

## Governança em Privacidade.

Processos, produtos e serviços com desenho de privacidade não surgem do nada. Eles são o resultado de uma verdadeira estruturação de governança: uma governança específica, voltada à privacidade. Quando falamos disso, logo vem à mente o cargo do DPO – o Data Protection Officer. Criado na legislação alemã nos anos 70, para que a lei de proteção de dados fosse efetivamente aplicada nas empresas, ele continua com essa função principal: fazer a lei de proteção de dados ser realidade nas empresas.

Aqui no Brasil, o DPO ganhou um nome em português: é o encarregado pelo tratamento de dados pessoais. Ele pode ser uma pessoa física ou jurídica, como uma empresa que presta serviços de DPO: é o DPO as a service. Ele é uma pessoa que entende de segurança da informação, mas também comprehende profundamente a legislação de proteção de dados. Ele é autônomo, não recebe ordens para o exercício das suas funções, e responde apenas para o mais alto nível hierárquico da empresa. Mas também é alguém de confiança, pois vai ter acesso a todos os dados da empresa. É um cargo-chave, sem dúvida, mas um cargo só não faz governança.

De acordo com o tamanho da empresa, o contexto, a complexidade e a criticidade dos dados que ela trata, deve-se pensar em um modelo de governança que faça sentido para ela! Podemos ter, por exemplo, todo um time de privacidade.

O DPO é o cargo mencionado pela lei, mas existem outros – Data Chief Officers, Privacy Leaders, entre tantos outros! Esse time deve ser responsável por elaborar a Política de Privacidade – integrada às demais políticas, principalmente à Política de Segurança da Informação, além de redigir documentos e fazer análises importantes sobre a criticidade dos dados tratados, o impacto das atividades de tratamento nos titulares, como o Relatório de Impacto à Proteção de Dados Pessoais e o Legitimate Interest Assessment.

Eles participam desde logo na preparação de uma resposta para incidentes de segurança, que funciona como uma brigada de incêndio treinada – mas para o vazamento de dados. A LGPD, assim como a legislação europeia, exige que a Autoridade Nacional de Proteção de Dados seja comunicada quando houver violação de dados e mais: exige que os titulares afetados sejam comunicados também. Isso, claro, pode gerar um dano reputacional grave às empresas, que devem estar preparadas para uma comunicação assertiva para sobreviver – e sair mais forte – de um data breach.

Essas equipes, no momento da adequação à LGPD, são o ponto focal do projeto – e cuidam do mapeamento das atividades de tratamento de dados, da classificação de prioridades com base em risco no gap analysis, que é a análise dos pontos em desconformidade com a lei, e da construção de um plano de ação efetivo. Existem vários frameworks que servem de guia para implementação desse projeto. Depois da adequação, eles cuidam do monitoramento do compliance de dados e devem adotar métricas específicas de performance para garantir sua efetividade e conscientizar a todos sobre o valor de privacidade e proteção de dados para a empresa.

De forma geral, todos devem saber que privacidade importa e como aplicar esse valor em seu dia a dia. Além disso, eles acompanham cada novo projeto desde o início, para que eles tenham um desenho de privacidade. É o que chamamos de Privacy by Design. O termo foi cunhado nos anos 90, por Anne Cavoukian, e observa 7 grandes princípios:  
O primeiro é ser preventivo e nunca reativo. Isso trata especialmente de segurança, porque em dados, como já vimos, não há volta atrás! Uma vez que o dado perde a confidencialidade e que pessoas que não deveriam ter acesso a ele, o tem, não há como des-saber, como desconhecer algo que já se conhece.

Depois, privacidade deve ser padrão sempre. A gente nunca pode presumir que o usuário aceita compartilhar os seus dados. Por isso, todas as configurações de produtos e serviços devem ter como padrão a privacidade. Ela deve estar embarcada no design.

Além disso, o meu favorito: funcionalidade completa, com soma positiva diferente de zero. É uma referência à teoria dos jogos, que significa que tecnologia e privacidade não podem ser consideradas um jogo onde sempre que um ganha, o outro perde. Por que não pensamos em tecnologia e privacidade como um jogo de ganha-ganha. Sempre que eu ganho em tecnologia, eu ganho em privacidade e vice-versa! Segurança ponta a ponta, por todo o ciclo de vida do dado, também é fundamental! Uma vulnerabilidade técnica em algum ponto da jornada do dado na empresa é o bastante para por tudo a perder.

Por isso, o mapeamento é importante e a reflexão sobre se as medidas de segurança técnicas e administrativas que já foram adotadas são suficientes para proteger os pontos em que transitam dados pessoais. Visibilidade e transparência para o usuário, sobre o tratamento de dados pessoais.

E o meu favorito – esse é meu segundo favorito? Rs – É, esse é o principal favorito: respeito pelo usuário. Isso resume bem toda a legislação de proteção de dados. Em um mundo onde a velocidade faz com que muitas vezes as pessoas não olhem para o outro, não sintam empatia, falar em proteção de dados pessoais é, no fundo, se perguntar como eu e minha atividade impactamos o outro.

É se colocar no lugar dele por um instante, para saber de forma legal, mas também de forma ética, por qual caminho seguir. Um dos meus filósofos atuais favoritos, o Luciano Floridi diz que em tecnologia a gente tem sempre a tentação de ir cada vez mais rápido, mas que deve se perguntar: para onde?

Eu espero que essa conversa ajude você a refletir para onde quer ir e como vai desenvolver tecnologia e respeito com o outro.