

TUDO QUE VOCÊ PRECISA
SABER SOBRE

PRIVACY BY DESIGN E PRIVACY BY DEFAULT

08 DE MAIO DE 2020 – 13H30

PROF. MATHEUS PASSOS

- DPO L'ORÉAL PORTUGAL
- PROFESSOR CONVIDADO NA FDUNL (LISBOA)



O QUE É O *PRIVACY BY DESIGN* E O *PRIVACY BY DEFAULT?*



As legislações de proteção de dados (RGPD/LGPD) trazem novas obrigações aos agentes de tratamento, exigindo que estes integrem as preocupações com a proteção de dados em **cada aspecto de suas atividades de tratamento**. A isto chama-se (genericamente) de *privacy by design* e de *privacy by default*.



Privacy by design (“proteção de dados desde a concepção”): “a proteção de dados desde a concepção é, em última análise, uma abordagem que garante que você considere questões de privacidade e proteção de dados na fase de criação/concepção de qualquer sistema, serviço, produto ou processo e, em seguida, ao longo do ciclo de vida”.



Privacy by default (“proteção de dados por padrão”): “a proteção de dados por padrão exige que você trate apenas os dados necessários para atingir seu objetivo específico. Ela está vinculada a princípios fundamentais de proteção de dados como o da minimização e o da limitação de objetivos”.

Fonte: ICO (<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default>)

MAS A PROTEÇÃO DE DADOS POR PADRÃO NÃO É NOVA!

O conceito foi desenvolvido ainda na **década de 1990** por Ann Cavoukian, que atuou como Comissária de Informação e Privacidade de Ontário, Canadá, entre 1997 e 2014.

A Dra. Cavoukian criou e desenvolveu os chamados **7 PRINCÍPIOS FUNDAMENTAIS** da proteção de dados desde a concepção.

[Clique aqui para download \(em inglês\).](#)

PONTOS DE PARTIDA

“O futuro da privacidade não pode ser garantido apenas pelo cumprimento das estruturas regulatórias; em vez disso, a garantia da privacidade deve idealmente se tornar o modo de operação padrão de uma organização”.

O resultado da privacidade deve ser uma **soma positiva** entre privacidade e segurança, e não o “ou” da soma zero – que gera uma “falsa dicotomia”.

A proteção de dados desde a concepção se assenta em uma “trilogia”: a) Sistemas de TI; b) Práticas comerciais responsáveis; e c) Projeto físico e infraestrutura em rede.

Os **7 princípios fundamentais** podem ser aplicados a qualquer tipo de dado pessoal, mas com mais ênfase em dados sensíveis: a aplicação destes princípios pode variar conforme o nível de risco.

Os objetivos da proteção de dados desde a concepção são: para os **titulares**, garantir a privacidade e obter controle pessoal sobre as informações; para as **organizações**, obter uma vantagem competitiva sustentável.

Fonte: Ann Cavoukian, *The 7 Foundational Principles*.

I) AÇÃO PROATIVA, NÃO REATIVA; PREVENTIVA, NÃO CORRETIVA

- “A abordagem de proteção de dados desde a concepção (*privacy by design – PbD*) é caracterizada por medidas proativas e não reativas.
- “Ele antecipa e evita eventos invasivos de privacidade antes que eles aconteçam.
- “O PbD não espera que os riscos de privacidade se materializem, nem oferece remédios para resolver infrações de privacidade depois que elas ocorrerem – ele visa impedir que elas ocorram.
- “Em resumo, o Privacy by Design vem *antes do fato*, não depois”.
- Deve-se pensar a respeito da proteção de dados **desde o início do projeto**, e não quando o mesmo já estiver em desenvolvimento.

2) PRIVACIDADE COMO A CONFIGURAÇÃO PADRÃO



“Todos podemos ter certeza de uma coisa: o padrão ‘manda’! O PbD busca oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou prática comercial. **Se um indivíduo não faz nada, sua privacidade ainda permanece intacta.** Nenhuma ação é necessária por parte do indivíduo para proteger sua privacidade – ela é incorporada ao sistema *por padrão*”.



O utilizador **não precisa fazer absolutamente nada** para que sua privacidade esteja garantida.



Exemplo: pedidos de acesso à câmera quando um aplicativo é iniciado.

3) PRIVACIDADE INCORPORADA AO DESIGN



“O PbD está incorporado ao design e à arquitetura dos sistemas de TI e das práticas de negócios. Não é adicionado como um complemento, após o fato [ou processo]. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que está sendo entregue. A privacidade é parte integrante do sistema, **sem diminuir a funcionalidade**”.



A privacidade não pode ser vista como um impedimento ou como uma dificuldade ao desenvolvimento dos processos que envolvem dados pessoais.

4) FUNCIONALIDADE TOTAL – SOMA POSITIVA, NÃO SOMA ZERO

- “O PbD busca acomodar todos os interesses e objetivos legítimos de maneira positiva em que **todos saem ganhando** e não por meio de uma abordagem antiquada de soma zero, em que trocas [trade-offs] desnecessárias são feitas.
- “O PbD evita a **pretensão de falsas dicotomias**, tais como privacidade versus segurança, demonstrando que é possível ter ambas”.
- Portanto, não há que se falar em garantia da privacidade **OU** da segurança.
- Exemplo claro: situação de pandemia.



5) SEGURANÇA DE PONTA A PONTA – PROTEÇÃO TOTAL DO CICLO DE VIDA

- “O PbD, tendo sido incorporado ao sistema **antes do primeiro dado pessoal ser coletado**, se estende com segurança por **todo o ciclo de vida dos dados envolvidos** – fortes medidas de segurança são essenciais para a privacidade, do início ao fim.
- “Isso garante que todos os dados sejam retidos com segurança e destruídos com segurança no final do processo, em tempo hábil.
- “Assim, o PbD garante, **do início ao fim**, o gerenciamento seguro do ciclo de vida das informações, **de ponta a ponta**”.
- Isto é, não se pode falar em proteção de dados apenas “nesta” ou “naquela” fase da atividade de tratamento de dados, mas sim do início ao fim – *incluindo na (eventual) etapa de anonimização*.

6) VISIBILIDADE E TRANSPARÊNCIA – “MANTENHA ABERTO”

- “O PbD busca garantir a todos os interessados que, independentemente da prática ou tecnologia comercial envolvida, ela [a proteção de dados] esteja de fato operando **de acordo com as promessas e objetivos declarados**, sujeita a verificação independente.
- “Suas partes integrantes e suas operações permanecem **visíveis e transparentes**, tanto para utilizadores quanto para fornecedores.
- “Lembre-se, **confie, mas verifique**”.
- Não adianta “falar” que você garante a privacidade em todo o ciclo de vida: **isto precisa ser comprovado de maneira independente** (*princípio da responsabilidade*).

7) RESPEITO PELA PRIVACIDADE DO UTILIZADOR – CENTRADO NO UTILIZADOR

- “Acima de tudo, o PbD exige que arquitetos e operadores mantenham os interesses do titular de dados pessoais em primeiro plano, oferecendo medidas como padrões de privacidade fortes, avisos de privacidade apropriados e opções empoderantes [*empowering*] para o utilizador.
- “Mantenha o PbD **centrado no utilizador**”.

COMO APLICAR ESTES PRINCÍPIOS NO TRATAMENTO DE DADOS PESSOAIS?

A própria Dra. Ann Cavoukian publicou **outro documento** referente aos 7 princípios fundamentais intitulado “Implementation and Mapping of Fair Information Practices” – algo como “Implementação e Mapeamento de Práticas Justas de Informação”.



“Os princípios universais das Fair Information Practices (FIPs) são sustentados pelos de PbD, mas vão além deles para buscar o mais alto padrão global possível.

“Estendendo-se além dos FIPs, o PbD representa uma ‘ampliação’ significativa do nível na área de proteção da privacidade”.



“A privacidade [...] evoluiu ao longo dos anos: além de ser vista apenas como um requisito legal de conformidade, [passou a ser] também reconhecida como um **imperativo de mercado** e um **facilitador crítico da confiança** e das liberdades em nossa atual sociedade da informação”.

COMO APLICAR ESTES PRINCÍPIOS NO TRATAMENTO DE DADOS PESSOAIS?

A PRIVACIDADE DEVE SER INCORPORADA AOS SISTEMAS E TECNOLOGIAS DE DADOS EM REDE POR PADRÃO.

A PRIVACIDADE DEVE SE TORNAR **PARTE INTEGRANTE** DAS PRIORIDADES ORGANIZACIONAIS, OBJETIVOS DO PROJETO, PROCESSOS DE DESIGN E OPERAÇÕES DE PLANEJAMENTO **DE TODOS OS PROCESSOS DE UMA ORGANIZAÇÃO**.

COMO IMPLEMENTAR AS “FAIR INFORMATION PRACTICES”?

I) AÇÃO PROATIVA, NÃO REATIVA; PREVENTIVA, NÃO CORRETIVA

Deve haver:

Um compromisso claro, nos níveis mais altos da organização, em **definir e fazer cumprir altos padrões de privacidade**, geralmente **mais altos** do que os padrões estabelecidos pelas leis e regulamentos globais.

Um compromisso de privacidade que é comprovadamente compartilhado por comunidades de utilizadores e partes interessadas, em uma **cultura de melhoria contínua**.

Métodos estabelecidos para reconhecer projetos de privacidade inadequados, antecipar práticas de privacidade inadequadas e seus resultados, e corrigir quaisquer impactos negativos **muito antes de ocorrerem**, de maneira proativa, sistemática e inovadora.

COMO IMPLEMENTAR AS “FAIR INFORMATION PRACTICES”?

2) PRIVACIDADE COMO A CONFIGURAÇÃO PADRÃO

- Corresponde à proteção de dados por padrão (“*privacy by default*”) e sustenta-se pelos seguintes princípios:
 - **Definição clara de finalidades**, com transparência para com o titular de dados;
 - **Limitação da coleta de dados pessoais** – limitação das finalidades;
 - **Minimização dos dados**;
 - **Limitação de uso, retenção e divulgação.**

COMO IMPLEMENTAR AS “FAIR INFORMATION PRACTICES”?

3) PRIVACIDADE INCORPORADA AO DESIGN

01

Deve-se adotar uma **abordagem sistêmica e baseada em princípios** para incorporar a privacidade no seu projeto. Esta abordagem deve se basear em padrões e estruturas aceitos, passíveis de revisões e auditorias externas.

02

Sempre que possível, avaliações de impacto e de riscos à privacidade detalhadas devem ser realizadas e publicadas, **documentando de maneira clara os riscos à privacidade e todas as medidas tomadas para mitigá-los**, incluindo a consideração de alternativas e a seleção de métricas.

03

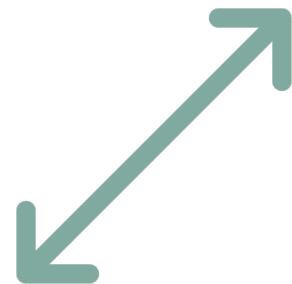
Os impactos na privacidade resultantes da tecnologia, da operação de tratamento ou da arquitetura de informações, bem como seus usos, devem ser **comprovadamente minimizados e não facilmente degradados por uso, configuração incorreta ou erro**.

COMO IMPLEMENTAR AS “FAIR INFORMATION PRACTICES”?

4) FUNCIONALIDADE TOTAL – SOMA POSITIVA, NÃO SOMA ZERO



A privacidade deve ser incorporada ao produto ou serviço de forma que **a funcionalidade completa do mesmo não seja prejudicada** e, na maior extensão possível, que todos os requisitos sejam otimizados.



A privacidade é muitas vezes posicionada em uma perspectiva de soma zero, como se tivesse de competir com outros interesses legítimos, objetivos de design e/ou recursos técnicos. O PbD rejeita essa abordagem: ele abrange todos os objetivos legítimos de “não privacidade” e os adapta, de maneira inovadora, com foco em uma **situação de soma positiva**.



Todos os interesses e objetivos devem ser claramente documentados, as funções desejadas articuladas, as métricas acordadas e aplicadas, e os trade-offs rejeitados por serem **frequentemente desnecessários**, a fim de encontrar uma solução que permita a multifuncionalidade.

COMO IMPLEMENTAR AS “FAIR INFORMATION PRACTICES”?

5) SEGURANÇA DE PONTA A PONTA – PROTEÇÃO TOTAL DO CICLO DE VIDA

Segurança: as organizações devem assumir a responsabilidade pela segurança dos dados pessoais (geralmente compatíveis com o grau de sensibilidade) durante todo o ciclo de vida, consistente com os padrões que foram desenvolvidos por organismos reconhecidos de desenvolvimento de padrões.

Os padrões de segurança aplicados devem garantir a **confidencialidade, a integridade e a disponibilidade** (CID) dos dados pessoais durante todo o seu ciclo de vida, incluindo, entre outros, métodos de destruição segura, criptografia apropriada e métodos seguros de controle de acesso e registro.

COMO IMPLEMENTAR AS “FAIR INFORMATION PRACTICES”?

6) VISIBILIDADE E TRANSPARÊNCIA – “MANTENHA ABERTO”



Responsabilização (accountability): a coleta de dados pessoais implica em um dever de cuidar de sua proteção. A responsabilidade por todas as políticas e procedimentos relacionados à privacidade deve ser documentada e comunicada conforme apropriado e atribuída a um indivíduo específico. Ao transferir informações pessoais para terceiros, uma proteção de privacidade equivalente deve ser garantida – por meios contratuais ou outros.



Abertura: abertura e transparência são fundamentais para a prestação de contas. As informações sobre as políticas e práticas relacionadas ao gerenciamento de informações pessoais devem ser prontamente disponibilizadas aos titulares.



Conformidade: devem ser estabelecidos mecanismos para reclamação e reparação, e informações sobre tais mecanismos devem ser comunicadas aos titulares de dados, incluindo como acessar o próximo nível de recurso. As etapas necessárias para monitorar, avaliar e verificar a conformidade com as políticas e procedimentos de privacidade devem ser tomadas.

COMO IMPLEMENTAR AS “FAIR INFORMATION PRACTICES”?

7) RESPEITO PELA PRIVACIDADE DO UTILIZADOR – CENTRADO NO UTILIZADOR

Consentimento: o consentimento livre e específico do indivíduo é necessário para a coleta, uso ou divulgação de informações pessoais, exceto quando existirem outras bases legais permitidas por lei. Quanto maior a sensibilidade dos dados, mais clara e específica será a qualidade do consentimento necessário. O consentimento pode ser retirado posteriormente.

Precisão: os dados pessoais devem ser precisos, completos e atualizados conforme o necessário para cumprir os propósitos especificados.

Acesso: os titulares devem ter acesso aos seus dados pessoais e ser informados sobre seus usos e divulgações. Os titulares devem ser capazes de contestar a precisão e a integridade dos dados e alterá-los conforme apropriado.

Conformidade: as organizações devem estabelecer mecanismos para reclamação e reparação, e informações sobre tais mecanismos devem ser comunicadas aos titulares de dados, incluindo como acessar o próximo nível de recurso.

QUEM DEVE CUMPRIR O PBD NO REGULAMENTO EUROPEU?

- Conforme o Regulamento Europeu, **apenas o responsável pelo tratamento (controlador)** deve aplicar os princípios do *Privacy by Design* e do *Privacy by Default*.
- Artigo 25.º, n.º 1: “[...] o **responsável pelo tratamento** aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados”.
- Artigo 25.º, n.º 2: “**O responsável pelo tratamento** aplica medidas técnicas e organizativas para assegurar que, por defeito [por padrão], só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento [...].”

E O OPERADOR?

O operador **não é obrigado** a cumprir os princípios do PbD.

No entanto, o artigo 28.º especifica as **considerações que o controlador deve ter sempre que estiver selecionando um operador**. Por exemplo, o controlador deve usar apenas operadores “que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do presente regulamento e assegure a defesa dos direitos do titular dos dados”.

Esse requisito abrange a **proteção de dados desde a concepção** presente no artigo 25.º, bem como suas **obrigações de segurança** nos termos do artigo 32.º (*todos do Regulamento Europeu*).

O operador não pode necessariamente ajudá-lo com suas obrigações de PbD (*ao contrário das medidas de segurança*); no entanto, o **controlador deve contratar apenas operadores que forneçam garantias suficientes para atender aos requisitos do RGPD**.

E NA LGPD?

- Não há um artigo específico sobre o PbD, mas pode-se inferi-lo a partir dos seguintes artigos:
 - Art. 6º, VIII – princípio da prevenção (*aplicado a controladores apenas*): “adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais”;
 - Art. 46, § 2º (*aplicado a controladores e operadores*): “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 (*aplicado a controladores e operadores*): “os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares”;
 - Art. 50, § 2º (*aplicado a controladores apenas*): “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; [...].”

OBRIGADO!

<https://profmatheus.com/webinares-gratuitos>

profmatheuspassos 

profmatheuspassos 

profmatheuspassos 

WEBINAR | INSCRIÇÕES PELO SYMLA

PROTEÇÃO DE DADOS E A CARREIRA DE DPO

DIA 08/05

às 17:00 HORÁRIO BRASÍLIA

MATHEUS PASSOS
DPO DA L'OREAL



RENATA LUZ
REPRESENTANTE ANPPD

RODRIGO AZEVEDO
MEMBRO ANPPD

CAP. WILLIAM LIMA
SESDEC

GABRIEL TEIXEIRA
MEMBRO ANPPD

MÁRCIO BASSANI
MEMBRO ANPPD
ADVOGADO

Symplä



Project Management Institute Distrito Federal

WEBINAR

08/05, 18h30



Matheus Passos

Alysson Ribeiro

Ana Palu

Inscreve-se: <https://linktr.ee/pmidf>

Oportunidades e impactos da LGPD na gestão de projetos

EVENTOS AINDA HOJE



Informações detalhadas : <https://bit.ly/maratona-prot-dados>

Inscrições: <https://bit.ly/inscricao-maratona-pd>

@profmatheuspassos

Maratona de PROTEÇÃO DE DADOS



25 A 29 DE MAIO



- Demetrius Klitou, *A solution, but not a panacea for defending privacy: the challenges, criticism and limitations of privacy by design*. In: *Privacy technologies and policy: first annual privacy forum*. APF 2012, Springer, Heidelberg, 2014.
- John J. Borking et all, *Privacy-enhancing technologies: the path to anonymity*, I e II. Ontário, Canadá; Países Baixos, 1995.
- Considerandos 78, 87 e 108 do RGPD.
- EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 2019.

REFERÊNCIAS PARA SABER MAIS