PROTEÇÃO DE DADOS EM FOCO

VOL. II

COORDENADORAS:
Ana Paula Canto de Lima
Carolina Margonari
Eloá Caixeta

EDITORA IMPÉRIO

LGPD SEM JURIDIQUÊS: SEGURANÇA PRIVADA E MONITORAMENTO INTELIGENTE COM RESPEITO À PRIVACIDADE

Rosalia Toledo Veiga Ometto[1]

1. INTRODUÇÃO

LGPD Sem Juridiquês é uma abordagem que aposta na simplicidade da linguagem, deixando de lado termos técnicos e rebuscados. O foco está em tornar as informações mais claras, acessíveis e úteis para quem precisa se adequar a uma legislação que é ao mesmo tempo inovadora e complexa.

LGPD Sem Juridiquês é, portanto, uma ponte entre a legislação e a prática, garantindo que a lei atinja sua finalidade principal: transformar a relação com os dados pessoais em algo seguro, ético e compreensível para todos os públicos.

Quando uma lei não é compreendida, torna-se inacessível para a maioria e acaba servindo apenas como um mecanismo de punição. A LGPD (Lei Geral de Proteção de Dados Pessoais - Lei 13.709/18) de fato prevê sanções para quem não a cumpre, mas seu verdadeiro objetivo vai muito além disso. Trata-se de estimular uma cultura de respeito à privacidade e à proteção de dados. Para

1 Bacharel (1992) e mestre (2004) em Direito Civil (FADUSP), especialista em Direito Digital, Inovação e Ética nos Negócios FIA (2022), especialista em Direito Empresarial PUC/SP (2010). Advogada desde 1993, atuante em LGPD, Direito Médico, Direito das Famílias, Direito Cooperativo e Compliance em Proteção de Dados Pessoais. Integrante do Programa Legal Consult da OAB/SP (2023) Membro das seguintes Comissões da OAB/SP: Privacidade, Proteção de Dados e Inteligência Artificial; Bioética e Biodireito; Direito Médico e da Saúde; da Mulher Advogada. Membro da Comissão Nacional de Família e Tecnologia do IBDFAM (IBDFAMTEC). Certificada Compliance em LGPD (CPC-PD/LEC) e Exin (PDPE - LGPD). Sócia fundadora da Ometto Advocacia (1998) em Piracicaba/SP. Encarregada de Dados Pessoais (DPO) externa de diversas empresas e entidades. Apaixonada por direitos da personalidade, design gráfico, *Visual Law*, das soluções criativas e da LGPD Sem Juridiquês. Autora de obras jurídicas.

que isso aconteça, é indispensável que ela seja bem entendida, aplicada com coerência e efetivamente incorporada ao cotidiano das pessoas e empresas.

2. SEGURANÇA PRIVADA. RISCOS, LIMITES E CUIDADOS COM A PRIVACIDADE.

No mundo contemporâneo todas as formas de viver coexistem: físico, digital, público e privado, profissional e pessoal. Os dados pessoais[2] são valiosos, as pessoas titulares têm direito à privacidade[3] e cuidado. Ao mesmo tempo é um mundo inseguro que busca soluções tecnológicas para proteção de perímetros e estabelecimento de vigilância[4]. Como se cuidar e se prevenir? Há muitas

2 "Entretanto, o ponto de partida de toda essa engrenagem [Big Data e Big Analytics] é a coleta de dados, cada vez mais maciça e muitas vezes realizada sem o consentimento e sem a ciência dos titulares desses dados. Se os cidadãos não conseguem sabem nem mesmo os dados que são coletados, têm dificuldades ainda maiores para compreender as inúmeras destinações que a eles pode ser ada e a extensão do impacto destas em suas vidas)." FRAZÃO, Ana. *Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da Lei Geral de Proteção de Dados*. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters RT, 2019, p. 26.

3 "Parte-se da análise da evolução do conceito de privacidade, que inicialmente era relacionado à ideia de exclusão de terceiros, para a atual acepção do termo como a possibilidade de cada indivíduo determinar as informações sobre si que merecem ser protegidas (...)" CUEVA, Ricardo Villas Bôas. *A proteção de dados pessoais na Jurisprudência do Superior Tribunal de Justiça*. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters RT, 2019, p. 86.

4 "A vigilância é um aspecto cada vez mais presente nas notícias diárias, o que reflete sua crescente importância em muitas esferas da vida. Mas, na verdade, a vigilância tem se expandido silenciosamente por muitas décadas e é uma característica básica do mundo moderno. À medida que esse mundo vem se transformando ao longo de sucessivas gerações, a vigilância assume características sempre em mutação. Hoje, as sociedades modernas parecem tão fluidas que faz sentido imaginar que elas estejam numa fase "líquida". Sempre em movimento, mas muitas vezes carecendo de certezas e de vínculos duráveis, os atuais cidadãos, trabalhadores, consumidores e viajantes também descobrem que seus movimen-

formas, mas o recorte desse texto é como as empresas de monitoramento e alarme ajudam nessa solução.

Como saber dos riscos que pessoas comuns estão sujeitas nesse tempo? Como os invasores se aproveitam do pouco conhecimento das pessoas para aplicar seus golpes? Algumas práticas para mitigar riscos de: invasores, agentes maliciosos, pessoas estelionatárias (conhecidas no mundo tecnológico como hackers e crackers). Qual é o objetivo desses ataques? Existem mundos subterrâneos que a maior parte das pessoas não conhece? Há sombras ao nosso redor? Tudo isso existe e precisa ser conhecido para ser combatido.

Fundamental é compreender que a privacidade[5]-[6] do indiví-

tos são monitorados, acompanhados e observados. A vigilância se insinua em estado líquido." BAUMAN, Zygmunt. Vigilância líquida. Rio de Janeiro: Zahar, 2024. E-book.

5 "A literatura atual sobre privacidade tem destacado, quase que de forma unânime, que a noção tradicional de privacidade, restrita à intimidade e ao direito de ser deixado só, não é mais compatível com a complexidade dos desafios inerentes à economia movida a dados e à vigilância. Daí a advertência de Rodotá, de que 'o problema da circulação das informações pessoais, portanto, não pode ser solucionado somente a partir das noções correntes de privacidade' e que 'privacidade não mais se confunde com o que é secreto', motivo pelo qual '(... pode-se dizer que hoje a sequência quantitativamente mais relevante é 'pessoa-informação-circulação-controle', e não mais apenas 'pessoa-informação-sigilo', em torno da qual foi construída a noção clássica de privacidade". FRAZÃO, Ana. *Objetivos e alcance da Lei Geral de Proteção de Dados*. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters RT, 2019, p. 105.

6 "Privacidade como autodeterminação informativa/existencial e reconhecimento da construção dinâmica da identidade pessoal conjugam-se, assim, como novas normas de manifestação da proteção jurídica da pessoa humana conta as ameaças de estigmatização e discriminação oriundas do desenvolvimento tecnológico. Com efeito, a principal preocupação com relação ao armazenamento e circulação de informações relativas à pessoa humana diz respeito à sua utilização para submetê-la a estigmas, viabilizando sua discriminação perante as demais. Entre os direitos dados relativos à pessoa, alguns são especialmente idôneos a facilitar processos sociais de exclusão e segregação, razão pela qual seu controle deve ser ainda mais rigoroso. Essa é a chave de leitura adequada para compreender a qualificação de dados pessoais sensíveis." KONDER, Carlos Nelson. *O tratamento de dados sensíveis à luz da Lei 13.709/2018.* In: TEPEDINO, Gustavo;

duo é um direito fundamental previsto na Constituição, bem como a proteção de dados pessoais, a inviolabilidade da intimidade, da honra e da imagem (CF, art. 5º, X, XI, XII e LXXVIII e LGPD, art. 2º, I e IV), considerados também direitos da personalidade[7]-[8].

Para facilitar a compreensão, segue esquema elaborado pela autora, a respeito da privacidade, intimidade e sua relação com a LGPD, na tríade pessoa – informação – sigilo:

PRIVACIDADE | É o oposto de Público. No cotidiano, privacidade é algo restrito ao público em geral. Na esfera privada há possibilidade de outras inseridas, como: esfera privada ampla (dados pessoais em contratos, parceiros com informações importantes para negócios, redes sociais públicas cujo conteúdo é definido pela própria pessoa, etc.), esfera privada restrita (pessoas do trabalho, pessoas amigas em geral, familiares distantes, redes sociais restritas definidas pela própria pessoa), esfera íntima (círculo restrito de pessoas escolhidas pela própria pessoa e suas redes sociais privativas com conteúdo controlado), esfera do segredo (só a pessoa o sabe).

FRAZÃO, Ana; OLIVA, Milena. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters RT, 2019, p. 451

7 A prof. Silmara J. Chinellato, destaca, ao comentar os artigos 11 e 12 do Código Civil, que os direitos da personalidade são inalienáveis, imprescritíveis e impenhoráveis e que qualquer ameaça ou lesão ao direito da personalidade gera possibilidade do exercício do direito de reclamar perdas e danos, inclusive em caráter preventivo, que a opção do legislador (CC, art. 12) foi pela enumeração não exaustiva dos direitos, ou seja, os direitos da personalidade não têm um rol taxativo. Traz que a classificação de Carlos Alberto Bittar de que direitos da personalidade são divididos em três categorias básicas: físicos, psíquicos e morais. Sobre Direitos da personalidade ver. CHINELLATO, Silmara Juny. Comentários ao art. 11 e 12 do CC (dos direitos da personalidade). In: MACHADO, Antonio Cláudio da Costa; _____. (Coords.) Código Civil Interpretado artigo por artigo. 15 ed. São Paulo: Ed. Manole, 2022. p. 116-117

8 Nas sábias, atualíssimas e oportunas palavras de Rubens Limongi França, "Direitos da personalidade são faculdades jurídicas cujo objeto são os diversos aspectos da própria pessoa do sujeito, bem como, as suas emanações e prolongamentos.", que começou suas análises sobre o tema em 1954, consolidando em coordenadas fundamentais do Direito da Personalidade no texto publicado em 1983, ainda ferramenta fundamental para o estudo da matéria. FRANÇA, Rubens Limongi. Direitos da personalidade: coordenadas fundamentais. Revista dos Tribunais, São Paulo, ano 567, p. 9, jan. 1983

INTIMIDADE | São esferas limitadas, pequenas. Intimidade significa escolher quem pode pertencer à sua esfera íntima (a pessoa estabelece os limites, seleciona, com cuidado, nas redes sociais sua intimidade pode vazar e se torna incontrolável a amplitude da divulgação). Só há intimidade plena se houver liberdade de seleção de quem pertence à sua esfera mais restrita. O segredo é essencialmente interno, de dentro da pessoa humana. Se houver compartilhamento, pode deixar de ser segredo, um risco a ser analisado. Segredo, sobretudo, deveria ser só algo que não prejudica a pessoa (se prejudica, pode ser um trauma ou mesmo um sinal de abuso sofrido) ou que não prejudique outros (se prejudica outros, pode ser um ilícito ou por ser algo antiético).

PRIVACIDADE e INTIMIDADE na LGPD | A LGPD traz obrigações para quem cuida de dados das pessoas, o foco é a defesa dos dados pessoais do ser humano vivo, ou pessoa titular de dados pessoais. Destaque: Há um direito em evidência, o da autodeterminação informativa, direito da pessoa titular de poder escolher, entre outros, de com quem ele quer compartilhar seus dados pessoais e determinar até quando. Significa que a pessoa titular estabelece os limites das informações na esfera da privacidade ampla e preserva sua intimidade, A lei traz algumas regras que agentes de tratamento (empresas em geral) podem cuidar dos dados pessoais porque está dentro de obrigação legal, contratual, proteção do crédito, tutela da saúde, etc. Há ainda a regra de ouro, o consentimento da pessoa titular (regra primordial da LGPD, apenas não utilizada quando há bases legais que excluem sua necessidade), que pode ser revogado a qualquer tempo. Sem atendimento às regras ninguém pode tratar os dados pessoais nos negócios.

A imagem abaixo, apresenta um esquema hierárquico elaborado pela autora, com cinco níveis de privacidade de dados, do mais público ao mais privado. A educação para a preservação da intimidade e do direito ao segredo é fundamental. Em resumo, o esquema demonstra um gradiente de privacidade, desde dados completamente acessíveis por qualquer pessoa até dados altamente protegidos e confidenciais.

E com esse parâmetro definido da privacidade, advém outra vertente fundamental na vigilância líquida, amplia-se para informação, circulação e controle. Não basta mais só proteger a intimidade e o segredo, é necessário cuidar para evitar circulação desnecessária de dados pessoais, e estabelecer controles de acesso a tais dados pessoais. Com isso segue-se para sugestões de ações, cuidados a serem aprimorados e diminuir o risco da exposição e utilização de forma diversa da finalidade inicial. Três visões dessa mesma área, da pessoa titular de dados pessoais; do poder público e a segurança do indivíduo e das empresas privadas de monitoramento e alarmes.

3. PESSOAS TITULARES DE DADOS PESSOAIS SABEM QUE ESTÃO SENDO VIGIADAS?

A grande massa da população ainda não tem alcance de que se vive atualmente em ambientes com alto risco de serem vigiadas e monitoradas sem sua percepção. O ponto de virada ocorreu quando surgiram os smartphones (celulares que tem câmeras, microfones, interatividade com a internet, geolocalização, compartilhamento

de dados, muitos pessoais e até sensíveis), são computadores portáteis.

Quem nunca aceitou uma política de privacidade de um novo aplicativo só para ir mais rápido? Quem nunca usou uma rede Wi-fi pública para não ter que usar seu pacote de dados? Quem nunca tirou uma foto sem se preocupar com quem estava ou fundo e publicou em redes sociais? Quem questiona para onde estão essas informações e para o que são utilizadas? Quem nunca recebeu uma oferta de um produto durante um passeio num centro de compras ou mesmo uma enxurrada de ofertas nas suas redes sociais? Mágica? Não, seus dados pessoais estão circulando.

Qual o grande desafio? Que as pessoas sabem que estão sendo vigiadas, inclusive com possibilidade de isso acontecer no seu ambiente privado restrito, IoT (internet das coisas), assistentes virtuais, câmeras dos seus celulares e até câmeras de circuito interno de monitoramento e reflitam. O limite entre o físico e o digital. por trás das telas e das câmeras há um outro mundo e lá que seus dados pessoais estão circulando.

Como promover a educação e conscientização da pessoa titular a exercer a autodeterminação informativa, compreendendo por onde seus dados pessoais transitam, quem tem acesso a eles, e como estabelecer limites. Isso é desafiador.

Essa é uma tarefa de todas as pessoas físicas, mas sobretudo das pessoas jurídicas, dos negócios que tem muito mais poder econômico e informacional do que os indivíduos. E na perspectiva do Código de Defesa do Consumidor e da LGPD, o indivíduo é que precisa receber toda a informação suficientemente clara e transparente, ele é o elo mais frágil dessa cadeia de transmissão de dados, sobretudo, dados pessoais.

Todo negócio que tem proveito econômico é um agente de tratamento, ou seja, responsável pela educação das pessoas titulares de dados pessoais. O ônus é do controlador de dados pessoais, quer seja no ambiente público ou privado.

Também é tarefa da ANPD (Autoridade Nacional de Proteção de Dados) promover a cultura e a informação necessária para

que a pessoa titular possa exercer seus direitos na sua plenitude.

De forma suscinta, traz-se alguns pontos-chave:

COLETA DE *DADOS: localização, muitos aplicativos rastreiam a localização do indivíduo. Microfone e Câmeras, vários aplicativos podem acessar o microfone e a sua câmera também, e por vezes podem até gravar sons e imagens. Informações de contatos, histórico de navegação, até dados biométricos podem ser coletados*

COLETA DE DADOS: localização, muitos aplicativos rastreiam a localização do indivíduo. Microfone e Câmeras, vários aplicativos podem acessar o microfone e a sua câmera também, e por vezes podem até gravar sons e imagens. Informações de contatos, histórico de navegação, até dados biométricos podem ser coletados.

PERMISSÕES: nem sempre é necessário fornecer todas as permissões, é possível customizar, limitar, mas isso dá trabalho, e muitas pessoas não sabem que estão sendo vigiadas e elas mesmas que deram a permissão. Isso pode e deve ser revisto pelas pessoas e cobrado das empresas essa transparência cada vez maior.

REDES WI-FI: tenha cuidado, normalmente essas redes públicas e gratuitas tem pouca proteção e podem ser um "excelente" campo para hacker e crackers. Evite o máximo que puder, ou limite o uso o mínimo necessário.

ATUALIZE sempre seus aplicativos e celulares, isso é prevenção, pois normalmente incluem correções de segurança que foram descobertas e melhoradas. Desative rastreadores, leia políticas de privacidade.

*ATENÇÃO: As pessoas devem ficar muito atentas às câmeras de vigilância, muitas tem possibilidade de captar som além da imagem, e até podem realizar reconhecimento facial. Questione sobre a política de proteção de dados da empresa pública ou privada. E nas questões de segurança pública, ainda que não aplicável a LGPD, é necessário cobrar como pessoa cidadã que melhorem a captação das imagens e que sejam revistos os algoritmos discriminatóri*os.

4. ENTRE O PÚBLICO E O PRIVADO. QUAL O LIMITE E QUAIS OS APRENDIZADOS? PREVENÇÃO DE VIESES RACISTAS EM ALGORITMOS.

A utilização de algoritmos em sistemas de monitoramento pode inadvertidamente perpetuar vieses racistas, especialmente em tecnologias de reconhecimento facial. Estudos indicam que

esses sistemas apresentam taxas de erro mais altas ao identificar indivíduos de pele mais escura, o que pode levar a discriminações[9]. É crucial que as políticas públicas revejam essa dinâmica e revisem seus algoritmos e utilizem bases de dados diversificadas para treinar seus sistemas, minimizando assim o risco de vieses.

É fundamental que a Segurança Pública, as investigações criminais sejam realizadas a não perpetuar os estigmas e preconceitos que as populações socialmente menos favorecidas não continuam a serem marginalizadas e criminalizadas apenas pela sua localização (seu CEP pode determinar, inclusive, a seleção de uma vaga de emprego), pela sua etnia, pelo seu gênero, pela sua opção sexual, pela sua cor, pelo seu poder aquisitivo.

Isso de faz com investimento público, conscientização dos direitos das pessoas, políticas públicas e cobrança da sociedade.

5. SEGURANÇA PRIVADA. RISCOS, LIMITES E CUIDADOS COM A PRIVACIDADE

O tratamento inadequado de dados pessoais pode causar riscos diversos, como vazamento de informações, uso indevido de dados e discriminação[10]. Para empresas de monitoramento, que fre-

9 Eu não posso me dar ao luxo de lutar por uma forma de opressão apenas. Não posso me permitir acreditar que ser livre de intolerância é um direito de um grupo particular. E eu não posso tomar a liberdade de escolher entre as frentes nas quais devo batalhar contra essas forças de discriminação, onde quer que elas apareçam para me destruir." LORDE, Audre. Não existe hierarquia de opressão. 1983. https://www.geledes.org.br/nao-existe-hierarquia-de-opressao/ Acesso em 12 de dezembro de 2024

10 "Em relatório realizado pela Rede Observatório da Segurança Pública no ano de 2019, mais de 90% das prisões realizadas naquele ano com ouso de reconhecimento facial no Brasil foram de pessoas negras (NUNES, 2019). Intelectuais e ativistas questionam o uso da tecnologia, apontando que em razão de vieses racistas/de gênero/idade/identidade de gênero, o reconhecimento facial leva a verdadeiros danos para pessoas negras, mulheres, idoso e transsexuais/travestis – em especial no seu uso na segurança pública e no controle imigratório. Ao mesmo tempo, por estarem livres do escrutínio e da violência do monitoramento, a tecnologia reafirma privilégio e acessos dos detentores do poder: o homem branco cisheteronormativo." SALOMÃO, Elizandra; MONTEIRO, Pedro Diogo Carvalho.

quentemente utilizam sistemas de vigilância por vídeo e tecnologias de reconhecimento facial, esses riscos são amplificados. Quais suas responsabilidades e quais precauções devem ser atendidas?

Certo que imagem é dado pessoal comum, mas pode se tornar sensível dependendo da tecnologia empregada, que pode ser reconhecimento facial, reconhecimento de voz, reconhecimento de íris, uso de inteligência artificial, incluindo a generativa, entre outras tantas tecnologias existentes e que virão a ser criadas ou desenvolvidas.

Para mitigar os riscos, as empresas de monitoramento e alarmes devem adotar práticas robustas de segurança da informação, incluindo a implementação de políticas claras de privacidade, treinamento contínuo de seu time e a realização de avaliações de impacto sobre a proteção de dados, sempre considerando a necessidade da privacidade desde a concepção dos serviços (Privacy by Design).

Os contratos devem ser didáticos o suficiente para que as pessoas que contratarem os serviços de monitoramento e alarme saibam qual a capacidade técnica dos equipamentos, se eles captam som ou não, se tem possibilidade de reconhecimento facial ou não, se tem utilização de inteligência artificial, e como estão configurados todos esses sistemas.

Importante também é a conscientização da pessoa contratante dos serviços da sua responsabilidade no armazenamento e divulgação das imagens recebidas, porque em algumas oportunidades o armazenamento é realizado pela pessoa contratante apenas, se fora compartilhado o armazenamento conhecer o limite de responsabilidade de cada parte, tempo de armazenamento, e modos de descarte seguro.

Limitar ao máximo o número de pessoas que possam ter acesso a esses dados, se colaboradores, que seus contratos de trabalho prevejam cláusulas de confidencialidade e de sigilo, com im-

---

Entre aparelhos de repressão e a quilombagem: vigilância e contra-vigilância negra a partir do olhar de Clovis Moura. In: BARROS, Thiane Neves; SILVA, Tarcízio. Griots e Tecnologias Digitais. São Paulo: LiteraRUA, p.92.

putação de penalidades, até mesmo de demissão por justa causa, alicerçadas por políticas de condutas previamente estabelecidas pelas partes de lado a lado.

A importância da conscientização das partes envolvidas do cuidado na instalação dos dispositivos que façam a captação de imagens, sons, além de dados biométricos e reconhecimento facial, por exemplo, bem como, da qualidade dos cabos e equipamentos, configurações, com os melhores controles de segurança da informação possíveis.

É essencial educar as pessoas de que o monitoramento é invasivo, devendo ser realizado corretamente e divulgado de forma ostensiva, informando que o ambiente está monitorado por câmeras, com captação de sons ou outros atributos específicos. A atividade empresarial de monitoramento, alarme e vigilância precisa ser ética e responsável. Destaca-se alguns pontos importantes para o monitoramento de ambientes internos, sobretudo:

PRO*PÓSITO E NECESSIDADE DO MONITORAMENTO. Finalidade específica, explícitas e legítimas (LGPD, art. 6º, I). Empresas devem justificar o uso de câmeras e sistemas de vigilância para proteção patrimonial ou segurança. Minimização de Dados Pessoais: Apenas colete informações estritamente necessárias, como imagens em locais com risco de furto ou acesso restrito, com o nível de tecnologia condizente com a finalidade. Será que tudo precisa de reconhecimento facial? Não tem outra alternativa menos invasiva?*

LOCALIZAÇÃO DAS CÂMERAS NAS EMPRESAS. Zonas Permitidas: Locais comuns, como recepções, corredores e áreas de trabalho coletivo. Zonas Proibidas: Banheiros, vestiários e áreas de descanso que comprometam a privacidade dos indivíduos (art. 6º, IX - direitos fundamentais).

LOCALIZAÇÃO DAS CÂMERAS EM RESIDÊNCIAS PRIVADAS. Ambientes externos. No perímetro atenção se não invade a privacidade de vizinhos. Na área de lazer ou espaços de convivência, alerta e cuidado para que as pessoas tenham conhecimento que estão sendo monitoradas, para evitar questões de violação da privacidade (como pessoas nuas, com roupas íntimas nessas áreas, visitantes, por exemplo). Nesse caso a parte contratante deverá assinar um termo de responsabilidade da divulgação entre seus familiares e convidados sobre a

questão do monitoramento e que não responsabiliza a empresa por ter acesso a imagem dessa natureza. Zonas desaconselhadas: quartos, banheiros, área íntima. Sempre necessário um termo de que a pessoa contratante dos serviços de monitoramento e vigilância tenha sido informada e desaconselhada a instalar monitoramento nesses ambientes, assumindo a responsabilidade por essa contratação.

INFORMAÇÕES ÀS PESSOAS TITULARES DE DADOS PESSOAIS. Transparência: É obrigatório informar as pessoas que há monitoramento naquele espaço, inclusive se há captação de sons e outras características específicas. Fundamental que haja avisos visíveis e claros, como placas indicando "Ambiente Monitorado por vídeo e captação de som" com uma política de privacidade detalhada acessível. Consentimento: Para monitoramento em residências, é recomendável obter o consentimento explícito de residentes ou pessoas empregadas nas residências ou, no mínimo, da pessoa contratante assumindo o compromisso e a responsabilidade pela divulgação do monitoramento. Alerta especial para ambientes com crianças e adolescentes, sempre atender ao melhor interesse do menor.

RISCOS CONHECIDOS. Invasão de Privacidade. Monitoramento excessivo pode gerar desconforto ou ser percebido como uma violação de direitos fundamentais, em que judicialmente casos envolvendo vigilância não consentida podem resultar em indenizações por danos morais.

VAZAMENTO DE DADOS PESSOAIS. Câmeras conectadas à internet (IoT) são vulneráveis a invasões, redes WI-FI com senhas fracas e amplamente compartilhada com diversas pessoas aumenta a possibilidade de o acesso indevido por terceiros e com isso graves consequências, inclusive de extorsão por estelionatários.

USO INDEVIDO DE IMAGENS. Dados pessoais captados podem ser mal utilizados, seja por pessoas internas ou externas ao local do monitoramento. Se for por pessoas colaboradoras a empregadora tem responsabilidade objetiva pela ação de seus subordinados, tamanha a sua responsabilidade.

DISCRIMINAÇÃO E PRECONCEITO. Algoritmos de reconhecimento facial podem introduzir vieses que afetam negativamente grupos específicos, refletindo a sociedade que é racista, misógina e discriminatória.

BOAS PRÁTICAS. Relatório de Impacto à Proteção de Dados (RPID) Realizar análises periódicas para identificar riscos associados ao monitoramento e implementar medidas preventivas. Segurança da Informação. Adotar medidas , sempre que possível, como criptografia, firewalls e sistemas de autenticação robustos para proteger as gravações. Gestão do Ciclo de Vida dos Dados. Definir prazos de armazenamentos compatíveis com a finalidade do monitoramento, constando inclusive dos contratos de prestação de serviços, com a devida eliminação segura dos dados pessoais após o período estabelecido. Controle de Acessos. Restringir o acesso às gravações a pessoas estritamente autorizadas. Treinamento e Educação. Realizar treinamento de todas as pessoas envolvidas no processo e responsáveis pelo monitoramento que entendam os requisitos legais e as melhores práticas.

PROPOSTAS DE MITIGAÇÃO. Desenvolvimento de Políticas Internas. Criar documentos internos sobre o uso do monitoramento, com objetivos, procedimentos e responsabilidades. Implementação de Tecnologia Ética. Dar prioridade a sistemas que utilizem dados anonimizados ou soluções que evitem capturas invasivas. Supervisão e Auditoria. Realizar auditorias periódicas para verificar a conformidade com a LGPD e evitar abusos. Monitoramento Alternativo. Considerar o uso de sensores de movimento ou alarmes que não capturem imagens como soluções menos invasivas. Acompanhamento da pessoa encarregada de dados pessoais. Contrate um profissional especializado em proteção de dados (DPO) para acompanhar e adaptar os processos de monitoramento às exigências legais.

6. CONCLUSÕES

O monitoramento em ambientes internos, quando bem estruturado, pode promover segurança sem sacrificar a privacidade. Empresas e residências devem aliar tecnologia e boas práticas à conformidade legal, garantindo que as operações sejam éticas e transparentes. A implementação cuidadosa não apenas mitiga riscos jurídicos, mas também fortalece a confiança dos indivíduos monitorados.

A conformidade com a LGPD não é apenas uma obrigação legal, mas também uma oportunidade para as empresas de monitoramento e alarmes reforçarem a confiança das pessoas clientes e do mercado. Ao adotar medidas proativas de proteção de dados

pessoais e garantir a equidade em seus sistemas algorítmicos, essas empresas contribuem para uma sociedade mais justa e segura.

A utilização de treinamentos e contratos na linguagem LGPD Sem Juridiquês, a função social do contrato e das ações empresariais contribuem significativamente na construção da consciência da importância do conhecimento da utilização de dados pessoais nos negócios. Além de proporcionar uma maneira diferente e eficaz para o fomento da cultura da privacidade.

Por fim, transformar o complexo em simples, sem perder a profundidade, significa traduzir uma linguagem técnica densa em termos claros, acessíveis e compreensíveis, que possam ser aplicados pelo maior número possível de pessoas. É um compromisso com a responsabilidade social, ética e legal, integrando a privacidade a todos os setores, negócios e aspectos da vida cotidiana.

REFERÊNCIAS

BAUMAN, Zygmunt. Vigilância Líquida (Portuguese Edition). Zahar. Edição do Kindle.

CHINELLATO, Silmara Juny. Comentários ao art. 11 e 12 do CC (dos direitos da personalidade). In: MACHADO, Antonio Cláudio da Costa; _____. (Coords.) Código Civil Interpretado artigo por artigo**.** 15 ed. São Paulo: Ed. Manole, 2022. p. 116-127.

CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na Jurisprudência do Superior Tribunal de Justiça. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters RT, 2019, p. 85-98.

FRANÇA, Rubens Limongi. Direitos da personalidade: coordenadas fundamentais. *Revista dos Tribunais*, São Paulo, ano 567, p. 9-16, jan. 1983

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena (Orgs.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.* São Paulo: Thomson Reuters RT, 2019. p. 23-52.

_____. Objetivos e alcance da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters RT, 2019, p. 99-129.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters RT, 2019, p. 445-463

LORDE, Audre. Não existe hierarquia de opressão. Geledés, 1983. Disponível em: https://www.geledes.org.br/nao-existe-hierarquia-de-opressao/. Acesso em: 12 dez. 2024.

SALOMÃO, Elizandra; MONTEIRO, Pedro Diogo Carvalho. *Entre aparelhos de repressão e a quilombagem: vigilância e contra-vigilância negra a partir do olhar de Clovis Moura*. In: BARROS, Thiane Neves; SILVA, Tarcízio. Griots e Tecnologias Digitais. São Paulo: LiteraRUA, p. 81-94.