JUNHO 2021

GLOSSÁRIO COMENTADO

INTRODUÇÃO À LGPD PARA SEGURANÇA PATRIMONIAL

criação
PATRICIA PUNDER
FABIO DAVID

Sumário

Patrícia Punder

Profissional de Compliance com sólida experiência no Brasil e América Latina, com mais de 12 anos de experiência na implementação e gestão de programas de Compliance, gestão de riscos e governança corporativa. Certificada pela ECOA, Fordham University, George Washington Law University e CPC-A. Uma das autoras do Manual de Compliance/2019 e Compliance – Além do Manual/2020, ambos publicados pela LEC. Coautora do Manual de Compliance, onde desenvolveu capítulo sobre o tema ESG, que será publicado pela ComplianceLab no segundo semestre de 2021.

Atuou em diversas empresas nacionais e internacionais, com foco na implementação de Programas de Compliance, Governança, LGPD, investigações envolvendo DOJ/SEC/CGU/CADE e gestão de crises reputacionais. Professora no MBA da UFSCAR, LEC, Tecnológico de Monterrey e Universidade do Panamá. Tem atuação bastante relevante em congressos nacionais e internacionais, além de contribuir com a elaboração de artigos sobre temas relevantes publicados em jornais, websites e mídias de grande circulação nacional e internacional.

Fundadora do escritório Punder Advogados desde 2016, com foco em Compliance, Governança, Riscos, Gestão Reputacional, LGPD e ESG. Possui uma equipe com alta qualidade e expertise nos temas e parcerias internacionais que podem ajudar de forma customizada os clientes, que assim necessitam.

O escritório Punder Advogados firmou parceria internacional com a F&C Consulting Group em 2020, bem como com a empresa nacional focada e treinamentos/cursos denominada de Pro Performance em 2021.

Fabio David

Fabio David tem experiência internacional como militar e foi comandante de Esquadrão no Exército Israelense na Brigada de Engenharia de Combate, é formado como agente governamental pelo Estado de Israel na Diretoria de Segurança Aeroportuária e Aviação Civil (Aeroporto Ben Gurion), participou do Programa de segurança VIP nacional para o Ex-Presidente do Panamá (Ricardo Martinelli), ajudou na formação da equipe de segurança pessoal de Família ameaçada na Eslováquia (Bratislava).

Em retorno ao Brasil (a partir de 2010) realizou o trabalho de Coordenador de Segurança Patrimonial para a Fundação Safra, projetos de consultoria como CLT e PJ para JHSF (Fazenda Boa VIsta), Cyrela, BRC, Allianz Seguros, Interfile, Condomínios diversos, Tecnisa S.A., entre outros. Em 2015 realizou o curso de Compliance no Insper pois lhe foram exigidas adequações de compliance para segurança patrimonial pelos seus clientes e terceiros, assim realizando as primeiras adequações no contexto brasileiro.

Em sua passagem pelo Dia Brasil Supermercados como Supervisor de Projetos do Departamento de Riscos (2016 a 2019) foi nomeado o champion de Compliance da diretoria de operações, o que levou a participar da 1o Turma do MBA de Riscos de Fraude e Compliance da FIA após ser graduado pela Anhembi Morumbi como Administrador de empresas.

Realizou o único TCC de LGPD voltado a Segurança Patrimonial com a pergunta: “Qual o Impacto da LGPD para a Indústria de câmeras IPs”. Se especializou em LGPD pelo Data Privacy Brasil visando atender ao mercado de segurança patrimonial e prestar o serviço de DPO.

Atualmente adequa departamentos de segurança para LGPD, desenvolve projetos de LGPD em empresas de terceirização de serviços, condomínios empresariais e residenciais.

Introdução

A proposta deste Glossário é ajudar os profissionais de Segurança Patrimonial, Síndicos Profissionais, Gestores de Condomínio e compradores de equipamentos e serviços de segurança a se adequarem com mais facilidade a LGPD.

Dessa forma, contribuímos para que possam ter acesso à informação de modo rápido e direto, trazendo uma comunicação mais próxima da realidade do dia-a-dia para todos os profissionais de segurança patrimonial.

É importante ressaltar que a Lei não foi escrita pensando no processo de Segurança Patrimonial, então existe a necessidade de serem realizadas interpretações para a adequação correta neste mercado, que possui peculiaridades próprias.

A LEI <> OS PILARES

"respeito e boa-fé devem estar explícitos em nossa mudança de procedimento e formulários.".

A LGPD se relaciona com a Segurança Patrimonial em seus 4 pilares (Segurança Física, Segurança Eletrônica, Procedimentos e RH de Segurança).

Segurança física: Muita interação com arquitetos e designers, esse pilar é muitas vezes o mais conflitante para um projeto de segurança. As paredes de vidro que são usadas como divisórias entre salas em um escritório, por exemplo, muitas vezes possibilitam a visualização do conteúdo das telas dos computadores pelas pessoas que estão na outra sala, invadindo sua privacidade.
Em escritórios as paredes são de drywall e/ou não acústicas possibilitam ouvir o que acontece do outro lado da parede, esta vulnerabilidade não é considerada por nenhum departamento atualmente e extremamente importante para uma adequação correta.

Segurança Eletrônica: O mais latente nesta relação, as câmeras e controles de acesso são meios de coleta efetiva de dados pessoais, os dados pessoais coletados pelas câmeras são dados sensíveis, como etnia, opção religiosa, opção sexual e outros. Esses dados são armazenados em nuvem ou DVR local, transmitidos para celulares e outros equipamentos via internet. A Segurança e Proteção desses dados está estipulada na lei e devem ser considerados em todo o ambiente de segurança.

Procedimentos: A forma de escrita e os formulários de cadastro (físico ou eletrônico) utilizados nos controles de acesso, são exemplos desta relação com a LGPD. A LGPD tem a expectativa de respeito ao dado pessoal que não se tinha antes. Esse respeito e boa-fé devem estar explícitos em nossa mudança de procedimento e formulários.

RH de Segurança: As empresas são feitas de pessoas e essas pessoas tratam dados de nossos clientes, todos os atores nesta relação são contemplados na LGPD. O treinamento de equipe, forma de abordagem e postura são itens esperados na Lei para uma relação mais respeitosa com nossos clientes e das nossas empresas com nossos funcionários.

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

Comentário: Nenhum destes itens abaixo podem ser abraçados pela Segurança Patrimonial, eles foram escritos apenas para Segurança Pública e Segurança Nacional. O item "D" (investigação) é polêmico, mas se aplica exclusivamente a investigações realizadas pelas forças públicas também. Mesmo em um processo de investigação particular onde os órgãos públicos sejam envolvidos posteriormente, esse Artigo só entra em vigor após se "passar o bastão" para o órgão público efetivamente e formalmente.

III - realizado para fins exclusivos de:
a) segurança pública;
b) defesa nacional;
c) segurança do Estado; ou
d) atividades de investigação e repressão de infrações penais; ou

Art. 5º Para os fins desta Lei, considera-se:

Comentário: este artigo traz as definições dos termos da lei. Nós comentamos dando exemplos e relacionado com a realidade da Segurança Patrimonial para facilitar e ajudar no entendimento do relacionamento do item com a Segurança Patrimonial.

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Comentário: Câmeras coletam todos os dados relacionados acima, e a cada segundo de aproximação do indivíduo se tem mais volume de dados e mais profundidade no dado.

III - dado anonimizado: dado da pessoa que não possibilite a identificação dela, considerando a utilização de recursos técnicos e/ou tecnológicos razoáveis e disponíveis na ocasião de seu tratamento;
Comentário: Máscaras e outros desenvolvimentos tecnológicos são ótimos recursos para se atender a este item. A palavra razoável nos trás um ponto de atenção, pois precisamos saber que o entendimento de segurança para os profissionais da área não é o mesmo que o do Juiz.

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
Comentário: O DVR, nuvem, PenDrive, HD externo, memória do celular e backup do whatsapp são exemplos de banco de dados. Quantas vezes não foram salvas imagens e cadastros em PenDrive para arquivo ou mesmo provas de processo de demissão? Quantas vezes não foram tiradas fotos das telas dos computadores e envio por whatsapp para agilizar procedimentos? O arquivo morto também entra neste item, sendo assim armários e outros tipos de gaveteiros precisam ser considerados.

V - titular: pessoa de quem o dado pessoal é tratado;
Comentário: Um exemplo para entendermos o item é: Em um monitoramento por CFTV, as imagens dos titulares (ou pessoas) são tratadas pelos operadores de central.

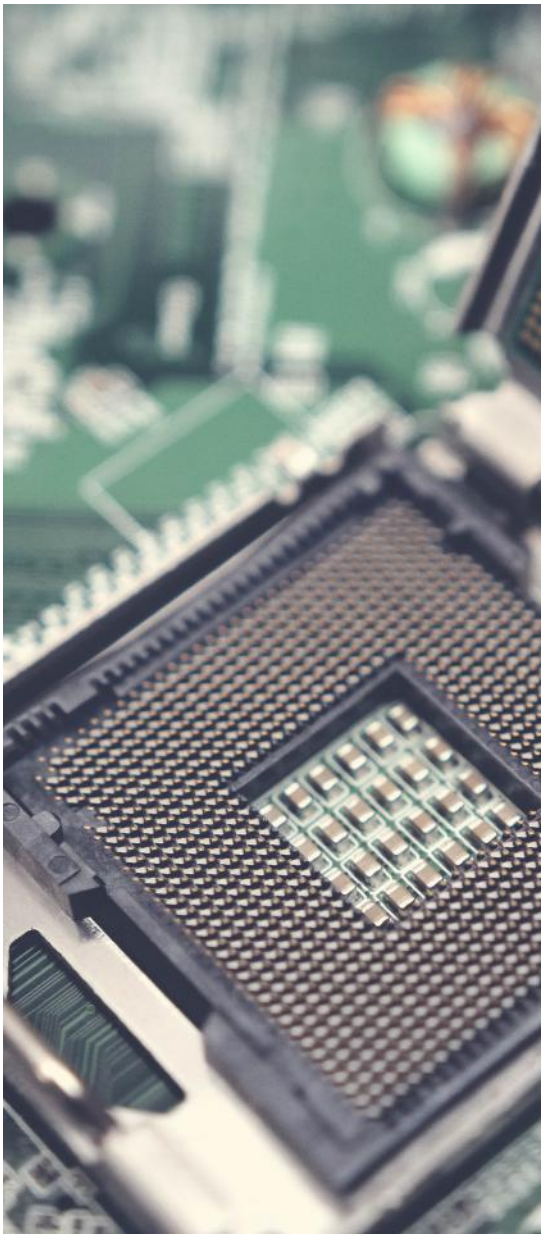
VI - controlador: pessoa física ou pessoa jurídica, órgão público ou privado, que tomas as decisões sobre o tratamento de dados pessoais;
Comentário: A empresa contratante do serviço de segurança é o controlador, ou seja o tomador do serviço. Quando se compra um kit de câmeras em uma loja de departamento para ser instalada em sua casa, apartamento ou loja, você se torna o controlador também.
IMPORTANTE: Esse item pode ser discutível em um ponto da lei que deve ser especialmente citado, onde em caso de uma central de segurança, dependendo do entendimento do Juiz, a empresa contratada pode ser equiparada como controladora dos dados e assumir o ônus pelas decisões caso haja infração pela contratada (operador).

VII - **operador:** pessoa física ou pessoa jurídica, órgão público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
Comentário: É empresa contratada (terceirizada) de serviço de segurança é o operador.
IMPORTANTE: Esse item pode ser discutível um único ponto da lei que deve ser especialmente citado, onde em caso de uma central de segurança, dependendo do entendimento do Juiz, a empresa contratada pode ser equiparada como controladora dos dados e assumir o ônus pelas decisões caso haja infração pela contratada (operador). .

VIII - **encarregado:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
Comentário: Pode ser uma pessoa interna ou externa, CLT ou PJ, mas as grandes características são: relacionamento com a ANPD, entender do business, entender da lei, entender de tecnologia. Essas atribuições são para que ele / ela consiga se comunicar com todos, representar a empresa no tema, treinar a todos e principalmente orientar a alta administração.

IX - **agentes de tratamento:** o controlador e o operador;
Comentário: Efetivamente são eles quem tratam os dados, tem a responsabilidade sobre o que é realizado. Em uma situação de recepção de prédio, a administradora do prédio é o controlador e a empresa terceirizada de recepção o operador, os dados dos clientes que acessam o prédio estão dentro da responsabilidade e tratamento de ambos.

OBS.: O encarregado (Data Protection Officer ou DPO) não é agente de tratamento, suas atribuições são outras. (vide VIII)



X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
Comentário: Muito importante deixar clara toda essa lista de itens chamada tratamento, as atividades desenvolvidas pela segurança podem ser vistas como uma das opções acima. O monitoramento, gravação e cadastramento são exemplos de tratamento, o VMD (vídeo movement detection) quando a câmera grava apenas quando há movimento, não é um redutor de pena e também pode ser entendido como um ampliador da pena, por deixar a gravação por mais tempo armazenada.

XI - anonimização: utilização de meios técnicos e tecnológicos razoáveis, disponíveis no momento do tratamento, por meio dos quais não conseguimos identificar ou associar o dado a uma pessoa direta ou indiretamente;
Comentário: é o processo para se chegar no dado anonimizado, item III. Máscaras e outras tecnologias são entendidas e analisadas para que esse processo seja de anonimização seja válido ou não perante a lei. É importante entender que essas tecnologias precisam ser efetivas como um todo (rosto, corpo, ...).

XII - consentimento: é o ato em que a pessoa / titular consente o tratamento do seu próprio dado. Esse consentimento precisa seguir algumas características como: ser livre, informado e inequívoco. Importante frisar que é para uma "finalidade determinada" e não generalizada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
Comentário: Este é um caso referente a sanções da lei, como exemplo podemos trazer o bloqueio de tratamento de dados pessoais de um departamento de segurança, isso significa parar de gravar, monitorar, realizar o controle de acesso e outras possibilidades temporariamente.

XIV - eliminação: é a exclusão / eliminação total dos dados armazenados. A lei não define como esse processo deve ocorrer;
Comentário: o exemplo mais tradicional é o tempo de gravação de DVR, que elimina sozinho o 1o dia gravado dado espaço para o dia atual. Esta eliminação automática, pode ser entendida como insuficiente caso não haja um trabalho de verificação posterior a eliminação.

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
Comentário: Pouco visto na segurança mas com certa frequência em multinacionais, os datacenters estão em diferentes países, nossas imagens de CFTV, dados de cadastros e controles de acesso podem ser globais, estes dados podem estar sendo processados em outros países, o envio de imagens como parte de um reporte para certas investigações também pode ser um bom exemplo.

XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
Comentário: pode ser tido como exemplo a operação de uma central de segurança interna a uma empresa, onde os dados são compartilhados entre o contratante e a contratada, entre a recepção do prédio e a recepção de uma empresa ou na utilização de softwares para realização de interação entre relatórios eletrônicos.

XVII - relatório de impacto à proteção de dados pessoais: é o documento mais abrangente da LGPD, além de ser um documento oficial para reporte de tratamento de dados para a ANPD. Ele contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
Comentário: Em um dos documentos escritos pelo Ministério da Economia onde ele orienta as demais agências do Governo, ele indica a possível necessidade de relatórios de impacto específicos para algumas áreas, ficando a critério da empresa. A análise de necessidade de um RIPD SEG é de grande valia e recomendável tanto para órgãos governamentais como para o setor privado.
É importante lembrar que não temos ainda o Guia de Segurança Patrimonial elaborado pela ANPD, que virá a partir de 2023, então ter a ciência da possível necessidade de um RIPD SEG é indispensável.

XIX - autoridade nacional: É responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional
Comentário: É a ANPD (Agência Nacional de Proteção de Dados) que tem seu calendário bienal estipulado e deve elaborar posteriormente os guias setoriais sendo um deles o de Segurança Patrimonial.

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

Comentário: A lei espera que cada ponto de câmera e ponto de controle de acesso, por exemplo, deva ser justificado com estes 10 princípios, pois são eles que regem a privacidade de dados de todos.

No título ele traz o "11o princípio" (boa-fé), que falamos no item procedimento e pode ser entendido como “princípio dos princípios”. É esperado pela LGPD que seja considerada a boa-fé em todos os momentos da operação de segurança patrimonial.

I - finalidade: Para entender esse princípio precisamos nos perguntar: Para qual objetivo final eu preciso disso (câmera, biometria, procedimento, pessoa)? Para estarmos abraçados por ele, precisamos cumprir alguns pontos: propósitos legítimos, propósitos específicos, propósitos explícitos e informados ao titular. Porém ele amarra esses pontos limitando o tratamento dizendo: sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: esse princípio é uma triangulação entre o tratamento, finalidades informadas e o contexto do tratamento. Este princípio traz o balanceamento entre os três pontos para que sejam protegidas as informações. Como exemplo podemos ter uma câmera que coleta os dados pessoais, trata eles. Este tratamento precisa ser informado para as pessoas naquele ambiente, bem como entender o local da coleta de dados e qual a relação com as pessoas.

III - necessidade: Fazer um exercício interno com a seguinte pergunta: estou usando o mínimo necessário de informação para que consiga atingir a minha finalidade? Caso a resposta seja sim, estamos cumprindo este princípio.

IV - livre acesso: garantir às pessoas um canal de comunicação para que possam realizar a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantir aos titulares que os dados pessoais tratados são exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantir aos titulares que os dados tratados são claros, precisos e facilmente acessíveis e os respectivos agentes de tratamento (contratante e contratada), não precisando serem abertos os segredos comercial e industrial;

VII - segurança: utilização de medidas 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 difusão;
Comentário: quais medidas de segurança meu TI / Integrador adotou impedir o acesso de hackers ao meu CFTV? Quais procedimentos administrativos proativos eu tenho? Qual foi a última manutenção?

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
Comentário: quais medidas de prevenção a empresa adotou para situações de crise após o dado ser vazado (por exemplo)? Quais procedimentos administrativos proativos eu tenho para esta crise?

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
Comentário: ótimo exemplo e muito atual, são as tecnologias de reconhecimento facial, onde algumas identificam as pessoas com uma acuracidade menor, como por exemplo: a acuracidade de identificação de pessoas brancas é de 95% e para pessoas negras e asiáticos é de 75% em média.

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a auditoria de processos de privacidade de dados e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.
Comentário: demonstrar por meio de relatórios, gráficos e controles que o processo de Segurança Patrimonial é eficaz e auditado.

Nossos contatos

patricia-punder-69b8b0
patricia@punder.adv.br
(11) 9.9293.9421

fabiodavid.consulting
fabio-davidt
fd@fabiodavid.consulting
linktr.ee/fabiodavid.consulting
(11) 9.6494.2618