CURSO LGPD

LEI GERAL DE PROTEÇÃO DE DADOS

IEL

Instituto Euvaldo Lodi

PELO FUTURO DA INDÚSTRIA

SUMÁRIO

MÓDULO 01 - GOVERNANÇA, COMPLIANCE E HISTÓRICO DA LGPD 5

AULA 01 - APRESENTAÇÃO DO CURSO E DO PROFESSOR 6

AULA 02 – O QUE É A LEI GERAL DE PROTEÇÃO DE DADOS? 6

AULA 03 – QUAL A RELAÇÃO ENTRE LGPD E GOVERNANÇA? 8

AULA 04 – QUAL A RELAÇÃO ENTRE LGPD E *COMPLIANCE*? 10

AULA 05 – O QUE É PRIVACIDADE E POR QUE DEVEMOS PROTEGÊ-LA? 11

AULA 06 – COMO SÃO TRATADAS AS LEIS DE PRIVACIDADE NO MUNDO 12

AULA 07 - LINHA DO TEMPO DA PROTEÇÃO DE DADOS NO BRASIL 15

MÓDULO 02 - DIREITO À PRIVACIDADE E PROTEÇÃO DE DADOS, BEM COMO SUA RESSIGNIFICAÇÃO NO MUNDO DIGITAL 20

AULA 08 – PRIVACIDADE E PROTEÇÃO DE DADOS COMO DIREITO GARANTIDO – PARTE 1 21

AULA 09 - PRIVACIDADE E PROTEÇÃO DE DADOS COMO DIREITO GARANTIDO – PARTE 2 22

AULA 10 – PRIVACIDADE NA NOVA ECONOMIA – PARTE 1 23

AULA 11 – PRIVACIDADE NA NOVA ECONOMIA – PARTE 2 24

MÓDULO 03 - OS PRINCÍPIOS, FUNDAMENTOS E CONCEITOS DA LGPD 26

AULA 12 – OS FUNDAMENTOS DA LGPD – PARTE 1 27

AULA 13 - FUNDAMENTOS DA LGPD – PARTE 2 28

AULA 14 – OS PRINCÍPIOS DA LGPD – PARTE 1 31

AULA 15 – OS PRINCÍPIOS DA LGPD – PARTE 2 33

AULA DE REVISÃO 01 34

AULA 16 – REVISÃO MÓDULO 01 - GOVERNANÇA, COMPLIANCE E HISTÓRICO DA LGPD. 34

AULA 17 - REVISÃO MÓDULO 02 – DIREITO À PRIVACIDADE E PROTEÇÃO DE DADOS, BEM COMO SUA RESSIGNIFICAÇÃO NO MUNDO DIGITAL 36

AULA 18 - REVISÃO MÓDULO 03 - OS PRINCÍPIOS, FUNDAMENTOS E CONCEITOS DA LGPD 38

MÓDULO 04 - INTRODUÇÃO À APLICAÇÃO PRÁTICA DA LEI GERAL DE PROTEÇÃO DE DADOS, COM EXPOSIÇÃO DAS BASES LEGAIS QUE JUSTIFICAM O TRATAMENTO DE DADOS PESSOAIS DENTRO DE UMA INSTITUIÇÃO 41

AULA 19 – APLICAÇÃO TERRITORIAL DA LEI GERAL DE PROTEÇÃO DE DADOS E SUAS BASES LEGAIS 42

AULA 20 – CONSENTIMENTO E CUMPRIMENTO DE OBRIGAÇÃO LEGAL E REGULATÓRIA 44

AULA 21 – EXECUÇÃO DE POLÍTICAS PÚBLICAS, REALIZAÇÃO DE ESTUDOS POR ÓRGÃO DE PESQUISA E DE EXECUÇÃO DE CONTRATOS 47

AULA 22 – EXERCÍCIO REGULAR DE DIREITOS EM PROCESSOS JUDICIAIS, ADMINISTRATIVOS OU ARBITRAIS E PROTEÇÃO À VIDA OU À INCOLUMIDADE DO TITULAR OU DE TERCEIROS 48

AULA 23 – TUTELA DA SAÚDE, LEGÍTIMO INTERESSE E PROTEÇÃO AO CRÉDITO 49

MÓDULO 05 - TRATAMENTO E MAPEAMENTO DE DADOS 51

AULA 24 – O QUE É TRATAMENTO DE DADOS? 52

AULA 25 – O QUE É MAPEAMENTO DE DADOS? 53

AULA 26 - MAPEAMENTO DE DADOS NA PRÁTICA 54

MÓDULO 06 - AGENTES DE TRATAMENTO: CONTROLADORES E OPERADORES 56

AULA 27 – CONTROLADOR E CO-CONTROLADOR DE DADOS PARTE 1 57

AULA 28 – CONTROLADOR E CO-CONTROLADOR DE DADOS PARTE 2 57

AULA 29 – OPERADOR E SUB-OPERADOR DE DADOS – PARTE 1 58

AULA 30 – OPERADOR E SUB-OPERADOR DE DADOS – PARTE 2 59

AULA DE REVISÃO 02 60

AULA 31 - REVISÃO MÓDULO 04 – INTRODUÇÃO A APLICAÇÃO PRÁTICA DA LEI GERAL DE PROTEÇÃO DE DADOS COM EXPOSIÇÃO DAS BASES LEGAIS QUE JUSTIFICAM O TRATAMENTO DE DADOS PESSOAIS DENTRO DE UMA INSTITUIÇÃO. 60

AULA 32 - REVISÃO MÓDULO 05 – TRATAMENTO E MAPEAMENTO DE DADOS PESSOAIS 62

AULA 33 - REVISÃO MÓDULO 06 – AGENTES DE TRATAMENTO: CONTROLADORES E OPERADORES 63

MÓDULO 07 - O ENCARREGADO DE DADOS E SUAS RESPONSABILIDADES 65

AULA 34 - O ENCARREGADO DE DADOS NA LGPD 66

AULA 35 - O PERFIL E INDICAÇÃO DO ENCARREGADO DE DADOS 67

AULA 36 - MODALIDADES DE CONTRATAÇÃO DO ENCARREGADO DE DADOS 67

AULA 37 – A RESPONSABILIDADE DO ENCARREGADO DE DADOS 69

AULA 38 – O QUE É A ANPD? 71

AULA 39 – ATIVIDADES ESSENCIAIS DA ANPD – PARTE 1 71

AULA 40 – ATIVIDADES ESSENCIAIS DA ANPD – PARTE 2 72

AULA 41 - ENTIDADES FISCALIZADORAS DE PROTEÇÃO DE DADOS NO ÂMBITO INTERNACIONAL 73

MÓDULO 09 - TIPOS DE SANÇÕES E PARÂMETROS DE APLICAÇÃO DE PENALIDADES ENVOLVENDO LGPD COM ESTUDO DE CASO 75

AULA 42 – TIPOS DE SANÇÕES APLICADAS PELA ANPD PARTE 1 76

AULA 43 - TIPOS DE SANÇÕES APLICADAS PELA ANPD PARTE 2 77

AULA 44 – OS PARÂMETROS DE APLICAÇÃO DE SANÇÕES PELA ANPD 79

AULA 45 – REFLEXOS JUDICIAIS DO DESCUMPRIMENTO DA LGPD 80

AULA 46 – CASOS JUDICIAIS ENVOLVENDO A LGPD 81

AULA DE REVISÃO 03 87

AULA 47 - REVISÃO MÓDULO 07 - O ENCARREGADO DE DADOS E SUAS RESPONSABILIDADES 87

AULA 48 - REVISÃO MÓDULO 08 - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) - SUA IMPORTÂNCIA E FUNCIONAMENTO. 88

AULA 49 – REVISÃO MÓDULO 09 - TIPOS DE SANÇÕES E PARÂMETROS DE APLICAÇÃO DE PENALIDADES ENVOLVENDO LGPD COM ESTUDO DE CASO 90

MÓDULO 10 - AÇÕES DE ADEQUAÇÃO À LGPD: SEGURANÇA DA INFORMAÇÃO 93

AULA 50 – PRINCIPAIS MEDIDAS TÉCNICAS PARA IMPLEMENTAÇÃO DA LGPD 94

AULA 51 – A IMPORTÂNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO 95

AULA 52 – OS 20 CONTROLES CIS – PARTE 1 95

AULA 53 – OS 20 CONTROLES CIS – PARTE 2 98

AULA 54 - SEGURANÇA DA INFORMAÇÃO NA VIDA PESSOAL E PROFISSIONAL 101

AULA 55 - PRINCIPAIS AMEAÇAS EM AMBIENTES LÓGICOS 102

AULA 56 - PRINCIPAIS AMEAÇAS EM AMBIENTES FÍSICOS 103

MÓDULO 11 - AÇÕES DE ADEQUAÇÃO À LGPD: PROJETO DE ADEQUAÇÃO E DA GOVERNANÇA DE PROTEÇÃO DE DADOS 104

AULA 57 – COMO ESTRUTURAR UM PROGRAMA DE GOVERNANÇA 105

AULA 58 - A IMPORTÂNCIA DE SE INSTITUIR UM COMITÊ DE PRIVACIDADE 106

AULA 59 – ETAPAS PARA IMPLEMENTAÇÃO DA LGPD PARTE 1 107

AULA 60 – ETAPAS PARA IMPLEMENTAÇÃO DA LGPD PARTE 2 109

AULA 61 – DIAGNÓSTICO PARA IMPLEMENTAÇÃO DA LGPD 110

AULA 62 – A IMPORTÂNCIA DE UM PLANO DE AÇÃO 112

MÓDULO 12 - COMPLIANCE E LGPD COM EXEMPLO PRÁTICO DE UM PROJETO DE ADEQUAÇÃO 114

AULA 63 – INTRODUÇÃO AO COMPLIANCE DIGITAL 115

AULA 64 – A IMPORTÂNCIA DA GESTÃO DE TERCEIROS 116

AULA 65 – COMO MANTER UM PROGRAMA DE *COMPLIANCE* À LGPD 118

AULA 66 – ESTABELECENDO O "TONE AT THE TOP" 120

AULA 67 – EXEMPLOS PRÁTICOS DE IMPLEMENTAÇÃO DA LGPD 121

AULA DE REVISÃO 04 122

AULA 68 - REVISÃO MÓDULO 10 - AÇÕES DE ADEQUAÇÃO À LGPD: SEGURANÇA DA INFORMAÇÃO 122

AULA 69 - REVISÃO MÓDULO 11 - AÇÕES DE ADEQUAÇÃO À LGPD: PROJETO DE ADEQUAÇÃO E DA GOVERNANÇA DE PROTEÇÃO DE DADOS 125

AULA 70 - REVISÃO MÓDULO 12 – COMPLIANCE E LGPD COM EXEMPLO PRÁTICO DE UM PROJETO DE ADEQUAÇÃO 127

MÓDULO 01

GOVERNANÇA, COMPLIANCE E HISTÓRICO DA LGPD

]

AULA 01 - APRESENTAÇÃO DO CURSO E DO PROFESSOR

Prezado(a) Aluno (a),

Com o objetivo auxiliar o entendimento da LGPD (Lei Geral de Proteção de Dados n. 13.709/18 aprovada em agosto de 2018), o IEL conta com o apoio do Instituto Latino - Americano de Governança e Compliance Público (IGCP), que tem como missão promover, disseminar e colaborar na implementação de políticas de Governança e Compliance no Brasil e na América Latina.

Nesse contexto, o IGCP desenvolveu um Curso de Capacitação em LGPD que tem como objetivo a construção de competências, habilidades e atitudes necessárias para uma atuação profissional totalmente de acordo com as diretrizes atuais sobre a proteção de dados.

O presente curso conta com 15 módulos de aprendizagem, que abordam aspectos teóricos e práticos envolvendo a Lei Geral de Proteção de Dados, Segurança da Informação e Projetos de Adequação. Portanto, para o máximo aproveitamento de cada módulo, é altamente recomendável que as aulas sejam assistidas com atenção e assiduidade.

Sua trilha de aprendizagem neste Curso será guiada pelo **Professor Lucas Paglia**, que é pós-graduado em *Compliance* pela Fundação Getúlio Vargas – FGV, certificado pelo INSPER em Proteção de Dados & Privacidade, e certificado como Especialista PMO (Líder de Projeto) para Governança em Privacidade pelo *Data Privacy Brasil*. Lucas também é professor da Unicamp, Presidente do Comitê de LGPD da Rede Governança Brasil - RGB e sócio fundador da empresa de consultoria P&B *Compliance*.

AULA 02 – O QUE É A LEI GERAL DE PROTEÇÃO DE DADOS?

Como a preocupação com a proteção dos dados pessoais tem crescido cada vez mais, considerando o *boom* nas relações e transferências instantâneas de informações no âmbito virtual, foi inevitável que no Brasil fosse estabelecida uma legislação para tratar do assunto.

Assim, de forma um pouco tardia, foi promulgada no Brasil a Lei Geral de Proteção de Dados (Lei 13.709 de 2018), entrando em vigor apenas em 18 de setembro de 2018 de forma parcial, uma vez que as sanções que podem ser aplicadas às empresas por violação à lei apenas entraram em vigor em 1 de agosto de 2021. A lei surgiu com o objetivo de estabelecer regras específicas para o tratamento (qualquer operação realizada com um dado pessoal, como por exemplo o *armazenamento*), criar responsabilidades às empresas, além de estabelecer diversas diretrizes a serem seguidas.

Há que se dizer que a LGPD possui bastante influência do Regulamento da União Europeia, como os seus princípios e direitos dos titulares de Dados. Essa semelhança

com a GDPR facilita a aplicação da legislação brasileira e adequação às novas exigências que são impostas às empresas.

No Brasil, após a aprovação de uma lei, existe um período chamado de *vacatio legis,* que compreende o período entre o dia da publicação da lei e a sua entrada em vigor. No caso da Lei Geral de Proteção de Dados, várias foram as movimentações legislativas para alterar os prazos de vigor de seus dispositivos. O resultado prático dessas movimentações foi o seguinte:

- **28 de dezembro de 2018**: Entrada em vigor dos artigos 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B;
- **14 de agosto de 2020**: Entrada em vigor, ressalvados os artigos 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B (Referentes à criação da Autoridade Nacional de Proteção de Dados);
- **1 de agosto de 2021**: Entrada em vigor dos artigos 52, 53 e 54 (Referentes às sanções administrativas).

Finalmente, em agosto de 2021, a Lei Geral de Proteção de Dados passou a ser aplicada no Brasil. Com dez capítulos e 65 artigos, a LGPD é a norma brasileira mais específica sobre privacidade e proteção de dados. O conteúdo mais importante da lei está distribuído entre os seguintes capítulos:

CAPÍTULO 1: Contendo apenas seis artigos, este capítulo dispõe sobre os fundamentos, princípios e conceitos da Lei. Através dele é que se determina o modo de interpretação da LGPD e a vontade do legislador ao regular a matéria.

CAPÍTULO 2: Este capítulo contém tópicos sobre o tratamento de dados pessoais, definindo diretrizes às hipóteses que poderão ocorrer, prevendo peculiaridades entre dados pessoais, dados pessoais sensíveis, dados de crianças e adolescentes e algumas observações sobre o término do tratamento de dados.

CAPÍTULO 3: É aqui que se encontra o cerne da LGPD, uma vez que o rol de Direitos do Titular está previsto durante todo o capítulo. Esta parte da lei busca garantir mecanismos aos titulares para que possam fazer valer seus direitos envolvendo dados pessoais, como os seguintes: confirmação, acesso, correção, anonimização, bloqueio ou eliminação, portabilidade e informação sobre dados pessoais, bem como a revogação de seu consentimento.

CAPÍTULO 4: Neste capítulo há previsões sobre o tratamento de dados pelo Poder Público, determinando diretrizes para que seus órgãos desempenhem suas atividades com lisura, isto é, sem esbarrar nos dispositivos da própria LGPD.

CAPÍTULO 5: Este capítulo versa sobre a transferência internacional de dados. Considerando que é sempre complexo estabelecer limites a países estrangeiros, o legislador se limitou a discorrer sobre as possibilidades de tratamento internacional, bem como sobre algumas atribuições da Autoridade Nacional envolvendo a matéria.

CAPÍTULO 6: Aqui há a previsão de algumas atividades dos agentes de tratamento (controlador e operador de dados), que serão abordados a seguir, bem como suas atividades e responsabilidades.

CAPÍTULO 7: Este capítulo discorre brevemente sobre a importância de os agentes de tratamento adotarem controles de segurança, bem como promoverem boas práticas de segurança à informação e regras de governança.

CAPÍTULO 8: Aqui ficam os artigos mais temidos pelos agentes de tratamento de dados pessoais. O capítulo trata das sanções administrativas e das atividades de fiscalização da Autoridade Nacional, mas o faz de forma introdutória. Isto, pois o legislador reservou à ANPD a responsabilidade da regulação deste processo, o que se iniciou com a Resolução n. 1, publicada em outubro de 2021.

CAPÍTULO 9: Este capítulo é responsável por instituir dois órgãos fundamentais para efetividade da lei: a Autoridade Nacional de Proteção de Dados e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

CAPÍTULO 10: Dispõe sobre aspectos pontuais envolvendo competências da ANPD e de outros órgãos públicos, bem como prevê os artigos de *vacatio legis* apontados anteriormente.

AULA 03 – QUAL A RELAÇÃO ENTRE LGPD E GOVERNANÇA?

De acordo com o próprio Instituto Brasileiro de Governança Corporativa (IBGC), a Governança Corporativa é:

> "(...) o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. "

A união entre o conceito de Governança Corporativa e as diretrizes extraídas da LGPD, nos permite entender por que ambos exercem papel fundamental na criação de uma cultura de proteção de dados dentro das instituições.

Cumpre ressaltar que os princípios básicos da Governança Corporativa estão alinhados com princípios da Lei Geral de Proteção de Dados. A partir da leitura do Código das Melhores Práticas de Governança Corporativa (visite o código neste link), podemos identificar quais são **os 4 (quatro) princípios da Governança Corporativa**:

- **Transparência** – Consiste no desejo de disponibilizar para as partes interessadas as informações que sejam de seu interesse e não apenas aquelas impostas por disposições de leis ou regulamentos. Não deve restringir-se ao desempenho econômico-financeiro, contemplando também os demais fatores (inclusive intangíveis) que norteiam a ação gerencial e que conduzem à preservação e à otimização do valor da organização;

- **Equidade** – Caracteriza-se pelo tratamento justo e isonômico de todos os sócios e demais partes interessadas (stakeholders), levando em consideração seus direitos, deveres, necessidades, interesses e expectativas;
- **Prestação de contas (*accountability*)** – Os agentes de governança devem prestar contas de sua atuação de modo claro, conciso, compreensível e tempestivo, assumindo integralmente as consequências de seus atos e omissões e atuando com diligência e responsabilidade no âmbito dos seus papéis;
- **Responsabilidade corporativa** – Os agentes de governança devem zelar pela viabilidade econômico-financeira das organizações, reduzir as externalidades negativas de seus negócios e suas operações e aumentar as positivas, levando em consideração, no seu modelo de negócios, os diversos capitais (financeiro, manufaturado, intelectual, humano, social, ambiental, reputacional etc.) no curto, médio e longo prazos.

Em seguida, os princípios básicos de Governança Corporativa devem ser convertidos em recomendações objetivas, por meio de boas práticas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da empresa, contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum.

A partir do momento que percebemos a importância da Governança Corporativa e enxergamos os princípios que ela compartilha com a própria lei Geral de Proteção de Dados, não restam dúvidas sobre sua influência no Projeto de Adequação à LGPD.

Aplicando-se os preceitos da governança dentro do projeto de adequação à LGPD, é possível organizar e entender as funcionalidades da empresa, orientando e conscientizando todos os membros da instituição, desde a alta direção até os membros que não possuem autonomia para tomar decisões. Desta forma, é possível disseminar a cultura de proteção de dados na instituição.

Durante um projeto de adequação à LGPD, é necessário que todas as áreas trabalhem em conjunto, mas principalmente é de extrema importância o trabalho em parceria entre as áreas de Tecnologia e Segurança da Informação, Controladoria e, caso ainda não exista, a implementação do comitê de privacidade.

Trabalhando conjuntamente, esses departamentos poderão entender de forma ampla como é realizado o tratamento de dados pessoais dentro da companhia, realizando as adequações necessárias e, ainda, constatando se algum procedimento interno não segue as regras da Governança Corporativa.

É de suma importância que as empresas implementem práticas relacionadas a proteção de dados pessoais no cotidiano, mantendo os fluxos e riscos mapeados, sempre com objetivo de evitar qualquer dano à empresa e, tratando-se de LGPD, dano aos titulares de dados pessoais. Além disso, é recomendada a criação de um departamento exclusivo para governança de dados pessoais, entretanto, as áreas devem continuar agindo de forma conjunta para manter toda a empresa preservada.

Ademais, devem ser adotados mecanismos que garantam a segurança dos dados pessoais dos colaboradores e de qualquer outro titular que forneça os dados à empresa.

Conclui-se, então, que o projeto de adequação à LGPD (que será esmiuçado mais à frente no curso) é realizado em observância à preceitos da Governança Corporativa.

Com a finalização do projeto de adequação, torna-se imprescindível a manutenção das práticas adotadas a partir do Programa de Governança, para que seja possível manter a segurança dos dados pessoais tratados pela empresa.

AULA 04 – QUAL A RELAÇÃO ENTRE LGPD E *COMPLIANCE*?

A palavra compliance tem origem no verbo inglês *to comply*, que significa agir de acordo com uma regra, uma instrução interna, um comando ou um pedido. No âmbito corporativo, o compliance pode ser interpretado como um conjunto de ações que tem como objetivo assegurar que as empresas estejam adequadas às leis, normas de boa conduta, regulamentos, entre outros critérios que servem para minimizar riscos e manter a organização dentro da legalidade.

Nesse sentido, a LGPD surge como mais um processo de adequação pelo qual as empresas precisam passar.

Um sistema de gestão de compliance eficaz permite que a empresa demonstre, na prática, seu comprometimento com as suas obrigações previstas, ou não, em lei. Em síntese, trata-se da adoção de práticas integradas, com o objetivo de assegurar o bom funcionamento do ambiente corporativo.

É nesse contexto que a LGPD deve ser inserida, uma vez que um processo de adequação a LGPD tem como objetivo a implementação permanente de um programa de proteção de dados, com foco na adequação de controles e na construção de uma cultura organizacional pautado pelo respeito às normas de proteção de dados.

Assim, a área de compliance deve ser instrumento para a concretização do projeto de adequação à LGPD

Além disso, existem alguns pontos importantes com relação aos princípios de Compliance que são essenciais em qualquer ação relacionada à adequação à Lei Geral de Proteção de Dados.

Ainda, é importante destacar que o setor de compliance de uma empresa terá papel fundamental tanto no desenvolvimento, quanto na manutenção do projeto de adequação à LGPD. Isto porque (conforme será explicado em momento oportuno), é interessante que o setor de compliance faça parte do Comitê de Privacidade, área especifica que poderá ser criada durante o projeto de adequação.

Em contrapartida, a adequação à LGPD também exerce influência sobre o desenvolvimento do compliance, uma vez que os programas de compliance precisam

estar de acordo com o disposto na LGPD, afinal, serão tratados diversos dados pessoais durante todo o processo.

Nesse sentido, conclui-se que para otimizar os processos organizacionais e manter a regularidade das atividades, LGPD e compliance devem atuar de forma harmônica e complementar.

AULA 05 – O QUE É PRIVACIDADE E POR QUE DEVEMOS PROTEGÊ-LA?

A preocupação com a privacidade e a liberdade dos cidadãos tende a crescer cada vez mais com o desenvolvimento de novos dispositivos e tecnologias. Não raro, nos deparamos com matérias relacionadas ao vazamento de dados de empresas, expondo milhares e até mesmo milhões de usuários, impactando empresas nos aspectos jurídicos, financeiros e reputacionais.

Sobretudo com sociedades altamente globalizadas e conectadas, as pessoas e seus dados pessoais tendem a ficar mais e mais vulneráveis, existindo uma grande necessidade de regulamentação de diversas práticas (legais, técnicas e organizacionais) para que cidadãos não sejam prejudicados.

Até recentemente, os países não contavam com qualquer regulamentação sobre o tema de proteção de dados. Logo, inexistindo penalidades às empresas infratoras, as práticas relacionadas ao tratamento de dados pessoais não necessariamente garantiam a privacidade dos titulares. É por isso que a privacidade tem sido um dos tópicos mais discutidos no mundo desde o surgimento da rede mundial: com o surgimento da denominada internet das coisas, os ambientes digital e real se fundem, fazendo com que precisemos retomar discussões sobre assuntos que antes nos pareciam claros e pacificados. **Então, o que exatamente é privacidade?**

A palavra “privado” é uma derivação do vocábulo latino “privatus”, que significa algo “retirado da vida pública”. Por consequência, podemos entender que o substantivo **privacidade** representaria a ideia de um estado ou condição de algo que é privado. Ao promovermos privacidade, portanto, buscamos evitar que algo seja de conhecimento ou acesso público, reservando essa permissão apenas àqueles que consideramos aptos a obtê-la.

Agora que percorremos o conceito etimológico de privacidade e entendemos melhor o que ela significa, podemos aplicar esse conceito em nossa vida digital: privacidade significa o estado de segurança atingido ao impedir que pessoas ou sistemas tenham acesso não autorizado a quaisquer dados pertencentes a um Titular (pessoa física ou natural), o que se obtém principalmente através da proteção de dados.

E POR QUE DEVEMOS PROTEGER NOSSA PRIVACIDADE?

Responder a esse questionamento se torna uma tarefa mais fácil quando pensamos em nossas casas: não seria nada confortável permitir que pessoas desconhecidas entrassem em nossas residências sem qualquer tipo de autorização, correto? No ambiente físico, isso fica muito evidente, pois há muito tempo as sociedades possuem legislações que impõem algum tipo de restrição à violação ou invasão de propriedades privadas, em um esforço de se garantir os direitos dos reais proprietários.

A noção de privacidade passa a ficar mais complexa quando pensamos no ambiente virtual, que é considerado extremamente recente em nossa história. Vale ressaltar que somente a partir dos anos 80 é que recursos de tecnologia da informação começaram a se democratizar, sendo antes restritos a grupos sociais muito específicos. Até recentemente, não possuíamos qualquer tipo de legislação que pudesse garantir proteção à nossa privacidade especificamente em ambientes virtuais, tornando esses locais propícios a todo o tipo de golpes e invasões.

Apesar disso, podemos dizer que a privacidade nas redes deve ser protegida para impedir que o usuário tenha suas informações expostas de forma indevida, o que pode torná-lo vítima de crimes, ameaças e prejuízos financeiros. Proteger a privacidade do indivíduo significa, em última análise, proteger sua segurança. Assim, com o advento das novas legislações e normas técnicas sobre o assunto, a proteção à privacidade tende a ser considerada universalmente, abrangendo tanto o ambiente físico quanto o virtual, cada um com mecanismos jurídicos próprios.

AULA 06 – COMO SÃO TRATADAS AS LEIS DE PRIVACIDADE NO MUNDO

São diversas as leis sobre proteção de dados ao redor do mundo, mas neste curso trataremos apenas das principais e mais relevantes legislações. Para que se entenda o surgimento desses instrumentos, precisamos antes relembrar alguns pontos históricos importantes.

A preocupação com a proteção de dados pessoais, especificamente com a privacidade (lembre-se, a proteção de dados leva à proteção da privacidade), já estava presente na Declaração Universal de Direitos Humanos de 1948, mesmo que de forma genérica:

> Artigo 12 - Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e

> reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.[1]

Em 1950, na União Europeia, a preocupação com a privacidade também foi tema, também de forma mais introdutória e geral, na Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais:

> Artigo 8º - Direito ao respeito pela vida privada e familiar
>
> 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
>
> 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.[2]

De forma similar, podemos encontrar alguma previsão sobre proteção à privacidade no Pacto San Jose da Costa Rica:

> Artigo 11 - Proteção da honra e da dignidade 1. Toda pessoa tem direito ao respeito da sua honra e ao reconhecimento de sua dignidade. 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação. 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.[3]

Com o passar do tempo e considerando o aumento da transferência de dados entre países em razão da própria globalização, em 1980 a OCDE (Organização para a Cooperação e Desenvolvimento Econômico), elaborou as Diretrizes sobre a Proteção de Privacidade e Circulação Transfronteiriça de Dados (*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*). Como essas diretrizes não possuem força de lei, foram consideradas como uma *soft law*, ou seja, uma percursora regulamentação sobre o assunto.

---

[1] ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948. Disponível em: <https://www.ohchr.org/en/udhr/documents/udhr_translations/por.pdf>. Acessos em 03 dez. 2021.

[2] CONVENÇÃO EUROPEIA DOS DIREITOS DO HOMEM, 1950. Disponível em: <https://www.echr.coe.int/documents/convention_por.pdf>. Acessos em 03 dez. 2021.

[3] CONVENÇÃO AMERICANA DE DIREITOS HUMANOS, 1969. Disponível em: <https://www.conjur.com.br/dl/pacto-san-jose-costa-rica.pdf>. Acessos em 03 dez. 2021.

Sequencialmente, pouco antes do Regulamento Europeu, a União Europeia trouxe a Diretiva 95/46/CE, que previa as diretrizes para que os dados fossem enviados para outros países, ressaltando que era necessário que o país receptor dos dados enviados possuísse um nível adequado de proteção de dados pessoais.

UNIÃO EUROPEIA - GDPR (GENERAL DATA PROTECTION REGULATION)

Anteriormente à Lei Geral de Proteção de Dados no Brasil, entrou em vigor o Regulamento Geral sobre Proteção de Dados na União Europeia. O mencionado Regulamento foi aprovado em 2016 e no dia 25 de maio de 2018 entrou definitivamente em vigor.

O Regulamento é sensivelmente mais extenso do que a lei brasileira, possuindo 99 artigos e serviu como base para a composição da LGPD. Ressalta-se que a lei brasileira não é um reflexo absoluto da legislação europeia, existindo diversas diferenças que são apenas aplicáveis no Brasil.

Além dos mencionados artigos, o regulamento é acompanhado de 173 *Recitals* (Considerandos) que direcionam a compreensão dos artigos da lei. A legislação possui um escopo bem amplo e, similarmente à lei brasileira, imputa às empresas algumas penalidades em caso de descumprimento de seus artigos.

Ressalta-se que a GDPR se aplica às seguintes organizações: empresas que são internacionais e possuem filiais na União Europeia; empresas com filial ou representação na União Europeia; empresas que, mesmo sem presença física na União Europeia, ofereçam serviços ao mercado europeu, coletem dados de pessoas naturais localizadas na União Europeia, monitorem pessoais naturais localizadas na União Europeia e/ou terceirizem o processamento de dados para empresas localizadas na União Europeia.

Ou seja, a legislação tem uma aplicação que **não é limitada ao território da União Europeia,** dependendo da operação da empresa. Assim, mesmo que a empresa não possua a sua sede física no território da União Europeia, precisará estar adequada à legislação para não sofrer qualquer tipo de penalidade.

ESTADOS UNIDOS

Antes de ser tratado o assunto da legislação no Brasil, os Estados Unidos passaram a adotar normas e regulações interessantes sobre a proteção de dados, abrangendo tanto legislações federais quanto estaduais sobre a matéria. Diferentemente do Brasil, nos Estados Unidos o sistema jurídico adotado é o *common law*, que tem por base a utilização de julgamentos anteriores (precedentes), dependendo menos da elaboração de regulamentos pelo poder legislativo.

Assim, mesmo possuindo um sistema jurídico diferente do brasileiro, os Estados Unidos também possuem legislações que tratam sobre o tema de proteção de dados, mas são poucas as legislações **específicas** sobre o tema. De forma abrangente, os Estados Unidos possuem em torno de 7 (sete) leis federais. Entretanto, uma delas é de extrema relevância, chamada de COPPA (*Children's Online Privacy Protection Act*), que regulamenta a utilização das informações de crianças menores de 13 (treze) anos por certos tipos de empresas, principalmente quando se trata de utilização desses dados na internet.

No âmbito estadual, os Estados Unidos possuem duas legislações que tratam do assunto de forma mais específica, sendo a CCPA (California Consumer Privacy Act) e a NY SHIELD (New York Stop Hacks and Improve Eletronic Data Security Act).

A CCPA é a legislação da Califórnia que traz novos direitos aos consumidores, de forma que eles possam ter maior controle de suas próprias informações, além de estabelecer algumas diretrizes para certas empresas. Já o NY SHIELD é a legislação da Nova Iorque que estendeu a lei de notificação de violação de dados existentes no estado, exigindo que certas empresas tenham certos cuidados durante o tratamento dos dados pessoais, além de solicitar uma maior transparência para com os titulares de dados pessoais.

AULA 07 - LINHA DO TEMPO DA PROTEÇÃO DE DADOS NO BRASIL

Antes mesmo da entrada em vigor da Lei Geral de Proteção de Dados, o Brasil já tratava de questões de privacidade, liberdade e outros direitos fundamentais na Constituição Federal e em outros instrumentos jurídicos, como por exemplo o Código Civil, o Código de Defesa do Consumidor e o Marco Civil da Internet.

No entanto, sem qualquer regulamentação específica e inexistindo penalidades às empresas, as práticas relacionadas aos dados pessoais não encontravam restrições. Nosso objetivo, nesta aula, é explorar cada um dos pontos que culminaram na promulgação da Lei Geral de Proteção de Dados em 2018.

1988 – CONSTITUIÇÃO DA REPÚBLICA

Com o processo de redemocratização nacional impulsionado pela Constituição Federal de 1988, também denominada Constituição Cidadã, foi amplamente debatida pela Assembleia Constituinte a necessidade de um rol de direitos e garantias fundamentais aos brasileiros. Como consequência disso, hoje encontramos na Constituição uma série de incisos que resguardam direitos referentes à privacidade do cidadão. Podemos mencionar os seguintes:

> Art. 1° A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:
>
> III - a **dignidade** da pessoa humana;
>
> Art. 5° Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> X - **são invioláveis a intimidade, a vida privada,** a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
>
> XII **- é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas**, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;[4]

Assim, conforme visto, a Constituição Federal dispõe sobre aspectos elementares envolvendo a privacidade e proteção de dados, mesmo que de forma indireta, uma vez que não se imaginava à época a necessidade de dispositivos específicos sobre proteção de dados da forma como percebemos atualmente.

1990 – CÓDIGO DE DEFESA DO CONSUMIDOR

Pouco após a Constituição Federal é promulgado o Código de Defesa do Consumidor. Aqui, a intenção do legislador foi de tutelar relações de consumo, prevendo uma série de direitos e deveres aos cidadãos e empresas. No entanto, ao fazê-lo, também foram incluídos no documento artigos importantes à noção atual de direitos dos Titulares de Dados Pessoais, tais como a solicitação de acesso e correção de dados. O seguinte excerto demonstra essa previsão:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
>
> § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

[4] BRASIL, 1988. Constituição da República Federativa do Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acessos em 03 dez. 2021.

§ 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

§ 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.[5]

Como se pode observar, esses direitos dialogam sobretudo com o princípio da transparência, previsto na LGPD. Esse e outros princípios serão abordados de forma detalhada nos módulos seguintes.

2011 – LEI 12.527 – LEI DE ACESSO À INFORMAÇÃO

Embora direcionada especificamente a órgãos públicos, a Lei de Acesso à Informação (LAI) dispõe sobre algumas prerrogativas do cidadão, tratando-se o acesso à informação como direito fundamental e estabelecendo alguns conceitos, como os seguintes:

Art. 4° Para os efeitos desta Lei, considera-se:

I - **informação**: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

II - **documento**: unidade de registro de informações, qualquer que seja o suporte ou formato;

III - **informação sigilosa**: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

IV - **informação pessoal**: aquela relacionada à pessoa natural identificada ou identificável;

V - **tratamento da informação**: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

VI - **disponibilidade**: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

---

[5] BRASIL, 1990. Código de Defesa do Consumidor. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acessos em 03 dez. 2021.

> VII - **autenticidade**: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;
>
> VIII - **integridade**: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;[6]

Como visto, a LAI prevê conceitos envolvendo o que são informações sigilosas, informações pessoais e tratamento de informações. Você perceberá nos módulos a seguir que esses conceitos são muito similares aos adotados atualmente pela Lei Geral de Proteção de Dados. Também se pode observar a previsão de conceitos de segurança da informação, como disponibilidade, autenticidade e integridade de informações. Eles são o ponto central da proteção à privacidade, e a previsão desses conceitos em lei simboliza sua importância.

2012 – LEI 12.737 CAROLINA DIECKMANN

Essa Lei surge após um escândalo envolvendo a atriz Carolina Dieckmann, que teve fotos íntimas divulgadas na internet após o ataque de um invasor. A lei prevê punições no âmbito criminal para invasões de dispositivos através da violação de mecanismos de segurança, com o objetivo de acesso indevido aos dados do titular. A seguir temos um trecho da lei, que aborda justamente o tipo penal (conduta criminosa):

> Invasão de dispositivo informático
>
> Art. 154-A. **Invadir dispositivo informático alheio, conectado ou não à rede de computadores**, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.[7]

Assim, embora não disponha diretamente sobre proteção de dados de forma direta, é possível notar que a Lei expressa a preocupação do legislador com a privacidade dos titulares de dados pessoais.

---

[6] BRASIL, 2011. Lei de Acesso à Informação. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acessos em 03 dez. 2021.

[7] BRASIL, 2012. Lei N. 12.737 (Lei Carolina Dieckmann). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acessos em 03 dez. 2021.

2014 – LEI 12.965 – MARCO CIVIL DA INTERNET

O Marco Civil da Internet foi crucial para que se pudesse elevar a discussão sobre privacidade aos patamares atuais. A Lei dispõe sobre princípios, valores e objetivos envolvendo o uso da Internet no Brasil, além de reiterar o compromisso do Poder Público com a garantia à privacidade dos cidadãos. Dispõe também sobre um dos pilares da LGPD: o consentimento do titular.

> Art. 7º O acesso à internet é **essencial ao exercício da cidadania**, e ao usuário são assegurados os seguintes direitos:
>
> VII - **não fornecimento a terceiros de seus dados pessoais**, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
>
> VIII - **informações claras e completas** sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
>
> a) justifiquem sua coleta;
>
> b) não sejam vedadas pela legislação; e
>
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
>
> IX - **consentimento expresso** sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
>
> X - **exclusão definitiva dos dados pessoais** que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;
>
> Art. 8º A **garantia do direito à privacidade** e à **liberdade de expressão** nas comunicações é **condição** para o pleno exercício do direito de acesso à internet.[8]

Assim, embora não disponha de forma tão aprofundada sobre proteção de dados como feito pela LGPD, ainda assim o Marco Civil da Internet possui uma importância histórica sobre o tema, ao formalizar a necessidade de se garantir a privacidade do cidadão no meio digital, bem como de se resguardar seus direitos enquanto titular de dados pessoais.

[8] BRASIL, 2014. Lei N. 12.965 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acessos em 03 dez. 2021.

MÓDULO 02

DIREITO À PRIVACIDADE E PROTEÇÃO DE DADOS, BEM COMO SUA RESSIGNIFICAÇÃO NO MUNDO DIGITAL

AULA 08 – PRIVACIDADE E PROTEÇÃO DE DADOS COMO DIREITO GARANTIDO – PARTE 1

Como mencionado anteriormente, sob a influência internacional europeia do Regulamento Geral de Banco de Dados Pessoais (GDPR), foi promulgada, no Brasil, a Lei n. 13.709/18, conhecida como Lei Geral de Proteção de Dados (LGPD).

Com isso, os principais objetivos da Lei são estabelecer princípios, garantias, direitos e obrigações para a proteção de dados pessoais no Brasil, além de elencar os direitos do titular, determinar o regime jurídico do tratamento de dados pessoais e estabelecer regras para a tutela administrativa dos dados pessoais.

Como será demonstrado nos módulos seguintes, a lei é fundada em princípios, como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, entre outros. Quando esses princípios não são respeitados, representa uma afronta a alguns direitos fundamentais, principalmente da privacidade.

Conforme abordado anteriormente, a privacidade é tão importante para os seres humanos que ela é preservada inclusive na Constituição Federal do Brasil. Ainda mais na atualidade, considerando-se a globalização e o crescimento dos meios de comunicação e interação entre as pessoas ao redor do mundo, é de suma importância tratarmos esse princípio com respeito, já que sua inobservância pode ocasionar a violação de alguns direitos fundamentais, prejudicando o cidadão.

Antes mesmo da Constituição Federal, o direito à privacidade já havia nascido de forma simbólica, no ano de 1890, quando se publica, na Havard Law Review, o ensaio *The right to privacy*, de autoria de Samuel Warren e Louis Brandeis. Neste ensaio, são feitas diversas observações, considerando-se inclusive à privacidade enquanto direito absoluto.

Atualmente, no Brasil, este entendimento é flexibilizado, pois não há que se falar em hierarquia entre direitos fundamentais. Deve-se observar que o sujeito passivo do direito à privacidade são todas as pessoas naturais ou jurídicas, de direito público ou privado. Com isso, o que ocorre no direito à privacidade é que a vontade do titular ganha dimensão especial em relação a alguns direitos da personalidade. É um assunto relativamente filosófico, mas na prática é totalmente compreensível.

AULA 09 - PRIVACIDADE E PROTEÇÃO DE DADOS COMO DIREITO GARANTIDO – PARTE 2

Esta aula é uma continuação da aula: Privacidade e Proteção de Dados como Direito Garantido – Parte 1. Para melhor compreensão e fixação do conteúdo, recomendamos que seja revisitada a discussão da aula anterior.

Pense em você enquanto cidadão brasileiro que vive tranquilamente em sua casa. O que te torna confortável em seu lar? Não seria a liberdade e a privacidade para gozar de seus direitos da forma que bem entende, desde que não lese os direitos de outras pessoas? É justamente essa a noção que devemos ter de privacidade.

Assim, considerando a discussão apontada anteriormente, para que compreendamos a importância que o legislador buscou dar à privacidade e proteção de dados, precisamos antes compreender o que é um direito fundamental. Muitos pensadores se debruçaram sobre o tema, mas podemos ilustrar o conceito através do pensamento de Ferrajoli:

> [...] são 'direitos fundamentais' todos aqueles direitos subjetivos que correspondem universalmente a "todos" os seres humanos enquanto dotados do status de pessoas, cidadãos ou pessoas com capacidade de agir; entendido por 'direito subjetivo' qualquer expectativa positiva (de prestações) ou negativa (de não sofrer lesões) ligada a um indivíduo por uma norma jurídica; e por 'status' a condição de um sujeito, prevista também por uma norma jurídica positiva, como pressuposto de sua idoneidade para ser titular de situações jurídicas e/ou autor dos atos que são exercício destas (2004, p. 37).[9]

Assim, para possuir direito à privacidade, basta que o indivíduo seja um sujeito de direitos. Isso significa que qualquer pessoa faz jus ao rol direitos fundamentais elencados na Constituição da República, incluindo-se a inviolabilidade da intimidade, da vida privada, da honra e imagem.

Além disso, com a compreensão de que a Lei Geral de Proteção de Dados tem um apreço enorme sobre o direito à privacidade, devemos relembrar que a lei preserva também a autodeterminação informativa; a liberdade de expressão, de informação, comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, livre concorrência e defesa do consumidor e aos direitos humanos de liberdade e dignidade das pessoas.

---

[9] FERRAJOLI, Luigi. **Derechos y garantias**: la ley del más débil. Tradução para o espanhol: Perfecto Andrés Ibánez e Andrea Greppi. Madri: Editorial Trotta, 2004. p.37, tradução nossa para o português.

Esses valores incutem no cenário jurídico, resultando na impossibilidade de se violar o direito à privacidade – nele inclusa a privacidade no âmbito digital. A flexibilização do direito à privacidade, no entanto, é permitida, devendo ocorrer apenas em casos excepcionais. Sobre isso, a Lei Geral de Proteção de Dados é taxativa em seu rol de hipóteses de tratamento.

A título exemplificativo, podemos indicar a necessidade de se manter históricos criminais de alguns indivíduos. É evidente que o titular, caso pudesse, não gostaria de ser investigado pelas autoridades. Neste caso, não faria sentido atribuir-lhe a possibilidade de refutar o processamento de seus dados, pois é dever do Poder Público manter informações sobre criminosos ou investigados em sua base. Sem essa medida, estaria sendo violado o dever da Segurança Pública de promover segurança aos cidadãos.

É evidente que a proteção de dados caminha cada vez mais para se consolidar enquanto direito fundamental, tendo sido recentemente aprovada pelo Senado a PEC 17, que dispõe sobre a matéria. No entanto, a interpretação deverá ser sempre sopesada com base na razoabilidade das circunstâncias fáticas e com proporcionalidade aos demais direitos envolvidos nas atividades de tratamento, uma vez que não há que se falar em direito absoluto em nosso sistema jurídico.

AULA 10 – PRIVACIDADE NA NOVA ECONOMIA – PARTE 1

Após demonstrar a relação entre o direito à privacidade e a Lei Geral de Proteção de Dados, é fundamental tecermos alguns comentários sobre a privacidade no mundo atual, principalmente com relação à Nova Economia.

Mas o que é a nova Economia e o que a privacidade tem a ver com isso?

Termo que surgiu em 1980, a Nova Economia é responsável por uma série de transições pelas quais todo o mercado e as empresas estão passando atualmente, como as novas indústrias de base tecnológica com altas taxas de crescimento. Para entendermos a importância da privacidade nesse "novo" cenário, é preciso saber como, onde, por quem e para que esses dados são usados, conforme será explicado.

Por exemplo, quando disponibilizamos – mesmo que indiretamente – nossos dados a serviços de *streaming* ao avaliarmos o filme que acabamos de assistir, quando fazemos um *check-in* no bar que acontece o *happy-hour* da empresa ou até quando fazemos pedidos nos aplicativos de delivery, de alguma forma essas informações se transformam em dados para as empresas de serviços, sendo também são coletados pelos fabricantes de *hardware* ou *software* dos dispositivos. Esses dados são processados, criando inteligência para as empresas e consequentemente gerando lucro.

Assim, através da transformação digital, as empresas têm acesso a quantidades maciças de dados (*big data*), aprofundando seu conhecimento sobre o consumidor para

identificar suas necessidades e desejos. Com isso, uma das maiores mudanças foi a priorização dos funcionários dentro das organizações e a forma que os consumidores são valorizados fora dos muros, solidificando áreas como a experiência do usuário (UX).

Contudo, quando os dados estão atrelados a um sujeito titular de direitos, eles representam uma parcela de sua individualidade, passando, portanto, a compor a sua própria privacidade, e, por conseguinte, um atributo dos direitos da personalidade.[10]

Nesta mesma perspectiva, a informação como um bem econômico decorre não só do valor social da informação analisada sob o ponto vista comportamental do consumo, mas também da própria transformação das pessoas (consumidores) em mercadorias, visto que a prática de comercialização de dados dos consumidores é uma realidade.

Certamente você sabe o que é o *Facebook*, mas talvez não tenha conhecimento do que é a *Cambridge Analytica*. Foi uma empresa privada que combinava mineração e análise de dados com comunicação estratégica para o processo eleitoral dos Estados Unidos. A relação entre ambos envolveu a coleta de informações pessoalmente identificáveis de até 87 milhões de usuários do Facebook.

Isso demonstra como os dados ficam vulneráveis na internet e que a privacidade pode ser violada por aqueles que não possuem boas intenções. Além disso, é possível notar que a sofisticação das formas de exploração de dados do titular evolui à medida que novas tecnologias surgem.

AULA 11 – PRIVACIDADE NA NOVA ECONOMIA – PARTE 2

Esta aula é uma continuação da aula: Privacidade na Nova Economia – Parte 1. Para melhor compreensão e fixação do conteúdo, recomendamos que seja revisitada a discussão da aula anterior.

Com o aumento exponencial do consumo de serviços digitais, formou-se um grupo de "Gigantes da Tecnologia", composto pelo grupo Gafa (Google, Amazon, Facebook e Apple), que dominam o setor e determinam as regras do jogo em termos de tratamento de dados pessoais. Esse privilégio sobre o mercado de tecnologia proporcionou um cenário de mitigação da privacidade de titulares, onde milhões de pessoas tinham pouca ou nenhuma possibilidade de gerenciamento sobre seus dados.

Você provavelmente utilizou alguma rede social nos últimos meses. Neste caso, reflita: qual a possibilidade de a entidade controladora desses dados ser alguma das empresas do grupo Gafa? Seguramente, as chances de nenhuma das empresas terem coletado seus dados pessoais em algum momento é praticamente nula.

---

[10] CATALA, Pierre, "Ebauche d´une théorie juridique de l´information", p. 20, apud DONEDA, Danilo. Da privacidade à proteção dos dados pessoais. Rio de Janeiro: Saraiva, 2006. p. 157.

Recentemente, no entanto, a Comissão Europeia anunciou dois instrumentos jurídicos para um maior controle dessas empresas: a Lei de Serviços Digitais e o Ato dos Mercados Digitais. Essas normas estimulam a livre concorrência com empresas de menor porte, tornando as *Big Techs* obrigadas a compartilhar os dados coletados, além elaborar relatórios detalhando o funcionamento de suas plataformas aos órgãos reguladores.

A batalha travada entre agências reguladoras, órgãos jurisdicionais e empresas de tecnologia está longe de ter seu fim declarado, mas é necessário perceber que não há muitas alternativas às empresas além de fazer cumprir os direitos dos titulares de dados. Isso ficará evidente ao longo dos próximos módulos, sobretudo quando discutirmos o fenômeno da judicialização da proteção à privacidade e apresentarmos alguns *cases* práticos sobre o tema.

Vimos que a discussão sobre o direito à privacidade e proteção de dados é totalmente necessária para o novo modelo de sociedade que estamos construindo, pois afeta diretamente o que temos de mais valioso hoje em dia, que são nossos dados. Conforme Costa Júnior, "a tecnologia provoca um aumento desenfreado nas possibilidades e na velocidade do acesso à informação, levando, consequentemente, a uma maior fragilidade da esfera privada, da intimidade das pessoas". A economia, parte deste processo, deverá se adaptar aos novos desafios impostos pela aceleração do desenvolvimento tecnológico.

MÓDULO 03

OS PRINCÍPIOS, FUNDAMENTOS E CONCEITOS DA LGPD

AULA 12 – OS FUNDAMENTOS DA LGPD – PARTE 1

Agora que você tem um conhecimento maior sobre a história da privacidade e, consequentemente, possui um olhar mais cuidadoso com relação à proteção de dados no mundo e no Brasil, chegou a hora de aprofundar os seus conhecimentos sobre a própria Lei Geral de Proteção de Dados.

A lei brasileira, logo em seu início, ensina que o seu objetivo é abordar da questão do tratamento (qualquer operação com dados pessoais, como por exemplo a coleta) de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Como a própria lei diz, o cuidado e o respaldo legal com relação aos dados pessoais deverão ocorrer em qualquer âmbito e não só no digital, sendo que até mesmo uma folha de papel com dados pessoais em cima de uma mesa de escritório também é abarcada pela LGPD. Feita esta introdução, vamos juntos aos fundamentos e princípios da Lei Geral de Proteção de Dados.

Ao tratarmos sobre a Lei Geral de Proteção de Dados, temos que entender como o tema é abordado e, principalmente, acerca do direito à privacidade e proteção de dados, compreendendo a sua importância no mundo atual. Para tanto, precisamos compreender antes quais são os fundamentos da LGPD, pois são eles que embasam toda a compreensão da Lei:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I - o respeito à **privacidade**;
>
> II - a **autodeterminação** informativa;
>
> III - a **liberdade de expressão**, de **informação**, de comunicação e de opinião;
>
> IV - a **inviolabilidade da intimidade, da honra e da imagem**;
>
> V - o **desenvolvimento** econômico e tecnológico e a inovação;
>
> VI - a livre iniciativa, a livre concorrência e a **defesa do consumidor**; e
>
> VII - os **direitos humanos**, o livre desenvolvimento da personalidade, a **dignidade** e o exercício da cidadania pelas pessoas naturais.

Conforme observado anteriormente, alguns dos valores acima elencados podem ser encontrados na Constituição Federal, no Código de Defesa do Consumidor, na Lei de Acesso à Informação, na Lei Carolina Dieckmann e no Marco Civil da Internet. A LGPD é, portanto, fruto de um processo histórico de busca pela proteção à privacidade dos cidadãos, sendo esses fundamentos a base para a interpretação de todos os artigos subsequentes da LGPD.

De forma geral, a Lei Geral de Proteção de Dados busca estabelecer em seu artigo 2º que os indivíduos são livres para se manifestarem, obterem informações e empreenderem digitalmente, desde que observados alguns valores, como por exemplo o respeito à privacidade e dignidade dos indivíduos e os direitos do consumidor. A seguir, iremos detalhar cada fundamento, para que todos possam ser compreendidos em sua integralidade.

AULA 13 - FUNDAMENTOS DA LGPD – PARTE 2

Esta aula é uma continuação da aula: Os Fundamentos da LGPD – Parte 1. Para melhor compreensão e fixação do conteúdo, recomendamos que seja revisitada a discussão da aula anterior.

Prosseguindo em nosso estudo, abordaremos os fundamentos previstos na Lei Geral de Proteção de Dados individualmente. Esse processo é necessário, pois com uma adequada compreensão dos fundamentos se viabiliza a interpretação de todos os demais dispositivos da Lei. São eles que constituem o alicerce de qualquer diploma legal, sendo imprescindível que analisemos cada fundamento para o máximo aproveitamento deste Curso:

Respeito à Privacidade: O primeiro fundamento é o *respeito à privacidade*. Através dos módulos anteriores, você é capaz de entender que um dos principais objetivos da proteção de dados é proteger a privacidade dos titulares. Esse fundamento assegura os direitos fundamentais de inviolabilidade da intimidade, da honra, da imagem e da vida privada, constantes na Constituição Federal, no seu artigo 5º, inciso X. Esse fundamento também consta no Marco Civil da Internet;

Autodeterminação Informativa: O nome pode parecer estranho e causar pequenas confusões, como já ocorrera inclusive com membros do Poder Legislativo. No entanto, a chamada *Autodeterminação Informativa* nada mais significa que *o poder de decisão no tratamento de Dados Pessoais está nas mãos de seu titular*, isto é, o titular é quem possui o direito de escolha sobre quais de seus dados serão tratados e, possivelmente, no futuro, a eliminação destes.

Como ainda será explicado nesse curso, nem sempre o titular poderá escolher quais dados serão tratados, como em caso de a empresa necessitar dos dados do empregado para cumprir com alguma normativa da Receita Federal. Nesse caso, o titular, mesmo não querendo fornecer eventual dado, será obrigado em razão de determinação legal ou regulatória;

Liberdade de Expressão, de Informação, de Comunicação e de Opinião: Este princípio reitera o exposto na Constituição Federal, que trata dos direitos e garantias fundamentais, mais especificamente em seu artigo 5º, inciso IX: "*é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença (...)*".

Muito se questiona sobre a relação desse fundamento com a proteção de dados, uma vez que as pessoas não conseguem criar a correlação entre eles. Porém, tente imaginar o seguinte caso:

Um titular de dados, após expressar sua opinião nas redes sociais sobre algum assunto polêmico, começa a receber ameaças de outros usuários. Agora, imagine que, por um descuido, a rede social exponha todas as informações que possui sobre esse titular de dados que recebeu as ameaças, como por exemplo seu telefone de contato ou endereço.

Já pensou como poderia ser perigoso ao usuário que proferiu sua opinião nas redes sociais? Seu direito fundamental de se expressar poderia ser suprimido, uma vez que os ameaçadores poderiam coagi-lo por saberem alguns de seus dados pessoais;

Inviolabilidade da Intimidade, da Honra e da Imagem: Assim como o anterior, este fundamento reitera uma garantia constitucional, também garantida pelo artigo 5º, inciso X: "*são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação*".

A título de exemplo, podemos mencionar a troca de mensagens pelas redes sociais ou pelos aplicativos de mensagens instantâneas. Caso essas empresas não observem corretamente os procedimentos de segurança da informação e demais controles, podem propiciar o vazamento de dados ou até mesmo invasões por falhas de segurança, violando a intimidade dos usuários que não têm qualquer interesse de tornar seus dados públicos;

Desenvolvimento Econômico e Tecnológico e a Inovação: Aqui se põe refletida a novíssima situação em que o ordenamento jurídico brasileiro está se inserindo no contexto da privacidade e da proteção de Dados Pessoais.

Leis brasileiras que versam sobre a o chamado "corpo digital" de seus cidadãos são extremamente recentes na história do país, sendo elas: i) **Lei nº 13.709, de 14 de agosto de 2018**, Lei Geral de Proteção de Dados Pessoais ("LGPD"); ii) **Lei nº 12.965, de 23 de abril de 2014**, Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil; e iii) **Decreto 8.771, de 11 de maio de 2016**, Decreto regulamentador do Marco Civil da Internet, que trata das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indica procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, além de apontar medidas de transparência na requisição de dados cadastrais e estabelecer parâmetros para fiscalização e apuração de infrações contidas no Marco Civil da Internet.

Ou seja, entende-se que, pautas do tipo só entraram em cena há, no máximo, 7 (sete) anos. A LGPD, assim, passa a ocupar um importante papel na criação de um cenário de segurança jurídica em todo o país sobre o tema;

Livre Iniciativa, a Livre Concorrência e a Defesa do Consumidor: Por ser uma Lei geral, a LGPD se aplica a todos os setores da sociedade, indistintamente. Seja público ou privado, de pequeno, médio ou grande porte, todas as pessoas jurídicas (ou físicas) que tratam Dados Pessoais por algum motivo, devem ter ciência dos principais dispositivos e, para tanto, devem estar devidamente adequadas à Lei.

Quando se fala em livre iniciativa, livre concorrência e a defesa do consumidor, a ideia que a lei traz, mais uma vez, é a de que a proteção de dados pessoais leva, consequentemente, à segurança desses fundamentos.

Especificamente com relação à defesa do consumidor, é fácil visualizar a intenção da LGPD. Isto, pois o consumidor sempre é a parte hipossuficiente (mais fraca) na relação negocial com a empresa. Assim, caso a empresa faça o uso abusivo dos dados do consumidor, este poderá ficar desamparado em razão de sua hipossuficiência, como em casos em que a empresa solicitada dados que não tem qualquer relação para que o consumidor possa realizar uma compra.

Desta forma, a LGPD, bem como o Código de Defesa do Consumidor, preza pela defesa dos direitos dos consumidores.

OS DIREITOS HUMANOS, O LIVRE DESENVOLVIMENTO DA PERSONALIDADE, A DIGNIDADE E O EXERCÍCIO DA CIDADANIA PELAS PESSOAS NATURAIS:

O sétimo e último fundamento reúne diversos conceitos distintos, mas que se complementam.

No início do curso, foi demonstrado que a preocupação com a privacidade e, consequentemente, com a proteção dos dados pessoais surgiu há anos, como na Declaração Universal dos Direitos Humanos, da ONU (criada após o fim da 2ª Guerra Mundial) e na própria Constituição Federal de 1988 (promulgada após o fim do período militar brasileiro - de 1964 a 1985). Assim, este fundamento nada mais é do que a preocupação com a preservação dos direitos fundamentais, mais uma vez presentes na LGPD.

Por sua vez, quando se fala em *Livre Desenvolvimento da Personalidade*, a lei se refere, sobretudo, aos chamados direitos intrínsecos ao homem. Cada indivíduo tem o direito de tomar as próprias decisões e se desenvolver, em sua própria intimidade, como bem entender. Assim, a proteção aos dados pessoais permite que as pessoas possam continuar se desenvolvendo como pretendem, tomando suas próprias decisões e respeitando sua individualidade. Eventualmente violada, por exemplo, a privacidade de um titular de dados, o seu direito de livre desenvolvimento da personalidade também estará violado. A Dignidade dispensa comentários, uma vez que, por si só, já exprime todo o seu conceito.

E, por fim, quando tratamos do *Exercício da Cidadania*, falamos do pertencimento de cada titular à uma vida em sociedade e, portanto, tem direito ao exercício de seus direitos (é, inclusive, um fundamento da Constituição Federal - Art 1º).

Ressalta-se que este fundamento não é divergente do Livre Desenvolvimento da Personalidade, mas, sim, uma complementação. Mesmo cada pessoa possuindo sua individualidade, esta pessoa faz parte de um grupo e tem todo o direito de exercer a sua cidadania.

AULA 14 – OS PRINCÍPIOS DA LGPD – PARTE 1

Agora que você já tem o conhecimento sobre os fundamentos da Lei Geral de Proteção de Dados, é imprescindível que sejam tratados os *princípios* da lei, estes necessários para a aplicação completa da lei e que, além disso, orientam todo e qualquer tratamento de dados pessoais que há de ser realizado.

A LGPD prevê 10 princípios norteadores para a realização de tratamento de dados pessoais e, conforme já mencionado neste curso, como a LGPD possui grande influência do Regulamento Geral de Proteção de Dados da União Europeia, 6 desses 10 princípios também constam na legislação europeia.

Considerando a importância desses princípios, iniciaremos a explicação por eles, de forma prática, quais sejam:

a) Transparência (artigo 6º, inciso VI, LGPD) e o respectivo dever de informação;

b) Finalidade (artigo 6º, inciso I, LGPD);

c) Necessidade (em outras palavras, minimização e proporcionalidade – artigo 6º, inciso III, LGPD);

d) Adequação (artigo 6º, inciso II, LGPD);

e) Segurança e Prevenção (artigo 6º, incisos VII e VIII, LGPD).

Observando-se os princípios acima mencionados, é possível concluir *que todo tratamento de dados pessoais deve ser informado ao titular*, de forma transparente, principalmente com a utilização de uma linguagem clara. Além disso, é necessário constar, pelo menos, quais são os dados tratados, como será realizado esse tratamento e para qual finalidade.

Para evitar qualquer problema, a finalidade da utilização dos dados deve ser apresentada ao titular de forma evidenciada, principalmente para comprovação às autoridades competentes (caso seja necessário), ao mercado e aos próprios titulares, sempre com o objetivo de cumprir com o princípio da transparência constante na lei.

Ressalta-se que é de extrema importância também observar a minimização e proporcionalidade no tratamento de dados pessoais. De acordo com o princípio da necessidade, apenas os dados pessoais estritamente necessários para o cumprimento das finalidades legitimadas junto ao titular é que poderão ser tratados de modo legal.

Nesta linha, é importante verificar se a quantidade de dados de modo geral e os tipos de dados pessoais estão em conformidade com esse uso, não podendo, por exemplo, exigir a coleta e uso de dados de filiação sindical para a compra de um produto em uma loja, tendo em vista que a coleta da filiação sindical nada tem a ver com o objetivo da compra do produto.

Juntamente do princípio da necessidade está o princípio da adequação, este que tem o objetivo de exigir a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Além do mencionado princípio, a necessidade também está atrelada ao princípio da limitação de armazenamento dos dados pessoais, correspondente ao tempo (período) em que os dados ficarão armazenados. Ou seja, os dados pessoais somente poderão ser armazenados após a sua utilização, enquanto forem necessários para o cumprimento de obrigação legal ou regulatória e/ou uso exclusivo do controlador, vedado seu acesso por terceiro e desde que anonimizados.

Com o advento da LGPD, as empresas não possuem mais a liberalidade de guardar os dados pessoais como bem entendem, devendo observar todos os princípios mencionados. Assim, toda empresa precisa estabelecer prazos para o armazenamento de cada categoria de dado pessoal que trata, difundir essa cultura entre os colaboradores e fiscalizar seu efetivo cumprimento, nos termos do artigo 16 da LGPD.

Os princípios da segurança e da prevenção estão atrelados a todas as atividades com dados pessoais realizadas pelas empresas. Assim, atualmente, as empresas necessitam utilizar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas que possam destruir os dados ou, até mesmo, violar os direitos do titular.

Para que isso seja realizado, há de ser observado o princípio da **prevenção**, este que é basicamente definido como a prevenção de ocorrência de danos em virtude do tratamento de dados pessoais, consistente na tomada de ações preventivas, como os projetos de adequação à LGPD e suas devidas manutenções, para evitar qualquer dano ao titular.

Na próxima aula, prosseguiremos com a análise dos princípios do livre acesso, qualidade, não discriminação e da responsabilização e prestação de contas.

AULA 15 – OS PRINCÍPIOS DA LGPD – PARTE 2

Esta aula é uma continuação da aula: Os Princípios da LGPD - Parte 1. Para melhor compreensão e fixação do conteúdo, recomendamos que seja revisitada a discussão da aula anterior.

Vamos prosseguir com a análise dos outros 4 princípios previstos na Lei Geral de Proteção de Dados, quais sejam:

f) Livre acesso (artigo 6°, inciso IV, LGPD);

g) Qualidade (artigo 6°, inciso V, LGPD);

h) Não discriminação (artigo 6°, inciso IX, LGPD); e

i) Responsabilização e prestação de contas (artigo 6°, inciso X, LGPD).

Estes princípios não estão presentes no Regulamento Europeu, mas não significa que não sejam tão importantes quanto os seis primeiros princípios trazidos na primeira aula deste módulo.

Quando se fala em **livro acesso**, significa a garantia que é dada aos titulares referente à consulta facilitada e gratuita sobre a forma e duração do tratamento, bem como sobre a integridade de seus dados pessoais. Lembre-se que todos os princípios estão conectados e, o princípio do **livre acesso** anda lado a lado com o princípio da **transparência**, tendo em vista que as empresas necessitam demonstrar como são realizados os tratamentos de dados de forma transparente, garantindo o livre acesso aos titulares dos dados pessoais.

Também pode-se dizer que o princípio da **qualidade**, consistente na garantia aos titulares sobre a exatidão, clareza, relevância e atualização de seus dados, é totalmente vinculado a outros princípios, como os princípios da **transparência**, **necessidade** e **finalidade**.

Diz-se isso, porque, os dados devem estar corretos e de acordo com a necessidade e para o cumprimento da finalidade do tratamento a ser realizado, ressaltando-se que a exatidão dos dados só é possível ser comprovada através da transparência para com o titular.

O penúltimo princípio é o princípio da **não discriminação,** que consiste na impossibilidade de realização do tratamento do dado pessoal para fins

discriminatórios, ilícitos ou abusivos. Um bom exemplo com a possibilidade de cometimento de discriminação é a seguinte:

Considere-se como usuário de um aplicativo para controlar suas atividades físicas. Não só o registro das atividades físicas, mas este aplicativo também realiza o controle de seus batimentos cardíacos, alimentação e possíveis doenças relacionadas à essas atividades. Na hipótese desse aplicativo fornecer os dados para empresas de seguros que os utilizam para calcular os riscos, e verificando o possível problema de saúde e maior chances de utilização dos serviços hospitalares, acabam aumentando o valor do seguro saúde, violando completamente o princípio da não discriminação.

No exemplo mencionado, não só o princípio da não discriminação estaria sendo violado, mas também os princípios da transparência, adequação e finalidade.

Por fim, tem-se o princípio da **responsabilização e prestação de contas,** que implica na obrigação de demonstração, pelo agente de tratamento de dados pessoais, da *adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais* e, inclusive, da eficácia dessas medidas.

Ou seja, este princípio está totalmente relacionado à necessidade de as empresas realizarem as adequações à Lei Geral de Proteção de Dados, com a devida implementação de programas de governança direcionados à proteção de dados; medidas técnicas para tornar seguros os sistemas internos e demais outras providências realizadas nos programas de adequação à legislação de proteção de dados.

AULA DE REVISÃO 01

Revisaremos o conteúdo visto dos módulos 01, 02 e 03.

AULA 16 – REVISÃO MÓDULO 01 - GOVERNANÇA, COMPLIANCE E HISTÓRICO DA LGPD

REVISÃO AULA 02 - O QUE É A LEI GERAL DE PROTEÇÃO DE DADOS?

- A LGPD surgiu com o objetivo de estabelecer regras específicas para o tratamento de dados pessoais, criar responsabilidades às empresas, além de estabelecer diversas diretrizes a serem seguidas;
- A LGPD possui bastante influência do Regulamento da União Europeia (GDPR);

- Com dez capítulos e 65 artigos, a LGPD é a norma brasileira mais específica sobre privacidade e proteção de dados.

REVISÃO AULA 03 – QUAL A RELAÇÃO ENTRE LGPD E GOVERNANÇA?

- Segundo o Instituto Brasileiro de Governança Corporativa (IBGC), governança corporativa é: "(...) o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas.";
- Há 4 (quatro) princípios da governança corporativa que se relacionam a LGPD, sendo: Transparência, Equidade, Prestação de contas (accountability), Responsabilidade corporativa;
- Todos os projetos de LGPD devem ser realizados em observância à preceitos da Governança Corporativa.

REVISÃO AULA 04 – QUAL A RELAÇÃO ENTRE LGPD E COMPLIANCE?

- O termo compliance tem origem no verbo inglês *to comply*, que significa agir de acordo com uma regra, uma instrução interna, um comando ou um pedido;
- Um processo de adequação a LGPD tem como objetivo a implementação permanente de um programa de governança em privacidade, com foco na adequação de controles e na transformação da cultura organizacional;

REVISÃO AULA 05 - O QUE É PRIVACIDADE E POR QUE DEVEMOS PROTEGÊ-LA?

- A palavra "privado" é uma derivação do vocábulo latino "privatus", que significa algo "retirado da vida pública";
- A promoção de privacidade é buscar evitar que algo seja de conhecimento ou acesso público, reservando essa permissão apenas àqueles que consideramos aptos a obtê-la;
- Proteger a privacidade do indivíduo significa proteger sua segurança;

REVISÃO AULA 06 - COMO SÃO TRATADAS AS LEIS DE PRIVACIDADE NO MUNDO

- O art. 12 da Declaração Universal de Direitos Humanos de 1948 preocupou-se com a proteção de dados pessoais;

- A Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, nos termos do seu art. 8°, também se preocupou com privacidade;
- Há previsão sobre a proteção à privacidade no Pacto San Jose da Costa Rica, precisamente em seu art. 11;
- A OCDE elaborou as Diretrizes sobre a Proteção de Privacidade e Circulação Transfronteiriça de Dados (*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data);*
- Em 25 de maio de 2018 entrou em vigor a GDPR, possuindo 99 artigos. Sua competência de aplicação não é limitada ao território da União Europeia;
- Os Estados Unidos da América possuem 7 (sete) leis federais sobre o tema privacidade. Sendo o COPPA (*Children's Online Privacy Protection Act*).
- No âmbito estadual há algumas leis relevantes, a CCPA (California Consumer Privacy Act) e a NY SHIELD (New York Stop Hacks and Improve Eletronic Data Security Act).

REVISÃO AULA 07 - LINHA DO TEMPO DA PROTEÇÃO DE DADOS NO BRASIL

- A Constituição da República prevê a dignidade da pessoa humana no seu art. 1°, inc. III, além do art. 5°, inc. X e XII que dispõem sobre a inviolabilidade a intimidade, a vida privada;
- O Código de Defesa do Consumidor em seu art. 43, prevê direitos dos Titulares de Dados Pessoais;
- A Lei de Acesso à Informação (Lei n° 12.527), em seu art. 4°, dispõe sobre algumas prerrogativas do cidadão, tratando-se o acesso à informação como direito fundamental;
- A Lei n° 12.737 (Lei Carolina Dieckman), prevê punições no âmbito criminal para invasões de dispositivos através da violação de mecanismos de segurança, com o objetivo de acesso indevido aos dados do titular;
- A lei n° 12.965 (Marco Civil da Internet), dispõe sobre princípios, valores e objetivos envolvendo o uso da Internet no Brasil, além de reiterar o compromisso do Poder Público com a garantia à privacidade dos cidadãos;
- Por fim, promulgada a lei n° 13.709 (lei Geral de Proteção de Dados Pessoais (LGPD).
-

AULA 17 - REVISÃO MÓDULO 02 – DIREITO À PRIVACIDADE E PROTEÇÃO DE DADOS, BEM COMO SUA RESSIGNIFICAÇÃO NO MUNDO DIGITAL

REVISÃO AULA 08 - PRIVACIDADE E PROTEÇÃO DE DADOS COMO DIREITO GARANTIDO – PARTE 1

- O conceito de privacidade nasceu de forma simbólica, no ano de 1890, quando se publicada a pesquisa denominada *The right to privacy*, de autoria de Samuel Warren e Louis Brandeis, na Havard Law Review;
- A LGPD estabelece princípios, garantias, direitos e obrigações para a proteção de dados pessoais no Brasil, além de elencar os direitos do titular, determinar o regime jurídico do tratamento de dados pessoais e estabelecer regras para a tutela administrativa dos dados pessoais;
- Não há hierarquia entre direitos fundamentais.

REVISÃO AULA 09 - PRIVACIDADE E PROTEÇÃO DE DADOS COMO DIREITO GARANTIDO – PARTE 2

- Para possuir direito à privacidade, basta que o indivíduo seja um sujeito de direitos;
- Qualquer pessoa faz jus ao rol direitos fundamentais elencados na Constituição da República, incluindo-se a inviolabilidade da intimidade, da vida privada, da honra e imagem;
- A LGPD preza pela autodeterminação informativa, a liberdade de expressão, de informação, comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem;

REVISÃO AULA 10 - PRIVACIDADE NA NOVA ECONOMIA PARTE 1

- Nova Economia é uma expressão criada na década de 1980, para descrever a substituição da lógica de fabricação manufatureira por outra, que é o fornecimento de produtos e serviços associados ao desenvolvimento de tecnologia proprietária, formado por empresas com modelos de negócio digitais;
- Através da transformação digital, as empresas têm acesso a quantidades maciças de dados (*big data*), aprofundando seu conhecimento sobre o consumidor para identificar suas necessidades e desejos;
- Exemplos práticos: Relação do Facebook com a Cambridge Analytica.

REVISÃO AULA 11 - PRIVACIDADE NA NOVA ECONOMIA PARTE 2

- GAFA = Google, Amazon, Facebook e Apple. São gigantes da tecnologia que ditam as regras do jogo em termos de tratamento de dados;

- Comissão Europeia estabeleceu dois instrumentos jurídicos para um maior controle dessas empresas: a Lei de Serviços Digitais e o Ato dos Mercados Digitais;
- Os instrumentos estimulam a livre concorrência com empresas de menor porte, tornando as *Big Techs* obrigadas a compartilhar os dados coletados, além elaborar relatórios detalhando o funcionamento de suas plataformas aos órgãos reguladores;
- A tecnologia provoca um aumento desenfreado nas possibilidades e na velocidade do acesso à informação, levando, consequentemente, a uma maior fragilidade da esfera privada, da intimidade das pessoas.

AULA 18 - REVISÃO MÓDULO 03 - OS PRINCÍPIOS, FUNDAMENTOS E CONCEITOS DA LGPD

REVISÃO AULA 12 - OS FUNDAMENTOS DA LGPD – PARTE 1

- A LGPD estabeleceu um total de sete fundamentos, sendo:
  - O respeito à privacidade;
  - A autodeterminação informativa;
  - A liberdade de expressão, de informação, de comunicação e de opinião;
  - A inviolabilidade da intimidade, da honra e da imagem;
  - O desenvolvimento econômico e tecnológico e a inovação;
  - A livre iniciativa, a livre concorrência e a defesa do consumidor;
  - Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

REVISÃO AULA 13 - OS FUNDAMENTOS DA LGPD – PARTE 2

- Respeito à Privacidade: assegura os direitos fundamentais de inviolabilidade da intimidade, da honra, da imagem e da vida privada, constantes na Constituição Federal;
- Autodeterminação Informativa: significa que o poder de decisão no tratamento de Dados Pessoais está nas mãos de seu titular;
- Liberdade de Expressão, de Informação, de Comunicação e de Opinião: artigo 5º, inciso IX, da Constituição federal: "é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença (...)";
- Inviolabilidade da Intimidade, da Honra e da Imagem: artigo 5º, inciso X, da Constituição Federal: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

- Desenvolvimento econômico e tecnológico e a inovação: leis brasileiras que versam sobre o chamado "corpo digital" de seus cidadãos são extremamente recentes à história do país, sendo elas: LGPD, Marco Civil da Internet, e Decreto regulamentador do Marco Civil da Internet;
- Livre Iniciativa, a Livre Concorrência e a Defesa do Consumidor: a ideia de que a lei nos traz é que a proteção do dado pessoal leva à segurança desses fundamentos;
- Livre Iniciativa, a Livre Concorrência e a Defesa do Consumidor: caso a empresa faça o uso abusivo dos dados do consumidor, por este ser hipossuficiente, este poderá ficar desamparado;
- Os Direitos Humanos, o Livre Desenvolvimento da Personalidade, a Dignidade e o Exercício da Cidadania pelas Pessoas Naturais: O livre desenvolvimento da personalidade, refere-se, sobretudo, à tomada pelos chamados direitos intrínsecos ao homem;

REVISÃO AULA 14 - OS PRINCÍPIOS DA LGPD – PARTE 1

- Transparência: Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- Finalidade: Realização do tratamento de dados para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
- 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;
- Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

REVISÃO AULA 15 - OS PRINCÍPIOS DA LGPD – PARTE 2

- Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- Qualidade de Dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

- Não Discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- Prestação de Contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

MÓDULO 04

INTRODUÇÃO À APLICAÇÃO PRÁTICA DA LEI GERAL DE PROTEÇÃO DE DADOS, COM EXPOSIÇÃO DAS BASES LEGAIS QUE JUSTIFICAM O TRATAMENTO DE DADOS PESSOAIS DENTRO DE UMA INSTITUIÇÃO

AULA 19 – APLICAÇÃO TERRITORIAL DA LEI GERAL DE PROTEÇÃO DE DADOS E SUAS BASES LEGAIS

Após os ensinamentos do módulo anterior relacionados aos fundamentos e princípios da Lei Geral de Proteção de Dados, chegou a hora de tratar da **aplicação** da LGPD (onde, como e quando é aplicada) e das chamadas **bases legais** que, conforme será demonstrado, são as hipóteses que a lei autoriza a realização do tratamento de dados.

Neste módulo será possível aprender, inclusive, que a LGPD não é aplicada apenas no território brasileiro, além de aprender que o consentimento não é regra para a realização do tratamento de dados pessoais, dados sensíveis ou de crianças e adolescentes.

Introduzido o assunto, vamos iniciar com os ensinamentos sobre a aplicação da lei.

Como é aplicada a Lei Geral de Proteção de Dados? A LGPD é aplicada sempre que o tratamento de dados for *realizado no território brasileiro* ou se *a atividade envolver oferecimento de produtos ou serviços de pessoas que se encontram em território nacional.*

Quando o assunto é territorialidade, diz-se que a LGPD adotou a regra chamada de *público-alvo*, consoante é possível observar em seu art. 3°. Ressalta-se que não só a LGPD adota esta regra, como também o GDPR e o Marco Civil da Internet.

A regra do público-alvo significa que a coleta de dados em território nacional ou a oferta dos serviços aos cidadãos brasileiros ou pessoas que estejam em território nacional, ensejando a aplicação da lei brasileira, mesmo que seja realizado por empresa sediada no estrangeiro ou seja seu tratamento realizado no exterior.

Uma diferença da LGPD com as mencionadas leis é que a LGPD não é aplicada apenas aos cidadãos brasileiros, mas é aplicada à toda e qualquer pessoa que esteja no Brasil, desde que seja relacionada a algum tratamento de dados pessoais.

APLICAÇÃO EXTRATERRITORIAL

Conforme mencionado acima, a LGPD adotou a regra chamada de *público-alvo* para aplicação de sua lei e que, muitas vezes, a sua aplicação não dependerá da presencialidade no território brasileiro.

É importante reforçar que os efeitos da LGPD não se restringem aos limites territoriais do Brasil e, assim como a *General Data Protection Regulation* (GDPR), **pode ser aplicada mesmo em empresas que não tenham qualquer estabelecimento em nosso território**. Para que isso seja possível, é necessário o preenchimento de **pelo menos** um dos requisitos abaixo:

1. Ter estabelecimento no Brasil;

2. Oferecem serviços ao mercado consumidor brasileiro;
3. Coletam e tratam dados de pessoas localizadas no país.

Caso a empresa tenha estabelecimento no Brasil; ofereça serviços ao mercado consumidor brasileiro e/ou colete e faça o tratamento de dados pessoais de titulares que estejam localizados no Brasil, a Lei Geral de Proteção de Dados é aplicada.

Para facilitar a compreensão, verifique o seguinte exemplo:

A empresa americana ABC Products, com sede exclusivamente nos Estados Unidos, presta serviços de *call center* a diversas empresas ao redor do mundo, mas não tem em sua base de clientes qualquer empresa brasileira. Porém, um de seus clientes, também empresa Americana, presta serviços de *personal shopper (*auxiliam clientes a realizarem o consumo correto de acordo com as preferências do cliente) a clientes que são pessoas físicas brasileiras.

Como a empresa terceiriza seu serviço de atendimento à ABC Products, esta terá que fazer o atendimento e coletar dados de pessoas físicas que são brasileiras, mesmo não prestando o serviço diretamente ao mercado brasileiro ou possuindo filial no Brasil. Considerando que a empresa terá que fazer o tratamento de dados pessoais de pessoas residentes no Brasil, a empresa ABC Products deverá obedecer às regras da LGPD?

Sim, pois a empresa terá que realizar o tratamento de dados pessoais de pessoas residentes no Brasil.

Finalizando, necessário destacar pontos que não são relevantes para a aplicação da LGPD, como por exemplo:

1. Meio de operação de tratamento de dados;
2. País sede da empresa;
3. Localização dos dados;
4. Nacionalidade dos titulares de dados.

Por que os mencionados pontos não são relevantes para a aplicação da LGPD? Porque a LGPD (relembrando) adota a regra do *público-alvo* e o que é relevante para a aplicação da LGPD é se a empresa possui estabelecimento no Brasil, oferece serviços ao mercado consumidor brasileiro ou se faz o tratamento de dados de pessoas localizadas no país.

Percorridos os ensinamentos com relação à aplicação da lei, chegamos à parte em que discutiremos as hipóteses em que a lei autoriza a realização do tratamento de dados pessoais.

É importante relembrar estes conceitos, pois a LGPD dá um tratamento distinto com relação aos dados pessoais, dados sensíveis e dados de crianças e adolescente (estes últimos serão explicados no decorrer deste módulo).

AULA 20 – CONSENTIMENTO E CUMPRIMENTO DE OBRIGAÇÃO LEGAL E REGULATÓRIA

CONSENTIMENTO

O Consentimento é a primeira base legal (hipótese de autorização) constante na Lei Geral de Proteção de Dados e que muitas vezes gera uma grande confusão nas cabeças dos leitores. Embora seja a primeira base legal da lei, **não significa é que a base legal prioritária**, tendo em vista que não existe hierarquia entre as bases legais.

Ou seja, o consentimento não é a regra geral. Para cada tratamento de dados que será realizado, deverá ser observado todos os 10 (dez) princípios já ensinados neste curso e, após a análise do caso concreto, deverá ser escolhida a base legal mais adequada para a realização do tratamento.

Quando falamos em consentimento, deve-se observar que o consentimento deve ser livre e expresso (a pessoa não pode ser forçada a conceder o consentimento e deve constar expressamente no documento – prova – que o titular consentiu).

Um exemplo prático da possibilidade de utilização do consentimento como base legal para tratamento de dados pessoais é em casos de recebimento de e-mails de marketing de uma empresa que cujo titular não possua qualquer relação. Esta pessoa, após verificar alguma oferta, inscreve-se na base de dados da empresa para recebimento de e-mails com ofertas, consentindo com o tratamento de dados para essa única finalidade.

Outro ponto importante relacionado ao consentimento é a **possibilidade de sua revogação**. Caso o titular de dados não tenha mais interesse no tratamento de dados, poderá revogar o consentimento anteriormente fornecido.

O último ponto importante é sobre a **prova** do consentimento. Para evitar problemas futuros, a empresa que está fazendo o tratamento de dados com base no consentimento precisa possuir a prova de que coletou corretamente o consentimento, sob pena de no futuro o titular se opor ao tratamento informando que nunca o concedeu, podendo ensejar a aplicação de multas ou ações judiciais.

CUMPRIMENTO DE OBRIGAÇÃO LEGAL E REGULATÓRIA

Outra base legal é a de cumprimento de obrigação legal e regulatória. Nessa hipótese, a empresa (agente de tratamento de dados) está autorizada a fazer o tratamento de dados pessoais em razão de uma obrigação legal ou regulatória. Não é necessária qualquer autorização do titular ou utilização de outra base legal para que seja possível realizar o tratamento de dados pessoais.

Um bom exemplo de autorização do tratamento de dados em razão de obrigação legal é o caso dos Provedores de Aplicações de Internet (as redes sociais se encaixam como provedores). De acordo com o Marco Civil da Internet, em seu art. 15°, os Provedores de Aplicação são obrigados a manter os registros de acesso a aplicações de internet pelo prazo de 6 meses, ou seja, mesmo que o titular de dados não concorde, o Provedor de Aplicações está autorizado pela lei.

Agora vamos dar um exemplo com relação à obrigação regulatória. Quando o assunto é videomonitoramento de vias públicas, sempre há a discussão com relação à utilização das imagens das pessoas, cabendo, inclusive, outras bases legais para este tipo de caso, como a base do legítimo interesse.

Porém, quando se tem uma resolução, como é o caso da Resolução n° 471 de 2013 do Conselho Nacional de Trânsito (CONTRAN) que regulamenta a fiscalização de trânsito por intermédio de monitoramento em estradas e rodovias, os agentes públicos têm a autorização para a realização do tratamento de dados pessoais sem a autorização do titular, sendo essa uma obrigação regulamentar.

COMENTÁRIOS SOBRE TRATAMENTO DE DADOS SENSÍVEIS

Demonstradas as bases legais que existem na legislação, é importante, neste momento, realizar alguns comentários com relação às mencionadas bases legais direcionadas aos dados sensíveis, tendo em vista que existem algumas pequenas diferenças que precisam ser observadas.

No momento de realizar um tratamento de dado sensível, também é possível utilizar a base legal do consentimento. Porém, há uma pequena ressalva com relação ao dado sensível que a lei não estipula para os dados pessoais "comuns".

Realizando a leitura da lei (art. 11, I), há a seguinte redação: Art. 11, I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas.

A grande diferença quando se fala em dado sensível e consentimento é que o **consentimento deve ser dado de forma específica e destacada para finalidades específicas**. Portanto, no momento de ser coletado o consentimento do titular para tratamento de dados sensíveis, é necessário demonstrar ao titular, de forma minuciosa, qual é a finalidade desse tratamento de dado sensível.

Muitas empresas, no momento de realizar esse tratamento, oferecem um termo de consentimento ao titular de dados sensíveis. Nesse termo, constam todas as informações sobre o tratamento que será realizado, como por exemplo sua finalidade, como os dados serão compartilhados, as formas de armazenamento do dado etc.

COMENTÁRIO SOBRE DADOS DE CRIANÇAS E ADOLESCENTES

Finalizando esta aula, é necessário trazer alguns comentários com relação aos dados de crianças e adolescentes, ainda mais pelo fato de a lei separar um capítulo específico para esse assunto.

Precisamos apenas relembrar que, de acordo com as leis brasileiras, criança é toda pessoa que possui até 12 anos incompletos. Então, crianças são pessoas de 0 até 12 anos incompletos e adolescentes são pessoas entre 12 e 18 anos de idade.

É importante ter cuidado ao realizar o tratamento de dados de crianças e adolescentes, porque são pessoais vulneráveis que não possuem o discernimento completo, principalmente para tomarem decisões em nome próprio, sendo, inclusive, esse o motivo do Código Civil Brasileiro trazer as questões de capacidade civil (aptidão que a pessoa tem de adquirir e exercer os seus direitos).

A LGPD traz uma redação interessante com relação ao assunto, informando que "o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado **em seu melhor interesse**, nos termos deste artigo e da legislação pertinente". Então, a lição que deve ser sempre relembrada é de que qualquer tratamento de dados de crianças e de adolescentes deve observar o melhor interesse deles.

E o que é melhor interesse de crianças e adolescentes? Como mencionado, as crianças e adolescentes são pessoas vulneráveis e que precisam de uma maior atenção. Assim, qualquer decisão relacionada a elas deve observar todos os seus direitos. É o que acontece nos casos de ações de guarda compartilhada, os direitos das crianças se sobressaem aos direitos dos pais, sendo primordial os interesses e necessidades das crianças para a decisão judicial.

Tratando-se do assunto de proteção de dados, os direitos das crianças e adolescentes de sobressaem com relação a qualquer outro direito, devendo todo o tratamento ser cuidadoso e zelar pela preservação dos direitos dos menores. É necessário observar também que conforme a LGPD, o consentimento envolvendo o tratamento de dados de crianças e adolescentes deverá ser fornecido por pelo menos um dos pais ou responsáveis.

AULA 21 – EXECUÇÃO DE POLÍTICAS PÚBLICAS, REALIZAÇÃO DE ESTUDOS POR ÓRGÃO DE PESQUISA E DE EXECUÇÃO DE CONTRATOS

EXECUÇÃO DE POLÍTICAS PÚBLICAS

Os agentes de tratamento – que nesse caso são da administração pública - também estão autorizados a realizar o tratamento de dados pessoais em caso de execução de políticas públicas. Mas o que são políticas públicas?

Para ficar mais fácil a compreensão, pensemos em um exemplo prático. Imaginemos que uma cidade, após verificar que a criminalidade tem aumentado nos últimos meses, decida instalar câmeras de monitoramento ao redor da cidade, sem violar a privacidade dos cidadãos.

Como se trata de uma política pública, visando o interesse público que é a própria segurança dos residentes da cidade, não é necessária qualquer outra base legal para autorizar esse tratamento, sendo que a base legal de execução de políticas públicas é suficiente para legitimar esse tratamento.

REALIZAÇÃO DE ESTUDOS POR ÓRGÃO DE PESQUISA, GARANTIDA, SEMPRE QUE POSSÍVEL, A ANONIMIZAÇÃO DOS DADOS PESSOAIS

De início, relembremos que a anonimização dos dados pessoais é o processo técnico que visa retirar a possibilidade de o Dado Pessoal identificar uma Pessoa Natural de forma irreversível.

Assim, sendo possível a anonimização do dado pessoal, a lei autoriza que os órgãos de pesquisa realizem estudos, não tornando tal prática ilegal. Um exemplo prático desse caso é a própria pesquisa do IBGE (Instituto Brasileiro de Geografia e Estatística), que seria inviável caso não existisse esta autorização legal para que fosse realizada.

EXECUÇÃO DE CONTRATOS E PROCEDIMENTOS PRELIMINARES

Um grande equívoco que muitos cometem é a utilização da base legal do consentimento no lugar da execução de contratos e procedimentos preliminares.

Esta base legal consiste na autorização da lei para a realização do tratamento dos dados pessoais em caso de execução do contrato. Nas hipóteses em que as pessoas celebram contratos entre elas, como um contrato de compra e venda de imóvel, como seria possível a execução desse contrato caso uma das duas partes não autorizasse a utilização dos dados? O negócio seria totalmente prejudicado.

Este tipo de erro ocorre com frequência quando o assunto é relação de trabalho, pois muitas pessoas cometem o equívoco de afirmar que para a execução de um contrato

de trabalho é necessário coletar o consentimento do empregado. Tal situação é equivocada pela mesma razão do exemplo acima, pois a execução do contrato de trabalho ficaria frustrada, pois para toda atividade que envolvesse os dados de funcionários, seria necessária a coleta de seu consentimento, inviabilizando a atividade econômica.

AULA 22 – EXERCÍCIO REGULAR DE DIREITOS EM PROCESSOS JUDICIAIS, ADMINISTRATIVOS OU ARBITRAIS E PROTEÇÃO À VIDA OU À INCOLUMIDADE DO TITULAR OU DE TERCEIROS

EXERCÍCIO REGULAR DE DIREITOS EM PROCESSOS JUDICIAIS, ADMINISTRATIVOS OU ARBITRAIS

Imagine a sua empresa está passando por um processo trabalhista e o departamento responsável não armazenou os documentos do ex-empregado, acreditando que não era possível fazer esse armazenamento porque o ex-empregado não havia autorizado.

E agora? Como apresentar a defesa adequada no processo em que está sofrendo pelo ex-colaborador?

É por essa razão que a lei criou essa possibilidade de os agentes de tratamento realizarem o tratamento de dados (como o armazenamento) para exercer seus direitos em processos judiciais, administrativos ou arbitrais.

PROTEÇÃO À VIDA OU INCOLUMIDADE DO TITULAR OU TERCEIROS

Esta é outra possibilidade que, felizmente, a lei concede aos agentes de tratamento de dados pessoais. A mencionada hipótese de tratamento pode ocorrer para proteger a vida ou a incolumidade do titular ou terceiros.

Podemos pensar na utilização desta hipótese em casos de tratamento de saúde, uma vez que inexistindo o tratamento de dados do paciente, seria impossível realizar o procedimento de saúde que tem o objetivo de salvar a vida sua vida ou de terceiros. Além disso, podemos afirmar que essa hipótese é aplicada principalmente em casos de emergência em que o titular não tem condições de expressar a sua vontade, visto que seria impossível a não concordância do titular em um caso emergencial.

AULA 23 – TUTELA DA SAÚDE, LEGÍTIMO INTERESSE E PROTEÇÃO AO CRÉDITO

TUTELA DA SAÚDE

Tratando-se do assunto de tutela da saúde, podemos afirmar que esta hipótese de tratamento de dados pessoais ocorre exclusivamente em casos de procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

É relativamente óbvio o motivo de tal autorização ser concedida pela lei. Imagine uma pessoa sendo direcionada ao ortopedista porque foi constatada uma fratura no dedo da mão. No momento em que o paciente chega ao ortopedista, este se nega a fornecer os seus dados pessoais. Como é possível o ortopedista realizar o procedimento que tem a única finalidade tutelar a saúde do indivíduo?

INTERESSE LEGÍTIMO DO CONTROLADOR OU DE TERCEIRO

Chegando às últimas bases legais, agora estamos diante da autorização que é a mais aberta a interpretações. Para que se comprove o que foi afirmado, vamos trazer o trecho da lei:

> Art. 7º, IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Esta base chamada de legítimo interesse é praticamente uma cópia da redação da Regulamentação Europeia que, da mesma forma, é relativamente vaga. A ideia deste estudo não é nos aprofundarmos nas discussões jurídicas, mas sim, ensinar os preceitos e suas aplicações práticas.

Um simples exemplo da possibilidade de utilização dessa base legal é em casos de *utilização de câmeras de segurança em estabelecimentos*. Essas câmeras fazem a captação de imagens que, consequentemente, são possíveis de identificar uma pessoa, ou seja, tratando-se de um dado pessoal. Desta forma, desde que seja dada a devida **transparência** ao titular de dados com relação ao tratamento realizado, como por exemplo a fixação de uma placa informando "sorria, você está sendo filmado", é possível a utilização da base legal do legítimo interesse nesses casos.

O legítimo interesse no caso mencionado é o simples interesse (legítimo) em manter o ambiente – que pode ser uma loja – seguro e eventualmente utilizar as filmagens para buscar os direitos que forem lesados.

PROTEÇÃO AO CRÉDITO

Por fim, chegamos à base legal de proteção ao crédito. Neste caso, a autorização para a proteção ao crédito não é para todo tipo de empresa, mas sobretudo para instituições financeiras, não sendo possível um agente de tratamento fazer a alegação de que irá realizar o tratamento de dados em razão de visar a proteção ao crédito.

Vejamos o que a lei dispõe: Art. 7°, X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Este inciso impediria que os titulares alegassem os preceitos da LGPD para evadirem de uma eventual consulta pelas instituições financeiras ao cadastro de inadimplentes.

A lei menciona "legislação pertinente", sendo a legislação dos "birôs" de crédito, mais conhecida como LCP (Lei 12.414 de 2011), que trata sobre a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.

Assim, caso uma empresa que não se enquadre nessa hipótese faça o tratamento de dados sob a pretensa alegação de proteção ao crédito, realizará o tratamento de dados de forma equivocada.

MÓDULO 05

TRATAMENTO E MAPEAMENTO DE DADOS

AULA 24 – O QUE É TRATAMENTO DE DADOS?

No módulo anterior, aprendemos como a Lei Geral de Proteção de Dados é aplicada e quais são as hipóteses legais que autorizam a realização do tratamento de dados. Mas o que de fato é uma atividade de tratamento de dados pessoais? Conforme a LGPD, temos o seguinte conceito:

> Art. 5° Para os fins desta Lei, considera-se:
>
> **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;

Como podemos compreender pela leitura da lei, atividades de tratamento seriam então quaisquer ações envolvendo um dado pessoal, desde o mero acesso até a exclusão da informação. É seguro dizer, portanto, que o tratamento de dados implica qualquer atividade de processamento realizada durante o ciclo de vida de um dado. Passemos a alguns exemplos práticos:

Quando o consumidor decide ir à farmácia em busca de medicamentos, quaisquer que sejam, alguns estabelecimentos perguntam ao titular qual seria seu CPF, com a pretensão de lhe oferecer algum desconto em produtos. Neste caso, observe: mesmo que a farmácia não armazene ou compartilhe suas informações pessoais, o mero acesso que teve às informações já configura uma atividade de tratamento.

É comum também ser abordado por ativistas ou representantes de instituições não governamentais. Ao informar seu nome, o sujeito o escreve em uma prancheta para buscar engajamento em alguma causa social. Para além da discussão sobre a relevância ou não de campanhas desse tipo, é correto afirmar que o tratamento de dados ocorreu em dois momentos: tanto na coleta do seu dado pessoal pelo representante da organização, quanto no registro desse dado em uma base física (prancheta).

É importante ressaltar que dados pessoais apenas poderão ser tratados pelos denominados "Agentes de Tratamento" que serão abordados futuramente. Isso significa que somente entidades controladoras e operadoras de dados pessoais realizam o tratamento de dados pessoais, e não seus representantes. Assim, nos exemplos apontados acima, a farmácia e a organização social realizam as atividades de tratamento, e não seus subordinados.

Além disso, como observado, o tratamento de dados não ocorre apenas digitalmente, como nas plataformas e websites, mas também fisicamente, em qualquer tipo de meio ou suporte em que seja possível a identificação de uma pessoa natural (pessoa física).

Isso significa que eu posso simplesmente me recusar a oferecer minhas informações a quaisquer pessoas ou estabelecimentos?

Em teoria, sim, sobretudo quando observamos o fundamento da autodeterminação informativa, explanado anteriormente no Curso. Através dele, se atribui ao cidadão a possibilidade de optar se e quando seus dados serão tratados, sendo seu direito exigir informações claras a respeito das atividades de tratamento. No entanto, no âmbito prático isso pode ser inviável, considerando que o tratamento de dados pessoais pode ser condição indispensável ao oferecimento de alguns produtos e serviços aos titulares.

Por fim, devemos relembrar que em alguns casos é impossível impedir o tratamento de dados pessoais, como observado nas aulas sobre hipóteses de tratamento. É por isso não se pode afirmar que o direito à privacidade seja um direito absoluto, considerando que por vezes os dados pessoais do titular poderão ser processados independentemente de sua vontade para propósitos específicos.

AULA 25 – O QUE É MAPEAMENTO DE DADOS?

Neste momento, será explicado o que é o mapeamento de dados e a sua importância em toda a empresa, principalmente nos projetos de adequação das empresas à Lei Geral de Proteção de Dados.

Além de ser um procedimento de extrema relevância durante projetos de adequação, o mapeamento de dados é o passo anterior ao registro das operações de tratamento de dados pessoais que o Controlador e o Operador (agentes de tratamento – módulo 6) devem manter para cumprimento da lei.

O Mapeamento de Dados não é algo exclusivo da Lei Geral de Proteção de Dados, também existindo tal procedimento no Regulamento Europeu e até na lei de proteção de dados da Califórnia. Este mapeamento também é conhecido como *data mapping* e *data flow*, é um procedimento que irá dar nascimento ao inventário de dados, um documento que contará com todos os fluxos de dados pessoais de uma determinada organização, sendo possível identificar todos os agentes de tratamento, origem dos fluxos de dados e, principalmente, equívocos que devem ser corrigidos no tratamento de dados pessoais.

De início, é importante ressaltar que a realização do mapeamento é de extrema importância para cumprimento de um dever imposto pela Lei Geral de Proteção de Dados que é a criação de um **inventário de dados**.

Esse inventário é basicamente uma planilha que constará todos os fluxos de dados pessoais da empresa e, em cada fluxo, será demonstrada: qual a origem dos dados de determinado processo, quais os sistemas envolvidos no tratamento de dados, se existe compartilhamento externo, como se dá o armazenamento, qual é a base legal para o tratamento de dados etc.

Para que fique mais fácil a compreensão, é necessário trazer um caso hipotético:

Vamos pensar em uma empresa que está fazendo o mapeamento de dados pessoais e está verificando os fluxos de dados pessoais do departamento de Recursos Humanos. O primeiro fluxo mapeado foi o fluxo de "entrevistas de candidatos à vaga". Nesse fluxo, será observado que os dados chegam na empresa diretamente pelo candidato que enviou o seu currículo ao e-mail da empresa. Além disso, será verificado qual é a base legal que autoriza esse tratamento e com quais departamentos internos a empresa faz o compartilhamento dos dados, como por exemplo com o chefe da área comercial que irá fazer a entrevista do candidato. Não só isso: dentro do inventário, constará quais sistemas são utilizados para fazer esse tratamento, como o sistema interno da empresa, bem como se existe algum compartilhamento desses dados com outras empresas.

Com a compreensão de que **o mapeamento é anterior** ao inventário de dados (obrigação legal das empresas), ressalta-se que outro grande objetivo do mapeamento é verificar como a empresa está tratando do assunto da privacidade e quais salvaguardas adota para a proteção dos dados pessoais tratados, constatando-se ao final se a empresa está ou não adequada à Lei Geral de Proteção de Dados.

AULA 26 - MAPEAMENTO DE DADOS NA PRÁTICA

Na Lei Geral de Proteção de Dados não existe uma determinação de como deve ser realizado o mapeamento, nem ao menos quais são as informações necessárias que devem constar no inventário de dados que as empresas devem manter em registro. Assim, é necessário observar o que as outras legislações e órgãos nos ensinam, como é o caso do ICO (*Information Commissioner's Office*), instituição pertencente à União Europeia.

O mencionado ICO possui um modelo de inventário de dados disponibilizado em seu *site*, com o intuito de demonstrar às empresas quais são as informações relevantes para demonstrar que os dados pessoais estão sendo tratados corretamente. Assim, de acordo com o seu modelo, as informações que devem ser anotadas, criando um paralelo com a LGPD, são as seguintes:

- Nome e Contato da pessoa informante sobre o tratamento de dados;
- Cargo;
- Finalidade do tratamento de dados (ex: contratação de novos talentos);
- Categoria do titular de dados (ex: Colaborador);
- Categoria do receptor dos dados (ex: Departamento de RH);
- Prazo de retenção dos dados;
- Descrição das medidas técnicas de segurança;
- Base legal para o tratamento;
- Direitos dos titulares disponíveis;
- Existência de decisões automatizadas;
- Origem do dado pessoal (ex: colaborador); e

- Local em que está o dado pessoal (ex: contas a pagar);

Para que seja possível ter ciência de quais dados são tratados, como são tratados e se a empresa está adequada à Lei Geral de Proteção de Dados, é inevitável que a empresa possua um inventário de dados pessoais com as mencionadas informações.

E como as mencionadas informações são coletadas?

Existem *softwares* no mercado que são capazes de auxiliar na elaboração deste inventário de dados, mas, da mesma forma, as informações que serão inseridas no *software* serão inseridas por alguma pessoa responsável da empresa, sendo impossível possuir uma coleta de todas essas informações por inteligência artificial.

Então, mesmo existindo essas facilidades tecnológicas, **as informações que são inseridas no inventário de dados são coletadas diretamente dos departamentos internos**. Essas informações coletadas, normalmente, são realizadas através de entrevistas com as pessoas responsáveis pelos departamentos escolhidos, com os questionamentos sobre todos os pontos acima mencionados que constam do inventário de dados.

Através dessas entrevistas, é possível coletar toda a informação necessária para verificar se a empresa está adequada à legislação. Caso seja apurado que algo está inadequado ou até mesmo ilegal, é possível tomar as devidas providências após o procedimento que foi realizado, como por exemplo a adequação de algum fluxo que está realizando a coleta equivocada de dados pessoais.

IEL
Instituto Euvaldo Lodi
PELO FUTURO DA INDÚSTRIA

MÓDULO 06

AGENTES DE TRATAMENTO: CONTROLADORES E OPERADORES

AULA 27 – CONTROLADOR E CO-CONTROLADOR DE DADOS PARTE 1

O primeiro agente de tratamento que será abordado neste módulo será o Controlador, considerado o ator principal dentro do processo de tratamento de dados. Basicamente, o Controlador é a pessoa física ou jurídica (em qualquer formato jurídico, podendo ser desde EIRELI até uma grande holding ou conglomerado) responsável pelas decisões relativas à finalidade e forma de tratamento dos dados pessoais.

Muitos acreditam que os Controladores são as pessoas naturais vinculadas profissionalmente a uma empresa (como por exemplo o chefe do departamento de compras). Entretanto**, estas pessoas são apenas representantes da empresa**, que é de fato a Controladora, uma vez que todas as decisões e ações tomadas por essas pessoas naturais são relacionadas à própria empresa e não à vida pessoal delas.

Outro ponto importante com relação aos controladores é que estes também podem ser figuras da Administração Pública, como a própria Previdência Social que possui dados de diversos cidadãos e possui autonomia para tomar decisões com relação a esses dados pessoais.

Vejamos agora quais são as fontes da competência do controlador:

COMPETÊNCIA ADVINDA DA LEI

Essa hipótese normalmente ocorre em relações trabalhistas, como é o caso de a CLT determinar à empresa o registro de entrada e saída de empregados, cabendo à empresa realizar esse tratamento de dados em razão de obrigação legal.

COMPETENTE PELA TOMADA DE DECISÕES NO CASO CONCRETO

Normalmente, a empresa será considerada Controladora em razão do próprio caso concreto e não advindo de lei. Assim, caso a empresa tenha grande influência no tratamento de dados e autonomia para tomar decisão com relação a isso, será a Controladora.

AULA 28 – CONTROLADOR E CO-CONTROLADOR DE DADOS PARTE 2

Na GDPR, existe a figura denominada *joint controller*, possuindo basicamente a tradução de Controlador Conjunto, que age conjuntamente com outro Controlador para tomar as decisões relativas ao tratamento de dados pessoais.

Mesmo inexistindo na LGPD tal figura, é possível verificar na redação do art. 42, §1°, II, da lei, uma situação que se conclui pela relação de dois Controladores Conjuntamente, senão vejamos: "II - os controladores que estiverem diretamente envolvidos no

tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. ”

Quando é falado o termo solidário/solidariamente nas legislações brasileiras, significa que a responsabilidade não é apenas de uma pessoa/agente, mas de ambos. Neste caso, verificado também que os Controladores podem tomar decisões em conjunto com relação a certo tratamento de dados, é possível concluir que existe a figura do Controlador Conjunto.

Lembre-se que existe uma diferença entre Controladores Conjuntos (decidem de forma conjunta sobre um mesmo tratamento de dados) e Controladores que podem ser chamados de Independentes, uma vez que os independentes não atuam de forma conjunta para determinada finalidade, nem ao menos são solidários com relação à eventual responsabilização.

Para que seja possível constatar a existência de Controladores Conjuntos, basta apenas observar que seria inviável o tratamento de dados sem a participação de ambas as partes decidindo sobre o tratamento e buscando um mesmo fim. Diferencia-se da questão Operador e Controlador, uma vez que, conforme será demonstrado na próxima aula, o Operador não tem autonomia para decidir sobre o tratamento de dados pessoais.

AULA 29 – OPERADOR E SUB-OPERADOR DE DADOS – PARTE 1

O operador é o agente responsável por realizar o tratamento de dados em nome do controlador e conforme a finalidade por este delimitada. A definição legal se encontra no art. 5º, inciso X da LGPD: “Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”. Nesse mesmo sentido é a previsão do art. 39 da LGPD: “O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.”

A previsão acima implica dizer que o operador só poderá tratar os dados para a finalidade previamente estabelecida pelo controlador. Isso demonstra a principal diferença entre o controlador e operador, qual seja, o poder de decisão: o operador só pode agir no limite das finalidades determinadas pelo controlador.

Com as definições e casos práticos mencionados sobre os Controladores, iremos definir e mostrar como é possível identificar o Operador, outro agente de tratamento de extrema importância na Lei Geral de Proteção de Dados.

De acordo com a lei, o Operador é um agente de tratamento que também pode ser pessoa física ou jurídica, de direito público ou privado, que tem a função de realizar o tratamento de dados pessoais em nome do Controlador. De maneira simples, podemos dizer que o Operador é um braço do Controlador, possuindo pouca ou nenhuma autonomia para determinar as principais atividades do tratamento de dados.

No tópico acima, demonstramos que a pessoa física que trabalha dentro de um Controlador (pessoa jurídica) não pode ser confundida com o próprio Controlador, uma vez que essa pessoa apenas representa legalmente a pessoa jurídica. Com relação ao Operador, aplica-se a mesma compreensão. A pessoa física que trabalha em uma empresa que Operadora não pode ser considerada a própria Operadora.

Tratando-se da responsabilização, de acordo com a lei, caso o Operador não siga as instruções que foram dadas pelo Controlador, ou até mesmo viole a lei, será equiparado à figura do Controlador e responderá civilmente e deverá arcar com a indenização ao titular de dados que foi lesado.

Como última observação, é interessante destacar que a empresa para se configurar como Operadora não é necessário que a atividade dela esteja diretamente ligada com o tratamento de dados pessoais. Um exemplo é o caso das empresas que terceirizam o serviço de motorista. O principal objetivo é o fornecimento de serviço de motorista, mas, inevitavelmente, o motorista contratado fará o tratamento de dados do funcionário que irá transportar, não possuindo qualquer autonomia para decidir o que irá fazer com os dados dessa pessoa.

AULA 30 – OPERADOR E SUB-OPERADOR DE DADOS – PARTE 2

A LGPD não trata especificamente da figura do sub-operador, no entanto, embora inexista conceito de sub-operador na LGPD, o tema pode ser utilizado como parâmetro de análise para compreensão de cadeias mais complexas de tratamento de dados.

A falta do conceito de sub-operador na LGPD não impossibilita ou torna ilegal que ele exista ou que tenha funções, competências e responsabilidade no ambiente de proteção de dados pessoais brasileiro, principalmente porque pode desempenhar a função de operador em subordinação a outro operador.

Dito isso, importa saber que o sub-operador é um agente contratado pelo Operador para realizar um serviço. Imagine que a empresa A contrata a empresa B para realizar toda a operação de contas a receber e contas a pagar (Empresa A é a Controladora e a empresa B é a Operadora). Em seguida, a empresa B contrata a empresa C para realizar parte desses serviços, como por exemplo o pagamento dos fornecedores.

No exemplo mencionado, A é Controladora, B é Operadora e C é sub-operadora. A empresa A tem autonomia para decidir sobre o tratamento dos dados. A empresa B apenas segue as instruções da empresa A. E, por fim, a empresa C apenas segue as instruções passadas à B.

Por fim, no que se refere às responsabilidades, o sub-operador pode ser é equiparado ao operador perante a LGPD em relação às atividades que foi contratado para executar. Ocorre, dessa forma, a ampliação da cadeia de responsabilidade solidária prevista no art. 42, §1°, I da LGPD. Ademais, é importante destacar que deve constar em contrato a autorização para a contratação de Sub-operador

AULA DE REVISÃO 02

Revisaremos o conteúdo visto nos módulos 04, 05 e 06.

AULA 31 - REVISÃO MÓDULO 04 – INTRODUÇÃO A APLICAÇÃO PRÁTICA DA LEI GERAL DE PROTEÇÃO DE DADOS COM EXPOSIÇÃO DAS BASES LEGAIS QUE JUSTIFICAM O TRATAMENTO DE DADOS PESSOAIS DENTRO DE UMA INSTITUIÇÃO.

REVISÃO AULA 19 – APLICAÇÃO TERRITORIAL DA LEI GERAL DE PROTEÇÃO DE DADOS E SUAS BASES LEGAIS

- A LGPD é aplicada sempre que o tratamento de dados for realizado no território brasileiro ou se a atividade envolver oferecimento de produtos ou serviços de pessoas que se encontram em território nacional;
- LGPD adotou a regra chamada de público-alvo, que significa que a coleta de dados em território nacional ou a oferta dos serviços aos cidadãos brasileiros ou pessoas que estejam em território nacional, mesmo que seja realizado por empresa sediada no estrangeiro, é aplicada à LGPD;
- Para aplicação da LGPD, são irrelevantes ponto como: a) meio de operação de tratamento de dados; País sede da empresa, Localização dos dados; Nacionalidade dos titulares de dados.

REVISÃO AULA 20 – CONSENTIMENTO E CUMPRIMENTO DE OBRIGAÇÃO LEGAL E REGULATÓRIA

- O consentimento:
  - é a primeira base legal (hipótese de autorização) constante na Lei Geral de Proteção de Dados;
  - Consentimento não é regra geral, porque não há hierarquia entre bases legais;
  - Consentimento tem que ser livre e expresso;
  - Deve existir a possibilidade de revogação do consentimento;
  - Há a necessidade de provar o consentimento;
  - Consentimento deve ser dado de forma específica e destacada para finalidades específicas quando há tratamento de dados pessoais sensíveis.
  - Cumprimento de obrigação legal e regulatória:
  - não é necessária qualquer autorização do titular ou utilização de outra base legal para que seja possível realizar o tratamento de dados pessoais;
  - O tratamento de dados pessoais de crianças e adolescentes deve ser feito em seu melhor interesse

REVISÃO AULA 21 – EXECUÇÃO DE POLÍTICAS PÚBLICAS, REALIZAÇÃO DE ESTUDOS POR ÓRGÃO DE PESQUISA E EXECUÇÃO DE CONTRATOS

- Execução de Políticas Públicas:
  - Uma concepção institucionalizada para a solução de problemas públicos que afetam uma coletividade;
- Realização de estudos por órgão de pesquisa:
  - O tratamento do dado com base nesse fundamento deve, sempre que possível, garantir a anonimização dos dados pessoais;
- Execução de contratos e procedimentos preliminares:
  - Fases preliminares, isto é, pretéritas a pactuação do contrato também estão inclusas;
- Contratos de trabalho são o principal exemplo de uso dessa base legal.

REVISÃO AULA 22 – EXERCÍCIO REGULAR DE DIREITOS EM PROCESSOS JUDICIAIS, ADMINISTRATIVOS OU ARBITRAIS E PROTEÇÃO À VIDA OU INCOLUMIDADE DO TITULAR OU TERCEIROS

- Exercício regular de direitos em processos judiciais:
  - Processos administrativos e arbitrais também podem valer desta base legal.
  - Proteção à vida ou incolumidade do titular ou terceiros:
  - Hipótese geralmente aplicada em emergências, a qual o titular dos dados não pode dar seu aceite e consentir com o tratamento dos seus dados e, que sem eles, sua vida estaria em risco;

REVISÃO AULA 23 – TUTELA DA SAÚDE, LEGÍTIMO INTERESSE E PROTEÇÃO AO CRÉDITO

- Tutela da saúde: ocorre exclusivamente em casos de procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
  - Interesse legítimo do Controlador ou de Terceiro:
  - O clássico exemplo é de *utilização de câmeras de segurança em estabelecimentos;*
  - Transparência deve ser respeitada quando do uso do interesse legítimo.
- Proteção ao crédito:
  - Base legal muito usada por instituições financeiras e birôs de crédito;
- A lei do cadastro positivo (Lei n° 12.414 de 2011), complementa o uso desta base legal.

AULA 32 - REVISÃO MÓDULO 05 – TRATAMENTO E MAPEAMENTO DE DADOS PESSOAIS

REVISÃO AULA 24 – O QUE É TRATAMENTO DE DADOS?

- Atividades de tratamento são quaisquer ações envolvendo um dado pessoal, desde o mero acesso até a exclusão da informação, definido no art. 5º da LGPD;
- O tratamento de dados implica qualquer atividade de processamento realizada durante o ciclo de vida de um dado;
- Os dados pessoais apenas poderão ser tratados pelos denominados Agentes de Tratamento;
- O Tratamento de dados pessoais pode ocorrer em meios analógicos;
- Em hipóteses específicas, os dados pessoais do titular podem ser processados independentemente da sua vontade.

REVISÃO AULA 25 – O QUE É MAPEAMENTO DE DADOS?

- Mapeamento de Dados também é conhecido como *data mapping e data flow;*
- Um procedimento que irá dar nascimento ao inventário de dados, um documento que contará com todos os fluxos de dados pessoais de uma determinada organização, sendo possível identificar todos os agentes de tratamento, origem dos fluxos de dados e, principalmente, equívocos que devem ser corrigidos no tratamento de dados pessoais;
- Inventário de dados é uma planilha que constará todos os fluxos de dados pessoais da empresa e, em cada fluxo, será demonstrada: a origem dos dados de determinado processo, quais os sistemas envolvidos no tratamento de dados, se existe compartilhamento externo, como se dá o armazenamento, qual é a base legal para o tratamento de dados etc.

REVISÃO AULA 26 – MAPEAMENTO DE DADOS NA PRÁTICA

- A LGPD não explicita o que como fazer um mapeamento e nem o que constar no inventário de dados.
- Segundo a ICO (*Information Commissioner's Office*), o inventário de dados deve conter os seguintes pontos:
    - Nome e Contato da pessoa informante sobre o tratamento de dados;
    - Cargo;
    - Finalidade do tratamento de dados (ex: contratação de novos talentos);
    - Categoria do titular de dados (ex: Colaborador);
    - Categoria do receptor dos dados (ex: Departamento de RH);
    - Prazo de retenção dos dados;
    - Descrição das medidas técnicas de segurança;
    - Base legal para o tratamento;

- Direitos dos titulares disponíveis;
- Existência de decisões automatizadas;
- Origem do dado pessoal (ex: colaborador); e
- Local em que está o dado pessoal (ex: contas a pagar);
- O mapeamento das informações se faz, comumente, com um auxílio de Software especializado. Já a coleta - informações que são inseridas no inventário de dados - são coletadas diretamente dos departamentos internos;

AULA 33 - REVISÃO MÓDULO 06 – AGENTES DE TRATAMENTO: CONTROLADORES E OPERADORES

REVISÃO AULA 27 – CONTROLADOR E CO-CONTROLADOR DE DADOS – PARTE 1

- O Controlador é a pessoa física ou jurídica responsável pelas decisões relativas à finalidade e forma de tratamento dos dados pessoais;
- Controladores são as pessoas jurídicas, e não os seus colaboradores;

REVISÃO AULA 28 – CONTROLADOR E CO-CONTROLADOR DE DADOS – PARTE 2

- A GDPR prevê uma figura denominada *joint controller.* É quem age conjuntamente com outro Controlador para tomar as decisões relativas ao tratamento de dados pessoais.
- Na LGPD não há previsão expressa do controlador. Porém pela redação do art. 42, §1°, II, entende-se por uma situação que se conclui pela relação de dois Controladores;
- Controladores Conjuntos: decidem de forma conjunta sobre um mesmo tratamento de dados;
- Controladores que Independentes: não atuam de forma conjunta para determinada finalidade;

REVISÃO AULA 29 – OPERADOR E SUBOPERADOR DE DADOS – PARTE 1

- A definição legal de operador é encontrada no art. 5°, inciso X da LGPD: "Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".
- O operador só poderá tratar os dados para a finalidade previamente estabelecida pelo controlador, possuindo pouca ou nenhuma autonomia para determinar as principais atividades do tratamento de dados;

- A figura do operador e controlador não se confundem;
- Responsabilização do operador: não respeitando os limites da ordem do controlador, o operador será equiparado à figura do Controlador e responderá civilmente e deverá arcar com a indenização ao titular de dados que foi lesado;

REVISÃO AULA 30 – OPERADOR E SUB-OPERADOR DE DADOS – PARTE 2

- A LGPD não trata da figura do sub-operador. Porém, não há empecilhos legais para que exista;
- Sub-operador é um agente contratado pelo Operador para realizar um serviço;
- Responsabilidades: pode ser equiparado ao operador, assim, há a ampliação da cadeia de responsabilidade solidária prevista no art. 42, §1°, I da LGPD.

MÓDULO 07

O ENCARREGADO DE DADOS E SUAS RESPONSABILIDADES

AULA 34 - O ENCARREGADO DE DADOS NA LGPD

Encarregado de Dados é baseada no DPO da GDPR, é possível compreender, com a leitura do tópico acima, qual seria o perfil e algumas atribuições desta figura constante na LGPD. Entretanto, vamos tratar de algumas especificidades do Encarregado de Dados.

De acordo com o art. 5º, VII, LGPD, o Encarregado **é a 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).**

Com a descrição constante na lei, é possível verificar que a figura é parecida com o DPO da GDPR, tendo em vista que realiza toda a intermediação entre os titulares, os agentes e a ANPD.

A importância do Encarregado de Dados, de acordo com a LGPD, é clara: ele **centraliza** a discussão sobre a conformidade à nova lei e **coordena** a implementação de melhorias, bem como **acompanha** a evolução do tema junto da instituição, do mercado e da sociedade, tendo uma atuação relevante na fase de adaptação, mas também no que precisa ser depois atualizado.

Ao contrário de outras legislações de proteção de dados estrangeiras, a LGPD não determinou em que circunstâncias uma organização deve indicar um encarregado. Assim, deve- se assumir, como regra geral, que toda organização deverá indicar uma pessoa para assumir esse papel.

De acordo com o § 3o do art. 41, normativas futuras da ANPD poderão trazer hipóteses de dispensa da necessidade de indicação do encarregado, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

O artigo 41 da LGPD não faz distinção quanto a instituições públicas ou privadas e por isso é importante que ambas estejam cientes da sua obrigação de indicar um encarregado de dados. A esse respeito, o art. 23, III, reforça a necessidade de um encarregado ser indicado por órgãos e entidades públicas.

A LGPD também não distingue se o encarregado deve ser pessoa física ou jurídica, e se deve ser um funcionário da organização ou um agente externo. Considerando as boas práticas internacionais, o encarregado poderá ser tanto um funcionário da instituição quanto um agente externo, de natureza física ou jurídica. As modalidades de contratação do Encarregado serão analisadas na Aula 28.

AULA 35 - O PERFIL E INDICAÇÃO DO ENCARREGADO DE DADOS

Com a leitura da lei, facilmente é possível identificar as tarefas que um Encarregado de Dados há de cumprir, porém, não se sabe ao certo quais seriam as características e experiências para que uma pessoa seja nomeada como Encarregado de Dados.

Não há qualquer pré-requisito, como por exemplo a graduação em Tecnologia da Informação ou em Direito. Nem ao menos existe a necessidade de realização de cursos de aprimoramento com relação às leis de proteção de dados.

Porém, observando-se a GDPR e as organizações que auxiliam na adequação das empresas às leis de privacidade, bem como relembrando que um programa de proteção de dados envolve muitas disciplinas, como o conhecimento em gestão, governança corporativa, legislações específicas sobre proteção de dados, Segurança da Informação e Tecnologia da Informação, é possível afirmar que **o profissional a ser nomeado como Encarregado de Dados precisa ter conhecimentos interdisciplinares**.

Além de conhecimentos interdisciplinares, é importante ressaltar um assunto relevante quanto o Encarregado de Dados. Muitas empresas nomeiam um Encarregado de Dados que já é colaborador na empresa, exercendo, além da função anterior, a própria função de Encarregado de Dados. Nesses casos, há uma grande necessidade de se verificar se existirá conflitos de interesses, uma vez que o Encarregado de Dados precisa de autonomia para exercer suas atividades e não pode, por exemplo, sujeitar-se a requerimentos de um superior hierárquico.

A LGPD não determinou em que circunstâncias uma organização deve indicar um encarregado. Assim, deve- se assumir, como regra geral, que toda organização deverá indicar uma pessoa para assumir esse papel.

O artigo 41 da LGPD, aliás, não faz distinção quanto a instituições públicas ou privadas e por isso é importante que ambas estejam cientes da sua obrigação de indicar um encarregado de dados. A esse respeito, o art. 23, III, reforça a necessidade de um encarregado ser indicado por órgãos e entidades públicas.

A LGPD também não distingue se o encarregado deve ser pessoa física ou jurídica, e se deve ser um funcionário da organização ou um agente externo. Considerando as boas práticas internacionais, o encarregado poderá ser tanto um funcionário da instituição quanto um agente externo, de natureza física ou jurídica.

AULA 36 - MODALIDADES DE CONTRATAÇÃO DO ENCARREGADO DE DADOS

O Encarregado de Dados, nos termos da LGPD e, adotando as melhores práticas de mercado, aplicadas pela GDPR, o DPO pode ser um empregado da empresa ou um

terceirizado. Para tanto, existem vantagens e desvantagens que devem ser analisadas quando da escolha do profissional.

Compreendendo-se que o Encarregado de Dados necessita de autonomia, conhecimentos interdisciplinares e, além disso, caso exercesse outra função além da do DPO estaria sobrecarregado, uma maneira interessante de nomear um profissional adequado e que não tenha influências negativas da empresa é com a contratação do Encarregado terceirizado.

Essa modalidade está prevista na LGPD em razão da alteração sofrida com a Lei 13.853/2019, possuindo os seguintes benefícios:

- **Ganho na experiência multidisciplinar:** o DPO *as service* tem a alternativa de contar com equipe multidisciplinar, recebendo apoio das equipes jurídicas, de tecnologia, governança, segurança da informação etc.;
- **Independência:** Como destacado, o Encarregado de Dados necessita de autonomia para exercer suas atividades. Assim, o DPO *as service* possui uma independência maior que o DPO interno, inexistindo envolvimento na determinação de como e de qual forma os dados pessoais serão tratados;
- **Flexibilidade:** Devidamente finalizado o projeto de adequação à LGPD, o acionamento do Encarregado será menor, inexistindo tantas tarefas necessárias para que se contrate um DPO interno. Assim, a atividade é mais bem exercida por um DPO externo, além de se tornar menos onerosa a relação; e
- **Benchmarking:** Como normalmente o DPO terceirizado presta os serviços para diversas empresas, é possível o compartilhamento de boas ideias e práticas entre as empresas.

Além dos pontos fortes, existem alguns pontos fracos que precisam ser evidenciados, como por exemplo o cuidado com a experiência do profissional a ser contratado, sob pena de contratar algum prestador que não possui conhecimento sobre a lei.

Não bastasse, também é importante estabelecer em contrato alguns pontos importantes, como por exemplo a responsabilização do contratado em casos de danos causados ao titular ou sanções sofridas pelas empresas, em razão de alguma ação ou omissão do DPO contratado.

Como é importante em qualquer contrato, também há de se observar as obrigações do DPO *as service*, necessitando estarem devidamente especificadas para evitar qualquer existência de questões ou serviços não realizados pelo profissional contratado.

AULA 37 – A RESPONSABILIDADE DO ENCARREGADO DE DADOS

A Lei Geral de Proteção de Dados não atribui diversas tarefas ao Encarregado de Dados, mas apenas quatro, sendo as seguintes:

> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
>
> II - receber comunicações da autoridade nacional e adotar providências;
>
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
>
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Conforme disposto no tópico acima, é possível confirmar que o Encarregado de Dados tem o objetivo de ser um canal de comunicação entre os agentes, os titulares e a Autoridade Nacional de Proteção de Dados, além de ter uma tarefa de gestão e, eventualmente, de execução que irá depender de normas complementares caso a caso.

INDICAÇÃO E IDENTIFICAÇÃO

Como foi destacado, a principal função do DPO é a realização da intermediação, sendo um canal de comunicação. Mas para isso, como é que os titulares, os agentes e a Autoridade Nacional de Proteção de Dados sabem quem é o Encarregado de Dados?

Então, no art. 41, § 1° da LGPD, existe a seguinte determinação: "§ 1° A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador."

Ou seja, é obrigação do agente de tratamento i**nformar os dados de contato e identificar em seu site** o Encarregado de Dados de forma clara e objetiva. Inclusive, esta é uma forma fácil de identificar se uma empresa está adequada à LGPD. Basta acessar o site, buscar pela Política de Privacidade e verificar a existência da identificação do Encarregado de Dados.

É claro que a Política de Privacidade no site da companhia não significa que a empresa está adequada à LGPD, tendo em vista que a Política de Privacidade é apenas uma mínima parte das ações de adequação, em observância ao princípio da transparência.

MÓDULO 08

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) - SUA IMPORTÂNCIA E FUNCIONAMENTO

AULA 38 – O QUE É A ANPD?

De início, ressalta-se que um dos temas mais controversos durante a criação da Lei Geral de Proteção de Dados foi a instituição da Autoridade Nacional de Proteção de Dados (ANPD).

Essa discussão girou em torno da necessidade ou não da existência de um órgão independente para a fiscalização, regulação e cumprimento da Lei Geral de Proteção de Dados. Isto porque, a criação do órgão envolvia o aumento de gastos e dotação orçamentária, o que contrariava o movimento de redução de despesas adotado durante a crise político-econômica causada pela pandemia do Coronavírus (COVID-19). Por outro lado, sem a instituição de um órgão regulamentador, a nova legislação teria sua eficácia prejudicada, afinal, na ausência de uma fiscalização capaz de garantir que as novas regras estejam sendo seguidas, o processo de adequação da sociedade à norma seria consideravelmente mais lento.

Em que pese toda a discussão envolvendo a criação da Autoridade, os legisladores decidiram constituir a Autoridade Nacional de Proteção de Dados, um órgão independente que faz parte do Poder Executivo do Governo Federal e tem como objetivo proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme estabelecido no Decreto nº 10.474, de 26 de agosto de 2020.

Cumpre ressaltar que a independência dada à instituição se evidencia através de algumas características que lhe foram conferidas, como a autonomia técnica e decisória e o mandato fixo dos Diretores.

AULA 39 – ATIVIDADES ESSENCIAIS DA ANPD – PARTE 1

A Lei Geral de Proteção de Dados prevê, em seu artigo 55-J, tarefas que são de competência da Autoridade Nacional de Proteção de Dados.

Dentre elas, iremos destacar aquelas que consideramos principais, como a competência de **impor padrões técnicos mínimos para o tratamento dos dados pessoais**, estimulando a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis.

Também destacamos a possibilidade de **fiscalizar e aplicar sanções** em caso de tratamento de dados realizado em descumprimento à legislação das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança, mas também as ações de cooperação com autoridades de proteção de dados pessoais de outros países.

É extremamente importante a presença da ANPD para o *enforcement* da própria lei, pois não se trata apenas de um órgão para regulamentar a legislação, mas também com o objetivo de conciliar os interesses de mercado e a proteção dos cidadãos brasileiros, sempre visando a proteção de seus direitos fundamentais.

O órgão também tem o poder de **editar regulamentos e procedimentos**, garantindo que os princípios gerais de proteção de dados pessoais sejam sempre respeitados. Por fim, cumpre à ANPD implementar mecanismos para o registro e o esclarecimento de reclamações sobre o tratamento de dados pessoais em desconformidade com LGPD.

AULA 40 – ATIVIDADES ESSENCIAIS DA ANPD – PARTE 2

Além das atividades mencionadas na aula 30, cumpre destacar outros papéis altamente importantes da ANPD, quais sejam a sua atribuição de **apreciar as petições de titular contra controlador "após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação"**

Além disso, podemos evidenciar algumas outras competências da ANPD, quais sejam: (i) de promoção na população do conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; e (ii) de promoção a elaboração estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade.

A ANPD possui ainda, competência de implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a LGPD.

Esses papéis possuem alta relevância, já que, através da leitura dos incisos do artigo 55 J da lei LGPD, podemos notar a preocupação do legislador em proteger a parte mais vulnerável no tratamento de dados, qual seja, o próprio cidadão, titular das informações envolvidas no tratamento de dados.

Além disso, vemos uma clara intenção em exigir transparência por parte dos agentes quanto ao tratamento, de forma a proporcionar o compartilhamento mais seguro de informações, sobretudo no ambiente digital. Confira lista geral com todas as atividades essenciais da ANPD:

- Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
- Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;

- Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;
- Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;
- Editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD;
- Ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;
- Editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se à Lei;
- Deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação da LGPD, as suas competências e os casos omissos;
- Articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e
- Implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a LGPD.

Por fim, cumpre destacar que as competências do Conselho Diretor, do Diretor-Presidente e dos Diretores estão no Decreto n° 10.474, de 26 de agosto de 2020, que aprovou a estrutura regimental da ANPD. Todos esses também possuem importantes atribuições, como por exemplo, a prevista no art. 4° de solicitar ao controlador o relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, obser0076ados os segredos comercial e industrial.

AULA 41 - ENTIDADES FISCALIZADORAS DE PROTEÇÃO DE DADOS NO ÂMBITO INTERNACIONAL

É inegável a influência do Regulamento Europeu de Proteção de Dados Pessoais/ RGPD sobre a Lei Geral brasileira de Proteção de Dados/LGPD, por essa razão, uma análise será realizada sobre as *Data Protection Authorities*, ("DPA") ou Autoridade de Proteção de Dados, em português.

Por ser uma norma aplicável em diversos países europeus, a GDPR delegou a cada país integrante da União Europeia a responsabilidade por selecionar o conselho que formará

autoridade reguladora e indicar os poderes garantidos à mesma, ou seja, as responsabilidades específicas de cada DPA. Dessa forma, as leis de cada DPA dependem das leis nacionais de cada país-membro.

No entanto, algumas regras são consolidadas entre todos os países membros como, por exemplo, o direito de aplicação de multas e o valor dessas.

Para as violações severas, violações essas listadas no art. 83 – 5, a multa possui seu valor máximo de 20 milhões de euros. Para as empresas, essa mesma multa pode chegar até 4% do faturamento total global do ano fiscal anterior, o que tiver maior valor. Já para as violações menos severas, listadas nos arts. 83-4, a multa pode chegar a 10 milhões de euros ou 2% do faturamento nos mesmos termos anteriores.

Visando uma aplicação uniforme da GDPR, foi criado o *European Data Protection Board* ("EDPB"), Conselho Europeu para a Proteção de Dados em português. O EDPB é um organismo independente cujo objetivo é promover a cooperação e o intercâmbio eficaz de informações entre as DPAs de cada país-membro.

O EDPB é composto por representantes das DPAs e pelo *European Data Protection* Supervisor ("EDPS"), Autoridade Europeia para a Proteção de Dados em português. Uma de suas principais funções é emitir diretrizes sobre a interpretação dos conceitos centrais da GDPR e regularizar através de decisões vinculativas as disputas relacionadas ao processamento transfronteiriço, garantindo uma aplicação uniforme das regras na UE para evitar que o mesmo caso possa ser tratado diferentemente em várias jurisdições.

Dessa forma, percebe-se que o modelo europeu de proteção de dados delegou à autoridade de controle grande parte da competência legislativa para determinar sobre questões específicas e técnicas, tendo também os poderes de fiscalizar, sancionar e atuar na esfera administrativa, buscando resolver possíveis conflitos entre as partes, e evitando a judicialização das questões. Chamado de modelo-eclético, o regulamento da UE combina normas estatais com soluções tecnológicas e até mesmo com um interessante meio de engajamento ativo, ao classificar as empresas por meio de selos que indicam o grau de zelo com os dados de seus usuários.

MÓDULO 09

TIPOS DE SANÇÕES E PARÂMETROS DE APLICAÇÃO DE PENALIDADES ENVOLVENDO LGPD COM ESTUDO DE CASO

AULA 42 – TIPOS DE SANÇÕES APLICADAS PELA ANPD PARTE 1

Conforme demonstrado no módulo 1 do presente curso, a LGPD passou por algumas situações diferentes do comum, como a entrada em vigor de parte da lei em 2020 e, apenas em agosto de 2021, a entrada em vigor integral com os artigos referentes às sanções administrativas.

Estas sanções que entraram em vigor apenas no corrente ano, são aplicadas, caso o agente de tratamento de dados viole as normas previstas na LGPD, são aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República.

A ANPD é a única entidade que tem autonomia para tratar do assunto. Além de poderes para aplicação das sanções administrativas, conforme o art. 55-J da lei, possui competência para fiscalizar, editar normas, editar regulamentos e procedimentos, promover estudos sobre a matéria, e entre outras competências.

TIPOS DE SANÇÕES

De acordo com a lei, são 9 (nove) sanções que podem ser imputadas aos agentes de tratamento que violarem a legislação, sendo as seguintes, conforme art. 52 da LGPD:

> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III - multa diária, observado o limite total a que se refere o inciso II;
>
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI - eliminação dos dados pessoais a que se refere a infração;
>
> VII - (VETADO);
>
> VIII - (VETADO);
>
> IX - (VETADO).
>
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019).
>
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)

> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019).

Importante destacar que essas são as únicas sanções passíveis de aplicação pela ANPD, uma vez que a lei possui este rol taxativo (limitado e sem a possibilidade de uma interpretação extensiva sobre o assunto).

Com a análise das sanções constantes da lei, podemos concluir que foram, basicamente, separadas para aplicações em violações leves, médias e graves. Trataremos, de forma breve, sobre cada uma.

A **advertência** é, nitidamente, a penalidade para violações leves, uma vez que a empresa apenas será advertida e deverá, caso determinado pela ANPD, adotar as medidas necessárias para minimizar ou estancar os efeitos da violação cometida.

As **multas simples**, para casos que nos parecem de uma gravidade um pouco mais acentuada, são imputadas com base no valor de faturamento do ano anterior da instituição, limitada à 2% do faturamento, não podendo ultrapassar o valor de R$ 50.000.000,00 (cinquenta milhões de reais).

Pensando-se em sanções administrativas da LGPD, é nítido que a sanção acima destacada é a que mais causa medo no mercado. É totalmente compreensível o motivo pelo qual a mencionada sanção causa alvoroços no mundo dos negócios, eis que o faturamento será implicado e, consequentemente, menos lucro.

Entretanto, todas as sanções são delicadas e merecem a devida atenção., principalmente a sanção que *proíbe parcialmente ou totalmente o exercício de atividades relacionadas a tratamento de dados,* conforme será aplicado ainda neste tópico.

Também de forma pecuniária são as **multas diárias**. Estas multas, com o mesmo limite da multa simples, tem a função de imputar ao ente que violou a legislação a obrigação de cessar a atividade ilegal. Caso a atividade não cesse e continue lesando titulares ou demais princípios da legislação, a multa permanecerá em vigor.

AULA 43 - TIPOS DE SANÇÕES APLICADAS PELA ANPD PARTE 2

Outra sanção da legislação é a **publicização** da infração. De imediato, tal punição não parece tão ofensiva quanto as multas pecuniárias. Entretanto, as consequências negativas na reputação dos entes que praticaram a violação à legislação podem ser irreversíveis. Cometer um erro, principalmente com relação à privacidade de pessoas, pode ser fatal à uma empresa.

Ainda com relação à publicização, é importante mencionar que a Autoridade Nacional de Proteção de Dados ainda necessita regulamentar como essa publicização ocorrerá, para que não extrapole e prejudique o agente de tratamento que cometera o equívoco.

Duas outras sanções são o **bloqueio** e a **eliminação** dos dados pessoais referentes à infração cometida. Com relação à primeira, a intenção é que o ente não possa continuar exercendo a atividade com os dados pessoais em posse até que realize a adequação necessidade. Já com relação à eliminação, a ideia é realmente eliminar o dado em razão de não ser mais possível realizar alguma correção na violação que ocorreu.

A lei também traz a sanção de **suspensão parcial do funcionamento do banco de dados.** Esta sanção é praticamente a mesma que o bloqueio, porém, é um pouco mais gravosa em razão da suspensão de um banco de dados por inteiro pelo período máximo de 6 (seis) meses que, ainda, poderá ser renovado.

Por fim, a última sanção e mais gravosa, a princípio, é **a proibição do exercício das atividades relacionadas ao tratamento de dados**. Diz-se mais gravosa porque é possível que a sanção impossibilite as atividades empresariais do agente de tratamento que violou a legislação, causando, inclusive, mais prejuízos do que as sanções pecuniárias.

Cumpre destacar, que, de acordo com o *caput* do artigo 52 da LGPD, as sanções administrativas previstas pela LGPD são passíveis de aplicação somente pela ANPD. Nenhum outro órgão público pode aplicar essas sanções.

Além disso, a Lei estabelece que as competências da ANPD prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.

Vale lembrar, entretanto, que, nos termos da Lei, a aplicação das sanções previstas na LGPD não substitui a aplicação de sanções administrativas, civis ou penais definidas no Código de Defesa do Consumidor e em legislação específica. Assim, eventual atuação de outros órgãos públicos, como agências reguladoras ou órgãos de defesa do consumidor, deve se dar segundo as suas próprias competências, ao abrigo de suas legislações específicas.

Para que fique mais claro as sanções aplicadas pela LGPD, vejamos o exemplo a seguir:

Mais uma vez, utilizaremos o exemplo das empresas de *cloud*. Imagine que a empresa A oferece os serviços de armazenamento em nuvem. Porém, por uma grande violação às normas de proteção de dados, a Autoridade Nacional de Proteção de Dados imputou a mencionada sanção de *proibição do exercício das atividades relacionadas ao tratamento de dados*.

Como a empresa A sobreviveria, sendo que a sua atividade principal envolve totalmente o tratamento de dados pessoais?

Consoante será demonstrado no seguinte tópico, existem parâmetros para aplicação das sanções. Assim, neste exemplo, é claro que diversos pontos devem ser observados para que seja aplicada uma sanção adequada e razoável. Porém, faz sentido esta sanção assustar mais do que a multa pecuniária, não?

Finalizando o tópico, é de extrema importância destacar que nenhuma dessas sanções poderá ser aplicada sem a regulamentação de um Processo Administrativo pela

Autoridade Nacional de Proteção de Dados, sob pena de violação dos princípios constitucionais do devido processo legal, do contraditório e da ampla defesa.

AULA 44 – OS PARÂMETROS DE APLICAÇÃO DE SANÇÕES PELA ANPD

Entendendo quais são as sanções possíveis de serem aplicadas pela Autoridade Nacional de Proteção de Dados aos agentes de tratamento que violarem a lei, agora chegou o momento de entendermos os parâmetros para a aplicação das sanções.

Observando-se o texto da LGPD, é possível compreender que para cada violação ocorrida, deverá ser analisado, após procedimento administrativo que possibilidade a garantia do direito de defesa do agente violador, *cada caso concreto* e alguns *parâmetros*.

Igualmente na justiça comum, algumas decisões da ANPD serão levadas como base para nortear as seguintes decisões. Então, o mercado e os estudiosos da área de proteção de dados estão ansiosos para entender como a ANPD irá regulamentar os processos administrativos e como será o seu comportamento nos primeiros julgamentos.

De acordo com a lei, os parâmetros a serem considerados são os seguintes:

> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
>
> II - a boa-fé do infrator;
>
> III - a vantagem auferida ou pretendida pelo infrator;
>
> IV - a condição econômica do infrator;
>
> V - a reincidência;
>
> VI - o grau do dano;
>
> VII - a cooperação do infrator;
>
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
>
> IX - a adoção de política de boas práticas e governança;
>
> X - a pronta adoção de medidas corretivas; e
>
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Assim, existindo alguma violação, o agente de tratamento será devidamente julgado administrativamente. Entretanto, para que seja julgado corretamente e observando o caso concreto, a Autoridade Nacional de Proteção de Dados deverá observar todos os 11 (onze) parâmetros para determinar qual sanção será imposta.

Os parâmetros são lógicos e norteiam a ANPD durante o julgamento. A título de exemplo, levemos em consideração uma empresa que nunca havia cometido qualquer violação com relação à proteção de dados, possui programas internos de governança corporativa voltada à proteção de dados e, logo após saber da violação cometida, tomou todas as medidas necessárias para tentar conter os danos causados pela violação.

Faria algum sentido a ANPD multar o agente de tratamento com a proibição do tratamento de dados relativos à atividade (mais gravosa sanção) neste caso hipotético? Não nos parece razoável, tendo em vista os parâmetros acima destacados.

Desta forma, sempre tentando minimizar os danos causados pela violação e prezando pela justiça, **a ANPD necessita observar todos os parâmetros destacados** e, após essa análise, estará pronta para decidir sobre qual multa será imposta ao agente violador.

AULA 45 – REFLEXOS JUDICIAIS DO DESCUMPRIMENTO DA LGPD

A LGPD é uma lei que possui como um de seus principais objetivos a proteção de direitos individuais fundamentais e, ao mesmo tempo, incentiva as atividades empresariais de tecnologia e inovação, provendo regras transparentes e abrangentes para o tratamento adequado de Dados Pessoais, criando um enquadramento jurídico para o tratamento em meios físicos e digitais de Dados Pessoais no Brasil.

Conforme explicado na aula anterior, a LGPD prevê uma série de penalidades para o seu descumprimento, no entanto, percebe-se um movimento de judicialização envolvendo os casos relacionados à LGPD.

Um estudo divulgado pela *Juit*, empresa especializada pela realização de varredura de decisões judiciais, percebeu a existência de cerca de 600 ações envolvendo o uso de dados pessoais dos titulares pelas empresas até junho do presente ano.

A Pesquisa identificou que 74% das sentenças são de primeiro grau e estão restritas a São Paulo. Foram observadas, algumas tendências como a preferência na base legal do conceito de consentimento, onde a autorização expressa do cidadão é necessária para que seus dados possam ser usados.

Independentemente da possibilidade de aplicação de severas sanções administrativas previstas na LGPD, partimos para um cenário em que alguns setores, principalmente aqueles que possuem uma base de dados significante de consumidores, podem sofrer com uma judicialização dos direitos previstos na LGPD.

Embora não se possa descuidar da importância da proteção dos dados pessoais, reconhecida como direito fundamental já contemplado em nossa Constituição Federal pelo Supremo Tribunal Federal, no julgamento da Ação Direta de Inconstitucionalidade (ADI) nº 6.387, a judicialização em massa de demandas

envolvendo a proteção de dados pessoais pode sobrecarregar ainda mais o Poder Judiciário.

AULA 46 – CASOS JUDICIAIS ENVOLVENDO A LGPD

COMENTÁRIOS INICIAIS

Muito se fala sobre a sobrecarga de ações judiciais no Poder Judiciário no Brasil. Há um estudo de 2019 que afirma que os gastos com o Poder Judiciário brasileiro são equivalentes a 2% do PIB (Produto Interno Bruto), enquanto, em outros países da OCDE, as despesas com o Poder Judiciário equivalem apenas a 0,5% do PIB nacional.

Embora a proposição de ações judiciais muitas vezes se faça necessária, sobretudo quando outros métodos de resolução de controvérsias não se mostram eficazes, ainda persiste a cultura da judicialização no Brasil.

Nesse sentido, considerando a recente publicação da LGPD, existe uma tendência de que, considerando a cultura da judicialização, muitos titulares proponham ações contra empresas que tratam seus dados pessoais de forma inadequada, um dos motivos pelos quais se mostra tão importante a implementação de um projeto de adequação à LGPD, como já vimos anteriormente.

Até o setembro de 2021, de acordo com a empresa denominada JUIT, empresa que realiza pesquisas para *jurimetria*, "a cidade de São Paulo lidera o ranking de decisões envolvendo LGPD (com 325 decisões), seguida de Osasco (177) e São José dos Campos (47). Cerca de 1 em cada 8 decisões reconheceu vazamento de dados. Quanto a base legal, 36,4% dos julgados citam os dados com acesso público (Art. 7°, § 3°) como principal motivador do mérito. Em segundo lugar fica o Consentimento do Art 7°, I e no terceiro está o exercício regular do direito do Art. 7°, VI."

Dessa forma, já se tem o conhecimento, inclusive, das motivações a respeito das ações ingressadas no Poder Judiciário. Ainda assim, é importante que sejam acompanhados esses processos, a fim de dar atenção às demandas mais recorrentes, inclusive como base para o projeto de adequação.

Vale destacar que não é possível afirmar que todas as ações que serão propostas terão êxito, obtendo, por exemplo, o pagamento de danos morais. Conforme será demonstrado em um dos casos abaixo, para que se condene a empresa ao pagamento de danos morais em razão de violação aos direitos do titular, há de ser comprovado, por meios de prova de direito, que houve dano.

Por fim, inexiste a necessidade de anonimizar os nomes das empresas mencionadas abaixo porque: i) não se trata de dados pessoais visto que são pessoas jurídicas; ii) os casos descritos são públicos, não havendo informações sigilosas.

CASO CONSTRUTORA CYRELA

No Brasil, acredita-se que o caso da Construtora Cyrela foi o percursor na mídia, em relação à LGPD. O caso em questão tem uma grande relação com o Direito do Consumidor, tendo em vista que envolve a compra e venda de um imóvel entre a construtora Cyrela e uma pessoa física.

De acordo com o que consta no processo judicial, o cliente discorre que, após a compra de um imóvel da Cyrela em São Paulo, ele passou a receber diversas mensagens e ligações de serviços ligados ao mercado imobiliário, como financiamentos, reformas e decoração. Discorre, ainda, que nas tentativas de contato, havia a menção do nome do local em que o imóvel foi adquirido.

No juízo de primeira instância, o autor teve êxito na ação, pois a juíza responsável pelo caso entendeu que havia existido a violação à proteção da privacidade do cliente (autor), condenando a Cyrela a pagar indenização por danos morais no valor de R$ 10.000,00 (dez mil reais).

A Cyrela, insatisfeita com a decisão, decidiu recorrer e teve sucesso. O Tribunal de Justiça do Estado de São Paulo reformou a sentença, fundamentando que não existiam provas suficientes de que as informações passadas aos prestadores de serviço que fizeram as abordagens haviam sido realizadas pela Cyrela.

Além da falta de provas, o Tribunal fundamentou que "o simples encaminhamento de mensagens genéricas por e-mail ou WhatsApp não é conduta suscetível de causar dano moral" e é apenas um "mero aborrecimento".

Conforme destacado nos comentários no tópico anterior, este é um entendimento comum nas decisões relativas aos direitos dos consumidores, tendo em vista que não se observa qualquer dano moral, apenas um aborrecimento decorrente das condutas da empresa fornecedora.

Ressalta-se que é essa interpretação é perigosa e abre-se precedentes para que diversas empresas que não observam os direitos dos titulares de dados pessoais possam continuar as práticas de compartilhamento de dados sem nenhuma transparência para com o titular de dados que, neste caso, era o cliente.

É importante ressaltar alguns dos argumentos da Cyrela em defesa, como por exemplo a informação de que a incorporadora efetuou criação de um **comitê interno de privacidade**, contratou especialistas voltados exclusivamente para a gestão da proteção dos dados e treinamentos de funcionários.

Observando-se os argumentos levantados pela Cyrela, pode-se confirmar que todas as lições mencionadas neste curso com relação à adequação podem auxiliar a empresa em momentos de processos administrativos e judiciais, tendo em vista que conseguem comprovar que a empresa age preventivamente, não existindo descaso com relação ao tratamento de dados pessoais.

CASO COOPERATIVA ECOCITRUS

Diferentemente do caso anterior que tramitava na vara comum, o caso da Cooperativa Ecocitrus tramitou na Justiça do Trabalho e, mesmo assim, totalmente relacionado à proteção de dados pessoais, mais precisamente, dos dados pessoais dos trabalhadores da mencionada cooperativa.

O caso aconteceu no Rio Grande do Sul, sendo a cooperativa Ecocitrus condenada, em primeira instância, a realizar a adequação à Lei Geral de Proteção de Dados, no prazo de 90 dias, sob pena de multa diária de R$ 1.000,00 (mil reais). Além da mencionada ação, são outras 12 ações civis públicas ajuizadas pelo Sindicato dos Trabalhadores nas Indústrias da alimentação de Montenegro e Região, sendo esta a primeira decisão favorável aos trabalhadores.

Neste processo judicial, existe a reclamação do sindicato de que há o descumprimento sistemático na proteção de dados e o compartilhamento de informações pela cooperativa, inexistindo qualquer cautela necessária consoante dispõe a legislação. Não bastasse, o sindicato alega que os dados são compartilhados na internet, não existindo qualquer observância aos princípios da intimidade e privacidade.

Ao julgar a ação, a juíza destacou que os trabalhadores têm direitos assegurados na LGPD para que seus dados sejam protegidos. Ainda segundo a magistrada, não há comprovação pela cooperativa que existe a adequação à legislação, afirmando que a cooperativa "demonstrou por nenhum meio a implementação de um único dispositivo LGPD".

Considerando a inexistência de qualquer ação referente à Lei Geral de Proteção de Dados, a juíza determinou que a Ecocitrus realize a adequação à LGPD, preservando os preceitos da lei, além determinar a indicação de um Encarregado de Dados. Conforme ensinado no curso, a indicação do Encarregado de Dados é uma das diversas obrigações dos agentes de tratamento.

Embora existam pontos em aberto na legislação que ainda serão regulados pela Autoridade Nacional de Proteção de Dados, é interessante vislumbrar uma preocupação do Poder Judiciário com relação à matéria, não beneficiando as empresas que tiveram desde a promulgação da empresa em 2018 para, no mínimo, entender o que era necessário realizar para estar de acordo com a lei.

O único ponto a ser ressaltado é com relação à jurisprudência, porque não se pretende consolidar decisões no mesmo sentido inexistindo o posicionamento da Autoridade Nacional de Proteção de Dados, tendo em vista que não cabe ao judiciário, através de leis, legislar sobre o tema.

CASO MERCADO LIVRE

Caso interessante e que envolve, além da proteção de dados pessoais, a aplicação de direito digital nos marketplaces. Todo mundo sabe que o mercado livre é um marketplace que autoriza que outras empresas façam a publicação de anúncios de produtos para vender e, em contrapartida, o Mercado Livre retira a sua taxa.

De acordo com a própria empresa, eles se definem assim:

> "Somos uma empresa de tecnologia que tem como objetivo democratizar o comércio eletrônico oferecendo a melhor plataforma e os serviços necessários para que pessoas e empresas possam comprar, pagar, vender, enviar, anunciar e gerir seus negócios na Internet"

Como existe a disponibilização de um espaço, de forma democrática para que empresas façam as vendas, é possível que outras empresas que atuem de forma irregular propaguem seus anúncios.

Foi o que ocorreu em um processo judicial em Brasília, sendo determinado ao Mercado Livre a suspensão do anúncio referente a venda de banco de dados e cadastro em geral. Além da determinação ao Mercado Livre que, não era o autor da infração à Lei Geral de Proteção de Dados, foi determinando à empresa Sidnei Sassi a abstenção de disponibilização de dados pessoais, de forma gratuita ou onerosa, digital ou física, no *market place*, sob pena de pagamento de multa de R$ 2.000,00 por cada descumprimento.

Quem foi o autor da ação foi o Ministério Público do Distrito Federal. O MP afirmou que que foi identificada a comercialização de dados pessoais de brasileiros por meio do site Mercado Livre, onde o anunciante faz a oferta banco de dados e cadastros, com o principal comprador sendo uma empresa do Rio Grande do Sul, também violadora da LGPD.

Não é necessário ter profundo conhecimento na LGPD para ter ciência de que esta prática errada. De acordo com os ensinamentos do curso, podemos compreender que existem diversas violações na prática realizada pela empresa anunciante, como por exemplo a violação dos princípios da finalidade e transparência. O titular de dados pessoais não tinha ciência dessa finalidade, nem ao menos tinha ciência de que seu dado estava em posse da empresa, não existindo qualquer transparência pela empresa anunciante.

É interessante ressaltar que neste caso o Mercado Livre nem sequer é agente de tratamento, tendo em vista que a base de dados comercializada não é disponibilizada no site. Assim, o Mercado Livre é apenas agente de tratamento com relação aos dados dos usuários, inexistindo o tratamento de dados da base de dados vendida ilegalmente.

CASO CONCESSIONÁRIA DE METRÔ EM SÃO PAULO

Um caso interessante em que a sentença foi proferida em maio de 2021 é a ação judicial do IDEC - Instituto Brasileiro de Defesa do Consumidor e da Defensoria Pública movida em face da concessionária da linha 4 do metrô de São Paulo (Via Quatro). Os pedidos da ação foram com relação à proibição da coleta e tratamento de imagens e dados biométricos, sem prévio consentimento, dos usuários da linha de metrô operada pela empresa.

A ação foi movida em 2018, já com o pedido liminar para que a Via Quatro parasse a coleta dos mencionados dados, solicitando-se, ainda, a comprovação de que o desligamento das câmeras instaladas, sob pena de multa diária.

Como pedido final da ação, a defensoria e o IDEC requereram a condenação da concessionária a não utilizar dados ou qualquer outro tipo de identificação dos consumidores/usuários do transporte público, além de requerer o pagamento de indenização pela utilização indevida da imagem dos consumidores em valor não inferior a R$ 100 milhões.

A concessionária apresentou defesa alegando que o tratamento de dados realizado era legal, tendo em vista que não existia a coleta ou o armazenamento dos dados pessoais no sistema. A operação realizada somente detectava facialmente os usuários para fins estatísticos, não sendo possível a identificação do usuário (lembre-se, dado pessoal é toda informação relacionada a pessoa natural identificada ou identificável).

Após a apresentação de defesa, a liminar solicitada pela defensoria e pelo IDEC foi deferida, ainda em 2018, obrigando a Via Quatro a cessar a captação de imagens, sons e quaisquer outros dados através de câmeras ou outros dispositivos envolvendo as portas digitais, além de determinar o desligamento dos dispositivos.

A juíza compreendeu os motivos levantados pela Via Quatro com relação a inexistência de armazenamento e coleta das imagens dos usuários. Por outro lado, a magistrada informou que tais situações não foram comprovadas no processo, sendo inviável considerar as alegações feitas pela concessionária.

Vejamos a motivação da juíza:

> "ainda que se constatasse concretamente a ausência de efetivo reconhecimento facial pelo equipamento instalado, não há dúvidas de que há captação da imagem de usuários, sem o seu conhecimento ou consentimento para fins comerciais que beneficiam a ré e a empresa por ela contratada".

Mesmo inexistindo a identificação do usuário do metrô, existe o tratamento de dados sensíveis, uma vez que a biometria facial, de acordo com a Lei Geral de Proteção de Dados, é um dado sensível.

A lei dá um tratamento diferenciado aos dados sensíveis exatamente pelo motivo de possuir uma criticidade maior em caso de violação. Neste passo, para que seja realizado

o tratamento de dados possíveis, é, no mínimo, necessário ser transparente com o titular de dados que, neste caso, é o usuário do metrô.

Além da biometria, dados sensíveis também podem ser dados de saúde. Imagine uma empresa realizando o tratamento de dados de saúde, como por exemplo, verificando quem tem tuberculose, mas não realizam a coleta e o armazenamento, uma vez que fazem apenas a leitura de formulários preenchidos pelos titulares para outra finalidade. Da mesma forma que a biometria, são dados sensíveis e que merecem no mínimo transparência com relação à finalidade do tratamento.

A juíza ainda ressaltou o seguinte

> "Restou incontroverso que os usuários não foram advertidos ou comunicados previa ou posteriormente acerca da utilização ou captação de sua imagem pelos totens instalados nas plataformas, ou seja, os usuários nem mesmo tem conhecimento da prática realizada pela requerida, o que viola patentemente o seu direito à informação clara e adequada sobre os produtos e serviços, bem como à proteção contra a publicidade enganosa e abusiva (...)."

Ponto importante levantado pela magistrada foi com relação à conduta da concessionária. Aduz a juíza que a conduta da concessionária é reprovável em razão da capacidade de atingir a moral e os valores coletivos. Não é possível mensurar quantos usuários tiveram seus direitos violados, além, inclusive, de crianças e adolescentes que também possuem tratamento diferenciado pela lei.

Com relação ao pedido de pagamento de indenização por danos morais coletivos no valor de 100 milhões de reais, a magistrada entendeu que era excessivo, ainda mais em razão da ausência de demonstração de que as imagens capturadas tenham sido compartilhadas e armazenadas de forma inadequada, ou até mesmo, compartilhada em meios de comunicação de forma equivocada.

Mesmo a juíza entendendo exorbitante o valor de 100 milhões de reais, entendeu razoável a condenação da concessionária ao pagamento de indenização por danos morais no valor de 100 mil reais, ou seja, 0,1% do pretendido.

Esta decisão é recente e ainda não transitou em julgado (não houve uma decisão definitiva), de forma que o Tribunal de Justiça do Estado de São Paulo poderá reformar a decisão de primeira instância.

Em que pese não estar finalizada, é uma decisão interessante de ser analisada, ainda mais pelo fato de que envolve a utilização de dados biométricos de usuários do metrô sem qualquer informação para tanto.

A lição que fica com relação à esta decisão é que os titulares de dados pessoais merecem, no mínimo, a informação de que seus dados serão tratados, ainda mais quando se trata de dados sensíveis. Durante todo o curso foi demonstrado que a violação à proteção de dados acaba gerando a violação dos direitos fundamentais. O que se pretende com o estudo de proteção de dados é garantir os direitos fundamentais,

de forma que resta impossível às empresas tomarem decisões arbitrárias com relação aos nossos dados, sem ao menos, nos dar a prévia comunicação.

AULA DE REVISÃO 03

Revisaremos o conteúdo visto nos módulos 07, 08 e 09.

AULA 47 - REVISÃO MÓDULO 07 - O ENCARREGADO DE DADOS E SUAS RESPONSABILIDADES.

REVISÃO AULA 34 – O ENCARREGADO DE DADOS NA LGPD.

- Art. 5°, VII, LGPD, o Encarregado é a 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);
- O encarregado centraliza a discussão sobre a conformidade à nova lei e coordena a implementação de melhorias, bem como acompanha a evolução do tema junto da instituição, do mercado e da sociedade, tendo uma atuação relevante na fase de adaptação;
- A LGPD não determinou em que circunstâncias uma organização deve indicar um encarregado, mas o tornou obrigatório para órgãos, entes e instituições públicas;
- De acordo com o § 3o do art. 41, normativas futuras da ANPD poderão trazer hipóteses de dispensa da necessidade de indicação do encarregado;

REVISÃO AULA 35 - O PERFIL E INDICAÇÃO DO ENCARREGADO DE DADOS.

- Não há qualquer pré-requisito legal para ser um Encarregado;
- Pelas boas práticas internacionais, o profissional a ser nomeado como Encarregado de Dados precisa ter conhecimentos interdisciplinares;
- Considerando as boas práticas internacionais, o encarregado poderá ser tanto um funcionário da instituição quanto um agente externo, de natureza física ou jurídica.

REVISÃO AULA 36 – MODALIDADES DE CONTRATAÇÃO DO ENCARREGADO DE DADOS

- O DPO pode ser um empregado da empresa ou um terceirizado;
- O DPO que é colaborador da empresa pode ser sobrecarregado com o trabalho, e não seria dotado de autonomia e conhecimentos interdisciplinares necessários para a função;
- A prática internacional é o *DPO as servisse,* havendo inúmeros benefícios nesta escolha, como:
    - Ganho na experiência multidisciplinar;
    - Independência;
    - Flexibilidade;
    - Benchmarking.
    - A lei não traz normas de responsabilização do Encarregado, por isso, quando de sua contratação, recomenda-se inseri-las no contrato;

REVISÃO AULA 37 - A RESPONSABILIDADE DO ENCARREGADO DE DADOS

- A lei atribui quatro tarefas ao encarregado, sendo:
- aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- receber comunicações da autoridade nacional e adotar providências;
- orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
- É obrigação do agente de tratamento informar os dados de contato e identificar em seu site o Encarregado de Dados de forma clara e objetiva;

AULA 48 - REVISÃO MÓDULO 08 - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) - SUA IMPORTÂNCIA E FUNCIONAMENTO.

REVISÃO AULA 38 – O QUE É A ANPD?

- ANPD é a sigla para Autoridade Nacional de Proteção de Dados;
- É um órgão independente que faz parte do Poder Executivo do Governo Federal;
- Tem como objetivo proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural;
- Possui características específicas, como a autonomia técnica e decisória e o mandato fixo dos Diretores.

REVISÃO AULA 39 – ATIVIDADES ESSENCIAIS DA ANPD - PARTE 1

- A Lei Geral de Proteção de Dados prevê, em seu artigo 55-J, tarefas que são de competência da Autoridade Nacional de Proteção de Dados, sendo as principais:
- Impor padrões técnicos mínimos para o tratamento dos dados pessoais;
- Fiscalizar e aplicar sanções;
- Editar regulamentos e procedimentos

REVISÃO AULA 40 - ATIVIDADES ESSENCIAIS DA ANPD - PARTE 2

- Algumas tarefas de competência da ANPD são:
  - Apreciar as petições de titular contra controlador após a comprovação pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;
  - Promoção na população do conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
  - Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
  - Editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade;
  - Deliberar, na esfera administrativa, sobre a interpretação da LGPD;
  - Implementar mecanismos simplificados para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a LGPD.

REVISÃO AULA 41– ENTIDADES FISCALIZADORAS DE PROTEÇÃO DE DADOS NO ÂMBITO INTERNACIONAL

- A GDPR delegou a cada país integrante da União Europeia a responsabilidade por selecionar o conselho que formará autoridade reguladora e indicar os poderes garantidos à mesma, ou seja, as responsabilidades específicas de cada DPA (*Data Protection Authorities);*
- Para aplicação uniforme da GDPR, foi criado o *European Data Protection Board* ("EDPB"). O EDPB é um organismo independente cujo objetivo é promover a cooperação e o intercâmbio eficaz de informações entre as DPAs de cada país-membro;
- A missão do EDPB é emitir diretrizes sobre a interpretação dos conceitos centrais da GDPR e regularizar através de decisões vinculativas as disputas relacionadas ao processamento transfronteiriço.

AULA 49 – REVISÃO MÓDULO 09 - TIPOS DE SANÇÕES E PARÂMETROS DE APLICAÇÃO DE PENALIDADES ENVOLVENDO LGPD COM ESTUDO DE CASO.

REVISÃO AULA 42 – TIPOS DE SANÇÕES APLICADAS PELA ANPD - PARTE 1

- A ANPD é a única entidade que tem autonomia para tratar do assunto de sanções;
- De acordo com a lei, há um rol taxativo de nove tipos de sanções, a saber:
  - advertência com indicação de prazo para adoção de medidas corretivas; multa simples de até dois por cento do faturamento da pessoa jurídica de direito privado, limitado a cinquenta milhões de reais; Multa diária; Publicização da infração; Bloqueio dos dados pessoais até regularização; Eliminação dos dados; suspensão parcial do funcionamento do banco de dados, por até seis meses prorrogáveis; Suspensão do exercício da atividade de tratamento dos dados pessoais; Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.
  - A advertência é para infrações leves;
- Multas simples são para infrações com gravidade um pouco mais acentuada.
- As multas diárias têm a função de imputar ao ente que violou a legislação a obrigação de cessar a atividade ilegal.

REVISÃO AULA 43 - TIPOS DE SANÇÕES APLICADAS PELA ANPD - PARTE 2

- A publicização da infração visa abalar a reputação da instituição que praticou a violação à legislação;
- Bloqueio tem intenção de cessar a atividade até a correção da violação;
- Eliminação do dado ocorrerá quando não é mais possível realizar alguma correção na violação;
- Suspensão parcial do funcionamento do banco de dados é uma punição mais agressiva que o bloqueio pela temporalidade;
- A proibição do exercício das atividades relacionadas ao tratamento de dados pode causar mais prejuízos que as sanções pecuniárias;
- As sanções previstas na LGPD não substituem a aplicação de sanções administrativas, civis ou penais definidas;

REVISÃO AULA 44 – OS PARÂMETROS DE APLICAÇÃO DE SANÇÕES PELA ANPD

- Para aplicação de sanções, a ANPD necessita observar todos os parâmetros destacados em lei e, após essa análise, estará pronta para decidir sobre qual multa será imposta ao agente violador;
- Para aplicação de sanções sempre será respeitado o devido processo legal, contraditório e ampla defesa;
- Os parâmetros são:
  - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
  - a boa-fé do infrator;
  - a vantagem auferida ou pretendida pelo infrator;
  - a condição econômica do infrator;
  - a reincidência;
  - o grau do dano;
  - a cooperação do infrator;
  - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano;
  - a adoção de política de boas práticas e governança;
  - a pronta adoção de medidas corretivas;
  - proporcionalidade entre a gravidade da falta e a intensidade da sanção.

REVISÃO AULA 45 – REFLEXOS JUDICIAIS DO DESCUMPRIMENTO DA LGPD

- Em conclusão a um estudo por empresa especializada em jurimetria (JUIT), há cerca de 600 processos judiciais que envolvam o uso de dados pessoais dos titulares pelas empresas;
- A Pesquisa identificou que 74% das sentenças são de primeiro grau e estão restritas a São Paulo;
- O STF, no julgamento da Ação Direta de Inconstitucionalidade (ADI) nº 6.387, reconheceu a proteção de Dados Pessoais como um direito fundamental.

REVISÃO AULA 46 – CASOS JUDICIAIS ENVOLVENDO LGPD

- Caso Construtora Cyrela: ação judicial que entre a construtora e um cliente pessoa física.

- O cliente discorre que, após a compra de um imóvel da Cyrela, passou a receber diversas mensagens e ligações de serviços ligados ao mercado imobiliário, como financiamentos, reformas e decoração.
- Em que pese o juiz de piso ter condenado a Cyrela ao pagamento de danos morais por violação à privacidade, o Tribunal de Justiça entendeu pela falta de provas e que o simples encaminhamento de mensagens genéricas por e-mail ou WhatsApp não é conduta suscetível de causar dano moral e é apenas um mero aborrecimento.
- Caso Mercado Livre: empresa parceira do site que anunciou a venda de banco de dados.
- Judicialmente, foi determinado ao Mercado Livre a suspensão do anúncio referente a venda de banco de dados e cadastro em geral;
- De igual modo, foi determinando à empresa anunciantes a abstenção de disponibilização de dados pessoais.

MÓDULO 10

AÇÕES DE ADEQUAÇÃO À LGPD: SEGURANÇA DA INFORMAÇÃO

AULA 50 – PRINCIPAIS MEDIDAS TÉCNICAS PARA IMPLEMENTAÇÃO DA LGPD

Inicialmente, é imprescindível a criação de uma **Política de Segurança da Informação** com procedimentos para a proteção de dados, tanto de forma física, quanto digital.

Na política de segurança devem constar as responsabilidades e as permissões envolvendo o tratamento de dados pessoais na empresa, bem como as formas de controle e as penalidades em caso de descumprimento das políticas internas. Este processo deverá ser supervisionado pelo Encarregado de Dados (Módulo 07).

Depois de instituída a Política de Segurança da Informação, a empresa deverá realizar um **treinamento** com todos os colaboradores, para que estes fiquem cientes das práticas que deverão ser adotadas no âmbito da manipulação de dados pessoais.

Outra aplicação prática fundamental é **a manutenção dos sistemas internos da empresa**, para que estejam sempre atualizados. As atualizações dos sistemas são importantes para que os erros sejam corrigidos e novas formas de seguranças sejam implementadas ou alteradas. Essas atualizações podem ser automatizadas, criando-se uma rotina de atualização que não atrapalhe o trabalho diário do colaborador.

Neste sentido, é importante que a empresa invista em **anti-spam**, *firewall* e **antivírus**.

Os filtros **anti-spam** tem o objetivo de evitar que os colaboradores da empresa sejam enganados por armadilhas virtuais, como o *phishing*, fraude em que e-mails aparentemente reais são enviados a um destinatário com objetivo obter informações pessoais como usuário e senha eletrônicos.

O *firewall* é um método de segurança que tem como objetivo monitorar o tráfego de rede, identificando as entradas e saídas, para evitar que dados sejam propagados na internet.

Ademais, o **antivírus** tem o objetivo de proteger o computador contra as ameaças que possam prejudicar os *softwares*. Neste sentido, é recomendável que se utilize apenas um antivírus por computador, sob pena de causar inconsistências capazes de tornar o sistema vulnerável.

Outra importante ação é a realização de **backups periódicos** nas máquinas da empresa. Isto é necessário para evitar que informações sejam perdidas, tanto por erros do sistema, quanto por ataques de criminosos ou falhas humanas.

A ação dos colaboradores também contribuirá para o sucesso da implementação de medidas de segurança, hábitos como o de **criar senhas fortes**, que contenham caracteres especiais, números e combinação de letras maiúsculas e minúsculas, são capazes de diminuir consideravelmente as chances de um eventual vazamento de dados. Ainda no âmbito interno, orienta-se que os funcionários **não compartilhem suas senhas** com companheiros de trabalho, muito menos com terceiros.

Ressalta-se que Política de Segurança da Informação visa a prevenção de incidentes e deve ser acompanhada de um **Plano de Recuperação** para os casos em que os incidentes já tenham ocorrido, de modo que os colaboradores saibam como agir para evitar que os prejuízos sejam ainda maiores.

AULA 51 – A IMPORTÂNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Conceitualmente, uma Política de Segurança da Informação tem o objetivo de estabelecer diretrizes estratégicas, responsabilidades, competências, normas e procedimentos de uso, visando assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações armazenadas pela empresa.

A instituição dessa Política tem se tornado cada vez mais relevante para o tratamento seguro de dados pessoais por parte das empresas, tendo em vista o incremento da legislação sobre proteção de dados, associado ao avanço dos mecanismos de controle da ANPD.

No tocante a estes mecanismos, destaca-se a previsão de sanção administrativa em forma de multa simples de até 2% (dois por cento) do faturamento da pessoa jurídica, diante do descumprimento às normas previstas na LGPD, conforme art. 52, II, da lei.

Além disso, cumpre destacar que um eventual vazamento de dados pode representar uma ofensa grave à direitos previstos, inclusive, na Constituição Federal, a violação destes direitos tem o poder de causar prejuízos irreversíveis à vida dos indivíduos afetados por ela.

Com efeito, seguir a Política de Segurança da Informação passou a ser uma medida necessária para o bom andamento das atividades da empresa, pois, além de evitar prejuízos às finanças e à reputação da companhia, é capaz de garantir os direitos dos Titulares de dados pessoais tratados por ela.

Ademais, a Política de Segurança da Informação é imprescindível para o sucesso do projeto de adequação à LGPD, isto porque, ela viabiliza a manutenção das demais medidas de segurança implementadas durante o processo de adequação.

AULA 52 – CIS 20 CONTROLES CIS – PARTE 1

A *Center for Internet Security* (CIS) é uma organização americana, sem fins lucrativos, que tem como objetivo promover soluções estratégicas para tornar a internet um lugar mais seguro. Dentre as sugestões apresentadas pelo CIS, encontram-se os "20 Controles Críticos de Segurança", um conjunto de diretrizes contendo práticas que visam aumentar a proteção de sistemas e dados.

Essas diretrizes são modificadas sempre que se percebe a necessidade de novos mecanismos de segurança envolvendo sistemas digitais. A exemplo disso, tem-se a versão V8, aprimorada para abranger a nova realidade imposta pela pandemia do coronavírus. Ao divulgar sua oitava versão dos Controles, afirma a organização:

> Os Controles Críticos de Segurança CIS (Controles CIS) são um conjunto priorizado de proteções para mitigar os ataques cibernéticos mais prevalentes contra sistemas e redes. Eles são mapeados e referenciados por diversas estruturas jurídicas, regulatórias e políticas. Os Controles CIS v8 foram aprimorados para acompanhar os sistemas e softwares modernos. **A mudança para computação baseada em nuvem, virtualização, mobilidade, terceirização, trabalho em casa e mudanças nas táticas do invasor motivou a atualização e oferece suporte à segurança de uma empresa conforme eles mudam para ambientes totalmente em nuvem e híbridos (tradução nossa).**

Estes vinte controles são divididos em três categorias, a saber: controles básicos (1-6), controles essenciais (7-16) e controles organizacionais (17-20). Nesta aula, abordaremos os seis controles básicos, sendo:

1.INVENTÁRIO E CONTROLE DE ATIVOS DE HARDWARE

Gerenciar ambientes complexos é uma tarefa que requer tempo e paciência, e nem sempre as empresas estão dispostas a se dedicar a essa atividade em específico. Já os invasores estão, pois ao inventariar os ativos de hardware de organizações conseguem viabilizar seus ataques.

Assim, uma forma de mitigar esse problema é monitorar e gerenciar todos os dispositivos de hardware conectados à sua rede interna da empresa, mantendo um inventário atualizado de todos aqueles que tem permissão para acessar a rede, de modo a impedir que dispositivos não autorizados possam acessá-la.

2. INVENTÁRIO E CONTROLE DE ATIVOS DE SOFTWARE

Da mesma forma que ocorre com os ativos de hardware, através do controle de inventário de software é possível identificar quais são os programas utilizados por uma organização, verificando onde podem estar potenciais vulnerabilidades passíveis de exploração por agentes maliciosos.

Assim, é fundamental ter um sistema de inventário de software em vigor para rastrear e gerenciar ativamente todos os softwares em execução na rede, garantindo que somente o software autorizado seja instalado e executado, e que o software não autorizado seja bloqueado. Deste modo, é possível se prevenir dos ataquem que oportunizem ao invasor tomar o controle do sistema utilizado pela empresa.

3. GERENCIAMENTO CONTÍNUO DE VULNERABILIDADES

Escanear vulnerabilidades é a maneira que uma organização possui de entender a quão protegida está contra eventuais ataques, além de determinar quais as próximas ações em termos de segurança da informação deverão ser adotadas, observando pontos de melhoria em seu ambiente.

Assim, é necessário adquirir, avaliar e executar ações continuamente para identificar vulnerabilidades, bem como para corrigir e minimizar a janela de oportunidade para invasores.

4. USO CONTROLADO DE PRIVILÉGIOS ADMINISTRATIVOS

Realizar o uso controlado de privilégios administrativos implica monitorar os controles de acesso, bem como os comportamentos, do usuário de contas privilegiadas, leia-se, aquele que tem acesso a dados partes exclusivas do sistema.

Esse procedimento é necessário, uma vez que quanto maior o nível de acesso de determinado usuário aos sistemas da organização, maior será o impacto em caso de acesso por terceiros não autorizados. Logo, a partir desse monitoramento, junto com as medidas de restrição de acesso cabíveis, é possível impedir o acesso indevido a informações críticas da empresa.

5. CONFIGURAÇÕES SEGURAS PARA HARDWARE E SOFTWARE EM DISPOSITIVOS MÓVEIS, LAPTOPS, ESTAÇÕES DE TRABALHO E SERVIDORES

É corriqueiro que alguns dispositivos e sistemas sejam adquiridos ou implementados com configurações e senhas padrão, que não são modificadas posteriormente. Isso possibilita que sejam invadidos com esforços mínimos, comprometendo todo o ecossistema organizacional.

Como forma de prevenção, deve-se estabelecer e manter um padrão de configurações de segurança a serem utilizadas em dispositivos móveis, laptops estações de trabalho e servidores. Neste sentido, é fundamental que o sistema possa identificar alterações nas configurações definidas, pois estas mudanças podem abrir espaço para alguma vulnerabilidade no sistema.

6. MANUTENÇÃO, MONITORAMENTO E ANÁLISE DE LOGS DE AUDITORIA

Os logs são registros de eventos relevantes em determinado sistema. Assim como a caixa preta de um avião, os logs permitem auditar quais foram os aspectos que culminaram para determinado incidente ou intercorrência.

Quando o registro e análise desses logs são insuficientes ou deficientes, os invasores podem ocultem sua localização com maior facilidade, bem como softwares maliciosos infiltrados e atividades indevidas nas máquinas das vítimas. Mesmo que as vítimas saibam que seus sistemas foram comprometidos, sem registros de registro protegidos

e completos, elas não têm acesso aos detalhes do ataque e às ações subsequentes dos invasores.

Sem registros de auditoria sólidos, um ataque pode passar despercebido indefinidamente e os danos específicos causados podem ser irreversíveis. Apenas através de um monitoramento e análise eficientes dos logs armazenados é que se torna possível a detecção e resposta a incidentes de segurança.

AULA 53 – OS 20 CONTROLES CIS – PARTE 2

Esta aula é uma continuação da aula: Os 20 Controles CIS – Parte 1. Para melhor compreensão e fixação do conteúdo, recomendamos que seja revisitada a discussão da aula anterior.

A Segurança da Informação, para que seja eficaz, deve observar uma série de controles e mecanismos, não se esgotando apenas com políticas e treinamentos. Dando continuidade à nossa aula, vamos tratar sobre os Controles CIS essenciais e organizacionais, observando sempre que não há uma hierarquia entre eles, uma vez que a simples desconsideração de um Controle pode oportunizar incidentes de segurança.

CONTROLES ESSENCIAIS

1. PROTEÇÕES PARA E-MAIL E NAVEGADORES WEB

Para atingir um nível adequado de proteção nesses provedores, é importante gerenciar os controles de proteção dos navegadores da Web e dos sistemas de e-mail, através de medidas como: desativar os navegadores não autorizados e plug-ins de clientes, bem como manter filtros de URL.

Desta maneira, é possível evitar a entrada de *hackers* através dos e-mails recebidos e dos sites acessados.

2. DEFESAS CONTRA MALWARE

Os malwares são códigos maliciosos, capazes de prejudicar sistemas e redes. Há inúmeras formas de se infiltrar malwares em organizações, por isso é importante controlar a instalação e execução de programas que possam contê-los, geralmente através da configuração de um *software antimalware*, de forma a proteger o sistema da presença de algum programa que deseje acessar informações de um dispositivo.

3. LIMITAÇÃO E CONTROLE DE PORTAS, PROTOCOLOS E SERVIÇOS DE REDE

Uma das formas de se controlar a ocorrência de incidentes de segurança na rede é através do monitoramento da atividade em portas, protocolos e serviços da rede, de

modo a garantir que apenas que somente aqueles que sejam validados tenham acesso ao sistema.

4. RECURSOS DE RECUPERAÇÃO DE DADOS

Tão importante quanto armazenar as informações com segurança é garantir sua recuperação em caso de incidentes. Assim, deve-se realizar, frequentemente, o *backup* completo dos principais sistemas utilizados pela empresa, bem como manter um processo de restauração de dados, para que seja possível recuperar informações caso o sistema venha a ser atacado.

5. CONFIGURAÇÃO SEGURA PARA DISPOSITIVOS DE REDE, COMO FIREWALLS, ROTEADORES E SWITCHES

Estabelecer e manter um processo rigoroso de gerenciamento e controle das configurações dos dispositivos de rede é muito importante para evitar a infiltração de malwares e mitigar os riscos de eventuais ataques. Assim, através de configurações seguras de rede se pode evitar ou até mesmo impedir que *hackers* explorem vulnerabilidades das configurações pré-definidas pelo sistema.

6. DEFESA DE PERÍMETRO

O Perímetro à qual o Controle se refere é a existente entre as redes internas e externas. Assim, recomenda-se usar os limites de rede para controlar o fluxo de informações que passam pelo sistema, identificando movimentações que ultrapassem os limites estabelecidos e negando acesso ao que não for autorizado.

7. PROTEÇÃO DE DADOS

A nível de segurança da informação, a proteção de dados é igualmente importante. A proteção de dados, nesse caso, resulta da implementação de processos de segurança que permitam o armazenamento e fluxo seguro de dados (Ex.: criptografia), tanto para limitar o acesso interno a determinados dados, quanto para impedir que *hackers* realizem a infiltração ou a extração de dados pessoais tratados pela empresa.

8. ACESSO CONTROLADO COM BASE NA NECESSIDADE DE SABER

Deve-se controlar acesso dos colaboradores aos dados armazenados pela empresa, levando em consideração se o usuário tem realmente a necessidade de ter acesso às informações que deseja obter.

Do mesmo modo, é relevante manter um registro dos acessos às pastas e sistemas da rede interna da empresa, para que seja possível investigar eventuais incidentes envolvendo vazamento de informações.

9. CONTROLE DE ACESSO À REDE SEM FIO

Cada vez mais, a utilização de redes sem fio é implementada em casas e organizações para facilitar a conexão à internet. No entanto, é importante que sejam utilizados programas que verifiquem periodicamente a rede interna para detectar a existência de pontos de acesso, sistemas ou dispositivos não autorizados.

10. MONITORAMENTO E CONTROLE DE CREDENCIAIS DE ACESSO

Acompanhar ativamente todo o ciclo de vida das contas existentes no sistema da empresa, desde sua criação e uso até sua exclusão se faz um controle necessário para impedir que invasores utilizem contas inativas para acessar o sistema sem levantar suspeitas.

CONTROLES ORGANIZACIONAIS

1. IMPLEMENTAÇÃO DE PROGRAMA DE CONSCIENTIZAÇÃO E TREINAMENTO DE SEGURANÇA

Dentro de uma organização, não apenas são necessários controles relacionados a produtos ou serviços tecnológicos. Também é importante que todos os funcionários entendam como utilizar os ativos de forma adequada, quais os cuidados necessários envolvendo dados da empresa e como reagir em caso de incidentes.

Assim, é importante implementar um programa de conscientização, bem como disponibilizar treinamentos aos colaboradores para instrui-los quanto às práticas a serem adotadas no dia a dia para que a empresa possa manter seu projeto de segurança da informação.

2. SEGURANÇA DE SOFTWARE DE APLICAÇÃO

Para verificar o nível de segurança de determinado software, é fundamental realizar testes regulares envolvendo os ativos desenvolvidos ou adquiridos pela empresa. Isso possibilitará a identificação de irregularidades e vulnerabilidades, bem como o estabelecimento de critérios mais rigorosos no momento da avaliação de softwares de terceiros.

3. RESPOSTA E GERENCIAMENTO DE INCIDENTES

Mitigar riscos é uma das maiores preocupações de organizações, o que por vezes faz negligenciar o gerenciamento posterior ao incidente. Assim, para ter maior efetividade na resposta organizacional, é necessário desenvolver e implementar um sistema de gerenciamento de incidentes que permita que a empresa consiga identificar uma invasão, erradicar a presença do invasor e restaurar o equilíbrio da rede interna o mais rápido possível.

4. TESTES DE PENETRAÇÃO E EXERCÍCIOS DE “RED TEAM”

Por vezes, para que se tenha conhecimento das vulnerabilidades exploradas por um invasor é preciso pensar como um. Existem testes capazes de simular uma

penetração nos ambientes da organização, verificando o nível de proteção existente e sugerindo melhorias de defesa.

Desta forma, é interessante realizar testes periodicamente acerca das defesas internas para evidenciar eventuais falhas ou lacunas, bem como realizar atividades voltadas à simulação de ataques ao sistema.

AULA 54 - SEGURANÇA DA INFORMAÇÃO NA VIDA PESSOAL E PROFISSIONAL

Sabe-se que, principalmente no mundo digital, são diversas as informações que transitam entre as pessoas através de aplicativos e *softwares* de computadores e, por este motivo, estamos vulneráveis a ameaças capazes de sequestrar dados de nossos dispositivos eletrônicos.

Por isso a segurança da informação é extremamente relevante na vida pessoal e profissional, pois não é apenas a integridade da empresa que se busca preservar, mas principalmente os direitos de privacidade e proteção de dados das pessoas naturais.

Com a aplicação de procedimentos internos, políticas e outras diretrizes para orientar os colaboradores da empresa, as chances de ocorrer incidentes de Segurança da Informação no ambiente corporativo diminuem consideravelmente.

Do igual modo, cuidados com a Segurança da Informação na vida pessoal são fundamentais para que o indivíduo mantenha seus dados pessoais protegidos nas interações do dia a dia.

Em que pese muitas pessoas seguirem as regras e políticas de Segurança da Informação implementadas pela empresa em que trabalham, quando o assunto é a vida privada, o esforço, definitivamente, não é o mesmo.

O que os indivíduos não percebem é que no dia a dia pessoal também há exposição a ameaças envolvendo dados pessoais. Caso não sejam tomados os devidos cuidados com o armazenamento de senhas pessoais, a sua inserção em sites desconhecidos, o uso de *softwares* piratas, entre outras situações vulgares, nossas informações podem ser obtidas e utilizadas maliciosamente por criminosos.

Um bom exemplo de roubo de dados é a realização de compras em sites desconhecidos, em que acabamos, sem perceber, passando informações pessoais a criminosos. Os criminosos captam dados pessoais como o nome,

CPF, número de cartão, senha do cartão etc. Porém, existem práticas que podem ser adotadas para evitar que esse tipo de situação se concretize, a saber:

- Não clicar em *links* recebidos por e-mail;
- Não cadastrar informações pessoais em sites desconhecidos;
- Não utilizar *software* pirata;
- Utilizar um bom antivírus e o mantê-lo atualizado;
- Criar senhas complexas, com números, letras maiúsculas, minúsculas e caracteres especiais.
- Não acessar suas redes sociais em computadores desconhecidos;
- Não fornecer suas senhas a ninguém;
- Não deixar informações importantes anotadas em qualquer lugar (como *post it's* no monitor).

AULA 55 - PRINCIPAIS AMEAÇAS EM AMBIENTES LÓGICOS

Passemos a uma exposição sobre as principais ameaças à Segurança da Informação no ambiente lógico. A palavra "lógicos", no dito contexto, refere-se aos softwares utilizados pelas empresas e indivíduos, isto é, os programas responsáveis pelo funcionamento das máquinas empresariais e que possuem diversas informações.

A primeira ameaça é chamada "*phishing*", que consiste na utilização de aplicativos e sites falsos, praticamente iguais aos originais, com o simples objetivo de enganarem os usuários e ter acesso de todas as informações desejadas.

Esta prática criminosa pode ocorrer de diversas formas. Muitos criminosos atuam de forma ativa, realizando, inclusive, uma conversa por chat para que o usuário tenha confiança de que se trata de uma empresa séria. Além disso, os criminosos também utilizam e-mails para solicitar as informações, como e-mails praticamente idênticos aos e-mails dos bancos, órgãos públicos (como INSS), entre outros.

Através dessa técnica, caso as informações sejam fornecidas, os criminosos conseguem invadir os dispositivos e coletar as informações que desejarem. Assim, conseguirão, inclusive, acessar contas de instituições bancárias.

Outra famosa ameaça é o vírus que, dentre eles, destaca-se o *ransomware*, que tem como principal função fazer a cópia das informações de um computador ou, até mesmo, de uma rede inteira. Após a realização da cópia das informações, o criminoso solicita um pagamento para devolução do que foi copiado.

Também existem os Ataques DDoS (*Distributed Denial of Service*), traduzidos em "Ataques Distribuídos de Negação de Serviços". Esta ameaça tem o objetivo de infectar hardwares, causando a indisponibilidade dos serviços para seus usuários. Com isso, uma sobrecarga é gerada em um determinado servidor ou computador comum, indisponibilizando o sistema. Este tipo de ação também tem a intenção de tornar o dispositivo vulnerável para a realização dos crimes.

A espionagem é outra ameaça que assusta as empresas, uma vez que os criminosos acessam as câmeras e microfones de dispositivos com o objetivo de espionar o usuário. Essa ameaça amedronta os usuários também na esfera pessoal.

AULA 56 - PRINCIPAIS AMEAÇAS EM AMBIENTES FÍSICOS.

Por "ambientes físicos" entende-se os locais em que os computadores, servidores e meios de comunicação (hardwares) estão fisicamente instalados. Neste caso, as ameaças não estão na atividade virtual dos criminosos, mas sim no controle de acesso aos ambientes físicos.

Primeiramente, cumpre ressaltar as ameaças que envolvem a própria estrutura física da empresa, pois, sem a realização constante de *backups*, fenômenos como **quedas de energia**, **incêndios** e **outros capazes de inutilizar os computadores e hardwares instalados**, podem se tornar ameaças para o armazenamento de informações no sistema, afinal, os dados poderão ser perdidos durante o processo de desligamento abrupto do sistema.

Ademais, o **controle de acessos físicos** aos locais deve ser rigoroso, apenas funcionários autorizados devem ter acesso aos locais em que os documentos relevantes são armazenados. Além disso, o uso de chaves nos armários e a instalação de câmeras, são medidas importantes para a proteção dos ambientes físicos da empresa.

MÓDULO 11

AÇÕES DE ADEQUAÇÃO À LGPD: PROJETO DE ADEQUAÇÃO E DA GOVERNANÇA DE PROTEÇÃO DE DADOS

AULA 57 – COMO ESTRUTURAR UM PROGRAMA DE GOVERNANÇA

ADOÇÃO DE PROCESSOS E POLÍTICAS INTERNAS

O primeiro passo é a organização interna da empresa. Após comunicar toda empresa sobre o início do processo de adequação à LGPD e nomear um DPO, é possível começar a pensar na criação dos procedimentos e políticas internas.

As políticas devem abranger todo o conteúdo de proteção de dados, desde a Política de Privacidade, Descarte correto dos dados até a Política de Segurança da Informação.

TORNAR O PROGRAMA APLICÁVEL A TODO O CONJUNTO DE DADOS PESSOAIS

Para a segurança da empresa, será necessário implementar o programa em relação a todos os conjuntos de dados pessoais que estarão no controle da empresa, independentemente de como ocorreu a coleta, ou seja, independentemente de como se deu o início do tratamento.

TORNAR O PROGRAMA ADAPTÁVEL

Quando a lei fala a respeito da adequação do programa, ela indica que o programa deve ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados.

ESTABELECER POLÍTICAS E PROTEÇÃO ADEQUADAS

Para que o programa se torne eficiente, é preciso se resguardar de eventuais danos, sendo assim, é importante que a empresa se baseie em uma avaliação sistêmica, ou seja, organizada, regular e minuciosa para que seja possível prever impactos e riscos à privacidade.

ESTABELECER CONFIANÇA COM O TITULAR

Um bom Programa de Governança em Privacidade, sem dúvidas, deverá ser capaz de trazer segurança ao Titular dos dados. Esta segurança se dará através da transparência e do cuidado no tratamento de cada dado pessoal. Desta forma, é fundamental que a empresa estabeleça uma relação de confiança com o titular através da adoção de métodos que possibilitem a participação do titular nos processos: deixando disponíveis canais de atendimento, dúvidas e mantendo as políticas de privacidade atualizadas e acessíveis.

INTEGRAÇÃO DAS POLÍTICAS ESTABELECIDAS

É imprescindível que a empresa seja capaz de harmonizar o conteúdo de todas as suas políticas. Neste sentido, ressalta-se que o Programa de Governança em Privacidade deve estar integrado à estrutura geral de Governança da empresa.

ESTABELECER MECANISMOS DE SUPERVISÃO

Para que o programa não fique desatualizado, deve-se criar métodos para supervisionar as políticas e a efetivação do programa interna e externamente, através de um monitoramento contínuo e avaliações periódicas.

CRIAÇÃO DE PROCEDIMENTO DE RESPOSTA A INCIDENTES ENVOLVENDO DADOS PESSOAIS

Neste sentido, é essencial que o DPO elabore respostas a eventuais incidentes de vazamento de dados ou até mesmo do uso indevido de dados. Além disso, é interessante possuir um plano de ação prévio nestes casos para diminuir os efeitos nocivos que estes incidentes podem causar ao titular e à empresa.

DEMONSTRAÇÃO CONSTANTE DA EFETIVIDADE DO PROGRAMA

Demonstrar a efetividade do projeto é relevante tanto em relação aos que estão em posições de liderança, quanto em relação aos próprios colaboradores.

Também, devem ser elaboradas estratégias para demonstrar os resultados aos clientes, prestadores de serviços e todos que direta ou indiretamente são envolvidos em sua empresa.

PUBLIQUE AS REGRAS DE BOAS PRÁTICAS

Por fim, a empresa deve publicar suas políticas e boas práticas em todos os meios possíveis, de modo a possibilitar o fácil acesso de seus clientes às regras de segurança.

AULA 58 - A IMPORTÂNCIA DE SE INSTITUIR UM COMITÊ DE PRIVACIDADE

O Comitê de Privacidade é um instrumento de grande relevância pois esse facilita a atuação do encarregado, bem como poderá promover uma cultura de proteção de dados pessoais dentro das instituições.

As boas práticas instituídas pelo comitê convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da instituição, contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum.

Outrossim, o comitê poderá avaliar mecanismos de tratamento e proteção de dados, propor políticas, estratégias e metas de adequação, além de possui as seguintes responsabilidades:

- Demonstrar comprometimento em adotar políticas e assegurar o cumprimento das normas estabelecidas;
- Integrar a estrutura geral de governança e estabelecer e aplicar mecanismos de supervisão internos e externos;
- Contar com planos de resposta a incidentes e remediação;
- Estabelecimento de políticas e salvaguardas adequadas, baseadas em processos de avaliação de impactos e riscos à privacidade;
- Zelar pelo do Programa de LGPD e, no caso de descumprimento, apurar e adotar as medidas cabíveis;
- Gerenciar atividades relativas ao tratamento de dados; e
- Estar constantemente atualizado com base nas alterações legislativas e informações obtidas internas a partir de reuniões de monitoramento e avaliações periódicas.

Além disso, o comitê poderá ser o responsável por levar ao conhecimento do DPO os atos de incidente de segurança da informação e/ou vazamento de dados que ofereçam risco de exposição da companhia, investigação e toda e qualquer conduta capaz de causar a instituição dano de qualquer natureza, alinhado às diretrizes globais de notificação de incidentes, as quais deverão ser respeitadas concomitantemente, assumindo o papel

Sendo assim, o Comitê de Privacidade e Proteção de Dados assume o papel de se responsabilizar, mesmo que internamente, que a instituição ao qual pertencem estejam de acordo com as normas e princípios listados na LGPD, implementando assim uma cultura de proteção de dados pessoais.

Por fim, cumpre ressaltar que um comitê de privacidade e proteção de dados bem desenvolvido poderá ser reconhecido e divulgado pela ANPD, tornando a companhia referência no assunto de proteção de dados.

AULA 59 – ETAPAS PARA IMPLEMENTAÇÃO DA LGPD PARTE 1

Este curso foi preparado para que você consiga compreender, de uma forma lógica, a importância e as etapas de um projeto de adequação à LGPD para agentes de tratamento de dados pessoais. Assim, chegando aos módulos finais do curso, demonstraremos como normalmente são divididos os projetos de adequação, bem como a importância da Governança em Proteção de Dados para a manutenção das medidas implementadas.

Ressalta-se que inexiste na lei um procedimento específico a ser seguido no momento de implementação do projeto de LGPD, entretanto, é importante que os projetos observem todos os preceitos já demonstrados no presente curso.

Este módulo não entrará na seara prática, mas apenas demonstrará quais são os passos e etapas para um adequado projeto de LGPD que irá resguardar a empresa/órgão após a sua implementação.

Todo projeto de adequação à Lei Geral de Proteção de Dados deve ser considerado como um projeto técnico com base na própria legislação, em preceitos de Governança Corporativa e Segurança da Informação, objetivando as alterações, caso necessárias, dos fluxos de dados pessoais, adequações de contratos e documentos, além do estabelecimento de procedimentos internos para manutenção da instituição em Compliance com a lei.

Lembre-se que as instituições que não estão em conformidade com a lei podem sofrer algumas consequências, como crises reputacionais e financeiras; exigência de conformidade por parte de empresas ou instituições correlacionadas à empresa não adequada; judicialização com o ajuizamento de ações individuais e coletivas de indenização em benefício dos titulares de dados pessoais; e aplicação de penalidades judiciais e administrativas pela Autoridade Nacional de Proteção de Dados, Ministério Público e Órgãos do Consumidor.

Independentemente de o projeto acontecer em uma empresa ou órgão público, o procedimento a ser adotado é idêntico, com a mudança apenas relacionada às áreas internas que serão consideradas como prioritárias para análise e alteração.

Ainda acerca da metodologia, existem algumas ferramentas no mercado que são utilizadas para incrementar a gestão e governança de dados das empresas, mas não são essenciais dentro de um projeto de adequação à Lei Geral de Proteção de Dados.

Ressalta-se que antes de iniciar as etapas de implementação, é necessário buscar toda a documentação da empresa para uma análise prévia, como contratos e políticas internas. É interessante que essa prática seja realizada para que se consiga organizar um cronograma, mesmo que provisório, para orientação do projeto e prazos a serem cumpridos ao longo das etapas.

Além disso, é interessante que os projetos sejam separados em etapas, sendo a última forma mais detalhada. Dessa forma, é possível aplicar a metodologia que se mostre mais eficiente e viável para cada organização, sem deixar de lado as ações essenciais à adequação.

A primeira etapa pode ser chamada de etapa de **Preparação**, que possui o objetivo de realizar o planejamento do projeto, através das seguintes atividades: definição do comitê de privacidade e nomeação do DPO; coleta de leis que impactam o negócio; mapeamento de dados; análise de gaps; análise de risco de TI; estabelecimento de um programa de proteção de dados e a criação de um plano de ação para implementação.

A segunda etapa é a de **Organização**. Com os gaps e requisitos de adequação devidamente identificados, o projeto necessitará de um planejamento específico para determinar a forma pela qual se dará a conformidade. Na etapa de preparação: são definidas funções e responsabilidades para a equipe; busca-se o engajamento da alta administração; são definidos quais treinamentos ocorrerão, bem como estabelecidas algumas políticas (privacidade, segurança da informação, controle de acessos, gestão de riscos, resposta a incidentes etc.).

A terceira etapa é a de **Desenvolvimento e Implementação**. Aqui o projeto migrará para o plano prático, com as seguintes atividades: adoção de práticas de conformidade, implementação das políticas previamente estabelecidas, implantação de novas ferramentas, processos e procedimentos, realização de treinamentos e gestão de terceiros.

Neste momento, após a realização das três primeiras etapas, podemos dizer que a implementação do projeto já tomou certa forma, e que a organização provavelmente está protegendo com maior apuração técnica os dados que controla.

AULA 60 – ETAPAS PARA IMPLEMENTAÇÃO DA LGPD PARTE 2

Esta aula é uma continuação da aula: Etapas para Implementação da LGPD – Parte 1. Para melhor compreensão e fixação do conteúdo, recomendamos que seja revisitada a discussão da aula anterior.

Após as etapas estudadas no módulo anterior, o projeto possui um corpo bem definido através de mecanismos e ferramentas de segurança da informação, bem como políticas, normas internas e outros controles organizacionais. No entanto, uma ampla proteção à privacidade deve também contar com mecanismos preventivos para a organização, o que se faz através da quarta e quinta etapas.

A quarta etapa é a de **Governança**. Nela, são realizadas auditorias e avaliações no projeto de adequação, como forma de verificar se os riscos de fato foram minimizados, eliminados ou aceitos pela organização, bem como reavaliar e atualizar toda a documentação elaborada anteriormente (políticas, normas, procedimentos e códigos internos). Na etapa de Governança a empresa possui uma maior maturidade para responder às solicitações dos titulares e para se comunicar com a Autoridade Nacional de Proteção de Dados.

A quinta e última etapa é chamada de **Avaliação e/ou Melhoria Contínua**. Nesta etapa, a organização lança mão de técnicas de gestão de processos e qualidade para garantir que esteja sempre a par das transformações que ocorrem ao longo de suas atividades. Isso se faz através da constante atualização tecnológica, reciclagens e capacitação de profissionais, acompanhamento de indicadores e auditorias, avaliações de riscos e monitoramento de novas leis e regulamentos sobre Proteção de Dados. Ao fim da

quinta etapa, a instituição provavelmente contará com um arcabouço documental muito abrangente, contendo algumas ou até mesmo todas as documentações a seguir:

- Política de Privacidade;
- Termos de consentimento, se necessário;
- Política de Governança de Dados Pessoais;
- Procedimento de Avaliação de Privacidade (Design & Default);
- Normativo de Análise de Legítimo Interesse (LIA);
- Normativo de RIPD (Relatório de Impacto à Proteção de Dados Pessoais) + Modelo de RIPD;
- Procedimento de Processamento das Requisições dos Titulares
- Segurança da informação:
- Política de Segurança da Informação e Cibernética;
- Termo de Responsabilidade;
- Norma de Classificação da Informação;
- Norma de Uso dos Recursos de TIC;
- Norma de Resposta a Incidentes de Segurança;
- Norma de Teletrabalho;
- Norma de Gestão de Logs e Trilhas de Auditoria;
- Norma de Uso de Dispositivos Móveis.

Contratos:

- Atualização do Acordo de Confidencialidade;
- Termos de Uso e Política de Privacidade e Cookies dos ambientes virtuais;
- Contrato com o Encarregado pelo Tratamento de Dados Pessoais;
- Questionário de Due Dilligence de terceiros (aplicação de checklist);
- Atualização do Contrato de Trabalho;
- Revisão de todos os contratos em vigência.

Com isso, concluímos todas as etapas de um projeto de adequação. No entanto, ao contrário de todo o procedimento para adequar-se à lei, a organização jamais poderá cessar seu esforço pela manutenção das medidas e controles adotados, pois embora seja impossível eliminar os riscos envolvendo incidentes com dados pessoais, uma instituição com mecanismos defasados certamente corre riscos maiores.

AULA 61 – DIAGNÓSTICO PARA IMPLEMENTAÇÃO DA LGPD

Uma das principais etapas do projeto de adequação à LGPD consiste no diagnóstico da maturidade da empresa quanto à Privacidade e Proteção de Dados, bem como dos principais pontos de alerta das atividades que envolvem dados pessoais, a fim de conhecer os riscos das atividades desempenhadas e, posteriormente, delinear um Plano de Ação que vise à sua mitigação.

Há que se ressaltar, no entanto, que embora a realização de diagnósticos da instituição seja importante para mitigação de riscos, nem sempre isso ocorrerá. Isto, pois o responsável poderá entender que o risco inerente à atividade é compensado pelos possíveis ganhos ou benefícios gerados à empresa. Nesses casos, a assunção do risco deverá ser a última opção adotada, ocorrendo apenas nos casos em que a empresa verifica ser impossível a mitigação ou quando impossível a obtenção do mesmo proveito por meio de outra atividade.

Para a obtenção de um diagnóstico, há inúmeros softwares capazes de mapear riscos, mas outra opção viável para obtê-lo é através da realização de entrevistas com os departamentos críticos, aplicando-se também os questionários sobre LGPD. Nas entrevistas, são diversas as perguntas que podem e precisam ser feitas, sobretudo em relação às tarefas de alguns colaboradores.

É necessário que a equipe responsável pelo projeto esteja atenta ao organograma da empresa, pois através deste documento será possível visualizar qual o nível hierárquico de cada profissional no ambiente da organização, seus setores e a relação de subordinados diretos e indiretos. Tendo-se uma visão geral do quadro de colaboradores, a equipe deverá realizar a priorização de áreas e profissionais de maior impacto para realização de entrevistas, sobretudo em empresas onde se é impossível conhecer individualmente as atividades desempenhadas pelos funcionários. Algumas das perguntas que podem ser realizadas são:

- Quais dados pessoais estão envolvidos na atividade de tratamento?
- A quem pertencem os dados pessoais?
- Há dados de menores de idade na atividade?
- Qual a finalidade do tratamento?
- Quais os sistemas envolvidos e seus controles de segurança?
- Há atividades de tratamento em meio físico? Quais?
- Os dados são compartilhados entre setores?
- Os dados são compartilhados externamente?
- Há obrigações legais atreladas à atividade?

Com as respostas dessas e outras perguntas, será elaborada uma matriz com o fluxo de todos os dados mapeados, viabilizando análises de risco de cada atividade, bem como a elaboração de recomendações e estratégias para mitigar as chances de um incidente. Também poderão ser desenvolvidos relatórios de diagnóstico contendo um resumo da situação atual da empresa e as principais conclusões.

Após as entrevistas, a equipe responsável pela adequação deverá manter o registro dos dados mapeados e atualizar os fluxos periodicamente, uma vez que o caráter orgânico de uma empresa implica na adoção constante de novos procedimentos para a realização de atividades internas.

Essa revisão é necessária e altamente recomendável, pois eventual defasagem entre os fluxos e a realidade da organização pode acarretar a elaboração de documentos

incapazes de refletir suas reais demandas em termos de proteção de dados, maximizando o risco de incidentes e multas pela ANPD.

AULA 62 – A IMPORTÂNCIA DE UM PLANO DE AÇÃO

Uma das principais características de um projeto de adequação à LGPD bem-sucedido é a organização. Para que nenhuma medida importante seja esquecida e para que toda a equipe responsável pelo projeto esteja alinhada, é de extrema relevância a elaboração de um plano de ação definido e detalhado para a segunda etapa, logo após a fase do diagnóstico, que irá delinear o caminho a ser seguido, de acordo com a análise realizada na etapa anterior.

Vale destacar, no entanto, que não há uma regra específica para que seja realizado o plano de ação para etapa 2, mas é recomendável que contenha diferentes tipos de ações e que observe alguns pilares que não podem ser esquecidos. Assim, um plano de ação adequado deve atender aos pilares técnico, documental/procedimental e cultural/organizacional.

Os três pilares estão relacionados com todo o projeto de adequação e com a própria legislação, tendo em vista que o pilar técnico é focado nas medidas técnicas que devem ser adotadas para impedir violações à lei; o pilar documental/procedimental é relacionado à parte jurídica, com a implementação e alteração dos documentos necessários; e o pilar cultural é relacionado à própria manutenção do projeto, mantendo-se a cultura de proteção de dados dentro da empresa (Governança Corporativa).

Ainda com relação ao plano de ação, é recomendável que contenha ações estruturantes e ações específicas. As ações estruturantes são ações de Governança que não possuem vínculo direto com um processo mapeado, mas que necessitam ser implementadas para adequação da empresa à LGPD. Logo, as ações específicas são aquelas diretamente ligadas aos processos mapeados, e sua prioridade será dada de acordo com a classificação do risco do processo a ela vinculado.

Observa-se que, caso necessário, as ações estruturantes podem ser divididas entre imediatas e necessárias. Considerando que a LGPD já entrou em vigor, as ações consideradas imediatas são aquelas com maior visibilidade aos titulares de dados pessoais e devem ser priorizadas, assim, com sua rápida aplicação, a empresa conseguirá diminuir sua exposição em relação aos titulares que buscam a empresa por meio de plataformas digitais, caso aplicável.

As ações necessárias, por sua vez, possuem menor visibilidade, mas também precisam ser realizadas para adequação total da empresa à LGPD e, para isso, não devem ser abandonadas após a implementação das ações imediatas.

Por fim, importa destacar que o plano de ação define as ações a serem tomadas a curto e médio prazo para garantir que a adequação se concretize; no entanto, a manutenção

das medidas e das boas práticas implementadas a longo prazo é essencial para garantir que a organização siga em conformidade com a lei. Assim, não devem ser deixadas de lado ações que visem à continuidade da cultura de Privacidade e Proteção de Dados, sobretudo no que tange à Governança Corporativa.

IEL
Instituto Euvaldo Lodi
PELO FUTURO DA INDÚSTRIA

MÓDULO 12

COMPLIANCE E LGPD COM EXEMPLO PRÁTICO DE UM PROJETO DE ADEQUAÇÃO

AULA 63 – INTRODUÇÃO AO COMPLIANCE DIGITAL

No módulo passado, você aprendeu o que é o Projeto de Adequação à Lei Geral de Proteção de Dados, bem como quais são os pontos importantes para que se mantenha uma boa Governança com relação à proteção de dados. Com esse repertório, será mais fácil a compreensão deste módulo, em que serão apresentadas algumas ações pontuais de adequação à LGPD, considerando que você já tem conhecimento de toda a estrutura de um programa de privacidade de dados.

Além disso, abordaremos também alguns pontos importantes com relação aos princípios de Compliance que são essenciais em qualquer ação relacionada à adequação à Lei Geral de Proteção de Dados. Para que se tenha uma melhor compreensão sobre as ações de adequação à LGPD que temos analisado até agora, vamos trazer alguns pilares sobre o compliance que são inerentes a qualquer projeto de adequação à LGPD.

O primeiro deles é chamado de ***Tone at the Top (O exemplo vem de cima)***, termo que representa o apoio dos altos executivos da empresa, significando não apenas possibilitar que um programa de compliance seja criado e implementado, mas que a alta administração o apoie incondicionalmente, dando o primeiro exemplo aos demais. Este princípio é aplicável não apenas em LGPD, mas em demais assuntos dentro das empresas. Com base neste princípio, todos devem participar dos treinamentos e administrar pelo exemplo do cumprimento das normas.

O segundo é chamado de ***Risk Assessment (Avaliação de Riscos)***, consistente no levantamento dos riscos com relação à atividade. Além dos riscos, é necessária a análise do impacto diretamente ao negócio, de forma que não existe um modelo padrão para que essa análise seja realizada. Quando se fala em LGPD e implementação de um novo sistema na empresa, esta atividade há de ser desempenhada, sendo inclusive realizado um relatório de impacto, onde ficarão comprovados os riscos e as eventuais salvaguardas aptas a mitigá-lo. Caso seja verificado que este novo sistema ou processo forneça mais riscos do que benefícios, o relatório demonstrará que não vale a pena sua implantação, podendo o responsável decidir se irá ou não descartá-lo.

Outro pilar do compliance é a **documentação** através de políticas e normativos, conforme já explanado por diversas vezes neste curso. Através desses documentos, será possível manter um padrão de conduta e estabelecer as penalidades aos colaboradores que não seguirem as normas. Uma vez elaborados, é de extrema importância que se dê a devida publicidade a esses documentos, podendo-se inclusive solicitar a assinatura de termos de ciência para comprovar que os colaboradores estão cientes dos padrões que precisam seguir.

Também é pilar do compliance o estabelecimento de **controles internos**, com o objetivo de criar mecanismos que possibilitem à empresa alcançar seus objetivos de

conformidade, como a própria utilização de sistemas internos que auxiliem na execução dos trabalhos ou até mesmo prevenindo de ameaças externas, como um firewall.

Treinamento e **comunicação** são outros pilares imprescindíveis com relação ao compliance. Conforme demonstrado no módulo anterior, uma das primeiras tarefas em um projeto de adequação à LGPD é a conscientização dos colaboradores. Ao final do projeto, para que seja feita a manutenção da adequação à LGPD, é imprescindível que se mantenham em dia os treinamentos.

O que não é de conhecimento geral e acaba sendo uma das maiores utilidades/princípios dentro dos ensinamentos de compliance é a criação de **canais de denúncia**, uma vez que se trata de ferramentas essenciais para manter uma comunicação segura, anônima e que garanta a não identificação das pessoas que alertam sobre as atitudes que estão em desconformidade dentro de uma empresa.

As **investigações internas** também são importantíssimas, eis que complementares aos canais de denúncia. Se a denúncia é feita e não existe a investigação interna, nunca será possível constatar se a denúncia procede ou se a denúncia era apenas um alarme falso. Inclusive, as investigações internas, devidamente documentadas, podem ser usadas em processos judiciais como prova.

Mais uma prática que é essencial e considerada como um dos pilares do compliance é a aplicação de ***due dilligence***, consistente na avaliação dos fornecedores, parceiros, revendedores, e demais empresas relacionadas à empresa.

Por fim, o último pilar do compliance é a **auditoria** e **monitoramento**, úteis para manter o programa de proteção de dados ou até mesmo o projeto de adequação em dia. Inexistindo o acompanhamento, impossível fazer que as normas, políticas e novos procedimentos sejam cumpridos.

AULA 64 – A IMPORTÂNCIA DA GESTÃO DE TERCEIROS

No módulo anterior, vimos a relevância do compliance enquanto ferramenta para garantir a conformidade das organizações às normas, inclusive, à LGPD. No entanto, é preciso ressaltar que as empresas não só devem se preocupar com as atividades realizadas internamente, mas também precisam ter diligência e atenção às operações desempenhadas por fornecedores, terceirizados, licenciados, agentes e parceiros. A partir das práticas de compliance, passou a existir um foco regulatório acerca da gestão de terceiros, tendo em vista os riscos inerentes às atividades desempenhadas por eles. Nesse sentido, portanto, o gerenciamento de terceiros é o processo que visa a assegurar um bom relacionamento com parceiros, além de viabilizar o controle e a análise de riscos.

Como já vimos, a prática de ***due dilligence*** é de suma importância para o compliance e consiste em um dos mecanismos para garantir uma boa gestão de terceiros, pois faz-se uma avaliação dos terceiros relacionadas à empresa. Nessa avaliação, é realizada

uma averiguação do histórico das pessoas, físicas ou jurídicas, que se relacionam com a organização, por meio de consulta em tribunais e plataformas. A mencionada ação é necessária para que se evite qualquer correlação com empresas que não respeitam às leis, evitando, consequentemente, que a empresa tenha a sua reputação prejudicada, e, principalmente, não seja responsabilizada solidariamente sendo inocente. Para além dos riscos jurídicos propiciados pela ausência de um programa de gestão de terceiros, vale destacar também os riscos reputacionais inerentes às parcerias. Nesse sentido, um incidente ou escândalo, por exemplo, relacionado a uma empresa pode pôr em xeque a boa reputação de organizações parceiras, impactando, até mesmo, seus lucros e seu valor de mercado.

Alguns procedimentos que podem ser adotados na gestão de terceiros seguem listados abaixo:

- **Identificar e monitorar eventuais riscos:** além da avaliação dos terceiros, realizada por meio da prática de *due diligence* já vista, é importante que sejam estabelecidos mecanismos de controle e monitoramento dos riscos percebidos, quando a relação com o terceiro já existir, efetuando processos de teste, bem como políticas e contratos que definam as funções e responsabilidades de cada parte envolvida para reduzir os riscos.
- **Realizar as práticas de triagem e *onboarding*:** outros dois procedimentos relevantes no programa de gerenciamento de terceiros são a triagem inicial de terceiros e a prática de *onboarding*. O primeiro consiste em categorizar os terceiros avaliados com base em diversos critérios que serão estabelecidos de acordo com a realidade da organização. Já o *onboarding* deve englobar elementos como questionários e entrevistas que concedam as informações necessárias para o início da relação contratual. Além disso, a prática de *onboarding* também tem a função de conscientizar os parceiros, fornecedores e terceiros quanto à cultura da organização, demonstrando os valores pelos quais ela preza.
- **Integrar os processos de gerenciamento de terceiros:** unificar, em um único departamento, as práticas de gestão de terceiros. Com isso, são prevenidas redundâncias e limita-se a visibilidade dos riscos identificados.
- **Utilizar a tecnologia ao favor dos procedimentos:** quando possível, é interessante utilizar plataformas de tecnologia GRC (governança, risco e conformidade), de modo que seja possível avaliar, simultaneamente, um elevado número de terceiros, levando em conta diversos fatores e critérios, bem como automatizar processos de mitigação de riscos.

Considerado o conteúdo exposto neste módulo, percebe-se que um programa de gerenciamento de terceiros, que conte com procedimentos diligentes e bem definidos, é capaz de identificar riscos, como violação de dados, descumprimento de leis e normas, riscos de contrato. Sendo possível, dessa forma, selecionar minuciosamente os parceiros confiáveis para a organização e, consequentemente, evitar implicações nos âmbitos jurídicos e corporativos

AULA 65 – COMO MANTER UM PROGRAMA DE *COMPLIANCE* À LGPD

Após o entendimento quanto à estruturação e ao funcionamento de um projeto de adequação à LGPD, que se divide em algumas etapas de implementação, finalmente, tem-se a última etapa, em que ocorre a manutenção e monitoramento do programa de proteção de dados.

Entretanto, não foram explicadas algumas ações práticas necessárias para todo projeto de adequação à Lei Geral de Proteção de Dados. E, considerando que os pilares do compliance auxiliarão na compreensão dos motivos de aplicação das ações que serão aqui expostas, optamos por deixar as ações como uma forma de sintetização dos pontos mais importantes quando se fala em projetos de adequação.

Dessa forma, vamos às recomendações com relação às ações que devem ser tomadas, considerando, inclusive, os ensinamentos do SERPRO (Serviço Federal de Processamento de Dados – Maior empresa pública de prestação de serviços em tecnologia no Brasil):

- É imprescindível que seja feita uma análise aprofundada das leis que servem para regular o tratamento dos dados pessoais. De acordo com o que foi exposto nesse curso, não só a Lei Geral de Proteção de Dados há de ser levada em consideração, como também as legislações de outros países (GDPR etc.), a Constituição Federal, o Código Civil, o Código de Defesa do Consumidor, o Marco Civil da Internet etc. Além disso, a organização deve sempre estar a par de novas normas pertinentes à privacidade e proteção de dados;
- Devem identificar e organizar os dados pessoais, especialmente, àqueles de pessoas sensíveis e os de crianças e adolescentes, afinal estes exigem cuidados mais específicos no tratamento. Não podemos deixar de realizar essa distinção, pois, a depender do caso, as bases legais (autorizações da lei) serão diferentemente aplicas;
- Informe o titular dos dados antes que o tratamento seja feito, bem como as finalidades da ação – afinal, devem ser compatíveis com a função da empresa ou órgão - os dados pessoais que foram coletados, os destinatários dos dados e os direitos dele em matéria de proteção de dados. Durante o projeto de LGPD, é imprescindível que se constate isto, principalmente observando a transparência que há de ficar comprovada na Política de Privacidade; as empresas devem divulgar de maneira clara e atualizada, por meio do seu site ou meios de comunicação "as hipóteses em que, no exercício de suas competências, trata dados pessoais, e a previsão legal, os procedimentos e as práticas utilizadas";

- As empresas ou órgão devem, na medida do possível, elaborar medidas técnicas, normas e políticas que sejam complementares aos requisitos que estão elencados na LGPD, a fim de alcançar a conformidade e então, quando necessário, demonstrar tais diretrizes a pedido do cidadão e até mesmo da ANPD;
- A implementação de plano de formação, conscientização e capacitação "dos empregados, terceirizados e demais colaboradores sobre a importância da privacidade de dados pessoais". Relembrando os princípios da governança corporativa e compliance, é possível aplicar essa sugestão nos projetos de adequação à LGPD;
- Nas adequações, devem ser feitas adaptações e revisões de procedimentos e formulários, bem como habilitar meios digitais, para atender o público nas demandas de solicitação e revogação do consentimento. Relembrando o módulo das bases legais, é importante ressaltar que na hipótese do tratamento se realizado com base no consentimento, este consentimento há de ser revogado caso seja solicitado pelo titular. Pois então, cuidado na escolha da base legal;
- As empresas não podem se olvidar de que o indivíduo, titular dos dados, têm direitos garantidos, especialmente, perante um órgão público, que são regidos por outras legislações, além da LGPD;
- Deve-se realizar análises de riscos, bem como adotar medidas para fazer frente a falhas que possam violar direitos e liberdades das pessoas. Essa recomendação está diretamente relacionada com o pilar de risk assessment discorrida no tópico acima.
- Por fim, é necessário o estabelecimento de protocolos para gerir e notificar "brechas de segurança e vazamentos de dados [...] pessoais vazados acidental ou ilicitamente a destinatários não autorizados, ou que fiquem temporariamente indisponíveis ou sejam alterados: qualquer violação deve ser notificada ao titular dos dados e à ANPD, sem demora injustificada. Tal recomendação também é relacionada aos princípios do compliance e governança corporativa, uma vez que inexistente as políticas e normas, impossível manter um bom programa de proteção de dados.

Com as sugestões de aplicações de algumas ações para adequações à LGPD, bem como explicados os pilares do mundo do compliance, finalizamos mais um módulo. Agora, provavelmente, os seus conhecimentos sobre o mundo da proteção de dados são maiores e cada vez mais você se interessará pelo assunto.

Para finalizar o curso, ainda demonstraremos casos práticos de aplicações de multas e processos judiciais que já foram ingressados com base em violações da Lei Geral de Proteção de Dados.

AULA 66 – ESTABELECENDO O "TONE AT THE TOP"

Um dos pilares do compliance, como já visto na aula "Introdução ao Compliance Digital", é o "tone from the top", também chamado de "tone at the top". Em tradução livre, podemos equivaler essa expressão a "o exemplo vem de cima", aplicando-se não só à LGPD, mas a diversas outras questões corporativas. Esse pilar, como é possível imaginar, transmite a ideia de que a integridade e a ética devem ser generalizadas em uma organização, a começar pela alta direção. Assim, é necessário que os líderes de uma empresa estejam dispostos a apoiar mecanismos de implementação de compliance.

Acredita-se, nesse sentido, que, se estabelecido, a postura ética dos líderes, por meio do "tone at the top", seja capaz de influenciar positivamente os comportamentos de todos os subordinados, seja por influência, lealdade ou receio. Com isso, por meio do exemplo dos altos cargos, instaura-se uma cultura de conformidade, coibindo condutas que se direcionem ao sentido contrário disso.

O Decreto n. 8.420, que regulamenta a Lei Anticorrupção, já dispunha sobre a necessidade de engajamento da alta administração, sobretudo para fins de apuração de irregularidades e aplicação de sanções. Conforme disposto em seu art. 42:

> Art. 42. Para fins do disposto no § 4º do art. 5º, o programa de integridade será avaliado, quanto a sua existência e aplicação, de acordo com os seguintes parâmetros:
>
> I - comprometimento da alta direção da pessoa jurídica, incluídos os conselhos, evidenciado pelo apoio visível e inequívoco ao programa;
>
> II - padrões de conduta, código de ética, políticas e procedimentos de integridade, aplicáveis a todos os empregados e administradores, independentemente de cargo ou função exercidos;

Para estabelecer esse pilar na prática, é preciso que as pessoas que ocupam altos cargos em uma empresa apoiem, engajem-se e promovam a concretização de uma cultura organizacional que leve em conta os pilares de compliance, assumindo a responsabilidade de fomentar a comunicação e a conscientização de todos os colaboradores a respeito do tema.

Não é suficiente, portanto, declarar seu apoio, o líder deve participar ativamente das reuniões e das ações práticas de Compliance. Compreende-se que a eficácia e o sucesso de programas de compliance, incluindo o programa de adequação à LGPD, dependem, em primeiro lugar, da iniciativa e do engajamento da alta direção de uma organização. Se líderes não demonstrarem um olhar preocupado e cuidadoso quanto às questões de

conformidade, tampouco irão seus subordinados, tornando-se impossível a implementação prática e a transformação da cultura organizacional.

AULA 67 – EXEMPLOS PRÁTICOS DE IMPLEMENTAÇÃO DA LGPD

Neste módulo, após termos analisado, em módulos anteriores, as etapas que compõem um projeto de adequação à LGPD e as ações necessárias para que a adequação se concretize, veremos agora os principais desafios, na prática, à implementação da LGPD ao longo de um projeto verídico.

Neste caso, trataremos do caso verídico da empresa 'A', que passou por todas as etapas do projeto, vivenciando as conquistas e dificuldades da implementação, que serão descritas abaixo:

ETAPA 1: No início da etapa 1, o projeto foi apresentado à empresa "A", por meio de um treinamento inicial, que teve como finalidade alinhar as equipes responsáveis pelo projeto, bem como conscientizar a respeito da estrutura e da metodologia adotadas. Em sequência, os colaboradores da empresa responderam a formulários de proteção de dados, em que descreveram as principais atividades que desempenham com dados pessoais. Neste momento, foi encontrado um óbice: muitos colaboradores, por não terem familiaridade com o tema, responderam de forma incorreta ou incompleta, atrasando o diagnóstico e as demais etapas. Nesse ponto, vale destacar que tanto o mapeamento quanto o diagnóstico só serão perfeitamente fiéis à realidade da empresa se as respostas concedidas pelos departamentos internos contiverem todas as informações necessárias à análise. Superada essa questão, foi possível dar andamento ao registro das atividades e ao diagnóstico, que foi apresentado por meio de um relatório inicial.

ETAPA 2: Já na segunda etapa, que conta com as principais ações de implementação da LGPD, foram encontrados outros desafios. Neste momento, ressalta-se que os documentos de implementação, embora sigam um padrão pré-determinado, devem ser desenvolvidos de acordo com a realidade de cada empresa, diagnosticada na etapa anterior. Assim, a empresa "A", por ser do ramo da saúde, teve de atentar-se ao uso de Dados Pessoais Sensíveis e à elaboração de termos de consentimento para alguns tratamentos em específico. Dessa forma, conclui-se que as normas, políticas, termos e outros entregáveis pertinentes ao projeto devem seguir o padrão das boas práticas de LGPD, mas não devem ignorar as especificidades de cada organização, a fim de evitar que se tenha o que se chama de "projeto de prateleira", que poderia ser aplicado indistintamente a qualquer empresa, mas não se atenta às minúcias de cada caso.

ETAPA 3: Por fim, na etapa de monitoramento, a equipe da empresa "A" já se encontrava mais familiarizada com o tema de Privacidade e Proteção de Dados, após a experiência do projeto de adequação à LGPD. Surgiu, neste momento,

uma demanda de parceiros da organização, que solicitou o preenchimento de questionários de auditoria sobre Privacidade e Proteção de Dados. Tendo em vista que as etapas de implementação já haviam sido realizadas, bastou confirmar a existência de cada documentação solicitada, bem como enviar evidências a respeito de cada documentação, provando que o programa de adequação à LGPD já era uma realidade prática.

A partir do exemplo ilustrativo, nota-se que embora haja uma metodologia e um plano de ação bem definidos, na prática, podem surgir desafios ou demandas inesperadas, de modo que é necessário desenvolver estratégias para contorná-los, sempre tendo como base a metodologia adotada e os preceitos da LGPD.

AULA DE REVISÃO 04

Revisaremos o conteúdo visto nos módulos 10, 11 e 12.

AULA 68 - REVISÃO MÓDULO 10 - AÇÕES DE ADEQUAÇÃO À LGPD: SEGURANÇA DA INFORMAÇÃO

REVISÃO AULA 50 – PRINCIPAIS MEDIDAS TÉCNICAS PARA IMPLEMENTAÇÃO DA LGPD

- Criação de uma Política de Segurança da Informação;
- Realizar um treinamento com os colaboradores;
- Manutenção dos sistemas internos da empresa;
- Investimento da empresa em anti-spam, firewall e antivírus;
- Realização de backups periódicos;
- Criar senhas fortes e não as compartilhar;
- Elaboração de um Plano de Recuperação.

REVISÃO AULA 51 – A IMPORTÂNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- Política de Segurança da Informação tem o objetivo de estabelecer diretrizes estratégicas, responsabilidades, competências, normas e procedimentos de uso, visando assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações armazenadas pela empresa;
- Política de Segurança da Informação é uma medida necessária para o bom andamento das atividades da empresa;

- Política de Segurança da Informação é imprescindível para o sucesso do projeto de adequação à LGPD, porque viabiliza a manutenção das demais medidas de segurança implementadas durante o processo de adequação.

REVISÃO AULA 52 – OS 20 CONTROLES CIS - PARTE 1

Center for Internet Security é uma organização americana, sem fins lucrativos, que tem como objetivo promover soluções estratégicas para tornar a internet um lugar mais seguro;

O CIS apresentou um conjunto de diretrizes contendo práticas que visam aumentar a proteção de sistemas e dados, chamado: "20 Controles Críticos de Segurança". Estes vinte controles são divididos em três categorias, a saber: controles básicos (1-6), controles essenciais (7-16) e controles organizacionais (17-20). A título de exemplo, como controle básico, são seis deles:

- Inventário e Controle de Ativos de Hardware;
- Inventário e Controle de Ativos de Software;
- Gerenciamento Contínuo de Vulnerabilidades;
- Uso Controlado de Privilégios Administrativos;
- Configurações Seguras para Hardware e Software em Dispositivos Móveis, Laptops, Estações de Trabalho e Servidores;
- Manutenção, Monitoramento e Análise de Logs de Auditoria.

REVISÃO AULA 53 - OS 20 CONTROLES CIS - PARTE 2

- Sobre os Controles CIS essenciais e organizacionais, não há uma hierarquia entre eles, eis que a simples desconsideração de um Controle pode oportunizar incidentes de segurança.
- Controles Essenciais:
    - Proteções para E-mail e Navegadores Web;
    - Defesas Contra Malware;
    - Limitação e Controle de Portas, Protocolos e Serviços de Rede;
    - Recursos de Recuperação de Dados;
    - Configuração segura para dispositivos de rede, como firewalls, roteadores e switches;
    - Defesa de Perímetro;
    - Proteção de Dados;
    - Acesso Controlado com base na necessidade de saber;
    - Controle de Acesso à Rede Sem Fio;
    - Monitoramento e Controle de Credenciais de Acesso;
    - Implementação de Programa de Conscientização e Treinamento de Segurança;
    - Segurança de Software de Aplicação;
    - Resposta e gerenciamento de incidentes;

- Testes de penetração e exercícios de "Red Team".

REVISÃO AULA 54 – SEGURANÇA DA INFORMAÇÃO NA VIDA PESSOAL E PROFISSIONAL

Cuidados com a Segurança da Informação na vida pessoal são fundamentais para que o indivíduo mantenha seus dados pessoais protegidos nas interações do dia a dia.

Existem práticas que podem ser adotadas para evitar que não ocorra o roubo de dados por criminosos, a saber:

- Não clicar em links recebidos por e-mail;
- Não cadastrar informações pessoais em sites desconhecidos;
- Não utilizar software pirata;
- Utilizar um bom antivírus e o mantê-lo atualizado;
- Criar senhas complexas, com números, letras maiúsculas, minúsculas e caracteres especiais.
- Não acessar suas redes sociais em computadores desconhecidos;
- Não fornecer suas senhas a ninguém;
- Não deixar informações importantes anotadas em qualquer lugar (como post it's no monitor).

REVISÃO AULA 55 – PRINCIPAIS AMEAÇAS EM AMBIENTES LÓGICOS

- A palavra "lógicos", no dito contexto, refere-se aos softwares utilizados pelas empresas e indivíduos, isto é, os programas responsáveis pelo funcionamento das máquinas empresariais e que possuem diversas informações;
- A primeira ameaça é chamada "*phishing*", que consiste na utilização de aplicativos e sites falsos, praticamente iguais aos originais, com o simples objetivo de enganarem os usuários e ter acesso de todas as informações desejadas;
- Outra ameaça é o *Ransomware*, tem como principal função fazer a cópia das informações de um computador ou, até mesmo, de uma rede inteira. Após a realização da cópia das informações, o criminoso solicita um pagamento para devolução do que foi copiado;
- Ataques DDoS (*Distributed Denial of Service)*, traduzidos em "Ataques Distribuídos de Negação de Serviços". O objetivo de infectar hardwares, causando a indisponibilidade dos serviços para seus usuários. Uma sobrecarga é gerada em um determinado servidor ou computador comum, indisponibilizando o sistema;
- Espionagem de vítimas através da webcam e microfone do computador.

REVISÃO AULA 56 – PRINCIPAIS AMEAÇAS EM AMBIENTES FÍSICOS

- Por "ambientes físicos" entende-se os locais em que os computadores, servidores e meios de comunicação (hardwares) estão fisicamente instalados. Neste caso, as ameaças não estão na atividade virtual dos criminosos, mas sim no controle de acesso aos ambientes físicos;
- Ameaças que envolvem a estrutura física da empresa capazes de inutilizar os computadores e hardwares instalados, como: quedas de energia, incêndios etc.;
- Deve haver o controle de acessos físicos aos locais, bem como o uso de chaves nos armários e a instalação de câmeras para evitar o acesso de pessoas inadequadas às informações da empresa.

AULA 69 - REVISÃO MÓDULO 11 - AÇÕES DE ADEQUAÇÃO À LGPD: PROJETO DE ADEQUAÇÃO E DA GOVERNANÇA DE PROTEÇÃO DE DADOS

REVISÃO AULA 57 – COMO ESTRUTURAR UM PROGRAMA DE GOVERNANÇA

- Adoção de processos e políticas internas;
- Tornar o programa aplicável a todo o conjunto de dados pessoais;
- Tornar o programa adaptável;
- Estabelecer políticas e proteção adequadas;
- Estabelecer confiança com o titular;
- Integração das políticas estabelecidas;
- Estabelecer mecanismos de supervisão;
- Criação de procedimento de resposta a incidentes envolvendo dados pessoais;
- Demonstração constante da efetividade do programa;
- Publique as regras de boas práticas;

REVISÃO AULA 58 - A IMPORTÂNCIA DE SE INSTITUIR UM COMITÊ DE PRIVACIDADE

- O Comitê de Privacidade é um instrumento que promove a cultura de proteção de dados pessoais dentro das instituições;
- O comitê pode ser o responsável por levar ao conhecimento do DPO os atos de incidente de segurança da informação e/ou vazamento de dados que ofereçam risco de exposição da companhia.
- O comitê é mais um agente responsável na instituição que tem por objetivo adequar a instituição às normas e princípios listados na LGPD;

- Dentre suas atividades, destacam-se: aplicar mecanismos de supervisão internos e externos, elaboração dos planos de resposta a incidentes de segurança, gerenciar atividades relativas ao tratamento de dados.

REVISÃO AULA 59 – ETAPAS PARA IMPLEMENTAÇÃO DA LGPD PARTE 1

- Preliminarmente, é necessário buscar toda a documentação da empresa para uma análise prévia, a fim de estruturar um cronograma do projeto de adequação;
- Primeira etapa é a preparação. Podendo, mas não somente, definir a estrutura do comitê de privacidade e nomeação do DPO, mapeamento de dados, análise de gaps, análise de risco de TI etc.;
- A segunda etapa é a de Organização. Com os gaps e requisitos de adequação devidamente identificados, o projeto necessitará de um planejamento específico para determinar a forma pela qual se dará a conformidade;
- A terceira etapa é a de Desenvolvimento e Implementação. Podendo, mas não somente, adotar práticas de conformidade, implementar políticas previamente estabelecidas etc.;

REVISÃO AULA 60 - ETAPAS PARA IMPLEMENTAÇÃO DA LGPD PARTE 2

- A quarta etapa é a de Governança. Realização de auditorias e avaliações no projeto de adequação, como forma de verificar se os riscos de fato foram minimizados, eliminados ou aceitos pela organização;
- A quinta e última etapa é chamada de Avaliação e/ou Melhoria Contínua. Trata-se de técnicas de gestão de processos e qualidade para garantir que a organização esteja sempre a par das transformações que ocorrem ao longo de suas atividades.
- Após a implementação das etapas, a empresa terá robusta documentação em mãos, são alguns exemplos: Política de Privacidade, Análise de Legítimo Interesse, Política de Segurança da Informação, Relatório de Impacto à Proteção de Dados Pessoais etc.;
- Vale ressaltar que a adequação à lei é eterna, o monitoramento do projeto implementado deve sempre existir.

REVISÃO AULA 61 – DIAGNÓSTICO PARA IMPLEMENTAÇÃO DA LGPD

- Diagnóstico da maturidade da empresa quanto à Privacidade e Proteção de Dados;
- É realizado via formulários, entrevista com os colaboradores da empresa, ou então por Software específico para mapeamento dos dados;

- O nível hierárquico de cada profissional no ambiente da organização, seus setores e a relação de subordinados diretos e indiretos são parâmetros a serem considerados antes da entrevista;
- Após o mapeamento de dados, é elaborada uma matriz com o fluxo de todos os dados mapeados, viabilizando análises de risco de cada atividade, bem como a elaboração de recomendações e estratégias para mitigar as chances de um incidente;
- Deve ser desenvolvidos relatórios de diagnóstico contendo um resumo da situação atual da empresa e as principais conclusões e recomendações para o tratamento de dados.

REVISÃO AULA 62 – A IMPORTÂNCIA DE UM PLANO DE AÇÃO

- É importante a elaboração de um plano de ação definido e detalhado para a segunda etapa, logo após a fase do diagnóstico, que irá delinear o caminho a ser seguido, de acordo com a análise realizada na etapa anterior;
- O plano de ação deve atender pilares técnico, documental/procedimental e cultural/organizacional;
- Pilar técnico: medidas técnicas que devem ser adotadas para impedir violações à lei; Pilar documental/procedimental: implementação e alteração dos documentos necessários; Pilar cultural: manter cultura de proteção de dados dentro da empresa;
- O plano de ação pode conter ações estruturantes e ações específicas. Estruturantes: não possuem vínculo direto com um processo mapeado, mas que necessitam ser implementadas para adequação da empresa. Específicas: diretamente ligadas aos processos mapeados;
- O plano de ação define as ações a serem tomadas a curto e médio prazo para garantir que a adequação se concretize.

AULA 70 - REVISÃO MÓDULO 12 – COMPLIANCE E LGPD COM EXEMPLO PRÁTICO DE UM PROJETO DE ADEQUAÇÃO

REVISÃO AULA 63 – INTRODUÇÃO AO COMPLIANCE DIGITAL

- Os pilares do compliance são inerentes a qualquer projeto de adequação à LGPD;
- *Tone at the top* (o exemplo vem de cima): a alta administração deve apoiar incondicionalmente o projeto de adequação, dando o primeiro exemplo aos demais;
- *Risk Assessment* (Avaliação de Riscos): consiste no levantamento dos riscos com relação à atividade. Em relação à LGPD, a avaliação de riscos é feita no

mapeamento de dados, identificado riscos pode ser elaborado relatório de impacto, onde ficarão comprovados os riscos e as eventuais salvaguardas aptas a mitigá-lo;

- Documentação: documentos que mantem um padrão de conduta e estabelecem as penalidades aos colaboradores que não seguirem as normas internas na organização;
- Controles internos: objetivo de criar mecanismos que possibilitem à empresa alcançar seus objetivos de conformidade;
- Treinamento e comunicação: para que seja feita a manutenção da adequação à LGPD, é imprescindível que se mantenham em dia os treinamentos;
- Canais de denúncia: ferramenta essencial para manter a comunicação segura, anônima e que garanta a não identificação das pessoas que alertam sobre as atitudes que estão em desconformidade dentro de uma empresa;
- Investigações internas: se a denúncia é feita e não existe a investigação interna, nunca será possível constatar se a denúncia procede ou se a denúncia era apenas um alarme falso;
- *Due dilligence:* avaliação dos fornecedores, parceiros, revendedores, e demais empresas relacionadas à empresa;
- Auditoria e monitoramento.

REVISÃO AULA 64 – A IMPORTÂNCIA DA GESTÃO DE TERCEIROS

- Visa a assegurar um bom relacionamento com parceiros, além de viabilizar o controle e a análise de riscos, como violação de dados, descumprimento de leis e normas, riscos de contrato etc.;
    - Alguns procedimentos que podem ser adotados na gestão de terceiros seguem listados abaixo:
    - Identificar e monitorar eventuais riscos: estabelecer mecanismos de controle e monitoramento dos riscos percebidos, quando a relação com o terceiro já existir;
    - Realizar as práticas de triagem e *onboarding:* categorizar os terceiros avaliados com base em diversos critérios que serão estabelecidos de acordo com a realidade da organização. O onboarding deve englobar elementos como questionários e entrevistas que concedam as informações necessárias para o início da relação contratual;
    - Integrar os processos de gerenciamento de terceiros: unificar todos os processos;
    - Utilizar a tecnologia ao favor dos procedimentos: se possível, utilizar plataformas tecnológicas para verificação de terceiros.

REVISÃO AULA 65 – COMO MANTER UM PROGRAMA DE COMPLIANCE À LGPD

- Para estruturar o programa de Compliance de dados, cita-se vamos às recomendações da SERPRO (Serviço Federal de Processamento de Dados):
  - Análise aprofundada das leis que servem para regular o tratamento dos dados pessoais;
  - Identificação e organização dos dados pessoais, especialmente, àqueles de pessoas sensíveis e os de crianças e adolescentes;
  - Ciência ao titular dos dados pessoais sobre o tratamento que será realizado, bem como as finalidades desse tratamento;
  - Elaboração de medidas técnicas, normas e políticas que sejam complementares aos requisitos que estão elencados na LGPD;
  - A implementação de plano de formação, conscientização e capacitação dos colaboradores e terceiros;
  - Habilitar meios digitais para atender o público nas demandas de solicitação e revogação do consentimento;
  - Realizar análises de risco e avaliar falhas que possam violar direitos e liberdades das pessoas;
  - Estabelecer protocolos para gerir e notificar as brechas de segurança e vazamentos de dados;

REVISÃO AULA 66 - ESTABELECENDO O 'TONE AT THE TOP'

- É necessário que os líderes de uma empresa estejam dispostos a apoiar mecanismos de implementação de Compliance;
- A postura ética dos líderes, por meio do “tone at the top” é capaz de influenciar positivamente os comportamentos de todos os subordinados;
- A alta direção deve se responsabilizar por fomentar a comunicação e a conscientização de todos os colaboradores a respeito do tema;

REVISÃO AULA 67 - EXEMPLOS PRÁTICOS DE IMPLEMENTAÇÃO DA LGPD

- Exemplo de implementação da LGPD:
  - **ETAPA 1:** treinamento inicial > colaboradores respondem formulários de proteção de dados.
  - **ETAPA 2:** Mapeamento de dados e elaboração do relatório diagnóstico > elaboração dos entregáveis específicos para as necessidades da empresa;
  - **ETAPA 3:** Projeto já implementado. Com os documentos elaborados para a empresa, há provas de que foi e está sendo respeitada a lei.