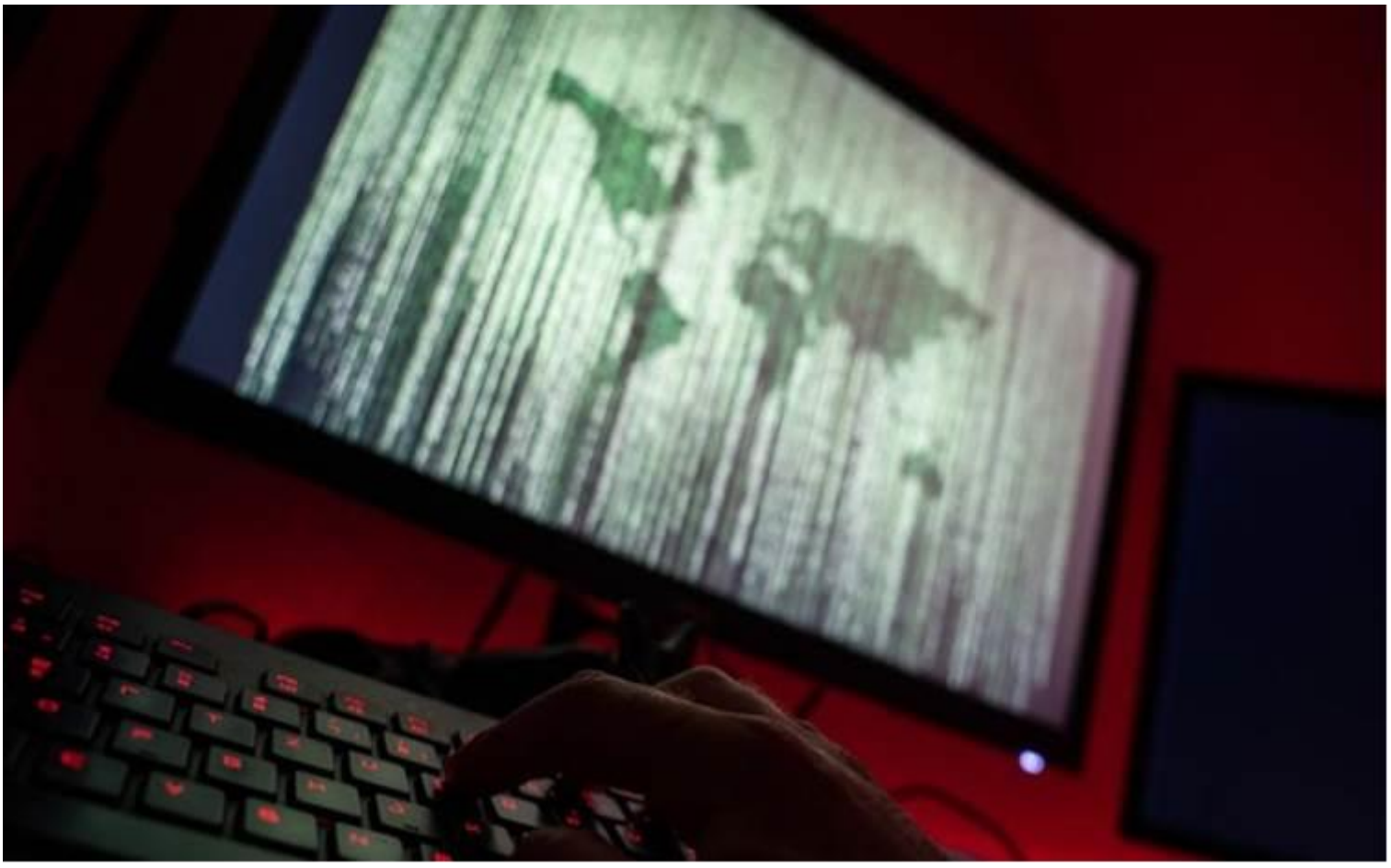
Na Mídia

08/02/2021 | Época Negócios

Piratas do século 21: mega vazamento serve de alerta para empresas sobre tratamento de dados

Tendência é que ciberataques se intensifiquem; qualquer empresa que lida com dados é um alvo em potencial

Ana Carolina Nunes



No mês passado, foi revelado que mais de 223 milhões de CPFs e outros dados foram capturados de um banco de dados – ainda não se sabe exatamente qual – e estão sendo vendidos na dark web, um ambiente na internet de difícil acesso, porém onde muitos crimes são cometidos. O arquivo contém ainda 40 milhões de CNPJs e 104 milhões de registros de veículos.

Especialistas não hesitam em classificar este como o maior vazamento de dados que se tem notícia no mundo. O número ultrapassa a população estimada do Brasil hoje, em torno de 210 milhões de pessoas, isso indica que pode haver dados sobrepostos e de pessoas já falecidas. O volume é preocupante.

"Foi um vazamento enorme. É até dificil de mensurar exatamente a dimensão que isso tem. Um vazamento farto, amplo, com uma base de dados bem estruturada", avalia Christian Perrone, coodenador da área de Direitos e Tecnologia do ITS-Rio (Instituto de Tecnologia e Sociedade).

Um dos principais riscos para quem teve os dados violados é o roubo de identidade. Christian destaca que a a população, de modo geral, não está acostumada ao quanto usamos e fornecemos nossos dados pessoais no dia a dia, e o quanto a nossa vida está indexada ao CPF, do hospital à padaria.

Do lado das empresas, no caso da violação de dados, podem haver sanções previstas na Lei Geral de Proteção de Dados (LGPD), que está em vigor no Brasil desde setembro de 2020. Por conta da pandemia, a aplicação de punições foi postergada e começa a valer em agosto deste ano, mas isso não significa que as empresas devem começar a seguir a lei apenas em julho. "Ainda há uma mentalidade focada nas sanções. **No Brasil não há uma cultura de prevenção, e a cultura da privacidade também está em construção", diz Eduardo Magrani, presidente Instituto Nacional de Proteção de Dados (INPD) e sócio do escritório Demarest Advogados. O advogado lembra que além das sanções, as empresas devem ter em mente que terão de lidar com o dano reputacional com clientes, funcionários e fornecedores.**

O roubo, o sequestro e a venda de dados pessoais está se tornando um crime cada vez mais comum e mais especializado. "É uma outra pandemia", diz Marco DeMello, CEO da empresa de cibersegurança Psafe, sobre o aumento dos ataques cibernéticos. Segundo Marco, as ciberameaças aumentaram no ano passado. Em 2020, o Defender Lab registrou um novo ataque a cada 16 segundos. No mercado ilegal, os dados valem muito: "na dark web, calcula-se a movimentação de US$ 1,8 trilhão em bitcoin, isso é mais que o PIB do Brasil. É a industrialização do cibercrime".

E a tendência é que os ataques – ou tentativas – continuem crescendo em número, dimensão e sofisticação. E engana-se quem considera que só as empresas financeiras são alvo dos hackers. "Todas as empresas que acumulam vasta quantidade de dados são alvos em potencial, primeiro pelo interesse no valor dos dados, segundo porque as empresas ou instituições viram reféns", diz Marco. As vítimas são variadas, mas se concentram prioritariamente em serviços essenciais. Na última semana, as elétricas Eletrobras e Copel confirmaram ter sofrido ataques a seus servidores. No fim de dezembro, a empresa italiana de biotecnologia IRBM, que participa do projeto da vacina anti-Covid desenvolvida pela Universidade de Oxford, também teve seu sistema invadido.

No final de 2020, o Superior Tribunal de Justiça (STJ) chegou a ficar com os trabalhos suspensos por conta de sequestro de dados. Em casos como esse, os hackers cobram para liberar os dados novamente, em um pagamento que deve ser feito em bitcoin.

Considerando o volume de dados e de ameaças, Marco reforça que as empresa têm de se proteger com ferramentas baseadas em inteligência artificial. Entretanto, muitas companhias estão usando "táticas antiquadas" para se defender dos ataques. "O que funcionava em 2019 não funciona em 2021".

Eduardo Magrani destaca a importância das empresas adotarem, conforme prevê a LGPD, o papel do Data Protection Officer (DPO) ou, como diz a lei brasileira, um encarregado da proteção dos dados. Magrani explica que ele teria um papel de ombudsman em relação aos dados, lidando os executivos c-level em uma empresa, as autoridades de proteção de dados e os titulares dos dados. O cargo é previsto para qualquer empresa que lide com dados pessoais, o que virtualmente se aplica a quase todas as empresas hoje, já que até os pequenos negócios reúnem dados dos clientes. "É preciso que ter em mente que a LGPD exige um trabalho continuado", aponta Eduardo Marco reforça que lidar com o tratamento e privacidade de dados é um trabalho constante e crítico. "A cultura empresarial deve incluir segurança na informação. Deve ser uma pauta perene de reunião de conselho", orienta.

Christian indica que a busca pela proteção dos dados pode ser uma oportunidade de inovação para empresas e startups neste momento. "É uma oportunidade para se organizar, gerir suas informações com mais eficiência e entender seus dados. Isso incentiva a buscar soluções, a criar novos mecanismos de proteção e repensar as formas de autenticação".