

Chegou a vez de o consumidor colocar as empresas contra a parede. Essa é a promessa da Lei Geral de Proteção de Dados (LGPD) , que entra em vigor a partir de 20 de agosto. Além dos clientes, que devem ter suas informações rigorosamente protegidas, a própria legislação esmaga as companhias, ao exigir uma série de responsabilidades para que os dados que elas detêm sejam cuidadosamente armazenados para não serem vazados ou roubados por hackers.

Se isso ocorrer, seja por ter sofrido ataque em seu sistema ou por erro no processo de arquivamento, a LGPD prevê multas que variam de 2% do faturamento da empresa a R\$ 50 milhões para cada falha constatada. Uma alta punição pecuniária, capaz de quebrar a maioria das empresas do país e que fará, segundo especialistas, com que a lei venha para ficar.

As companhias estão assustadas. Mas é lenta a movimentação para se adequar às novas regras, devido à complexidade, às mudanças de processos e cultura e aos custos. Conclusão: a quase 200 dias de a norma passar a valer, o arcabouço empresarial brasileiro não está preparado para atender às exigências previstas. E isso coloca em dúvida se a privacidade do cidadão será mesmo preservada a partir da LGPD.

A nova lei prevê que as empresas têm de proteger ou descartar os dados pessoais (nome, telefone, e-mail, RG, endereço e outros) de clientes e funcionários, por exemplo. E não só arquivos digitais. Os físicos também. Se houver vazamento, de qualquer tipo, será aplicada multa.

Dados sobre consumidores são considerados valiosos no ambiente corporativo para tomadas de decisões mais assertivas, visando alcançar o público-alvo do negócio de forma mais eficiente. Com essas informações em mãos bem trabalhadas e as estratégias definidas, vende-se mais, gastando menos energia e força de trabalho. Por isso, os dados são considerados o petróleo do futuro. E também por isso devem ser bem guardados, pois todo mundo está de olho neles: o cidadão, as empresas, os hackers e as companhias de cibersegurança que trabalham para protegê-los.

Segundo pesquisa da Serasa Experian, 85% das empresas brasileiras não estão preparadas para a LGPD. Foram ouvidos executivos de 508 companhias do País, de 18 setores e dos mais variados portes. Na opinião do diretor-geral da Kaspersky no Brasil, Roberto Rebouças, esse número pode ser ainda maior.

"É mais do que isso. Hoje, se você entrar em qualquer site, ele te pede um monte de informações. Estamos sendo procurados por empresas", afirma o executivo da maior companhia privada do Brasil no setor de segurança de dados. "Neste momento, ninguém está preparado. Tem muita coisa nebulosa, muita coisa que será definida em cima da hora e muita coisa que vai acontecer e será avaliada quando a lei estiver em vigência", diz.

Complexidade

Na avaliação do professor Maximiliano de Carvalho Jácomo, coordenador do curso de segurança digital do Instituto de Gestão e Tecnologia da Informação (IGTI), em Minas Gerais, além da proteção, as empresas precisam ter controles de como estão fazendo as coisas. "É complexo. Será alterada a cultura das firmas e dos cidadãos", observa.

Ele concorda com Roberto Rebouças sobre as empresas não estarem preparadas para atender à lei, apesar de ver a LGPD com olhar otimista, o que coloca em dúvida se a regra vai ser uma conquista ou dor de cabeça para a sociedade brasileira.

Embora Rebouças, da Kaspersky, precise vender seu peixe, o executivo garante que o brasileiro, em geral, defende muito mal seus dados. Pior: os expõem na internet voluntariamente. "Hoje, temos pouca privacidade. O brasileiro posta muita coisa dele mesmo. É campeão mundial de mídia social em praticamente todas elas. Em 10 ou 15 minutos de pesquisa sobre alguém, posso mandar e-mail com informações sobre ela, fazendo parecer que a conheço há 20 anos", garante o executivo

da Kaspersky, de origem russa e com escritório principal na Suíça. No Brasil, está instalada desde 2012.

"Não vemos nessa lei uma oportunidade de negócio. Temos trabalhado permanentemente com os clientes para deixá-los mais preparados e com conhecimento suficiente para entender qual é a problemática. Ninguém vai ter tempo nem dinheiro para fazer tudo, a tempo de a legislação começar a valer", diz Rebouças.

O executivo acredita que não há solução definitiva para evitar ataques cibernéticos que visam capturar dados. A solução mais eficaz para a proteção cibernética é transformar a eventual vítima num alvo de difícil acesso. "Não existe proteção 100% e nunca vai existir. Qualquer pessoa mal intencionada, se decidir invadir algum local, consegue. Depende de quanto ela está disposta a investir nesse ataque".

Multas podem incentivar "cibersequestro"

A LGPD avançou depois de ataques e vazamentos se intensificarem no Brasil. O país, que já ostentava as primeiras posições mundiais em phishing e outros ataques, viu alguns casos se tornarem famosos por sua grande escala, como divulgação ilegal de dados de clientes bancários e de consumidores de e-commerces - em âmbito mundial, o [caso do Facebook](#) é um dos mais famosos e no Brasil destaca-se o da Netshoes .

A legislação tem origem na Medida Provisória 869 de 2018, editada pelo então presidente Michel Temer. O atual comandante do Palácio do Planalto, Jair Bolsonaro, sancionou a lei 13.853 de 2019, que flexibilizou a Lei Geral de Proteção de Dados (13.709 de 2018) e criou a Autoridade Nacional de Proteção de Dados (ANPD), responsável pela futura fiscalização.

Com muitas incógnitas e altas multas, a LGPD pode levar a um caminho perigoso, fazendo surgir outros tipos de crime. "É possível que um invasor entre no sistema de uma empresa, pegue os dados e entre em contato com a própria empresa para pedir resgate, como num sequestro cibernético. Numa situação hipotética, com os dados vazados a empresa pagaria multa de R\$ 100 mil, por exemplo. O invasor pede R\$ 50 mil para não vazar", diz Roberto Rebouças, da Kaspersky.

Thiago Bordini, diretor de inteligência cibernética e pesquisa do Grupo New Space, que tem em uma de suas vertentes a prevenção a fraudes pela internet, aponta outros problemas. "Ainda existem muitas dúvidas sobre a nova lei. Principalmente, de como serão as investigações de vazamentos", destaca.

"Não se sabe como isso será feito. E são muitas variáveis. Imagine que uma pessoa tenha a mesma senha e e-mail para duas lojas virtuais diferentes e seus dados foram vazados. Pode haver confusão sobre onde, de fato, é a origem do vazamento e uma empresa pagar pela outra", avalia Bordini, ao sugerir tempo para "maturação" da lei, com orientações iniciais antes da aplicação das sanções.

Os especialistas apontam, ainda, uma distinção importante entre a lei brasileira e a europeia: o escalonamento. Enquanto na Europa a legislação prevê exigências diferentes para empresas de grande, médio e pequeno portes, por aqui todas as empresas são tratadas da mesma forma. Uma gigante automobilística terá as mesmas obrigações da pequena venda de verduras da esquina. A LGPD trata os diferentes como iguais. A seis meses do início de sua vigência, há mais dúvidas do que certezas. Afinal: a privacidade estará garantida ou mais perto de ser violada?

Fonte: [IG Tecnologia](#), em 26.01.2020