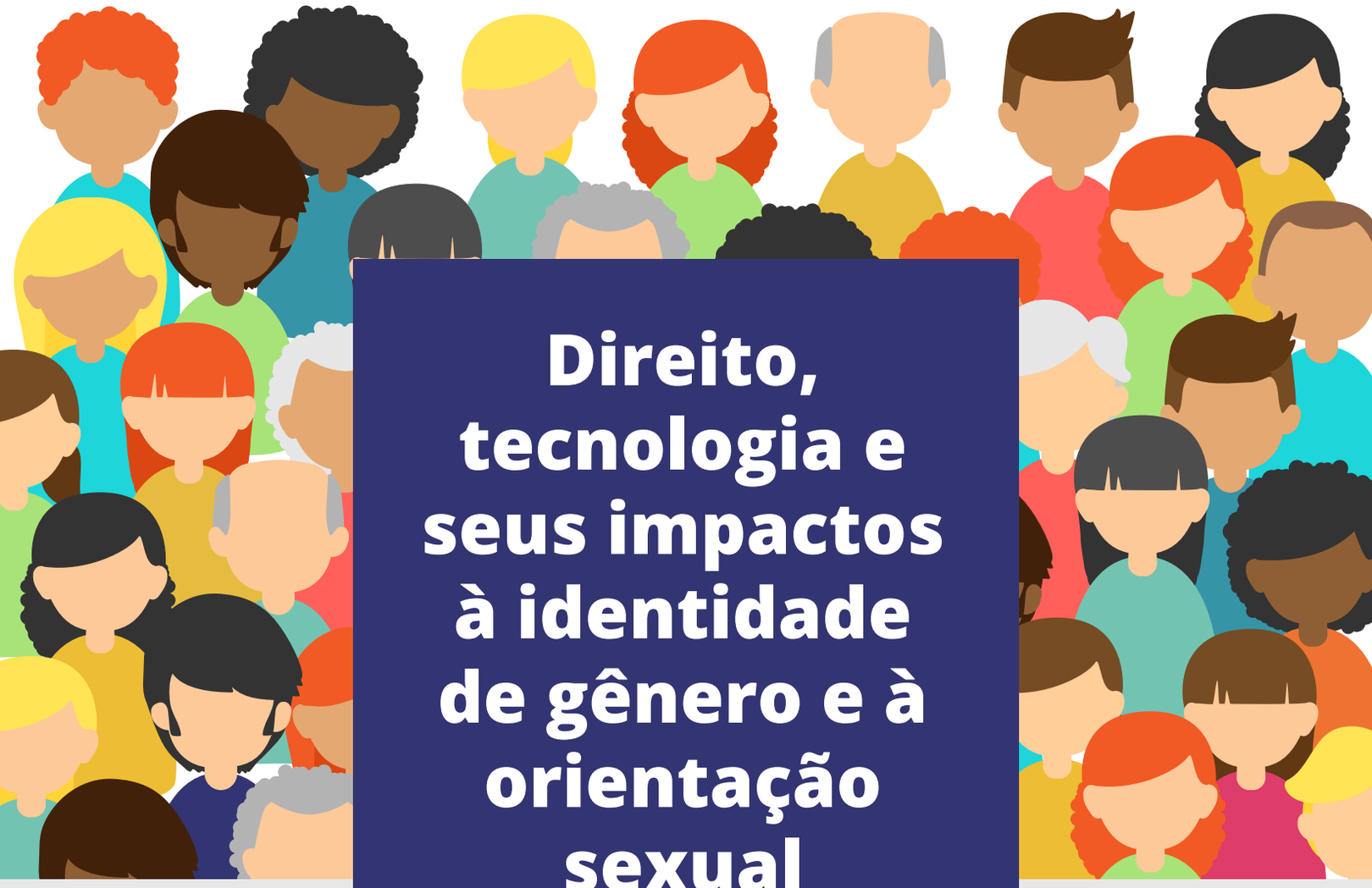
OPICE BLUM

25 anos

OPICE BLUM | BRUNO | VAINZOF



Direito, tecnologia e seus impactos à identidade de gênero e à orientação sexual

E-BOOK 2022

WWW.OPICEBLUM.COM.BR

Introdução

O Dia Internacional do Orgulho LGBTQIA+, que acontece em 28 de junho, remete ao episódio ocorrido no bar *Stonewall Inn*, em Nova Iorque, em 1969. Além da defesa dos direitos dessa comunidade, é importante pensarmos em respeito à diversidade e às minorias, seja por questões de gênero, étnicas, raciais ou religiosas.

Atualmente, muito se tem ouvido falar em práticas ESG (*environmental*, *social* e *governance*). O G dessa sigla tem, entre os destaques, a diversidade. Nós do Opice Blum, Bruno e Vainzof Advogados possuímos o **Comitê de Inclusão e Diversidade**, vinculado ao *squad* de RH, criado no primeiro semestre de 2020.

A partir da percepção de que temos avanços a buscar e de que contamos, cada vez mais, com um time plural, um dos objetivos do comitê é incentivar a formação de diferentes grupos de afinidades, bem como promover encontros mensais com discussões que provoquem reflexões e impacto dentro e fora do escritório.

É por isso que, no mês da diversidade, elaboramos uma série de artigos sobre a relação das questões LGBTQIA+ com a privacidade e a proteção de dados. Entre os destaques, temos: identidade de gênero e orientação sexual como dados sensíveis; cuidados com os dados em aplicativos de relacionamento; ações afirmativas e proteção de dados; moderação de conteúdo nas redes sociais; e importância de práticas ESG no mercado.

Boa leitura!

Índice

01 Identidade de gênero e orientação sexual como dados pessoais sensíveis
por Bernardo de Souza Dantas Fico, Guilherme Hernandez Sicuto e Henrique Meng Nóbrega

02 Vazamento de dados de aplicativos de relacionamento: risco aos usuários e vulnerabilidades da população LGBTQIA+
por Bernardo de Souza Dantas Fico e Nina Ramalho Pinheiro

03 Proteção de dados e ação afirmativa: base legal aplicável segundo a LGPD
por Bernardo de Souza Dantas Fico e Henrique Meng Nóbrega

04 A importância da moderação de conteúdo nas redes sociais: uma análise da LGBTfobia na Era Musk
por Tatiana Brenand Bauer Poli e Rebeca Bacci Martins Trigo

05 *Oversight Board*: Combater ou ocultar a violência digital contra a comunidade LGBTQIA+
por Anna Sambo Budahazi e Felipe Passos Bresciani

06 ESG – A importância do quesito social na inclusão da comunidade LGBTQI+
por Tatiana Brenand Bauer Poli e Rebeca Bacci Martins Trigo

01

Identidade de gênero e orientação sexual como dados pessoais sensíveis

Quando discutimos corpos, gênero e sexualidade, adjetivar certas pessoas como “normais” e outras como “desviantes” estratifica como esses indivíduos são vistos em nossa sociedade. Se "normal" significa cisgênero e heterossexual, a comunidade LGBTQIA+ (lésbica, gay, bissexual, transgênero, *queer*, inter-sexual, assexual e outras) é facilmente marginalizada e punida por não se conformar. As identidades LGBTQIA+ são globalmente **rejeitadas por meio de discriminação, inferiorização e criminalização**.

por Bernardo de Souza Dantas Fico, Guilherme Hernandez Sicuto e Henrique Meng Nóbrega

Atualização por Henrique Meng Nóbrega e adaptação por Bernardo de Souza Dantas Fico com base no artigo original em inglês publicado em co-autoria por Bernardo de Souza Dantas Fico, Guilherme Hernandez Sicuto, e Henrique Meng Nóbrega pela *International Association of Privacy Professionals* (IAPP) sob título “*Does Brazil’s LGPD recognize gender identity, sexual orientation as sensitive personal data?*“. Disponível em:

https://iapp.org/news/a/does-brazils-lgpd-recognize-gender-identity-and-sexual-orientation-as-sensitive-personal-data/

Nesse cenário, a lei é uma das formas de moldar a realidade e de proteger os mais vulneráveis, devendo ser essa proteção uma maneira de **"ser igual quando a nossa diferença nos inferioriza"** e **"ser diferente quando a nossa igualdade nos descaracteriza"**. Em um mundo progressivamente interconectado, o debate sobre identidade de gênero e orientação sexual como dados pessoais sensíveis é um passo inicial essencial que nem todos os países deram.

O reconhecimento dessas informações como dados sensíveis ajudaria a evitar o tratamento desses dados para fins ilícitos ou abusivos. Com a recente Emenda Constitucional nº 115/2022, a qual reconheceu a proteção de dados como um direito fundamental, esse debate ganha nova envergadura no Brasil. Apesar de adotarmos a lei brasileira como pano de fundo para essa discussão, questões nacionais são semelhantes às de outros países que não reconhecem explicitamente a "identidade de gênero" e a "orientação sexual" como dados pessoais sensíveis.

Orientação sexual como Dado Pessoal Sensível

A orientação sexual deve ser considerada como dado sensível nos termos do artigo 5, II, da Lei Geral de Proteção de Dados (LGPD). Ao identificar quais informações são sensíveis, a legislação se limita aos dados "referentes à vida sexual", mas, na verdade, não define esse termo. Assim, uma interpretação à luz dos direitos humanos poderia concluir que "vida sexual" compreende "orientação sexual", particularmente considerando o princípio da não-discriminação.

Normas e jurisprudências internacionais tendem a apoiar essa interpretação. Por exemplo, o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia reconhece tanto "dados relativos à vida sexual de uma pessoa física" quanto "orientação sexual" como dados pessoais sensíveis, utilizando esses conceitos em situações comparáveis nas Considerandas 71 e 75. Da mesma forma, **a Corte Interamericana de Direitos Humanos** usou o termo "vida sexual" ao julgar seu primeiro caso sobre direitos LGBTQIA+. Posteriormente, substituiu o termo por "orientação sexual" em suas decisões mais recentes, incluindo **Duke v. Colômbia** (2016), **Flor Freire v. Equador** (2016), **Parecer Consultivo 24** (2017), **Azul Rojas Marín v. Peru** (2020), e **Pavez Pavez v. Chile** (2021). Outros instrumentos internacionais, incluindo a **Convenção 108 do Conselho da Europa**, o **Relatório de Discriminação SOGIESC da OIT** e os **Princípios de Yogyakarta** +10, apoiam uma interpretação da LGPD inclusiva à população LGBQA+ (lésbica, homossexual, bissexual, queer, assexual e outros). Dessa forma, o uso de “vida sexual” é reflexo de uma linguagem atrasada, mas compatível com a interpretação de que esse conceito inclui “orientação sexual”.

Ainda que uma interpretação mais literal e conservadora pudesse argumentar que "vida sexual" significa apenas os aspectos centrais de como os indivíduos experimentam o sexo em si, essa interpretação conflitaria frontalmente com as orientações recentes da Autoridade Nacional de Proteção de Dados (ANPD). O **Guia Orientativo** para aplicação da LGPD por agentes de tratamento no contexto eleitoral, elaborado pela ANPD em conjunto com o Tribunal Superior Eleitoral (TSE), apresenta evidência adicional do sentido interpretativo do conceito de “vida sexual” ao listar explicitamente “orientação sexual” entre os exemplos de dados pessoais sensíveis, vejamos:

> “ 14. A LGPD determinou que os dados sensíveis sejam tratados com maior cautela, observadas regras mais restritivas do que aquelas que se aplicam a outros dados pessoais. A lei presumiu que a utilização indevida dessas informações tem o potencial de gerar restrições significativas ao exercício de direitos fundamentais, como atos de discriminação racial, étnica ou em razão de **orientação sexual** [...] ”

Identidade de gênero como Dado Pessoal Sensível

Apesar de não estar explicitamente listada na LGPD, bem como não estar presente na ampla maioria das normas de proteção de dados, a identidade de gênero deve ser considerada como dado pessoal sensível. A ausência desse termo nas leis de proteção de dados pode potencialmente comprometer a proteção de uma parcela considerável da população LGBTQIA+, mas não deve ser causa para que se conclua imediatamente por sua não inclusão na categoria de dados pessoais sensíveis. Não se discute aqui se a identidade de gênero deve ser abrangida pelo conceito de "vida sexual", pois esse argumento implicaria em debater a essência dos conceitos de gênero e sexualidade.

Há um debate contínuo sobre o caráter aberto ou fechado da lista de dados sensíveis da LGPD. Se a lista for aberta, não vemos nenhum motivo razoável para não incluir a identidade de gênero como dado pessoal sensível, considerando seu potencial discriminatório; por outro lado, se a lista for fechada, ela excluiria a possibilidade de simples inclusão da identidade de gênero como dado sensível.

Contudo, sem necessidade de mencionar esse debate, é possível estabelecer a proteção da identidade de gênero como dado sensível, pois, segundo a jurisprudência do Supremo Tribunal Federal (STF), a "discriminação por identidade de gênero" se enquadra dentro do conceito de discriminação racial. Logicamente, então, o termo "identidade de gênero" deve se enquadrar dentro da ideia de raça. Segundo a LGPD, "raça" é considerada como dado pessoal sensível. Portanto, segundo a decisão do STF, "identidade de gênero" é englobada sob o conceito de dados pessoais sensíveis.

Em março de 2004, o STF decidiu o habeas corpus 82.424/RS, quando a maioria dos juízes determinou que o conceito de "raça" não é simplesmente biológico e isolado; em vez disso, ele deriva de uma construção social e antropológica. O STF considerou, ainda, que o termo descrito como “raça” não possui bases biológicas, observando que o racismo reflete um comportamento decorrente de uma convicção discriminatória de que alguns grupos humanos são hierarquicamente superiores a outros, o que já foi utilizado para segregar, inferiorizar e exterminar pessoas.

Em junho de 2019, o STF reiterou sua posição na ADO 26 (Ação Direta de Inconstitucionalidade por Omissão) e no MI 4.733 (Mandado de Injunção) ao decidir se a discriminação com base na orientação sexual e na identidade de gênero poderia ser considerada racismo. O STF manteve sua interpretação anterior de que "raça" é um conceito de significado plural, englobando aspectos socioculturais. Nessa oportunidade, o STF reconheceu explicitamente tanto a discriminação por orientação sexual quanto a discriminação por identidade de gênero como racismo conforme as definições da Lei Anti-Racismo. Um dos ministros observou que a Lei Anti-Racismo busca impedir a discriminação inferiorizante, definida no conceito de racismo, mas que não se isola numa perspectiva biológica.

Segundo o STF, raça é mais do que aspectos biológicos rigorosos e o fenótipo das pessoas, sendo uma manifestação de poder. Assim, se o racismo engloba a discriminação baseada na identidade de gênero, "raça" também inclui o conceito de identidade de gênero. O mesmo argumento se aplica à orientação sexual.

Conclusão

Não pretendemos esgotar os argumentos sobre a relação entre direitos LGBTQIA+, não-discriminação e a proteção de dados, mas fomentar mais o debate sobre o assunto. Mesmo assim, podemos tirar algumas conclusões a partir dessa temática.

A LGPD deve ser abordada sob a perspectiva dos direitos humanos, protegendo as comunidades vulneráveis, como a população LGBTQIA+. Já a interpretação de uma lei de proteção de dados conforme o reconhecimento da diversidade permite aos países restringir o tratamento discriminatório ou abusivo de dados contra grupos minoritários.

Ainda, a orientação sexual deve ser considerada como dado pessoal sensível segundo a LGPD, porque a "vida sexual" engloba a "orientação sexual". Dessa forma, a identidade de gênero deve ser considerada como dado pessoal sensível de acordo com a jurisprudência do Supremo Tribunal Federal, que define "racismo" e "raça" como elementos que englobam a discriminação por identidade de gênero e a identidade de gênero, respectivamente. Por fim, a conclusão anterior se aplica plenamente à orientação sexual.

Esse debate tem aspectos inexplorados e muito espaço para crescer, sendo esperado que a interpretação das leis de proteção de dados e suas consequências sobre a não-discriminação amadureçam, enquanto grupos minoritários buscam o reconhecimento de sua proteção sob essas leis. Dessa forma, a comunidade jurídica deve manter esses debates em andamento para avançar as proteções necessárias àqueles que a necessitam.

02

Vazamento de dados de aplicativos de relacionamento: risco aos usuários e vulnerabilidades da população LGBTQIA+

Independentemente de ser usuário ou não, todo mundo já ouviu falar em aplicativos de relacionamento. Com popularidade já expressiva desde o início dos anos **2000**, os relacionamentos iniciados por meios digitais ganharam tração nos últimos anos e foram especialmente impulsionados pela pandemia, quando essas plataformas alcançaram, em 2021, **323 milhões de usuários**. Os brasileiros estão entre os que mais gastam tempo em **aplicativos de relacionamento**, além de o Brasil ser o segundo país **mais representado**, com cerca de **18 milhões de usuários**.

por Bernardo de Souza Dantas Fico e Nina Ramalho Pinheiro

Tipos de dados coletados nos apps de relacionamento

Nos aplicativos, o modelo de negócio (mecanismo utilizado para obtenção de lucro) aproxima as plataformas, pois funciona sob a lógica do "capitalismo de vigilância", ordem econômica construída pelo fornecimento de serviços predominantemente gratuitos em troca de dados pessoais. Em teoria, o tratamento dessas informações é feito para estudar, propor, construir e comercializar modelos preditivos de comportamento, os quais viabilizam ganhos financeiros dos *apps*.

A quantidade e a natureza dos dados pessoais utilizados pelas plataformas variam, mas, como regra geral, há coleta de alguns tipos de dados, como cadastrais, de localização, identificador do usuário na plataforma, identificador do dispositivo utilizado, histórico de compras, histórico de conteúdo (ex. áudio, fotos/vídeos, mensagens etc.), histórico de uso (ex. interação com produtos, dados de publicidade etc.), entre outros. Além destes, inúmeros aplicativos ainda coletam dados sensíveis, como informações de etnia, raça, orientação sexual, opinião política, dados biométricos e dados de saúde.

Conforme estabelece a Lei Geral de Proteção de Dados (**Lei nº 13.709/2018**), os dados pessoais e os dados pessoais sensíveis se diferenciam, entre outros fatores, pelas justificativas para seu tratamento.

No caso dos dados pessoais sensíveis, as hipóteses que autorizam seu uso são mais restritas e demandam atenção redobrada quando eles são utilizados como parte de um negócio. Esse cuidado é, particularmente, importante nos aplicativos de relacionamento, uma vez que a monetização da atividade envolve a criação de perfis de usuários utilizando dados de caráter bastante íntimo.

A existência de justificativas legítimas para que o usuário deseje comunicar informações classificadas como sensíveis para potenciais pares românticos não importa na presunção de que esses dados possam ser amplamente divulgados. A dualidade entre exposição legítima para potenciais pares e privacidade em relação aos demais é difícil de balancear, o que possibilita a concretização de diferentes ameaças digitais quando não realizada adequadamente pelos **aplicativos**.

Exposição de dados e riscos relativos a vulnerabilidades técnicas e não-técnicas

Frente à crescente divulgação das ameaças digitais, é natural que os usuários se questionem qual o nível de segurança dessas plataformas.

Em pesquisa da **Kaspersky Lab**, identificou-se como negativo à experiência dos usuários a existência de perfis falsos (53%), preocupações com o compartilhamento de informações pessoais (26%) e contatos realizados por golpistas (21%). Atualmente, 55% dos usuários desses *apps* reportam alguma ameaça ou problema durante o namoro *on-line*, além de terem duas vezes mais chances de serem atingidos por um incidente de segurança.

Sem a necessidade de conhecimentos técnicos, é possível acessar informações básicas a respeito de cada usuário. O nível de exposição varia de acordo com as escolhas de cada um ao divulgar informações que podem levar, com maior ou menor facilidade, à identificação do usuário fora do ambiente *on-line*. São exemplos disso a indicação do local de trabalho, *links* para redes sociais, nome completo, entre outros dados. Adicionalmente, todos os aplicativos de relacionamento permitem algum conhecimento da localização dos outros usuários, o que representa um de seus maiores atrativos: conhecer *on-line* pessoas que estejam próximas.

Da perspectiva técnica, a não atualização de segurança cibernética é uma das maiores causas de vulnerabilidades e, consequentemente, de incidentes envolvendo vazamento de dados. Apenas em 2021, **2,8 bilhões** de dados sensíveis foram expostos no Brasil, tendo cerca de **24,2 milhões** de perfis de brasileiros que tiveram suas informações expostas publicamente em razão de ataques cibernéticos ou vulnerabilidades sistêmicas.

No caso da perda de controle sobre informações de um usuário, o risco de roubo de senhas é prevalente. A repetição de senhas (ou uso de alterações mínimas) pode permitir que um único problema de segurança se alastre para diversas contas do usuário. Com os dados vazados, é possível também criar uma *persona*, seja com uso de imagens, seja com uso de informações pessoais verdadeiras para dar credibilidade ao perfil falso (*fake*).

A riqueza das informações vazadas também pode viabilizar a prática de engenharia social, técnica por meio da qual um agente mal-intencionado se utiliza de meios para enganar uma pessoa emprestando-se de uma suposta autoridade, fama, ou outra característica arrogadora de credibilidade. Usualmente, essa prática é associada ao conhecimento prévio de informações da pessoa, não raramente obtidas em razão de vazamento de dados.

Vulnerabilidades particulares às pessoas LGBTQIA+

Se da perspectiva da população em geral os incidentes de segurança da informação e demais ameaças digitais são preocupantes, isso se agrava quando falamos de populações vulneráveis. Particularmente em relação às pessoas LGBTQIA+, três consequências principais merecem atenção:

Uso de informações fruto de incidentes para perseguição a indivíduos

Exposição de orientação sexual e/ou identidade de gênero de maneira indesejada, ou a ameaça em fazê-lo

Persecuções penais em cerca de 1/3 (um terço) dos países no mundo

Ao vazar informações pessoais de pessoas LGBTQIA+, plataformas de relacionamento podem viabilizar a perseguição a esses indivíduos. Dada a prevalência da coleta de dados de localização nesses aplicativos, há a possibilidade de esses usuários terem locais chave de sua convivência diária identificados, incluindo casa, trabalho, casa de parentes e amigos, locais de lazer, entre outros. Ainda, é possível que usuários mal-intencionados no aplicativo desvirtuem a finalidade da plataforma, passando a utilizá-la para marcar encontros com o intuito de cometer atos de **violência contra pessoas LGBTQIA+**.

Não suficiente, considerando o frequente tratamento pelas plataformas de informações como gênero, orientação sexual, práticas sexuais, fotos enviadas e/ou recebidas associadas a comentários, filtros de identificação, entre outras, a exposição pública dos dados pode também causar um *outing* não planejado. Ou seja, ao expor informações na internet, é possível que indivíduos que não se identificassem abertamente como LGBTQIA+ sejam relacionados a informações que os identifiquem dessa forma.

Caso a informação vazada não seja amplamente divulgada, abre-se então a possibilidade de chantagem desses usuários, em uma dinâmica na qual o chantageado é ameaçado com a publicidade indesejada de seus dados vazados.

Ainda que esses sejam casos preocupantes, há riscos ainda maiores para os LGBTQIA+ nos 67 países onde suas **identidades são criminalizadas**. A simples associação de uma pessoa com uma *tag* relativa à sexualidade e/ou à identificação de gênero não normativa pode causar constrangimentos sancionados pelo Estado. Em alguns casos, há a possibilidade, inclusive, de morte. O uso dos aplicativos pelo Estado para rastrear e prender pessoas LGBTQIA+ foi observado em países como **Egito, Líbano e Irã, Rússia e África do Sul**.

Conclusão

Em que pese alguns aplicativos já tenham implementado medidas de segurança específicas objetivando a maior proteção de seus usuários LGBTQIA+, como a ocultação automática de localização e/ou do próprio perfil do usuário quando ele entra em regiões que possuem leis discriminatórias, medidas adicionais ainda se fazem necessárias.

Por esse motivo, com o intuito meramente de despertar o interesse na reflexão do tema, sendo muitas vezes necessário assumir a responsabilidade por sua própria proteção e segurança em ambientes *on-line*, é pertinente entender o que envolve a utilização de cada aplicativo, permitindo, assim, a tomada de decisões mais conscientes quanto à disponibilização ou não de suas informações pessoais.

Em termos de prevenção, os usuários podem utilizar-se de algumas opções para mitigar riscos existentes, como:

i- evitar a associação entre perfis nos aplicativos de relacionamento com perfis em outras redes sociais;

ii- utilizar senhas diferentes em cada aplicativo, ativando quando possível a autenticação em dois fatores;

iii- verificar nos termos de uso do aplicativo se existem medidas técnicas para proteção dos usuários, e com quem seus dados podem ser compartilhados;

iv- evitar compartilhar informações pessoais publicamente no perfil, como sobrenome, local de trabalho, endereço residencial etc;

v- evitar a seleção automática da localização;

vi- evitar acessar *links* fornecidos por outros usuários; e

vii- atentar-se a informações divulgadas pelas próprias plataformas em relação à ocorrência de incidentes de vazamento, ou de fatos relevantes na região em que o usuário utiliza a plataforma, usualmente noticiados pelos aplicativas por meio de *e-mails*, *pop-ups*, *banners* e outras formas de comunicação com usuários em massa.

O cuidado com a segurança da informação nos aplicativos de relacionamento não só permite a troca mais transparente entre pessoas (que estão seguras quanto à não divulgação posterior de determinadas informações), como evita inúmeros golpes e riscos aos quais as populações em situações vulneráveis, como pessoas LGBTQIA+, estão mais expostas.

03

Proteção de dados e ação afirmativa: base legal aplicável segundo a LGPD

No Brasil, semelhante à tradição jurídica de outros países ocidentais, o princípio da igualdade passou por etapas subsequentes em termos de reconhecimento, conteúdo e constituição de direitos. Em particular, a Constituição Federal de 1988 elevou a igualdade a um objetivo fundamental da República (artigo 3º, II e IV) e promoveu a diferenciação positiva com o objetivo de catalisar sua eficácia material. Por exemplo, o artigo 7, XX, da CF, estabeleceu a "proteção do mercado de trabalho da mulher, mediante incentivos específicos". Em seu artigo 37, VIII, a Carta Magna também reservou um percentual de empregos e cargos públicos para pessoas com deficiência.

por Bernardo de Souza Dantas Fico e Henrique Meng Nóbrega

Tradução por Bernardo de Souza Dantas Fico do artigo originalmente publicado em inglês em co-autoria por Bernardo de Souza Dantas Fico e Henrique Meng Nóbrega pela *International Association of Privacy Professionals* (IAPP) sob título "*Data privacy and affirmative action: What is the applicable legal basis under LGPD?*". Disponível em:

https://iapp.org/news/a/data-privacy-and-affirmative-action-what-is-the-applicable-legal-basis-under-the-lgpd

Exemplos adicionais de ações afirmativas podem ser encontrados na legislação federal brasileira e nas leis estaduais. Por exemplo, o artigo 1º da Lei Federal nº 12.711/2012, conhecida como "Lei de Cotas", prevê que parte das vagas de estudantes das universidades federais deve ser reservada para aqueles com renda familiar média igual ou inferior a 1,5 salários-mínimos. Além disso, o Estatuto da Igualdade Racial (Lei Federal nº 12.288/2010) estabelece no artigo 4º, II, que a "participação da população negra, em condição de igualdade de oportunidade, na vida econômica, social, política e cultural" do Brasil será promovida por meio da "adoção de medidas, programas e políticas de ação afirmativa".

Seja no setor público seja no privado, o emprego dessas ações afirmativas implica o processamento de dados pessoais. Assim, tendo em vista a Lei Geral de Proteção de Dados (LGPD), que base legal pode autorizar as ações afirmativas? Existe alguma hipótese que permita o uso de dados sensíveis em sua execução?

Ações afirmativas no setor privado

Não desconsiderando o cumprimento de outras exigências da LGPD, quando entidades privadas processam dados pessoais para implementar ações afirmativas, devem fazê-lo observando os artigos 7 ou 11 da LGPD, de acordo com as categorias de dados pessoais envolvidos.

Em um cenário no qual atores privados implementam ações afirmativas tratando apenas de dados pessoais "simples", o artigo 7º, IX, da LGPD, ou seja, interesse legítimo, aplica-se sem maiores controvérsias. Isso porque, apesar de certo grau de subjetividade em relação à definição de "interesse legítimo", as atividades que promovem igualdade e não-discriminação naturalmente se enquadram no "interesse legítimo" por duas razões principais.

Primeiro, as ações afirmativas de atores privados promovem objetivos republicanos fundamentais de acordo com os artigos 3, II e IV, da CF, e garantem os direitos fundamentais e as liberdades civis das pessoas em questão que têm suas informações processadas. Ainda, a própria LGPD enumera a não-discriminação como um de seus princípios (artigo 6, IX).

Por sua vez, para os atores privados que implementam ações afirmativas que lidam com dados sensíveis, outras bases legais devem ser analisadas. De um lado, a finalidade de uma ação afirmativa pode seguir determinação legal (lei federal, estadual ou municipal) ou regulamentar (decretos ou resoluções, entre outros). Se esse for o caso, aplica-se o artigo 11, II, a, da LGPD (cumprimento da obrigação legal ou regulatória). Isso é o que acontece, por exemplo, quando empresas processam dados de saúde, de acordo com o artigo 93 da Lei Federal nº 8.213/91, para reservar posições a pessoas com deficiências.

Alternativamente, suponha que não haja lei ou regulamentação que obrigue as empresas a implementarem ações afirmativas.

Nesse caso, ainda se pode argumentar que a base legal aplicável é "o cumprimento de uma obrigação legal ou regulamentar por parte do controlador". A promoção ativa da igualdade material é uma obrigação imposta pela Constituição Federal de 1988 a todas as pessoas físicas e jurídicas no Brasil, conforme explicado pela Ministra Carmen Lúcia Antunes Rocha:

> " [...] todos os verbos utilizados na expressão normativa – construir, erradicar, reduzir, promover – são de ação, vale dizer, designam um comportamento ativo. O que se tem, pois, é que os objetivos fundamentais da República Federativa do Brasil são definidos em termos de obrigações transformadoras do quadro social e político retratado pelo constituinte quando da elaboração do texto constitucional. "
>
> **ROCHA, Carmen Lúcia Antunes**

Independentemente de um comando detalhado consagrado na legislação, os atores privados podem, com base em um dever positivo de promover a igualdade, processar informações pessoais sensíveis para obter sucesso em suas ações afirmativas.

Os argumentos apresentados, baseados na legislação brasileira, poderiam ser replicados em países que também adotam o "interesse legítimo" e o "cumprimento de uma obrigação legal ou regulamentar por parte do controlador" como bases legais para o processamento, respectivamente, de dados pessoais "simples" e dados pessoais sensíveis. Esse é o caso, por exemplo, das **Ilhas Cayman**, **Macau**, **Marrocos**, **Quênia** e **Rússia**, assim como Alemanha, Espanha, França, Portugal, Reino Unido e outros **países sob o Regulamento Geral de Proteção de Dados da UE**, que tem semelhanças com a LGPD brasileira.

Ações afirmativas no setor público

Ao considerar as particularidades do setor público, a LGPD estabeleceu regras adicionais e específicas para o processamento de dados pessoais nesse contexto. Assim, seu artigo 23 determina que esse processamento deve ser realizado para atender à "sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público".

Dadas essas exigências adicionais, não há consenso sobre quais bases legais podem autorizar o tratamento de dados pessoais pelas autoridades públicas. Enquanto alguns consideram o artigo 23 da LGPD uma base legal autônoma, essa hipótese de tratamento já estaria englobada pelas bases legais listadas nos artigos 7 ou 11 da legislação. Em particular, uma vez que os artigos 7 e 11 têm uma lista fechada de bases legais, parece haver poucos argumentos para uma base legal autônoma consagrada em outro dispositivo.

Ações afirmativas de atores públicos tomam a forma de política pública e podem utilizar dados pessoais "simples" ou dados pessoais sensíveis. Em ambos os casos, essas políticas podem ser baseadas em duas bases legais, dependendo do caso em questão: cumprimento de uma obrigação legal ou regulamentar (artigos 7, II, e 11, II, a), ou execução de políticas públicas (artigos 7, III, e 11, II, b). Entretanto, isso implica a necessidade de que as ações afirmativas no setor público sejam detalhadas em seu escopo, uma vez que, apesar do comando geral de promoção ativa da igualdade material, qualquer ação afirmativa no setor público também deve obedecer aos princípios da administração pública, incluindo a legalidade (artigo 37, CF).

Conclusão

Ações afirmativas são possíveis nos setores público e privado e encontram justificativa na legislação de proteção de dados. No entanto, apesar das bases legais que autorizam essas ações afirmativas, existe o risco de não cumprimento dos direitos civis e das liberdades fundamentais das pessoas envolvidas. O tipo de dados processados pode levar à discriminação se cair em mãos erradas, ou mesmo se indivíduos bem-intencionados processarem as informações sem levar em conta os princípios de proteção de dados. Portanto, é prudente considerar a aplicação das melhores práticas de proteção de dados nesses casos.

Embora não seja uma exigência legal sob a LGPD, pode-se produzir uma avaliação de legítimo interesse ao processar informações sob um interesse legítimo (artigo 7, IX). Essa avaliação verificará se os interesses perseguidos, nesse caso, uma ação afirmativa, são legítimos e se eles criam desequilíbrios em detrimento dos titulares afetados pelo tratamento. Modelos e diretrizes para a avaliação de legítimo interesse foram disponibilizados pelas autoridades de proteção de dados, **incluindo o Escritório do Comissário de Informação do Reino Unido** (do inglês, ICO).

Para ações afirmativas que processam dados pessoais sensíveis, por outro lado, a produção de uma avaliação de legítimo interesse não é uma alternativa. Isso porque essas avaliações estão vinculadas a um interesse legítimo que não pode ser utilizado para justificar o processamento de informações sensíveis sob a LGPD.

O movimento adequado nesses casos é produzir um relatório de impacto de proteção de dados, conforme previsto no artigo 38 da LGPD (documentos semelhantes também podem ser denominados avaliação de impacto sobre a privacidade). A Autoridade Nacional de Proteção de Dados (ANPD) brasileira publicou **modelo** que os controladores de dados podem utilizar. Autoridades europeias, como o **Grupo de Trabalho de Proteção de Dados** (conhecido por sua denominação em inglês, *Data Protection Working Party*) e a **Agência Espanhola de Proteção de Dados** emitiram guias práticos sobre o assunto.

Esse relatório permite identificar e avaliar os riscos de processamento e projetar medidas para mitigá-los. Finalmente, medidas adequadas de segurança técnica e administrativa devem ser implementadas, de preferência de acordo com as melhores práticas nacionais e internacionais relativas à proteção de dados e à segurança da informação.

04

A importância da moderação de conteúdo nas redes sociais: uma análise da LGBTfobia na Era Musk

A declaração de Elon Musk, um dos homens mais ricos do mundo, a respeito da sua intenção de comprar o *Twitter* com o objetivo, entre outros, de reforçar a **liberdade de expressão absoluta**, suscitou debates sobre o uso da plataforma e a sua atuação no combate às mensagens consideradas prejudiciais.

O *Twitter* realiza moderação das postagens feitas por usuários ao possibilitar denúncias por promoção de ódio, conteúdo de desinformação, a exemplo de posts sobre a pandemia da Covid-19, valendo-se de moderadores para revisar conteúdos postados e contas denunciadas.

por Tatiana Brenand Bauer Poli e Rebeca Bacci Martins Trigo

Nesse contexto, também há a iniciativa da comunidade *BirdWatch*, grupo de moderadores, cujo objetivo é combater a desinformação, conforme consta no *Social Media Safety Index*, elaborado pela ***Gay & Lesbian Alliance Agains Defamation - GLAAD***, e nas políticas da própria rede social.

Assim, considerando que grupos minoritários costumam sofrer mais com ataques postados em redes sociais, a preocupação surge para a população LGBTQIA+, na medida em que esse grupo se destaca no centro dos ataques nos Estados Unidos, como mostra o referido levantamento feito em 2021 pela GLAAD. Os ataques consistem em postagens com linguajar ofensivo ou com o intuito de ridicularizar um grupo ou indivíduo, palavras de ódio, incitação à violência, entre outras ações.

Se o debate sobre liberdade de expressão já se mostrava relevante, após a intenção de compra do *Twitter* por Elon Musk, a atenção merece ser redobrada. No ordenamento jurídico brasileiro, a liberdade de expressão é direito fundamental previsto na Constituição Federal, sendo regulada em tratados internacionais, dos quais o Brasil é signatário, que vedam a "**apologia ao ódio nacional, racial ou religioso que constitua incitamento à discriminação, à hostilidade ou à violência**". A relativização da liberdade de expressão ganha espaço quando o discurso do indivíduo atinge negativamente a esfera individual de uma pessoa ou ultrapassa outro direito fundamental, como a igualdade ou a não discriminação.

Com isso, é possível identificar o que constitui o discurso de ódio e o impacto negativo que sua disseminação pode causar a pessoas pertencentes a minorias sociais. A exemplo do Brasil, que há 13 anos é o **país que mais mata trans e travestis no mundo**, e dos Estados Unidos, com uma taxa de 64% do discurso de ódio *on-line* em razão de **orientação sexual** e de homicídios contra mulheres transsexuais e pessoas não binárias. Nesse cenário, é imprescindível observar essas questões e promover políticas de mitigação e vias de minimizar a proliferação do ódio por meio das redes sociais. Isso porque a sociedade é refletida no ciberespaço e a violência verbal pode se transformar em **violência física**, taxas de **homicídio e de suicídio**.

Outro debate surge quando se trata de controlar conteúdos no ambiente *on-line*: a responsabilidade das plataformas de mídias sociais e dos Estados de controlar o conteúdo divulgado virtualmente. Apesar de estar ainda em discussão, a moderação de conteúdo tem ganhado espaço na medida em que plataformas regulam seu uso por meio de termos de uso e políticas internas voltadas aos usuários. No caso do *Twitter*, a rede conta com política de proibição de conteúdo de ódio e outra de conduta sobre **esse tipo de conteúdo**, o que inclui denúncia de usuários, revisão por parte da equipe e penalidades, como remoção da publicação.

Em contrapartida, é necessário cuidado, pois a autorregulação das plataformas pode colocar em risco a liberdade de expressão, ao garantir o poder de deliberar o que vai ser ou não discutido. Por isso, muitas opções são debatidas, como a autorregulação agindo em conjunto com a atuação estatal, principalmente para o discurso de ódio, além de ***sandbox* regulatórios**.

O atual receio é de que a postura de proatividade do *Twitter* contra esse tipo de conteúdo seja alterada caso haja a compra da rede social. Assim, algumas entidades, como a *Human Rights Watch* e a **Anistia Internacional**, apontaram a preocupação com a mudança na liderança da plataforma devido à responsabilidade do *Twitter* com a garantia de respeito aos direitos humanos dos usuários e o impacto que mudanças nas políticas internas poderiam causar, haja vista a atuação mundial do *app*.

Contudo, mesmo que a compra se concretize, já se sabe que Musk não poderá exercer o que defende em suas falas. Recentemente, a União Europeia aprovou o ***Digital Service Act***, legislação que garantirá consequências às plataformas que hospedam conteúdos proibidos, incluindo o **discurso de ódio**. Logo, o *Twitter* deverá estar adequado às medidas legislativas para atuar na Europa, o que pode dar início à regulação estatal em outros países.

Portanto, espera-se que esse tipo de ação não coloque em risco os direitos de seus usuários e medidas levantadas por entidades para auxiliar o combate à LGBTfobia sejam consideradas, como:

- Proibir linguagem que desumaniza o outro;
- Manter o refinamento do algoritmo para identificar discursos de ódio;
- Promover medidas de inclusão e capacitação de profissionais LGBTQIA+; e
- Qualificar moderadores humanos para interpretar conteúdos com termos da comunidade, a fim de evitar bloqueios e remoções indevidas.

05

Oversight Board: Combater ou ocultar a violência digital contra a comunidade LGBTQIA+

A proteção da boa convivência na internet é uma das principais pautas atualmente. A exemplo do que ocorre na sociedade, ao estabelecer regras de relacionamento entre indivíduos para evitar ou solucionar conflitos, canais de comunicação, em especial as redes sociais, também estão sujeitos a estritas regras de uso voltadas ao mesmo objetivo: proteger indivíduos que utilizam ambientes virtuais e incentivar a navegação **livre** e **pacífica**. Para efetivar essas normas e concretizar esses objetivos, a Meta, antigo Facebook, instituiu o *Oversight Board* ou Conselho de Supervisão.

por Anna Sambo Budahazi e Felipe Passos Bresciani

É inquestionável que, no contexto da convivência *on-line*, valoriza-se o direito de expressão e de manifestação do pensamento com ampla liberdade. As ferramentas de comunicação fornecidas pela rede potencializaram a propagação da voz dos usuários, que tornam públicos seus posicionamentos sobre qualquer assunto. Entretanto, justamente por ser uma extensão virtual da vida social, as problemáticas envolvendo esses direitos são reproduzidas e ampliadas em igual medida com o uso das redes. Para isso, é importante entender como o *Board* pretende lidar com essas questões com o intuito de solucionar conflitos e de fixar a boa convivência no ambiente digital.

O que é e o que faz o *Oversight Board* da Meta?

O *Oversight Board* é um órgão externo, que, por isso, não cria ou altera as políticas de uso das redes sociais da Meta. Ele é responsável por receber reclamações dos usuários que discordarem das restrições impostas pelas plataformas sobre determinada publicação, devido ao descumprimento das regras de uso da rede. A partir das decisões emanadas pelo Conselho, a Meta moldará suas políticas, com base no aperfeiçoamento indicado pelo *Board*, para melhorar a convivência virtual.

O *Board* já analisou 33 casos selecionados e iniciou a avaliação de 7 novas solicitações. Todos esses cenários são caracterizados pelo elevado grau de complexidade que a Meta, por si só, não solucionou, estando, entre eles, os mais polêmicos temas, incluindo o discurso de ódio e os direitos da comunidade LGBTQIA+.

Protestos contra o Presidente da Colômbia, Ivan Duque

Em 2021, circulou no Facebook um vídeo do protesto político e pacífico em que cidadãos colombianos utilizam-se, entre outros insultos, do termo "marica" traduzido livre e equivalentemente ao termo "bicha", para criticar o presidente da Colômbia, Ivan Duque. Em razão do termo, em análise inicial, o Facebook decidiu pela remoção do conteúdo por constituir discurso odioso e discriminatório contra a comunidade LGBTQIA+.

Inconformado, o jornalista-usuário que realizou a publicação decidiu recorrer ao Conselho para uma segunda fiscalização. Nesse caso, a delicada discussão submetida ao *Board* foi o intenso embate entre, de um lado, a liberdade de expressão em circunstâncias de interesse público e, de outro, a veiculação de um termo reconhecidamente ofensivo a homens homossexuais.

Ao decidir sobre o caso, o Conselho, em consonância com o Facebook, declarou veementemente que o uso do termo "marica" é insultuoso, uma vez que possui origem homofóbica, e seu uso, de todo o modo, pode continuar a marginalizar indivíduos da comunidade LGBTQIA+, associando-os a características negativas, como "estúpido" ou "fraco".

O **Conselho anulou a decisão que removeu o conteúdo**, considerando que existe um interesse público de expressão no caso e que o protesto estava voltado a uma crítica ao governo do presidente, não possuindo objetivo discriminatório, embora tenha deliberadamente veiculado um termo homofóbico.

Por ser um momento histórico-político importante da Colômbia, o *Board* entendeu que os danos à característica protegida pelo Facebook (a orientação sexual) não seriam tão intensos comparada à restrição da liberdade de expressão do protesto, na medida em que a publicação ou o seu compartilhamento não teria fim discriminatório, mas político, de apoio à filosofia da manifestação. A sugestão do *Board* foi de apenas notificar a violação e explicitar que a manutenção do conteúdo é excepcional, sustentada em interesse público.

Isso significa que o *Board* lida "com as questões mais difíceis sobre a liberdade de expressão". Nesse caso, o que se debate é a polêmica infindável sobre se a decisão de manter o conteúdo realmente equilibra a proteção aos direitos LGBTQIA+ e à liberdade de expressão. O uso desses termos deveria ser restringido ao máximo para, no futuro, serem excluídos de nosso vocabulário? O *Board* entendeu que não, prezando por uma análise mais contextual e que valorize a voz dada pelas redes aos protestos políticos.

Movimentações relevantes do *Oversight Board*

O caso acima apresentado é a primeira decisão do Board envolvendo direitos LGBTQIA+. Sua atuação, até o momento, entretanto, não se restringe a ela, em razão de diversos ativistas e vítimas terem acompanhado os andamentos com ampla criticidade e expectativa.

Em 2021, o **Conselho decidiu restringir** as contas do ex-presidente americano Donald Trump devido a postagens que criaram "ambiente que fomentou um risco grave de possíveis atos de violência". A decisão teve como principal aspecto a tutela do ambiente cibernético, principalmente devido à relevância **política de Trump** e os posicionamentos ofensivos à comunidade LGBTQIA+ que ele havia feito.

Neste ano, o *Board* deparou-se com novo caso envolvendo direitos LGBTQIA+. Dessa vez, uma conta com discussão de questões *queer* realizou postagem sobre palavras com carga depreciativa em árabe. A publicação tinha o objetivo "evidenciar o poder de termos nocivos" e condenar o uso deles, dado os danos causados à comunidade.

Horas após a publicação, uma série de denúncias foram realizadas e a **Meta decidiu pela remoção do conteúdo**. O *Board* optou por receber recomendações sobre o assunto, abrindo a questão para comentários públicos.

A intenção foi de captar a posição de especialistas e da comunidade, bem como de solicitar suporte desses agentes para a tomada de decisão final. A complexidade desse caso está na discussão de que, apesar de a publicação trazer termos nocivos e insultuosos, pode não existir caráter discriminatório. Pelo contrário, o publicador parece informar os efeitos do uso das palavras, o que demanda sua veiculação. O *Board*, em sua atuação, deve considerar o contexto da expressão? Ou somente prezar pelo respeito às normas? O caso ainda está pendente de decisão.

Ambos os casos demonstram a tendência do *Board* de endereçar as temáticas de violência nas redes sociais e garantia de direitos LGBTQIA+, mediante recursos internos e externos à sua atuação, buscando compreender o contexto e o histórico de cada caso.

Violência Digital e a atuação do *Oversight Board*

O **Board** tem atribuído significado e razão ao combate das novas formas de violência, no caso, digitais, que até o momento foram pouco analisadas pelo Direito. Conforme a ***Social Media Index report***, da GLAAD (*Gay & Lesbian Alliance Against Defamation*), publicado em maio de 2021, as plataformas de redes sociais possuem recursos para abrandarem assédio, intimidação, desinformação e discriminação. Mesmo reconhecendo esse potencial, as redes utilizam-se da segurança e da privacidade, muitas vezes, como propaganda ou mera teoria e, na prática, aplicam poucos esforços para protegerem os indivíduos contra abusos. Essa mesma pesquisa demonstra que as principais plataformas - Facebook, Instagram e *Twitter* - são consideradas pouco seguras para direitos LGBTQIA+.

Na era contemporânea, a violência passou a ser o cotidiano dos ambientes virtuais, nos quais usuários muito postam e pouco ponderam sobre as consequências de suas manifestações. Diferentemente do que fariam presencialmente, diversos indivíduos entendem as redes sociais como um lugar destacado da realidade, sem regulação relevante. Consequentemente, é insustentável garantir cega e irrestritamente a liberdade de expressão, sem assegurar medidas de freio e de contrapeso para preservar demais liberdades.

É nesse sentido que as redes sociais precisam garantir a proporcionalidade dos direitos que asseguram e protegem, priorizando a criação de ambientes acolhedores, principalmente ao envolver minorias. Na mesma medida em que as redes promovem um espaço para a liberdade de expressão, devem igualmente cuidar para tutelar os indivíduos dos espinhos decorrentes do exercício desse direito. Em outras palavras, as próprias redes serão protagonistas para regular a vida social *on-line*.

Em 2018, o Google recebeu **2,4 milhões** de pedidos de remoção imediata de conteúdo, e o Youtube removeu 58 milhões de vídeos e **224 milhões de conteúdos**. As redes sociais têm se encaminhado para autorregular seus ambientes e, ao que tudo indica, a Meta está caminhando nesse sentido por meio do *Board*.

A própria criação e efetivação dessa plataforma é um ponto positivo para a *Big Tech*, justamente por ser a instrumentalização da solução de polêmicas relacionadas à liberdade de expressão, considerando e ponderando os direitos e as liberdades envolvidas, os aspectos relevantes, como contexto político e social da publicação, e solicitando apoio de especialistas sobre como abordar o tema. Esses fatores demonstram o esforço do *Board* em controlar e não tolerar a violência digital.

É importante notar, porém, que o *Board* precisa amadurecer. Primeiramente, é preciso tomar cuidado ao estabelecer critérios na restrição da liberdade de expressão, para evitar a abertura de precedentes perigosos ou abusar da discricionariedade do *Board*. O Conselho tem avaliado temas que envolvem modulação da regra das políticas, com base no contexto em que se inserem, e isso deverá ser parametrizado, claramente estabelecido, divulgado e transparente, para evitar qualquer tipo de censura ou regulação indiscriminada entre postagens.

Essa necessidade é facilmente resolvível, demandando-se organização e consistência do *Board* para consolidar seus entendimentos, o que virá com a continuidade de sua atuação. Assim, os seus próximos andamentos são aguardados com anseio e otimismo, compreendendo seu desejo de fomentar um ambiente digital seguro, com restrições justificadas e proporcionais. Espera-se que essa seja a tônica, já que sua atuação é fundamental para a segurança, consolidando uma autorregulação criadora de tendências e influenciadora no Direito.

06

ESG – A importância do quesito social na inclusão da comunidade LGBTQI+

Amplamente discutida, a sigla ESG advém dos termos em inglês *Environmental, Social and Governance* – ou, em português, Ambiental, Social e Governança (ASG) – e diz respeito às melhores práticas adotadas no ambiente corporativo e aos seus reflexos nas empresas.

O quesito social evidencia que níveis de inovação, criatividade e desempenho de uma empresa crescem quando implementadas diversidade e inclusão, uma vez que a multiplicidade de indivíduos no meio corporativo fomenta resultados positivos.

por Tatiana Brenand Bauer Poli e Rebeca Bacci Martins Trigo

Nesse sentido, um **estudo da consultoria McKinsey**, realizado em 2020, revelou que empresas com maior nível de diversidade de gênero têm 25% mais vantagem financeira sobre outras, e a porcentagem se eleva para 36% quando se trata de diversidade étnica e racial.

Como é destacado nas diretrizes de grandes empresas, como **Nubank**, a maioria das discussões desse quesito trata sobre relacionamento com a comunidade, satisfação dos clientes, proteção de dados e privacidade, engajamento dos funcionários, diversidade da equipe e garantia dos direitos humanos e trabalhistas, e erra quem acredita que é necessário escolher entre as melhores práticas sociais e a obtenção de bons resultados financeiros.

O impacto da adoção do índice ESG não ocorre apenas em melhores práticas de gestão, mas resulta no fato de que a lente da comunidade LGBTQIA+ é considerada no quesito Social da sigla, o que agrega ao critério de sustentabilidade para investimentos. As consequências positivas, como aumento da lucratividade e do valor de mercado da empresa, apontam resultados melhores para as companhias e demonstram, assim, o impacto econômico decorrente da necessidade de garantir os direitos desses grupos no ambiente corporativo.

Entre as medidas citadas, quando se adota a perspectiva de inclusão da comunidade LGBTQIA+, empresários têm mais visibilidade quanto à mitigação dos riscos de exclusão social e discriminação, além dos benefícios de agregar maior diversidade ao ambiente corporativo, o que é um requisito mínimo para se ter uma sociedade plural.

Diante disso, uma **pesquisa do banco Credit Suisse** sobre os índices ESG, publicada em 2016, demonstrou que empresas com líderes LGBTQIA+ e que possuem gestão aberta à diversidade e funcionários integrantes desse grupo superaram em 3% as ações globais em um período de seis anos.

Além disso, em 2019 foi lançado pela LGBTQ *Loyalty Holdings*, empresa do ramo financeiro e de meios de comunicação, o **LGBT100 ESG Index**, que inclui dados das 100 empresas, entre as 500 maiores companhias abertas americanas, que mais investem em igualdade e que apresentam medidas a favor da comunidade LGBTQIA+. Por se tratar de índice ESG, contempla as 100 empresas mais empenhadas e aquelas que estão se tornando populares por adotarem essas práticas, considerando que novas companhias podem fazer parte do *ranking* de avaliação, desde que entrem com nota máxima de 100 pontos.

A classificação das empresas que fazem parte do Universo LGBTQ Index (LIU) vem do cruzamento de dados do mercado de capitalização com o resultado atribuído, inicialmente, por pesquisa promovida por entidade de direitos humanos reconhecida e baseada em três pilares:

i- políticas de não discriminação;

ii- benefícios para colaboradores LGBTQIA+ e suas famílias; e

iii- apoio à cultura inclusiva e de responsabilidade social no âmbito corporativo.

Desse resultado, é feito o ***ranking* das empresas** que atingiram a pontuação máxima citada acima.

Com o objetivo de proporcionar maior inclusão no âmbito corporativo e para auxiliar as empresas no aspecto prático, o curso de Mestre da Diversidade e Inclusão (MDI), da Pearson, **empresa especializada em educação corporativa**, aborda dicas de boas práticas inclusivas, que são: (i) implementação de política de seleção às cegas, o que elimina truques de vieses inconscientes de raça, idade e gênero; (ii) acesso à informação, implantação de política de tolerância zero a atitudes homofóbicas na empresa e comprometimento com a causa LGBTQIA+ por meio da assinatura de tratados com instituições nacionais e internacionais; (iii) benefícios iguais para toda comunidade, como reconhecimento da relação homoafetiva, licença à maternidade e paternidade, assistência médica; e (iv) permissão da empresa para uso do nome social e de preferência do colaborador.

Ainda, é necessário priorizar o cumprimento dos princípios constitucionais da igualdade e da dignidade da pessoa humana, segundo os quais todos devem ser tratados de forma igualitária, sem discriminação por orientação sexual ou qualquer outro critério que gere segregação. Dessa forma, o entendimento da Carta Magna pode ser expandido por meio de práticas sociais que tenham por consequência a inserção de grupos minoritários que são apartados da sociedade para garantir essa equidade.

Esse fato pode ser observado a partir de estudos realizados por consultorias internacionais, como ***Amundi Asset Management***, segundo os quais empresas que adotaram melhores práticas ambientais, sociais e de governança tiveram impactos positivos em suas atividades, levando às consequências já expostas. Como grande exemplo, cita-se **Michele Bettencourt**, mulher transexual, nomeada, em 2020, presidente do Conselho de Administração da Corelight, empresa do ramo tecnológico, além de estar entre o conjunto de empresários, investidores e executivos LGBTQIA+ que utilizam da posição e dos recursos para apoiar medidas inclusivas.

Casos e pesquisas como os citados comprovam maior pertencimento da comunidade LGBTQIA+ a partir de investimento das próprias empresas e de resultados cada vez mais promissores nos campos social e econômico. Espera-se a conscientização das empresas a fim de garantir maior oportunidade e inserção desse grupo social, marcado historicamente pela repressão de sua própria identidade e pelo estigma construído pela sociedade.

***Artigo publicado originariamente no Estadão em 28 de junho de 2021.**

Créditos

Sócios

José Roberto Opice Blum
Renato Opice Blum
Marcos Gomes da Silva Bruno
Rony Vainzof
Camilla Jimene
Caio César Carvalho Lima
Danielle Serafino
Juliano Souza de A. Maranhão
Ricardo Campos
Henrique Fabretti Moraes

Coordenação Editorial

Yasmin Brandão

Revisão

Rony Vainzof
Caio César Carvalho Lima
Juliano Souza de A. Maranhão
Yasmin Brandão

Conteúdo Jurídico

Anna Sambo Budahazi
Bernardo de Souza Dantas Fico
Felipe Passos Bresciani
Nina Ramalho Pinheiro
Rebeca Bacci Martins Trigo
Tatiana Brenand Bauer Poli
Guilherme Hernandez Sicuto
Henrique Meng Nóbrega

Direção de arte

Paola Melhem Cosentino

OPICE BLUM
25 anos
OPICE BLUM | BRUNO | VAINZOF