CEST Centro de Estudos Sociedade e Tecnologia
USP Universidade de São Paulo
Boletim - Volume 6, Número 06, Agosto/2021

Privacy by Design e Privacy by Default

Marcel Simonette

Com várias regulamentações de proteção de dados em todo o mundo, compreender os conceitos é essencial para construir uma boa base de conhecimento de como se deve lidar com a proteção de dados e privacidade sem sobrecarregar as áreas de *compliance*. Ao mesmo tempo, proteção e uso de dados pessoais não são apenas uma questão de conformidade; trata-se de construir uma relação de confiança com clientes e consumidores. Confiança é a chave para todas as empresas, especialmente aquelas que operam online.

A regulamentação europeia General Data Protection Regulation (GDPR) é o conjunto de normas regulatórias para práticas de uso de dados que foi criada pelo Parlamento Europeu e pelo Conselho da União Europeia. Essa regulamentação incorpora conceitos como Privacy by Design e Privacy by Default, e trata da diversidade de dados, seja um cookie de navegador, por exemplo, ou o nome e endereço de uma pessoa. A proteção de dados envolve dois conceitos fundamentais: transparência e responsabilidade.

As empresas precisam ter a proteção de dados e a privacidade em mente a cada passo que envolva o processamento de dados pessoais

Privacy by Design

Privacy by Design, também conhecido como PbD, é um conjunto de princípios elaborados na década de 90 pela Comissária de Informação e Privacidade de Ontário, Canadá, Dra. Ann Cavoukian. Uma entrevista com a Dra. Ann Cavoukian está disponível no canal do CEST no YouTube. Privacy by Design afirma que as empresas precisam ter em mente a proteção de dados e a privacidade em todas as etapas que envolvem o processamento de dados pessoais. Na prática, as iniciativas das empresas devem garantir que a privacidade e a proteção de dados sejam consideradas desde a idealização de qualquer inciativa que envolva dados pessoais, seja por iniciativa da área de TI ou de qualquer outra área da empresa. Projetos internos, desenvolvimento de produtos, desenvolvimento de software e sistemas de TI são alguns exemplos de iniciativas de empresas.

Apesar de ter sido criada na década de 1990, a Privacy by Design está diretamente relacionada com o GDPR. Seguir os princípios de privacidade desde a concepção de um projeto reduzem os riscos de privacidade e geram confiança, pois são medidas proativas, em vez de reativas. Os princípios não oferecem soluções para resolver infrações de privacidade uma vez que tenham ocorrido; eles têm como objetivo evitar a ocorrência de infrações. Em suma, Privacy by Design vem antes do fato, não depois.

Para colocar em prática as ideias de Privacy by Design, é necessário que se compreenda os pilares que a sustentam, pois esses princípios mudam a forma como muitas empresas idealizam seus projetos e ações.

A Privacy by Design é composta por sete princípios fundamentais:

- Seja proativo ao invés de reativo, opte por prevenir ao invés de curar;
- A privacidade e proteção dos dados pessoais deve ser garantida em todos os momentos, sem a necessidade de configurações por parte das pessoas (privacidade é uma configuração padrão);
- Incorporar a privacidade ao projeto, privacidade não pode ser considerada apenas como algo a mais no projeto, ela é parte do que será desenvolvido (privacidade embutida no design);
- Todas as funcionalidades possíveis devem estar completas e protegidas, gerando um benefício mútuo, para as pessoas e para a empresa (soma positiva, não soma zero);
- A segurança deve estar presente desde a captura até a destruição dos dados, e no compartilhamento dos dados, ou seja, ponta a ponta (proteção total do ciclo de vida);
- Manter a transparência com o titular dos dados, informando sobre o motivo da coleta da

informação e quem tem acesso a ela (visibilidade e transparência);
- A privacidade das pessoas deve ser sempre respeitada.

O foco de todas as ações da empresa deve ser justamente seus clientes ou consumidores. Deve ser garantido pela empresa que os dados estão protegidos e totalmente seguros.

Privacy by Default

Privacy by Default significa que as empresas precisam projetar seus sistemas, serviços, produtos e práticas comerciais para proteger automaticamente os dados pessoais. As pessoas não precisam tomar nenhuma providência para proteger seus dados - a privacidade está intacta e elas não precisam fazer nada. E, se o produto ou serviço exigir dados pessoais para permitir o uso ideal desse produto ou serviço, esses dados serão mantidos apenas pelo tempo necessário. Se mais dados do que o necessário forem solicitados, a "privacidade por padrão" foi violada.

A maioria das pessoas está apenas procurando conveniência e não se preocupa em descobrir como alterar as configurações de privacidade. Nesse cenário, a Privacy by Default é um diferencial para as empresas que valorizam a transparência. As empresas esclarecem os dados necessários e como as pessoas podem alterar a configuração padrão e suas consequências, fortalecendo a confiança no relacionamento. As pessoas ficam protegidas e são informadas de quais dados elas estão fornecendo e para quais finalidades.

A configuração de privacidade mais restritiva possível é estabelecida a partir do momento zero. Apenas os dados essenciais para fornecer o serviço ou entregar o produto são coletados.

Privacy by Design e Privacy by Default

Privacy by Design é sobre como um projeto deve ser desenvolvido por meio dos princípios mencionados acima. Desde o início de qualquer projeto envolvendo dados pessoais, é necessário considerar a segurança e privacidade dos dados, antecipando problemas e reduzindo o risco de furto e vazamento de dados.

Os projetos gerados por meio desse conceito são proativos. Eles oferecem controle para que as pessoas alterem as configurações padrão do sistema, optando por fornecer os dados ou não.

Quando falamos sobre Privacy by Default, é necessário entender que "por padrão" significa que as configurações mais seguras são aplicadas por padrão assim que o produto ou serviço é lançado ao público. Ou seja, as pessoas não precisam escolher as configurações de privacidade e proteção, pois essas configurações são pré-configuradas considerando a privacidade. Todas as informações pessoais fornecidas são coletadas apenas para a entrega do serviço ou produto. Mesmo com Privacy by Design e Privacy by Default, todos os dados necessários devem ser informados às pessoas, bem como a finalidade de cada um deles.

Quando se fala em tempo de armazenamento dos dados, vale ressaltar que eles são mantidos apenas pelo período em que o projeto ou sistema irão utilizá-los.

É possível entender que a Privacy by Default é uma consequência da Privacy by Design. Ambas são estratégias que, quando bem executadas, garantem a privacidade, ponto fundamental hoje em dia.

Relações com a LGPD

Apesar da Privacy by Design e Privacy by Default estarem presentes na GDPR, a legislação brasileira LGPD (Lei Geral de Proteção de Dados) não tem esses princípios explicitamente. No entanto, a legislação brasileira possui conceitos semelhantes ligados à proteção de dados, ditando como as empresas devem garantir a segurança.

Vale ressaltar que embora a LGPD não exija que as empresas sigam os princípios da Privacy by Design e da Privacy by Default, não há nada que impeça que se utilize esses princípios. Por fim, Privacy by Design e Privacy by Default ajudam as empresas a oferecer mais segurança e privacidade aos dados. Além disso, as pessoas passam a ser o principal moderador de seus dados, elas ganham controle sobre quais dados serão fornecidos e quais não serão, sabendo quais dados são obrigatórios para a finalidade explicitamente declarada pela empresa.

Marcel Simonette ***é*** *pesquisador do CEST-USP e professor do MBA-USP em Data Science and Analytics do PECE – USP*

Coordenador Acadêmico: Edison Spina

Este artigo resulta do trabalho de apuração e análise do autor, não refletindo obrigatoriamente a opinião do CEST.