário, permitir-se-ia que o infrator permanecesse no anonimato.

O Marco Civil da Internet estabelece, em seu artigo 22, ser sempre obrigatória a intervenção do Poder Judiciário para a revelação de informações de usuários da Internet, cabendo ao juiz determinar, conforme previsto no artigo 23, as providências necessárias para assegurar a proteção da privacidade dos envolvidos, nos seguintes termos:

Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I – fundados indícios da ocorrência do ilícito;

II – justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III – período ao qual se referem os registros.

Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

Note-se que o Marco Civil da Internet expressamente destaca que o fornecimento de dados pode ocorrer para fins de formação de conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, e não apenas em caso de investigação criminal ou instrução processual penal, o que demonstra que ordem judicial nesse sentido pode ser proferida em procedimento de qualquer natureza.

4. A remoção de conteúdo pré e pós Marco Civil da Internet

Entre os diversos temas regulados pelo Marco Civil da Internet, poucos despertam tanta polêmica quanto a remoção de conteúdo em plataformas digitais e redes sociais.

Pré-Marco Civil da Internet, a remoção de conteúdo de plataformas digitais e redes sociais estava sujeita a uma série de interpretações distintas. A jurisprudência brasileira apresentava, muitas vezes, soluções díspares e contraditórias.

Entre as diversas incertezas sobre o tema, destacavam-se:

i) plataformas digitais e redes sociais deveriam exercer controle editoral prévio sobre o conteúdo publicado por seus usuários?

ii) devem ser estabelecidos filtros para impedir a publicação de certos tipos de conteúdo?

iii) quais os critérios para a remoção de conteúdo? Eventual colisão entre a liberdade de expressão e outros direitos fundamentais deveria ser arbitrada pelas plataformas digitais e redes sociais?

iv) em que momento se poderia considerar que um conteúdo é ilegal? Bastaria a reclamação de quem se sinta prejudicado? Seria obrigatória a análise do Poder Judiciário como regral geral?

v) qual deveria ser a regra geral para remoção de conteúdo? Simples notificação? Requisição de autoridade? Ordem judicial?

vi) a remoção de conteúdo podia ser genérica ou deveria ser individualizada, com indicação dos endereços eletrônicos em que o conteúdo se encontra?

O Marco Civil da Internet passou por momentos distintos em relação ao tema. Ainda na fase de consulta pública, antes de o texto final ser consolidado e apresentado como projeto de lei 2.126/2011, a proposta para remoção de conteúdo era de um sistema de notificação e retirada ("notice and takedown") de qualquer tipo de conteúdo produzido por terceiros, que funcionaria da seguinte forma:

a) ao receber uma reclamação válida, o provedor deveria remover, em tempo razoável, o conteúdo questionado;

b) depois que o conteúdo questionado fosse removido, o provedor deveria notificar o usuário que o publicou, avisando-o sobre a remoção;

c) o usuário poderia aceitar a remoção ou assumir a responsabilidade, hipótese em que poderia contranotificar o provedor e exigir que o conteúdo questionado seja restabelecido;

d) se o provedor não recebesse resposta ou não conseguisse entrar em contato com o usuário, o conteúdo questionado permanece removido;

e) qualquer outra pessoa ou empresa poderia assumir a responsabilidade pelo conteúdo questionado e enviar contranotificação para que o provedor restabelecesse esse conteúdo. Ao fazer isso, essa pessoa ou empresa submeter-se-ia a todos os riscos e consequências a que estaria sujeito o usuário que originalmente publicou o conteúdo;

f) se o provedor seguisse esses procedimentos, não seria responsabilizado pelo conteúdo questionado.

Essa proposta foi abandonada ainda em fase de consulta pública, em razão dos tremendos riscos que apresentava para a liberdade de expressão online. Parece simples constatar que um sistema que permitisse a pronta remoção de informações online mediante simples reclamação do interessado, sem análise judicial, criaria espaço para que reclamações frívolas, que jamais seriam acolhidas pelo Judiciário, fossem necessariamente atendidas pelos provedores, que seriam obrigadas a fazê-lo para se isentar de responsabilidade.

O contraponto é que o usuário que tivesse suas informações removidas (ou mesmo outra pessoa, em seu lugar) também poderia exigir, mediante simples contranotificação, que elas fossem restabelecidas. À primeira vista, a solução pareceria excelente: garantiria o contraditório, presumindo que todo usuário que se sentisse injustamente cerceado rebateria o pedido de remoção e exigiria, de imediato, o restabelecimento de seu conteúdo.

Ocorre, porém, que não há como presumir que os usuários que tenham suas informações removidas iriam efetivamente rebater essas reclamações, ou ainda encontrar alguém que se responsabilizasse por elas em seu lugar.

Sem ter a segurança jurídica necessária a respeito de suas próprias manifestações e temerosos de serem responsabilizados por elas, a tendência óbvia desses usuários seria a de se calar e de aceitar a remoção injusta do conteúdo, por lhes faltar capacidade técnica, econômica e jurídica para defender suas opiniões. Isso era extremamente comum em blogs, redes sociais e outros serviços online, em que indivíduos se sentiam intimidados com o simples envio de notificação extrajudicial exigindo a remoção de conteúdo e, lamentavelmente, acabavam por acatar pedidos manifestamente descabidos, pelos motivos destacados.

Ao afastar a proposta de um sistema padrão de notificação e retirada, o legislador reconheceu que, ao menos como regra geral, mecanismos de notificação e retirada de conteúdo sem ordem judicial sofrem de graves problemas, detalhados a seguir:

a) Notificação e retirada incentiva a remoção arbitrária de conteúdo. A possibilidade de remoção sumária de informações online mediante simples reclamação do interessado, sem ordem judicial, cria espaço para que reclamações frívolas, infundadas ou até mesmo ilegais, que jamais seriam acolhidas pelo Judiciário, sejam necessariamente atendidas pelas plataformas online, que

ficariam obrigadas a fazê-lo para se isentar de responsabilidade. Essa situação incentiva a remoção arbitrária de conteúdo, atribuindo a uma requisição privada o mesmo poder de uma medida liminar, sem o necessário devido processo legal.

b) Regras procedimentais de notificação e retirada não impedem a censura temporária. Ainda que eventuais regras procedimentais tentem impedir abusos na utilização de mecanismos de notificação e retirada, isso não afasta o risco de imposição de censura temporária, calando manifestações cujo momento de divulgação é crucial (tais como campanhas políticas, acontecimentos recentes e notícias urgentes) e cuja divulgação posterior será inútil ou irrelevante.

c) Notificação e retirada permite abusos frequentes. Estudos realizados por membros da Electronic Frontier Foundation e do Berkman Center for Internet & Society da Harvard Law School demonstram[5], com riqueza de exemplos, que o sistema de notificação e retirada instituído nos Estados Unidos pelo DMCA é rotineiramente utilizado de forma abusiva, servindo como ferramenta de intimidação ou sendo empregado impropriamente para a retirada de conteúdo não protegido por direito autoral, trazendo enormes implicações para a liberdade de expressão, além de não combater adequadamente a violação de direitos online. Entre outras situações, o conteúdo indevidamente removido por abuso do DMCA inclui fatos e informações não sujeitos à proteção autoral, material em domínio público, crítica social e material de utilização livre em razão de limitações aos direitos autorais.

d) Notificação e retirada não oferece granularidade e é desproporcional. Em muitas situações, o conteúdo apontado como ilegal consiste em apenas um item (ou seja, um único arquivo, texto, vídeo, fotografia, post, link ou URL), mas a plataforma ou o serviço são obrigados a desativar completamente um website para atender à notificação e se beneficiar da isenção de responsabilidade. Como exemplo, isso ocorre quando o serviço apenas oferece espaço para armazenamento de websites e não controla nem gerencia as ferramentas utilizadas por seus usuários. Essa ausência de granularidade do mecanismo de notificação e

5 Cf. Fred Von Lohmann, "Unintended Consequences: Twelve Years under the DMCA" (texto de 2010, relatando prejuízos à inovação tecnológica, à pesquisa científica e aos direitos de consumidores como algumas das consequências indesejadas do DMCA), disponível em <https://www.eff.org/files/eff-unintended-consequences-12-years.pdf>.

(8) Cf. Wendy Seltzer, "Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment" (relatando diversos casos de abuso do sistema de notificação e retirada previsto pelo DMCA, com graves implicações para a liberdade de expressão online, disponível em <http://jolt.law.harvard.edu/articles/pdf/v24/24HarvJLTech171.pdf>).

retirada traz sérias implicações para a liberdade de expressão online e ofende a regra da proporcionalidade consagrada no sistema constitucional brasileiro.

Como se sabe, a liberdade de expressão é um direito fundamental consagrado tanto pela Constituição Federal brasileira quanto pelos tratados internacionais dos quais o Brasil é signatário, entre os quais a Declaração Universal dos Direitos Humanos, que em seu artigo 19 estabelece que todas as pessoas *"têm direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferências, ter opiniões e de procurar, receber e transmitir informações e ideias* ***por quaisquer meios****, independentemente de fronteiras"*.

O livre fluxo de informações é essencial para a criatividade e inovação, gerando desenvolvimento social, cultural e econômico. As plataformas e os serviços online exercem um papel fundamental nesse processo.

O Marco Civil da Internet enfatiza a importância da liberdade de expressão online em diversos pontos de seu texto e cria regras claras para assegurar sua tutela. Como exemplos, o texto estabelece que a disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão (art. 2º) e tem, entre outros princípios, a garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal (art. 3º), mencionando ainda que a garantia da liberdade de expressão nas comunicações é uma condição para o pleno exercício do direito de acesso à Internet (art. 8º).

No entanto, a regra mais importante para a tutela da liberdade de expressão online está prevista no artigo 19 do Marco Civil da Internet, que trata da responsabilidade civil dos provedores de aplicações, e que tem a seguinte redação:

> *Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.*
>
> *§ 1º A ordem judicial de que trata o* **caput** *deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.*
>
> *§ 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal.*
>
> *§ 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.*
>
> *§ 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.*

Como se constata, o artigo 19 do Marco Civil da Internet estabelece uma regra geral de isenção de responsabilidade dos *"provedores de aplicações"* pelo conteúdo gerado por terceiros. Como visto, o conceito de "provedores de aplicações" engloba, nos termos da definição prevista no artigo 5º, inciso VII, o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet e abrange, portanto, provedores de correio eletrônico, de hospedagem e de conteúdo, entre diversos outros.

Repita-se, para maior clareza: **o artigo 19 do Marco Civil da Internet não diz que remoção de conteúdo somente pode ocorrer por força de ordem judicial.** Ou seja: ***o artigo esclarece que o provedor pode ser responsabilizado em caso de descumprimento de ordem judicial de remoção forçada de conteúdo, mas não diz – e nem poderia dizer – que qualquer remoção de conteúdo somente pode ocorrer por ordem judicial.***

Isso significa que cada provedor continua livre para implementar as políticas que entender pertinentes para remoção voluntária de conteúdo. Não se deve pensar, portanto, que o provedor está de mãos atadas, aguardando por uma ordem judicial: ele pode perfeitamente remover o conteúdo de acordo com seus termos de uso, suas políticas e outras práticas.

Como se vê, a remoção judicial – ao menos como regra geral, admitidas exceções específicas para problemas extraordinários – é o mecanismo mais equilibrado para lidar com conteúdo ilícito online. Em linhas gerais, não é possível afastar a necessidade de análise pelo Judiciário e de ordem judicial específica

para a retirada forçada de conteúdo, já que decidir sobre a legalidade ou ilegalidade do material, em todas as suas possíveis formas, é algo necessariamente subjetivo, além de ser prerrogativa exclusiva do Judiciário.

Recorde-se que muitas informações controversas são mantidas online, hoje, porque aqueles interessados na remoção desse conteúdo sabem que o Judiciário não concederia ordens nesse sentido. Se assim não fosse, haveria um grande risco de que pessoas e empresas passariam a exigir a remoção de informações claramente lícitas, apenas porque a divulgação desse material não lhes agrada.

A exigência de análise judicial para a remoção do conteúdo privilegia a liberdade de expressão ao evitar que muitas manifestações relevantes, porém desagradáveis a estes ou aqueles interesses, sejam removidas sem razão jurídica.

Em minhas obras, sempre destaquei o seguinte:

> *(...) Havendo controvérsia sobre a ilicitude do conteúdo, e não tendo ocorrido violação dos termos de uso do web site, não devem os provedores de hospedagem ou de conteúdo remover ou bloquear o acesso às informações disponibilizadas mas, sim, aguardar a resolução do problema pelo Poder Judiciário, a quem caberá decidir se houve ou não excesso no exercício das liberdades de comunicação e de manifestação de pensamento, violação a direitos autorais ou de propriedade intelectual, entre outras práticas passíveis de lesar direitos alheios, e determinando, em caso positivo, as providências necessárias para fazer cessar a prática do ilícito. Recorde-se, ainda, que tal solução é a que melhor atende aos interesses da vítima, tendo como vantagem não sujeitar o provedor a emitir juízo de valor sobre a licitude do conteúdo, o que poderia causar distorções graves ou decisões arbitrárias."*[6]

Ressalte-se que esse modelo não é novo, pois a remoção judicial de conteúdo online já faz parte do sistema jurídico brasileiro. A Lei nº 12.034/2009, que tratou da reforma eleitoral, estabeleceu que provedores somente serão responsabilizados pela divulgação de propaganda eleitoral irregular caso sejam notificados da existência de decisão da Justiça Eleitoral e não tomem providências para cessar essa divulgação, dentro do prazo assinalado pela decisão judicial[7].

6 Cf. Leonardi, Marcel. *Responsabilidade Civil dos Provedores de Serviços de Internet.* São Paulo: Juarez de Oliveira, 2005, p. 182.

7 "Art. 57-F - Aplicam-se ao provedor de conteúdo e de serviços multimídia que hospeda a divulgação da propaganda eleitoral de candidato, de partido ou de coligação as penalidades previstas nesta Lei, se, no prazo determinado pela Justiça Eleitoral, contado a partir da notificação de decisão sobre a existência de propaganda irregular, não tomar providências para a cessação dessa divulgação. Parágrafo único - O provedor de conteúdo ou de serviços multimídia só será considerado responsável pela divulgação da propaganda se a publicação do material for comprovadamente de seu prévio conhecimento." Sobre o assunto, cf. Diego de Lima Gualda, "Responsabilidade civil dos provedores de internet por atos de terceiros. Reflexos da reforma eleitoral promovida pela Lei nº 12.034/09, disponível em <http://jus.uol.com.br/revista/texto/14008/responsabilidade-civil-dos-provedores-de-internet-por-atos-deterceiros>.

A Organização das Nações Unidas, em relatório divulgado em 24 de maio de 2011, expressamente destaca a necessidade de defender a liberdade de expressão online e recomenda uma cuidadosa ponderação dos direitos fundamentais em jogo quando se trata de remoção de conteúdo: *"(...) enquanto o sistema de notificação e retirada é uma forma de prevenir intermediários de se envolver ou encorajar ativamente comportamentos ilegais em seus serviços, esse sistema está sujeito a abuso tanto do Estado quanto de atores privados. Usuários que são notificados pelo provedor de serviços de que seu conteúdo foi assinalado como ilegal frequentemente possuem poucos recursos para desafiar o pedido de retirada. Além disso, levando-se em consideração que intermediários podem ainda ser considerados financeira e criminalmente responsáveis caso não removam o conteúdo após serem notificados, os intermediários estão inclinados a errar para não serem responsabilizados, censurando em excesso conteúdos potencialmente ilegais. Ausência de transparência no processo de tomada de decisão dos intermediários também esconde frequentemente práticas discriminatórias ou de pressão política que poderiam afetar as decisões dessas empresas. Adicionalmente, intermediários, como entidades privadas, não são os melhores posicionados para determinar que tipo de conteúdo* é *ilegal, pois requer um balanceamento cuidadoso dos interesses em jogo e consideração das defesas. O Relatório Especial acredita que medidas de censura nunca devem ser delegadas a uma entidade privada, e que ninguém deve ser responsabilizado por conteúdo na Internet que não é de sua autoria. Na verdade, nenhum Estado deve forçar ou usar intermediários para realizar censura em seu nome (...)".*

É importante ponderar que mecanismos voluntários de remoção de determinados conteúdos não excluem as salvaguardas de isenção de responsabilidade. Isso porque a retirada voluntária de conteúdo de usuários igualmente não gera responsabilidade às plataformas e aos serviços online, que podem estabelecer em seus termos de serviços políticas de edição, moderação e remoção voluntária de conteúdo. Isso permite a criação de soluções voluntárias eficazes, flexíveis e adaptadas à constante evolução tecnológica, substituindo uma regulação rígida incapaz de lidar com as nuances das novas tecnologias.

Outro ponto importante é a necessidade de que a ordem judicial de remoção contenha identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material (parágrafo 1º do art. 19). Isso se dá para evitar ordens genéricas de remoção (tais como *"remova todos os vídeos em que determinada pessoa aparece"*), sendo sempre necessário a indicação das URLs (uniform resource locators) que devem ser removidas. Com isso, o risco de remoção de conteúdo legítimo é minimizado, privilegiando-se a liberdade de expressão.

Por fim, vale destacar que a Lei 12.965/2014 admite exceções específicas para remoção forçada de conteúdo sem ordem judicial, tais como aquelas já existentes em nosso ordenamento jurídico (casos pornografia infantil, previstos no artigo 241 do Estatuto da Criança e do Adolescente) e cenas de nudez ou sexo de caráter privado, divulgadas sem autorização do participante (artigo 21 do Marco Civil da Internet).

Pós-Marco Civil, há quem alerte para o perigo de afogamento do judiciário para decidir sobre a remoção forçada de conteúdo, risco que não nos parece real. No cotidiano forense, muitas ações frívolas que teriam por objetivo remover conteúdo online deixam de ser propostas (ou são julgadas improcedentes) justamente em razão da seriedade de nosso Judiciário que, por mais que cometa seus erros ocasionais, tem se recusado a determinar a remoção de informações online sem a presença de elementos sérios que justifiquem esse cerceamento da liberdade de manifestação do pensamento.

Pensamos que só se tem a ganhar com um modelo que assegure a todos os envolvidos um mínimo de segurança jurídica. Vítimas querem poder remover rapidamente conteúdo ilegal da rede e responsabilizar os verdadeiros culpados pela veiculação; usuários querem exercer sua liberdade de manifestação de pensamento e manter seu conteúdo online sem correr o risco de sua remoção automática ou arbitrária, e provedores querem exercer suas atividades dentro dos limites de seus contratos de prestação de serviços, sem usurpar o papel do Estado-Juiz na solução desses conflitos e de eventuais colisões de direitos fundamentais. Apenas a análise judicial desses problemas traz a segurança jurídica necessária para sopesar todos os interesses e direitos em jogo, o que evidencia o acerto da redação do artigo 19 do Marco Civil da Internet como regra geral para definir responsabilidades e remoção de conteúdo online.

5. Privacidade comercial pré e pós Marco Civil da Internet

O Brasil ainda não tem normas específicas de proteção de dados pessoais. Nosso sistema jurídico tutela a privacidade de modo genérico, o que não é adequado para tratar das diversas hipóteses de tratamento de dados pessoais por empresas e governos.

Nesse cenário de incerteza jurídica, todos perdem. Indivíduos não têm controle sobre o que acontece com seus dados. Empresas sérias descartam modelos de negócio inovadores, temendo ser confundidas com vigaristas que não respeitam consumidores. Autoridades públicas inescrupulosas aproveitam-se da lacuna legislativa para montar dossiês invasivos. O vácuo legislativo praticamente inviabiliza negócios envolvendo fluxo de dados entre o Brasil e os países que impõem padrões mínimos para a proteção de dados pessoais.

Pré-Marco Civil da Internet, o tratamento de dados pessoais online para fins comerciais não dispunha nem mesmo de parâmetros gerais. O tema era tratado por meio de equiparação e analogia, com aplicação das normas genéricas mencionadas pela Constituição Federal (art. 5º, incisos X, XII) e Código de Defesa do Consumidor (art. 43). Entre as diversas incertezas sobre o tema, destacavam-se:

i) qual seria o conceito de dados pessoais?

ii) quais dados poderiam ser coletados, pessoais ou não?

iii) como os dados poderiam ser coletados? Mediante consentimento tácito? Somente mediante consentimento expresso do usuário?

iv) como demonstrar o consentimento do usuário?

v) de que formas os dados coletados poderiam ser utilizados?

vi) os dados poderiam ser repassados a terceiros? Se sim, em que circunstâncias? Se não, haveria exceções legítimas?

O Marco Civil da Internet apresenta algumas respostas, ainda que tímidas, a essas indagações. O artigo 7º da Lei 12.965/2014 menciona o seguinte em relação ao tema:

> *Art. 7º* O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> *(...)*
>
> *VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante*

consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

XI – publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet; (...)"

Como se observa, o texto da lei proíbe como regra geral o fornecimento a terceiros de dados pessoais do usuário, bem como de seus registros de conexão e de acesso a aplicações de Internet, salvo quando houver consentimento livre, expresso e informado por parte do usuário ou em outras hipóteses a serem definidas por lei.

Ocorre, porém, que o Marco Civil da Internet em momento algum definiu o conceito de "dados pessoais". A intenção do legislador é que essa lacuna conceitual seja preenchida pela futura lei brasileira de proteção de dados pessoais, cujo anteprojeto ainda não foi apresentado ao Congresso Nacional.

A ausência de definição legal para "dados pessoais" faz com que, neste ponto específico, o Marco Civil da Internet não apresente a necessária segurança jurídica às plataformas digitais, redes sociais e demais empresas com presença online. Utilizar conceitos emprestados da doutrina e da jurisprudência somente agrava esse problema – notadamente quando se recorda o quão vagos e amplos são esses conceitos.

Na Europa, a Diretiva 95/46/CE, por exemplo, define dados pessoais como *"qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social"*[8]. É simples observar que praticamente qualquer informação poderia ser considerada "dado pessoal" se utilizada essa definição.

Sem um conceito claro para "dados pessoais" definido em lei, não é possível ter certeza de quais dados podem ser tratados e utilizados livremente, quais situações exigem ao menos consentimento tácito, nem quais dados exigiriam consentimento livre, expresso e informado para seu tratamento e utilização comercial.

Essa lacuna legal é um grave problema pois, como se sabe, é a publicidade dirigida, possibilitada pelo tratamento de dados de usuários – pessoais ou não – que sustenta o ecossistema de serviços e de informações gratuitas online. Outros modelos de negócio – assinaturas, micropagamentos, sites fechados – não fizeram o mesmo sucesso perante a esmagadora maioria dos usuários, acostumados com "tudo grátis" online. Entre pagar uma pequena quantia por acesso, por dia ou por mês ou ceder dados pessoais, quase todos preferem pagar com seus dados.

Pagar com dados é uma escolha válida e precisa ser respeitada. É um modelo que permite a todos os usuários participar do ecossistema online, e não apenas a quem dispõe de recursos para pagar por conteúdo e serviços. Dificultar o tratamento de dados para fins comerciais pode inviabilizar práticas lícitas consagradas no mercado brasileiro e emperrar a economia digital.

Evidentemente, isso não significa que usuários não devam ter controle algum sobre seus dados pessoais – consumidores devem ser adequadamente informados de quais concessões fazem e que trocas aceitam quando optam por usar serviços e acessar conteúdo gratuito online, bem como devem ter acesso a ferramentas que viabilizem esse tipo de controle nas plataformas digitais e redes sociais de que fazem parte.

Para que isso ocorra, é preciso informar adequadamente o usuário, por meio de termos de uso e de políticas de privacidade, documentos que têm força

8 Cf. Diretiva 95/46/CE, art. 2º, letra "a".

vinculante e que foram consagrados pelo Marco Civil da Internet (inciso VIII, letra "c" do artigo 7º).

Esses documentos devem ser claros, curtos, objetivos e diretos, sempre veiculados publicamente, especificando quais são as práticas adotadas pela empresa em relação à coleta, uso, armazenamento, tratamento e proteção dos dados pessoais dos usuários, bem como para quais finalidades esses dados serão utilizados, as quais devem ser justificadas e permitidas pela legislação (inciso VIII, letras "a" e b" do artigo 7º).

É igualmente importante destacar separadamente as cláusulas dos termos de uso, políticas de privacidade e demais contratos celebrados com o usuário que tratem de seu consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, de forma a demonstrar que esse consentimento foi obtido nos termos da lei.

Note-se que práticas comerciais online que não coletam nem tratam dados pessoais não estão sujeitas a essas regras, sendo perfeitamente lícitas quando utilizadas para finalidades legítimas, tais como remarketing, mídia programática e similares. Isso porque essas práticas de publicidade normalmente utilizam o histórico de navegação dos usuários para tentar identificar preferências e formar perfis de consumo e, na ausência de definição legal específica, essas informações ainda não podem ser classificadas como "dados pessoais" no direito brasileiro.

Observe-se, também, que as empresas devem estar preparadas para eliminar os dados pessoais de determinado usuário ao término da relação existente com ele, mediante solicitação do usuário, ressalvado o dever legal de guarda desses dados para fins de investigação de atos ilícitos.

Por fim, tendo em vista que o Marco Civil da Internet não definiu o que seriam "dados pessoais", é recomendável que as plataformas digitais, redes sociais e demais empresas que coletam e tratam dados de usuários em razão de atividades online definam em seus próprios termos de uso e políticas de privacidade o que consideram "dados pessoais" e o que consideram como "dados não pessoais", preferencialmente por meio de exemplos práticos que elucidem e informem o usuário. Com isso, minimizam-se os riscos jurídicos em relação à proteção da privacidade desses usuários, ao menos até a existência de uma definição clara, prevista em lei, para o conceito de "dados pessoais".

13

O Impacto do Marco Civil da Internet nas Atividades de *E-Commerce*

Flávio Franco

Diretor Executivo Jurídico da Netshoes, Vice-Presidente da Comissão de Apoio a Departamentos Jurídicos da OAB/SP e Professor Convidado da Fundação Getúlio Vargas (Direito/GV)