CENTRO UNIVERSITÁRIO DO ESTADO DO PARÁ
CURSO DE BACHARELADO EM DIREITO

ANTÔNIO JOSÉ VASCONCELOS DA ROSA FILHO

# O PERIGO DA MANIPULAÇÃO DE DADOS EM MASSA NAS REDES SOCIAIS E O COMPLIANCE COMO MECANISMO DE SEGURANÇA

BELÉM
2022

ANTÔNIO JOSÉ VASCONCELOS DA ROSA FILHO

# O PERIGO DA MANIPULAÇÃO DE DADOS EM MASSA NAS REDES SOCIAIS E O COMPLIANCE COMO MECANISMO DE SEGURANÇA

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção de grau em Bacharel em Direito, pelo Centro Universitário do Estado do Pará.

Orientadora: Prof. Me. Amanda Maia Ramalho

BELÉM
2022

**Dados Internacionais de Catalogação na Publicação (CIP)**
**Biblioteca do CESUPA, Belém – PA**

R789p Rosa Filho, Antônio José Vasconcelos da.
O perigo da manipulação de dados em massa nas redes sociais e o compliance como mecanismo de segurança / Antônio José Vasconcelos da Rosa Filho. – Belém, 2022.

27 p.

Trabalho de Conclusão de Curso (Graduação) – Centro Universitário do Estado do Pará, Bacharelado em Direito, Belém, 2022.
Orientadora: Profa. Ma. Amanda Maia Ramalho

1. Redes sociais. 2. Proteção de dados. 3. Programas de compliance. I. Ramalho, Amanda Maia (orient.). II. Título.

CDD 341.5

Regina Coeli Araújo Ribeiro CRB-2/739

ANTÔNIO JOSÉ VASCONCELOS DA ROSA FILHO

# O PERIGO DA MANIPULAÇÃO DE DADOS EM MASSA NAS REDES SOCIAIS E O COMPLIANCE COMO MECANISMO DE SEGURANÇA

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção de grau em Bacharel em Direito, pelo Centro Universitário do Estado do Pará.

Orientadora: Prof. Me. Amanda Maia Ramalho

Data de aprovação: _____/_____/_____

Conceito:

**Banca Examinadora:**

_____
Prof. Me. AMANDA MAIA RAMALHO - Orientadora
Centro Universitário do Estado do Pará (CESUPA)

_____
Nome com titulação
Instituição a que pertence

_____
Nome com titulação
Instituição a que pertence

# O PERIGO DA MANIPULAÇÃO DE DADOS EM MASSA NAS REDES SOCIAIS E O *COMPLIANCE* COMO MECANISMO DE SEGURANÇA

# THE DANGER OF MASS DATA MANIPULATION IN SOCIAL NETWORKS AND COMPLIANCE AS SECURITY MECHANISM

Antônio José Vasconcelos da Rosa Filho[1]
Amanda Maia Ramalho[2]

**RESUMO**

A presente pesquisa realiza um estudo teórico sobre o perigo da manipulação de dados em massa nas redes sociais. No contexto levantado, avalia os conceitos básicos de Proteção de Dados Pessoais, e a quais riscos eles estão submetidos quando passam pelo âmbito do setor privado empresarial, em uma análise não exaustiva do assunto. Busca, a partir disso, elencar o *compliance* como mecanismo de segurança, levantando as principais ferramentas de um Programa de *Compliance* para evidenciar sua imprescindibilidade na autorregulação das companhias gestoras de redes sociais, auxiliando órgãos legitimados como a Autoridade Nacional de Proteção de Dados. A fundamentação para o trabalho é majoritariamente jurídica, tendo a Lei Geral de Proteção de Dados, a Regulamentação Geral de Proteção de Dados da União Europeia, autores da área e pesquisas bibliográficas como norteadores.

Palavras-chave: proteção de dados; redes sociais; programa de *compliance*.

**ABSTRACT**

This research performs a theoretical study on the danger of mass data manipulation in social networks. In the context raised, it evaluates the basic concepts of Personal Data Protection, and which risks they are subject to when they pass through the scope of the private business sector, in a non-exhaustive analysis of the subject. It seeks, from this point of view, to list compliance as a security mechanism, raising the main tools of a Compliance Program to demonstrate its indispensability in the self-regulation of social network management companies, helping legitimized bodies such as the National Data Protection Authority. The basis for the work is mostly legal, with the General Data Protection Law, the General Data Protection Regulation of the European Union, authors in the area and bibliographic research as guides.

Key-words: data protection; social networks; *compliance* program.

[1] Aluno do curso de graduação de Bacharelado em Direito do Centro Universitário do Pará (CESUPA), turma DI10TC, antoniojvrf@gmail.com, matrícula de número 18060181.

[2] Professora orientadora, bacharel em Direito pelo CESUPA e mestre em Direito pela UNAMA docente das disciplinas de Dir. Empresarial e Dir. de Proteção de Dados no Centro Universitário do Pará (CESUPA).

## INTRODUÇÃO

O presente trabalho tem como objetivo abordar quais são os riscos e perigos inerentes à atividade de manipulação de dados em grande quantidade, especificamente por parte de companhias responsáveis pela hospedagem de redes sociais. Em consequência à abordagem, busca também elencar o Compliance como mecanismo de segurança para prevenção e remediação dos objetos estudados. Dessa maneira, a pergunta problema da pesquisa passa a ser: como exatamente o *Compliance* pode servir como mecanismo de segurança para os riscos da manipulação de dados em massa nas redes sociais?

A problemática em questão foi investigada no interesse de compreender quais são os entraves contemporâneos que as companhias mais famosas do mundo enfrentam em termos de Proteção de Dados. No atual período, no qual vive-se a chamada Quarta Revolução Industrial, a automação e o uso dos dados no processamento empresarial torna-se imprescindível; a *internet* está em praticamente todos os lugares, e é necessária na devastadora maioria dos setores trabalhistas modernos.

Compreendendo a importância dos dados na vida em sociedade, torna-se também evidente a necessidade de uma investigação que consiga abordar os maiores riscos que esses dados correm ao serem tratados pelas empresas, de maneira que consigam se manter protegidos e resguardados, em respeito à privacidade de usuários de todo o globo.

A metodologia utilizada para o trabalho em questão calca-se no uso de pesquisa bibliográfica, em livros de autores atualizados e reconhecidos, além de *websites*. Foi-se abordado o trabalho, também, de maneira qualitativa de natureza básica, cujo objetivo é explicar o fenômeno dos riscos inerentes à manipulação de dados e delimitar o *Compliance* como mecanismo de segurança relacionado. (MARCONI; LAKATOS, 2022)

Tendo a divisão supracitada em mente, o trabalho será subdividido em duas partes. A primeira parte consistirá no ressaltar da importância da proteção de dados para o cotidiano das empresas de redes sociais, como a Meta e o Twitter, por exemplo, e abordar quais são os riscos relacionados ao manuseio dos dados de seus milhões de usuários.

Tendo o contexto em mente, o trabalho será subdividido em cinco partes. A primeira tratará do objeto de enfoque, que são os dados pessoais, fazendo um apanhado teórico dos conceitos básicos do assunto. A segunda parte tratará dos riscos em si que os dados pessoais

podem concorrer, trazendo os incidentes de segurança e o vazamento de dados como principais problemáticas enfrentadas. A terceira parte buscará apresentar a solução para a problemática dos riscos ao elencar o *Compliance* como mecanismo de segurança, destrinchando seus pormenores e compreendendo suas estratégias. A quarta parte mostrará como o *Compliance* é implementado na prática e, por fim, a quinta parte do presente artigo buscará mostrar documentações, em sede de exemplo, de mecanismos abordados no texto aplicados em empresas de redes sociais como a Meta, de Mark Zuckerberg; ao fim, se darão as considerações finais, para fechar o texto e demonstrar quais foram os resultados obtidos.

## 1. A IMPORTÂNCIA DA PROTEÇÃO DOS DADOS PESSOAIS

Os dados representam, na atualidade, um dos bens mais valiosos não apenas para o capitalismo, mas para a própria vida em sociedade. Desde 2017, por força da publicação de um texto jornalístico da The Economist, são constantemente comparados ao petróleo, que é uma das commodities mais valiosas do mundo. Não à toa, "O recurso mais valioso do mundo não é mais o petróleo, mas sim os dados" (ECONOMIST, 2017) foi a manchete para a opinião emitida. Deles, se conseguem precisar indivíduos, grupos, culturas e até países, na medida em que há uma infinidade de dados que podem ser extraídos de seus objetos de análise. Seu valor para os negócios é visto através do uso da Big Data[3], que pode ser utilizada para conhecer os clientes e consumidores no mercado e predizer, através de algoritmos, o que eles querem.

Para as redes sociais, a dinâmica é ainda mais intensa. A quantidade de informações é tamanha que, desde sua criação, as companhias modernas que hospedam esses tipos de site buscam crescer continuamente seus investimentos em capacidade de armazenamento de dados, algoritmos e programação complexa para seus servidores. Análises da empresa de marketing digital Kepios (2022, online) mostram que, no mundo, existem 4.76 bilhões de usuários de redes sociais em 2022; isso é o equivalente a mais da metade da população global. Esse número mostra como essa modalidade de negócio digital é parte da vida de muitas pessoas.

No Brasil, não é diferente. Dados mostram que o Brasil está em segundo lugar no ranking de países que mais usam redes sociais diariamente (SORTLIST, 2022, online). São informações que tornam nítida a presença das redes sociais nas vidas das pessoas. Por sua vez, essa presença também demonstra que, por outro lado, as empresas detém grandes quantidades

[3] Big Data é tido como sendo uma grande fonte de dados digitais passíveis de estudo, análise e categorização (CETAX, 2022, online).

de dados de uma ampla gama de pessoas, uma vez que alguns desses dados são requisitos mínimos necessários para poder utilizar-se das redes para se comunicar com os demais.

Com base nessas informações, pode-se compreender que no Brasil e no mundo, dados pessoais dos usuários, aqui chamados de titulares, estão sendo tratados constantemente pelas empresas e seus empregados, aqui chamados de controladores e operadores. Esses são termos técnicos utilizados pela Lei Geral de Proteção de Dados Pessoais e pela Agência Nacional de Proteção de Dados, que são, respectivamente, a legislação e o ente legitimado que versam sobre o tema (BRASIL, 2018).

Dados pessoais voltados para as redes sociais podem se subdividir em duas modalidades. São eles os dados pessoais de modo geral, já anteriormente conceituados, e os dados pessoais sensíveis, que segundo o Art. 5º, inciso II da LGPD, são dados

> sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. (BRASIL, 2018, online)

Esses são os principais tipos de dados que circulam nas redes sociais, e basta analisar o fato de que a rede social Instagram suportava, em 2016, o upload de 95 milhões de imagens por dia (WOOLASTON-WEBBER, 2016) para constatar o quanto as mídias visuais são poderosas — presume-se com facilidade que conteúdos políticos, religiosos e de gênero estão entre os mais difundidos, e eles, conforme estatuído pela LGPD, são também dados sensíveis.

Em fevereiro de 2022, a Câmara e o Senado Federal aprovaram o texto da Emenda Constitucional nº 115, que traz, agora, no Art. 5º, inciso LXXIX, como direito fundamental o da proteção dos dados pessoais, sejam através de meios físicos ou digitais. A mesma Emenda também trouxe à União a competência para legislar e tratar sobre a proteção dos dados pessoais, garantindo a uniformidade da palavra constitucional com a Lei Geral de Proteção de Dados (BRASIL, 2022).

## 2. RISCOS INERENTES À MANIPULAÇÃO DE DADOS EM MASSA NAS REDES SOCIAIS

A navegação em qualquer rede social requer que o usuário forneça seus dados para a criação de sua conta pessoal. Isso, pois esses *websites* são necessariamente uma espécie de

réplica dos círculos sociais da vida real, e implica-se, então, na personificação, ainda que virtual, de uma persona identificável. Para tal, dados pessoais são obrigatórios, sendo alguns exemplos o nome, idade e sexo. Ao fornecer esses dados para a empresa, eles são imediatamente processados, muitas das vezes de formas automáticas, através de algoritmos e cookies. Em dado momento, eles passam pelos terminais dos operadores de dados, que programam os códigos do *back-end*[4] para que o fluxo de dados seja feito da forma mais automatizada, ágil e eficaz o possível (BATISTELLA, 2021).

Durante o percurso dos dados adquiridos é que os riscos aparecem. Quando se fala em manipulação de dados, utiliza-se como sinônimo o conceito de tratamento de dados, cuja ideia principal está no Art. 5º, inciso X, da LGPD, que é definido como sendo:

> 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; (BRASIL, 2018, online)

Dessa maneira, operadores e controladores podem trabalhar com os dados dos titulares da maneira que bem compreenderem, dentro de um escopo específico, todavia, de interesses, normas e determinações regulatórias delimitadas.

## 2.1. INCIDENTES DE SEGURANÇA

A LGPD define, no Art. 46, que os chamados incidentes de segurança nada mais são do que o "acesso não autorizado aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" (BRASIL, 2018, online). A partir desse conceito, Carlos Affonso de Souza, pesquisador da área, suscita em seu artigo o levantamento feito pelo Grupo de Trabalho do Artigo 29, composto por autoridades europeias na área, que foi capaz de organizar e estruturar objetivamente os incidentes de segurança da seguinte maneira:

> (i) incidente de confidencialidade: quando há acesso e/ou divulgação não autorizada de dados pessoais; (ii) incidente de integridade: quando há alteração não autorizada de dados pessoais; (iii) incidente de disponibilidade: quando há perda de acesso ou destruição de dados pessoais (SOUZA, 2020, p. 428)

[4] Back-end é o termo utilizado para se referir aos "fundos" de determinado website, ou seja, seus servidores e os demais setores onde os dados são manejados.

Diante disso, é possível entender que uma série de espécies de incidentes existem. Mas nem todos possuem importância ou são tão recorrentes no âmbito das redes sociais; isso se mostrará através dos dados e estatísticas recolhidas para o tópico seguinte. A partir desse entendimento, compreende-se que o mais completo e perigoso risco a ser enfrentado é, sem sombra de dúvidas, o vazamento de dados.

## 2.2. VAZAMENTO DE DADOS

Os vazamentos de dados, também chamados de *Data Leak*, são um dos, senão o maior dos perigos e riscos encontrados na manipulação das grandes quantidades de dados que as redes sociais possuem. Seguindo o parâmetro de incidentes de segurança explicitado no tópico anterior, sua significância é tamanha que, segundo dados da empresa de segurança cibernética Syhunt, mais de 227 milhões de brasileiros — entre pessoas vivas e falecidas — tiveram seus dados pessoais vazados em ações criminosas expostas na Deep Web[5] (SYHUNT, 2021, online).

Eles são a exposição de dados pessoais e de outros dados de caráter sigiloso dos bancos de dados das empresas para terceiros ou hospedados na *Internet*. Decorrem, majoritariamente, de ações criminosas, como invasões hacker, mas também podem acontecer por intermédio de acidentes e falhas operacionais internas da companhia.

De acordo com a Cartilha de Segurança para Internet: Vazamento de Dados[6], o vazamento pode ser originado de uma série de fatores:

- "do furto de dados por atacantes e códigos maliciosos que exploram vulnerabilidades em sistemas
- do acesso a contas de usuários, por meio de senhas fracas ou vazadas
- da ação de funcionários ou ex-funcionários que coletam dados dos sistemas da empresa e os repassam a terceiros
- do furto de equipamentos que contenham dados sigilosos

[5] Deep Web foi um termo inventado por Michael Bergman em 2001 para se referir a uma área da Internet que não pode ser acessada através de métodos convencionais, como simplesmente indo aos motores de pesquisa, recorrentemente associada, também, a sites anônimos e de difícil acesso que reúnem conteúdos ilícitos e criminosos de toda sorte (GLOBO, 2019).

[6] A cartilha foi criada para que se pudesse compreender o significado de vazamento de dados, como ocorre e através de quais agentes se dá de modo objetivo e acessível. Foi desenvolvida pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT), em colaboração com a ANPD.

- de erros ou negligência de funcionários, como descartar mídias (discos e pen drives) sem os devidos cuidados" (CERT, 2021, online)

A partir dessas origens, pode-se depreender que uma série de dados pessoais e sensíveis podem estar expostos, a depender do conteúdo que possuem. Podem ser credenciais, informações identitárias, financeiras, e a depender do tipo de empresa que sofre o vazamento de dados, conteúdos como registros de saúde e contratos empresariais mantidos sob sigilo também podem estar à disposição do vazamento.

Nesse entendimento, tem-se o vazamento de dados como o maior risco que qualquer empresa que esteja gerindo uma rede social é capaz de correr. Afinal, as redes sociais trabalham com contas *online*, e um vazamento desse nível pode levar a várias consequências graves, como:

a) crime de falsidade ideológica, que ocorre quando terceiros criam uma conta no nome de alguém que teve seus dados vazados;

b) fraudes e golpes, que ocorrem quando terceiros, ciente de dados pessoais sensíveis, buscam ludibriar ou manipular cidadãos vulneráveis para que, por exemplo, movimentem, quantias em dinheiro para os criminosos, que se passam por familiares e amigos íntimos. Extorsões também se encaixam nessa categoria;

c) abertura não-autorizada de contas e contratação de serviços no nome de quem teve os dados vazados, que pode ocasionar, por exemplo, gastos financeiros e uso exagerado de crédito do titular dos dados, deixando-o com dívidas exorbitantes;

Diante de todos esses riscos e perigos, urge a necessidade de uma política empresarial interna que consiga evitar ao máximo possível que tais eventos aconteçam. Quando um incidente de segurança dessa magnitude acontece, o Art. 48 da LGPD obriga o controlador de dados a comunicar o ocorrido à ANPD em prazo razoável, indicando uma série de características que dizem respeito ao vazamento em questão. A previsão é adequada, mas atinge tão somente a esfera da responsabilidade civil do controlador de dados perante a agência. (BRASIL, 2018)

Pode-se observar, como um exemplo clássico, utilizado como parâmetro para se observar o prejuízo que o vazamento de dados pode causar, a situação pela qual a empresa *Facebook* passou nos últimos anos. Segundo notícia veiculada no portal do Ministério da Justiça e Segurança Pública, órgão do Governo Federal, a empresa em questão foi condenada a pagar R$6.600.000,00 (seis milhões e seiscentos mil reais) como multa pelo vazamento de dados de

usuários em 2018. O caso tornou-se famoso em razão de seu dano especulado: presume-se que o repasse de informações da empresa Cambridge Analytica possa ter influenciado diretamente as eleições presidenciais dos EUA em 2016 (GOVERNO FEDERAL, 2022).

## 2.3. OUTRAS ESPÉCIES DE INCIDENTES DE SEGURANÇA

Os vazamentos de dados são a principal problemática da cibersegurança contemporânea nas companhias que hospedam redes sociais, mas há muitos outros tipos de incidentes de segurança listados. No presente trabalho, busca-se elencar o conceito basilar do objeto de risco e sua principal espécie, mas também torna-se necessário listar, de forma não exaustiva e tão somente exemplificativa, algumas outras modalidades de incidentes de segurança existentes.

Dentre as quais pode-se compreender, dada a extensão do tema, têm-se a destruição dos dados. É quando, por algum motivo, seja acidental ou não, o controlador ou o operador de dados acabam fazendo o dado deixar de existir absolutamente; o que concorre com o incidente de alteração irreversível de dados, uma vez que, para se destruir uma informação, ela precisa necessariamente ser alterada. Carlos de Souza faz um paralelo entre ambos ao asseverar que podem ambos serem constatados ao se verificar que as informações inseridas em determinado banco de dados tornaram-se corrompidas, ilegíveis ou inúteis aos interesses do controlador e do operador por influência externa (SOUZA, 2020).

Outra espécie de infração conhecida e relativamente famosa é a perda de acesso aos dados. Diferente da destruição, que trata estritamente sobre o dado em si, esse objeto trata-se da perda da capacidade de acessar os bancos de informações nos quais os dados dos titulares estão disponíveis. Isso significa que o local onde as informações estão armazenadas pode estar intacto, tal como elas próprias, mas o controlador e o operador de dados são incapazes de tê-los sob sua dominância. Tal espécie é levantada por Carlos de Souza tendo como exemplo os ataques de terceiros do tipo *ransomware*, que são, em suma, o sequestro de dados e o bloqueio do acesso a eles, de modo que só poderão ser acessados mediante pagamento de resgate (SOUZA, 2020).

O autor supra referenciado finaliza sua listagem nos conformes do que conceitua o Art. 46 da LGPD, que é com o tratamento inadequado ou ilícito dos dados pessoais. Sem evidentemente exaurir o tema, esse é um dos incidentes mais abrangentes e abstratos que há. É dessa forma pois cobre, tecnicamente falando, tudo que esteja em desconformidade com as

sugestões e normas legais da LGPD, da ANPD e até mesmo do *padrão-ouro* internacionalmente reconhecido — a GDPR. Pode acontecer quando, por exemplo, um agente do setor X utiliza meios inadequados para obter acesso não autorizado aos dados pessoais recolhidos pelo setor Y. Isso recai em violação das hipóteses de autorização do tratamento de dados constantes no Art. 7º e subsequentes incisos. Torna-se um incidente ainda mais grave quando o uso desses dados destina-se a fim ilegítimo e não consentido (BRASIL, 2018).

Esses incidentes constam em previsão na Lei Geral de Proteção de Dados, e é possível observá-los recaindo sobre as redes sociais e sua manipulação de dados em larga escala. Parte dessa constatação foi evidenciada no uso de casos problemáticos como os da Meta, em etapa anterior do presente artigo, mas poderá ficar ainda mais clara no decorrer dele.

## 3. O *COMPLIANCE* COMO PRINCIPAL FERRAMENTA DE COMBATE À MANIPULAÇÃO DE DADOS EM MASSA NAS REDES SOCIAIS

Abordados os riscos, passa a surgir a necessidade de um conceito dúplice que consiga refrear e diminuir, na medida do possível e mantendo os princípios de boa-fé objetiva e o dever de segurança que a LGPD estatui. O Poder Público fez isso com a criação da anteriormente citada Autoridade Nacional de Proteção de Dados, que mais recentemente tornou-se uma autarquia de natureza especial, dotada de ainda mais poderes decisórios e de autonomia própria.

Apesar disso, o setor privado também necessita de enfoque, na medida em que as instruções normativas, ISOs como a 27003:2013, e demais regras da ANPD não conseguem regular empresas a nível organizacional. Com isso, surge a autorregulação da atividade empresarial, que nada mais é do que a implementação de práticas e regulamentos que consigam fazer da empresa algo capaz de ser gerido e organizado por dentro, levando em conta princípios como eficiência, segurança e outros (BIONI, 2020) para que o cumprimento das leis orquestradas pelo Poder Público seja efetivado.

O instrumento de autorregulação que será abordado para discutir como combater e atenuar os riscos anteriormente descritos será o *compliance.* Ele é, de acordo com Ana Frazão, conforme citado pela mesma autora em obra separada, feita em conjunto com Oliva e Abilio (2020, p. 675): :

> conjunto de ações a serem adotadas no ambiente corporativo para que se reforce a anuência da empresa à legislação vigente, de modo a prevenir a

> ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno à normalidade e legalidade.

Com esse conceito, pode-se compreender que o programa de compliance, que é tido como sinônimo de programa de conformidade ou de governança, busca deixar a sistemática organizacional da empresa de acordo com a normatividade legal ao utilizar, como carro-chefe, com dois planos de ação diferentes: prevenir e remediar.

A Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados, estabelece, em seu Art. 50, os requisitos e exigências mínimas que as empresas devem possuir para operarem em conformidade com a lei, isto é, com um adequado programa de *compliance*:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
>
> § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.
>
> § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
>
> I - implementar programa de governança em privacidade que, no mínimo:
>
> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
>
> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
>
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
>
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
>
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
>
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

> g) conte com planos de resposta a incidentes e remediação; e
>
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas; (BRASIL, 2018, online)

A prevenção que o *Compliance* possui com relação aos riscos explicitados se dá através da criação de estratégias voltadas para as raízes da criação dos conteúdos formais e materiais informáticos das redes sociais. Ele pode existir através de múltiplas maneiras, mas duas delas são as principais e mais fundamentais: a) *privacy-by-design*, e b) a regulamentação empresarial e as normas éticas de conduta.

A remediação, por outro lado, estabelece-se através da suposição de que nenhuma empresa é absolutamente imune a erros e riscos a serem enfrentados, e isso é inerente à atividade empresarial contemporânea. Diante desse desafio, ferramentas são utilizadas para que os operadores e controladores de dados consigam lidar com a implementação de novas ferramentas de negócio, sejam capazes de coordenar e organizar o fluxo de dados e estejam sempre aptos a identificar e amenizar os danos e riscos que as companhias estão passíveis de sofrerem. Aplicando-se ao ramo do desenvolvimento de redes sociais, três principais mecanismos voltados para a remediação e enfrentamento dos riscos da manipulação de dados são: a) o Registro de Operações, b) a Análise de Risco e c) o Relatório de Impacto.

### 3.1. *PRIVACY-BY-DESIGN*

Para prevenir que os riscos explicitados acima sejam prejudiciais ao titular dos dados manipulados ou que a pessoa jurídica lidando com eles seja lesada, torna-se imprescindível a ênfase no código como um dos principais mecanismo de segurança da informação na leva do que é abordado no presente artigo. O código, isto é, a arquitetura dos alicerces sobre os quais os *websites* das redes sociais são construídos precisam estar em conformidade com uma cultura de códigos limpos, éticos e que consigam antecipar e evitar eventuais falhas.

Frazão, Oliva e Abílio (2020, p. 701) evocam Lawrence Lessig[7] em sede de elucidação ao abordarem o tópico:

> Como aponta Lawrence Lessig, o papel da arquitetura, ou seja, do código, é fundamental para a regulação jurídica do ciberespaço, pois de nada adianta que a lei e outras formas de regulação, como os programas de compliance,

[7] Lawrence Lessig é um professor de Harvard, pesquisador da área de Segurança da Informação, criador da licença de direitos autorais Creative Commons e um dos maiores nomes no contexto da internet livre e segura.

> contemplem determinadas regras se a arquitetura pode torná-las ineficazes ou mesmo levar a resultados opostos.

Os autores asseveram, a partir do que é depreendido no tópico, a importância da adoção de ferramentas tecnológicas e empregados que consigam estar cada vez mais atualizados quando a matéria é proteção de dados. As arquiteturas que definem, por exemplo, quais conteúdos serão mostrados aos usuários no *feed* de notícias, ou que estabelecem normas e parâmetros de privacidade para conteúdos de terceiros, como *quizzes* (aqui cabendo lembrar do infame This Is Your Digital Life, anteriormente citado como um dos causadores do escândalo da Cambridge Analytica) e propagandas.

Na medida do que estabelece Carlos Affonso Pereira de Souza, cujo artigo encontra-se presente ainda no livro Lei Geral de Proteção de Dados, o *privacy-by-design* foi definido por Ann Cavoukian, ex-comissária de Informação e Privacidade da Província de Ontário, no Canadá. A autoridade no assunto, citada por Carlos Affonso, evoca a importante ideia de que:

> Um fator importante no conceito de privacy-by-design é o fato de que a proteção de dados não será apenas assegurada pelo cumprimento de parâmetros regulatórios, mas sim por meio de um repensar por parte do agente de tratamento de dados sobre como a sua atividade pode impactar o usuário e terceiros e traduzir isso em medidas que transformam os processos de criação, desenvolvimento, aplicação e avaliação de produtos e serviços. (SOUZA, 2020, p. 423)

Diante disso, o autor demonstra que o conceito acima faz parte de um projeto que precisa estar em constante adaptação, mas que prioriza a prevenção acima da reatividade. Ann Cavoukian, ainda referenciada, sugere que sete princípios sejam imprescindíveis para a aplicação de um programa de conformidade que consiga estabelecer o *privacy-by-design* apropriadamente, sendo eles:

> (i) proatividade e prevenção; (ii) privacidade por padrão; (iii) privacidade incorporada ao design; (iv) funcionalidade integral; (v) segurança em todo o ciclo de vida da informação; (vi) transparência e (vii) respeito à privacidade do usuário. (SOUZA, 2020, p. 424)

Esses princípios são definidos e destrinchados de forma mais aprofundado no texto-base, mas para a ênfase nas redes sociais, conforme proposto pelo presente artigo, torna-se necessário compreender tão somente por alto a definição de cada um deles, de maneira que se possa aplicá-los no contexto em tela.

O primeiro princípio trata da necessidade de uma estratégia regulatória que seja capaz de "antecipar os riscos à privacidade" (SOUZA, 2020, p. 424), tornando a evitá-los. A

arquitetura do sistema sob o qual a empresa opera deve estar pronta para identificar, avaliar, antecipar e se preparar para todos e quaisquer riscos existentes. Há de se ressaltar, aqui, a importância dos princípios contidos no Art. 6º da LGPD, que tratam justamente da segurança e prevenção aos riscos corridos.

O segundo versa sobre a "máxima de que nenhuma ação por parte do indivíduo deve ser necessária para proteger sua privacidade" (SOUZA, 2020, p. 424). Isso significa que o ônus da responsabilidade no que diz respeito à privacidade está com o agente que está gerenciando o tratamento de dados, e não com o titular deste — isto é, o usuário. Trazendo para o âmbito das redes sociais, pode-se deduzir que esse princípio aplica-se, de maneira bem simples, com um exemplo: redes sociais como Facebook e Twitter, sob posse de um forte programa de *compliance* que esteja aplicando o *privacy-by-design* como um de seus mecanismos de segurança, são responsáveis por assegurar os dados dos titulares, tal como seu tráfego no *website*, com redes de servidores seguros, confiáveis e sem brechas. Esse ônus não cabe ao usuário, nesse caso; não é dele o dever de usar um VPN *(Virtual Private Network)*, ou algum outro mecanismo de privacidade, para acessar a rede social. O que corrobora com essa concepção, na legislação brasileira, de acordo com Carlos de Souza, é o Art. 46 da LGPD, além do princípio da necessidade e o princípio da responsabilização (SOUZA, 2020).

O terceiro princípio trata sobre a necessidade da privacidade estar intrinsecamente ligada ao *design* do produto ou serviço ofertado. Para a problemática em tela, traduz-se no emprego da criação de jornadas de desenvolvimento, dentro dos times de programadores das redes sociais, que pensam em *features*[8] novas que, desde o começo, valorizem a privacidade e a segurança.

O quarto princípio aborda os conceitos de funcionalidade total, que é a ideia de que todos os elementos envolvidos nos interesses e objetivos da empresa estejam de acordo com a LGPD em uma proteção dúplice, isto é, que consiga satisfazer os interesses tanto dos controladores quanto dos titulares de dados .

O quinto princípio é o da segurança de ponta a ponta, que estabelece a ideia de que o ciclo pelo qual os dados dos titulares passam precisa estar seguro em todas as suas etapas. Esse

[8] *Feature* é o nome dado à funcionalidade, ferramenta ou experiência nova pensada, desenvolvida e entregue ao usuário final na plataforma; o termo é recorrentemente empregado dentro da cultura de trabalho de desenvolvedores de *software* do ramo internacional.

é crucial para as redes sociais, uma vez que o direito ao esquecimento está previsto na LGPD, este sendo uma das importantes etapas de todo o processo. Dado o fato de que as redes movimentam milhões de dados e informações diariamente (conforme exposto na introdução do trabalho), torna-se imprescindível atrelar o programa de *compliance* ao princípio que demanda segurança da informação desde a concepção do dado até sua eliminação.

O sexto princípio, conforme Ann Cavoukian disseca, ainda dentro da dissertação de Carlos Affonso de Souza, está intimamente ligado aos princípios-padrão da LGPD, sendo os principais evocados os da "*finalidade, adequação, livre acesso e transparência*" (SOUZA, 2020, p. 425). Ele é, logicamente, o princípio da transparência, com o qual usuários finais das redes sociais, assim como seus provedores, podem estar integralmente à par das políticas e medidas de segurança tomadas. É um princípio comumente visto na documentação de Política de Privacidade, que busca tornar visível aos titulares de dados quais procedimentos são tomados e por onde passam, via de regra, os dados dos usuários.

O sétimo e último princípio utiliza o termo em inglês *"user-friendly"* para definir a importância de "padrões de privacidade fortes, avisos apropriados e opções fáceis de serem utilizadas" (SOUZA, 2020, p. 426). Trata, nesse sentido, da criação de um *design* de interface amigável, que possa mostrar de forma clara, concisa e objetiva ao titular dos dados como a segurança da informação é feita no decorrer da manipulação dos dados que a empresa executa.

Dentro do escopo de princípios que Carlos Affonso de Souza traz, em referência à pesquisadora Ann Cavoukian, pode-se entender que o *privacy-by-design* é um mecanismo de segurança robusto, que busca trazer uma série de ferramentas interessantes à prevenção dos riscos que os dados concorrem quando dentro das redes sociais.

## 3.2. NORMAS ÉTICAS DE CONDUTA

Vê-se que, na prevenção, a utilização de ferramentas materiais aptas a tornar o programa de *compliance* efetivo é constante. Uma questão surge, todavia, no momento em que estamos falando de manipulação de dados; o aparato humano também precisa ser valorizado na hora de estruturar mecanismos de segurança e privacidade da informação. A melhor maneira pela qual isso pode ser realizado é através das normas de conduta e de ética empresarial, que valorizam os recursos humanos e os tomam como objeto de enfoque.

Os Códigos de Ética e de Conduta, na leva do que conceitua o autor citado constantemente no presente tópico, nada mais são do que documentações que mostram quais são os valores, princípios e comportamentos adequados que funcionários da empresa devem seguir. Também torna explícito quais manejos no tratamento de dados e no exercício das funções é terminantemente proibido, mostrando, assim, o que deve ser feito, e o que não deve. Precisam ser de linguagem clara, objetiva e acessível, para que todos os colaboradores sejam capazes de interpretá-los e segui-los. Além do mais, é de suma importância que seja de fácil acessibilidade, tanto físico quanto digitalmente, de maneira que os empregados sejam capazes de lê-lo a qualquer momento.

Cabe, em sede de normas empresariais e gestão administrativa, citar a Política de Segurança da Informação, também chamada de PSI. Segundo Souza (2020, p. 430), seu conceito é trazido da maneira a seguir:

> Trata-se de documento que apresenta as diretrizes para garantir a segurança das informações, prescrevendo ações, proibições, boas práticas e até mesmo sanções. Em outras palavras, a PSI funciona como um código de conduta a ser seguido pelos funcionários [...]

Com o que é citado, depreende-se que documentos específicos precisam existir para traçar com exatidão qual é a rota ideal que o colaborador deve traçar para atingir a finalidade do programa proposto. O operador ou controlador de dados, porém, é um recurso humano — o que faz dele um elemento no âmbito empresarial que precisa aprender para exercer. A partir disso, surge a importância do treinamento, uma vez que a eficiência do *compliance* depende de funcionários capazes, inteligentes e com os conhecimentos necessários para empregarem, em sua rotina, as normas de conduta referidas.

Frazão, Oliva e Abílio (2020) conseguem definir bem que os treinamentos de todos os funcionários precisam ser divididos em etapas, segmentando também setores para que os com maior risco tenham treinamentos mais avançados e complexos, enquanto que setores de baixo risco de incidentes de segurança possam ter treinamentos mais leves. Para além disso, os treinamentos precisam ser constantes, se aterem às linguagens específicas de cada segmento dentro da empresa e, acima de tudo, adaptativos, uma vez que novas ferramentas e mecanismos vão sendo implementados.

## 3.3. ANÁLISE DE RISCO

Foi esclarecido que dados estão, sempre que diante de um controlador e operador de dados, sob perigo constante. E esse risco, sem sombra de dúvidas, para a manutenção da conformidade da rede social com um programa de *compliance*, precisa ser mapeado; é aí que surge a Análise de Risco, um dos pontos fundamentais para a construção de uma estratégia adequada de governança corporativa. Sendo um dos pontos centrais de toda a esquemática de controle e gerenciamento dos riscos concernentes à manipulação dos dados, a análise de risco pode ser conceituada a partir do trecho a seguir:

> A análise de risco constitui um dos elementos essenciais de um programa de compliance: caso não executada de forma adequada, poderá representar a inefetividade dos mecanismos implementados, o objetivo é tentar antecipar as principais áreas de exposição da pessoa jurídica para que sejam tomadas medidas preventivas proporcionais aos riscos identificados. (FRAZÃO; OLIVA; ABÍLIO, 2020, p. 679)

A partir desse conceito, pode-se entender que as áreas de exposição da empresa a ser tratada precisam ser mapeadas e bem definidas. Deduz-se, portanto, a necessidade de uma compreensão integral do fluxo de dados dentro do âmbito interno empresarial, definindo por onde os dados dos titulares passam e como seu ciclo se estabelece.

## 3.4. RELATÓRIO DE IMPACTO (RIPD OU DPIA[9])

O Relatório de Impacto é um documento previsto no Art. 35º do GDPR e no Art.5º, inciso XVIII da LGPD, que trata sumariamente da dissecação por escrito do controle das atividades e funções da empresa que podem ou não botar em risco os dados pessoais dos usuários. Ele considera, de acordo com o que estabelece Luca Belli, em seu artigo incluso no livro Tratado de Proteção de Dados Pessoais, a análise sistemática de ferramentas e processamentos que o controlador de dados está implementando ou planeja implementar em um futuro próximo (BELLI, 2020). Se considera, na documentação em questão, a probabilidade e a gravidade do impacto dessas modalidades de manipulação de dados para os titulares.

A mitigação dos riscos concorridos, recolhidos e organizados previamente por uma sucinta Análise de Riscos, obedece a um critério elencado por Belli como sendo "não exaustivo". Precisa conter, invocando o Art. 38º da LGPD para fundamentar o que segue, a) a descrição dos dados coletados, b) a metodologia selecionada para a coleta e segurança dos

[9] Sigla em inglês para o termo em questão, que por extenso é Data Protection Impact Assessment.

dados, c) a análise do controlador a respeito do assunto e d) quais são as medidas que estão sendo, ou serão tomadas para mitigar e evitar os riscos que a empresa está correndo (BELLI, 2020).

O Relatório de Impacto, portanto, constitui elemento imprescindível à análise do comportamento empresarial como um todo. Para as redes sociais, é ainda mais importante, uma vez que, lidando com um setor de desenvolvimento *web*, muitas funcionalidades e ferramentas estão em fase de concepção e precisam passar por uma análise minuciosa. Somente assim serão capazes de serem implementadas com sucesso, de maneira a causar o menor risco possível — ou podem até ser descartadas, caso o risco concorrido seja desnecessário para a empresa. De todo modo, são essas opiniões e avaliações técnicas que estão presentes no RIPD, e que precisam ser levadas em conta quando o controlador de dados toma decisões a respeito dos dados em massa recolhidos dos usuários.

Selma Carloto, em seu livro Lei Geral de Proteção de Dados, estabelece um forte e adequado modelo de Relatório de Impacto, onde além de todas as informações acima citadas, uma série de outros detalhes relevantes, também exigidos pela GDPR, aparecem. No conteúdo, é possível analisar pontos a serem elaborados como minimização de dados, necessidade de processamento, limitação no armazenamento, qualidade dos dados, listagem completa dos operadores e controladores dos dados tratados, se há transferência internacional dos dados dos titulares. Consta, também, o mais importante: se a operação ou as operações, e caberia um RIPD tanto para uma implementação específica quanto para uma implementação em larga escala, possui riscos; quais são, se há contramedidas, nível do risco, e mapeamento gráfico completo dele em todas as áreas onde a RIPD busca abranger (CARLOTO, 2022).

### 3.5. REGISTRO DE OPERAÇÕES (ROPA)

O Registro de Operações, conhecido pela sigla ROPA, que em inglês é *Record of Processing Activities*, é uma documentação exigida pela GPDR no Art. 30º e pela Lei Geral de Proteção de Dados em seu Art. 37º, que explicita que "o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem". Mariana Gonçalves, mestre e pesquisadora no tema, aborda que o registro de operações justifica-se através do fato de que é necessário, para o funcionamento de todos os outros mecanismos de *compliance*, uma documentação que identifique quais dados pessoais são tratados, se são sensíveis ou não e quais suas fundamentações legais para autorização de tratamento (CARLOTO, 2022).

O ROPA, de maneira objetiva, também enseja atingir outras finalidades, quais sejam demonstrar aderência aos princípios da LGPD, ser capaz de atender apropriadamente as solicitações dos titulares para com os encarregados e ser capaz de aplicar de forma correta todos os outros mecanismos de segurança do programa de conformidade. Os princípios a serem atendidos são essencialmente dois: a) o da transparência, pois a empresa que adere ao ROPA para todos os seus segmentos é capaz de mostrar às autoridades e aos sócios gestores, quando necessário, todas as suas operações e atividades de forma clara e detalhada, e b) o da responsabilização, pois a legislação prevê sanções para a infringência dos incidentes de segurança, e torna-se imprescindível saber qual foi o agente interno responsável pelo cometimento, doloso ou não, dos atentados contra a palavra legal da LGPD.

A documentação em questão também coopera diretamente com as atividades do encarregado de dados, cuja existência está prevista no Art. 41 da LGPD. Ele é responsável por recepcionar reclamações, comunicações e ser a "ponte de diálogo" entre a empresa, a autoridade legitimada e o titular dos dados. Seu trabalho torna-se muito mais ágil e eficiente quando ele possui acesso a um ROPA adequado e nos conformes do programa a ser implementado, uma vez que ele torna a saber, por exemplo, por onde os dados de determinado titular, reclamando na ouvidoria da empresa, passaram, e onde estão; o encarregado, com o documento em questão, também pode responder na justiça e ser obrigado a mostrar, para o magistrado competente, por onde dados de cidadãos do polo ativo ou passivo de processos judiciais passaram.

A gama de possibilidades, para o ROPA, é vasta. Ele também torna-se crucial para a aplicação de programas de conformidade, independente do porte da empresa na qual serão aplicados. Afinal de contas, é através do mapeamento do fluxo de dados, também capaz de ser feito com esse instrumento, que estratégias como o *privacy-by-design* e treinamentos podem ser realizados.

## 4. FASES DA IMPLEMENTAÇÃO DO PROGRAMA DE *COMPLIANCE*

Selma Carloto também possui, em seu livro, uma explicação extensa para a aplicabilidade de um programa de compliance na prática. Ela o utiliza em sede exemplificativa, evidentemente, mas todas as instruções pela autora passada estão condizentes com a palavra da Lei Geral de Proteção de Dados e podem ser divididas e abordadas, de maneira objetiva para o contexto dos programas de conformidade das redes sociais.

A autora utiliza a estruturação do professor John Kyriazoglou[10] para subdividir a aplicabilidade do programa em questão em cinco fases. De acordo com Carloto (2022, p. 240), são:

> Fase 1: Preparação da privacidade e proteção de dados;
>
> Fase 2: Organização da privacidade e proteção de dados;
>
> Fase 3: Implementação da privacidade e proteção de dados;
>
> Fase 4: Governança da privacidade e proteção de dados;
>
> Fase 5: Avaliação e melhoria da privacidade e proteção de dados

Torna-se necessário explicar, de forma sucinta, cada uma das fases, de modo a compreender-se como o programa de *compliance* é aplicado, através desta metodologia.

## 4.1. PRIMEIRA FASE: PREPARAÇÃO DOS DADOS

A primeira fase versa sobre, conforme seu nome fala, a preparação dos dados. É preciso determinar metas, objetivos e coleta extensa da legislação, seja da Constituição Federal, da LGPD, dos regulamentos da ANPD e até mesmo as exigências *padrão-ouro* da GPDR. A criação de um comitê de privacidade é importante nessa etapa, preferencialmente com o DPO[11], os encarregados e controladores de dados, além de figuras de competência do setor jurídico da empresa. Esse comitê será responsável pelo exercício de uma auditoria preliminar, para constatar quais são os dados tratados, por onde passam, e mapear todo o fluxo de dados empresarial.

Além disso, ainda na primeira fase de implementação, também farão um inventário dos dados pessoais (IDP), que será a documentação que elencará quais dados existem manipulados na empresa (se são papéis, mídias, softwares, arquivos digitais disponíveis em hardware ou em nuvem e outros), onde estão (se estão em servidores da própria empresa, se estão em servidores de terceiros, se estão em bibliotecas ou sala de arquivos) e quem cuida de cada um deles (trata dos controladores e operadores de dados em espécie) (CARLOTO, 2022, p. 244).

---

[10] John Kyriazoglou é especialista em Proteção de Dados e atua há 45 anos na área, sendo criador do framework DP&P (Sistema de Proteção e Privacidade de Dados), reconhecido pela EXIN, empresa holandesa que certifica profissionais de TI em todo o mundo.

[11] DPO é o termo utilizado para *Data Protection Officer*, isto é, o cargo "máximo" no setor de gerência de segurança de dados de uma empresa.

Outrossim, na fase de preparação dos dados, torna-se necessário traçar um plano de treinamento. Este exercerá a função de ajudar os dirigentes do comitê a compreender como se darão os treinamentos; se serão por palestras, *workshops*, interações entre os colaboradores da empresa e afins (CARLOTO, 2022). O plano de ação, que é logicamente o mais importante, também consta na primeira fase, e é a documentação final a ser apresentada para a alta administração, na qual constam orçamento, prazos, sistemas e recursos humanos utilizados, além de um panorama geral sobre a aplicabilidade do programa de *compliance* no ambiente interno da companhia (CARLOTO, 2022).

## 4.2. SEGUNDA FASE: ORGANIZAÇÃO DOS DADOS

A segunda etapa é onde geralmente se nomeia o DPO permanentemente, mesmo que, na primeira, ele já exista em caráter provisório no contexto do comitê de *compliance* criado. Aqui, múltiplos interessados na nova reestruturação da empresa devem se juntar. Carloto implica que, na segunda fase, "é de suma importância o engajamento da alta direção, a qual patrocina as questões relacionadas à privacidade e proteção de dados e garantirá os recursos indispensáveis desta" (CARLOTO, 2022, p. 246). Incluídos os *stakeholders* e os controladores de dados, o gerenciamento do programa a partir daqui busca dar poder para que o DPO seja capaz de realizar as comunicações e a conscientização necessárias dentro da empresa para que ela passe a convergir para uma cultura de *compliance* (CARLOTO, 2022).

Dentro desse contexto surgem as Políticas de Privacidade, documentação conceituada em tópico anterior no artigo, que busca servir de guia não apenas para os empregados, mas também para os clientes, enfatizando transparência, segurança e a responsabilidade da empresa para com o tratamento de dados em larga escala. Ela deve ser mantida atualizada, e não pode subsistir tão somente nas primeiras fases de implementação do programa de *compliance*, e sim seguir sendo de fácil acesso, e sempre contendo as últimas novidades no que diz respeito às mudanças normativas e autorregulatórias de segurança da informação (CARLOTO, 2022).

## 4.3. TERCEIRA FASE: IMPLEMENTAÇÃO E DESENVOLVIMENTO DA PRIVACIDADE DE DADOS

A terceira fase é relativamente mais simples, pois trata da aplicabilidade de todos os planejamentos que foram abordados até então. É quando os treinamentos sobre *Compliance* e LGPD começam a ser dados, estes sendo em caráter completo para membros do comitê e *stakeholders*, e em caráter básico, contínuo e atualizado para demais empregados da empresa.

Também insere-se, nessa fase, a aplicação dos sistemas de controle de acesso, que nada mais são que as metodologias dos crachás, cartões e *tokens*, que servem para controlar qual categoria de funcionário possui acesso a quais setores, dados e sistemas da empresa (CARLOTO, 2022).

Um sistema de transferência internacional de dados também é implementado nessa fase, pensando em como exatamente as legislações dos países para os quais os dados serão transferidos se comportam. Cria-se uma integração condizente e respeitam-se as legislações respectivas, sendo que, em grande parte delas, o *padrão-ouro* da GPDR é tido como exemplar; essa integração precisa ser documental e sistemática, de forma que todo o fluxo de dados internacional consiga ser traçado da forma menos confusa e complexa possível.

Por fim, é nessa fase que a Política de Segurança da Informação (PSI) é aplicada, buscando tornar robusto, sofisticado e seguro os sistemas de informática empresarial, além de criar diretrizes específicas, também já explicitadas no presente trabalho. Os planos de segurança técnica de TI encontram lugar na terceira fase de implementação, e é nela que se iniciam os testes de segurança de dados do setor informático da empresa em questão, testando ataques contínuos e diferenciados para avaliar falhas no sistema e corrigi-las o quanto antes (CARLOTO, 2022).

### 4.4. QUARTA FASE: GOVERNANÇA DE PRIVACIDADE

A quarta fase pode ser considerada, de certo modo, a fase “final” da implementação do Programa de *Compliance*. Isso, pois é a partir dela que se observa a criação de mecanismos mais específicos para assessorar as estratégias implementadas na fase anterior. É aqui que nota-se a presença de avisos de privacidade dentro dos sistemas, planos de solicitações e toda a estruturação do setor do encarregado de dados, que ficará na ponte entre a empresa, o titular de dados e a autoridade legitimada, que neste caso, é a ANPD (CARLOTO, 2022).

Além disso, Carloto segue estabelecendo que é na quarta fase do processo que se implementam os relatórios de privacidade, que vão supervisionar a implementação como um todo e verificar o que pode e o que deve ser alterado. Nessa leva, identifica-se a existência dos relatórios de auditorias, que fiscalizam as estratégias já postas em prática. Os Relatórios de Impacto à Proteção de Dados (RIPDs) estabelecem-se na fase de governança, e são realizados pelos controladores para que se possa mensurar como os riscos do tratamento de dados até aquele momento foram atenuados pela implementação do programa de *Compliance*. A partir

dessa etapa, empresas de pequeno, médio e grande porte já são capazes de responder adequadamente aos órgãos que requisitarem a documentação em questão (CARLOTO, 2022).

Nessa etapa, por fim, estabelece-se um regime de subordinação do controlador com o operador, sendo que o segundo deve estar sempre atualizando o primeiro sobre eventuais *gaps* e riscos encontrados que não constem nas documentações e auditorias previamente realizadas. Um mecanismo de notificação de incidentes de segurança também deve surgir na quarta fase, de maneira que a ANPD seja devidamente comunicada, nos termos da LGPD, no que diz respeito às infrações e violações de dados que a empresa eventualmente sofra (CARLOTO, 2022).

## 4.5. QUINTA FASE: AVALIAÇÃO E MELHORIA DA PRIVACIDADE

Por fim, a quinta fase da implementação nada mais é do que uma extensão de todas as outras, pois trata estritamente da continuidade e atualização de todos os mecanismos de segurança aplicados. A fase de avaliação e melhoria serve precisamente ao que o nome indica; todos os programas já estão implementados e seguem em funcionamento, e basta que estejam atualizados com a legislação mais recente e com os ditames tidos como referenciais na doutrina internacional de Proteção de Dados.

Carloto (2022, p. 250) aborda, para esta última fase, a necessidade da existência dos seguintes aspectos:

> Auditorias internas e externas, benchmarks de melhoria, que consistem em um processo de comparação com os pares, sendo uma importante ferramenta de gestão e melhoria, sempre deverão fazer parte desta fase, já que buscamos a conformidade e resolver possíveis gaps ainda existentes, não detectados inicialmente no ‘gaps analysis’, além de quaisquer riscos de privacidade e proteção de dados.

Nota-se, diante desse ditame, que ainda há uma série de pormenores a serem aplicados dentro do contexto do Programa de *Compliance*, que nada mais é do que um polimento e um aperfeiçoamento de todo o conjunto.

Exemplificado, nas palavras da autora em questão, como funciona a implementação do *Compliance* na prática, torna-se imprescindível compreender como exatamente ele é aplicado na prática, o que será realizado no tópico em sequência.

## 5. EXEMPLO DE PROGRAMA DE *COMPLIANCE* APLICADO NA PRÁTICA

A Meta Platforms, Inc., empresa que gerencia a rede social Facebook, disponibiliza em seu *website* sua Política de Privacidade, que contém várias informações e avisos interessantes. Ela exerce exatamente o que o documento em questão, anteriormente citado, tem como função: explicar ao usuário final do produto ofertado como seus dados são recolhidos, analisados e processados, além de quando, onde e em quais circunstâncias essas operações ocorrem. Também aborda para quais produtos da empresa a política se aplica, além de explicitar como a companhia como um todo colabora com parceiros, fornecedores e terceiros. Toda a esquemática de *compliance* abordada até então está disponível no portal em questão, que é inclusive interativo o suficiente para que o usuário possa rever os dados e informações que compartilhou, além de solicitar a exclusão de seus dados, e dialogar com os encarregados de dados do setor responsável.

Além disso, a empresa em questão possui, para um de seus produtos (o Facebook, especificamente), um Termo de Segurança de Dados, contendo grande parte das informações legais relevantes ao tema. É possível ver uma série de mecanismos e estratégias características dos programas de conformidade quando se nota, na íntegra, os seguintes aspectos do termo:

> 1. **Organização da segurança das informações**. O Facebook tem uma equipe responsável pela supervisão da segurança dos Produtos Aplicáveis.
>
> 2. **Segurança física e ambiental**. As medidas de segurança do Facebook incluirão controles criados para garantir que o acesso aos data centers do Facebook seja limitado às pessoas autorizadas, bem como controles para detectar, prevenir e controlar a destruição gerada por riscos ambientais. Os controles incluirão:
>
> a. O registro e a auditoria dos acessos físicos ao data center por funcionários e contratados.
>
> b. Sistemas de câmeras de vigilância no data center.
>
> c. Sistemas que monitoram e controlam a temperatura e a umidade dos equipamentos e computadores no data center.
>
> d. Geradores de energia e de backup no data center.
>
> e. Procedimentos para exclusão segura de dados, sujeitos aos Termos do Produto Aplicável.
>
> f. Protocolos exigindo documentos de identidade para entrada em todas as instalações do Facebook para os funcionários trabalhando nos Produtos Aplicáveis.
>
> 3. Funcionários

a. **Treinamento**. O Facebook garantirá que todos os funcionários com acesso aos Dados Cobertos passem por treinamento de segurança.

b. Verificações de histórico e antecedentes. O Facebook terá um processo para:

i. verificar a identidade dos funcionários com acesso aos Dados Cobertos.

ii. realizar verificações de antecedentes, nos casos em que houver permissão legal, em relação aos funcionários trabalhando ou oferecendo suporte a aspectos pertencentes aos Produtos Aplicáveis em conformidade com os padrões do Facebook.

c. **Violação da segurança por funcionários**. O Facebook tomará medidas disciplinares em caso de acesso não autorizado aos Dados Cobertos por funcionários do Facebook, incluindo, nos casos em que houver permissão legal, punições e até mesmo demissão.

4. **Testes de segurança**. O Facebook realizará testes de segurança e de vulnerabilidade regularmente para avaliar se os controles essenciais estão sendo devidamente implantados e se estão funcionando.

[...]

6. **Segurança das comunicações**

a. **Segurança da rede**

a. O Facebook usará tecnologia consistente com os padrões do setor na separação das redes.

b. O acesso remoto à rede dos sistemas do Facebook exigirá comunicação criptografada com o uso de protocolos seguros e autenticação multifator.

b. **Proteção de dados em trânsito**

a. O Facebook imporá o uso de protocolos adequados criados para proteger a confidencialidade dos dados em trânsito nas redes públicas.

7. **Gerenciamento de vulnerabilidade**. O Facebook instituiu e manterá um programa de gerenciamento de vulnerabilidades cobrindo os Produtos Aplicáveis que inclui a definição de funções e responsabilidades para o monitoramento de vulnerabilidade, a avaliação de risco de vulnerabilidade e a implantação de patch.

8. **Gerenciamento de incidentes de segurança**

a. **Resposta a incidentes e segurança**. O Facebook manterá um plano de atendimento a incidentes de segurança para monitorar, detectar e lidar com possíveis incidentes de segurança que afetem os Dados Cobertos. O plano de atendimento a incidentes de segurança inclui no mínimo a definição de funções e responsabilidades, comunicação e análises de lições aprendidas, inclusive a análise da causa e planos de correção.

b. **Monitoramento**. O Facebook monitorará violações de segurança e atividades mal-intencionadas que afetem os Dados Cobertos. (META, 2020, online, grifos do autor)

No site, é dito que a vigência da documentação em questão entrou em 31 de agosto de 2020. Entende-se, portanto, que a Meta esteve aprimorando seu programa de *compliance* há bastante tempo, e como pode ser constatado com os enfoques trazidos, é um programa avançado, condizente e responsivo. É possível constatar que o *privacy-by-design* e seus princípios estão sendo atendidos, além dos treinamentos e das normas de conduta. No que diz respeito às políticas éticas internas, torna-se impossível fazer uma análise aprofundada em razão de ser documento de conteúdo confidencial. Apesar disso, verifica-se que a segurança da tecnologia física e ambiental da empresa é atendida, o gerenciamento e a gestão dos acessos são rigorosos, a análise de risco é de suma importância e certamente a empresa atende aos requisitos mínimos exigidos pela Autoridade Nacional de Proteção de Dados no que diz respeito às exigências contidas no Art. 50 da LGPD.

## 6. CONSIDERAÇÕES FINAIS

A conjuntura global encontra-se em um nível de avanço tecnológico que demanda cada vez mais sofisticação do setor corporativo e do setor jurídico das civilizações contemporâneas. Com isso, os dados — tidos como inerentes à pessoa natural e caracterizados como tendo valor imprescindível — entram no enfoque dos interesses de múltiplos agentes, sejam eles movidos por boa-fé objetiva ou mal intencionados. No interesse de resguardá-los, muito se foi feito pelos entes legitimados ao longo dos anos. Seja com o advento da Constituição Federal, o Marco Civil da Internet, a Lei Geral de Proteção de Dados, ECs e Leis Ordinárias subsequentes, o Estado mostra-se proativo em manter os dados pessoais seguros como um direito fundamental. A autorregulação, apesar disso, também não pode ser deixada para trás em nenhuma hipótese, sendo o âmbito público e o âmbito privado dois lados da mesma moeda.

Nesse sentido, as redes sociais entram como um dos ambientes digitais mais utilizados em todo o mundo, e como foi-se constatado, são geridos por empresas do setor privado que precisam manipular dados na maior escala que a história humana já viu. A legislação brasileira exige que sejam tratados de forma a seguir os conformes da LGPD e a ANPD, e sendo assim, surge a necessidade de um programa que consiga adequar as operações das empresas que gerem as redes sociais à legislação. A partir desse fato, surge o Programa de *Compliance*.

O referido programa vem para ser o norteador interno de grande parte, senão todas as tomadas de decisões empresariais. Com sua vasta gama de mecanismos, o *compliance* é uma matéria que segue, até hoje, em constante avanço. Sua importância como mecanismo de

segurança para a manipulação de dados em massa, no contexto das redes sociais, é tamanha que sanções milionárias são aplicadas anualmente quando as companhias cometem infrações e agem em desconformidade com a palavra legal.

No decorrer do trabalho, ao dissecar não exaustivamente os riscos que as empresas concorrem e quais mecanismos de segurança de um Programa de *Compliance* podem ser aplicados, o objetivo principal do texto torna-se atingido. Demonstra-se que a referida estratégia de segurança e privacidade de dados pode, sem sombra de dúvidas, ser o objeto mais crucial para que a gestão autorregulatória de uma companhia de uma redes sociais, seja a Meta ou qualquer outra, torne-se referência quando o assunto é proteção de dados pessoais.

## REFERÊNCIAS BIBLIOGRÁFICAS


BELLI, Luca. Como Implementar a LGPD por meio da Avaliação de Impacto sobre Privacidade e Ética de Dados. In: BIONI, Bruno (org.). **Tratado de Proteção de Dados Pessoais**. São Paulo: Grupo GEN, 2020. E-book, p. 398-428. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 28 nov. 2022.

SOUZA, Carlos Affonso Pereira de. Segurança e Sigilo dos Dados Pessoais**:** primeiras impressões à luz da Lei 13.709/2018. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2 ed. São Paulo: Thomson Reuters Brasil, 2020, p. 413-437.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de Dados pessoais. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2 ed. São Paulo: Thomson Reuters Brasil, 2020, p. 669-706.

PINHEIRO, Patrícia P. **PROTEÇÃO DE DADOS PESSOAIS: COMENTÁRIOS À LEI N. 13.709/2018 (LGPD)**. São Paulo: Editora Saraiva, 2021. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555595123/. Acesso em: 28 nov. 2022.

CARLOTO, Selma. **Lei Geral de Proteção de Dados:** incluindo modelos, segurança da informação e fases da implementação. 3 ed. São Paulo: LTr, 2022.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica.** 5. ed. São Paulo: Atlas, 2022.

GONÇALVES, Mariana Sbaite. **LGPD e o Registro das Operações de Tratamento ed Dados Pessoais – ROPA**. LGPD Brasil, 2020. Disponível em: https://www.lgpdbrasil.com.br/lgpd-e-o-registro-das-operacoes-de-tratamento-de-dados-pessoais-ropa/. Acesso em: 29 de nov. 2022.

**Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em: 01 de nov. 2022.

KEPIOS. **Global Digital Reports**. 2022. Disponível em: https://datareportal.com/social-media-users#:~:text=Analysis%20from%20Kepios%20shows%20that,of%20the%20total%20global%20population.. Acesso em: 26 de out. 2022.

SORTLIST. **Your Digital Year**. 2021. Disponível em: https://www.sortlist.com/blog/your-digital-year/ . Acesso em: 26 de out. 2022.

CETAX. **Big Data**: **O que é, Conceito e Definição**. 2022. Disponível em: https://cetax.com.br/big-data/. Acesso em: 26 de out. 2022.

THE ECONOMIST. **The world's most valuable source is no longer oil, but data**. 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 26 de out. 2022.

BATISTELLA, Carla. **Cookies em sites**: o que é e qual a relação com a LGPD?. Certifiquei, 2021. Disponível em: https://www.certifiquei.com.br/cookies/. Acesso em: 01 de nov. 2022.

WOOLASTON-WEBBER, Victoria. **Instagram now has half a billion users.** Wired UK, 2016. Disponível em: https://www.wired.co.uk/article/instagram-doubles-to-half-billion-users. Acesso em: 04 de nov. 2022.

ROHR, Altieres. '**Deep Web**': entenda o que é e os riscos. Globo, 2019. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2019/03/14/deep-web-entenda-o-que-e-e-os-riscos.ghtml. Acesso em: 07 de nov. 2022.

SYHUNT. **Megavazamentos**. 2021. Disponível em: https://www.syhunt.com/pt/?n=News.2021-Leaks&key=lucy17. Acesso em: 07 de nov. 2022.

CERT, NIC, CGI. Fascículo: Vazamento de Dados. *In*: **Cartilha de Segurança para Internet**, 2021. Online. Disponível em: https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf. Acesso em: 17 de nov. 2022.

GOVERNO FEDERAL. **Facebook é condenado a pagar R$ 6,6 mi por vazar dados de usuários**. 2022. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/facebook-e-condenado-a-pagar-r-6-6-mi-por-vazar-dados-de-usuarios. Acesso em: 17 de nov. 2022.

META. **Termo de Segurança de Dados**. 2020. Disponível em: https://www.facebook.com/legal/terms/data_security_terms#. Acesso em: 27 de nov. 2022.