

Privacidade de Dados: a quanto nos obrigas?

digitalinside.pt/privacidade-de-dados-a-quanto-nos-obrigas/



Celebrado a 28 de janeiro, o Dia Internacional da Privacidade de Dados, simboliza um marco significativo na consciencialização de todos os cidadãos para a importância da proteção dos dados pessoais. Esta data foi escolhida por ocasião da assinatura, em 1981, da Convenção 108 do Conselho da Europa, referente ao primeiro tratado internacional que abordou especificamente a proteção de dados pessoais. A implementação deste dia visa destacar a necessidade de salvaguardar a privacidade neste mundo cada vez mais digital, onde as informações pessoais são frequentemente partilhadas online. Esta

data simbólica serve o propósito primordial, para que, indivíduos, organizações e governos, exerçam as suas responsabilidades na garantia de proteção dos dados pessoais e na promoção da ética e boas práticas no tratamento de informações sensíveis.

Também a evolução legislativa no campo da proteção de dados tem sido pautada por significativos marcos regulatórios, visando adaptar-se ao rápido avanço da tecnologia e à crescente importância dos dados pessoais nesta era digital. A Diretiva de Proteção de Dados, adotada pela União Europeia em 1995, foi aliás, um dos primeiros esforços relevantes nesse sentido, estabelecendo princípios fundamentais para o tratamento de dados pessoais. Contudo, através da acelerada evolução tecnológica, foi exigida uma atualização vigorosa, culminando na implementação do Regulamento Geral de Proteção de Dados (RGPD) no ano de 2018. Doravante, o RGPD representou uma mudança significativa na abordagem à proteção de dados, introduzindo padrões mais rigorosos, direitos ampliados para os titulares dos dados e coimas substanciais para violações, promovendo uma cultura de responsabilidade e transparência no tratamento de informações pessoais.

Há que considerar também a Diretiva ePrivacy, que está em constante desenvolvimento, com foco específico nas comunicações eletrónicas e na privacidade online. O seu propósito vem complementar o RGPD, estabelecendo regras próprias para a confidencialidade de informações neste tipo de comunicações, como são os e-mails e mensagens instantâneas.

Estas legislações refletem a crescente tomada de consciência sobre a importância da proteção de dados num mundo digitalizado, procurando equilibrar os interesses comerciais com a salvaguarda dos direitos fundamentais dos indivíduos em relação à sua privacidade e, sobretudo, ao controlo sobre suas informações pessoais.

Devemos estar bem conscientes dos atuais desafios e das preocupações em matéria de privacidade relacionados com os motores de busca, analytics & big data, redes sociais e da transposição da vida social para o digital, realidade esta que implica um elevado impacto, a saber:

- 1) recolha excessiva de dados** – empresas e organizações recolhem uma quantidade massiva de dados sobre os utilizadores, seja por meio de motores de busca, redes sociais ou serviços de big data. Tal facto, levanta sérias questões sobre esta necessidade, e se, os utilizadores estão cientes do âmbito dessa recolha de dados pessoais;
- 2) análise de dados e perfilagem** – isto é, ferramentas de analytics e big data são capazes de analisar grandes volumes de dados para criar perfis detalhados dos utilizadores, resultando numa personalização extrema de conteúdo, e em simultâneo, num procedimento invasivo;
- 3) privacidade nas redes sociais** – as quais têm sido um terreno fértil para a recolha de dados pessoais. Questões de privacidade surgem quando essas plataformas partilham informações com terceiros ou utilizam dados para fins publicitários sem o consentimento claro dos mesmos;
- 4) transposição da vida social para o digital** – a pandemia acelerou esta transição com mais interações a acontecer em formato online, facto que despoletou a quantidade de dados gerados e partilhados, além de levantar questões como a segurança de videochamadas e a privacidade em

ambientes virtuais;

5) algoritmos de recomendação – utilizados em motores de busca, redes sociais e plataformas de entretenimento, limitam a diversidade de informações a que os utilizadores acedem, podendo levar a visões distorcidas do mundo e reforçar preconceitos;

6) segurança cibernética – com a crescente quantidade e disponibilidade de dados online, crescem também os riscos de violações de segurança cibernética. Fugas de dados poderão implicar sérias consequências para a privacidade das pessoas.

7) legislação e regulamentação – a necessidade de regulamentação e legislação eficaz para proteger a privacidade digital é um desafio em si mesmo. Em todos os países do mundo e com especial foco para o trabalho da Comissão Europeia, têm sido adotadas diferentes abordagens para enfrentar essas questões, contudo, a harmonização de normas globais é ainda complexa.

Para lidar com estes desafios, é crítico que haja um equilíbrio entre a inovação tecnológica e a proteção da privacidade individual. O futuro trará ainda mais ameaças à privacidade e à proteção de dados pessoais, com a expansão da inteligência artificial, a proliferação de deepfakes e o incremento do hacktivismo. O legislador necessitará de dar respostas céleres e efetivas, sob pena de promulgar leis que já nasçam defasadas do nosso tempo. A consciencialização dos utilizadores, a transparência nas práticas de recolha de dados e a implementação de regulamentações adequadas constituem passos vitais para enfrentar estes desafios, e garantir que a privacidade seja respeitada nesta era digital que a tanto nos obriga.

Bruno Castro é Fundador & CEO da VisionWare