

DEZ ANOS DO MARCO CIVIL DA INTERNET: A NULIDADE DO ARTIGO 8º, A CRISE DO CONSENTIMENTO E OS LIMITES DA TUTELA REATIVA NAS RELAÇÕES PRIVADAS DIGITAIS

Heloisa Helena de Almeida Portugal

Universidade Federal do Mato Grosso do Sul (UFMS),
Mato Grosso do Sul.
heloisaportugal@ufms.br

Jefferson Patrik Germinari

Universidade Federal de Santa Catarina (UFSC), Santa
Catarina.
jeffersonpgerminari@gmail.com

Valter Moura do Carmo

Escola da Magistratura Tocantinense (ESMAT),
Tocantins.
vmcarmo86@gmail.com

RESUMO: Decorridos dez anos de vigência do Marco Civil da Internet, os debates em torno da lei têm conferido maior atenção à neutralidade de rede e à liberdade de expressão do que aos seus efeitos sobre as relações privadas digitais. Nesse campo, a limitação da autonomia privada já encontrava fundamento normativo desde 2014, inclusive pela via da nulidade de pleno direito prevista no artigo 8º. O objetivo do presente artigo é avaliar em que medida o regime dos artigos 7º, inciso IX, e 8º do Marco Civil da Internet limitou eficazmente a autonomia da vontade nas relações privadas digitais, identificando os fatores que condicionaram a sua efetividade. Adota-se pesquisa qualitativa, de natureza teórico-dogmática, mediante revisão bibliográfica e análise documental comparada de dois casos selecionados por seu caráter contrastante, sob o marco teórico do diálogo das fontes. Como resultado, verifica-se que a nulidade prevista no artigo 8º não foi aplicada ao caso Cambridge Analytica, cuja sanção nacional se fundamentou no Código de Defesa do Consumidor. Na Ação Direta de Inconstitucionalidade 6.387, ao contrário, a proteção operou antes do dano. Sustenta-se, assim, que a diferença entre os resultados decorre menos da densidade normativa disponível do que da existência de legitimado institucional apto a acionar a tutela. Propõe-se, ao final, matriz de graduação de risco algorítmico vinculada a consequências jurídico-privadas, a partir do modelo firmado pelo Superior Tribunal de Justiça no Tema 710 e do critério previsto no artigo 3º, inciso VI, do Marco Civil da Internet.

PALAVRAS-CHAVE: Marco Civil da Internet. Autonomia da vontade. Consentimento. Responsabilidade civil. Risco algorítmico.

Ten years of the Brazilian Internet Civil Rights Framework: the nullity of article 8, the crisis of consent, and the limits of reactive protection in private digital relations

ABSTRACT: Ten years after the Brazilian Internet Civil Rights Framework came into force, debates surrounding the statute have devoted greater attention to net neutrality and freedom of expression than to its effects on private digital relations. In this field, limitations on private autonomy had already been established in 2014, including through the nullity as a matter of

law provided for in Article 8. This article aims to assess the extent to which the framework established by Article 7, item IX, and Article 8 effectively limited party autonomy in private digital relations, while identifying the factors that shaped its effectiveness. The study adopts a qualitative, theoretical-dogmatic approach, based on a literature review and a comparative documentary analysis of two cases selected for their contrasting features, under the theoretical framework of the dialogue of sources. The findings indicate that the nullity provided for in Article 8 was not applied in the Cambridge Analytica case, as the Brazilian sanction was instead grounded on the Consumer Protection Code. By contrast, in Direct Action of Unconstitutionality No. 6,387, legal protection operated before the occurrence of harm. It is therefore argued that the difference between these outcomes derives less from the available normative density than from the existence of an institutional claimant capable of invoking legal protection. Finally, the article proposes an algorithmic risk-graduation matrix linked to specific private-law consequences, drawing on the model established by the Brazilian Superior Court of Justice in Theme No. 710 and the criterion set forth in Article 3, item VI, of the Brazilian Internet Civil Rights Framework.

KEYWORDS: Brazilian Internet Civil Rights Framework. Party Autonomy. Consent. Civil liability. Algorithmic risk.

INTRODUÇÃO

Leis fazem aniversário como pessoas, com discursos que dizem mais sobre quem fala do que sobre quem é celebrado. O Marco Civil da Internet completou dez anos em abril de 2024 e foi festejado, com justiça, pela neutralidade de rede, pela proteção da liberdade de expressão e por ter antecipado, em vários pontos, o debate internacional sobre governança digital. Este artigo propõe olhar para outro lugar — menos visitado, e provavelmente mais desconfortável.

Há no Marco Civil um núcleo de direito privado que a década praticamente não discutiu, qual seja, o art. 7º, IX, o qual exige que o consentimento sobre tratamento de dados pessoais seja manifestado de forma destacada das demais cláusulas contratuais. Por sua vez, o art. 8º, parágrafo único, comina nulidade de pleno direito às cláusulas que ofendam a inviolabilidade e o sigilo das comunicações privadas. Outrossim, o art. 3º, VI, elege a responsabilização dos agentes de acordo com suas atividades. São três dispositivos que, lidos em conjunto, revelam uma afirmação de considerável ousadia dogmática, isto é, no ambiente digital, a autonomia privada encontra limites que não podem ser afastados pela simples manifestação de vontade do usuário.

Não se afirma, com isso, que o art. 8º estabeleça, isoladamente, um regime geral de nulidade aplicável ao tratamento de dados pessoais. A conclusão decorre da leitura sistemática desses dispositivos e da sua articulação com as demais normas de direito privado incidentes sobre essas relações. O legislador brasileiro já estabelecia, em 2014, limites à suficiência do consentimento, chegando, nas hipóteses alcançadas pelo art. 8º, à via mais severa de que o direito civil dispõe: a nulidade de pleno direito. A doutrina viria a desenvolver, nos anos seguintes, discussão semelhante sob o rótulo da crise do consentimento, sem que a dimensão privatista do Marco Civil recebesse atenção equivalente.

Daí o problema que orienta a investigação: decorridos dez anos, em que medida o regime dos arts. 7º, IX, e 8º do Marco Civil foi capaz de limitar eficazmente a autonomia da vontade nas relações privadas digitais, e quais fatores condicionaram a sua efetividade ou a sua ausência?

A hipótese aqui sustentada é que a insuficiência verificada na década não foi normativa, e sim institucional. A norma existia, era clara, era aplicável e cominava a sanção mais grave do direito privado. O que faltou foi quem a invocasse. O Marco Civil criou direitos materiais e entregou a sua tutela a um gatilho processual — a iniciativa individual, o dano provado, a ordem judicial —, num arranjo em que a violação difusa de milhares de titulares dificilmente encontra autor. Uma nulidade absoluta que ninguém alega é, na prática de mercado, uma nulidade que não existe.

A hipótese é submetida a dois episódios que funcionam como testes de estresse do regime. O primeiro é o escândalo Cambridge Analytica, ocorrido em 2018 com o Marco Civil em vigor havia quatro anos, e cujos números brasileiros, apurados em processo administrativo, são por si sós uma demonstração: oitenta e quatro pessoas instalaram no país o aplicativo que serviu de porta de entrada, e quatrocentas e quarenta e três mil tiveram dados expostos. O segundo é o conjunto de ações diretas de inconstitucionalidade contra a Medida Provisória nº 954/2020, encabeçado pela ADI 6.387, em que o Supremo Tribunal Federal suspendeu, antes de qualquer dano consumado, o compartilhamento compulsório de dados de assinantes de telefonia com órgão estatal. Dois episódios, a mesma espécie de bem jurídico, resultados opostos — e a variável que os separa não é a densidade da norma disponível.

O artigo oferece ainda uma contribuição propositiva, e convém dizer desde logo o que ela não é. Não é a invenção de um modelo de graduação de obrigações por faixas de risco, técnica consolidada na tradição regulatória europeia desde 2021. É a demonstração de que o direito privado brasileiro dispõe dos materiais para operar essa graduação — o art. 927, parágrafo único, do Código Civil, o relatório de impacto do art. 38 da Lei nº 13.709/2018 e, sobretudo, o precedente firmado pelo Superior Tribunal de Justiça no Tema 710, que dispensou o consentimento no credit scoring e o substituiu por deveres de transparência e responsabilidade objetiva e solidária. A proposta consiste em generalizar esse modelo e articulá-lo a consequências jurídico-privadas determinadas, dando ao art. 3º, VI, do Marco Civil o critério de aplicação que ele nunca teve.

A relevância do exercício não é apenas retrospectiva. Ao completar dez anos, o Marco Civil tinha o núcleo do seu regime de responsabilidade civil pendente de definição no Supremo Tribunal Federal e via a sua matéria ser objeto de proposta de absorção pelo Código Civil, no anteprojeto entregue ao Senado no mesmo mês do aniversário. O balanço da década, portanto, não descreve um sistema consolidado, descreve um sistema em transição — e é justamente em transições que as escolhas dogmáticas ainda podem ser feitas.

O texto organiza-se em oito seções. Após esta introdução, a segunda expõe o desenho metodológico e o marco teórico do diálogo das fontes. A terceira caracteriza o ambiente socio-técnico que o Marco Civil se propôs a disciplinar. A quarta reconstrói a lei como estatuto de direito privado, a partir dos arts. 3º, 7º, 8º, 11 e 18 a 21. A quinta submete a hipótese aos dois casos selecionados. A sexta examina a revisão a que o art. 19 vinha sendo submetido e o horizonte de sucessão aberto pela reforma do Código Civil. A sétima apresenta a matriz de risco algorítmico e as suas consequências no plano das relações privadas. A oitava sintetiza os resultados e delimita as questões que permanecem abertas.

1 DESENHO METODOLÓGICO

A investigação é qualitativa e de natureza teórico-dogmática. Vale dizer com clareza o que isso significa e, sobretudo, o que não significa. Não houve coleta de dados primários, não se aplicaram instrumentos de pesquisa empírica e não se pretende generalização estatística. O

que se realizou foi revisão bibliográfica interdisciplinar combinada com análise documental comparada de fontes normativas, decisórias e administrativas.

O *corpus* documental compreende quatro conjuntos. O primeiro é normativo: a Lei nº 12.965/2014 e o Decreto nº 8.771/2016; a Lei nº 13.709/2018; o Código de Defesa do Consumidor; o Código Civil; a Lei nº 12.414/2011; e a Emenda Constitucional nº 115/2022. O segundo é decisório: o Recurso Especial nº 1.419.697/RS, do Superior Tribunal de Justiça, e a medida cautelar referendada na ADI 6.387 e ações conexas, no Supremo Tribunal Federal. O terceiro é administrativo: a decisão do Departamento de Proteção e Defesa do Consumidor da Secretaria Nacional do Consumidor relativa ao caso *Cambridge Analytica*, além dos atos da *Federal Trade Commission* e do *Information Commissioner's Office* referentes ao mesmo episódio. O quarto é regulatório comparado, restrito ao desenho de graduação por faixas de risco proposto pela Comissão Europeia em 2021.

O marco teórico é a teoria do diálogo das fontes, formulada por Erik Jayme e desenvolvida no Brasil por Cláudia Lima Marques. O problema examinado situa-se na interseção de quatro diplomas que disciplinam, sob perspectivas distintas, a mesma relação jurídica — e a pretensão de resolvê-lo por critérios clássicos de antinomia conduziria a resultados empobrecedores, quando não absurdos. O próprio Marco Civil autoriza expressamente a articulação sistemática, ao declarar, no parágrafo único do art. 3º, que os princípios ali enunciados não excluem outros previstos no ordenamento, e ao determinar, no art. 7º, XIII, a aplicação das normas de proteção e defesa do consumidor às relações de consumo realizadas na internet.

A seleção dos dois casos analisados obedeceu a critério teórico de contraste. Ambos ocorreram sob a vigência do Marco Civil, condição sem a qual o exercício perderia sentido; ambos envolveram tratamento de dados pessoais de contingente expressivo de titulares brasileiros sem manifestação de vontade idônea; e ambos dispunham de norma proibitiva vigente e aplicável. Diferem, contudo, em todas as variáveis relevantes — a origem da violação, privada num caso e estatal no outro; o momento da tutela; a fonte normativa efetivamente acionada; e a existência ou inexistência de legitimado institucional. É precisamente essa combinação de semelhança no objeto e oposição nas condições que confere ao par a qualidade de teste, e não de mera ilustração. Os eixos de comparação estão sistematizados no Quadro 1, na seção 5.

Reconhecem-se três limitações. A análise de dois casos não autoriza inferência causal nem generalização estatística, e as conclusões aqui alcançadas têm alcance interpretativo, não preditivo. As informações relativas ao processo administrativo brasileiro provêm da decisão e das comunicações oficiais correspondentes, sem acesso aos autos integrais. E a matriz proposta na seção 7 é parâmetro dogmático de graduação, submetido às ressalvas ali declaradas, e não norma acabada nem instrumento validado empiricamente.

2 O AMBIENTE QUE O MARCO CIVIL BUSCOU DISCIPLINAR

Nenhuma lei se explica fora do mundo que pretendeu ordenar. Antes de examinar o que o Marco Civil fez com a vontade, convém reconstituir o ambiente em que essa vontade é manifestada — e que, década adentro, tornou-se menos hospitaleiro do que era em 2014. Três dimensões interessam aqui, e elas não operam em separado: a dataficação como fenômeno econômico, a governança algorítmica como exercício de poder normativo privado e a desigualdade digital como fator que converte a proteção contratual em ficção.

A transição da sociedade industrial para a sociedade informacional não se resume à adoção tecnológica em larga escala. Reflete alteração estrutural na qual a geração, o processa-

mento e a transmissão de dados convertem-se em fontes primárias de produtividade e poder (Castells, 2017, p. 64-65). O que distingue esse arranjo do anterior não é a presença de máquinas, e sim o deslocamento do eixo de valor, ou seja, quem detém o maquinário industrial cede posição a quem controla fluxos de extração de dados e ferramentas de predição comportamental.

Convém distinguir, nesse percurso, a digitalização da dataficação. A primeira é conversão de suportes; noutros dizeres, o documento em papel que se torna arquivo, a fotografia que se torna pixel. A segunda é outra coisa, e é a que importa. A dataficação consiste na conversão de ações, relações e ambientes cotidianos em registros passíveis de mensuração, correlação e inferência (Bruno, 2013, p. 123-124). Assim, os rastros digitais deixam de ser subprodutos passivos da interação e passam a ser matéria-prima de um imperativo econômico próprio. Zuboff (2019) descreve o mecanismo com precisão: parcela dos dados coletados retorna ao usuário sob a forma de serviço aprimorado, mas o excedente comportamental é desviado para processos de inteligência de máquina que fabricam produtos preditivos, vendidos em mercados dos quais o titular dos dados não participa e cuja existência com frequência ignora. Não há aqui metáfora nem denúncia, mas uma descrição de modelo de negócio.

Nesse ecossistema, as plataformas assumem posição de infraestrutura, e a posição de infraestrutura confere poder normativo. Longe de figurarem como espaços neutros, elas estruturam escolhas e condicionam condutas pela própria arquitetura técnica — senhas, permissões, limites de caracteres, configurações padrão, algoritmos de ordenação e recomendação exercem função regulatória análoga à das normas estatais, na formulação já clássica de Lessig (2006, p. 121-124) sobre o código como lei. A diferença decisiva é que a norma estatal é pública, discutível e impugnável, ao passo que a norma embutida no código não é nenhuma das três. É aqui que a opacidade deixa de ser inconveniência técnica e passa a ser problema jurídico.

Pasquale (2015, p. 3-7) diagnosticou o cenário como sociedade da caixa-preta. O cidadão é rastreado, classificado e pontuado — para concessão de crédito, triagem de currículos, precificação de seguros, policiamento preditivo — sem acesso à lógica que produz a classificação. Nesse sentido, segredo industrial, complexidade técnica e ofuscação corporativa sobrepoem-se em camadas que tornam a decisão inaudível por quem a sofre. E uma decisão inaudível desafia frontalmente categorias jurídicas assentadas na transparência, no contraditório e no devido processo. Quando a arquitetura decisória é uma caixa-preta, aquilo que tem natureza normativa é subtraído da esfera pública sem nunca ter sido submetido a ela.

Estudo realizado por Verbicaro e Nóvoa demonstra a vulnerabilidade algorítmica como aprofundamento da assimetria informacional. Mecanismos apresentados como instrumentos de participação e escolha podem servir, simultaneamente, à extração de dados, à predição de comportamentos e à manipulação das decisões do usuário. A aparência de empoderamento, portanto, não elimina a posição estruturalmente passiva do consumidor diante da opacidade das plataformas (Verbicaro; Nóvoa, 2023, p. 127-129).

O quadro adquire contornos particulares quando projetado sobre a realidade brasileira, e é nesse ponto que os números merecem exame cuidadoso — inclusive porque, lidos apressadamente, sugerem o oposto do que revelam. Segundo a pesquisa TIC Domicílios 2023, oitenta e quatro por cento dos domicílios brasileiros dispunham de acesso à internet, aproximadamente sessenta e quatro milhões de residências, e a mesma proporção da população com dez anos ou mais utilizara a rede nos três meses anteriores, cerca de cento e cinquenta e seis milhões de pessoas (COMITÊ GESTOR DA INTERNET NO BRASIL, 2024b, p. 64). Se o exame parasse aí, o diagnóstico seria de inclusão consolidada.

Ele não para aí. Doze milhões de domicílios permaneciam desconectados. A conexão alcançava oitenta e seis por cento dos domicílios urbanos e setenta e quatro por cento dos rurais, diferença de doze pontos percentuais que a expansão do acesso não reduziu. Entre as classes sociais, o contraste é mais agudo: noventa e oito por cento na classe *A* contra sessenta e sete por cento nas classes *D* e *E*. E, sobretudo, cinquenta e oito por cento dos usuários acessavam a rede exclusivamente pelo telefone celular, proporção que subia para oitenta e sete por cento nas classes *D* e *E* (COMITÊ GESTOR DA INTERNET NO BRASIL, 2024b, p. 64-71).

O indicador decisivo, contudo, é o de conectividade significativa, que pondera custo, dispositivos disponíveis, qualidade da conexão e ambiente de uso. Por esse critério, cinquenta e sete por cento da população brasileira situava-se nas duas faixas mais baixas, e apenas vinte e dois por cento reunia condições satisfatórias de acesso. Confronte-se esse número com o anterior: oitenta e quatro por cento conectados, vinte e dois por cento conectados de modo significativo. A distância entre as duas cifras é precisamente a distância entre o sujeito de direito que o contrato pressupõe e o sujeito real que o celebra (COMITÊ GESTOR DA INTERNET NO BRASIL, 2024a, p. 103).

As consequências dogmáticas são diretas, e vale enunciá-las sem eufemismo. Um usuário cujo único meio de acesso é um aparelho celular de tela reduzida, operando sob franquia de dados limitada, não está em condições materiais de examinar um instrumento contratual de dezenas de páginas antes de aceitá-lo — e a exigência legal de que o consentimento seja manifestado de forma destacada das demais cláusulas, por mais bem-intencionada, pressupõe uma superfície de leitura que essa pessoa não tem. Some-se a isso que o serviço em questão é, frequentemente, condição de acesso a benefícios sociais, oportunidades de trabalho e comunicação familiar, e a recusa de contratar deixa de ser alternativa disponível. Como sustenta Bioni (2021), a autonomia da vontade não pode operar como vetor único de legitimação do tratamento de dados em cenário de assimetria dessa ordem. O que se tem não é autodeterminação informativa, mas sim uma adesão informacional.

A dificuldade não se resolve pela simples atribuição formal de controle ao titular. A circulação intensa e sucessiva de informações entre empresas cria uma desproporção prática em que o ônus de vigiar cada operação pode tornar o exercício da privacidade excessivamente gravoso. A proteção exige, por isso, limites que permitam ao indivíduo controlar seus dados sem transferir-lhe integralmente os custos e a complexidade do sistema de tratamento (Magaalhães; Oliveira, 2021, p. 67-68).

Convém, porém, resistir à conclusão fácil. A descrição acima costuma ser apresentada como diagnóstico à espera de resposta legislativa — como se o direito brasileiro ainda devesse decidir se protege o titular independentemente da sua anuência. Essa decisão foi tomada em 2014, no mesmo diploma cujo aniversário se celebra, e por meio dos instrumentos mais severos de que o direito privado dispõe. A seção seguinte demonstra que o Marco Civil não apenas antecipou o cenário aqui descrito: extraiu dele consequências que a década seguinte não soube reconhecer.

3 O MARCO CIVIL DA INTERNET COMO ESTATUTO DE DIREITO PRIVADO

O Marco Civil da Internet foi batizado, ainda no berço, de Constituição da internet brasileira. A metáfora era generosa e cobrou um preço. Ao elevar a Lei nº 12.965/2014 à dignidade constitucional, o apelido empurrou-a para o direito público e a subtraiu do lugar onde ela também opera, com menos alarde e muito mais consequência: o direito das obrigações. Uma

década depois, o balanço da lei continua a ser feito na chave da neutralidade de rede, da liberdade de expressão e da remoção de conteúdo. Fala-se pouco do que o Marco Civil fez com a vontade. E o que ele fez com a vontade foi, do ponto de vista dogmático, o gesto mais radical já praticado pela legislação brasileira no ambiente digital.

Convém, pois, ler a lei como quem lê um código: não pelos princípios que proclama, mas pelos efeitos que produz sobre o negócio jurídico. O exercício exige um deslocamento de olhar. Enquanto se lê o Marco Civil como carta de princípios, ele parece documento programático, generoso em enunciados e discreto em consequências. Lido como estatuto de relações privadas, revela-se outra coisa, qual seja, uma sequência de restrições à liberdade contratual, dispostas em ordem crescente de severidade, que culmina numa sanção de invalidade. O percurso começa no art. 7º, que abre com uma afirmação habitualmente tratada como retórica — o acesso à internet é essencial ao exercício da cidadania. Não é retórica, mas a premissa que justifica tudo o que vem depois, porque, se o acesso é essencial, a recusa de contratar deixa de ser opção real do usuário, e a autonomia da vontade, que pressupõe a possibilidade de dizer não, começa a ranger.

O catálogo que se segue é um catálogo de desconfiança. O inciso VII proíbe o fornecimento de dados pessoais a terceiros salvo mediante consentimento livre, expresso e informado. Acrescenta-se o inciso VIII ao exigir informações claras e completas sobre coleta, uso, armazenamento e tratamento, e amarra os dados a finalidades que justifiquem a coleta, não sejam vedadas em lei e estejam especificadas no contrato ou nos termos de uso. Por sua vez, o inciso X assegura a exclusão definitiva dos dados ao término da relação. São, todos eles, deveres impostos ao fornecedor contra a lógica econômica do serviço gratuito, deveres que o mercado não produziria espontaneamente e que o contrato, sozinho, jamais teria gerado.

Frisa-se o inciso IX como mais revelador, e é o menos citado. Ele exige consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, "que deverá ocorrer de forma destacada das demais cláusulas contratuais" (Brasil, 2014). Repare-se no que o legislador está dizendo, e no que está calando. Ele está exigindo tipografia, determinando que a manifestação de vontade apareça graficamente separada do restante do instrumento — e uma exigência de tipografia é o modo pelo qual o direito costuma admitir, sem nunca dizer em voz alta, que a leitura não acontece.

A genealogia do dispositivo não deixa dúvida, pois o art. 54, § 4º, do Código de Defesa do Consumidor já determinava que as cláusulas limitativas de direito nos contratos de adesão fossem redigidas com destaque, permitindo compreensão imediata e fácil. O art. 7º, IX, do Marco Civil é a transposição dessa técnica para o ambiente digital: mesma patologia, mesmo remédio, trinta e quatro anos depois. O que o Código de Defesa do Consumidor diagnosticou no contrato de massa impresso — a vontade que se dissolve na letra miúda —, o Marco Civil reconheceu no contrato de massa eletrônico (Marques, 2019; Miragem, 2020). Daí uma conclusão que o debate dos dez anos não extraiu: o Marco Civil não presumiu um usuário autônomo, presumiu um aderente. E legislou para ele.

Mas desconfiar é pouco. Um catálogo de deveres informacionais, por mais denso que seja, ainda opera dentro da gramática do contrato: obriga o fornecedor a informar melhor, a destacar, a especificar finalidades — e, no limite, deixa intacta a premissa de que a vontade assim informada vincula. O dispositivo seguinte rompe com essa premissa. Se o art. 7º desconfia da vontade, o art. 8º a fulmina. O caput estabelece que a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet, e o parágrafo único extrai daí a consequência, ao dispor que "São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput" (Brasil, 2014), exempli-

ficando com as que impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas pela internet e com as que, em contrato de adesão, não ofereçam ao contratante o foro brasileiro como alternativa.

Nulidade de pleno direito. Não anulabilidade, sujeita a prazo decadencial e a iniciativa do interessado. Não abusividade a ser sopesada caso a caso. Nulidade — a sanção mais severa que o direito privado reserva à manifestação de vontade, aquela que opera *ipso iure*, é insuscetível de confirmação, não convalesce pelo decurso do tempo e pode ser conhecida de ofício pelo juiz, nos termos do regime geral dos arts. 166 e seguintes do Código Civil.

O paralelo com o art. 51 do Código de Defesa do Consumidor, que abre com a mesma fórmula ao arrolar as cláusulas abusivas, é evidente e foi certamente deliberado. Também o é a convergência com o art. 424 do Código Civil, que fulmina, nos contratos de adesão, a renúncia antecipada a direito resultante da natureza do negócio. Três diplomas, três momentos históricos, um só movimento: o direito privado brasileiro retirando do alcance da autonomia privada aquilo que a assimetria estrutural tornou indisponível de fato (Tepedino, 2008; Schreiber, 2013).

É preciso dizer, com todas as letras, o que isso significa em 2014. O legislador brasileiro declarou que, no ambiente digital, há um campo em que a vontade manifestada pelo usuário é juridicamente irrelevante. Não importa que ele tenha clicado. Não importa que tenha rolado a barra até o fim e assinalado a caixa. Se a cláusula ofende o núcleo protegido pelo *caput*, ela não é anulável a pedido: é nula, e sempre foi. A tese que este artigo sustenta encontra aqui o seu apoio normativo mais firme, e o encontra dez anos antes de ser formulada — o que a doutrina viria a construir sob os rótulos da crise do consentimento e da insuficiência da autodeterminação (Doneda, 2019; Bioni, 2021; Mendes, 2014) já estava, em estado de norma, no parágrafo único do art. 8º. O Marco Civil não precisou esperar a Lei Geral de Proteção de Dados para dizer que o consentimento não legitima tudo. Disse em 2014, e disse pela via mais forte de que o direito civil dispõe.

O que devolve à pergunta incômoda, e a que o restante deste estudo procura responder: se a norma existia, e existia nessa intensidade, por que não funcionou? A hipótese mais confortável seria atribuir a falha ao texto — imprecisão redacional, lacuna, insuficiência de alcance. Não é o caso, e a leitura sistemática acaba de demonstrá-lo. A resposta está noutro lugar, e está na própria lei: no modo como ela organizou a tutela daquilo que declarou. O art. 11 estende a legislação brasileira a qualquer operação de coleta, guarda ou tratamento de dados em que ao menos um ato ocorra em território nacional — dispositivo de alcance extraterritorial ambicioso, concebido sob o impacto das revelações de vigilância global que precederam a votação. O Decreto nº 8.771/2016 acrescentou a camada infralegal, detalhando padrões de segurança e procedimentos de guarda de registros. No papel, a arquitetura é sofisticada: princípios no art. 3º, direitos materiais no art. 7º, sanção civil no art. 8º, alcance no art. 11, regulamento no Decreto.

Vale deter-se num desses princípios, porque ele carrega bem mais do que aparenta. O art. 3º, VI, elege a responsabilização dos agentes de acordo com suas atividades, nos termos da lei. Enunciado assim, em uma linha, o inciso passa por obviedade. Ele estabelece que a medida da responsabilidade não decorre da qualidade do sujeito nem da natureza do vínculo, mas do que cada agente efetivamente faz na cadeia — e, por consequência, do risco que a sua atividade introduz. É o mesmo raciocínio que o Código Civil consagrara no parágrafo único do art. 927, ao vincular a responsabilidade objetiva à atividade normalmente desenvolvida pelo autor do dano quando ela implica, por sua própria natureza, risco para os direitos de outrem. Ao transpor essa lógica para o ambiente digital, o Marco Civil anunciou em 2014 aquilo que o debate

regulatório internacional viria a formular sob o rótulo da abordagem baseada em risco: obrigações calibradas pela intensidade com que cada agente intervém sobre bens jurídicos alheios. E o fez sem alarde, num inciso de princípio cuja fecundidade dogmática permanece largamente inexplorada — inclusive porque o parágrafo único do mesmo artigo declara que os princípios ali expressos não excluem outros previstos no ordenamento, cláusula de abertura que autoriza, no próprio texto da lei, a articulação sistemática com o Código de Defesa do Consumidor e com o Código Civil que este estudo pratica.

O problema não está no desenho, mas na pergunta que o desenho não responde: quem aciona esse aparato? Uma arquitetura normativa vale o que valem os seus legitimados, e é precisamente aqui que o Marco Civil hesita. Os arts. 18 a 21 respondem à pergunta, e a resposta é mais reveladora do que o legislador provavelmente pretendia. O provedor de conexão não responde civilmente por conteúdo de terceiro, só responde se descumprir ordem judicial específica de remoção. A exceção do art. 21, para a divulgação não consentida de material de nudez ou de atos sexuais, admite notificação extrajudicial — e é justamente por ser exceção que confirma a regra: o Marco Civil escreveu direitos em linguagem de direito material e entregou a sua tutela a um gatilho processual. O dever nasce da lei; a consequência depende de um juiz. E de um autor que o procure. Há aqui, ademais, uma incoerência interna que merece registro: o art. 3º, VI, prometera graduar a responsabilidade conforme a atividade de cada agente, e os arts. 18 e 19 entregaram, em lugar disso, uma graduação de imunidade — quanto mais estruturante a posição do provedor na cadeia, mais protegido ele saiu do arranjo.

O desenho processual, contudo, ainda não explica tudo. Some-se a ele o dado institucional decisivo — aquele que o balanço da década costuma registrar como cronologia e quase nunca como causa. Entre 2014 e a entrada em vigor da Lei nº 13.709/2018, e mais ainda até a estruturação efetiva da autoridade nacional, os arts. 7º e 8º não tinham a quem ser dirigidos senão ao Judiciário, caso a caso, por iniciativa individual e depois de consumado o dano. A nulidade do art. 8º é absoluta, mas alguém precisa alegá-la. E, num contrato de adesão celebrado por milhões de usuários que jamais leram a cláusula que os fulmina, ninguém alega.

Estudo aponta que a efetividade da proteção de dados depende de infraestrutura institucional preventiva. Entre as medidas indicadas estão regulação com sanções proporcionais, fiscalização efetiva, autoridade dotada de independência e recursos, segurança das plataformas públicas e exigências de transparência sobre coleta e uso de informações. Esse conjunto reforça que a existência do direito material, isoladamente, não garante sua concretização (Fernandes; Machado, 2022, p. 86-87).

É essa a fratura que o presente estudo identifica como decisiva no balanço da década, e que a seção seguinte submete a teste documental. O Marco Civil não falhou por insuficiência normativa, mas sim, criou o dever e terceirizou o guardião — e uma nulidade que ninguém invoca é, na prática de mercado, uma nulidade que não existe.

4 DOIS TESTES DE ESTRESSE: CAMBRIDGE ANALYTICA E A ADI 6.387

Toda tese sobre eficácia normativa precisa, em algum momento, deixar o plano do enunciado e enfrentar o que aconteceu. Esta seção submete a hipótese formulada anteriormente a dois episódios que funcionam como testes de estresse do regime privatista do Marco Civil: um em que a violação partiu de agente privado, outro em que partiu do Estado. Foram selecionados por serem polares e por terem ocorrido sob a vigência da Lei nº 12.965/2014 — condição sem a qual o exercício não teria sentido. O que se busca não é a descrição dos casos, lar-

gamente disponível, mas a resposta a uma pergunta única: em cada um deles, a norma foi acionada, e por quem?

Começa-se pelo mais conhecido, e é preciso começar por um dado que o debate brasileiro sobre o caso raramente destaca. O escândalo Cambridge Analytica não ocorreu num vazio normativo. Ocorreu com o Marco Civil da Internet em pleno vigor havia quatro anos.

A mecânica é simples e vale lembrá-la pelo que ela revela, não pelo que ela tem de espetacular. O aplicativo de teste de personalidade *thisisyourdigitallife*, desenvolvido por Aleksandr Kogan, foi instalado por cerca de duzentos e setenta mil usuários em todo o mundo. Desses duzentos e setenta mil consentimentos resultou a extração de dados de aproximadamente oitenta e sete milhões de pessoas, porque a arquitetura da interface de programação então vigente permitia que a instalação por um usuário liberasse o acesso à sua rede de amigos. No Brasil, o desequilíbrio assume proporções ainda mais eloquentes. Segundo os números apurados no processo administrativo instaurado pela Secretaria Nacional do Consumidor, oitenta e quatro pessoas instalaram o aplicativo em território nacional, e quatrocentos e quarenta e três mil brasileiros tiveram dados expostos. Mais de cinco mil atingidos para cada usuário que efetivamente manifestou alguma vontade.

Há que se deter a esse número, porque ele é a tese deste artigo em forma aritmética. Não se trata de consentimento mal-informado, de leitura apressada dos termos de uso ou de assimetria informacional — categorias que a doutrina já domina e que pressupõem, todas elas, que existiu uma vontade defeituosa. Aqui não houve vontade alguma a defeituar. Quatrocentos e quarenta e dois mil novecentos e dezesseis brasileiros tiveram seus dados extraídos sem terem clicado em coisa nenhuma. O consentimento de um sujeito produziu efeitos jurídicos sobre milhares de terceiros que jamais foram consultados, e o fez por desenho de arquitetura, não por acidente. É a demonstração empírica mais limpa de que o modelo contratual de legitimação do tratamento de dados não descreve o que efetivamente acontece.

Confronte-se agora esse arranjo com o texto da lei brasileira então vigente. O art. 7º, VII, do Marco Civil veda o fornecimento de dados pessoais a terceiros salvo mediante consentimento livre, expresso e informado — e o consentimento de um usuário não é, por evidência, consentimento dos seus amigos. O art. 7º, IX, exige manifestação expressa e destacada das demais cláusulas contratuais, o que a permissão embutida em configuração padrão de plataforma manifestamente não era. O art. 8º, parágrafo único, comina nulidade de pleno direito às cláusulas que ofendam a inviolabilidade e o sigilo das comunicações privadas. E o art. 11 estende a legislação brasileira a qualquer operação de coleta ou tratamento em que ao menos um ato ocorra em território nacional, o que afasta de antemão a objeção de jurisdição. A norma existia, era clara, era aplicável e cominava a sanção mais severa do direito privado.

O que se seguiu, contudo, foi outra coisa. Nos Estados Unidos, a Federal Trade Commission anunciou, em julho de 2019, acordo pelo qual o Facebook se obrigou a pagar penalidade civil de cinco bilhões de dólares em razão do descumprimento da ordem de privacidade expedida pela própria agência em 2012 (FEDERAL TRADE COMMISSION, 2019b, online). A medida não foi imposta à Cambridge Analytica: no procedimento administrativo específico instaurado contra essa empresa, a Federal Trade Commission reconheceu a ocorrência de práticas enganosas na coleta de dados pessoais e expediu ordem final que a proibiu de realizar declarações falsas sobre a proteção da privacidade e a confidencialidade das informações, além de determinar a exclusão de dados obtidos por meio do aplicativo utilizado no episódio (FEDERAL TRADE COMMISSION, 2019a, online). No Reino Unido, o Information Commissioner's Office aplicou ao Facebook multa de quinhentas mil libras, correspondente ao valor máximo permitido pelo Data Protection Act 1998 (INFORMATION COMMISSIO-

NER'S OFFICE, 2018, p. 38). No Brasil, o Departamento de Proteção e Defesa do Consumidor da Secretaria Nacional do Consumidor aplicou, em 30 de dezembro de 2019, multa de seis milhões e seiscentos mil reais ao Facebook, por prática abusiva relacionada ao compartilhamento indevido de dados de usuários e às falhas do modelo de consentimento e das informações prestadas sobre privacidade (BRASIL, 2019, online).

O contraste entre as cifras é retoricamente tentador, mas não é o ponto. O ponto é o fundamento jurídico. A sanção brasileira foi aplicada com base no Código de Defesa do Consumidor, mediante reconhecimento expresso, na decisão administrativa, de que se configurava relação de consumo e de que a plataforma ostentava a posição de fornecedora nos termos do art. 2º do Código, ainda que os serviços não fossem remunerados pelos usuários. O órgão consignou que o modelo de consentimento adotado teve implicações determinantes sobre o número de pessoas expostas. Está tudo correto. E os arts. 7º, VII, 7º, IX, e 8º do Marco Civil — os dispositivos que o caso violou de modo mais direto e mais frontal — não foram o fundamento da sanção.

Eis o achado que este estudo reputa central no balanço da década. Não é que o Marco Civil tenha sido aplicado e se revelado insuficiente. É que ele não foi aplicado. A nulidade do art. 8º, absoluta, imprescritível e cognoscível de ofício, permaneceu inerte diante da hipótese que parecia desenhada para ela, e a proteção que efetivamente ocorreu veio de outro diploma, por outra via e por iniciativa de outro órgão. A explicação não está no direito material, e sim naquilo que a seção anterior identificou, isto é, o Marco Civil criou direitos sem criar quem os invocasse. Em 2018, o Brasil não tinha autoridade de proteção de dados — a Lei nº 13.709 seria sancionada em agosto daquele ano e a autoridade nacional demoraria ainda mais a se estruturar. Quem restava era o consumidor individual, diante de um tribunal, provando dano. Quatrocentos e quarenta e três mil pessoas não litigaram; sequer souberam.

O segundo teste inverte todas as variáveis, e é por isso que ele instrui.

Em abril de 2020, no auge da emergência sanitária, a Medida Provisória nº 954 determinou que as prestadoras de serviços de telecomunicações compartilhassem com o Instituto Brasileiro de Geografia e Estatística a relação de nomes, números de telefone e endereços de seus assinantes, para suporte à produção estatística oficial durante a pandemia. O ato tinha finalidade pública legítima, prazo determinado e destinatário estatal. Ainda assim, foi imediatamente questionado perante o Supremo Tribunal Federal por meio de cinco ações diretas de inconstitucionalidade, ajuizadas por partidos políticos e pelo Conselho Federal da Ordem dos Advogados do Brasil, autuadas sob os números 6.387, 6.388, 6.389, 6.390 e 6.393.

Em 7 de maio de 2020, o Plenário referendou a medida cautelar deferida pela relatora, Ministra Rosa Weber, suspendendo a eficácia da medida provisória. Não houve, registre-se com precisão, julgamento de mérito. A Medida Provisória nº 954 veio a caducar e as ações perderam o objeto. Mas o que se decidiu na cautelar bastou para fixar entendimento de alcance duradouro. A Corte submeteu o ato a exame de proporcionalidade e o reprovou pela indeterminação da finalidade, pela ausência de definição do objeto e pela insuficiência dos mecanismos de proteção — e, sobretudo, reconheceu a autodeterminação informativa como direito autônomo extraível do texto constitucional, dois anos antes de a Emenda Constitucional nº 115/2022 positivá-la expressamente. É o mesmo movimento que o Tribunal Constitucional Federal alemão realizara em 1983, na decisão sobre a Lei do Censo, ao extrair da dignidade e do livre desenvolvimento da personalidade o direito à autodeterminação informacional.

Compare-se, então, o que os dois episódios têm de estruturalmente distinto. Em ambos, dados pessoais de milhões de brasileiros foram objeto de tratamento sem manifestação de vontade idônea. Em ambos, havia norma proibitiva vigente e aplicável. Num deles a proteção ope-

rou antes do dano, suspendendo o ato; no outro, operou quatro anos depois, por outro diploma, e em valor que não altera modelo de negócio algum. A variável que os separa não é a densidade da norma, mas sim a existência de alguém com legitimidade, capacidade técnica e incentivo para acioná-la.

Quadro 1 – Eixos de comparação entre os casos

Eixo	Cambridge Analytica	ADI 6.387
Origem da violação	agente privado transnacional	ato normativo estatal
Momento da intervenção protetiva	<i>ex post</i> , após dano consumado	<i>ex ante</i> , antes da execução
Fonte normativa efetivamente acionada	Código de Defesa do Consumidor	Constituição Federal
Papel atribuído ao consentimento	legitimador presumido do tratamento	irrelevante — proteção independe de vontade
Natureza do remédio	sanção administrativa pecuniária	suspensão da eficácia do ato
Legitimado que acionou a tutela	órgão de defesa do consumidor, por provocação da imprensa	partidos políticos e Conselho Federal da OAB
Existência de canal coletivo próprio	inexistente à época	controle concentrado de constitucionalidade
Eficácia protetiva verificada	nenhuma reversão do dano	integral

Fonte: elaborado pelos autores (2024).

O quadro autoriza uma conclusão que o discurso comemorativo dos dez anos tende a evitar. O ordenamento brasileiro protegeu com eficiência os dados de duzentos milhões de titulares contra o próprio Estado, e não protegeu quatrocentos e quarenta e três mil titulares contra uma plataforma privada — dispondo, nos dois casos, de norma proibitiva expressa. A diferença não está no direito material, mas no acesso ao remédio. Enquanto a violação estatal encontra legitimados institucionais, procedimento célere e foro concentrado, a violação privada, no desenho do Marco Civil, encontra o usuário individual, o dano difuso e a via judicial ordinária.

Não é, portanto, de reforma do direito material que a proteção de dados dependia em 2014, nem é disso que ela depende hoje. É de deslocamento do momento e do sujeito da tutela — da reação individual para o dever estrutural, do dano provado para o risco graduado. É o que a seção seguinte examina, a partir da revisão a que o próprio regime de responsabilidade do Marco Civil vem sendo submetido.

5 O ART. 19 SOB REVISÃO E O HORIZONTE DE SUCESSÃO

Se a proteção depende menos da norma do que de quem pode invocá-la, então o desenho do art. 19 do Marco Civil deixa de ser um detalhe de técnica processual e passa a ser o núcleo do problema. Vale, por isso, olhá-lo de frente.

O dispositivo condiciona a responsabilidade civil do provedor de aplicações ao descumprimento de ordem judicial específica de remoção. A escolha tinha justificativa robusta em 2014, e continua tendo, qual seja, transferir ao particular o juízo sobre a ilicitude do conteúdo alheio produz remoção preventiva por conveniência, e remoção por conveniência é censura terceirizada. O legislador preferiu correr o risco da permanência do ilícito ao risco do silencia-

mento privado, e reservou ao juiz a palavra sobre o que sai do ar. É uma opção defensável, e o art. 21, ao admitir notificação extrajudicial nos casos de divulgação não consentida de material de nudez ou de atos sexuais, mostra que o próprio legislador reconheceu haver situações em que ela não se sustenta.

O problema é que essa arquitetura foi desenhada para um tipo de dano que não é o único, nem hoje o principal. O art. 19 responde bem à pergunta sobre conteúdo ilícito individualizado — uma publicação, um perfil, uma imagem. Responde mal, ou não responde, à pergunta sobre danos que não decorrem de nenhuma publicação em particular, e sim do modo como a plataforma organiza a coleta, o direcionamento e a exposição. O caso examinado na seção anterior é exatamente desse segundo tipo: não havia conteúdo a remover, havia arquitetura a corrigir. Contra arquitetura, ordem judicial de remoção não opera.

Reaparece aqui, com nitidez, a incoerência apontada anteriormente, pois o art. 3º, VI, do próprio Marco Civil prometera responsabilização dos agentes de acordo com suas atividades — critério material, graduado, ancorado no risco que cada agente introduz. Por sua vez, os arts. 18 e 19 converteram essa promessa num regime de imunidade condicionada, em que a extensão da atividade do provedor não agrava a sua responsabilidade, e em que o agente estruturalmente mais relevante da cadeia é justamente o menos exposto. O princípio olhava para a atividade; a regra olhou para o conteúdo. Uma década depois, é o descompasso entre os dois que está sob exame. E está sob exame no sentido literal.

Ao completar dez anos, em abril de 2024, o Marco Civil da Internet tinha o núcleo do seu regime de responsabilidade civil pendente de definição no Supremo Tribunal Federal, nos Recursos Extraordinários nº 1.037.396 e nº 1.057.258, submetidos à sistemática da repercussão geral sob os Temas 987 e 533. Discute-se ali, precisamente, se a exigência de ordem judicial prévia é compatível com a proteção constitucional dos direitos de personalidade e com o dever estatal de proteção — e, no mesmo passo, se e em que medida a plataforma pode ser responsabilizada a partir de notificação extrajudicial. A revisão figurava na pauta da Corte desde o ano anterior, e a expectativa manifestada publicamente por ministros era de conclusão no curso de 2024. Há, portanto, uma constatação a registrar no balanço da década, e ela não é celebratória, pois o Marco Civil chega ao seu décimo aniversário sem que se saiba, com segurança, qual é o regime de responsabilidade civil das plataformas no Brasil.

A coincidência de calendário é quase literária, e merece registro. No mesmo mês de abril de 2024 em que a Lei nº 12.965 completou dez anos, a comissão de juristas presidida pelo Ministro Luis Felipe Salomão entregou ao Senado Federal o anteprojeto de reforma do Código Civil, cuja inovação mais estruturante é a criação de um livro autônomo dedicado ao direito civil digital na Parte Especial do Código. O aniversário e a proposta de sucessão ocorreram na mesma quinzena.

O conteúdo dessa proposta interessa diretamente à tese aqui sustentada, e interessa pela tensão que carrega. Entre os vetores declarados da reforma figura o propósito de assegurar maior autonomia de vontade às pessoas. E, simultaneamente, o livro digital projetado assenta-se em fundamentos que só fazem sentido porque a autonomia da vontade não basta: transparência algorítmica, autodeterminação informativa, proteção contra práticas discriminatórias, auditabilidade e responsabilidade civil pelos danos causados por sistemas automatizados. A reforma promete robustecer a vontade e, no mesmo movimento, ergue em torno dela salvaguardas heterônomas. Não é contradição — é o reconhecimento, agora em sede codificada, daquilo que o parágrafo único do art. 8º já dissera em 2014 sem que ninguém extraísse as consequências, porque há um campo em que a proteção não pode depender do que o titular declarou querer.

Convém, ainda, registrar o que mudou no plano institucional, porque a década não foi estéril. A lacuna diagnosticada na seção 4 — direitos sem quem os invocasse — foi parcialmente fechada. A Lei nº 13.709/2018 criou base legal própria e autoridade nacional; a Emenda Constitucional nº 115/2022 elevou a proteção de dados a direito fundamental autônomo; o projeto de marco legal da inteligência artificial tramita no Senado Federal. O Brasil de 2024 dispõe de um aparato que o Brasil de 2018 não tinha.

Resta saber se isso basta, e é aqui que o balanço dos dez anos deve encerrar-se em pergunta, não em resposta. A questão que se coloca ao ciclo seguinte não é mais a de 2014 — quem invoca a norma. É outra, e mais exigente, no sentido de quais deveres o ordenamento impõe ao agente antes de qualquer invocação, e segundo que critério eles se graduam. O art. 3º, VI, do Marco Civil oferece o critério e nunca foi operacionalizado. É a essa lacuna que a seção seguinte se dirige.

6 MATRIZ DE RISCO ALGORÍTMICO: UM CRITÉRIO PARA O CICLO SEGUINTE

A seção anterior encerrou-se numa pergunta: que deveres o ordenamento impõe ao agente antes de qualquer invocação, e segundo que critério eles se graduam. Convém dizer desde logo que a resposta exige o reconhecimento de que o direito privado brasileiro já respondeu a essa pergunta uma vez, num caso específico, e nunca generalizou a resposta.

Inicia-se pela honestidade quanto à origem da técnica. A graduação de obrigações por faixas de risco não é contribuição destes autores nem do direito brasileiro. Trata-se da arquitetura que a tradição regulatória europeia vem consolidando desde a proposta de regulamento sobre inteligência artificial apresentada pela Comissão Europeia em 2021, cujo desenho em níveis — do risco inaceitável, vedado, ao risco mínimo, apenas sujeito a deveres gerais — foi mantido no regulamento aprovado em 2024. Apresentar essa estrutura como achado original seria, além de incorreto, desnecessário. O que aqui se propõe é verificar se o direito privado brasileiro dispõe dos materiais para operar essa graduação e, em caso afirmativo, articulá-los num critério único, vinculado a consequências civis determinadas.

E dispõe. O parágrafo único do art. 927 do Código Civil já condiciona a responsabilidade objetiva à atividade que, por sua natureza, implica risco para os direitos de outrem — modelo de imputação que não pergunta pela vontade nem pela culpa, mas pela atividade desenvolvida. O art. 3º, VI, do Marco Civil, como demonstrado na seção 4, transpõe esse mesmo raciocínio para o ambiente digital ao eleger a responsabilização dos agentes de acordo com suas atividades. Acrescenta-se o art. 38 da Lei nº 13.709/2018 ao prever o relatório de impacto à proteção de dados pessoais, definido no art. 5º, XVII, instrumento que só faz sentido numa lógica de avaliação prévia de risco. As peças estão todas dispostas. O que nunca foi construído é o critério que as articula.

Há, contudo, um precedente que fez exatamente isso — e o fez no mesmo ano em que o Marco Civil entrou em vigor, o que a literatura sobre a década curiosamente não registra. Em 12 de novembro de 2014, a Segunda Seção do Superior Tribunal de Justiça julgou o Recurso Especial nº 1.419.697/RS, sob a sistemática dos repetitivos, fixando o Tema 710 e dando origem à Súmula nº 550. O objeto era o sistema credit scoring: um mecanismo estatístico que atribui pontuação de risco a consumidores a partir de variáveis múltiplas — em outras palavras, um sistema de decisão algorítmica, décadas antes de o vocabulário se popularizar.

O que a Corte decidiu merece leitura atenta, porque contraria o senso comum sobre proteção de dados. Primeiro, reconheceu a licitude da prática, com fundamento na Lei nº 12.414/2011. Segundo — e este é o ponto decisivo —, assentou que o consentimento do consumidor avaliado é desnecessário, assegurando-lhe, em contrapartida, o direito de obter esclarecimentos sobre as fontes dos dados considerados e sobre as informações pessoais valoradas. Terceiro, estabeleceu que o desrespeito aos limites legais configura abuso no exercício do direito, nos termos do art. 187 do Código Civil, podendo ensejar responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente, nas hipóteses de utilização de informações excessivas ou sensíveis e de recusa indevida de crédito baseada em dados incorretos ou desatualizados.

Observe-se a arquitetura da decisão. O consentimento é expressamente afastado como fundamento de legitimação. Em seu lugar entram deveres de transparência exigíveis independentemente de manifestação de vontade, um parâmetro material de licitude — a adequação e a atualidade dos dados — e um regime de imputação objetiva e solidária que alcança toda a cadeia de agentes. É, em substância, o modelo que este artigo defende, construído por um tribunal de direito privado, sete meses depois da sanção do Marco Civil, para um único sistema algorítmico.

A lacuna, portanto, não é de materiais nem de precedente, mas de generalização. O Superior Tribunal de Justiça resolveu o problema para o credit scoring; o Marco Civil enunciou o princípio e não o operacionalizou; a Lei Geral de Proteção de Dados criou o instrumento de avaliação prévia e deixou a definição das hipóteses de sua exigibilidade à discricionariedade da autoridade nacional. Ninguém construiu o critério geral. É o que se propõe a seguir, não como norma pronta, mas como parâmetro dogmático de graduação.

Quadro 2 — Matriz de risco algorítmico e consequências jurídico-privadas

Faixa	Critério de enquadramento	Consequência jurídico-privada proposta	Fundamento
Inaceitável	finalidade incompatível com a dignidade: classificação social generalizada, exploração de vulnerabilidade reconhecida, vigilância biométrica indiscriminada	nulidade de pleno direito da cláusula autorizativa e ineficácia do consentimento eventualmente colhido	MCI, art. 8º, § único; CDC, art. 51; CC, arts. 166 e 187
Alto	decisão automatizada com efeito sobre acesso a crédito, emprego, saúde, seguro, educação ou serviço essencial	responsabilidade objetiva e solidária dos agentes da cadeia; inversão do ônus da prova; dever qualificado de esclarecimento sobre fontes e variáveis; relatório de impacto obrigatório	CC, arts. 187 e 927, § único; CDC, art. 6º, VIII; LGPD, arts. 20 e 38; Lei nº 12.414/2011, art. 16; STJ, Tema 710
Moderado	personalização, recomendação e direcionamento sem efeito jurídico direto sobre o titular	dever de transparência reforçado; direito efetivo de revisão e de oposição; responsabilidade subjetiva com culpa presumida	MCI, art. 7º, VIII e XI; LGPD, art. 20; CDC, art. 6º, III
Baixo	tratamento acessório, anonimizado ou de suporte operacional	deveres gerais de segurança e de prestação de contas; presunção de conformidade	MCI, art. 3º, V; LGPD, arts. 46 a 50

Fonte: elaborado pelos autores (2024).

Duas observações sobre o quadro, ambas necessárias ao rigor da proposta. A primeira diz respeito à faixa de risco alto, e é uma extrapolação assumida: o Superior Tribunal de Justiça vinculou a responsabilidade objetiva e solidária ao abuso no exercício do direito, e não à atividade considerada em si. O que aqui se propõe é deslocar o fundamento do art. 187 para o parágrafo único do art. 927 do Código Civil, de modo que a imputação decorra da natureza arriscada da atividade e não da demonstração de excesso — solução coerente com o art. 3º, VI, do Marco Civil, que gradua responsabilidade por atividade, e que dispensa a vítima de provar aquilo que, num sistema opaco, ela estruturalmente não pode provar. A segunda observação é que o enquadramento não se faz pela tecnologia empregada, e sim pelo efeito jurídico produzido sobre a esfera do titular. Um mesmo modelo estatístico pode ocupar faixas distintas conforme decida sobre a concessão de um empréstimo ou sobre a ordem de exibição de um catálogo.

A utilidade prática do critério aparece quando aplicado. O sistema examinado no Tema 710 é, por essa matriz, de risco alto: decide sobre acesso a crédito, produz efeito jurídico direto e opera sobre dados cuja incorreção o titular não tem como auditar. O caso do sistema de triagem de currículos desenvolvido e posteriormente abandonado pela Amazon, que reproduziu vieses de gênero presentes nos dados históricos de contratação (Dastin, 2018), enquadra-se na mesma faixa, e o enquadramento traz consequências concretas, quais sejam, relatório de impacto prévio obrigatório, dever de esclarecimento sobre as variáveis empregadas e responsabilidade objetiva pelos danos, sem que o candidato preterido precise demonstrar culpa de quem quer que seja. Já um mecanismo de ordenação de conteúdo sem repercussão sobre direitos permanece na faixa moderada, sujeito a transparência e oposição, mas não ao regime agravado.

A diversidade de funções desempenhadas por sistemas automatizados reforça a necessidade de avaliar a atividade concreta e os efeitos produzidos, e não apenas o rótulo tecnológico. Germinari, Carmo e Galindo Ayuda demonstram que aplicações tecnológicas são úteis no contexto informacional atual, mas a sua incorporação deve permanecer subordinada à celeridade, à prontidão e, sobretudo, à segurança jurídica (Germinari; Carmo; Galindo Ayuda, 2024, p. 9, 17).

Nada disso substitui o Marco Civil, e é importante que assim seja lido. A matriz não propõe nova lei, mas o estabelecimento de um critério de aplicação para um princípio que a Lei nº 12.965/2014 positivou e jamais operacionalizou. Dez anos depois, o art. 3º, VI, continua sendo o dispositivo mais promissor e mais inerte do diploma — e a tarefa do ciclo seguinte, seja ele conduzido pelo Supremo Tribunal Federal na revisão do art. 19, seja pela codificação do direito civil digital, é menos a de escrever normas novas do que a de dar consequência às que já existem.

CONCLUSÃO

Este artigo partiu de uma pergunta simples e de resposta desconfortável: decorridos dez anos, o Marco Civil da Internet conseguiu limitar eficazmente a autonomia da vontade nas relações privadas digitais? O percurso realizado corrobora a hipótese formulada na introdução — a insuficiência verificada na década não foi de norma, foi de instituição.

Quatro resultados sustentam essa conclusão. O primeiro é dogmático: os arts. 3º, VI, 7º, IX, e 8º, parágrafo único, da Lei nº 12.965/2014 estabeleceram, desde 2014, um limite heterônimo à autonomia privada no ambiente digital, e o fizeram pela via da nulidade absoluta, sanção que opera de pleno direito, não convalesce e pode ser conhecida de ofício. O Marco Civil

não presumiu um usuário autônomo; presumiu um aderente, na linha que o art. 54, § 4º, do Código de Defesa do Consumidor inaugurara três décadas antes.

O segundo resultado é o mais eloquente, e é aritmético. No caso Cambridge Analytica, oitenta e quatro instalações do aplicativo em território brasileiro corresponderam a quatrocentas e quarenta e três mil pessoas atingidas no país. Em mais de noventa e nove por cento dos casos não houve vontade viciada, houve ausência integral de vontade. Não se trata, portanto, de consentimento mal-informado — categoria que a doutrina domina e que pressupõe alguma manifestação a ser corrigida —, mas de um modelo de legitimação que simplesmente não descreve o que acontece.

O terceiro resultado decorre do contraste entre os dois casos examinados. A única sanção brasileira no episódio Cambridge Analytica foi aplicada com fundamento no Código de Defesa do Consumidor, e não nos dispositivos do Marco Civil que o caso violou de modo mais direto. Na ADI 6.387, ao contrário, a proteção operou antes do dano, por iniciativa de legitimados institucionais dotados de acesso ao controle concentrado. Sustenta-se, assim, que a diferença entre os resultados decorre menos da densidade normativa disponível do que da existência de legitimado institucional apto a acionar a tutela.

O quarto resultado é propositivo e tem caráter mais modesto do que aparenta. O art. 3º, VI, do Marco Civil oferece o critério de graduação de responsabilidade por atividade que a década não operacionalizou, e o Superior Tribunal de Justiça, no Tema 710, demonstrou em 2014 que esse modelo funciona: dispensou o consentimento no credit scoring, substituiu-o por deveres de transparência exigíveis independentemente de vontade e imputou responsabilidade objetiva e solidária a toda a cadeia de agentes. A matriz apresentada na seção 7 não inventa esse arranjo; generaliza-o e vincula cada faixa de risco a consequências jurídico-privadas determinadas.

As limitações do estudo foram declaradas na seção 2 e merecem reafirmação. Dois casos não autorizam inferência causal. A matriz é parâmetro dogmático, não norma validada. E a extrapolação que desloca o fundamento da responsabilidade objetiva do art. 187 para o art. 927, parágrafo único, do Código Civil está assumida no texto, com as razões que a justificam e a ressalva de que se afasta, nesse ponto específico, do que o precedente decidiu.

Resta o que o balanço da década não pode responder. Ao completar dez anos, o Marco Civil tinha o núcleo do seu regime de responsabilidade civil submetido a exame de constitucionalidade e via a sua matéria ser objeto de proposta de codificação no anteprojeto de reforma do Código Civil. Se o próximo ciclo preservará, absorverá ou diluirá o núcleo privatista dos arts. 7º, IX, e 8º é questão em aberto, e escapa ao alcance deste estudo. O que se pode afirmar é que a tarefa mais urgente não é escrever normas novas, mas sim, dar consequência às que já existem — e a década examinada demonstrou, com clareza incômoda, que essas duas coisas não são a mesma.

REFERÊNCIAS

ALEMANHA. Tribunal Constitucional Federal. **Volkzählungsurteil**: sentença sobre a Lei do Censo. BVerfGE 65, 1. Karlsruhe, 15 dez. 1983.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988.

BRASIL. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014. Diário Oficial da União: Brasília, DF, 11 maio 2016.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Diário Oficial da União: Brasília, DF, 11 fev. 2022.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: Brasília, DF, 12 set. 1990.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União: Brasília, DF, 11 jan. 2002.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento. Diário Oficial da União: Brasília, DF, 10 jun. 2011.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: Brasília, DF, 24 abr. 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União: Brasília, DF, 15 ago. 2018.

BRASIL. **Medida Provisória nº 954, de 17 de abril de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações com a Fundação Instituto Brasileiro de Geografia e Estatística. Diário Oficial da União: Brasília, DF, 17 abr. 2020.

BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional do Consumidor. Departamento de Proteção e Defesa do Consumidor. **Decisão no processo administrativo relativo ao compartilhamento indevido de dados de usuários brasileiros**. Brasília, DF, 30 dez. 2019.

BRASIL. Senado Federal. Comissão de Juristas responsável pela revisão e atualização do Código Civil. **Relatório final e anteprojeto de reforma do Código Civil**. Brasília, DF: Senado Federal, abr. 2024.

BRASIL. Senado Federal. **Projeto de Lei nº 2.338, de 2023**. Dispõe sobre o uso da inteligência artificial. Brasília, DF: Senado Federal, 2023.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.419.697/RS**. Tema 710. Relator: Min. Paulo de Tarso Sanseverino. Segunda Seção, julgamento em 12 nov. 2014, DJe 17 nov. 2014. Brasília, DF: STJ, 2014.

BRASIL. Superior Tribunal de Justiça. **Súmula nº 550**. Brasília, DF: STJ, 2015.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 1.037.396**. Tema 987 da repercussão geral. Relator: Min. Dias Toffoli. Brasília, DF: STF. Pendente de julgamento.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 1.057.258**. Tema 533 da repercussão geral. Relator: Min. Luiz Fux. Brasília, DF: STF. Pendente de julgamento.

BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387/DF**. Relatora: Min. Rosa Weber. Tribunal Pleno, julgamento em 7 maio 2020. Brasília, DF: STF, 2020.

BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013.

CASTELLS, Manuel. **A sociedade em rede**. 18. ed. São Paulo: Paz e Terra, 2017. v. 1.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Conectividade significativa**: propostas para medição e o retrato da população no Brasil. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2024a.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros**: TIC Domicílios 2023. São Paulo: CGI.br, 2024b.

DASTIN, Jeffrey. Amazon scraps secret AI recruiting tool that showed bias against women. **Reuters**, 10 out. 2018. Disponível em: <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G>. Acesso em: 20 jun. 2024.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

INFORMATION COMMISSIONER'S OFFICE. **Investigation into the use of data analytics in political campaigns**: a report to Parliament. Wilmslow: Information Commissioner's Office, 2018.

FEDERAL TRADE COMMISSION. **Cambridge Analytica, LLC, in the matter of**. Washington, DC: FTC, 2019a.

FEDERAL TRADE COMMISSION. **FTC imposes \$5 billion penalty and sweeping new privacy restrictions on Facebook**. Washington, DC: FTC, 24 jul. 2019b.

FERNANDES, André Dias; MACHADO, Cláudio Gerlando Sampaio. A contribuição do Estado para a mitigação dos riscos e danos decorrentes da Quarta Revolução Industrial. **Revista Jurídica da FA7**, Fortaleza, v. 19, n. 3, p. 75-98, set./dez. 2022. DOI: 10.24067/rjfa7;19.3:1758. Disponível em: <https://periodicos.uni7.edu.br/index.php/revistajuridica/article/view/1758>. Acesso em: 20 jun. 2024.

GERMINARI, Jefferson Patrik; CARMO, Valter Moura do; GALINDO AYUDA, Fernando. Inteligência artificial, automação de processos, interoperabilidade e custo-benefício: onde está o problema da efetividade da justiça brasileira? **Revista Brasileira de Direito**, Passo Fundo, v. 20, n. 2, e5148, maio/ago. 2024. DOI: 10.18256/2238-0604.2024.v20i2.5148. Disponível em: <https://seer.atitus.edu.br/index.php/revistadedireito/article/view/5148>. Acesso em: 20 set. 2024.

INFORMATION COMMISSIONER'S OFFICE. **Investigation into the use of data analytics in political campaigns**: a report to Parliament. Wilmslow: ICO, 2018.

JAYME, Erik. Identité culturelle et intégration: le droit international privé postmoderne. **Recueil des Cours de l'Académie de Droit International de La Haye**, Haia, t. 251, v. II, 1995.

LESSIG, Lawrence. **Code**: version 2.0. New York: Basic Books, 2006.

MAGALHÃES, Rodrigo Almeida; OLIVEIRA, Erika Cristina Rodrigues Nardoni. O direito à privacidade na era digital. **Revista Jurídica da FA7**, Fortaleza, v. 18, n. 1, p. 55-70, jan./abr. 2021. DOI: 10.24067/rjfa7;18.1:1173. Disponível em: <https://periodicos.uni7.edu.br/index.php/revistajuridica/article/view/1173>. Acesso em: 20 jun. 2024.

MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor**: o novo regime das relações contratuais. 9. ed. São Paulo: Revista dos Tribunais, 2019.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MIRAGEM, Bruno. **Curso de direito do consumidor**. São Paulo: Thomson Reuters Brasil, 2020.

PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

SCHREIBER, Anderson. **Direitos da personalidade**. São Paulo: Atlas, 2013.

TEPEDINO, Gustavo. **Temas de direito civil**. Rio de Janeiro: Renovar, 2008.

UNIÃO EUROPEIA. Comissão Europeia. **Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial**. COM(2021) 206 final. Bruxelas, 21 abr. 2021.

UNIÃO EUROPEIA. **Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho**, que estabelece regras harmonizadas em matéria de inteligência artificial. Jornal Oficial da União Europeia, 12 jul. 2024.

VERBICARO, Dennis; NÓVOA, Natasha Siqueira Mendes de. O falso empoderamento do consumidor no sistema de avaliação de plataformas digitais: um estudo da inteligência artificial sob a perspectiva da vulnerabilidade algorítmica. **Revista Jurídica da FA7**, Fortaleza, v. 20, n. 1, p. 123-145, jan./abr. 2023. DOI: 10.24067/rjfa7;20.1:1676. Disponível em: <https://periodicos.uni7.edu.br/index.php/revistajuridica/article/view/1676>. Acesso em: 20 jun. 2024.

ZUBOFF, Shoshana. **The age of surveillance capitalism: the fight for a human future at the new frontier of power**. New York: PublicAffairs, 2019.