Informação da CNPD e recomendações

Exposição de dados pessoais de redes sociais afeta milhões de utilizadores em Portugal

No passado fim-de-semana, foram expostos na Internet dados pessoais de 533 milhões de utilizadores da rede social Facebook, nos quais se incluem dados de mais de 2 milhões de utilizadores de Portugal. Também a rede social Linkedin viu publicamente expostos alguns registos dos seus utilizadores como prova de que foram obtidos por terceiros dados pessoais de cerca de 500 milhões de utilizadores.

Nos últimos três dias, a Comissão Nacional de Proteção de Dados (CNPD) tem trocado informação relevante sobre ambos os casos com a sua congénere irlandesa (Data Protection Commission – DPC), que atua como interlocutora do Facebook e do Linkedin na União Europeia, uma vez que ambas as empresas têm o seu estabelecimento principal na Irlanda.

Até ao momento, ainda não foi possível apurar todos os factos. Quer o Facebook quer o Linkedin estão a proceder a investigações internas para responder às várias questões colocadas pela autoridade irlandesa.

De acordo com informações prestadas pelo Facebook, ocorreu um incidente de segurança entre junho de 2017 e abril de 2018, devido a uma vulnerabilidade que o Facebook continha na funcionalidade de importação de contactos, que permitiu que dados pessoais de milhões de utilizadores fossem ilegalmente recolhidos na rede social e posteriormente divulgados na Internet. Estão ainda a ser averiguadas as circunstâncias em que tal incidente de segurança ocorreu e qual a sua relação com a exposição pública de dados daquela rede social em 2018, 2019 e, agora, em 2021.

Numa primeira análise aos registos relativos a utilizadores de Portugal, a CNPD verificou que, além de alguns dados corresponderem a informação publicamente disponível nos respetivos perfis, na sua grande maioria contêm números de telefone dos utilizadores e, em alguns casos, também endereços de email.

O Linkedin[1], por seu lado, afirma que os dados dos seus utilizadores foram recolhidos, por terceiros, a partir dos perfis publicamente disponíveis. A amostra de dados tornada pública contém também números de telefone dos utilizadores.

[1] O Linkedin tem disponível um contacto público para pedidos de informações ou reclamações: dpo@linkedin.com

A exposição pública desta quantidade de números de telefone, associados a outros dados pessoais, suscita grandes preocupações e requer a adoção de medidas não só por parte dos utilizadores, mas também de algumas entidades públicas e privadas para prevenir ou mitigar ações de usurpação de identidade para fins ilícitos, incluindo o cometimento de crimes.

Nesse sentido, **a CNPD recomenda** o seguinte:

1. Aos utilizadores do FB e do Linkedin:
    - Devem estar atentos ao recebimento de mensagens não solicitadas ou de origem desconhecida, que podem ter fins maliciosos, seja por email (*phishing*) ou por SMS (*smishing*), devendo apagar de imediato essas mensagens e, em particular, nunca devem clicar nos links contidos nas mensagens;
    - Devem estar especialmente alertados para perdas ou dificuldades em captação do sinal de rede de telemóvel em locais onde habitualmente costumam ter boa rede, devendo reportar esse facto de imediato à respetiva operadora telefónica;
    - Sempre que usem o endereço de email ou o número de telefone como 'nome de utilizador' (*username*) para aceder a um determinado website ou serviço, e desde que tal seja permitido pelo próprio sistema, devem alterar esses dados de autenticação (login); e devem solicitar à entidade em causa que deixe de aceitar o endereço de email ou número de telefone como dados de autenticação;

2. Aos operadores telefónicos:
    - Devem fazer uma verificação cuidada e segura da identidade do titular do contrato, no caso de pedidos de segunda via do cartão SIM;
    - Devem criar canais específicos de atendimento aos clientes para reporte de situações de perda inexplicável de sinal da rede telefónica e adotar procedimentos internos que permitam responder com rapidez e eficácia a eventuais interferências externas.

3. Aos outros prestadores, públicos ou privados, de serviços online:

   - Devem reforçar os seus sistemas de alarmística e fazer uma monitorização acrescida de pedidos inusitados relacionados com acesso a contas de clientes ou utilizadores;
   - Devem adotar medidas adequadas e eficazes para prevenir e reduzir o impacto de eventuais ataques aos seus sistemas de informação;
   - Devem reequacionar, a breve trecho, o envio de SMS com um código, como segundo fator de autenticação, para validação da identidade do utilizador que está a aceder ao serviço (banca, chave móvel digital, recuperação de senhas, etc.), uma vez que aquilo que parecia ser uma alternativa viável ao risco inerente da Internet tornou-se, entretanto, bastante insegura com a crescente exposição pública de números de telefone associados à identidade dos seus titulares, como estes dois casos recentes tão bem atestam, e com as vulnerabilidades já conhecidas e documentadas neste domínio (*SIM swapping* protocolo SS7).

A CNPD continuará a acompanhar estes casos[2], em estreita cooperação com a autoridade de proteção de dados da Irlanda, e com as restantes autoridades de proteção de dados do Espaço Económico Europeu, dando nota pública de eventuais desenvolvimentos quando tal se justifique.

Lisboa, 9 de abril de 2021

[2] A CNPD já se manifestou como autoridade de controlo interessada, para efeitos do procedimento de cooperação previsto no artigo 60.º do RGPD.