INSTITUTO IGARAPÉ
a think and do tank

ARTIGO
ESTRATÉGICO
39
DEZEMBRO 2018

Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?

Renato Leite Monteiro

Sumário

Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?

Renato Leite Monteiro[1]

Resumo

Decisões automatizadas cada vez mais controlam as nossas vidas. Elas estão presentes na definição da melhor rota para fugir do trânsito, na seleção de candidatos para vagas de trabalho e na formulação de políticas públicas. Esses são exemplos triviais de atividades (quase que) inteiramente gerenciadas por algoritmos, mas que podem ter impacto significativo na vida dos cidadãos. Todavia, sua maior presença no cotidiano é acompanhada de pouca transparência com relação ao seu funcionamento – o que torna mais complexa a identificação de práticas abusivas, discriminatórias ou, ainda, monopolísticas. Para mitigar tais efeitos legislações nacionais e internacionais de proteção de dados buscam assegurar os direitos à transparência, à explicação e a não estar sujeito a decisões automatizadas. O presente estudo faz uma análise dos aspectos jurídicos da proteção de dados pessoais no Brasil trazendo, mais especificamente, uma reflexão sobre a existência do direito à explicação no contexto de decisões automatizadas. Conclui que a legislação nacional, mais especificamente a lei de proteção de dados pessoais, foi além de outras regulações internacionais, como a GDPR, no que concerne este assunto. Isso porque expandiu o escopo de exercício desse direito, quando comparada com a regulamentação europeia.

Palavras-chave: **decisões automatizadas; dados pessoais; regulação; governança.**

1 Doutorando em Filosofia e Teoria Geral do Direito na Universidade de São Paulo - USP e Mestre em Direito Constitucional pela Universidade Federal do Ceará - UFC. LL.M em Technology Law pela NYU e NUS. Foi study visitor e consultor do Departamento de Proteção de Dados do Conselho da Europa. Professor convidado de diversas instituições, como Mackenzie e FGV. Colaborou ativamente com as discussões da Lei Geral de Proteção de Dados do Brasil - LGPD. Fundador e Coordenador do Data Privacy Brasil.

1. Introdução

Um indivíduo chega a um banco. Ele pretende dar entrada em um pedido de financiamento do seu primeiro apartamento. Se dirige ao gerente, que o recebe, pede o seu CPF, e o insere em um sistema da instituição. Ao assim fazer, os demais campos do formulário eletrônico são imediatamente preenchidos. O gerente solicita, ainda, informações sobre o valor do imóvel, quanto o indivíduo pretende dar de entrada, quanto pretende financiar, e em quanto tempo. Imediatamente o sistema calcula uma taxa de juros muito superior àquela anunciada pela instituição nos inúmeros outdoors e propagandas espalhadas pela cidade. O valor é tão alto que torna impossível contratar tal financiamento, impedindo, desta forma, que o indivíduo possa adquirir o imóvel. Ele pergunta ao gerente por que a taxa de juros do seu financiamento seria tão alta, já que não tem dívidas, sempre pagou suas contas em dia, e recebe um salário que claramente o permite pagar uma parcela normal de um financiamento. O gerente apenas informa que o sistema faz o cálculo e exibe na sua tela e que não tem qualquer ingerência sobre os valores das taxas de juros e das parcelas mensais. Quem faz e controla tudo é um programa de computador. Em outras palavras, um programa de computador, alimentado, a princípio, por dados sobre o indivíduo e sobre o imóvel que desejava adquirir, definiu suas chances de adquirir ou não um bem, e de usufruir de forma efetiva do seu direito à moradia. Um algoritmo tomou uma decisão que teve um impacto direto na vida deste indivíduo.

Assim como no exemplo acima, cada vez mais, nossas vidas são controladas por algoritmos. Trata-se de sequências pré-definidas de comandos automatizados que, com base em dados pessoais e não pessoais,[2] chegam a conclusões que podem sujeitar alguém a uma determinada ação, a qual pode ou não ter impacto significativo na sua vida. Em sistemas mais complexos, como os que se valem de aprendizado de máquina,[3] essas sequências pré-definidas podem ser alteradas de acordo com as variáveis usadas como substrato,[4] e também pelas conclusões intermediárias.[5] Essa natureza adaptativa tem se tornado mais comum, graças a complexos sistemas de inteligência artificial e aprendizado de máquina capazes de influenciar as conclusões intermediárias – a ponto de não ser mais possível prever os resultados finais ou entender sua lógica subjacente. Essa opacidade impede que as pessoas entendam e verifiquem se seus dados pessoais são tratados de forma legítima, adequada e proporcional.

Regular o uso e o tratamento de dados pessoais é o principal objetivo das leis de proteção de dados. Estas visam não somente proteger a privacidade, mas também outros direitos fundamentais e liberdades individuais, que somente podem ser exercidos na sua completude caso seja garantido o uso adequado dos dados pessoais que, muitas vezes, funcionam como representação do indivíduo. Desta forma, as leis de proteção de dados são como "guarda-chuvas" regulatórios que protegem outros direitos. Elenca-se, abaixo, diferentes contextos nos quais as decisões automatizadas têm impacto no exercício e acesso a uma série de direitos fundamentais e aponta-se como a opacidade no tratamento dos dados pessoais

2 A Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados do Brasil ("LGPD"), define, em seu Art. 5º, I, que dado pessoal é a "informação relacionada a pessoa natural identificada ou identificável". Ou seja, toda informação que (isolada ou agregada) pode permitir a identificação de uma pessoa natural. Nomes, telefone, CPF, e-mail, gostos, interesses, localização, são exemplos de dados pessoais. Ou, ainda, permitir que esta seja individualizada e, portanto, sujeita a determinados comportamentos, ainda que não identificada, como no caso de processamento de informações que possam fazer a análise de comportamento de grupos, influenciando a vida dos indivíduos que fazem parte destes. Já dados não-pessoais são informações que não dizem respeito a uma pessoa natural, portanto, fora do escopo de aplicação de leis de proteção de dados pessoais.

3 O termo "aprendizado de máquina" (*machine learning*, em inglês) faz referência a um método algorítmico que permite a um sistema chegar a conclusões mediante tentativas e erros, até alcançar o resultado almejado. O sistema aprende com seus erros em uma espécie de inteligência artificial. Entre as modalidades de aprendizado de máquina, existe o "aprendizado profundo" (*deep learning*, em inglês), que utiliza sistemas paralelos para aprender e, muitas vezes, seu resultado final pode ser diferente do antevisto por quem desenvolveu o algoritmo. Ver: BURRELL (2016).

4 O termo substrato é aqui utilizado em referência aos dados de entrada que alimentarão os algoritmos, que podem ser dados pessoais ou não-pessoais. Assim como uma fórmula matemática que recebe valores numéricos para que o cálculo seja feito, um algoritmo recebe dados para processá-los e atingir um resultado.

5 Algoritmos baseados em metodologias de aprendizado de máquina e aprendizado profundo podem chegar a várias conclusões intermediárias antes de atingir o seu resultado final. Estas servem para ensinar o algoritmo a atingir o resultado correto, a partir de tentativa e erro, ou até mesmo alterar o algoritmo para atingir outros resultados, alguns deles não antevistos por seus desenvolvedores.

impede que seus titulares tenham total compreensão de como seus direitos são impactados:

- **Direito à saúde:** o uso de dados pessoais no campo da saúde visa, entre outras práticas, a realização de diagnósticos e, até mesmo, a prevenção de doenças. Não é difícil imaginar uma situação onde um paciente será submetido a um tratamento preventivo baseado na probabilidade de desenvolver uma enfermidade. Análises de dados genéticos são um bom exemplo desse cálculo probabilístico. Com base nas conclusões derivadas de um algoritmo que teve como substrato os dados pessoais genéticos de um indivíduo, um plano de saúde pode decidir conceder ou não uma apólice ou calcular o seu valor.[6] Pode, ainda, de forma totalmente automatizada,[7] agregar tais dados a bases públicas, como do Sistema Único de Saúde (SUS), e fazer inferências de dados a partir de outras fontes, como redes sociais e dados de locais frequentados pelos indivíduos. Quando cruzados, esses dados formam um perfil comportamental que alimentará sistemas capazes de influenciar de forma contundente o acesso a serviços de saúde de qualidade.[8]

- **Direito à educação:** algumas escolas já utilizam sistemas complexos para adaptar suas metodologias de ensino às características individuais de cada criança – processo conhecido como aprendizado adaptativo (*adaptative learning*, em inglês), – ou para definir em que turmas ou estabelecimentos educacionais os alunos devem ser alocados, visando aulas de maior qualidade e eficiência. Para tanto, são utilizadas variáveis como as notas anteriores dos alunos, local onde residem e as supostas inclinações para ciências humanas, exatas, biológicas, habilidades manuais ou intelectuais. Tais sistemas irão determinar como, quando e onde essas crianças deverão estudar, tudo isso apenas com base nas informações apresentadas na matrícula no início do semestre.[9] Todavia, o que pode parecer um grande benefício, pode fazer com que indivíduos com características e habilidades similares sejam aglomerados em grupos que terão pouca exposição a outras realidades que não as suas, levando a uma provável pasteurização do ambiente educacional.[10] Pode, ainda, marginalizar crianças classificadas com alguma dificuldade, afetando seu acesso a uma educação de qualidade.

- **Direito ao pleno emprego:** é cada vez mais comum que empresas anunciem vagas de emprego em suas páginas institucionais e perfis em redes sociais. A exposição por tais meios pode levar a uma quantidade tão grande de candidatos, que se tornaria inviável para uma única pessoa a analisar todos os currículos recebidos. Por isso, já existem sistemas que fazem triagens dos candidatos com base em critérios pré-definidos, como a fluência em idiomas estrangeiros, os anos de experiência com determinada matéria, o conhecimento específico sobre uma questão técnica e um conjunto de habilidades interpessoais. O candidato será selecionado ou não pelo sistema quando for verificado que suas informações coincidem com tais critérios. Caso não coincidam, não passará para as fases onde haverá uma aferição humana.[11]

- **Direito à informação:** o conteúdo da linha do tempo de uma rede social ou os resultados de pesquisa de um serviço de busca são diretamente influenciados pelos dados pessoais dos seus usuários. Preferências, interesses, localização e serviços acessados são exemplos de categorias de dados pessoais utilizadas pelos algoritmos dessas plataformas para decidir a quais

6 SASAKI et al. (2010).

7 Decisões totalmente automatizadas são aquelas que prescindem de intervenção humana. Em outras palavras, o algoritmo irá processar os dados até chegar a uma decisão. A intervenção humana se limitará a cumprir, comunicar ou verificar a conclusão do sistema.

8 POWLES; HODSON (2017).

9 MONTEIRO; CARVINO (2015).

10 O termo pasteurização faz referência a uma situação de normalidade, onde tudo e todos do ambiente se comportam e pensam de forma idêntica ou similar. No contexto educacional, isso poderia ter impacto nos processos dialéticos, de críticas e no próprio aprendizado.

11 PURAM; SADAGOPAL (2001).

informações seus usuários terão acesso. A decisão dos algoritmos pode influenciar, assim, aquilo que o usuário vê em seu *feed* e o modo como forma sua visão de mundo sobre determinados assuntos. Os algoritmos podem, inclusive, ser manipulados para dar preferência a determinados conteúdos, com o objetivo de influenciar o comportamento das pessoas.[12] Em um contexto de campanhas de desinformação, o uso de dados pessoais para determinar a quais notícias e conteúdos os indivíduos serão expostos pode ter um grande impacto no acesso à informação.[13]

- **Direito à liberdade:** o cálculo da pena de um condenado por um crime leva em consideração alguns aspectos, tais como: bom comportamento, reincidência, pena base e circunstâncias do delito praticado. Esse cálculo geralmente é feito por um magistrado, que deve justificá-lo. Todavia, alguns sistemas jurídicos permitem a utilização de programas de computador para auxiliar no referido cálculo.[14] Tais sistemas, podem, ainda, comparar o caso com outros similares que estejam cadastrados em bases de dados públicas, e levar em consideração as peculiaridades das condenações anteriores para alimentar o algoritmo que irá auxiliar a atribuição da pena. Assim, o algoritmo alimentado com dados pessoais dos condenados irá, por meio de um processo totalmente automatizado, determinar o tempo de encarceramento de indivíduo.

- **Direito à cidadania:** em determinadas regiões do mundo o acesso a serviços públicos pode ser influenciado por uma pontuação atribuída a indivíduos com base em dados pessoais ou dados sobre as comunidades e grupamentos nos quais estão inseridos.[15] Dados como taxas de inadimplência e adimplência de pagamentos, geolocalização, interesses, e até mesmo manifestações públicas a favor ou contra governos, podem servir como variáveis para o cálculo da referida pontuação. Caso o "score social", como por vezes são chamados tais sistemas, diminua a pontuação de uma pessoa quando esta criticar o governo, comportar-se de forma considerada anormal, ou contra o senso comum da sociedade em que se encontra, isto pode levar a uma aversão ao diferente e a discriminações exacerbadas.[16] Nesse tipo de cenário, processos totalmente automatizados e opacos podem limitar direitos básicos dos cidadãos já que possuem possível assimetria de informações entre o indivíduo e o Estado/entes privados.

Os exemplos acima permitem contextualizar a necessidade de dois novos direitos garantidos pela Lei Geral de Proteção de Dados do Brasil (Lei 13.709/2018, também chamada de "LGPD") e pela Regulação Geral de Proteção de Dados da União Europeia[17] (aqui sob o acrônimo de "GDPR"). O primeiro, o *direito à explicação*, diz respeito ao direito de receber informações suficientes e inteligíveis que permita ao titular dos dados entender a lógica e os critérios utilizados para tratar seus dados pessoais para uma ou várias finalidades. Já o segundo, denominado *direito à revisão* de decisões totalmente automatizadas, compreende o direito do titular de requisitar a revisão, por um humano, de uma decisão totalmente automatizada que possa ter um impacto nos seus interesses, principalmente os relacionados à definição do seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. Ambos serão melhor abordados a seguir.

Esse artigo aborda, em linhas gerais, o que seria o direito à explicação e qual a sua importância e o faz a partir de um exercício de comparação entre a GDPR e a LGPD. Em seguida, discorre sobre como leis setoriais de proteção de dados brasileiras e a lei geral de proteção de dados buscam regular e garantir os direitos à explicação e à revisão de decisões automatizadas, todavia, impondo limitações que podem ter impacto no seu efetivo exercício. Mais adiante, será descrito como a nova regulamentação europeia de proteção de dados tratou dos mesmos direitos. Isto permitirá uma comparação entre os dois

12 ADAM et al. (2014).

13 INFORMATION COMMISSIONER'S OFFICE (2018).

14 ANGWIN; LARSON; MATTU; KIRCHNER (2016).

15 ROLLET (2018).

16 ROLLET (2018).

17 UNIÃO EUROPEIA (2016).

arcabouços regulatórios, visando verificar se, efetivamente, existe no Brasil – e em que medida – um direito à explicação de decisões automatizadas baseadas em dados pessoais. A hipótese a ser verificada é que não apenas tais direitos existem, como a forma como foram desenvolvidos na lei brasileira lhes dá um escopo de aplicação muito mais amplo do que aquele do contexto europeu.

Por fim, o artigo visa proporcionar uma interpretação aos direitos à explicação e à revisão de decisões automatizadas na forma como foram previstos na LGPD. Assim, contribui, para que os responsáveis por sua aplicação e posterior regulação tenham subsídios mínimos para garantir tais direitos, principalmente no contexto brasileiro, onde a cultura de proteção de dados ainda está na sua infância.

O direito à explicação deriva diretamente do princípio da transparência, previsto na maioria das leis de proteção de dados do mundo

2. O direito à explicação

O direito à explicação deriva diretamente do princípio da transparência, previsto na maioria das leis de proteção de dados do mundo,[18] e que garante aos titulares dos dados "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento",[19] em conjunto com critérios de legitimidade e justiça.[20] No contexto da GDPR, Selbst e Powles, defendem a existência efetiva de tal direito na nova regulamentação europeia e afirmam que, apesar de não haver uma previsão textual específica na norma, esse direito não seria ilusório.[21] Em claro contraponto a outros autores que defendem a sua inexistência,[22] afirmam categoricamente que a GDPR, ao estabelecer direitos de informação sobre a lógica de processos de decisões automatizadas,[23] confere claramente o direito à explicação,[24] e este deve ser interpretado de modo a permitir ao titular dos dados o exercício de seus direitos previstos na GDPR e no ordenamento jurídico.[25]

2.1. O direito à explicação no contexto brasileiro

Após quase uma década de discussão, duas consultas públicas, mais de 2500 contribuições, várias audiências públicas no Congresso Nacional e interações com diversos atores nacionais e internacionais, foi aprovada, no dia 14 de agosto de 2018, a Lei Geral de Proteção de Dados do Brasil (Lei 13.709/2018). A nova lei, que foi elaborada de forma multissetorial e transversal, contempla direitos que já eram encontrados no conjunto de leis nacionais, como o direito à transparência e de explicação. Todavia, antes da aprovação da LGPD, tais direitos só eram garantidos em decisões automatizadas

18 GREENLEAF (2017a).

19 De acordo com o artigo 6º da Lei de Proteção de Dados Brasileira, "as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (...) VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial". Ver: BRASIL (2018).

20 GDPR. Art. 5. Personal data shall be: 1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').

21 SELBST; POWLES (2017).

22 WACHTER; MITTELSTADT; FLORIDI (2017).

23 Os artigos 13 e 14 da GDPR garantem o direito a "informações úteis relativas à lógica subjacente".

24 SELBST; POWLES (2017).

25 Idem, Ibidem.

relativas à concessão de crédito, modelagem e cálculo de risco de crédito. Isto quer dizer que, em nenhum dos casos apresentados no início do artigo, o titular poderia, com base na legislação nacional então vigente, requisitar explicações sobre o tratamento de seus dados pessoais, o que ilustra uma verdadeira situação de obscuridade e opacidade em relação aos processos decisórios.

Para entender como esse direito evoluiu de uma proteção setorial para uma geral, discute-se seu tratamento pelo Código de Defesa do Consumidor e pela Lei do Cadastro Positivo. Também se analisa a decisão paradigmática do Superior Tribunal de Justiça (STJ), que conferiu a atual interpretação ao texto desta lei. Em seguida, verifica-se como a LGPD consolidou o entendimento da corte superior.

2.2. Regulações setoriais: Código de Defesa do Consumidor, Lei do Cadastro Positivo e o posicionamento dos tribunais superiores

Um dos setores da economia e do mercado que mais se vale do uso e tratamento de dados pessoais, principalmente para viabilizar decisões automatizadas para ofertar seus serviços, é o de consumo. Este setor é caracterizado pela necessidade de se entender o consumidor e, inclusive, influenciar seus hábitos. No entanto, neste cenário, o consumidor se encontra em posição vulnerável em sua relação com as empresas[26] e, por isso, deve ser protegido. Entre as medidas de proteção, deve-se incluir o fornecimento de informações adequadas para que possa exercer seus direitos e evitar práticas abusivas e discriminatórias.[27] À medida que variados modelos de negócio se baseiam, cada vez mais, na coleta e processamento de dados pessoais, o uso intenso desse tipo de informação pode levar à práticas indesejadas, abusivas e prejudiciais – conforme ilustrado nos exemplos no início deste trabalho. Para entender como o mercado de consumo instrumentalizou ferramentas para combater tais práticas, analisamos o Código de Defesa do Consumidor e a Lei do Cadastro Positivo.

O Código de Defesa do Consumidor (Lei 8.078/90, ou CDC), é uma regulação setorial que se aplica às relações de consumo, sejam elas *online* ou *off-line*, e estabelece a transparência e a boa-fé como princípios que orientam essas relações.[28] No que diz respeito à boa fé, em sua forma objetiva,[29] é entendimento do STJ que "(...) seria como um modelo ideal de conduta, que se exige de todos os integrantes da relação obrigacional (devedor e credor) na busca do correto adimplemento da obrigação, que é a sua finalidade".[30] A interpretação conjunta do CDC e da decisão do STJ, aponta para o dever de informar o consumidor de maneira clara e objetiva, a respeito da relação contratual, o que inclui o período de formação dessa relação (pré-negocial) e o dever de máxima transparência dos arquivos de consumo. Nesse sentido, o dever de informação se deve às obrigações derivadas da boa-fé objetiva.

26 CDC. Art. 4º. A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios: I - reconhecimento da vulnerabilidade do consumidor no mercado de consumo.

27 CDC. Art. 6º. São direitos básicos do consumidor: (...) III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem; (...) IV - a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços.

28 Ver artigo 4º do Código de Defesa do Consumidor.

29 A boa-fé subjetiva se refere ao estado psicológico da pessoa, consistente na justiça, ou, na licitude de seus atos, ou na ignorância de sua antijuricidade. Já a boa-fé objetiva consiste em um dever ativo de conduta contratual de ambos os contratantes e os obriga a colaborar e cooperar, levando em consideração os interesses um do outro, a fim de alcançar o efeito prático que justifica a existência jurídica do contrato celebrado. Ver: COELHO (2011).

30 SUPERIOR TRIBUNAL DE JUSTIÇA (2012).

Destaca-se dois artigos do CDC que tratam do acesso a informações cadastrais e bancos de dados. O primeiro deles, o artigo 43, ao regular os arquivos de consumo, deixou expresso o direito de acesso do consumidor, nesses cadastros e bancos de dados, a informações a seu respeito e às respectivas fontes. Também determinou o dever de clareza dos arquivos, o direito de retificação de informações incorretas e que o consumidor deve ser notificado sobre a coleta e o uso de seus dados, [31] ainda que o consentimento prévio não seja necessário – com a exceção de casos de compartilhamento com terceiros, conforme o entendimento do Ministério da Justiça.[32] Além disso, estipula um período máximo de armazenamento dos dados do consumidor de cinco anos. Já o artigo 46 determina que:

> (...) os contratos que regulam as relações de consumo não obrigarão os consumidores, se não lhes for dada a oportunidade de tomar conhecimento prévio de seu conteúdo, ou se os respectivos instrumentos forem redigidos de modo a dificultar a compreensão de seu sentido e alcance.

O artigo não só reafirma o direito à informação sobre a relação de consumo, mas também determina que deve ser repassada de forma inteligível, para garantir a sua compreensão.

Dessa forma, quando houver decisão automatizada no contexto de uma relação de consumo, como a concessão ou não de um financiamento de veículo, por exemplo, o consumidor tem o direito de acessar os (seus) dados que basearam a tomada da decisão. Caso seja criada uma obrigação jurídica, é seu direito, também, ter conhecimento de suas finalidades e propósitos, seu alcance e como foi formada, incluindo critérios e valoração dos atributos utilizados para tomar a decisão. Em outras palavras, entender como se deu a formação da obrigação jurídica é essencial para a sua aceitação e exercício dos direitos previstos no CDC. E isso inclui entender como um algoritmo deu origem a tal obrigação.

Esta lógica também foi empregada pela Lei do Cadastro Positivo (Lei 12.414/2011, LCP), que estabelece normas voltadas à "disciplina e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para a formação de histórico de crédito".[33] Entre os principais objetivos desta lei estão reduzir a assimetria de informações e possibilitar a coleta de dados de adimplência após o consentimento prévio do consumidor. Afirma-se que isso possibilitaria a redução de taxas de juros e uma consequente ampliação das relações comerciais, o que favoreceria e protegeria todo o ecossistema consumerista.[34] A norma visa, também, a adequada proteção de dados pessoais de consumo, ao prever uma série de novos direitos, entre eles o direito à explicação.

Nesse contexto, lista-se alguns direitos previstos no seu Art. 5º, aqui escritos na sua íntegra:

> Art. 5º. São direitos do cadastrado: (…)
>
> IV - conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial;

---

31 CDC. Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

32 BRASIL (2002b).

33 BRASIL (2011).

34 PORTO (2009).

> V - ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento;
>
> VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; e
>
> VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados.

Estes quatro direitos se originam a partir do direito à transparência e não-discriminação e formam a espinha dorsal do direito à explicação

Estes quatro direitos se originam a partir do direito à transparência e não-discriminação e formam a espinha dorsal do direito à explicação de decisões automatizadas em relações de consumo. Eles exigem que o consumidor seja esclarecido sobre as fontes de dados utilizadas e as informações pessoais consideradas para o cálculo do risco de inadimplência na concessão ou não de crédito. A Lei também tenta limitar os tipos de dados que podem ser utilizados para cálculo do risco de crédito, vedando o uso de dados não relacionados com a análise do risco de crédito do consumidor, assim como dados pessoais sensíveis e os pertinentes "à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas".[35]

O STJ julgou a legalidade no uso de dados pessoais, sem o consentimento do indivíduo, para fins de análise de risco de crédito e concluiu que essa prática é possível, desde que presentes os fatores limitadores descritos acima e garantidos os direitos do consumidor, entre eles o direito à explicação.[36] Essa decisão culminou na Súmula 550, que prescreve:

> Súmula 550. A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo.

Posteriormente, o tribunal julgou se o direito de acesso às fontes dos dados e a explicação da lógica do seu tratamento encontravam algum fator limitador.[37] Concluiu que existe interesse de agir do consumidor que deseja conhecer os principais elementos e critérios considerados para a análise do seu histórico e as informações pessoais utilizadas – respeitado o segredo empresarial, – desde que tenha sido atingido por tais critérios quando tentou obter crédito no mercado,[38] p.ex., deixou de conseguir crédito devido à pontuação que lhe foi atribuído. O STJ estabeleceu, assim, um critério que até então não encontrava respaldo na lei, possibilitando reconhecer a existência do direito à explicação de decisões totalmente automatizadas, desde que tais decisões tenham um impacto específico na vida das pessoas.

Dessa forma, em conjunto com o CDC, esta norma forma um microssistema de proteção de dados pessoais que, infelizmente, se restringe apenas ao caso da concessão de crédito. Nestas situações, o consumidor pode requisitar informações sobre o uso de seus dados em uma decisão automatizada

35 BRASIL (2011).

36 RESP nº 1.419.697 RS. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/152068666/recurso-especial-resp-1419697-rs-2013-0386285-0/relatorio-e-voto-152068681>.

37 RESP nº 1.304.736/RS. Disponível em: < https://stj.jusbrasil.com.br/jurisprudencia/178798658/recurso-especial-resp-1304736-rs-2012-0031839-3>.

38 MENDES (2014).

de classificação de risco para concessão ou não do crédito. Caso não concorde com esta decisão por entender que foi tomada em desacordo com os critérios permitidos pela Lei do Cadastro Positivo, pode pedir a sua revisão por uma pessoa, conforme garantido no rol de direitos listado acima. A revisão humana, em tese, afastaria os elementos que foram indevidamente utilizados pelo algoritmo, como dados em excesso ou dados sensíveis. Todavia, cabe questionar se uma decisão tomada por uma pessoa, e não por um sistema, seria menos enviesada.[39]

Nota-se, ainda, que os direitos e balizas previstos nas leis e precedentes judiciais foram absorvidos pela Lei Geral de Proteção de Dados do Brasil, o que sugere que a lógica adotada pelo STJ também deve ser utilizada para interpretar a LGPD, como se verifica a seguir.

2.3. Lei Geral de Proteção de Dados do Brasil (LGPD)

Como visto, o Código de Defesa do Consumidor e a Lei do Cadastro Positivo regulamentam o direito à explicação e à revisão de decisões automatizadas no âmbito das relações de consumo, mais especificamente quando envolvem a concessão de crédito e cálculo de risco de inadimplência. Mas essa proteção setorial é insuficiente. Na verdade, em nenhum dos exemplos mencionados nesse trabalho os instrumentos de proteção consumerista seriam satisfatórios. Daí a importância de previsões capazes de expandir esses direitos para contextos mais variados, *online* e *off-line*, envolvendo o uso de dados pessoais. Para esse fim, foi promulgada a Lei Geral de Proteção de Dados do Brasil (LGPD), que transplanta o sistema setorial de proteção nacional para um geral, que abrange o tratamento de dados pessoais, independente do contexto, setor e mercado.

A LGPD complementa, harmoniza e unifica um ecossistema de mais de quarenta normas setoriais que regulam, de forma direta e indireta, a proteção da privacidade e dos dados pessoais no Brasil.[40] Foi inspirada nas discussões que culminaram na GDPR europeia e tem por objetivo não apenas conferir às pessoas maior controle sobre seus dados, mas também fomentar um ambiente de desenvolvimento econômico e tecnológico, mediante regras flexíveis e adequadas para lidar com os mais inovadores modelos de negócio baseados no uso de dados pessoais. Isso inclui modelos de negócio que se valem de algoritmos para auxiliar na tomada de decisões automatizadas. A LGPD também busca equilibrar interesses econômicos e sociais, garantindo a continuidade de decisões automatizadas e também limitando abusos nesse processo, por meio da diminuição da assimetria de informações, e, por consequência, de poder, entre o indivíduo, setor privado e o Estado.

Ao incluir 10 princípios gerais de proteção de dados pessoais, a Lei garante aos titulares dos dados[41] o direito à transparência,[42] ou seja, o direito de obter "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento,[43] observados os segredos comercial e industrial". Ou seja, a garantia para que se requisite de órgãos públicos e privados informações sobre como os seus dados são usados. Esse direito, que dá origem ao direito de acesso aos dados, é complementado pelo artigo 19, que determina que "A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular" e se darão "por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular".

39 MILLER (2018).

40 MONTEIRO (2017).

41 De acordo com o art. 5º da LGPD, é titular de dados toda pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

42 Artigo 6º, IV.

43 LGPD. Art. 5º. Para os fins desta Lei, considera-se: (...) controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; (...) operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; (...) agentes de tratamento: o controlador e o operador.

Ou seja, o princípio da transparência deve reger toda e qualquer relação do responsável pelo tratamento de dados pessoais com o titular dos dados, garantindo a este o direito de acesso aos seus dados pessoais. Esse princípio também pressupõe o dever de informar os critérios de tratamentos utilizados para finalidades informadas ao titular.[44]

o artigo 20 da LGPD garante o direito de solicitar a revisão, por um ser humano, de uma decisão tomada unicamente com base em tratamento automatizado

Já o artigo 20 da LGPD garante o direito de solicitar a revisão, por um ser humano, de uma decisão tomada unicamente com base em tratamento automatizado. O objetivo é evitar que indivíduos sejam alvo de práticas discriminatórias dos algoritmos responsáveis pela decisão. Todavia, não é qualquer decisão totalmente automatizada que pode ser alvo de uma revisão humana: somente as que afetam os interesses dos titulares dos dados pessoais, o que inclui, mas não se limita, àquelas utilizadas para definir perfis comportamentais de cunho pessoal, profissional, de consumo e de crédito. Salienta-se que os exemplos listados no artigo 19 não são exaustivos.

Além destes artigos, cabe destacar o tratamento dado pela Lei ao caso de re-identificação de dados anonimizados.[45] Quando utilizados para composição de um perfil comportamental, dados dessa natureza poderão ser considerados como pessoais, desde que façam referência a uma pessoa identificada. De acordo com o artigo 12, dados anonimizados somente são considerados dados pessoais "quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido" ou então quando se tratar de dados "utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada".[46]

O que o artigo trata como "pessoa identificada" faz referência ao conceito de dado pessoal previsto no artigo 5º, I, que pode incluir formas de diretamente identificar uma pessoa natural, por meio do seu nome ou características distintivas únicas; identificadores únicos, como CPF, RG, CNH; e até mesmo identificadores eletrônicos, como e-mail e *cookies*.

Caso o responsável pelo processamento dos dados se recuse a fornecer os dados pessoais utilizados na decisão automatizada e a explicar os critérios e/ou a lógica subjacente dos algoritmos que controlam o processo de tomada de decisão, a Lei prevê que poderá ser requisitado à futura Autoridade Nacional de Proteção de Dados (ANPD)[47] que seja realizada, após processo administrativo em que deve ser garantido a ampla defesa e o contraditório,[48] auditoria nos sistemas da entidade. Esse procedimento visa verificar, principalmente, a existência de aspectos discriminatórios, tais como o uso de dados

44 A redação do artigo 20 da lei é similar àquela do inciso II do artigo 19. Vide: Art. 20. O titular dos dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. §1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

45 LGPD. Art. 5º Para os fins desta Lei, considera-se: (...) III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; (...) XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

46 Art. 12, caput e §2º.

47 No momento em que este artigo foi escrito, a Autoridade Nacional de Proteção de Dados, a ANPD, ainda não havia sido criada, em visto do veto presidencial ao artigo 52 da Lei de Proteção de Dados. Todavia, como a competência da autoridade, prevista no Art. 22, § 2º, não foi vetada, permanece a possibilidade de sua criação.

48 Art. 23. § 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

pessoais sensíveis ou que excedam a finalidade pretendida.[49] Todavia, aferir eventuais discriminações pode ser um trabalho extremamente técnico, devido à complexidade dos algoritmos, o que demonstra a necessidade de a ANPD ter um corpo de profissionais altamente especializado e preparado. Portanto, a LGPD amplia essas vedações no uso de dados para além das relações de consumo, para incluir outros usos de dados pessoais.

Em síntese, a LGPD garante aos indivíduos o direito a ter acesso a informações sobre que tipos de dados pessoais seus são utilizados para alimentar algoritmos responsáveis por decisões automatizadas. Caso o processo automatizado tenha por finalidade formar perfis comportamentais ou se valha de um perfil comportamental para tomar uma decisão subsequente essa previsão também incluirá o acesso aos dados anonimizados utilizados para enriquecer tais perfis. Esse direito ainda inclui a possibilidade de conhecer os critérios utilizados para tomar a decisão automatizada[50] e de solicitar a revisão da decisão por um ser humano[51] quando esta afetar os interesses dos titulares.

Pela Lei, os direitos à explicação e à revisão de decisões automatizadas podem ser usufruídos em qualquer tipo de tratamento de dados pessoais, independente do setor ou mercado. Isto confere ao titular dos dados pessoais ferramentas importantes para coibir abusos e práticas discriminatórias no uso dos seus dados. Tais direitos devem contribuir diretamente para uma mudança na forma como produtos, serviços e processos são desenvolvidos, devido às obrigações de informar e explicar atribuídas aos agentes de tratamento. Estes terão que pensar, desde a concepção, como garantir os direitos previstos na LGPD. Espera-se que isso diminua a obscuridade e a opacidade dos algoritmos.[52]

A próxima seção apresenta o tratamento dado a esses direitos pela Lei de Proteção de Dados europeia.

3. O contexto da União Europeia: a Regulação Geral de Proteção de Dados da União Europeia

A União Europeia e as instituições do velho continente há décadas lideram as discussões sobre leis de proteção de dados.[53] Em 1995, foi aprovada a Diretiva Europeia de Proteção de Dados.[54] Concebida em uma era anterior ao surgimento da internet comercial e muito antes da difusão dos modelos de negócio e tecnologias que se valem do uso intenso de dados pessoais e que são quase que onipresentes na vida das pessoas, precisou passar por um processo de atualização que culminou com a atual Regulação Geral de Proteção de Dados da União Europeia (GDPR, da sigla em inglês).

---

49 Art. 20, § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

50 A Lei prevê duas exceções: os casos de segredo industrial e comercial. Observa-se que nessas hipóteses, é importante analisar caso a caso, uma vez que a Lei não especifica critérios para determinar quando se trata do caso de segredo comercial/industrial.

51 Nesse caso, com base no princípio da transparência, a pessoa deverá esclarecer quais critérios utilizou para chegar à decisão.

52 PASQUALE (2016).

53 As primeiras discussões sobre a necessidade de leis para regular o fluxo de dados e garantir direitos sobre o uso destes começaram ainda nos anos 1970, na Europa. Em 1980, a OCDE aprovou as "Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais", que foram atualizadas em 2013. Em 1981 foi aprovada a "Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais", sendo este o primeiro tratado internacional sobre o tema. E em 1995, a União Europeia aprovou a Diretiva de Proteção de Dados. Para um contexto histórico detalhado, ver GREENLEAF (2017b).

54 Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

A GDPR entrou em vigor no dia 25 de maio de 2018, atualizando, harmonizando e adaptando a antiga Diretiva Europeia de Proteção de Dados às mais novas formas de uso massivo de dados pessoais, tais como os modelos de negócio baseados em tecnologias de *big data*, inteligência artificial e aprendizado de máquina. Muito embora a GDPR garanta o direito à explicação e também o de revisão de decisões automatizadas, estes direitos encontram mais restrições no contexto europeu do que no brasileiro – o que pode impactar no livre usufruto de direitos e liberdades fundamentais das pessoas que estão sob a sua jurisdição, como será demonstrado a seguir.

3.1. O direito à explicação e à revisão de decisões automatizadas na GDPR

O direito à informação no contexto de decisões automatizadas encontra respaldo no artigo 13 da GDPR, que determina que devem ser fornecidas ao titular dos dados informações significativas sobre a lógica do processamento automatizado, bem como sobre o significado e as consequências previstas, para o titular dos dados, do processamento.[55] A explicação sobre a lógica envolvida no tratamento dos dados pessoais é, de certa forma, uma explicação sobre o que será feito com tais dados, ou seja, um direito à explicação.

Essa previsão deve ser lida em conjunto com o artigo 22 da Lei, que trata do direito de não estar sujeito a decisões totalmente automatizadas, incluindo os referentes à formação ou uso de perfis comportamentais que produzam efeitos jurídicos relevantes na vida do titular dos dados.[56] Mas esse direito não se aplica quando o procedimento automatizado for necessário para entrar ou executar um contrato. Exemplos incluem o cálculo automatizado do risco de crédito para decisão sobre a concessão ou não de um empréstimo. Também não se aplica quando o processo automatizado se basear no uso de dados pessoais coletados e tratados com o consentimento explícito do titular, como acontece com a maioria dos serviços oferecidos através da Internet, em que os usuários consentem com o tratamento dos seus dados por meio de políticas de privacidade. O artigo ainda diferencia entre direito de oposição, ou o de não se sujeitar às decisões automatizadas, e o de pedir revisão por uma pessoa natural e trata, também, do direito do titular de expressar sua opinião e contestar a decisão automatizada, o que somente é possível quando há informações suficientes para o exercício desses direitos. Como poderia alguém contestar uma decisão se não entende como o sistema que a tomou funcionou?

> Para isso, é necessário o direito à explicação.

Neste contexto, o *considerando*[57] 71 da GDPR afirma que tais direitos incluiriam: (i) o de obter uma explicação referente a decisão tomada; e (ii) o de desafiar essa decisão, vide:

> Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de *obter uma explicação sobre a decisão tomada* na sequência dessa avaliação e de contestar a decisão.[58] (Grifo do autor)

55 Ver artigo 13, (2), (f) da GDPR. A mesma redação é encontrada nos Art. 14(2) (g) e no 15(1) (h). Disponível em: https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=celex%3A32016R0679.

56 Ver artigo 22 da GDPR. Decisões individuais automatizadas, incluindo definição de perfis. Disponível em:https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=celex%3A32016R0679.

57 No direito da União Europeia, um "considerando" é um texto que estabelece as razões para as disposições de um ato, evitando linguagem normativa e argumentação política. Um considerando pode e deve ser tido em conta na interpretação do significado de um acordo contratual. Embora não seja vinculante, fornece a provável intenção do legislador ao positivar a norma. Disponível em: http://publications.europa.eu/code/en/en-120200.htm.

58 GDPR. Considerando 71. Disponível em: https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=celex%3A32016R0679.

Assim, apesar do termo “explicação" não estar previsto no corpo do regulamento, apenas no seu preâmbulo – que não é vinculante – é possível argumentar que há um direito à explicação na GDPR. Ele teria como bases o princípio da transparência e o direito de acesso aos dados, que incluiria o direito a receber explicação sobre a lógica subjacente de decisões totalmente automatizadas com impacto na vida dos indivíduos – principalmente as que incluem perfis comportamentais. Ele é necessário para exercer plenamente outros direitos, como à saúde, educação, liberdade, emprego, entre outros, e visa assegurar um tratamento equitativo e transparente, evitando assim práticas discriminatórias e abusivas.

Essa interpretação tem sido debatida por especialistas, que chegam a conclusões distintas. Na Lei europeia, a existência ou não de um direito à explicação sobre a lógica por trás de decisões automatizadas é o centro da discussão. Os debates opuseram aqueles que, por um lado, argumentavam que a ausência do termo “explicação” no texto da GDPR não permitiria afirmar categoricamente a existência de um direito à explicação.[59] Por outro, estão aqueles que argumentam que tal direito poderia ser inferido a partir dos artigos 13, 14 e 15 da Regulação,[60] pois fazem referência ao dever de fornecer de informações significativas sobre a lógica envolvida na tomada de decisões automatizadas, quando estas impactarem na vida dos titulares dos dados.

A interpretação em prol da existência de tais direitos visa dar sentido à intenção do legislador, como demonstrado através dos *considerandos* da GDPR, e também conforme as necessidades oriundas dos atuais modelos de negócio e tecnologias que cada vez mais têm um impacto direto nas nossas vidas, influenciando-a por meio de decisões controladas por algoritmos opacos e obscuros. Garantir tal direito significa influenciar a forma como sistemas são desenvolvidos para deixá-los mais transparentes e justos.

4. Conclusão

Situações que envolvem questões relacionadas à saúde, educação, segurança, crédito, emprego, redes sociais, informações e até mesmo os rumos de um Estado Democrático de Direito dependem, cada vez mais, do uso massivo de dados pessoais e de processos totalmente automatizados de tomada de decisões que podem ter impactos diretos nas nossas vidas, inclusive nos sujeitando a práticas abusivas e discriminatórias. Para coibir e evitar a violação de tais liberdades e direitos fundamentais, é necessário entender como tais processos decisórios funcionam, o que irá permitir contestá-los; ou pedir que sejam avaliados por pessoas naturais, a fim de que não reproduzam comportamentos enviesados a partir de processamentos inadequados sobre os dados inadequados ou para finalidades ilícitas. Previsões legais, como o direito à explicação e à revisão de decisões automatizadas, que, no Brasil, já constavam, ainda que de modo limitado, em legislação setorial, são importantes para isso. A Lei Geral de Proteção de Dados veio expandir estes e outros direitos.

A LGPD, na forma como foi aprovada, prevê o direito à explicação no caso de decisões totalmente automatizadas que possam ter um impacto na vida do titular dos dados, principalmente no contexto de formação e uso de perfis comportamentais. A explicação deve incluir não somente informações sobre os dados pessoais que serviram de substrato para o algoritmo, mas também sobre a lógica por trás de tais decisões. O direito à explicação também é possível quando houver o tratamento de dados anonimizados, quando esse tipo de dado for utilizado na formação de perfis comportamentais de pessoas identificadas. Em suma, a LGPD garante ao titular dos dados pessoais o direito a:

59 Op. cit. 15.

60 Op. Cit. 13.

i. Ter acesso aos tipos de dados e a quais de seus dados pessoais são utilizados para alimentar algoritmos responsáveis por processos de decisões automatizadas;

ii. Caso o processo automatizado tenha por finalidade formar um perfil comportamental, ou se valha de um perfil comportamental para tomar uma decisão subsequente, o direito de acesso aos dados poderá incluir, também, os dados anonimizados utilizados para enriquecer tais perfis;

iii. Esse direito inclui o de receber explicações sobre os critérios utilizados para tomar a decisão automatizada, observados os segredos comercial e industrial, que deve ser analisado caso-a-caso, uma vez que tais conceitos não encontram subsídio na Lei; e

iv. Caso tais decisões tenham impacto nos interesses dos titulares, o que se presume, no caso de perfis comportamentais, é um direito requisitar que haja revisão por uma pessoa natural, a qual deverá observar o princípio da transparência, devendo deixar claro os critérios utilizados para tomar sua decisão.

Assim como na Lei europeia, o direito à explicação previsto no caso brasileiro pode encontrar algumas limitações, como a manutenção dos segredos industriais dos responsáveis pelo tratamento. Porém, o regulamento europeu impõe mais restrições do que a Lei brasileira, principalmente por não incluir o caso dos dados anonimizados e por limitar o direito de oposição quando a base legal para tratamento dos dados for o consentimento explícito ou a execução de um contrato. Nesse sentido, é bastante positivo que o rol de proteções propostos pela legislação brasileira seja substancialmente mais amplo do que o presente na regulação europeia, que inicialmente lhe serviu de inspiração.

Todavia, definir quais serão os limites das informações que devem ser repassadas para o titular dos dados e quais devem permanecer sob segredo será papel da Autoridade Nacional de Proteção Dados, da doutrina jurídica e da jurisprudência. Este artigo visou pautar o debate ao trazer uma possível interpretação à LGPD, com o claro objetivo de garantir ao cidadão o exercício efetivo de seus direitos e liberdades fundamentais.

Referências

ADAM, D. et al. (2014). "Emotional contagion through social networks". Proceedings of the National Academy of Sciences, vol. 111, nº 24, p. 8788-8790. Disponível em: http://www.pnas.org/content/111/24/8788.full. Acesso em: 20 out. 2018.

ANGWIN, J. et al. (2016). "Machine Bias". ProPublica. Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Acesso em: 28 out 2018.

BRASIL. Lei 13.709 de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da República Federativa do Brasil, 15 ago. 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 20 out 2018.

BRASIL. Lei 12.414 de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Diário Oficial da República Federativa do Brasil, 10 jun. 2011. Disponível em: http://www2.camara.leg.br/legin/fed/lei/2011/lei-12414-9-junho-2011-610758-norma-pl.html. Acesso em: 20 out 2018.

BRASIL. Ministério da Justiça. Portaria nº 5 de 27 de agosto de 2002. Dispõe sobre cláusulas abusivas em contratos de vendas de produtos e prestação de serviços. Diário Oficial da República Federativa do Brasil, Brasília, DF, 28 ago. 2002. Disponível em: https://www.procon.go.gov.br/legislacao/portarias/portaria-n%C2%BA-5-27-08-2002-mj-sde-clausulas-abusivas-nome-de-consumidor-a-banco-de-dados.html. Acesso em: 20 out 2018.

BRASIL. Lei 8.078 de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da República Federativa do Brasil, 12 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em: 20 out. 2018.

BURRELL, J. (2016). "How the machine 'thinks': Understanding opacity in machine learning algorithms". Big Data & Society. Disponível em: http://ssrn.com/abstract=2660674. Acesso em: 20 out 2018.

COELHO, F. U. (2011). *Manual de direito comercial: direito de empresa*. São Paulo: Saraiva.

DANAHER, J. (2016). "Algorithmic decision-making and the problem of opacity". SCL. Disponível em: https://www.scl.org/articles/3713-algorithmic-decision-making-and-the-problem-of-opacity. Acesso em: 20 out 2018.

DIAKOPOULOUS, N.; FRIEDLER, S. (2016). "How to hold algorithms accountable". MIT Technology Review. Disponível em https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/. Acesso em: 20 out 2018.

GREENLEAF, G. (2017a) "European data privacy standards implemented in laws outside Europe". Privacy Laws & Business International Report, vol. 21-23, nº 18-2. Disponível em: https://ssrn.com/abstract=3096314. Acesso em: 20 out 2018.

GREENLEAF, G. (2017b). "Countries with data privacy laws – by year 1973-2016 (Tables)". Privacy Laws & Business International Report, vol. 18. Disponível em: https://ssrn.com/abstract=2996139. Acesso em: 20 out 2018.

INFORMATION COMMISSIONER'S OFFICE (2018). "Democracy disrupted? Personal information and political influence". ICO. Disponível em: https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf. Acesso em: 28 out 2018.

MENDES, L. S. (2014). *Privacidade, proteção de dados e defesa do consumidor*. São Paulo: Saraiva.

MILLER, A. P. (2018). "Want less-biased decisions? Use algorithms". Business Review. Disponível em: https://hbr.org/2018/07/want-less-biased-decisions-use-algorithms. Acesso em: 20 out 2018.

MONTEIRO, R. L. (2017). "Proteção de dados e a legislação vigente no Brasil". Baptista Luz. Disponível em: http://baptistaluz.com.br/wp-content/uploads/2017/11/Privacy-Hub-Leis-Setoriais.pdf. Acesso em: 20 out 2018.

MONTEIRO, R. L. CARVINO, F. I. (2015). "Adaptative learning – o uso de inteligência artificial para adaptar ferramentas de ensino ao aluno". Educação Digital. São Paulo: Revista dos Tribunais.

NISSENBAUM, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Bloomington: Stanford Law Books.

O'NEIL, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. New York: Crown.

PASQUALE, F. (2016). *The blackbox society: The secret algorithms that control money and information.* Cambridge: Harvard University Press.

PORTO, A. J. M. (2009). "O Direito e a economia do cadastro positivo". Conjuntura Jurídica, nº 77, p. 77-80. Disponível em:http://bibliotecadigital.fgv.br/ojs/index.php/rce/article/viewFile/24693/23466. Acesso em: 15 out 2018.

POWLES, J.; HODSON, H. (2017). "Google DeepMind and healthcare in an age of algorithms". Health and Technology, vol. 7, nº 4, p. 351-367. Disponível em: https://link.springer.com/article/10.1007%2Fs12553-017-0179-1. Acesso em: 28 out 2018.

PURAM, K.; SADAGOPAL, G. US Patent 6,289,340 (2001). Consultant matching system and method for selecting candidates from a candidate pool by adjusting skill values. Disponível em: https://patents.google.com/patent/US6289340B1/en. Acesso em: 28 out 2018.

ROLLET, C. (2018). "The odd reality of life under China's all-seeing credit score system". Wired. Disponível em: https://www.wired.co.uk/article/china-social-credit. Acesso em: 10 out 2018.

SASAKI, S. et al. (2010). "Using genetic algorithms to optimise current and future health planning--the example of ambulance locations". International Journal of Health Geographics, vol. 9, nº 4, p. 1-10. Disponível em: https://ij-healthgeographics.biomedcentral.com/articles/10.1186/1476-072X-9-4. Acesso em: 15 out 2018.

SELBST, A. D.; POWLES, J. (2017). "Meaningful information and the right to explanation". International Data Privacy Law, vol. 7, nº 4, p. 233-242. Disponível em: https://ssrn.com/abstract=3039125 Acesso em: 10 out 2018.

SMITH, L. (2016). “Algorithmic transparency: Examining from within and without”. IAPP Privacy Perspectives. Disponível em: https://iapp.org/news/a/algorithmic-transparency-examining-from-within-and-without/. Acesso em: 15 out 2018.

SUPERIOR TRIBUNAL DE JUSTIÇA. (2012). “Teoria do adimplemento substancial limita o exercício de direitos do credor”. Jusbrasil. Disponível em: https://stj.jusbrasil.com.br/noticias/100054780/teoria-do-adimplemento-substancial-limita-o-exercicio-de-direitos-do-credor. Acesso em: 20 out 2018.

UNIÃO EUROPEIA. Parlamento Europeu e Conselho da União Europeia. Regulamento 2016/679 de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Publicações da União Europeia. Disponível em: https://publications.europa.eu/pt/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1. Acesso em: 15 out. 2018.

WACHTER, S.; MITTELSTADT, B.; FLORIDI, L. (2017). “Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation”. International Data Privacy Law. Disponível em: https://ssrn.com/abstract=2903469. Acesso em: 20 out 2018.

Outras publicações do Instituto Igarapé

ARTIGOS ESTRATÉGICOS

ARTIGO ESTRATÉGICO 38 - Na porta de saída, a entrada no trabalho: políticas para a expansão do emprego de presos e egressos no Rio de Janeiro
Dandara Tinoco e Ana Paula Pellegrino
(Novembro 2018)

ARTIGO ESTRATÉGICO 37 - A Internet das Coisas no Brasil: Estado da arte e reflexões críticas ao fenômeno
Eduardo Magrani
(Novembro 2018)

ARTIGO ESTRATÉGICO 36 - La "Mano Dura": Los costos de la represión y los beneficios de la prevención para los jóvenes en América Latina
Adriana Erthal Abdenur
(Maio 2018)

ARTIGO ESTRATÉGICO 35 - Garantindo a paz: O Brasil e o processo de paz com o ELN da Colômbia
Adriana Erthal Abdenur
(Maio 2018)

ARTIGO ESTRATÉGICO 34 - Colômbia e as FARC: Cenários pós-conflito e repercussões regionais
Guilherme Damasceno Fonseca e Christian Vianna de Azevedo
(Maio 2018)

ARTIGO ESTRATÉGICO 33 - Citizen Security in Latin America: Facts and Figures
Robert Muggah e Katherine Aguirre Tobón
(Abril 2018)

ARTIGO ESTRATÉGICO 32 - A agenda sobre mulheres, paz e segurança no contexto latinoamericano: desafios e oportunidades
Renata Avelar Giannini, Ana Paula Pellegrino, Carol Viviana Porto, Luisa Lobato, Maiara Folly e Mariana Gomes da Rocha
(Março 2018)

ARTIGO ESTRATÉGICO 31 - Implementando a agenda sobre "Mulheres, Paz e Segurança" no Brasil: uma revisão do Plano Nacional de Ação
Paula Drumond e Tamya Rebelo
(Março 2018)

ARTIGO ESTRATÉGICO 30 - Gênero, justiça e segurança no Brasil e na Colômbia: como prevenir e tratar da violência contra mulheres?
Renata Avelar Giannini, Orlinda Cláudia Rosa de Moraes e Marcelo Diaz
(Março 2018)

ARTIGO ESTRATÉGICO 29 - Migrantes invisíveis: a crise de deslocamento forçado no Brasil
Maiara Folly
(Março 2018)

ARTIGO ESTRATÉGICO 28 - Salas de Consumo de Drogas: situando o debate no Brasil
Rafael Tobias de Freitas Alloni e Luiz Guilherme Mendes de Paiva
(Outubro 2017)

ARTIGO ESTRATÉGICO 27 - Situações extraordinárias: a entrada de mulheres na linha de frente das Forças Armadas brasileiras
Renata Avelar Giannini, Maiara Folly e Mariana Fonseca Lima
(Agosto 2017)

ARTIGO ESTRATÉGICO 26 - A percepção de crianças e adolescentes sobre a segurança e a violência: a aplicação do Indice de Segurança da Criança em uma escola
Renata Avelar Giannini, Maiara Folly, Monica de Cassia Nehrebeck e Willian Vinícius Silva
(Junho 2017)

ARTIGO ESTRATÉGICO 25 - O Brasil e o Marco Civil da Internet. O Estado da Governança Digital Brasileira
Daniel Arnaudo
(Abril 2017)

ARTIGO ESTRATÉGICO 24 - Confiança em desenvolvimento: o Brasil e os projetos de impacto rápido
Eduarda Hamann, Henrique Garbino e Maiara Folly
(Abril 2017)

ARTIGO ESTRATÉGICO 23 - Controlando el territorio y construyendo seguridad y justicia en el posconflicto colombiano. Edición especial de los Diálogos por la Seguridad Ciudadana
(Dezembro 2016)

ARTIGO ESTRATÉGICO 22 - Durões contra os fracos; fracos frente aos durões: as leis de drogas e a prática da ação policial
Juan Carlos Garzón Vergara
(Outubro 2016)

ARTIGO ESTRATÉGICO 21 - Infância e Segurança: um estudo sobre a percepção da violência por crianças e adolescentes do Complexo do Muquiço, Rio de Janeiro
Renata A. Giannini, Maiara Folly, Victor Ladeira, Andressa Werneck e Renata Siqueira
(Julho 2016)

ARTIGO ESTRATÉGICO 20 - Making Cities Safer: Citizen Security Innovations from Latin America
Robert Muggah, Ilona Szabo de Carvalho, Nathalie Alvarado, Lina Marmolejo e Ruddy Wang
(Junho 2016)

ARTIGO ESTRATÉGICO 19 - Construindo Planos Nacionais de Ação eficazes: coletânea de boas práticas
Renata A. Giannini
(Março 2016)

ARTIGO ESTRATÉGICO 18 - “When Kids Call the Shots” Children’s perceptions on violence in Recife, Brazil, as per the ‘Child Security Index’
Helen Moestue, Katherine Aguirre e Renata A. Giannini
(Dezembro 2015)

ARTIGO ESTRATÉGICO 17 - Where is Latin America? Reflections on Peace, Security, Justice and Governance in the Post-2015 Sustainable Development Agenda
Renata A. Giannini
(Outubro 2015)

ARTIGO ESTRATÉGICO 16 - Políticas de Drogas no Brasil: A Mudança já Começou
Ilona Szabó de Carvalho e Ana Paula Pellegrino
(Março 2015)

ARTIGO ESTRATÉGICO 15 - Nuevos retos y nuevas concepciones de la seguridad en México
Edición especial de los Diálogos por la Seguridad Ciudadana
(Março 2015)

ARTIGO ESTRATÉGICO 14 - A 'Third Umpire' for Policing in South Africa – Applying Body Cameras in the Western Cape
David Bruce e Sean Tait
(Março 2015)

ARTIGO ESTRATÉGICO 13 - Brazil and Haiti: Reflections on 10 Years of Peacekeeping and the Future of Post-2016 Cooperation
Eduarda Passarelli Hamann (org.)
(Janeiro 2015)

ARTIGO ESTRATÉGICO 12 - Measurement Matters: Designing New Metrics for a Drug Policy that Works
Robert Muggah, Katherine Aguirre e Ilona Szabó de Carvalho
(Janeiro 2015)

ARTIGO ESTRATÉGICO 11- Desconstruindo a segurança cibernética no Brasil: ameaças e respostas
Gustavo Diniz, Robert Muggah e Misha Glenny
(Dezembro de 2014)

ARTIGO ESTRATÉGICO 10 - Expansão Digital: como as novas tecnologias podem prevenir a violência contra crianças nos países do hemisfério sul
Helen Mostue e Robert Muggah
(Novembro 2014)

ARTIGO ESTRATÉGICO 9 - Promover Gênero e Consolidar a Paz: A Experiência Brasileira
Renata A. Giannini
(Setembro 2014)

ARTIGO ESTRATÉGICO 8 - Tornando as Cidades Brasileiras mais Seguras: Edição Especial dos Diálogos de Segurança Cidadã
Michele dos Ramos, Robert Muggah, José Luiz Ratton, Clarissa Galvão, Michelle Fernandez, Claudio Beato, Andréa Maria Silveira, Melina Ingrid Risso e Robson Rodrigues.
(Julho 2014)

ARTIGO ESTRATÉGICO 7 - Changes in the Neighborhood: Reviewing Citizen Security Cooperation in Latin America
Robert Muggah e Ilona Szabó de Carvalho
(Março 2014)

ARTIGO ESTRATÉGICO 6 - Prevenindo a violência na América Latina por meio de novas tecnologias
Robert Muggah e Gustavo Diniz
(Janeiro 2014)

ARTIGO ESTRATÉGICO 5 - Protegendo as Fronteiras: o Brasil e sua estratégia "América do Sul como prioridade" contra o crime organizado transnacional
Robert Muggah e Gustavo Diniz
(Outubro 2013)

ARTIGO ESTRATÉGICO 4 - To Save Succeeding Generations: UN Security Council Reform and the Protection of Civilians
Conor Foley
(Agosto 2013)

ARTIGO ESTRATÉGICO 3 - Momento Oportuno: Revisão da Capacidade Brasileira para Desdobrar Especialistas Civis em Missões Internacionais
Eduarda Passarelli Hamann
(Janeiro 2013)

ARTIGO ESTRATÉGICO 2 - A Fine Balance: Mapping Cyber (in)security in LatinAmerica
Gustavo Diniz e Robert Muggah
(Junho 2012)

ARTIGO ESTRATÉGICO 1- Mecanismos Nacionais de Recrutamento, Preparo e Emprego de Especialistas Civis em Missões Internacionais
Eduarda Passarelli Hamann
(Maio 2012)

NOTAS ESTRATÉGICAS

NOTA ESTRATÉGICA 30 - Uma Estratégia para a Governança da Segurança Cibernética no Brasil
Louise Marie Hurel e Luisa Cruz Lobato
(Setembro 2018)

NOTA ESTRATÉGICA 29 - Will Cuba Update its Drug Policy for the Twenty First Century?
Isabella Bellezza-Smull
(Dezembro 2017)

NOTA ESTRATÉGICA 28 - Desafios e Boas práticas para Implementação da Agenda sobre Mulheres, Paz e Segurança
Renata Avelar Giannini e Maiara Folly
(Novembro 2017)

NOTA ESTRATÉGICA 27 - À Margem do Perigo: preparo de civis brasileiros para atuação em países instáveis
Eduarda Passarelli Hamann
(Junho 2017)

NOTA ESTRATÉGICA 26 - Haitian Women's Experiences of Recovery from Hurricane Matthew
Athena Kolbe, Marie Puccio, Sophonie M. Joseph, Robert Muggah e Alison Joersz
(Junho 2017)

NOTA ESTRATÉGICA 25 - The Future of United Nations Peacekeeping Operations from a Brazilian Perspective (implementing the HIPPO report)
Eduarda Hamann and Adriana Erthal Abdenur
(Março 2017)

NOTA ESTRATÉGICA 24 - Em Busca da Igualdade de Gênero: boas práticas para a implementação da agenda sobre mulheres, paz e segurança
Maiara Folly e Renata Avelar Giannini
(Março 2017)

NOTA ESTRATÉGICA 23 - Filling the accountability gap: principles and practices for implementing body cameras for law enforcement
Robert Muggah, Emile Badran, Bruno Siqueira e Justin Kosslyn
(Novembro 2016)

NOTA ESTRATÉGICA 22 - Latin American Dialogue on International Peace and Security
Reviewing the prospects for peace operations, peacebuilding and women, peace and security
(Maio 2016)

NOTA ESTRATÉGICA 21 - Assessing Haiti's Electoral Legitimacy Crisis – Results of a 2016 Survey
Athena R. Kolbe e Robert Muggah
(Fevereiro 2016)

NOTA ESTRATÉGICA 20 - Impact of Perceived Electoral Fraud on Haitian Voter's Beliefs about Democracy
Athena R. Kolbe, Nicole I. Cesnales, Marie N. Puccio e Robert Muggah
(Novembro 2015)

NOTA ESTRATÉGICA 19 - A Força de uma Trajetória: O Brasil e as operações de paz da ONU (1948-2015)
Eduarda Passarelli Hamann
(Outubro 2015)

NOTA ESTRATÉGICA 18 - Implementing UNSC Resolution 1325 in Brazil: surmounting challenges and promoting equality
Renata A. Giannini, Mariana Lima e Pérola Pereira
(Outubro 2015)

NOTA ESTRATÉGICA 17 - A Reforma do Conselho de Segurança da ONU: visão de mundo e narrativas do Brasil
Eduarda Passarelli Hamann
(Maio 2015)

NOTA ESTRATÉGICA 16 - Break Your Bones: mortality and morbidity associated with Haiti's Chikungunya epidemic
Athena R. Kolbe, Augusta Herman e Robert Muggah (Julho 2014)

NOTA ESTRATÉGICA 15 - New Technologies for Improving Old Public Security Challenges in Nairobi
Mads Frilander, Jamie Lundine, David Kutalek e Luchetu Likaka
(Junho 2014)

NOTA ESTRATÉGICA 14 - O Despertar da América Latina: uma revisão do novo debate sobre politica de drogas
Ilona Szabó de Carvalho
(Fevereiro 2014)

NOTA ESTRATÉGICA 13 - The Changing Face of Technology Use in Pacified Communities
Graham Denyer Willis, Robert Muggah, Justin Kossyln e Felipe Leusin
(Fevereiro 2014)

NOTA ESTRATÉGICA 12 - A Inserção de Civis Brasileiros no Sistema ONU: oportunidades e desafios
Renata Avelar Giannini
(Janeiro 2014)

NOTA ESTRATÉGICA 11 - A Diáspora Criminal: o alastramento transnacional do crime organizado e as medidas para conter sua expansão
Juan Carlos Garzón Vergara
(Novembro 2013)

NOTA ESTRATÉGICA 10 - Smarter Policing: tracking the influence of new information technology in Rio de Janeiro
Graham Denyer Willis, Robert Muggah, Justin Kosslyn e Felipe Leusin
(Novembro 2013)

NOTA ESTRATÉGICA 9 - Is Tourism Haiti's Magic Bullet? An Empirical Treatment of Haiti's Tourism Potential
Athena R. Kolbe, Keely Brookes and Robert Muggah (Junho 2013)

NOTA ESTRATÉGICA 8 - Violencia, Drogas y Armas ¿Otro Futuro Posible?
Ilona Szabó de Carvalho, Juan Carlos Garzón e Robert Muggah
(Julho 2013)

NOTA ESTRATÉGICA 7 - A Promoção Da Paz No Contexto Pós-2015: o papel das potências emergentes
Robert Muggah, Ivan Campbell, Eduarda Hamann, Gustavo Diniz e Marina Motta
(Fevereiro 2013)

NOTA ESTRATÉGICA 6 - After the Storm: Haiti's coming food crisis
Athena Kolbe, Marie Puccio e Robert Muggah
(Dezembro 2012)

NOTA ESTRATÉGICA 5 - Brazil's Experience in Unstable Settings
Eduarda Passarelli Hamann e Iara Costa Leite
(Novembro 2012)

NOTA ESTRATÉGICA 4 - Cooperação Técnica Brasileira
Iara Costa Leite e Eduarda Passarelli Hamann
(Setembro 2012)

NOTA ESTRATÉGICA 3 - A Experiência do Brasil em Contextos Instáveis
Eduarda Passarelli Hamann e Iara Costa Leite
(Agosto 2012)

NOTA ESTRATÉGICA 2 - The Economic Costs of Violent Crime in Urban Haiti (Aug 2011 - Jul 2012)
Athena R. Kolbe, Robert Muggah e Marie N. Puccio
(Agosto 2012)

NOTA ESTRATÉGICA 1 - Haiti's Urban Crime Wave? Results from Monthly Households Surveys
(Aug 2011 - Feb 2012)
Athena R. Kolbe e Robert Muggah
(Março 2012)

INSTITUTO IGARAPÉ
a think and do tank

O Instituto Igarapé é um think and do tank independente, dedicado às agendas da segurança, da justiça e do desenvolvimento. Seu objetivo é propor soluções inovadoras a desafios sociais complexos, por meio de pesquisas, novas tecnologias, influência em políticas públicas e articulação. O Instituto atualmente trabalha com cinco macrotemas: (i) política sobre drogas nacional e global; (ii) segurança cidadã; (iii) cidades seguras; (iv) consolidação da paz; e (v) segurança cibernética. O Instituto Igarapé tem sede no Rio de Janeiro, com representação em Bogotá, Cidade do México, Lisboa e outras partes do mundo.

Instituto Igarapé
Rio de Janeiro – RJ – Brasil - 22281-000
Tel/Fax: +55 (21) 3496-2114
contato@igarape.org.br
facebook.com/institutoigarape
twitter.com/igarape_org

www.igarape.org.br

Direção de arte: Raphael Durão - http://storm.pt

ISSN 2359-098X

INSTITUTO IGARAPÉ

a think and do tank

Rio de Janeiro – RJ – Brasil - 22281-000
Tel/Fax: +55 (21) 3496-2114
contato@igarape.org.br
facebook.com/institutoigarape
twitter.com/igarape_org

www.igarape.org.br