Edição 39 - 1º Trimestre - Ano 2024

BOLETIM 5Rs

INFORMATIVO DO COMÉRCIO ATACADISTA DE RECICLÁVEIS

A LGPD E O SETOR DE RECICLAGEM

Eu trabalho para o meio ambiente

A LH 30 M Industry Litronic

O LH 30 oferece alto desempenho de manipulação, em todos os tipos de aplicação. Rápido, potente e estável, está disponível em várias versões que se adaptam de forma ideal ao trabalho a ser executado. Sempre presente, onde for necessário!
www.liebherr.br

LIEBHERR

Manipuladores de materiais

Liebherr Brasil • Rua Dr. Hans Liebherr, 1 - Vila Bela • 12522-635 Guaratinguetá/SP • Phone +55 12 2131-4200
info.lbr@liebherr.com • www.facebook.com/LiebherrConstruction • www.liebherr.com.br

A LGPD e o setor de reciclagem

Autor: Marcio Mello Chaves
Advogado, DPO e professor de Direito Digital e Proteção de Dados

O descarte de resíduos eletrônicos, como abordado na edição anterior, traz à tona a importância de se endereçar uma das principais crises da modernidade: a proteção da privacidade. Isto porque na sua destinação, os resíduos eletrônicos frequentemente utilizam dados pessoais em seu funcionamento e, com isso, trazem riscos de sua exposição, principalmente quando manejados de forma inadequada no processo de descarte. Neste cenário, recentes exigências legais de proteção da privacidade trazidas pela Lei Geral de Proteção de Dados Pessoais (LGPD) passaram a colocar nas pautas de discussão e planejamento das empresas na cadeia da reciclagem, da necessidade de estarem em conformidade com a referida lei. E a preocupação abrange não apenas os referidos insumos utilizados, mas também como as empresas do setor utilizam dados pessoais internamente em suas operações, a exemplo dos dados de colaboradores, representantes de prospects, clientes e fornecedores, entre outros tantos.

Antes de assumirmos que estamos diante apenas de uma preocupação adicional para as empresas que atuam na cadeia da reciclagem, por conta das consequências do descumprimento da lei acrescendo ao "custo Brasil", é importante entendermos os motivos de sua existência e seus reflexos nas operações. Afinal, por que temos uma LGPD?

O direito à privacidade não é algo novo: sua previsão em nossa Constituição, inclusive como Direito Fundamental, também está presente em outras legislações, a exemplo do Código de Defesa do Consumidor, da Consolidação das Leis Trabalhistas, do Código Civil, e até de legislações mais recentes como é o caso do Marco Civil da Internet e o regulamento do comércio eletrônico. No entanto, antes de sua existência o "como fazer" para garantir esse antigo direito ainda dependia de boas práticas de mercado, algo que por não ser detalhadamente exigido resultava na simples falta de preocupação por parte da grande maioria das empresas. E que, somada ao aumento significativo da capacidade de processamento e armazenamento de dados nos últimos anos, exigiu uma legislação específica para proteger os dados pessoais dos cidadãos.

Nesse sentido, a LGPD traz importantes definições e princípios que devem ser obedecidos por todas as organizações que usem dados pessoais, tanto em meios físicos, como nos papéis presentes das mesas aos infindáveis e esquecidos arquivos-morto, quanto eletrônicos nas mais variadas possibilidades de armazenamento – do pendrive à nuvem, por pessoas naturais e jurídicas de direito público ou privado, de qualquer forma que seja. Pois para garantir a privacidade é necessário proteger o dado pessoal em qualquer operação realizada com dados pessoais, como: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, avaliação ou controle da informação, modificação, comunicação, transferência, difusão, extração, e inclusive a eliminação. Ou seja: não importa o que é feito com o dado pessoal, sua utilização ativa ou passiva deve ser segundo os requisitos estabelecidos pela lei para garantir sua proteção. E não importa se o uso do dado pessoal está sendo feito para proveito próprio da empresa (denominado pela lei como "Controlador"), ou em atendimento a pedido de outra empresa (chamado de "Operador"): ambos têm obrigação de seguir a LGPD, inclusive com a possibilidade de serem solidariamente responsáveis pelos danos causados em virtude do descumprimento da lei.

GUINDASTE ESTACIONÁRIO

POTENZA

COMPLETA LINHA DE GARRAS

+55 49-32260677
www.potenzaindustria.com.br
comercial@potenzaindustria.com.br
/PotenzaIndustria

Quando pensamos em violações à LGPD a primeira coisa que nos vem à mente são os casos de vazamento e sequestro de dados. E não é por menos: os maiores casos de violação de privacidade por exposição de dados pessoais que ocorreram, no Brasil e no mundo, foram no ambiente digital, uma vez que o grande volume de dados manuseados nesse ambiente aumenta exponencialmente o impacto. Exemplos dos incidentes ocorridos envolvendo o Facebook em 2021[1] o qual resultou no vazamento de mais de meio bilhão de usuários da rede social; o megavazamento do Governo brasileiro naquele mesmo ano[2], onde 223 milhões de CPFs e outras várias informações pessoais como renda, escolaridade, benefícios do INSS e programas sociais foram ofertados para venda por cibercriminosos; e a maior violação da história, que ficou conhecida como *MoAB* (do inglês *Mother of All Breaches* ou Mãe de Todas as Violações), ocorrida em 2023[3], na qual nada menos que 26 bilhões de registros, compilados de vazamentos anteriores e de milhares de novos vazamentos que ainda não haviam sido noticiados, mostrou para o mundo que não existe limite quando o tema é exposição de dados.

No setor da reciclagem, alguns dos recentes casos de incidentes de dados mais recentes foram os da Freecycle[4], a instituição de caridade que faz reciclagem de detritos que seriam destinados a aterros sanitários, que identificou que os dados pessoais de usuários, incluindo nomes, Ids de usuário, endereços de e-mail e senhas haviam sido expostos; e da TOMRA[5], a gigante norueguesa que atua nas áreas de mineração e reciclagem, com receitas de US$ 1,2 bi e ações na bolsa de valores de Oslo, sofreu ataque cibernético extenso que impactou as divisões de soluções de resíduos e reciclagem, seus sistemas e equipamentos de triagem, impactando a cadeia de suprimentos e as principais unidades que permanecerem *offline*, obrigando a equipe a atuar em teletrabalho.

Não são só os incidentes envolvendo ataques cibernéticos que podem expor dados pessoais. Muitas vezes o vazamento pode ser no simples descarte de documentos, incluindo embalagens, como no caso das etiquetas de logística e notas fiscais contendo informações pessoais de identificação e de contato (nome completo, CPF e endereço residencial). Descartados sem o devido cuidado, permitem a prática conhecida pelos *hackers* como *dumpster diving* ou o "mergulho na lixeira", onde um agente mal-intencionado pode pesquisar resíduos descartados para descobrir informações relevantes que podem ajudar a invadir sistemas ou levantar informações para a prática de fraudes.

E os incidentes podem ainda ocorrer nas mais corriqueiras atividades, como é o caso do envio de e-mail, copiando pessoa errada, com planilha anexada desprotegida contendo dados pessoais de contato de colaboradores; no armazenamento de documentos por período além do necessário e legalmente permitido; e até no simples esquecer de documentos contendo dados pessoais nas impressoras, permitindo um acesso indevido por colaboradores ou terceiros que estiverem nas proximidades do equipamento. Isso para mencionar apenas alguns dos diversos tipos de violações corriqueiramente ocorridas nas empresas que coroam a máxima de que não é uma questão de se, ou de quando teremos um incidente de privacidade: é uma questão de quando identificaremos que ele ocorreu, pois o tempo médio entre ele acontecer e ser descoberto é de mais de 200 dias[6].

1 Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/04/07/facebook-atribui-vazamento-de-dados-de-530-milhoes-de-dados-a-raspagem.ghtml. Acesso em: 28/02/2024.
2 Disponível em: https://www.cnnbrasil.com.br/economia/novo-megavazamento-de-dados-e-teste-de-fogo-para-lgpd-dizem-especialistas/. Acesso em: 28/02/2024.
3 Disponível em: https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/. Acesso em: 28/02/2024.
4 Disponível em: https://www.theregister.com/2023/09/05/freecycle_becomes. Acesso em: 28/02/2024.
5 Disponível em: https://www.theregister.com/2023/07/18/tomra_cyberattack. Acesso em: 28/02/2024.
6 Disponível em: https://www.ibm.com/reports/data-breach. Acesso em: 28/02/2024.

Apesar de a LGPD ter sido promulgada há mais de cinco anos (em 2018), suas obrigações entraram em vigor em 2020. Seu regulamento para a fiscalização e o processamento, em vigor desde agosto de 2021, e a metodologia para o cálculo das sanções previstas na lei, em vigor desde fevereiro de 2023, permitem a aplicação de forma retroativa desde julho do ano passado das penalidades administrativas, o que tem resultado na penalização de empresas, públicas e privadas, pelo descumprimento da LGPD.

Quando se fala em consequências por descumprir a LGPD a multa administrativa é a preocupação das empresas, principalmente pelo alto valor que pode ser aplicada – até 2% do faturamento limitada a 50 milhões de reais – por infração. E nesta seara administrativa, a ANPD tem dado os primeiros passos devido ao seu curto período de existência e carência de pessoal e verba para funcionar: até o momento, a ANPD sancionou 9 agentes de tratamento, sendo 8 órgãos públicos e uma empresa privada[7], com concluídos 17 processos de fiscalização[8] e outros 13 estão em andamento[9], envolvendo desde provedores de tecnologia até farmácias e seus programas de pontos. Números realmente iniciais, principalmente considerando a longa fila de milhares de denúncias e comunicados de incidentes a serem apuradas pela autoridade, o que resultará em um aumento exponencial de novas penalidades.

Mas o que pouco se fala é que não são apenas as multas que devem chamar a atenção, pois demais penalidades administrativas cabíveis previstas na LGPD, como é o caso da publicização da infração, do bloqueio e da eliminação de dados, e da suspensão e a proibição, parciais ou totais de dados pessoais podem resultar na própria impossibilidade de a empresa violadora operar. Afinal, como uma empresa pode operar sem usar dados pessoais?

Além das penalidades administrativas outras consequências que podem trazer graves reflexos, principalmente financeiros, para as empresas que a descumprirem. É o caso da judicialização, onde os titulares ou entidades representativas podem pedir na justiça indenizações individuais ou coletivas pelas violações causadas, como ocorreu na justiça do Maranhão que condenou o Facebook pelo vazamento de 2021 mencionado anteriormente a pagar 72 milhões de reais por danos morais coletivos[10]; e a perda reputacional, que pode inclusive impactar o valor de mercado da empresa violadora, como aconteceu com esta mesma empresa ao perder 9 bilhões de dólares de valor de mercado após outro escândalo de vazamento de dados ocorrido em 2018[11].

CONVENÇÕES COLETIVAS DE TRABALHO

As Convenções Coletivas de Trabalho da categoria econômica do Comércio Atacadista de Sucata Ferrosa e Não Ferrosa do Estado de São Paulo, encontram-se disponíveis para download em nosso site: www.sindinesfa.org.br

7 ANPD. Processos administrativos sancionadores. Disponível em Processos Administrativos Sancionadores — Autoridade Nacional de Proteção de Dados (www.gov.br). Acesso em 06/02/2024.
8 ANPD. Processos de fiscalização concluídos. Disponível em Processos de Fiscalização Concluídos — Autoridade Nacional de Proteção de Dados (www.gov.br). Acesso em 06/02/2024.
9 ANPD. Processos de fiscalização em andamento. Disponível em Processos de Fiscalização em Andamento — Autoridade Nacional de Proteção de Dados (www.gov.br). Acesso em 06/02/2024.
10 Disponível em: https://g1.globo.com/ma/maranhao/noticia/2023/03/24/justica-do-maranhao-condena-facebook-a-indenizar-brasileirosque-tiveram-dados-vazados.ghtml. Acesso em: 28/02/2024.
11 Disponível em: https://www.infomoney.com.br/carreira/mark-zuckerbergperde-us-9-bilhoes-em-48-horas-apos-escandalo-de-vazamentode-dados/. Acesso em: 28/02/2024.

Como se adequar à LGPD?

Para evitar uma penalização por um incidente ocorrido, somente uma medida está no alcance das empresas: a capacidade de demonstrar que cumpriu todas as exigências legais de possuir medidas de proteção de dados. Quando se fala em segurança dos dados, temos como principais exemplos as ferramentas de controle de acesso, gestão de identidade, uso de controles criptográficos e até mesmo de segurança patrimonial física, como é o caso das chaves em portas, arquivos e gavetas.

Mas não é só isso: como não há como se proteger algo que não se conheça, e para demonstrar possuir a governança de dados pessoais, deve-se garantir-se que os usos de dados pessoais sejam registrados e inventariados, contemplando todas as operações efetuadas, desde a coleta até a destruição do dado pessoal (ao longo de todo seu ciclo de vida que inclusive na maioria das vezes envolve terceiros como fornecedores de plataformas digitais); e diante de tal mapeamento, avaliar e ajustar cada uso para os requisitos legais, inclusive das próprias medidas técnicas, e por meio das análises de risco e da elaboração de Relatórios de Proteção de Dados quando necessários.

A governança também advém das Políticas e Procedimentos que orientam o uso dos dados pessoais na organização. Normas como Plano de Resposta à Incidentes de Privacidade, Políticas de Privacidade do site da internet, de Governança interna da empresa, de Retenção e Descarte de Dados, além de procedimentos de Resposta a Titulares e Autoridades são algumas das principais normativas das empresas. Dentro deste tema temos ainda a obrigação de possuir as devidas garantias contratuais nas relações das empresas, tanto internas com seus colaboradores, quanto externas com seus prestadores de serviço, por meio das cláusulas de privacidade, especialmente importantes quando há a transferência de dados pessoais para outros países, algo comum devido à popularização dos serviços em nuvem.

Estar adequado à LGPD significa também garantir o atendimento das possíveis solicitações de titulares no exercício de seus direitos, que não são poucos: (i) confirmação da existência de tratamento; (ii) acesso aos dados; (iii) correção de dados incompletos, inexatos ou desatualizados; (iv) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei; (v) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (vi) eliminação dos dados pessoais tratados com o consentimento do titular; (vii) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; (viii) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e (ix) o direito de revogar seu consentimento. Para estar apta a cumprir com a obrigação legal de atendimento às solicitações dos titulares, a empresa precisa possuir as atividades de uso de dados pessoais mapeadas e documentadas, além de normas implementadas que orientem como deve ser processada uma solicitação desta natureza dentro dos curtos prazos legais (imediato, para as informações resumidas ou até 15 dias, para informações detalhadas).

Outra importante obrigação é a de possuir um Encarregado pela proteção de dados pessoais da empresa, também conhecido como Data Protection Officer ou DPO. O Encarregado é o responsável por aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências com as funções de DPO; receber comunicações da

autoridade nacional e adotar providências; orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares, em breve definidas em resolução já em fase de elaboração pela ANPD. Tal função pode ser exercida internamente ou terceirizada, e dispensada apenas dos considerados Agentes de Pequeno Porte (microempresas e empresas de pequeno porte, startups, pessoas jurídicas sem fins lucrativos e pessoas naturais).

Vale ainda destacar a obrigação de, para a empresa fazer qualquer tipo de uso de dado pessoal, estar embasada em uma das hipóteses legais que vão além do próprio consentimento, podendo ser validadas para fins de cumprimento de obrigação legal, execução de contratos (incluindo obrigações pré-contratuais), defesa em processos administrativos, judiciais, administrativos ou arbitrais, proteção da vida, tutela da saúde, além do legítimo interesse do Controlador (como nos casos de proteção patrimonial por câmeras de segurança e verificação de antecedentes). E também a obrigação de seguir os princípios da proteção da privacidade, necessários para cobrir as infinidades de usos possíveis, dentre os quais destacamos além da segurança, os de finalidade, necessidade e adequação, livre acesso, qualidade, transparência e não-discriminação perante os titulares, e responsabilização e prestação de contas.

Filie-se e fortaleça a representatividade da Associação dos Recicladores do Brasil "INESFA". Entre em contato e informe-se: secretaria@inesfa.org.br

Conformidade com a LGPD: crise/oportunidade

Não restam dúvidas de que adequar-se à todas as exigências da nova lei trazem custos para as empresas, demandando investimentos em tecnologias, não apenas as digitais, em processos, em especial nos normativos internos, contratos e documentos de acesso ao público, e em pessoas por meio da conscientização e da capacitação acerca do tema.

Mas, como observado pelo ex-presidente norte-americano John F. Kennedy ao parafrasear o ditado "quando escrita em chinês, a palavra crise é composta de dois caracteres: um representa perigo e o outro representa oportunidade", a crise trazida pelas obrigações da LGPD também podem trazer um cenário de oportunidades para as empresas que estiverem devidamente adequadas: se destacar frente às concorrentes que, por não o tiverem feito, podem perder concorrências ou até mesmo suas relações contratuais com as empresas que exigem a conformidade de seus parceiros comerciais; ou ainda, fornecer meios para o descarte apropriado para as empresas que não o conseguem ou tiverem dificuldades em fazê-lo. E sob essa ótica de crise/oportunidade, as empresas podem reforçar as justificativas e os planejamentos de investimentos do setor nesta importante e destacada legislação brasileira.

Apoiadores do Seminário
Reciclagem Valorizada, Sustentabilidade Equilibrada
8 de maio de 2024

TALK #06 - Exportação no Setor de Reciclagem

Apresentador:
Roger Amarante

Convidados:
Marcio Rodriguez, José Arévalo e Marcos Fonseca

TALK #07 - Mulheres na Reciclagem

Apresentador:
Roger Amarante

Convidadas:
Daniela Barros, Karine Vieira e Nathali Aparicio

TALK #08 - Relacionamento Governamental e Legislação

Apresentador:
Roger Amarante

Convidadas:
Carolina Rebelo e Renata Satorno

TALK #09 - Do Pequeno Depósito a Uma Grande Empresa

Apresentador:
Roger Amarante

Convidados:
Roberto Barros, Ismar Vieira e Valentin Escamilla

INESFA SINDINESFA

Expediente: O INESFA e o SINDINESFA não se responsabilizam pelos conceitos emitidos em artigos assinados.

Rua Rui Barbosa, 95 - 5º andar - Bela Vista - 01326-010 - São Paulo - SP

Telefones: (11) 3251-0277 / 3251-0362 - www.inesfa.org.br - www.sindinesfa.org.br