

BRASIL 2024

NOSTALGIA OU
PERSPECTIVAS



COLEÇÃO
IPSOS FLAIR

GAME CHANGERS



BRASIL 2024 NOSTALGIA OU PERSPECTIVAS

Edição Ipsos®
Julho 2023

A PRIVACIDADE A SEU FAVOR: COMO CONQUISTAR OS CONSUMIDORES E CRIAR AS OPORTUNIDADES UTILIZANDO A GOVERNANÇA DE DADOS

CAROLINA FAIRBANKS
ADVOGADA SR., IPSOS NO BRASIL

ESG É A SIGLA DO MOMENTO. INICIATIVAS RELACIONADAS À REDUÇÃO DE PEGADA AMBIENTAL E AO APOIO ÀS POPULAÇÕES CARENTES SÃO FACILMENTE DIVULGADAS E TRAZEM UM RETORNO PERCEPTÍVEL DE VALOR DE MARCA. CONTUDO, COMO DEMONSTRAR O G DE ESG? A PRIVACIDADE PODE SER UMA FORMA MAIS ATUAL E DIRETA DE DEMONSTRAR A GOVERNANÇA CORPORATIVA RESPONSÁVEL.

Atender às expectativas dos consumidores nunca foi tão difícil. O consumidor contemporâneo leva em conta não apenas as características do produto em si, mas também como a marca se posiciona e se relaciona com o mundo à sua volta. As expectativas deles incluem nesse contexto a sigla ESG, como detalha, nesta edição, o artigo “ESG - Os desafios de implementar uma governança eficaz, sustentável e que deveria trazer retorno financeiro”. Porém, enquanto as campanhas ambientais e sociais têm fácil apelo de *marketing*, a governança acaba sendo deixada de lado em muitas comunicações e pode apresentar um campo inexplorado de oportunidades, em especial no gerenciamento de dados pessoais e privacidade.

Mais de dois terços (68%) dos

consumidores ao redor do mundo afirmam estar preocupados com a sua privacidade *on-line*⁴⁸. A empatia com que você, enquanto empresa, gerencia os dados dos seus clientes e comunica as suas políticas de privacidade pode fortalecer o seu relacionamento com esses consumidores.

A maturidade na gestão de privacidade permite abandonar a postura retraída e cautelosa que predominou no ambiente corporativo após a publicação da Lei Geral de Proteção de Dados Pessoais (LGPD) e passar a enxergar a privacidade como um ativo importante.

Investir em gestão de privacidade pode ser uma forma de reter os clientes, melhorar a imagem e a comunicação, e, até mesmo, gerar oportunidades de negócio.

A IMPORTÂNCIA DA PRIVACIDADE PARA A SUA MARCA

Por outro lado, o custo de não gerir adequadamente a privacidade é alto e pode gerar uma grande insatisfação. Além da perda de confiança, um incidente de segurança com

vazamento de dados leva 82% dos consumidores a parar de usar uma marca, um serviço ou produto em algumas ocasiões, ou para sempre, segundo a Associação Internacional

de Profissionais de Privacidade (IAPP, na sigla em inglês).

É de senso comum entre os especialistas de segurança da informação que um incidente de segurança é algo inevitável. Vai acontecer, é somente uma questão de tempo. Mas é possível minimizar os danos causados por essa ocorrência, o que pode ser uma razão para 30% dos consumidores afetados permanecerem no relacionamento.

Para que seja possível reagir bem, é necessário ter feito a lição de casa compreendendo quais são os dados tratados pela empresa, quais são os riscos envolvidos, e estabelecendo políticas e procedimentos adequados tanto para o dia a dia quanto para o caso de uma situação de crise.

As pesquisas apontam, porém, que o

foco da privacidade não deve recair somente sobre os vazamentos. Para a IAPP, a mesma porcentagem de consumidores considera que um vazamento ou pedir mais dados do que o necessário são práticas que causam desconforto (63%).

Na mesma linha, outra pesquisa revela que expor o consumidor a uma experiência negativa de privacidade tem efeitos quase tão ruins quanto um vazamento, com 35% de perda de confiança (contra 44% no vazamento de dados), e levaria 39% dos respondentes a abandonar a sua marca favorita em favor de um concorrente⁴⁹.

Como, então, organizar a sua empresa para que ela realize uma gestão de dados que minimize os impactos em um vazamento e crie uma experiência positiva de proteção de dados para o consumidor?

CONQUISTANDO A CONFIANÇA DO CONSUMIDOR

Novas legislações referentes à proteção de dados surgiram ao redor do mundo desde a entrada em vigor da legislação europeia sobre o tema,

a General Data Protection Regulation, em 2018. Com diretrizes semelhantes e alinhadas à GDPR, elas trazem, em geral, uma novidade interessante: a

imposição de governança corporativa sobre dados, incluída também na legislação brasileira, publicada em 2018 e em vigor desde 2020.

O Legislativo tem, por princípio, deixar que as empresas e o mercado se organizem como preferirem, trazendo exigências maiores somente quando necessário, tal como em casos de concentração de mercado ou nas empresas com capital aberto. A LGPD, porém, exige uma adaptação das empresas, de maneira transversal.

Mais do que isso, a legislação estabelece um princípio específico para a responsabilidade e a prestação de contas, que demanda a produção de uma documentação adequada.

Hoje, quase 5 anos após a publicação da LGPD, muitas empresas ainda não completaram esse processo. A necessidade de realizar o mapeamento dos dados pessoais e a análise de risco sobre a forma como esses dados são tratados causou alvoroço nas empresas.

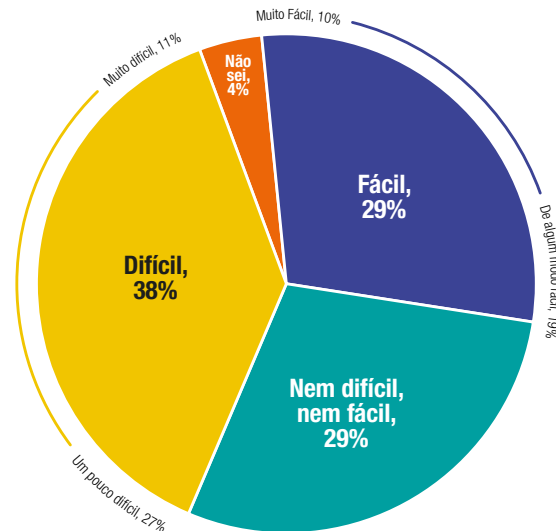
“NÃO LI E CONCORDO”: DIZEM QUE A ÚNICA CONSEQUÊNCIA DA LGPD É TER QUE ACEITAR EXTENSAS E INCOMPREENSÍVEIS POLÍTICAS DE PRIVACIDADE PARA ACESSAR QUALQUER SERVIÇO. ESSA IMPRESSÃO É RASA E INFUNDADA. A LEI EXIGE UM TRATAMENTO RESPONSÁVEL DOS DADOS PESSOAIS, AINDA QUE COM CONSENTIMENTO – O CONSENTIMENTO NÃO É PASSE LIVRE PARA O ABUSO.

De todo esse preparo, apenas uma pequena parte transparece para o consumidor. Além do eventual contato direto com os funcionários que tratam de temas de privacidade - e que devem ser bem treinados -, o principal documento que permite uma empresa se comunicar com o consumidor é uma política, aviso ou termo de privacidade. Por isso, é essencial

aproveitar essa oportunidade para começar a moldar as expectativas e estabelecer uma relação de confiança e transparência.

As políticas que encontramos, porém, não são nada atraentes. Como elas têm o foco de blindar a empresa contra os riscos e atender as exigências legais, é

comum a facilidade para a leitura e compreensão ser deixada em segundo plano, e a política se tornar um texto extenso e cansativo. O resultado é claro: apenas 29% da população considera fácil entender o quão bem as empresas protegem os seus dados, e 38% consideram difícil ou muito difícil, de acordo com a IAPP.



Facilidade de compreender o quão bem uma empresa protege as suas informações pessoais: 4%, não sabem; 29%, fácil; 29%, nem um nem outro; 38%, difícil.

É hora de propor novos formatos. Mesmo quando não for possível reduzir ou dinamizar o texto principal do termo ou da política de privacidade, não há nada que impeça o acréscimo de uma explicação curta, objetiva e com linguagem simples em destaque no início da página, trazendo os maiores pontos de preocupação para o consumidor. Assim, ele pode ler só o que o interessa e buscar mais detalhes quando necessário.

O impacto de um bom termo de privacidade não pode ser subestimado. A clareza das informações e o controle do consumidor sobre como os seus dados são tratados estão entre as alternativas mais citadas como

ações das empresas que aumentam a confiança dos consumidores, com 64% de menções. Em um estudo do Google em que os participantes foram expostos às experiências positivas e negativas de privacidade, 43% dos entrevistados afirmaram que trocariam a sua marca preferida por uma segunda opção, caso essa segunda opção trouxesse uma experiência de privacidade positiva.

Além de criar um resumo em destaque, outro caminho para melhorar a comunicação é demonstrar empatia com o microcontexto do consumidor (aliás, esse conceito é detalhado na narrativa de sucesso de marca da Ipsos⁵⁰) no momento em que ele entra em contato com

o aviso de privacidade. Em vez de bombardear o consumidor com avisos genéricos e aceites gerais, podemos trazer informações ou consentimentos *just in time*, disponíveis no exato momento em que são utilizados ou solicitados os dados, e que permitem ao consumidor entender claramente o que está acontecendo.

Já vimos nos sistemas operacionais, por exemplo, o pedido de acesso à câmera do aparelho somente no momento necessário para ler um QR Code ou realizar a identificação por biometria facial, evitando o desconforto do usuário de ter que autorizar uma lista de acessos e permissões confusas ao instalar um aplicativo que, geralmente, ele ainda não conhece.

Além dessa boa prática, ainda há formas simples de dar maior sensação de controle ao consumidor. Ao trazer uma propaganda direcionada em um *site*, podemos incluir uma nota ou um *link* que explique como as informações de perfil e de consumo são coletadas e utilizadas para direcionar essa propaganda, e um botão que permita ao titular de dados ajustar essas informações ou, até mesmo,

apagá-las. Dessa forma, ele receberá publicidades que, de fato, o interessem e aumentará as chances de visualização e compra com base nessas visualizações. É como o conceito de *cookies*, mas um pouco além.

Explico: em vez de confiar que os algoritmos das empresas vão usar as minhas informações da melhor maneira, após clicar em “aceito os *cookies* de publicidade”, os anunciantes poderiam ser mais claros e me dizer “você tem interesse em produtos X, viagens Y e serviços Z”, e eu, enquanto consumidor, deveria ter a chance de responder “sim, mas, neste momento, preferiria receber publicidades direcionadas somente dos serviços Z”.

A comunicação clara e no momento certo é a principal ferramenta para ganhar a confiança e segurança do consumidor, permitindo que o tema da privacidade evolua de um incômodo ou uma preocupação para uma fonte de oportunidades de negócio.

SAINDO DA PARALISIA INICIAL E CRIANDO OPORTUNIDADES DE NEGÓCIO

Outra grande mudança trazida pela nova onda legislativa foi a transição dos dados pessoais de uma *commodity* - vendida livremente entre as empresas - para um direito fundamental do titular. Os dados não podem mais ser tratados como uma mercadoria de venda livre, em que empresas acumulam, analisam, lucram, tomadas pela febre do *Big Data*. Como mencionamos, as empresas devem ter uma explicação

plausível, tal como o consentimento do indivíduo, e tratar os dados de forma responsável.

Vale lembrar, porém, que o consentimento não é a única nem a principal, mas, apenas, uma entre as dez bases legais ou justificativas dadas pela lei para o tratamento dos dados pessoais, que incluem também outras alternativas como o legítimo interesse ou a execução de contratos.

OPT-IN PARA TUDO: O CONSENTIMENTO PODE SER REVOGADO PELO TITULAR E DEPENDE DE COMPROVAÇÕES COMPLEXAS. EM MUITOS CASOS, OUTRAS BASES LEGAIS COMO O LEGÍTIMO INTERESSE OU A EXECUÇÃO DE CONTRATO PODEM E DEVEM SER UTILIZADAS, COM A TRANSPARÊNCIA GARANTIDA POR MEIO DE UM AVISO DE PRIVACIDADE CLARO E COMPREENSÍVEL.

As dificuldades das empresas em compreender bem a lei, selecionar uma base legal adequada e ajustar as suas práticas geraram uma paralisação de muitas atividades. Notamos na indústria de pesquisa o congelamento das vendas de listagens, que são os bancos de

dados de pessoas físicas.

A legislação, porém, não impede a comercialização de dados, desde que sejam respeitados os princípios da lei e que haja uma base legal adequada. A novidade é que o beneficiado pelos dados deve ser o próprio titular.

Um exemplo interessante que encontramos foi o de uma empresa de investimentos que oferece um *voucher* de compras em troca da possibilidade de reter os dados pessoais e de perfil para as análises. Outra ideia é a formação

de parcerias e a oferta de descontos voltados a um público específico cujos dados sejam visados, tal como descontos na compra de um carro que permita compartilhar os dados do comprador com as companhias de seguros.

OS DADOS PODEM SER COMERCIALIZADOS PELO PRÓPRIO TITULAR, GERANDO UM RELACIONAMENTO GANHA-GANHA COM AS EMPRESAS. PARA QUE ISSO FUNCIONE, É NECESSÁRIO ESTABELECEER UMA RELAÇÃO DE CONFIANÇA COM O TITULAR E UMA PROXIMIDADE COM A EQUIPE DE PRIVACIDADE.

Notamos também uma abertura da população à comercialização dos seus dados, já que 45% dos entrevistados na pesquisa “Global Trends Survey” da Ipsos⁵¹ indicaram que não estão preocupadas com

o que as empresas ou o governo sabem sobre elas, e consideram que as pessoas estão preocupadas demais com a privacidade, e, em outra pesquisa global conduzida pela Ipsos, 54% dos entrevistados⁵²

VOCÊ SE SENTE MAIS CONFORTÁVEL PARA COMPARTILHAR DADOS PESSOAIS AS EMPRESAS CASO ELAS SEJAM CLARAS SOBRE O TRATAMENTO QUE SERÁ DADO A ESSAS INFORMAÇÕES E SE PROMETER NÃO COMPARTILHAR ESSAS INFORMAÇÕES COM TERCEIROS

Se estiver plenamente claro o que a empresa vai fazer com aquela informação



Se a empresa se comprometer não compartilhar nem vender as informações para terceiros



Se a empresa nunca ter sido alvo de vazamento, violação ou uso fraudulento de dados



Se você tiver muitas experiências com esta empresa



Se a empresa oferecer algum tipo de compensação pelo fornecimento de informações (por exemplo, desconto, prêmios, etc.)



■ Muito confortável ■ Um pouco confortável ■ Um pouco desconfortável ■ Muito desconfortável

Fonte: pesquisa Ipsos Global Citizens Data Privacy. P. Até que ponto você se sentiria mais confortável para compartilhar suas informações pessoais com empresas ou marcas...

afirmam que os indivíduos deveriam ser recompensados pelo uso dos seus dados. Essa oferta de compensação financeira, contudo, não pode ser tratada como uma solução simples para todos os problemas. Sem uma comunicação adequada, ela pode gerar no consumidor uma retração

e desconfiança ao ver uma tarja de preço conectada aos seus dados.

A abertura para o compartilhamento de dados em troca de descontos é melhor recebida em transações de maior valor, e se for mal utilizada pode causar uma perda de confiança.

TAKE AWAY

Para explorar melhor essas oportunidades de negócio, é imprescindível a comunicação empática com o microcontexto do consumidor realizada por uma equipe competente de *marketing*, mas também um time de privacidade que entenda do seu negócio e seja envolvido desde cedo nas novas ideias, redirecionando aquelas que apresentem os riscos e potencializando as que possam explorar melhor essa parceria com os consumidores. É da parceria entre essas áreas

internas que as marcas podem abrir portas para a inovação em privacidade. Em resumo, superamos o momento de cautela inicial, em que se congelavam as operações e escreviam políticas extensas, e, feita a lição de casa, podemos caminhar para os relacionamentos mais transparentes que conquistem os consumidores e buscar oportunidades de vantagens mútuas para que a gestão de privacidade se torne um ativo relevante, e não, apenas, uma preocupação para as empresas.

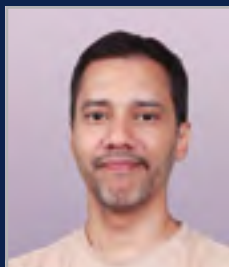




YVES BARDON
Diretor do Programa
Ipsos Flair, Ipsos
Knowledge Centre



MARCOS CALLIARI
CEO da Ipsos no Brasil



**ALEX CANDIDO
DOS SANTOS**
Head, Marketing &
Communications



CAROLINA FAIRBANKS
Advogada Sr.,
Ipsos no Brasil



**CHRISTIAN
OMMUNDSEN**
Head, Customer
Experience



**FERNANDA
WAJCHENBERG**
Head, Innovation



HELENA JUNQUEIRA
Gerente Sr.
Ipsos Synthesio



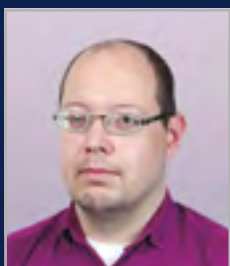
JOANA CAMARGO
Diretora,
Innovation



JOÃO VICTOR DALLA POLA
Analista, Public Affairs e
Corporate Reputation



JULIANA CHAVES
Diretora,
Innovation



MAILSON ROCHA
Diretor, Business
Innovation Partner



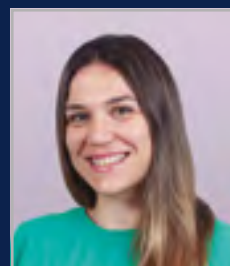
MALU ACEDO
Diretora,
Ipsos IUU



MARCELA AYRES
Gerente,
Innovation



MATEUS ROMA
Gerente, Brand
Health Tracking



PRISCILLA BRANCO
Gerente Sr., Public Affairs
e Corporate Reputation



PRISCILLA THOMÉ
Diretora, Brand
Health Tracking



SIDNEI MARTINEZ
Diretor, Customer
Experience



TANIA CERQUEIRA
Diretora, Client
Organisation



THIAGO RAMOS
Diretor, Global
Modelling Unit