FGV DCI
DIRETORIA DE
CONTROLES INTERNOS

GUIA DE PROTEÇÃO DE DADOS PESSOAIS

PRIVACIDADE POR *DESIGN*

CC.04.003.2024

OUTUBRO, 2024

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: PRIVACIDADE POR *DESIGN*

VERSÃO 1.0 – OUTUBRO, 2024.

FICHA TÉCNICA

Diretoria de Controles Internos – DCI
Maria Alice da Justa Lemos
Diretora de Controles Internos

Analista responsável por este Guia:
Nadja Nayra da Cruz Ferreira Ribeiro

Jordan Vinícius de Oliveira
Encarregado de Proteção de Dados Pessoais

Equipe Extracontratual:

Laila Sá Ferreira
Taís Povill Rocha
Alessandra Rigueti Barcellos
Nadja Nayra da Cruz Ferreira Ribeiro

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2024	DATA DA APROVAÇÃO: 24/10/2024	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

AVISO LEGAL

Este Guia foi elaborado pela Equipe do Encarregado de Proteção de Dados Pessoais da Fundação Getulio Vargas – FGV e tem como objetivo o compartilhamento de conhecimento envolvendo a conformidade de atividades de tratamento de dados pessoais para o tema escolhido.

O presente documento possui intuito meramente informativo, não sendo utilizado para fins de exploração comercial e apresenta a devida referência na página 2. Do mesmo modo, este documento não deve ser considerado como aconselhamento jurídico e não substitui a avaliação de uma equipe profissional de proteção de dados para cada caso.

SUMÁRIO

1. CONTEXTUALIZAÇÃO

O presente Guia é um dos frutos do projeto de adequação da Fundação Getulio Vargas – FGV em relação à Lei Geral de Proteção de Dados ("LGPD"), aprovada em agosto de 2018, e outras leis setoriais sobre o tema.

A LGPD é aplicável a qualquer operação de tratamento de dados pessoais, seja ela realizada por pessoa natural, pessoa jurídica de direito privado ou pessoa jurídica de direito público. Na condição de Instituição de Ensino Superior ("IES"), a FGV desenvolve, entre outras atividades, operações de caráter administrativo, acadêmico e educacional (como por exemplo, a necessidade de guarda permanente de históricos escolares, provas, realização de pesquisas, desenvolvimento de projetos etc.). Nesse sentido, na condição de Instituição Educacional, a FGV deverá observar as obrigações normativas específicas das entidades públicas reguladoras, como, por exemplo, o Ministério da Educação ("MEC") e a Autoridade Nacional de Proteção de Dados (“ANPD”).

Assim, a FGV desenvolveu, em maio de 2019, um projeto para cumprir com os objetivos de sua conformidade regulatória perante as leis de proteção de dados, denominado **Projeto Presidência – Implantação do Programa de Conformidade: Leis de Proteção de Dados Pessoais (“Projeto”)**. Esta iniciativa, entre outras atividades, buscou parametrizar ações de conformidade da FGV ao novo contexto regulatório de proteção de dados, bem como, a partir das lições aprendidas, fornecer subsídios e materiais de apoio ao setor educacional.

Após a conclusão do Projeto inicial, a FGV criou a **Equipe do Encarregado de Proteção de Dados Pessoais**, no âmbito de sua Diretoria de Controles Internos ("DCI"). Esta Equipe tem como finalidade principal manter a FGV em adequação às normas de proteção de dados aplicáveis às suas atividades, bem como funcionar na condição de interlocutora junto aos variados setores da Organização, à ANPD, aos titulares de dados pessoais e aos demais agentes de tratamento.

O objetivo geral deste Guia, desenvolvido pela **Equipe do Encarregado de Proteção de Dados Pessoais**, é fornecer algumas diretrizes para a aplicação da privacidade por *design* em ambientes digitais, especialmente em sistemas, aplicativos e/ou plataformas.

Assim, como objetivos específicos, este Guia pretende:

(a) Apresentar aspectos gerais sobre a abordagem de privacidade por *design*, relacionando-a com a Lei Geral de Proteção de Dados Pessoais e seus princípios fundamentais;

(b) Descrever algumas estratégias relacionadas à privacidade por *design*, bem como orientar em sua aplicação; e

(c) Destacar essa abordagem nos ambientes de desenvolvimento e aplicados a dados pessoais de crianças.

Este Guia está distribuído em 2 eixos centrais: no capítulo 2 serão apresentados os aspectos gerais da privacidade por *design*, relacionando essa abordagem com os princípios da LGPD. No capítulo 3 serão apresentadas as estratégias orientadas a dados e a processos. Ainda será destacado a importância dos ambientes em desenvolvimento e o cuidado especial ao tratamento de dados pessoais de crianças em ambientes digitais.

Ressalta-se que este Guia não possui a intenção de ser exaustivo sobre o tema, mas ser um documento orientativo para que as suas recomendações permaneçam relevantes e aplicáveis ao desenvolvimento de sistemas, aplicativos e/ou plataformas digitais.

2. PRIVACIDADE POR *DESIGN*: ASPECTOS GERAIS

Na atualidade há o uso massivo de dispositivos que podem se conectar à internet, como celulares, *tablets* e computadores. Esses aparelhos possibilitam o acesso a sistemas, aplicativos ou plataformas que podem realizar o tratamento[1] de dados pessoais[2]. Ao mesmo tempo, os usuários esperam que esses serviços sejam seguros e protejam sua privacidade de forma eficaz.

Nesse contexto, é importante que a privacidade seja pensada em todo o ciclo de vida do produto e/ou serviço, por meio de medidas técnicas e organizacionais que contribuam para garantir e respeitar os direitos de seus titulares[3]. Deste modo, a privacidade por *design* e a sua relação com a legislação de proteção de dados serão tratados nesta seção.

[1] Conforme o art. 5º, X da LGPD, **tratamento** é "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".
[2] De acordo com o art.5º, I da LGPD, **dado pessoal** é a "informação relacionada a pessoa natural identificada ou identificável".
[3] Segundo o art.5º, V da LGPD, **titular** é "Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento".

Preliminarmente será explorado o conceito de privacidade por *design* e, em seguida, a sua relação com a LGPD. Ainda, serão apresentados os 7 (sete) princípios fundamentais da privacidade por *design*, conforme idealizados por Ann Cavoukian.

2.1. O CONCEITO

A privacidade por *design (privacy by design,* "PbD") se refere à busca por incorporar a privacidade durante todo o ciclo de vida de um objeto, seja um sistema, um serviço ou um processo. O ciclo de vida de um objeto são todos os estágios por onde ele passa, abarcando, por exemplo, as etapas de desenvolvimento, teste e entrega.

Em decorrência disso, é importante que a proteção de dados[4] comece na fase de planejamento de um produto/serviço. Assim, nas atividades de tratamento pretendidas devem ser considerados os possíveis riscos que elas podem representar aos titulares e as medidas disponíveis para garantir que os princípios de proteção de dados sejam cumpridos desde a construção da atividade.

Nesse cenário, vale mencionar que o PbD foi popularizado na década de 90 pela canadense Ann Cavoukian, Comissária de Privacidade da província canadense de Ontário. Posteriormente este conceito foi apresentado na 31ª Conferência Internacional de Comissionados de Proteção de Dados e Privacidade com o título "*Privacy by Design: The Definitive Workshop*" e endossado internacionalmente na 32ª Conferência Internacional de Comissionados de Proteção de Dados e Privacidade em 2010, com a aprovação da "*Resolution on Privacy by Design*"[5].

Ainda, no âmbito da União Europeia, o Regulamento Geral de Proteção de Dados Europeu ("GDPR") reconhece como um requisito legal a proteção de dados por *design* e por padrão. Deste modo, segundo o art. 25 do Regulamento supramencionado, os agentes de tratamento[6] devem, tanto na determinação dos meios de tratamento como no próprio tratamento, implementar medidas técnicas e organizacionais adequadas, a fim de cumprir os requisitos legais e proteger os direitos dos titulares.

---

[4] Nota: os direitos de privacidade e proteção de dados pessoais possuem, na doutrina, tratamentos autônomos, contudo serão tratados neste Guia como complementares e não excludentes, uma vez que a própria LGPD trouxe o respeito à privacidade como um de seus fundamentos elementares.
[5] UNIÃO EUROPEIA. European Data Protection Supervisor. Resolution on Privacy by Design. *32nd International Conference of Data Protection and Privacy Commissioners.* Jerusalén (Israel) 27-29/10/2010. Disponível em: <link>. Acesso em 26 de dez. 2023.
[6] Conforme o art,5º, IX da LGPD, **agentes de tratamento** são "o controlador e o operador".

Nesse sentido, as medidas técnicas e organizacionais podem ser entendidas como qualquer método ou meio que um agente de tratamento possa empregar no tratamento de dados pessoais. Além disso, essas medidas devem ser adequadas para atingir o objetivo pretendido, ou seja, devem ser incorporados os princípios de proteção de dados de forma eficaz, garantindo que apenas sejam tratados os dados pessoais para uma finalidade específica e necessária[7].

A depender do contexto e dos riscos associados ao tratamento, podem ser implementadas, por exemplo, medidas como a anonimização[8], a pseudonimização[9], o uso de sistemas de detecção de *malware*[10], a separação dos ambientes de armazenamento e processamento de dados conforme a sua criticidade, a utilização de dados sintéticos/não reais na testagem de aplicações, entre outros.

2.2. PRIVACIDADE POR *DESIGN* E A LGPD

A LGPD estabelece as diretrizes para o tratamento de dados pessoais realizados por pessoa natural ou pessoa jurídica de direito público ou privado. Assim, no seu Capítulo VII, que trata "da segurança e das boas práticas", mais especificamente no artigo 46, caput e §2º, e artigo 49, as diretrizes principiológicas da PbD foram diretamente incorporadas por esta Lei:

> Art. 46. Os agentes de tratamento devem adotar **medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.
> (...)
> § 2º As medidas de que trata o caput deste artigo deverão ser **observadas desde a fase de concepção do produto ou do serviço até a sua execução**.
>
> Art. 49. Os **sistemas** utilizados para o tratamento de dados pessoais devem ser **estruturados** de forma a atender aos requisitos de **segurança, aos padrões de**

[7] UNIÃO EUROPEIA. European Data Protection Supervisor. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.* p.6. Disponível em: <link>. Acesso em: 17 mai. 2024.
[8] Conforme o art. 5º, XI, a **anonimização** corresponde à "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo". Nos termos da lei, em seu artigo 12, a anonimização torna o dado pessoal em não pessoal, mas só pode ser considerada como tal quando o seu processo não possa ser revertido mediante expedientes do próprio agente de tratamento ou razoavelmente esperados por terceiros.
[9] Segundo o art.12, §4º da LGPD: "os efeitos deste artigo, a **pseudonimização** é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro". Ao contrário do dado anonimizado, que não é considerado dado pessoal, o dado pseudonimizado ainda é regulado pela LGPD e é identificável mediante o uso de informações adicionais que se encontrem em ambiente apartado.
[10] Malware é um programa com potencial danoso inserido em um sistema ou dispositivo com o intuito de comprometer a sua confidencialidade, integridade ou disponibilidade, como vírus, cavalos de troia ou outros tipos de códigos maliciosos. ESTADOS UNIDOS. National Institute of Standards and Technology. *Glossary*. Disponível em: <link>. Acesso em: 18 jan. 2024.

> **boas práticas e de governança** e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Pontua-se que a privacidade por *design* gera reflexos nas searas administrativas, tecnológicas e jurídicas do tratamento de dados pessoais, sendo que o seu cumprimento/observância ajuda a prevenir sanções administrativas e cíveis aos agentes de tratamento. Cita-se, como exemplo, duas sanções aplicadas[11] pela ANPD em razão de casos em que os pressupostos de segurança dos sistemas não foram respeitados, violando assim o art. 49 da LGPD.

Pensando nisso, é relevante destacar o princípio da necessidade (art.6º, III da LGPD), ou seja, a observância da limitação do tratamento ao mínimo necessário para a realização de suas finalidades, abrangendo apenas dados pertinentes, proporcionais e não excessivos. Deste modo, caso haja o tratamento de dados pessoais, é recomendável que apenas sejam tratados os dados relevantes e estritamente necessários aos fins previstos, mantendo-os armazenados somente pelo período necessário à finalidade indicada[12].

EXEMPLO

PLATAFORMA QUE PERMITE A UTILIZAÇÃO DE SERVIÇOS SEM NECESSIDADE DE *LOGIN*

- Imagine que certa plataforma de cursos online gratuitos requeira de seus usuários certos dados pessoais para emissão de certificado de participação nos cursos, os quais são pagos. Após estudo sobre o seu público-alvo, os gestores se depararam com um número significativo de pessoas que não deseja realizar o teste final para emitir o certificado, mas apenas assistir às aulas gratuitas.

  Visando alcançar boas práticas de privacidade por *design*, os desenvolvedores decidiram, assim, criar na etapa de cadastro duas opções: **(i)** uma com *login* para fins de pagamento e emissão de declaração e, **(ii)** outra anônima, que permite acessar o conteúdo sem emissão de certificado.

  Esse é um exemplo sobre como pensar no uso dos dados e nas finalidades pode ser vantajoso tanto aos agentes de tratamento (que não reterão dados pessoais desnecessários) quanto aos titulares (que não precisarão fornecer dados pessoais caso não queiram emitir certificados).

[11] BRASIL. Autoridade Nacional de Proteção de Dados. Relatório de Instrução n° 2/2023/CGF/ANPD e Relatório de Instrução nº 4/2023/FIS/CGF/ANPD. Disponível em: <link>. Acesso em: 10 jan. 2024.
[12] Em conexão com o princípio da necessidade, a leitura do relatório da ICO (autoridade de proteção de dados do Reino Unido), sobre minimização de dados é recomendada: REINO UNIDO. Information Commissioner's Office (ICO). *Data minimization*. Disponível em: <link>. Acesso em: 12 jan. 2024.

Ainda, destaca-se o princípio da transparência (art.6º, VI da LGPD) que indica que os titulares deverão ser informados sobre o tratamento de seus dados de forma clara, precisa e facilmente acessível. Em vista disso, independentemente da base legal[13] utilizada para fundamentar o tratamento, os titulares precisam ter informações suficientes e acessíveis sobre as operações realizadas.

Também é importante que o aplicativo/plataforma forneça, pelo menos, as seguintes informações, segundo o art. 9º da LGPD: **(i)** a finalidade específica do tratamento, **(ii)** a forma e duração do tratamento, **(iii)** informações sobre quem são os agentes de tratamento e seus papéis, **(iv)** o contato do controlador[14] e, **(v)** o rol de direitos dos titulares previstos na LGPD.

Fechado este tópico, na próxima seção serão indicados os princípios fundamentais da privacidade por *design*, conforme sua idealizadora, Ann Cavoukian, e sua relação com a LGPD.

2.2.1. PRINCÍPIOS DA PRIVACIDADE POR *DESIGN* E DA LGPD

Destaca-se que Ann Cavoukian em seu artigo "*Privacy by Design: the 7 Foundational Principles*" fundamentou o FIPPs ("*Fair Information Practices Principles*"), um conjunto de 7 (sete) princípios fundamentais de privacidade a serem observados em produtos ou serviços. Estes princípios, conforme serão apresentados a seguir, não dizem respeito somente à seara da tecnologia da informação, mas também às ações das pessoas envolvidas e seus respectivos processos no tratamento de dados pessoais.

- **Proativo, não reativo; preventivo, não corretivo**

Qualquer sistema ou processo que trate dados pessoais deve ser concebido e desenhado desde o início, identificando os possíveis riscos aos direitos e liberdades dos titulares e minimizá-los para que não se concretizem em danos. Assim, devem ser adotadas medidas proativas que antecipam as ameaças, identificando as fraquezas dos sistemas, e processos para neutralizar ou minimizar os

[13] **Base legal**: trata-se do fundamento que autoriza o tratamento de dados pessoais por um agente, devendo ser definida, em casos concretos, a partir de uma das hipóteses dispostas na LGPD ao seu art. 7º (caso de dados pessoais) ou ao seu art. 11 (caso de dados pessoais sensíveis).
[14] O art.6º, VI estabelece que o **Controlador** é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

riscos de forma prévia, em vez de aplicar medidas corretivas para falhas de privacidade apenas após a sua materialização.[15]

Neste cenário, destaca-se o princípio da prevenção (art. 6º, VIII da LGPD), que significa a: "*adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais*". Este princípio indica uma postura mais proativa da proteção à privacidade no contexto do tratamento de dados pessoais, mantendo-se a máxima do ditado que diz ser "*melhor prevenir do que remediar*".

- **A privacidade como configuração por padrão**

A privacidade por padrão ("*privacy by default")* busca proporcionar ao usuário o maior nível de privacidade, considerado o estado da arte e, principalmente, que os dados estejam protegidos em quaisquer sistemas, produtos, serviços ou práticas de negócios. Assim, caso o usuário não realize nenhuma ação de configuração, sua privacidade deve ser garantida, pois ela está integrada ao tratamento dos dados pessoais e configurada por padrão[16].

Portanto, o tratamento deve seguir boas práticas que incluem a especificação clara da sua finalidade, a minimização de dados pessoais e o seu correto ciclo de vida desde o momento da sua obtenção até depois de atingido o propósito do tratamento. Por exemplo, a definição das técnicas de segurança da informação em trânsito de um sistema online que coleta dados sigilosos não podem depender da escolha de um usuário leigo, sendo que recursos de criptografia (como o protocolo HTTPS – *hypertext transfer protocol secure*) precisam ser implementadas independentemente de eventual escolha do usuário.

- **A privacidade incorporada no *design***

A proteção dos dados pessoais e da privacidade dos usuários deve ser parte integrante ao *design*, à arquitetura dos sistemas e as práticas do negócio, ou seja, ela não pode ser apenas um complemento adicionado ao término do projeto, serviço ou produto.

Desse modo, este princípio consiste na ideia de que a arquitetura do sistema terá a privacidade como um componente central para a própria funcionalidade do produto ou serviço, razão pela qual

[15] REINO UNIDO. *Data protection by design and by default.* Disponível em: <link>. Acesso em: 12 jan. 2024.
[16] ESPANHA. Agencia Española de Protección de Datos. Guía de Privacidad desde el Diseño. p.8. Disponível em: <link>. Acesso em: 22 abr. 2024.

o já abordado parágrafo 2º do artigo 46 da LGPD estipula que as medidas técnicas e administrativas devem ser observadas desde a concepção até a execução.

- **Funcionalidade completa**

Este princípio consiste em evitar a crença de que em qualquer sistema ou serviço apenas é possível ter a privacidade ou a segurança (soma zero, ou escolha/*trade-off* para qual delas priorizar), e não ambas simultaneamente (soma positiva)[17]. A privacidade não deve ser conquistada à custa da perda de outras funcionalidades do produto ou serviço, pois é possível manter a privacidade e a segurança ao mesmo tempo, garantindo-se, assim, a funcionalidade dos serviços oferecidos.

Este princípio tem por finalidade manter as perspectivas abertas para novas soluções, de modo a alcançar sistemas totalmente funcionais, eficazes e eficientes acerca do nível da privacidade. Nesse sentido, o artigo 2º da LGPD prevê como fundamentos da disciplina de proteção de dados pessoais o desenvolvimento econômico e tecnológico, a inovação e a livre iniciativa, livre concorrência e defesa do consumidor. Logo, a privacidade não deve ser vista como uma inimiga dos projetos ou funcionalidades, mas uma aliada na busca de soluções.

- **Segurança de ponta a ponta**

Devem ser implementadas medidas de segurança fortes desde o início e estendias ao longo do ciclo de vida dos dados (como: coleta, classificação, conservação, entre outras). Logo, é possível tratar os dados de forma segura e depois conservá-los (se necessário) ou eliminá-los quando atendida a finalidade à qual eles se destinam.[18]

Este princípio se relaciona com a conjunção de mais de um dos verbos utilizados para a definição de tratamento empregada no art. 5º, X da LGPD. Assim, o tratamento envolve todo o ciclo de vida dos dados, desde sua obtenção, uso e descarte. Portanto, os cuidados de privacidade se estendem para além da fase corrente de uso dos dados, atingindo também o momento posterior, ou seja, o modo de conservação e armazenamento ou, se for o caso, de eliminação das informações.

[17] REINO UNIDO. Information Commissioner's Office (ICO), op. cit., nota 14.
[18] ESPANHA. Agencia Española de Protección de Datos, op. cit., nota 15, p.9.

- **Visibilidade e transparência**

Para a privacidade ser garantida é necessário verificar se o tratamento está de acordo com a informação fornecida. Deste modo, é importante que haja a transparência no tratamento de dados, comprovando a diligência e responsabilidade proativa perante a Autoridade fiscalizadora e como medida de confiança perante o titular[19].

Neste contexto, destaca-se o princípio da transparência (art. 6º, VI, da LGPD). Assim, independentemente da base legal adotada para o tratamento, os titulares de dados pessoais, precisam ter informações suficientes e acessíveis sobre as operações realizadas. Seguindo-se a velha máxima do ditado russo "confie, mas verifique"[20], é importante que as ações de transparência sobre a privacidade estejam claras aos titulares para que possam compreender e confiar no tratamento de seus dados pessoais.

- **Respeito pela privacidade do usuário**

O objetivo final do tratamento de dados pessoais deve ser garantir os direitos e liberdades dos usuários cujos dados são a razão do tratamento. Isso significa projetar processos, viabilizando medidas com padrões de privacidade fortes, avisos adequados e opções amigáveis com foco na perspectiva do usuário ("*user-centric*")[21].

Pontua-se que não por acaso a previsão do relatório de impacto[22] à proteção de dados pessoais leva em conta os riscos das operações de tratamento não aos agentes controladores ou operadores envolvidos, mas sim às liberdades civis e direitos fundamentais dos próprios titulares.

RESUMO

PRIVACIDADE POR DESIGN E A LGPD

- A privacidade por *design* objetiva incorporar a privacidade durante todo o ciclo de vida de um objeto, sistema, serviço ou processo.
- Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais, que devem ser observadas desde

[19] ESPANHA. Agencia Española de Protección de Datos, op. cit., nota 15, p.10.
[20] O trecho correspondente em língua estrangeira é: "doveryai, no proveryai" ou "доверяй, но проверяй".
[21] ESPANHA. Agencia Española de Protección de Datos, op. cit., nota 15, p.10.
[22] Conforme o art. 5º, XVII da LGPD, **relatório de impacto à proteção de dados pessoais** é a "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco."

a fase de concepção do produto ou do serviço até a sua execução.

- A privacidade por *design* possui 7 (sete) princípios fundamentais, que podem se relacionar com os princípios elencados no art. 6º da LGPD.

3. PRIVACIDADE POR *DESIGN* EM AMBIENTES DIGITAIS

Compreender como um tratamento de dados pessoais pode afetar a privacidade dos titulares é essencial para projetar e desenvolver sistemas confiáveis do ponto de vista da proteção de dados. Deste modo, o projeto de sistemas deve estar centrado em analisar os riscos e responder às ameaças que podem afetar a privacidade e a segurança dos titulares.

Nesse sentido, é importante mencionar as tecnologias de aprimoramento da privacidade (*Privacy-Enhancing Technologies*, "PETs") que são soluções que visam aumentar a privacidade, tais como: criptografia, anonimização, autenticação, entre outras indicadas ao decorrer deste Guia. Essas tecnologias não são apenas uma medida defensiva, pois constituem um passo proativo para promover uma cultura de proteção de dados e garantir a reputação de uma empresa na era digital[23].

Ainda, nota-se que o desenvolvimento de um sistema é um processo cíclico, passando por várias fases, como: concepção, desenvolvimento, entrega etc. Assim, as estratégias de privacidade por *design* são principalmente aplicadas nas fases de concepção e desenvolvimento e, quando alcançadas, melhoram a privacidade do sistema geral. Em vista disso, nesse capítulo serão tratadas medidas que podem ser incorporadas ao produto/serviço com o objetivo de melhorar a privacidade.

3.1. ESTRATÉGIAS RELACIONADAS À PRIVACIDADE POR *DESIGN*

As estratégias relacionadas a privacidade por *design* se concatenam com os princípios previstos no art. 6º da LGPD e permitem que medidas de proteção de dados pessoais sejam incorporadas às operações de tratamento. Nesse sentido, são elas:

[23] SINGAPURA. Personal Data Protection Comission. Proposed Guide on Synthetic Data Generation, p.3. Disponível em: <link>. Acesso em: 30 jul.2024.

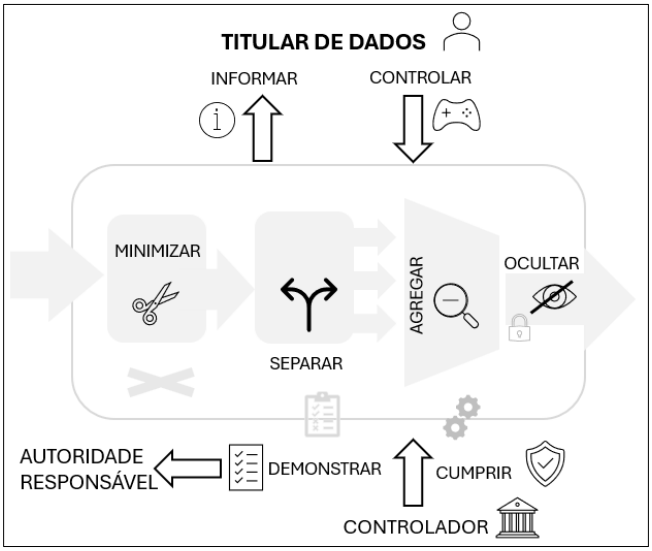
ESTRATÉGIAS DE PRIVACIDADE POR *DESIGN*	DESCRIÇÃO
Minimizar	Os dados pessoais devem ser reduzidos ao mínimo possível.
Ocultar	Os dados pessoais e as suas inter-relações devem ser ocultados.
Separar	Os dados pessoais devem ser tratados em compartimentos separados quando possível.
Agregar	Os dados pessoais deverão ser tratados com alto nível de agregação e com o mínimo de detalhes.
Informar	Os titulares devem ser adequadamente informados do tratamento de suas informações.
Controlar	Os titulares devem ter controle sobre o tratamento dos seus dados pessoais.
Cumprir	Uma política de privacidade compatível com os requisitos legais deve ser implementada e aplicada.
Demonstrar	Os responsáveis pelo tratamento de dados devem ser capazes de demonstrar o cumprimento da política de privacidade em vigor e de quaisquer requisitos legais aplicáveis.

Fonte: ENISA. Privacy by design in big data. Disponível em: <**link**>

Dependendo do contexto, determinadas estratégias podem ser mais adequadas do que outras no âmbito do desenvolvimento de sistemas. Contudo, se consideradas desde as etapas iniciais e se aplicadas conjuntamente, permitem que medidas de proteção de dados pessoais sejam devidamente incorporadas nas operações de tratamento, possibilitando que os resultados finais levem em conta os requisitos de privacidade e a garantia dos direitos e liberdades dos titulares.[24]

Assim, a imagem a seguir indica como essas estratégias se relacionam em projetos de privacidade.

[24] ESPANHA. Agencia Española de Protección de Datos, op. cit., nota 15, p.18.



Fonte: AEPD. Estratégias de privacidade por *design*[25].

Como será observado, essas estratégias[26] podem ser divididas em duas diferentes categorias, quais sejam: estratégias orientadas a dados e estratégias orientadas a processos.

3.1.1. ESTRATÉGIAS ORIENTADAS A DADOS

As estratégias orientadas a dados são de natureza mais técnica e se concentram no tratamento de dados que respeita a privacidade[27], conforme será demonstrado a seguir.

- **Minimizar**

A quantidade de dados pessoais tratados deve ser limitada ao estritamente necessário, bem como deverá ocorrer a eliminação desses dados quando a finalidade almejada for alcançada. Deste modo, pode se dizer que o risco será significativamente reduzido no que diz respeito aos dados pessoais que não são coletados, tendo-se em vista que eles não poderão ser usados indevidamente, sofrerem violações, ou serem alvo de incidentes acidentais ou propositais.

Nessa sequência, as seguintes táticas/estratégias podem ser aplicáveis[28]:

[25] Ibid., p.18. Figura 6 – Estrategias de diseño de la privacidade. Imagem adaptada para a tradução para o português.
[26] Nota: as estratégias citadas neste capítulo estão baseadas majoritariamente a partir de: Hoepman, J-H. Privacy design strategies (the little blue book). Disponível em: <link>. Acesso em: 16 mai. 2024.
[27] Ibid., p.3.
[28] ESPANHA. Agencia Española de Protección de Datos, op. cit., nota 15, p.18.

- **Selecionar**: deve-se determinar com antecedência quais pessoas serão envolvidas no processo e quais atributos são relevantes para o tratamento, seguindo uma atitude conservadora ao estabelecer os critérios de seleção. Tratar-se-á apenas os dados recebidos que satisfaçam os critérios de seleção, ou seja, apenas aqueles estritamente necessários.
- **Excluir**: corresponde à deleção/apagamento dos dados pessoais não mais necessários para o tratamento realizado. Neste caso, deverá ser adotada uma abordagem aberta, na qual o armazenamento de um dado sem a justificativa de manutenção deve ser evitado.
- **Retirar**: deverá ser indicada a necessidade de remover os dados parcialmente assim que não forem mais necessários. É importante determinar antecipadamente o momento no qual será necessário um certo dado e garantir que ele será suprimido ou excluído de documentos, processos ou bancos temporários tão logo não se faça mais necessário.
- **Destruir**: baseia-se em remover completamente os dados que não forem mais relevantes, para que eles não sejam recuperados após deletados, o que envolve outras estratégias que lidem com *backups*/cópias de segurança. Evidencia-se, ainda, que a diferença entre remover e destruir dados é sutil: remover acontece na camada de aplicação, enquanto a destruição se concentra na camada física de armazenamento[29].

PONTO DE ATENÇÃO

MINIMIZAR

- A exclusão ou seleção de dados pessoais não é somente relevante na coleta/obtenção desses dados, mas também ao usar os dados armazenados, já coletados em momento anterior. Certifique-se de que os processos e aplicações internas utilizam apenas os dados pessoais verdadeiramente relevantes para a(s) finalidade(s) desejada(s).
- Se necessário o compartilhamento com terceiros, garanta que apenas os dados pessoais necessários sejam compartilhados.
- Tenha cuidado quando o tratamento de dados criar novos dados pessoais. Neste caso, selecione ou exclua os novos dados que não são necessários.

- **Ocultar**

Os dados pessoais e suas interrelações não devem ser tratados à vista de todos. Ao ocultar dados pessoais, o risco de violações e/ou potenciais incidentes são reduzidos. Esta estratégia tem como

[29] Hoepman, J-H., op. cit., nota 25, p.7.

finalidade a desvinculação de dados e torná-los inobserváveis ou não rastreáveis. Os exemplos incluem pseudonimização, criptografia e agregação de dados pessoais[30]. As maneiras de implementar esta estratégia podem ser:

- **Restringir**: consiste na administração restritiva do acesso aos dados pessoais, limitando-o mediante uma política de controle de acesso que implemente o princípio "*need to know*" ("necessidade de saber", em tradução livre), tanto no espaço (detalhes e tipos de dados acessados) como no tempo (etapas de tratamento).
- **Ofuscar**: os dados pessoais passam a ser intangíveis para pessoas não autorizadas a consultá-los, utilizando-se técnicas de criptografia e *hashing*, tanto em operações de armazenamento como em transferência das informações.
- **Dissociar:** pressupõe a eliminação da vinculação entre conjunto de dados independentes, assim como os atributos identificáveis dos registros dos dados para evitar correlações entre eles, com especial atenção aos metadados.
- **Misturar**: agrupamento de informações relativas a vários titulares, utilizando técnicas de generalização e supressão para evitar correlações entre dados e eventos.

PONTO DE ATENÇÃO

OCULTAR

- Proteja os dados pessoais ou torne-os inobserváveis, ou não rastreáveis. Garanta que eles não se tornem públicos ou conhecidos.

- **Separar**

É importante separar (lógica ou fisicamente) as etapas de tratamento de dados pessoais. Assim, ao separar as fontes de dados pessoais que tratam diversas informações de um mesmo titular, reduz-se a possibilidade de criação de perfis completos de uma mesma pessoa.

A separação é também um meio eficaz para atingir a limitação da finalidade e evitar a combinação entre diferentes conjuntos de dados. Os dados pessoais podem, com base na sua finalidade, ser

[30] NORUEGA. NORWEGIAN DATA PROTECTION AUTHORITY. Software development with Data Protection by Design and by Default. Disponível em: <link>. Acesso em: 12 jan. 2024.

armazenados em bases de dados, unidades, componentes e ambientes separados[31]. Formas comuns de implementar essa estratégia são:

- **Isolar**: objetiva-se a coleta e armazenamento dos dados pessoais em diferentes bases de dados ou aplicativos que sejam independentes em termos lógicos/sistêmicos ou em diferentes suportes físicos (*hardwares*).
- **Distribuir**: pressupõe o uso de arquiteturas de sistemas descentralizadas ou mesmo distribuídas em vez de centralizadas. Indica-se a distribuição da coleta e do tratamento de dados pessoais por diferentes locais físicos e em arquiteturas descentralizadas. Quando possível, é recomendável utilizar o equipamento (computador, *smartphone* etc.) do próprio titular e usar menos os componentes centrais.

PONTO DE ATENÇÃO

SEPARAR

- Quando possível, separe (logicamente ou fisicamente) o tratamento de dados pessoais. Isto poderá tornar mais difícil combiná-los ou correlacioná-los.

- **Agregar**

Os dados pessoais devem ser tratados com o máximo de agregação possível para salvaguardar os direitos de seus titulares. Assim, é recomendável evitar dados detalhados, especialmente dados pessoais sensíveis[32]. Os exemplos incluem a redução do detalhe dos dados pessoais e a remoção de informações desnecessárias ou excessivas, sempre que possível[33]. Para isso, as táticas abaixo podem ser aplicadas:

- **Resumir**: resumem-se atributos detalhados em atributos gerais mais refinados. Por exemplo, usar uma categoria de idade em vez de data de nascimento, ou da cidade de residência no lugar de endereço completo.
- **Agrupar**: compreende em agregar a informação de um grupo de pessoas, em substituição às informações detalhadas de cada indivíduo do grupo. Assim, é recomendável trabalhar

[31] NORUEGA. NORWEGIAN DATA PROTECTION AUTHORITY, op. cit, nota 29.
[32] Segundo o art.5º, II da LGPD, o **dado pessoal sensível** é: "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural."
[33] NORUEGA. NORWEGIAN DATA PROTECTION AUTHORITY., op. cit, nota 29.

com os valores médios ou gerais, como compilar perfis de grupo com informações médias sobre os membros do grupo.

- **Perturbar:** constitui-se na utilização de valores aproximados ou modificação do dado real mediante empego de algum tipo de ruído aleatório, em vez de trabalhar com o valor exato do dado pessoal.

PONTO DE ATENÇÃO

AGREGAR

- Observe que mesmo os perfis de grupo podem representar um risco à privacidade quando houver a possibilidade de que os indivíduos sejam facilmente classificados como pertencentes a um grupo específico (como pessoas com uma determinada condição médica ou com determinado perfil de risco financeiro).
- Registros detalhados são necessários para agir rapidamente, por exemplo, no caso de ataques por hacker mal-intencionados ou de interrupção de um serviço. Assim, se possível, é recomendável que os dados pessoais sejam agrupados, para evitar que, na eventualidade de uma interrupção de serviço, sejam causados danos a esses titulares dos dados pessoais.

3.1.2. ESTRATÉGIAS ORIENTADAS A PROCESSOS

Estas estratégias são de natureza mais organizacionais e são orientadas em definir processos que implementem a gestão responsável dos dados pessoais.[34]

- **Informar**

O titular de dados pessoais deve ser suficientemente informado sobre o tratamento de suas informações. Neste sentido, é importante a transparência sobre quais dados pessoais estão sendo tratados, como são tratados e para qual finalidade. Ainda, deve constar informações sobre as medidas de segurança adotadas para proteger os dados pessoais. É possível a aplicação das seguintes táticas:

- **Facilitar**: traduz-se em fornecimento das informações acerca do tratamento de dados pessoais, como: finalidade e detalhes em relação ao armazenamento. Além disso, é importante ser indicado com quem e como os titulares podem entrar em contato para

[34] Hoepman, J-H., op. cit., nota 25, p.3.

questões relacionadas à proteção de dados pessoais. É possível, por exemplo, colocar um *link* para a política de privacidade na página inicial do *website* e/ou no aplicativo.

- **Explicar:** representa a facilitação do acesso à informação sobre o tratamento de dados pessoais, fornecendo-a de maneira simples, clara e acessível. Convém adotar nas políticas de privacidade uma abordagem em camadas ou em níveis, de modo a disponibilizar informações básicas para o usuário no primeiro nível e informações mais detalhadas e adicionais no segundo nível.
- **Notificar**: entende-se como comunicação aos titulares, por exemplo, sobre a previsão de transferência de dados deles a terceiros. Ainda, se possível, recomenda-se fazer notificações curtas e informativas, e permitir aos titulares controlarem sobre quais eventos eles desejam receber eventuais notificações. É necessário, contudo, se certificar também de não notificar o titular com muita frequência, sem a real necessidade.

PONTO DE ATENÇÃO

INFORMAR

- O titular deve ser informado sobre o tratamento dos seus dados pessoais, como na coleta direta desses dados (ex.: preenchimento de formulário, assinatura de contrato etc.) ou quando são coletados por meio de dispositivos ou tecnologias para observação da sua atividade (ex.: uso de *cookies*, geolocalização etc.).
- A informação deve estar atualizada, ser de fácil acesso (o usuário deve conseguir encontrá-la sem dificuldade) e fornecida de forma clara e compreensível.
- Também é importante informar aos titulares sobre os direitos previstos no Capítulo III da LGPD e como exercê-los.

- **Controlar**

Quando possível, o titular deve poder controlar o uso dos próprios dados pessoais. Isso inclui o direito de acessar, atualizar e/ou excluir os seus dados, respeitadas as condições e exceções exigidas pelas leis de proteção de dados pessoais e pelos contratos aplicáveis.

Uma boa alternativa é o uso de um menu ou uma página separada dentro da plataforma e/ou aplicativo para permitir a visualização e configuração dos dados pelo próprio titular. Deste modo, ele pode obter o controle sobre o tratamento de seus dados pessoais por meio das seguintes táticas:

- **Consentir**: nos casos em que não houver outra base legal mais adequada para respaldar o tratamento, é possível obter o consentimento[35] do titular, o qual deverá ser manifestado de maneira livre, informada e inequívoca por ele. Ainda, é necessário garantir que o titular possa retirar o seu consentimento a qualquer momento, por mecanismos e procedimentos que garantam que a ação de o retirar seja tão fácil quanto a de concedê-lo.
- **Escolher**: é recomendável fornecer, pelo menos, as funcionalidades básicas do serviço/produto ao titular, ainda que ele discorde de alguns pontos em relação ao tratamento de seus dados pessoais.
- **Atualizar**: se possível, recomenda-se a implementação de mecanismos que facilitem e/ou permitam que os usuários revisem e atualizem seus dados pessoais. Isso pode ser implementado, por exemplo, com um *dashboard* que permita a visualização dos dados pessoais pelo usuário.
- **Retirar:** é importante proporcionar mecanismos para que os usuários possam retirar ou solicitar a exclusão de seus dados pessoais fornecidos para o agente de tratamento.

PONTO DE ATENÇÃO

CONTROLAR

- Dentro do que for possível, é necessário garantir que os titulares exerçam um controle adequado sobre o tratamento de seus dados pessoais. Destaca-se, entretanto, que em determinadas situações esse controle não poderá ser viabilizado em sua totalidade, diante de algumas situações, como, por exemplo, a necessidade do armazenamento da informação para o cumprimento de obrigação legal ou regulatória pelo Controlador.
- Alerta-se, ainda, que o consentimento nem sempre será a melhor base legal para o tratamento de dados pessoais, uma vez que, a depender da situação, outra base legal pode ser mais apropriada. Caso se verifique a necessidade de obter o consentimento do titular, deve-se atentar para suas peculiaridades: além de livre, informado e inequívoco, precisa ser fornecido para fins específicos, garantida a revogação a qualquer tempo pelo titular.

[35] De acordo com o art. 5°, XII da LGPD: **consentimento** é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

- **Cumprir**

A busca por conformidade no tratamento de informações pessoais deve ser uma constante prática organizacional, de modo que esteja embutida em sua cultura e endossada pela alta administração. Nesse sentido, políticas de privacidade, por exemplo, são elementares para reforçar o comprometimento institucional com as boas práticas de proteção de dados. Assim, tem-se, como destaque, as seguintes ações:

- **Criar**: a política de privacidade organizacional deve ser clara, com recursos humanos e técnicos para sua execução. Os objetivos de processos de tratamento devem ser transparentes e conforme ao modelo de negócio, observando as bases legais aplicáveis.
- **Manter**: é essencial apoiar a política definida, estabelecendo procedimentos e implementando as medidas técnicas e organizacionais necessárias. Todos os agentes envolvidos na cultura organizacional, como fornecedores, funcionários e gestores precisam ter seus papéis e responsabilidades delimitados.
- **Revisar:** como as circunstâncias mudam com o tempo, se houver necessidade, é importante atualizar a política de privacidade, de modo que ela reflita a realidade das atividades diárias de tratamento da organização.

PONTO DE ATENÇÃO

CUMPRIR

- O comprometimento com a adequação das atividades de tratamento dos dados pessoais não é garantido apenas por meios técnicos, mas também por medidas organizacionais. A privacidade e a proteção de dados devem ser respeitadas em todos os âmbitos dentro de uma Instituição.

- **Demonstrar**

O agente de tratamento deve ser capaz de documentar a conformidade com a legislação de proteção de dados e a segurança do tratamento de dados pessoais. O produto/serviço deve ser concebido e desenvolvido de modo que o agente de tratamento possa documentar e demonstrar como os requisitos do regulamento de proteção de dados foram implementados.

Os exemplos incluem documentação que demonstre que o ambiente foi desenvolvido utilizando uma abordagem que garanta a proteção de dados desde a concepção e a segurança da informação. As seguintes ações são usadas para executar esta estratégia:

- **Registrar**: consiste na documentação das decisões tomadas e dos respectivos *logs* de sistemas, de modo a poder responder a anomalias.
- **Auditar**: dispõe sobre a auditoria e revisão regular dos *logs* e processos organizacionais que envolvam o tratamento de dados pessoais na organização.
- **Reportar**: compreende a apresentação de relatórios às Autoridades fiscalizadoras e manutenção destes registros para futuras prestações de contas.

PONTO DE ATENÇÃO

DEMONSTRAR

- Esta estratégia exige que o Controlador de dados pessoais seja capaz de demonstrar, especialmente à(s) autoridade(s) fiscalizadora(s), se a política de proteção de dados aplicável está sendo cumprida.

É importante pontuar que é possível a aplicação de mais de uma das ações citadas neste capítulo, ou seja, não é necessário escolher apenas uma em detrimento de outra. Portanto, dependendo do contexto do tratamento, há a possibilidade de combinação das estratégias ou pode ser que uma delas seja mais aplicável do que as outras. Desse modo, quanto mais estratégias forem aplicadas, mais "*privacy-friendly*" será o produto/serviço.

3.2. AMBIENTES DE *SOFTWARE*

É essencial garantir que os dados pessoais do usuário sejam suficientemente protegidos durante todo o ciclo de vida de um projeto. Assim, destaca-se, especialmente, a importância dos ambientes de pré-produção no desenvolvimento de um aplicativo e/ou plataforma digital.

O ambiente de produção tem por objetivo disponibilizar o produto/serviço para os usuários finais. Contudo, outros ambientes integram a criação das aplicações de *software* antes do lançamento aos usuários finais, como os de desenvolvimento (geralmente isolado ao dispositivo do desenvolvedor, isento de integrações com aplicações externas) e de homologação/*staging* (onde integrações com aplicações e bases de dados são testadas com maior precisão).

Assim, todos os testes devem ser concluídos antes da entrada ao ambiente de produção. Em vista disso, é recomendável manter os referidos ambientes separados, pois isso reduz o risco de modificações acidentais ou acessos não autorizados às aplicações e aos dados do negócio[36].

Cabe pontuar que dados pessoais e/ou confidenciais devem, sempre que possível, ser evitados para fins de testes. É preferível a utilização de dados sintéticos, ou seja, criados artificialmente a partir de dados reais (por exemplo, usando um algoritmo de aprendizado de máquina). Ainda, cita-se de forma exemplificativa serviços como o 4Devs, que é um *website* que permite ao usuário gerar números de CPF, CNPJ, entre outras informações com valores próximos ou similares a dados reais. Utilizar dados sintéticos no lugar de dados reais tem o benefício de evitar situações de violações aos dados pessoais caso algum dos ambientes de pré-produção seja comprometido.[37]

Contudo, se a utilização de dados pessoais para teste for estritamente necessária, convém que sejam implementadas medidas técnicas e organizacionais equivalentes àquelas usadas no ambiente de produção, para minimizar os riscos. Ainda, se tais medidas equivalentes não forem possíveis, é preciso que uma avaliação de riscos seja realizada para o controle apropriado das medidas de mitigação[38].

PONTO DE ATENÇÃO[39]

AMBIENTES DE *SOFTWARE*

- Dados pessoais reais não devem ser usados para fins de testes. Caso eles sejam usados fora do ambiente de produção, deve-se observar que os riscos de segurança também aumentam, como a possibilidade de comprometimento de confidencialidade, integridade ou disponibilidade da base de dados ou do serviço.
- É recomendável a criação de um conjunto de dados fictício que se pareça com os dados que serão tratados pelo aplicativo/plataforma.

[36] BRASIL. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ISO/IEC 27701:2019. *Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação*, p.50.
[37] SINGAPURA. Personal Data Protection Comission, op. cit, nota 22, p.10.
[38] BRASIL. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, op.cit., nota 35, p. 77.
[39] FRANÇA. Commission Nationale de l'Informatique et des Libertés. *GDPR developer's guide*.Disponível em:<link> Acesso em: 13 Ago. 2024.

3.2.1. TECNOLOGIAS DE APRIMORAMENTO DE PRIVACIDADE

Uma vez que as estratégias de privacidade do produto/serviço forem definidas e os padrões de privacidade forem projetados, chegamos ao momento de sua implementação utilizando soluções tecnológicas específicas. Deste modo, PETs são soluções que podem reduzir os riscos à privacidade e à proteção de dados pessoais.

Existem diferentes classificações de PETs, mas destacam-se, especialmente, dois grupos, que serão demonstrados na tabela abaixo. O primeiro grupo combina ferramentas e tecnologias que protegem ativamente a privacidade durante o tratamento de dados pessoais (ex.: ocultando dados pessoais ou eliminando a necessidade de identificação). O segundo grupo trata de ferramentas e tecnologias que apoiam procedimentos relacionados à gestão de privacidade, mas não ativamente operam com base nos dados[40].

CATEGORIA	SUBCATEGORIA	DESCRIÇÃO
Proteção de privacidade	Ferramentas de pseudonimização	Permitem transações sem solicitar informações pessoais identificadas.
	Produtos e serviços de anonimização	Fornecem acesso a serviços sem exigir dados identificados/identificáveis do titular.
	Fermentas de criptografia	Protegem documentos e transações de visualizações por terceiros.
	Filtros e bloqueadores	Evitam e-mails e conteúdo da web não desejados.
	Anti-rastreadores	Eliminam um possível rastreamento digital do titular de dados pessoais.
Gerenciamento de privacidade	Ferramentas de informação	Criam e verificam políticas de privacidade.
	Ferramentas administrativas	Gerenciam a identidade e permissões dos usuários.

Fonte: AEPD. Uma das possíveis classificações de PETs, 2019 (apud META Group Report, 2005)[41].

[40] ESPANHA. Agencia Española de Protección de Datos, op. cit., nota 15, p.28.
[41] ESPANHA. Agencia Española de Protección de Datos, op. cit., nota 15, p.28. Ministry of Science Technology and Innovation. Privacy Enhancing Technologies –META Group Report v1.1, Mar 2005. Disponível em: <link>. Acesso em: 01 ago. 2024.

3.3. PRIVACIDADE POR *DESIGN* E DADOS PESSOAIS DE CRIANÇAS

Em determinadas situações, é possível que os usuários da plataforma/sistema sejam crianças, ou seja, possuam até 12 (doze) anos de idade incompletos. Sobre o tema, evidencia-se que a ANPD publicou o Enunciado nº 1/2023, fixando a interpretação de que o tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da LGPD, desde que observado e prevalecente o seu melhor interesse.

É importante lembrar que se aplicam requisitos especiais se a plataforma/sistema for destinada a crianças. Por exemplo, é recomendável que as informações sobre o tratamento de dados pessoais delas sejam fornecidas de forma simples, clara e acessível, consideradas as características (físico motoras, perceptivas, sensoriais, intelectuais e mentais) do usuário dos produtos e serviços, conforme previsão do artigo 14, § 6º da LGPD.

Deste modo, imagens, ícones e símbolos podem ser usados para tornar as informações mais compreensíveis tanto para o entendimento da criança, quanto para proporcionar a informação necessária aos pais ou responsáveis legais. O uso de animação, vídeo e som também podem ser boas ferramentas para personalizar informações de acordo com o nível de compreensão do usuário.

Além disso, a depender da finalidade da plataforma/sistema, se possível, é recomendável que a criança tenha a opção de escolher quais elementos desse serviço ela deseja usar e, portanto, quantos dados pessoais ela precisa fornecer. Isto é particularmente importante para a coleta de dados pessoais, a fim de “melhorar” ou “personalizar” a experiência online dos usuários, para além da prestação do seu serviço principal.

De todo modo, a plataforma/sistema deverá coletar como “obrigatórios” apenas as informações necessárias para fornecer adequadamente o serviço/produto a que se propõe.

EXEMPLO

PLATAFORMA QUE PERMITE A UTILIZAÇÃO DE SERVIÇOS SEM NECESSIDADE DE *LOGIN*

- É aceitável coletar a localização de uma criança quando ela estiver usando uma aplicação baseada em mapas do seu serviço para ajudá-la a encontrar o caminho para um destino específico e fornecer um sinal óbvio para que ela saiba que sua localização está sendo rastreada.
- Contudo, não é recomendável continuar rastreando a localização após ela fechar o mapa ou chegar ao destino.

Destaca-se, ainda, que o artigo 12 da Resolução nº 245/2024[42] do Conselho Nacional dos Direitos da Criança e do Adolescente ("CONADA") indica que a privacidade de crianças e adolescentes deve ser respeitada e protegida em todos os ambientes e serviços digitais por padrão. Nesse sentido este dispositivo se conecta com os princípios da privacidade por *design*, conforme demonstrado no capítulo anterior.

RESUMO

PRIVACIDADE POR *DESIGN* EM AMBIENTES DIGITAIS

- As estratégias de privacidade por *design* quando aplicadas nas fases de concepção e desenvolvimento melhoram a privacidade do sistema.
- As estratégias orientadas a dados são de natureza mais técnica e se concentram no tratamento de dados que respeita a privacidade, sendo as principais táticas aplicáveis: minimizar, agregar, separar e ocultar.
- Já as estratégias orientadas a processo são de natureza mais organizacionais e são direcionadas a definição de processos que implementem a gestão responsável dos dados pessoais, sendo as principais táticas aplicáveis: informar, controlar, cumprir e demonstrar.
- Durante o desenvolvimento de um produto/serviço, convém evitar que dados pessoais sejam usados para propósitos de testes.
- O tratamento de dados pessoais de crianças em ambientes digitais deverá considerar o melhor interesse e o desenvolvimento psicossocial delas. Assim, os dados tratados pessoais devem ser proporcionais e não excessivos para realização das finalidades do tratamento.

[42] BRASIL. Ministério dos Direitos Humanos e da Cidadania/Secretaria Nacional dos Direitos da Criança e do Adolescente/Coordenação-Geral do Conselho Nacional dos Direitos da Criança e do Adolescente Resolução nº 245/2024. Disponível em: <link>. Acesso em: 17 mai. 2024.

4. CONSIDERAÇÕES FINAIS

Em síntese, este Guia buscou analisar os principais aspectos para aplicação da privacidade por *design* em ambientes digitais. Deste modo, é fundamental retomar alguns pontos centrais abordados ao longo deste documento.

Primeiramente, evidenciou-se que a privacidade por *design* tem por objetivo incorporar a privacidade durante todo o ciclo de vida de um serviço/produto. Nesse sentido, destacou-se a origem desse conceito e a sua correlação com os artigos 46, *caput* e §2º e 49 da LGPD. Ainda, foram citados os sete princípios fundamentais da privacidade por *design*, relacionando-os com os princípios previstos na LGPD.

Em seguida, buscou-se exemplificar medidas que podem ser incorporadas ao produto/serviço para melhorar a privacidade. Para tanto, foram citadas e exemplificadas estratégias orientadas a dados e estratégias orientadas a processos.

No tópico posterior, destacou-se a importância dos ambientes de desenvolvimento, evidenciando a diferença entre os ambientes de produção e homologação. Além disso, em vista de prover uma maior segurança, foi recomendado o uso de dados sintéticos para a finalidade de testes, antes do produto/serviço seguir para o ambiente de produção.

Também foi abordado brevemente tecnologias de aprimoramento de privacidade, citando-se dois grupos: proteção de privacidade e gerenciamento de privacidade. Por fim, foi mencionado acerca das especificidades para o tratamento de dados pessoais de crianças em ambientes digitais.

Atingido o fim deste Guia, espera-se que as ideias apresentadas possam contribuir e orientar sobre a aplicação de técnicas de privacidade por *design* em plataformas, aplicativos e sistemas.

FGV DCI

DIRETORIA DE
CONTROLES INTERNOS