

## Grizzi e Silva: O caráter transdisciplinar do ESG

O tema do momento é ESG (*environmental, social and governance*, ou ambiental, social e governança). Essa sigla surgiu pela primeira vez no relatório "*Who Cares Wins — Connecting Financial Markets to a Changing World*", do Departamento Suíço de Assuntos Exteriores, em parceria com a Organização das Nações Unidas (ONU), em dezembro de 2004, e culminou na edição dos "*Principles for Responsible Investment*" (PRI) em 2008 [1] [2], o qual determinou o conceito de investimento responsável (ou



A preocupação com meio ambiente, responsabilidade social e

com melhores práticas de governança está (ou deve estar) na pauta de todas as empresas, de todos os tamanhos e de todos os segmentos de mercado.

Mas por que ESG deve ser uma preocupação? Porque, de acordo com um estudo do Boston Consulting Group (BCG) [3], "*companies that outperform in industry-relevant environmental, social, and governance (ESG) areas boast higher valuation multiples and margins, all other factors being equal, than those with weaker performance in those areas*". Ou seja, empresas que adotam práticas de ESG tendem a render maiores lucros e a aumentar seu valor de mercado.

A verdade é que a sociedade e, conseqüentemente, o mercado passaram a exigir das empresas uma postura ativa, no sentido de que elas passem a prestar mais atenção no impacto social que imprimem e, com isso, insiram esse aspecto nas suas análises de risco e estratégias corporativas. Trata-se do *Total Social Impact* (TSI), que corresponde ao benefício total para a sociedade dos produtos, serviços, operações, capacidades essenciais e atividades de uma determinada empresa.

O TSI é o agregado de todas as maneiras pelas quais uma empresa impacta a sociedade — e atualmente nenhuma métrica única capta isso, como apurou o estudo do BCG em 2017. No entanto, o desempenho em áreas ESG importantes é um bom ponto de partida para entender o TSI de uma empresa —, fornecendo uma maneira concreta de avaliar a ligação entre o TSI de uma empresa e seu desempenho financeiro. Partindo dessa premissa, apresentaremos uma das áreas mais importantes que impacta diretamente no S e no G do ESG, especialmente na realidade brasileira: a proteção de dados.

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018, ou LGPD), para além de estabelecer o regramento aplicável às operações de tratamento de dados pessoais — o que, por si só, já é fundamental para a imagem da empresa e, portanto, impacta no ESG

---

—, dispõe de um capítulo específico para tratar de medidas de segurança e boas práticas (Capítulo VII da LGPD), as quais incluem segurança e sigilo de dados (Seção I, artigo 46 e seguintes da LGPD) e boas práticas e governança (Seção II, artigos 50 e seguintes da LGPD).

Nesse contexto, no esforço de criar uma cultura de privacidade e proteção de dados, a empresa deverá adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (cf. artigo 46 da LGPD), bem como formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais [4].

Trata-se, em verdade, das práticas de *privacy by design*, que consistem em aplicar os conceitos e princípios da proteção de dados desde a criação de uma tecnologia, de modo que esses estejam intrinsicamente integrados à sua funcionalidade, e de *privacy by default*, que exige que os controladores implementem medidas apropriadas, tanto em nível técnico quanto organizacional, para garantir que as tecnologias funcionem, natural e automaticamente, de forma a processar apenas o mínimo de dados pessoais necessário para cumprir seu propósito específico.

Esses modelos de desenvolvimento visam a evitar o processamento excessivo e auxiliar o controle sobre o armazenamento e a acessibilidade dos dados. Com isso, os dados deverão ser gerenciados como ativos organizacionais, de forma que não sejam mais vistos como itens colaterais de sistemas e processos; quer dizer, a forma como determinada empresa maneja dados pessoais no contexto do seu business passou a ser um fator crítico, especialmente diante do crescimento exponencial de tecnologias como *big data*, *IoT* e *machine learning*, bem como em face dos novos parâmetros de governança estabelecidos não apenas pela LGPD, mas também por outras regulamentações específicas em vigor no Brasil, como a Resolução nº 4.658/2018 do Banco Central. Nesse sentido, as empresas deverão passar a se preocupar com a qualidade dos dados pessoais que tratam, os aspectos legais que envolvem o tratamento de dados, a ética do tratamento e o potencial de geração de valor dos bancos de dados que possui [5].

Percebe-se, então, que é indispensável que a companhia estabeleça uma cultura de governança de dados e que adote todas as medidas operacionais e de segurança da informação para assegurar a integridade dos dados pessoais tratados durante a execução de suas atividades; quer dizer, a governança de dados — que, na realidade, é uma espécie do gênero "governança corporativa" — deve focar na organização e no controle dos dados pessoais (insumos) essenciais para determinada atividade, por meio de objetivos organizacionais e processos institucionalizados, para a produção de informação e conhecimento das empresas [6]. Em última análise, a governança de dados passou a ser um ativo organizacional e, como tal, por envolver o cruzamento de diversas disciplinas, pressupõe o envolvimento de todos os funcionários e prestadores de serviços, os quais deverão estar cientes de todas as práticas adotadas pela empresa para assegurar que a privacidade e os dados pessoais dos titulares de dados estão sendo devidamente tutelados.

Nesse contexto, estar adequado à LGPD e adotar uma cultura de governança de dados significa uma verdadeira mudança de hábitos, no sentido de que a empresa passe a ter mais cuidado com correspondências físicas e eletrônicas, compartilhamento de dados, controle de acesso aos sistemas operacionais, armazenamento de documentos na rede ou em nuvem, bem como com os conceitos de *privacy by design* e *privacy by default* apontados anteriormente, de acordo com os quais a privacidade e a proteção de dados devem ser considerados em todos os novos negócios e projetos. Além disso, medidas técnicas como a criptografia dos dados, isolamento das bases de dados que permitam a identificação do titular, uso de mecanismos de segurança e autenticação (*firewalls*, antivírus e dupla autenticação) também devem ser considerados e implementados, na medida e na extensão possíveis.

Em conclusão, na realidade brasileira, na qual os vazamentos de dados aumentaram 493% nos últimos anos [7], sendo que mais de 205 milhões de dados de brasileiros vazaram de forma criminosa em 2019 [8], é precisamente o conjunto dessas medidas de segurança e de governança de dados que, do ponto de vista da proteção de dados, irão refletir ao consumidor ou usuário do business da empresa a segurança necessária para uma relação comercial sustentável [9], o que se relaciona tanto com o eixo social, quanto o de governança, do ESG.

O ESG é um tema atual e de extrema relevância para todas as empresas, de todos os tamanhos e de todos os segmentos de mercado, justamente em razão de seu caráter transdisciplinar. ESG, portanto, engloba proteção de dados, relações de trabalho e de consumo, questões tributárias, societárias e concorrenciais, entre tantas outras [10].

[1] Disponível em:

[https://www.ifc.org/wps/wcm/connect/9eeb7982-3705-407a-a631-586b31dab000/IFC\\_Breif\\_whocares\\_online.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-9eeb7982-3705-407a-a631-586b31dab000-jkD12B5](https://www.ifc.org/wps/wcm/connect/9eeb7982-3705-407a-a631-586b31dab000/IFC_Breif_whocares_online.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-9eeb7982-3705-407a-a631-586b31dab000-jkD12B5). Acesso em: 20 mar. 2021.

[2] Disponível em: <https://www.unpri.org/download?ac=10948>. Acesso em: 20 mar. 2021.

[3] Disponível em: <https://www.bcg.com/pt-br/press/25october2017-total-societal-impact>. Acesso em: 20 mar. 2021.

[4] Cf. artigo 50 da LGPD.

[5] BARBIERI, Carlos. Governança de Dados: Práticas, Conceitos e Novos Caminhos. Rio de Janeiro: Alta Books, 2019. p. 33.

[6]

BARBIERI, Carlos. Governança de Dados: Práticas, Conceitos e Novos Caminhos. Rio de Janeiro: Alta Books, 2019. pp. 35-36.

[7] Disponível em: <https://dl.acm.org/doi/abs/10.1145/3439873>. Acesso em: 20 mar. 2021.

[8] Disponível em: <https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit/>. Acesso em: 20 mar. 2021.

[9] Veja mais em: <https://www.veirano.com.br/midia/resource-kit-lgpd>. Acesso em: 20 mar. 2021.

[10] Mais informações em: <https://www.veirano.com.br/expertise/pratica/esg-ambiental-social-e-governanca>. Acesso em: 20 mar. 2021.

**Date Created**

07/04/2021