

4<sup>a</sup> edição  
2024  
REVISADA E  
ATUALIZADA



# LOGO HERO



PRISMA  
BOOKS

Fabrizio Rodrigues

© PRISMA

Todos os direitos reservados e protegidos pela Lei nº 9.610, de 10/02/1998.

Nenhuma parte deste material poderá ser reproduzido, nem transmitido, sem autorização prévia por escrito do autor, sejam quais forem os meios: fotográficos, eletrônicos, mecânicos, gravação ou quaisquer outros.

Edição

Fabrizio Rodrigues

Revisão

Fabrizio Rodrigues

Capa

Fabrizio Rodrigues

Caso você deseje submeter alguma errata ou sugestão, acesse:

GitHub (página deste e-book LGPD HERO)

<https://github.com/fabriziorodrigues/ebook-lgpd-hero>

[2024] - v4.0.0

4<sup>a</sup> edição - 2024

3<sup>a</sup> edição - 2021

2<sup>a</sup> edição - 2020

1<sup>a</sup> edição - 2020

PRISMA Services

[prismaservices.io](http://prismaservices.io)

# SUMÁRIO

SUMÁRIO.....	3
INTRODUÇÃO.....	9
PARA QUEM É ESTE E-BOOK.....	11
SOBRE O AUTOR.....	12
SOBRE O E-BOOK.....	14
AGRADECIMENTOS.....	16
RESUMO DOS CAPÍTULOS.....	17
<b>1. INTRODUÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS.....</b>	<b>20</b>
A LGPD.....	22
O QUE SÃO DADOS À LGPD?.....	23
AGENTES DE TRATAMENTO.....	30
AGENTES DE TRATAMENTO - CONTROLADOR E OPERADOR.....	31
AGENTES DE TRATAMENTO - ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS....	32
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD).....	34
CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE (CNPD)....	36
TRATAMENTO DE DADOS.....	37
QUAL É O OBJETIVO DA LGPD PARA SUA ORGANIZAÇÃO?.....	38
QUAIS OS RISCOS AO NÃO SE ADEQUAR ÀS CONFORMIDADES DA LGPD?.....	39
DEMAIS CONSIDERAÇÕES E CONCEITOS RELACIONADOS A LEI.....	40
QUAIS SERÃO AS MUDANÇAS TRAZIDAS PELA LGPD?.....	43
O QUE EU PRECISO SABER PARA TRATAR OS DADOS PESSOAIS?.....	49
REQUISITOS PARA O TRATAMENTO DOS DADOS PESSOAIS.....	54
BASES LEGAIS DA LGPD.....	56
MEDIANTE CONSENTIMENTO DO TITULAR.....	56
PARA CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA PELO CONTROLADOR DOS DADOS.....	57
PARA O CUMPRIMENTO DE POLÍTICAS PÚBLICAS.....	58
PARA REALIZAÇÃO DE ESTUDOS E PESQUISAS.....	59
PARA EXECUÇÃO OU PREPARAÇÃO DE CONTRATO.....	59
PARA EXERCÍCIO DE DIREITOS EM PROCESSO JUDICIAL, ADMINISTRATIVO OU ARBITRAL	60
PARA PROTEÇÃO DA VIDA OU DA INCOLUMIDADE FÍSICA DO TITULAR OU DE TERCEIRO	60
PARA TUTELA DA SAÚDE DO TITULAR.....	61
PARA ATENDER AO LEGÍTIMO INTERESSE DO CONTROLADOR OU TERCEIRO.....	62
PARA PROTEÇÃO DO CRÉDITO.....	63
TRATAMENTO DOS DADOS PESSOAIS SENSÍVEIS.....	63
TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES.....	64
TÉRMINO DO TRATAMENTO DE DADOS.....	65
DIREITOS DO TITULAR.....	66
REGRAS DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO.....	68
TRANSFERÊNCIA INTERNACIONAL DE DADOS.....	69
RESPONSABILIDADE E RESSARCIMENTO DE DANOS.....	71
SEGURANÇA E SIGILO DOS DADOS.....	71
BOAS PRÁTICAS E GOVERNANÇA.....	72
DISPOSIÇÕES FINAIS E TRANSITÓRIAS DA LGPD.....	73

CONSIDERAÇÕES ADICIONAIS.....	73
CONSENTIMENTO.....	74
PRINCIPAIS ADEQUAÇÕES À LGPD.....	75
MUDANÇA DE CULTURA NA ORGANIZAÇÃO.....	76
IMPLEMENTAÇÃO DA LGPD E AÇÃO.....	76
<b>2. GESTÃO DE PROJETOS, COMO GERIR E QUANTIFICAR AS SUAS ATIVIDADES.....</b>	<b>78</b>
CONSIDERAÇÕES INICIAIS.....	78
PLANEJAMENTO DO PROGRAMA DE CONFORMIDADES.....	81
MAS AFINAL O QUE É KANBAN?.....	81
PLANO DE PROJETO.....	82
COLOCANDO AS INFORMAÇÕES DO PROJETO NO PAPEL (OU VIRTUAL).....	84
<b>3. LGPD HERO EM AÇÃO.....</b>	<b>97</b>
FORMAÇÃO DO COMITÊ DE SEGURANÇA.....	97
DEFINIÇÃO DE PAPÉIS E RESPONSABILIDADES NO PROGRAMA DE CONFORMIDADES.....	100
ME TORNAR OU TREINAR UM ENCARREGADO?.....	101
APRESENTANDO O QUE É A LGPD.....	103
ANÁLISE DA PERCEPÇÃO ORGANIZACIONAL EM RELAÇÃO A SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DOS DADOS.....	104
SUGESTÃO DE PERGUNTAS PARA O QUESTIONÁRIO DE DESCOPERTA.....	107
COMPREENSÃO DOS PROCESSOS VIGENTES.....	111
DIAGNÓSTICO (gap analysis).....	114
COLOCANDO TUDO EM PRÁTICA.....	119
REVISÃO NORMATIVA.....	124
CLASSIFICAÇÃO DE DOCUMENTOS.....	126
CICLO DE VIDA DOS DADOS.....	130
TABELA DE TEMPORALIDADE DOCUMENTAL.....	132
POLÍTICA DE PRIVACIDADE.....	133
TERMOS DE SERVIÇO.....	135
COOKIES.....	137
COMPARTILHAMENTO E TRANSFERÊNCIA DE DADOS POR E-MAIL.....	139
ACESSO E EXPORTAÇÃO DE DADOS PESSOAIS.....	140
EXPORTAÇÃO DE DADOS.....	141
EXCLUSÃO DE DADOS.....	142
PROCESSO DE ANONIMIZAÇÃO E PSEUDO ANONIMIZAÇÃO.....	143
MARKETING E PUBLICIDADE.....	145
GESTÃO DO REGISTRO DE PROCESSAMENTO DE LOGS.....	148
LOGS DE MONITORAMENTO.....	151
LOGS DE EVENTOS.....	152
AUDITORIA.....	152
LOGS DE SEGURANÇA.....	153
LOGS DE ACESSO.....	153
LOGS NA PRÁTICA.....	153
MAPEAMENTO DE DADOS (data mapping).....	154
ALINHAMENTO DAS HIPÓTESES DE TRATAMENTO E PRINCÍPIOS FUNDAMENTAIS.....	157
CHECKLIST - COMO IDENTIFICAR UMA HIPÓTESE DE TRATAMENTO.....	159
PRIMEIRA HIPÓTESE DE TRATAMENTO: MEDIANTE CONSENTIMENTO DO TITULAR.....	160
SEGUNDA HIPÓTESE DE TRATAMENTO: PARA O CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA.....	161

TERCEIRA HIPÓTESE DE TRATAMENTO: PARA A EXECUÇÃO DE POLÍTICAS PÚBLICAS.....	162
QUARTA HIPÓTESE DE TRATAMENTO: PARA REALIZAÇÃO DE ESTUDOS E PESQUISAS.....	163
QUINTA HIPÓTESE DE TRATAMENTO: PARA EXECUÇÃO DE CONTRATO OU DE PROCEDIMENTOS PRELIMINARES RELACIONADOS AO CONTRATO DO QUAL O TITULAR DOS DADOS SEJA PARTE.....	164
SEXTA HIPÓTESE DE TRATAMENTO: PARA EXERCÍCIO DE DIREITOS EM PROCESSO JUDICIAL, ADMINISTRATIVO OU ARBITRAL.....	164
SÉTIMA HIPÓTESE DE TRATAMENTO: PARA PROTEÇÃO DA VIDA OU DA INCOLUMIDADE FÍSICA DO TITULAR OU DE TERCEIRO.....	165
OITAVA HIPÓTESE DE TRATAMENTO: PARA TUTELA DA SAÚDE DO TITULAR.....	165
NONA HIPÓTESE DE TRATAMENTO: PARA ATENDER INTERESSES LEGÍTIMOS DO CONTROLADOR OU DE TERCEIROS.....	166
DÉCIMA HIPÓTESE DE TRATAMENTO: PARA PROTEÇÃO DO CRÉDITO.....	167
CONSIDERAÇÕES ADICIONAIS, QUANDO O CONTROLADOR FAZ PARTE DA ADMINISTRAÇÃO PÚBLICA.....	168
OBSERVAÇÕES IMPORTANTES PARA O TRATAMENTO DE DADOS SENSÍVEIS.....	170
OBSERVAÇÕES IMPORTANTES PARA O TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES.....	172
REALIZAÇÃO DO MAPEAMENTO DE DADOS NA PRÁTICA.....	172
RELATÓRIOS DINÂMICOS A PARTIR DO MAPEAMENTO DOS DADOS.....	178
RELATÓRIO DE LEVANTAMENTO E ANÁLISE DA EMPRESA.....	184
RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD).....	188
O QUE É UM RISCO?.....	189
TIPOS DE CONTROLES.....	189
POLÍTICA PARA MITIGAÇÃO DOS RISCOS.....	191
POLÍTICA DO MENOR PRIVILÉGIO.....	191
SEGMENTAÇÃO DE TAREFAS.....	192
ROTAÇÃO NO TRABALHO.....	193
ESTRUTURAÇÃO DO RIPD.....	193
IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO.....	194
IDENTIFICAÇÃO DAS NECESSIDADES QUE JUSTIFIQUEM A ELABORAÇÃO DA RIPD.....	195
DESCRIPAÇÃO E DETALHAMENTO DA FORMA DE TRATAMENTO.....	197
NATUREZA DO TRATAMENTO.....	198
ESCOPO DO TRATAMENTO.....	198
CONTEXTO DO TRATAMENTO.....	199
FINALIDADE DO TRATAMENTO.....	199
IDENTIFICAÇÃO DAS PARTES ENVOLVIDAS.....	201
DESCRIPAÇÃO DA NECESSIDADE DO TRATAMENTO.....	201
IDENTIFICAÇÃO E AVALIAÇÃO DOS RISCOS.....	202
TABELA PARA CLASSIFICAÇÃO DO RISCO.....	204
TABELA DE CLASSIFICAÇÃO POR CORES E PONTUAÇÕES DA MATRIZ DE PROBABILIDADE X IMPACTO.....	204
TABELA MODELO PARA LISTAGEM DOS RISCOS E O SEU NÍVEL DE PROBABILIDADE VEZES SEU IMPACTO.....	205
IDENTIFICAÇÃO DAS MEDIDAS DE MITIGAÇÃO E MINIMIZAÇÃO DOS RISCOS.....	206
TABELA DESCRIPTIVA PARA ANÁLISE DOS RISCOS E MEDIDAS ADOTADAS.....	207
APROVAÇÃO DO RIPD.....	209
CONTÍNUO APRIMORAMENTO E REVISÃO DO RIPD.....	209
RELATÓRIO DE STATUS (status report).....	211

<b>4. OPERAÇÕES PARA MANUTENÇÃO DO PERÍMETRO DE SEGURANÇA DOS DADOS.....</b>	<b>213</b>
QUESTÕES DE SEGURANÇA DURANTE A INTEGRAÇÃO COM TERCEIROS.....	213
PARCEIRO DE NEGÓCIOS (RELAÇÃO OPERADOR E CONTROLADOR).....	213
FATORES LEGAIS.....	214
FATORES TÉCNICOS DE SEGURANÇA.....	215
RISCOS NAS REDES SOCIAIS.....	216
FALAR SOBRE O TRABALHO.....	218
REVELAÇÃO DE DETALHES PESSOAIS.....	218
REVELAR DETALHES SOBRE BENS PESSOAIS.....	219
EXTERNAR PRECONCEITOS, PALAVRAS DE ÓDIO E AFINS.....	219
ACORDOS COM O PARCEIRO DE NEGÓCIOS.....	220
ACORDOS COM O PARCEIRO DE NEGÓCIOS.....	220
QUEM É O DONO DOS DADOS?.....	222
DADOS UTILIZADOS SEM AUTORIZAÇÃO.....	223
CONSCIÊNCIA DOS RISCOS.....	224
BACKUP.....	225
GERENCIAMENTO DINÂMICO.....	226
EM TIME QUE GANHA, NÃO SE MEXE (GESTÃO DE MUDANÇAS).....	227
USUÁRIOS E PERMISSÕES.....	230
GESTÃO DE INCIDENTES.....	231
O QUE É UM INCIDENTE?.....	232
ACORDO DE NÍVEL DE SERVIÇO (SLA).....	234
GERENCIAMENTO DE INCIDENTES.....	237
AUDITORIA.....	242
PADRÕES DE AUDITORIA.....	244
<b>5. CONTROLES DE SEGURANÇA FÍSICAS E ABSTRATAS.....</b>	<b>245</b>
SEGURANÇA FÍSICA.....	245
CONTROLE DE ACESSO FÍSICO.....	246
INGRESSO NO PERÍMETRO DE ACESSO DA ORGANIZAÇÃO.....	246
LISTA DE ENTRADA E SAÍDA.....	247
TRAVAS DE PROTEÇÃO.....	248
MAN-TRAP.....	249
DISPOSITIVO FÍSICO DE IDENTIFICAÇÃO.....	249
SISTEMA ELETRÔNICO DE VIGILÂNCIA E SEGURANÇA.....	250
AMBIENTE RESISTENTE.....	250
CONTROLE DO FOGO.....	251
INVENTÁRIO E CONTROLE DOS ATIVOS DE HARDWARE.....	254
BRING YOUR OWN DEVICE (BYOD).....	257
ADERÊNCIA ÀS POLÍTICAS DE SEGURANÇA DA ORGANIZAÇÃO E A ACEITAÇÃO DO USUÁRIO.....	259
SUPORTE BYOD.....	261
PROPRIEDADE DOS DADOS.....	261
ANÁLISE FORENSE BYOD.....	262
INVENTÁRIO E CONTROLE DOS ATIVOS DE SOFTWARE.....	262
GESTÃO DE VULNERABILIDADE CONTÍNUA DOS SOFTWARES.....	266
UTILIZAÇÃO DE PRIVILÉGIOS ADMINISTRATIVOS CONTROLADOS.....	267
SENHAS FORTES.....	269
AUTENTICAÇÃO EM DOIS FATORES (MFA/2FA).....	273

ATIVAÇÃO E AUDITORIA DE LOGS.....	274
HARDENING.....	275
DATA LOSS PREVENTION.....	278
IDENTIFICAÇÃO DE UM INCIDENTE.....	280
<b>6. ANALISANDO DADOS E PROCURANDO POR AMEAÇAS.....</b>	<b>301</b>
FERRAMENTAS DO ENCARREGADO E EQUIPE TÉCNICA.....	301
CONTATO COM OS TITULARES DE DADOS.....	302
CONTATO COM A AUTORIDADE NACIONAL DE DADOS (ANPD).....	303
ORIENTAÇÕES QUANTO AOS CUIDADOS COM O TRATAMENTO DE DADOS E SEGURANÇA DA INFORMAÇÃO.....	303
EXECUÇÃO DE DEMAIS ATRIBUIÇÕES DETERMINADAS PELO CONTROLADOR OU POR NORMAS COMPLEMENTARES.....	304
OUTRAS FERRAMENTAS PARA O ENCARREGADO DE DADOS.....	305
ANÁLISE DE PROTOCOLOS.....	306
ANÁLISE DE VULNERABILIDADES.....	307
COMO CALCULAR UM RISCO TECNOLÓGICO.....	309
COMO MENSURAR O RISCO.....	314
RISCO RESIDUAL.....	316
QUAIS SÃO AS AMEAÇAS TECNOLÓGICAS MAIS COMUNS?.....	317
CONFIDENCIALIDADE.....	318
INTEGRIDADE.....	318
DISPONIBILIDADE.....	318
AUTENTICIDADE.....	319
LEGALIDADE.....	319
<b>7. O QUE OU DE QUEM ESTOU PROTEGENDO OS DADOS?.....</b>	<b>320</b>
MALWARES.....	320
SPYWARE.....	320
ADWARE.....	320
VÍRUS.....	321
CAVALO DE TROIA.....	321
ROOTKITS.....	322
BOTNET.....	322
BOMBA LÓGICA.....	323
RANSOMWARE.....	323
MANEIRAS DE REALIZAR UM ATAQUE.....	323
MAN IN THE MIDDLE (MITM).....	324
DENIAL OF SERVICE (DoS).....	325
DISTRIBUTED DENIAL OF SERVICE (DDoS).....	326
REPLAY.....	328
SMURF.....	328
SPOOFING.....	329
SPAM.....	330
PHISHING.....	330
SPIM.....	333
ÁRVORE DE NATAL (XMAS TREE).....	333
PHARMING.....	334
ESCALANDO PRIVILÉGIOS.....	335
AMEAÇAS INTERNAS.....	335

ATAQUES DE SENHAS.....	336
SEQUESTRO DE URL (hijacking).....	337
ENGENHARIA SOCIAL.....	340
ATAQUES EM REDES SEM FIO.....	346
ATAQUES EM APLICAÇÕES.....	348
SEGURANÇA EM APLICAÇÕES.....	353
SEGURANÇA EM DISPOSITIVOS MÓVEIS.....	357
SEGURANÇA EM SERVIDORES.....	360
GERENCIAMENTO DE APLICAÇÕES.....	363
SEGURANÇA DO HARDWARE.....	364
SEGURANÇA EM BASE DE DADOS.....	367
SEGURANÇA EM SERVIÇOS DE NUVEM (cloud services).....	370
SEGURANÇA EM API (application programming interfaces).....	372
<b>8. PROTEÇÃO E PREVENÇÃO AVANÇADA.....</b>	<b>375</b>
PLANO DE CONTINUIDADE DAS OPERAÇÕES.....	376
CONTINGÊNCIA.....	378
TOLERÂNCIA À FALHAS.....	381
PLANEJAMENTO DE BACKUP.....	384
TIPOS DE BACKUP.....	385
BACKUP COMPLETO.....	386
BACKUP INCREMENTAL.....	386
PLANEJANDO O BACKUP.....	387
TREINAMENTOS.....	388
TREINAMENTOS POR CARGO.....	390
TREINAMENTO PARA TRATAMENTO DE DADOS.....	390
CLASSIFICAÇÃO DA INFORMAÇÃO.....	391
MELHORES PRÁTICAS.....	391
NORMAS E CONFORMIDADES.....	392
HÁBITOS SEGUROS.....	393
MÉTRICAS DE ACOMPANHAMENTO.....	393
ANÁLISE DE SEGURANÇA AVANÇADA - PENTEST.....	395
FASES DO PENTEST.....	396
PRINCIPAIS METODOLOGIAS PARA PENTEST.....	397
OWASP (Open Web Application Security Project).....	398
PTES (Penetration Testing Execution Standard).....	400
OSSTMM (Open Source Security Testing Methodology Manual).....	402
NIST 800-115.....	405
PTF (Pentest Framework).....	407
MITRE ATT&CK - CATÁLOGO DE TÁTICAS E TÉCNICAS E PROCEDIMENTOS CIBERCRIMINOSOS.....	409
CIS CRITICAL SECURITY CONTROLS - CONJUNTO PRIORITÁRIO DE AÇÕES PARA PROTEGER SUA ORGANIZAÇÃO E SEUS DADOS DE VETORES DE ATAQUES CIBERNÉTICOS.....	411
RED TEAM.....	413
BLUE TEAM.....	415
DIFERENÇAS ENTRE RED TEAM E BLUE TEAM.....	416
PERÍCIA FORENSE.....	417
AMANHÃ SERÁ INCERTO.....	419
<b>REFERÊNCIAS.....</b>	<b>421</b>

# INTRODUÇÃO

O ano era 1992 e eu tinha 8 anos de idade quando meu pai resolveu que seria interessante eu ter um computador, para explorar as suas capacidades e aprender a mexer em um. Naquela época havia uma loja de departamentos chamada Mesbla que vendia de tudo, como são a maioria das lojas de departamentos de hoje.

Esse evento transformador na minha vida ocorreu por advento do meu aniversário de 8 anos, então ganhei o meu primeiro computador pessoal e não era qualquer um, era um MSX 1.0 BR da Gradiente!

Quem sabe o que foi um MSX ou é saudosista, sabe do que estou falando. Resumidamente um MSX era um consórcio japonês (Sony, Panasonic, Yamaha e Casio, para citar algumas) que tinha por objetivo construir um padrão de PC (Personal Computer) para ser vendido ao mundo. Ele rodava o sistema operacional MSX-DOS (que foi desenvolvido pela Microsoft e era muito parecido com o famoso MS-DOS). Havia uma linguagem de programação chamada BASIC que tinha todas as suas instruções básicas no manual que acompanhava o computador.

A partir desse momento eu queria me tornar um programador (na verdade não sabia que se chamavam assim, apenas queria ser alguém que fazia coisas legais no computador).

Na época ninguém falava muito sobre tecnologia ou desenvolvimento de softwares, por coincidência tinha um vizinho que também tinha um MSX e o seu pai (que viajava muito) sempre trazia revistas (algumas importadas) sobre tecnologia, MSX, jogos e programação.

O meu computador acabou queimando em 1994 e o MSX já estava perdendo terreno para os PC's e entrando em decadência (empresas do consórcio começaram a sair e a coisa foi ficando escassa), ao mesmo tempo a Mesbla que foi a loja onde meu pai comprou o MSX já estava bem enrolada financeiramente (que faliu algum tempo depois), então ficou difícil consertar esse computador, sem suporte, sem peças, ficando sem ele para sempre desde então.

Comecei a mexer em PC's como conhecemos hoje em dia pelo Sistema Operacional Windows 3.11 nas casas de amigos, aprendendo comandos, fuçando e a mexer no MS-DOS quando possível, conquistando o meu primeiro PC por volta de 2002 (aí eu já tinha o Windows Millenium bruuuuuu).

Desde então estudo e comecei a trabalhar como programador profissional pela primeira vez em 2009 e de lá para cá, fui estudando linguagens de programação de alto nível, aprendendo sobre UNIX, depois morrendo de amores pelo Linux (mas não abandonando o Windows).

Hoje atuo como consultor em desenvolvimento de softwares e segurança da informação, faço levantamento de requisitos, desenho os dados, escrevo o front-end e back-end. Já para área de segurança da informação desenvolvo as minhas próprias ferramentas de suporte, proteção, privacidade, relatórios e faço pentests (são aqueles testes simulados, para saber se um software é seguro ou não, como se fosse um cibercriminoso, para no final elaborar um relatório e apontar as falhas encontradas, permitindo ao solicitante agir preventivamente corrigindo as falhas).

Contudo, a cibersegurança está mais para o jogo de gato e rato e os usuários comuns, além de não saberem os conceitos tecnológicos adequadamente, não compreendem muitos raciocínios criminosos envolvidos nos ataques digitais.

As empresas se esforçam cada vez mais para colocar segurança em suas operações e posso afirmar que não é algo fácil de fazer, pois depende de inúmeros fatores como tecnologia, estratégias comerciais, processos e operações, equipe treinada, orçamento para adquirir produtos e serviços de proteção e agora se adequar a legislação sob risco de punições administrativas ou financeiras.

Entretanto, o fator mais importante de tudo isso é o ser humano, sim eu, você e todos nós que consumimos tecnologia e dependemos dela para realizar as nossas atividades profissionais com eficiência e pessoal com facilidade.

A tecnologia está em todos os lugares e hoje somos reféns dela. A cada dia que passa novos serviços e facilidades surgem, nos tornando cada vez mais dependentes. Por isso o mundo do crime está mudando de eixo, transferindo

cada vez mais as suas ações e tentáculos para o ambiente onde as pessoas estão, que é o mundo digital.

O objetivo deste material é trazer esses conceitos e explicá-los de maneira facilitada, para que qualquer pessoal que adote tecnologia de forma profissional e/ou pessoal, tenha condições de identificar diversos riscos, compreender a situação e adotar medidas de proteção mais adequadas.

Muito tem se falado em segurança e neste material que lê, o objetivo é para além de falar dela (isso inclui proteção e privacidade), apresentando ações práticas que podem ser adotadas a fim de atender a legislação (LGPD), assim como diversos quesitos de segurança da informação para muitos dos crimes digitais hoje praticados.

## PARA QUEM É ESTE E-BOOK

Este e-book é totalmente dedicado aos profissionais (de qualquer área) que desejam implementar em suas empresas, local onde trabalha ou até trabalhando como consultor na adequação da empresa com a LGPD, compatibilizando ela com a legislação e mitigando riscos com crimes digitais.

Quem já perdeu dinheiro para criminosos virtuais, entendeu da pior maneira como foi ser vítima, este material lhe ajudará a agir de maneira prudente, para diminuir drasticamente as chances disso acontecer novamente e se você nunca caiu num golpe, meus parabéns, continue atencioso com tudo e este material lhe servirá para aprimorar ainda mais as suas habilidades e ações em situações suspeitas.

Este *e-book* não exige conhecimentos tecnológicos avançados, até porque o meu objetivo aqui é te trazer explicações e compreensão facilitada deste meio. Contudo existem requisitos básicos e eles envolvem conhecer e utilizar ferramentas digitais como navegador *web*, editores de planilhas, editores de textos e um certo grau de raciocínio lógico.

Caso não domine algum conteúdo necessário, não fique preocupado, pois a dinâmica da tecnologia é rápida (do crime digital também) e as coisas mudam

numa velocidade surpreendente, então recomendo que busque por pesquisas paralelas sempre que surgirem dúvidas eventualmente não explicadas neste material.

## SOBRE O AUTOR



Figura 1: Fabrizio Rodrigues

**Linkedin:** <https://www.linkedin.com/in/fabriziorodriguesr/>

Sou Fabrizio Rodrigues, especialista em segurança da informação e desenvolvedor de softwares. Trabalho com tecnologia há mais de uma década e faço o que gosto, ajudando empresas e pessoas a facilitarem as suas operações atendendo demandas com serviços tecnológicos personalizados.

Me formei em Análise de Sistemas e fiz uma pós-graduação em Segurança da Informação (SI). Trabalhei para várias empresas da área de

tecnologia, comunicação, engenharia e jurídico (passado por empresas como Centro de Inovação do SESI, afiliadas da Rede Globo, empresas estrangeiras dos EUA e muitas outras), hoje tenho minha empresa de consultoria e ainda sigo atendendo muitas dessas empresas que já fui funcionário e agradeço por acreditarem no meu trabalho.

Minha grande paixão profissional é o desenvolvimento de softwares, com essa habilidade, fiz um caminho raro para profissionais dessa categoria, que é ingressar na área da SI sendo um programador.

Parece fazer sentido, mas não é bem assim.

Pode não parecer, mas a tecnologia possui várias ramificações de conhecimento específico sendo o desenvolvimento de softwares (e ainda no meu caso para aplicações web) e a segurança da informação sendo duas ramificações ou trilhas bem distintas, apesar de se comunicarem entre si.

O mesmo vale para profissionais de infraestrutura (aqui me refiro ao físico), redes, dados, design, automação industrial e muitas outras

Sabe quando alguém pede para um programador “programar” o seu Facebook para recuperar a senha (normalmente aquele familiar com mais idade costuma pedir isso, não é mãe?!). Isso não faz sentido, pois mexer com tecnologia não capacita o profissional em questão a mexer com qualquer tecnologia física, abstrata ou sistema.

Isso seria como pedir ao médico neurologista para operar o seu tornozelo ou para um advogado consertar o seu ar condicionado.

Eu sei, exagero meu, mas é quase isso.

Antes da LGPD, eu já tinha feito a especialização em segurança da informação, que na época era o patinho feio das especializações que um programador poderia fazer. Até os meus amigos na época me olhavam com ares de reprovação e me questionavam se eu tinha certeza do que estava fazendo.

Como meu objetivo sempre foi fazer aquilo que gosto, segui em frente com as minhas convicções de forma despretensiosa.

Após a LGPD os profissionais com essa especialização foram caçados pelo mercado e não posso reclamar de naquele momento estar numa posição com capacitação profissional adequada a demanda.

## SOBRE O E-BOOK

Este *e-book* foi pensado para ser usado como fonte de referência, para atender as questões de privacidade e proteção exigidas pela LGPD do início ao fim. Sabemos que hoje, estão praticamente em extinção as empresas que não empregam tecnologia em algum grau (na verdade eu acho que essas empresas não existem mais) e o grande problema é a forma insegura como as empresas, inclusive as de grande porte, tratam os dados de forma insegura.

Tomarei por base que você não possui conhecimento em metodologias ágeis para gestão de projetos e nem possua conhecimentos sobre ferramentas nessa categoria. Não se preocupe, pois além de abordar a LGPD, apresentar mecanismos de proteção e segurança, também lhe apresentarei mecanismos de gestão, para que consiga acompanhar a cada pequena evolução e a mensurar o seu esforço empreendido.

Caso tenha conhecimento nas ferramentas e processos apresentados, sinta-se à vontade para avançar alguns capítulos do *e-book*.

O pensamento de que “isso não vai acontecer comigo” já não existe no mundo digital e tenho certeza que você está sendo alvo de ações criminosas a todo instante (inclusive agora), com a diferença de que as empresas ou serviços digitais que utiliza conseguem represar a maioria das tentativas.

Esse não é um problema isolado, pois praticamente pode afetar qualquer empresa ou pessoa que use tecnologia.

Contudo, esse *e-book* não se esquece de lhe apresentar meios e medidas de mitigação para dados armazenados em meios físicos, delimitação de espaços físicos, ferramentas e procedimentos físicos que visam incrementar a proteção dos dados. Você já deve ter percebido e em momento algum afirmei que lhe trarei um mecanismo de proteção infalível, até porque isso não existe.

No momento em que lê esta frase, pessoas e empresas já estão em estágios avançados para a próxima tecnologia disruptiva ou crime digital impensável, logo tratamos a segurança da informação como algo que deve ser incorporado em nossas vidas e todos em os processos que devem ser revisados diversas vezes ao longo do ano, para que ele esteja adequado a realidade do momento tecnológico e da área de atuação da empresa, pois também existem crimes digitais específicos que afetam apenas empresas em determinados setores econômicos como bancos, logística etc.

Não podemos nos esquecer do maior volume dos crimes digitais que estão aí há anos e só mudam a narrativa, mantendo o mesmo modo de operação como phishing e a engenharia social como um todo.

Este *e-book* lhe ajudará a incrementar a sua abordagem de segurança e a entender melhor como os crimes digitais operam e o que você pode fazer para evitá-los.

Reforço que a proteção só será incrementada se os procedimentos forem aplicados na prática. Não tenha medo de tentar, testar, pesquisar e se envolver, ficar parado pode até parecer seguro e também não nos levará para lugar algum.

Com cautela e muita atenção, vamos avançar juntos e afastar os crimes digitais do nosso cotidiano.

Este *e-book* possui um canal de atualizações, notas, erratas, correções e links de suporte que podem ser acompanhados pelo GitHub pelo link:

GitHub (página deste *e-book* LGPD HERO)  
<https://github.com/fabriziorodrigues/ebook-lgpd-hero>

## AGRADECIMENTOS

Primeiramente à Deus por ter condições de escrever e transformar minhas ideias e experiências em algo útil. Sem sua benção, não chegaria a lugar algum.

A minha família, minha esposa Ivy (minha parceira em aventuras, qualquer aventura) e meus filhos Marcos e Egon. Vocês são a razão da minha felicidade e motivação para continuar firme nos meus propósitos de vida.

Aos meus amigos que me aturam e que persistem na amizade comigo, mesmo sabendo que eu não gosto e não respondo mensagens rapidamente em comunicadores instantâneos, às vezes levando dias para ver que recebi alguma mensagem, vocês são resilientes. Gostaria de citar nominalmente meu amigo Matheus Leite que atua na área da comunicação, me ensinou e mostrou que sou capaz de produzir e lançar produtos digitais, transformando ideias e experiências em materiais que podem ser úteis para outras pessoas.

Aos meus empregadores e parceiros comerciais, que me trouxeram diversos desafios (alguns deles bem sinistros) para serem superados, o que me engrandeceu profissionalmente. Só o movimento, os desafios e empurrões deles me fizeram alcançar degraus mais elevados, agradeço todos vocês pelas experiências profissionais proporcionadas e pelo conhecimento adquirido nesses desafios.

E agradeço especialmente você que está adquirindo esse e-book, por estar confiando em minha abordagem, experiência e forma de apresentar a solução aqui trazida. Desejo que esse material possa lhe ajudar muito no processo de proteção digital em sua vida pessoal e na empresa onde atua.

# RESUMO DOS CAPÍTULOS

Este *e-book* foi dividido em 8 capítulos de forma que você consiga direcionar os seus estudos e pesquisas nas áreas de interesse, afinal, este *e-book* foi pensado para ser o seu guia de referências rápidas sempre que precisar.

**Capítulo 1**, “Introdução à Lei Geral de Proteção de Dados Pessoais”. Pode parecer óbvio para algumas pessoas que já estão dedicando tempo e esforços em conhecer a LGPD, no entanto não é difícil conversar com alguém que sequer sabe o que é LGPD e o que ela faz. Portanto abordarei a lei, explicarei o significado de diversos termos e principalmente os objetivos da mesma. Esse material só será plenamente operacional se o leitor possuir uma boa compreensão da LGPD e seus fundamentos.

**Capítulo 2**: “Gestão de projetos, como gerir e quantificar as suas atividades”. Na área da TI é comum o programador ter contato direto e vivenciar a gestão de projetos, nesse caso projetos ágeis. Esse capítulo lhe apresentará os fundamentos e a utilização de ferramentas de gestão, para que você consiga gerenciar o seu projeto de adequação a LGPD, acompanhar o seu desenvolvimento e se situar em relação ao início, meio e fim. O termo “projetos ágeis” vem da metodologia de gestão ágil, mas isso não significa que você será mais rápido (isso é consequência do seu emprego adequado), mas na verdade melhor adaptável às mudanças de curso do projeto em que está empenhado e que por vezes podem sofrer alterações bruscas e imprevistas.

**Capítulo 3**: “LGPD HERO em ação”. Inicie a sua jornada prática empregando *frameworks*, metodologias e ferramentas de operação para iniciar a prática de adequação da LGPD onde desejar. Não existe local onde não possa (e não deva) empregar as operações relacionadas à LGPD, para tornar o ambiente dos seus dados mais protegidos e afastá-los do alcance criminoso. A ação como diz o nome do capítulo é auto explicativo, então a partir desse ponto entramos na operação prática da proteção, privacidade e segurança da informação para mitigar os riscos que envolvem os dados pessoais.

**Capítulo 4**: “Operações para manutenção do perímetro de segurança dos dados”. Ter iniciativa para fazer algo prático para transformar é uma atitude louvável e quando falamos de dados e segurança da informação, essa prática

deve ser realizada todos os dias. O Capítulo 4 tem por objetivo lhe apresentar metodologias e ferramentas para operar a manutenção da segurança, realizando procedimentos de análise e validação do perímetro de segurança. Você já deve imaginar que os cibercriminosos não descansam aos finais de semanas e feriados, eles na realidade pouco se importam com você e exploram toda e qualquer situação, inclusive doenças, dívidas ou qualquer contexto que possa chamar a atenção da vítima, por isso a atenção deve ser permanente.

**Capítulo 5:** “Controles de segurança físicas e abstratas”. A segurança e proteção dos dados passa por diversos controles físicos e abstratos (sistemas, softwares, serviços digitais) no intuito de evitar que algo ruim possa acontecer. Esses controles são maneiras de mitigação dos riscos e afastam potenciais cibercriminosos de conseguirem realizar coleta de dados e inteligência, gerando insumos e conhecimento para que você articule suas camadas de proteção com maior taxa de sucesso defensivo. O objetivo deste capítulo é aplicar mecanismos de proteção que desincentivem as investidas criminosas desde os seus estágios iniciais.

**Capítulo 6:** “Analizando dados e procurando por ameaças”. Neste capítulo você conhecerá algumas abordagens e ferramentas que irão melhorar a sua consciência em relação ao dados e a calcular os riscos e vulnerabilidades. São diversas frentes de batalha na guerra digital e por isso, devemos ter condições de listar e elencar prioridades para as ações que serão tomadas.

**Capítulo 7:** “O que ou de quem estou protegendo os dados?”. Aqui serão apresentados os tipos de crimes digitais mais comuns (alguns nem tanto) e como os criminosos pensam nas suas investidas. Você só consegue se defender daquilo que conhece e sabe que existe, caso contrário, situações podem estar ocorrendo e passando diante dos seus olhos sem que você tenha ciência de que elas podem estar representando riscos ao seu esforço de segurança e ao perímetro defensivo digital.

**Capítulo 8:** “Proteção e prevenção avançada”. Neste capítulo apresentarei algumas abordagens defensivas importantes, como backups, treinamentos constantes, tolerância a falhas, plano de continuidade das operações e a apresentação de abordagens avançadas como pentests, blue team, perícia forense e aplicação de *frameworks* de segurança como OWASP, PTES,

OSSTMM, NIST e MITRE ATT&CK. Saber que eles existem e que podem ser contratados como serviço por empresas do ramo, pode ser o que falta para fechar a cadeia de segurança da empresa onde atua. Dependendo da empresa, um pentest pode ser item praticamente obrigatório na manutenção das operações, por exemplo.

DEMONSTRAÇÃO

## CAPÍTULO 1

# 1. INTRODUÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Histórias sempre são boas, pois nos apresentam o motivo das coisas serem como são. Isso serve para tudo nesse mundo, inclusive para LGPD. Conhecer a história nos esclarece a motivação das coisas terem acontecido, o que de certa forma nos abre a visão para conseguirmos vislumbrarmos o futuro, a fim de conseguirmos antecipar algumas situações. Contudo, esse vislumbre é limitado, pois a complexidade do mundo atualmente, considera inúmeras variáveis que fogem da capacidade humana para processar tantos dados e relacioná-los de maneira que traga algum benefício prático.

Contudo, a história é essencial para, principalmente, não repetirmos os erros do passado no presente. Vamos aos fatos!

Em agosto de 2018, foi aprovada a Lei Geral de Proteção de Dados (LGPD) que visa, sobretudo, trazer segurança às pessoas físicas no que tange a utilização dos seus dados pessoais. Sabemos que a maciça utilização da Internet, seja por e-mails, mídias sociais, sistemas de comunicação, serviços virtuais e tantos outros, solicitam o tempo todo os nossos dados pessoais para autorizar sua utilização.

O que alguns podem não perceber ou até ignorar, mas todos os dados fornecidos voluntariamente para permitir o acesso gratuito a esses serviços, cobram você na forma de propagandas direcionadas, análise do seu perfil, propagandas de terceiros e tantas outras possibilidades. Como todos sabemos, nada nesse mundo é simplesmente de graça.

A questão principal é que, até então, não havia uma lei que tratava diretamente sobre a segurança dos dados pessoais que hoje trafegam o mundo em questão de segundos. O problema com isso, é que muitas empresas que mantém os dados pessoais de vários titulares em suas bases, não costumavam atribuir a devida segurança desses dados como prioridade em seus

investimentos. Essa situação atinge a maioria das empresas nacionais e não se surpreenda se o seu cliente nunca tiver ouvido falar sobre LGPD!

A LGPD é resultado de uma série de incidentes e utilizações indevidas dos dados pessoais para as mais diversas atividades irregulares como: crimes, roubo de credenciais, chantagens e todo tipo de crime virtual que você possa imaginar ao longo de vários anos. Mesmo aquela empresa que coletou seus dados e nunca os utilizou para nada, deverá se enquadrar na lei.

A LGPD foi fortemente baseada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR - *General Data Protection Regulation*). Não por acaso, muitos quesitos da GDPR estão de alguma forma presentes na LGPD.

Atualmente, países como Estados Unidos, Canadá, Austrália, Japão e tantos outros, estão implementando seus próprios regulamentos de segurança para tratamento dos dados pessoais em suas fronteiras (ou para uma região como a GDPR que abrange todos os países membros da União Europeia). No Brasil, a LGPD começou a valer em agosto de 2020 e por conta da pandemia, as multas que poderão ser aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), foram prorrogadas para passar a valer a partir de agosto de 2021.

A nova lei cria uma série de regras para a coleta e tratamento de dados pessoais, onde qualquer empresa pública ou privada que coleta esses dados, deverá cumprir todos os quesitos e obrigações legais sobre segurança e governança. Nas circunstâncias atuais da informação e sua difusão, podemos considerar que praticamente todas as organizações terão que se adequar às novas regras. Considere também que profissionais liberais que tratem dados pessoais para fins econômicos, também deverão se adequar a lei.

Portanto, temos aqui uma grande necessidade para colocarmos em prática, a implantação da LGPD em muitas empresas nacionais (públicas e privadas). Um estudo publicado em março de 2020 pela consultoria ICTS Protiviti, aponta que no período de 6 meses onde uma amostragem com mais de 160 empresas avaliadas, 84% dessas empresas, continuam sem uma diretriz clara sobre a adequação a LGPD.

Esse número pode ser ainda maior, se considerarmos também as micro, pequenas e médias empresas nacionais.

Vamos descobrir por onde começar um programa de conformidade da LGPD para essas empresas (micro, pequena e média), que são a grande maioria.

## A LGPD

Vamos começar falando sobre a LGPD, explicando com um pouco mais de detalhes tudo aquilo que está escrito na lei. Se você já tem noção da lei e entende bem sobre suas bases legais, o que é tratamento de dados, o que são dados, quais são os agentes de tratamento envolvidos e demais características relacionadas à lei, então você poderá passar para o próximo capítulo.

Caso contrário, convido a permanecer por aqui e entender melhor todos esses detalhes abordados pela lei, será muito importante que tenha esse entendimento para seguirmos adiante!

A propósito, vamos revisar a Lei Geral de Proteção de Dados? Para acessar a lei no site do Planalto, clique no link a seguir:

Planalto Lei nº 13.709

[http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709compilado.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm)

A Lei Geral de Proteção de Dados Pessoais (LGPD) se aplica a qualquer empresa, de direito público ou privado, que realize tratamento de dados pessoais, ou seja, que exerça atividade em que se utilizem dados pessoais, seja coleta, armazenamento, exclusão e assim por diante. Considere todo tratamento de dados pessoais, aqueles que forem realizados por meios digitais ou físicos.

A LGPD trata sobre dados pessoais e sua utilização pela empresa que os detém. Perceba que o tratamento dos dados poderão ser inclusive por meios digitais, isso significa que meios físicos de qualquer natureza, também são

protegidos pela lei. Então a organização deverá assegurar que os dados pessoais de seus usuários, clientes e funcionários estejam protegidos.

Nesse contexto, as pessoas passam a ter direitos claros sobre seus dados e sua privacidade com poder de concedê-las ou não a qualquer organização, inclusive podendo solicitar sua exclusão. Há também um aumento do dever das organizações para proteger os dados armazenados em suas bases. Qualquer violação de dados deverá ser reportada aos titulares o mais rápido possível, assim como informações sobre o tratamento e ações que estão sendo realizadas. Com a resolução ou não de um incidente, a organização deverá realizar o levantamento da situação e criar um relatório de violação. No caso da LGPD temos o Relatório de Impacto a Proteção de Dados Pessoais (RIPD) que abordaremos mais à frente. As organizações que não se enquadram ou demonstrarem estar despreparadas para lidar com dados de seus clientes e funcionários de maneira segura, poderão sofrer penalidades por descumprimento da lei.

Considere algumas situações que a LGPD mudará nas organizações:

- Direitos de privacidade pessoal;
- Aumento no dever de proteger dados;
- Relatório de violação obrigatório;
- Penalidades por descumprimento.

Essas são apenas algumas situações de tantas outras que serão abordadas neste livro e que você aprenderá como tratá-los e implantá-los na organização sob sua avaliação.

## O QUE SÃO DADOS À LGPD?

Este capítulo cobre os dispositivos:

Art. 5º I, II, III, IV, XI e XII; Art. 7º § 3º e § 4º

A LGPD como mencionado anteriormente, tem por objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Tem como alguns de seus fundamentos a

privacidade, a liberdade de expressão, a inviolabilidade da intimidade, a livre iniciativa, os direitos humanos etc.

Com isso, a LGPD trata da privacidade e proteção dos dados que podem identificar ou categorizar um indivíduo. Desse modo, no universo de dados mantidos pelas organizações, seja ela por meios físicos ou digitais, são classificadas da seguinte maneira conforme a lei:

- Dados pessoais;
- Dados sensíveis;
- Dados não-pessoais (anonimizados);
- Dados públicos.

Para entendermos melhor como são esses dados, vamos definir que os dados pessoais são aqueles capazes de identificar um indivíduo de forma direta ou indireta. São exemplos de dados pessoais: nome, apelido, endereço residencial, endereço eletrônico, número de um cartão de identificação, hábitos de consumo, dados de localização, cookies, endereço de IP entre outros.

Perceba que os dados pessoais foram divididos em duas formas de identificação, sendo diretos ou indiretos. Para entendermos melhor as diferenças entre essas formas, entenda que os dados pessoais diretos são aqueles compreendidos como óbvios ou com grande chance para identificar determinado indivíduo.

Nome completo ou um apelido, podem ser considerados como um dado pessoal direto, quando ele identifica um indivíduo com um grande grau de confiabilidade ou até a certeza.

Já os dados pessoais indiretos, são aqueles que não identificam um indivíduo com tanta confiança, mas através de meios simples de relacionamento dos dados, conseguimos chegar até o indivíduo titular daquele dado.

Nos casos dos dados pessoais indiretos, considere a seguinte situação. Um estudante do curso de Direito da Faculdade XPTO perdeu o seu cartão do Registro Acadêmico (RA). Nesse cartão, existe apenas o nome da Instituição de

Ensino, curso realizado pelo titular e o código que compreende o seu Registro Acadêmico daquela instituição.

Perceba que neste exemplo, não sabemos quem é o dono daquele cartão, mas poderíamos iniciar uma investigação para conseguirmos encontrar esse indivíduo. Partindo desse princípio, sabemos que essa pessoa estuda na Faculdade XPTO, cursa Direito e possui o número de RA 12345. Obviamente que será muito mais fácil apenas entregar esse cartão na secretaria da faculdade, para que eles o entregaram ao seu dono, pois a instituição de ensino poderá consultar a sua base de dados com seus alunos cadastrados e identificá-lo através do número do RA contido no cartão, devolvendo o cartão ao seu dono.

Partindo desse princípio, percebe que num primeiro momento não conseguimos identificar diretamente o indivíduo titular daqueles dados e dono do cartão da faculdade? Tivemos que traduzir esses dados por meio de uma relação de dados para encontrar o seu dono.

Mas tudo depende da abordagem e da forma como os dados são apresentados, afinal, a interpretação de dados pode fazer sentido para algumas pessoas e não fazer sentido algum para outras. No caso do nome completo, vamos usar um nome que deve ser muito comum em nosso país que é José da Silva.

Dependendo da quantidade de José da Silva que você se depare, o que poderíamos considerar como um dado pessoal direto, se tornou indireto, pela quantidade de pessoas desconhecidas com o mesmo nome. Precisaríamos de mais dados para conseguirmos refinar a nossa busca até encontrarmos o José da Silva desejado. Um apelido também pode fazer mais sentido para alguns do que para outros, podendo para algumas pessoas, fazer sentido algum para identificar determinado indivíduo.

É importante entendermos essas diferenças e situações de interpretação, para conseguirmos distinguir melhor as diferenças e relações entre dados pessoais diretos e indiretos.

O tratamento de dados pessoais ou sensíveis de crianças ou adolescentes, seguem os mesmos critérios para adultos, entretanto, deve-se ter um consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

É importante lembrar que a LGPD abrange apenas os indivíduos que estejam vivos. Quando a LGPD fala em pessoa natural, ela se refere a todos aqueles que nasceram, foram registrados e estão vivos. Logo, a LGPD não oferece proteção aos dados pessoais de pessoas já falecidas.

Os dados sensíveis, são aqueles com capacidade de categorizar um indivíduo, o que poderá ocasionar discriminações. São exemplos de dados sensíveis: opção sexual, opinião política, dados de saúde, opção religiosa, origem racial ou étnica, informações biológicas (DNA, íris, etc), dentre outros.

O tratamento para dados sensíveis possui um apelo especial por parte da LGPD, justamente para combater a discriminação na sua forma geral e a discriminação algorítmica. Entenda que a discriminação algorítmica é aquela que discrimina determinado grupo de pessoas a partir dos seus dados lidos por algum algoritmo computacional.

A discriminação geral para fins de facilidade na compreensão, é toda aquela que é usada para discriminar um indivíduo como por exemplo uma opinião política. Não faria sentido numa entrevista de emprego para concorrer a vaga de Advogado Civil, eu eliminar todos os postulantes à vaga pretendida, por eles terem informado que a sua visão política diverge da visão do avaliador por exemplo. A discriminação algorítmica, independe da avaliação semântica realizada por um ser humano, mas sim por fatores considerados pela Inteligência Artificial a partir daquilo que ela foi programada para fazer.

Por exemplo, vamos supor que uma empresa que oferece cartões de créditos, não aceita liberar seus cartões quando o indivíduo postulante aquele serviço, informou na sua ficha cadastral que mora numa região próximo de uma favela. Obviamente que o sistema para liberar ou não o cartão de crédito (entre outros dados analisados), considerou um alto risco de inadimplência a este indivíduo e automaticamente, impediu a liberação deste serviço sem a necessidade de uma intervenção humana direta.

Claro que a programação desse algoritmo, foi realizada por um humano (ainda tem sido assim) e a Inteligência Artificial apenas executou a sua análise baseada nos parâmetros e limites definidos a ela.

Consegue perceber a importância da LGPD em atribuir importância aos dados sensíveis?!

Por fim, os dados não-pessoais são aqueles que não identificam um indivíduo. Como dados anonimizados, estatísticos e alguns dados considerados públicos. Qualquer dado que não se enquadre como pessoal ou sensível, poderá ser considerado não-pessoal.

Um dado sensível poderá se tornar anonimizado por critérios definidos pelo controlador (adiante esse termo será esclarecido). Entretanto, se for possível reverter esse processo por esforços razoáveis, então um dado aparentemente anonimizado poderá ter a sua proteção aplicável para atender a LGPD.

A lei traz o termo “esforços razoáveis”, mas não esclarece o que e como seriam esses esforços. Num exemplo anterior, usei a situação do cartão RA perdido. Podemos interpretar essa mesma situação como um exemplo de dados anônimos que na realidade eram dados pseudo anônimos, pois através de um esforço que entendo como razoável, entregar esse cartão na secretaria da instituição de maneira que ele possa ser traduzido, identificando seu titular a partir do número do RA, conseguiremos identificar o indivíduo.

Esforços razoáveis podem ser considerados como uma maneira não muito complexa para conseguir identificar um indivíduo a partir de um dado isolado. Mais uma vez, perceba que o entendimento sobre a classificação e interpretação de um dado pode não ser tão objetiva. Após a regulamentação da lei, espera-se que tenhamos algo como uma tabela que esclareça sem dúvidas o que são dados pessoais diretos, indiretos, sensíveis, anônimos ou pseudônimos. Ao menos sob a perspectiva da LGPD.

A isso eu me refiro aos dados que são entendidos como óbvios, como os números do CPF e RG e mesmo assim, a identificação do indivíduo dependerá de uma relação de mais dados. Por exemplo, para a Receita Federal qualquer

CPF relaciona-se ao indivíduo de maneira rápida. Mas não podemos afirmar o mesmo de qualquer pessoa comum como eu ou você, pois se eu apresentar uma lista com cem números de CPF, você saberia com segurança informar qual seria o meu CPF?

A grande questão sobre a segurança dos dados pessoais e sensíveis protegidos pela LGPD, é sobre a possibilidade da sua utilização. Portanto, um dado isolado dificilmente traria alguma vantagem ilícita, mas um conjunto de dados provavelmente sim.

Voltando aos dados anônimos, vamos entender melhor alguns conceitos sobre dados anonimizados:

- Processo de anonimização;
- Dados pseudo anonimizado;
- Reversibilidade da anonimização.

**Processo de anonimização:** É um procedimento técnico que impede ou remove a associação do titular com os dados apresentados.

**Dados pseudo anonimizados:** São os dados que permitem a associação a um titular através de meios técnicos mantidos pelo controlador dos dados. Exemplo disso são bases de dados que se relacionam e permitem a identificação do titular através da relação entre elas.

**Reversibilidade da anonimização:** É a possibilidade de reverter o processo de anonimização realizado. É importante destacar que isso dependerá dos meios técnicos e possibilidade de reversão, para associar os dados então anonimizados aos seus respectivos titulares identificáveis. Esse é um processo que nem sempre será possível de se realizar, caso não haja formas de resgatar a associação entre os dados anonimizados e dados do titular.

Perante a lei, um dado só será considerado efetivamente anonimizado se este não permitir que, por esforços técnicos, seja possível associar novamente o dado anonimizado ao seu titular original. Se isso for possível, então este dado pseudo anonimizado está sujeito à LGPD.

Os dados públicos são disponibilizados por alguma finalidade considerando a boa-fé e o interesse público da sua exposição. A LGPD permite que uma organização possa, sem precisar pedir um novo consentimento, tratar dados tornados públicos anteriormente pelo titular, mas se uma organização quiser compartilhar esses dados com outras, então ela deverá obter um novo consentimento para esta finalidade.

É importante lembrar que a LGPD se relaciona com a LAI (Lei de Acesso à Informação) e com princípios constitucionais que permitem por exemplo, o direito do titular de receber dos órgãos públicos informações de seu interesse particular, coletivo ou geral, desde que estes dados, não estejam protegidos por sigilo relacionado à segurança da sociedade e do Estado.

Por fim, os dados públicos são aqueles que foram manifestados publicamente pelo seu titular ou se tornaram públicos por alguma decisão judicial, como por exemplo as publicações e recortes de processos.

Os dados obtidos por meios públicos devem resguardar os direitos dos titulares e seguir os princípios previstos na LGPD de acordo com o art. 6º .

Um exemplo muito comum de dados manifestados públicos pelo titular, são aqueles que o próprio titular divulga em redes sociais, cartões de visita, grupos em comunicadores instantâneos, etc.

Qualquer outro meio onde os dados foram obtidos publicamente, mas por divulgações sem consentimento dos titulares ou por meio da publicação de listas contendo dados vazados, é ilegal e não podem ser utilizados. Tenha muito cuidado em obter as famigeradas listas de leads de fontes que não possuem critérios de segurança ou padrões de adequação alinhadas à LGPD.

Tenho observado que algumas pessoas usam os grupos de mensagens instantâneas como Telegram ou WhatsApp, para divulgar seus serviços, capturando os contatos nesses grupos, para divulgar seus serviços individualmente e sem consentimento dos titulares.

É importante observar que no caso descrito, deve ficar entendida a finalidade do grupo. Por exemplo, se um grupo de WhatsApp reúne profissionais de uma categoria, então é compreensível que as pessoas desse

grupo estão ali para um propósito comercial, seja para receber as novidades ou fazer negócios com outras pessoas.

Se for um grupo sobre discussão religiosa apenas, então presume-se que os contatos estão ali para esse propósito e não para serem abordadas comercialmente, num estilo de marketing agressivo. É importante ter noção dessas situações, pois interpretações sobre se os dados são públicos ou não, podem tornar esse conceito confuso em algum momento.

Na dúvida, siga as orientações da LGPD à risca.

## AGENTES DE TRATAMENTO

Este capítulo cobre os dispositivos:  
Art. 5º V, VI, VII, VIII, IX, XIX

A lei define alguns tipos de agentes com direitos e deveres dentro do contexto da proteção de dados. A LGPD traz a importância de ter os envolvidos com os dados pessoais mapeados. Os dados transitam entre os agentes denominados:

- Titular;
- Controlador;
- Operador;
- Encarregado;
- Autoridade Nacional de Proteção de Dados.

**Titular:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. O titular é o verdadeiro dono dos seus dados e quando ele utiliza algum serviço, ele deve ter consentimento e concordância sobre a utilização dos seus dados e finalidade. Exemplo real: clientes dos aplicativos e serviços fornecidos pela organização.

**Controlador:** Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; Os controladores deverão manter pública a informação sobre os tipos de dados