# Lex

PROTEÇÃO DE DADOS

# Advogados receiam tornar-se vítimas frequentes de ciberataques

**Há medidas e meios para minimizar a ocorrência de ciberataques, mas para os especialistas inquiridos pelo Negócios, "não é possível a nenhuma organização garantir a segurança a 100%".**

JOÃO MALTEZ
jmaltez@negocios.pt

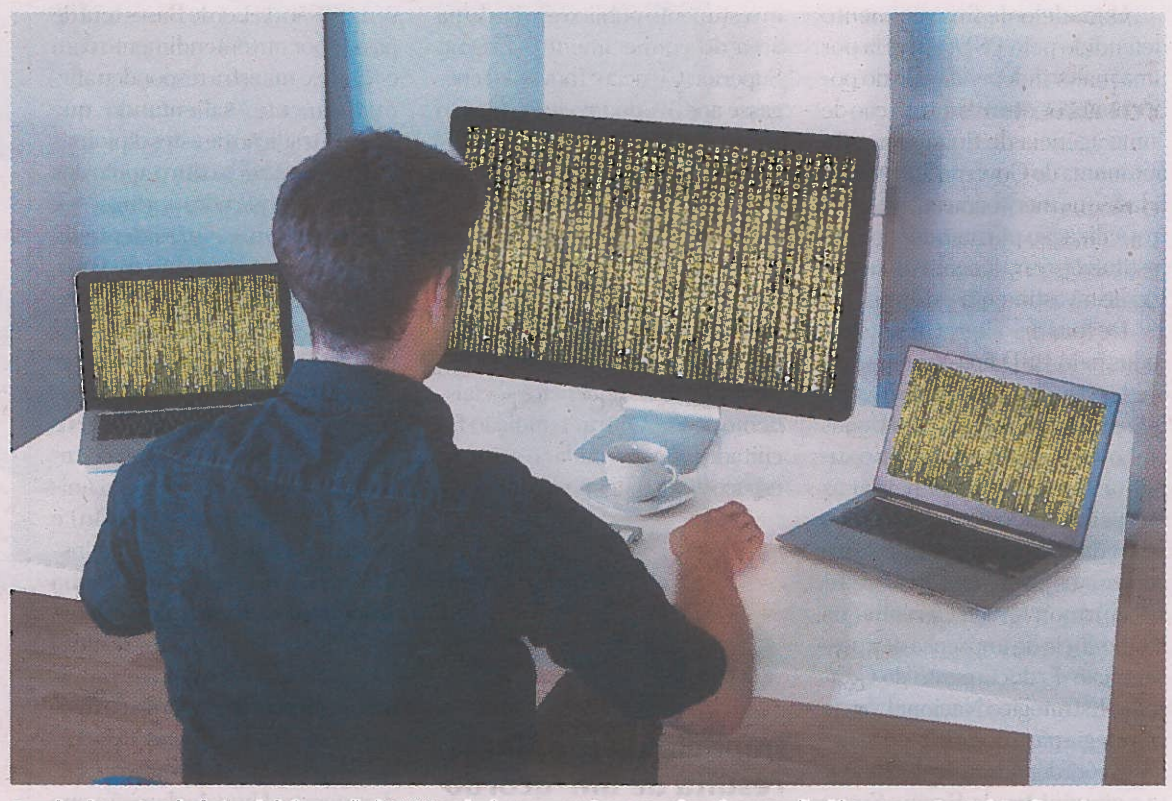
Os ciberataques a sociedades de advogados, à semelhança do caso que foi revelado esta semana e que envolveu a sociedade PLMJ, poderão repetir-se, com frequência, num futuro próximo, admitem especialistas contactados pelo Negócios. Tanto mais que nenhuma organização está a salvo e será até negligente afirmar que se está imune a este tipo de ataques, sustentam, por outro lado, vários atores do mercado da advocacia.

O caso veio a público esta semana, mas segundo a Polícia Judiciária, está em investigação "há já algum tempo". Um ciberataque à PLMJ redundou no alegado roubo de quatro gigabytes de informação sobre alguns dos principais clientes do escritório. Estará aqui em causa pelo menos um crime de acesso ilegítimo, mas também a necessidade de colocar, no mínimo, uma pergunta: Em Portugal, as sociedades de advogados estão preparadas para resistir à investida dos hackers?

António Caeiro, encarregado de proteção de dados e responsável de comunicações da Abreu Advogados, defende que, "na generalidade, as sociedades têm vindo a adotar tecnologia e a implementar procedimentos para ajudar a prevenir, detetar e reagir aos ataques informáticos".

No entanto, para este membro da direção da IT4Legal - Associação para as Tecnologias e Sistemas de Informação do Direito, "mesmo com toda a tecnologia, processos e equipas disponíveis e focadas na proteção dos sistemas e da informação, não é possível a nenhuma organização garantir a segurança a 100%".

Para Martim Bouza Serrano, advogado associado e coordenador da equipa de proteção de dados da CCA Ontier, "mesmo os sistemas informáticos tradicionalmente mais robustos, como aqueles associados à industria financeira ou até o próprio Estado são alvo de constantes ataques". Até por isso, sublinha ainda, "será um erro pensar que existem sistemas sem vulnerabilidades e negligente afirmar que se está imune a estes ataques".



O roubo de quatro gigabytes de informação à PLMJ poderá corresponder a um crime de acesso ilegítimo, segundo a Lei do Cibercrime.

**"A norma é dizer que vai acontecer [um ciberataque], só não sabemos quando", afirma Elsa Veloso.**

## Perdas reputacionais

O que fazer então para reduzir ao máximo eventuais fragilidades, que redundem no compromisso da informação privilegiada? "Não sendo possível eliminar o risco, as sociedades de advogados têm de estar bastante atentas às perdas financeiras e reputacionais que podem derivar de um ciberataque", defende Luís Neto Galvão, sócio da SRS e especialista em privacidade e proteção de dados.

Sofia Riço Calado, da mesma firma de advogados e também especialista em proteção de dados, lembra que o início da aplicação do Regulamento Geral Sobre a Proteção de Dados, em maio passado, veio reforçar a consciencialização quanto à importância da existência de uma politica adequada, fazendo assentar a "tónica na formação das pessoas em matéria de segurança da informação".

Fala-se aqui, também, tal como refere Martim Bouza Serrano, de adotar procedimentos internos "que limitem o acesso à informação", bem como de apostar "no melhoramento da segurança das redes informáticas" de que as sociedades de advogados dispõem.

Quando se fala de uma sociedade de advogados e do que procuram os hackers, é preciso levar em linha de conta, sublinha Luís Galvão Neto, que estão em causa dados relativos

# Cinco anos de prisão para acesso ilegítimo

OPINIÃO

**ELSA VELOSO**
Advogada, fundadora e CEO da DPO Consulting

## Página online foi encerrada

**O blogue "Mercado de Benfica" (mercadodebenfica.blogsky.com) onde foram divulgados os ficheiros alegadamente roubados à PLMJ, foi ontem encerrado, passando a ler-se na local onde estava alojado a seguinte mensagem: "esta página foi encerrada por violar os nossos termos e condições". A PLMJ, de onde terão desaparecido ficheiros relacionados com os casos E-Toupeira, Secretas, EDP e Operação Marquês, admitiu em comunicado que a segurança da sua rede "foi recentemente comprometida", estando a "avaliar o impacto potencial desse acesso ilegítimo a informação".**

**"É expectável que ataques idênticos [ao do caso PLMJ] se repitam com frequência.**
**LUÍS NETO GALVÃO**
Sócio da SRS

**Será um erro pensar que existem sistemas sem vulnerabilidades.**
**MARTIM BOUZA SERRANO**
Advogado coordenador da CCA-Ontier

**Qualquer ataque com repercussões fortes na operação de uma sociedade de advogados será decorrente de uma atividade criminosa.**
**ANTÓNIO CAEIRO**
Responsável de comunicações da Abreu Advogados

a "segredos comerciais, a direitos de propriedade intelectual ou informação sobre potenciais transações comerciais ou matérias em segredo de justiça". Até por isso, adianta: "infelizmente, num futuro próximo, é expectável que ataques idênticos [ao do caso PLMJ] se repitam com frequência."

A advogada Elsa Veloso, fundadora da DPO Consulting, frisa que "mesmo com todas as precauções ao nível da segurança da informação, ninguém está a salvo de um ataque informático". Aliás, "a norma é dizer que vai acontecer, só não sabemos quando", sentencia esta especialista em proteção de dados. ■

O ataque informático de que terá sido alvo a sociedade PLMJ é suscetível de configurar os crimes de acesso ilegítimo a um sistema informático e de disseminação por meios eletrónicos da informação obtida, que se encontram previstos na lei do cibercrime, explicou ao Negócios Manuel Durães Rocha, sócio da Abreu Advogados responsável pelas áreas de prática de Propriedade Intelectual e de Tecnologias da Informação.

A moldura penal para estes crimes, segundo o mesmo advogado foi estabelecida entre um a cinco anos. "A aplicação da pena mais grave ocorre quando o crime visar a obtenção e disseminação ilícita de segredos comerciais da vítima ou de informações confidenciais protegidas por lei", explica a mesmo advogado.

A lei atual, além da pena de prisão, também prevê a aplicação de penas acessórias, "nomeadamente a perda dos equipamentos que serviram para a prática do crime", adianta Manuel Durães Rocha.

Por outro lado, e de acordo com a advogada da SRS Sofia Riço Calado, especialista em proteção de dados, quando ocorra o acesso não autorizado a dados pessoais, haverá também "um crime de acesso indevido que, por ocorrer através de violação de regras técnicas de segurança, poderá dar lugar a uma pena entre prisão até dois anos ou multa até 240 dias". Isto, tendo em conta o que prevê a Lei de Proteção de Dados Pessoais, que ainda está em vigor. ■

# O futuro na segurança da informação das empresas

A União Europeia está a regular de forma cada vez mais ativa a transferência de dados na qual assenta a Indústria 4.0. A circulação de dados – de informação pessoal ou de negócio – vem colocar um conjunto de desafios cujo entendimento antecipado do alcance, dimensão e oportunidade constituirá um fator de oportunidade, podendo originar uma reorganização da cadeia de valor da indústria, nomeadamente ao nível dos 'players'.

No panorama regulatório atual, temos em vigor no espaço europeu o Regulamento Geral de Proteção sobre Dados que impõe medidas que obrigam a definir, documentar e implementar processos, a implementar estruturas de 'governance', bem como formar e sensibilizar os colaboradores da necessidade de alteração de comportamentos de risco face às ameaças da segurança da informação e às ainda mais críticas ameaças cibernéticas provenientes da interligação global, do fim das fronteiras e perímetros físicos das organizações e da reduzida maturidade das organizações face a estes riscos.

O alerta para a necessidade de incluir o risco de ataques cibernéticos e violações de dados (pessoais, de negócio ou de propriedade intelectual) na análise de risco corporativa [...] torna-se ainda mais premente como consequência do constante aumento do número de ataques com efeitos financeiros significativos e prejudiciais – destacam-se os mais recentes casos da Maersk, Saint-Gobain, FedEx, Reckitt Benckiser, Beiersdorf, entre tantos outros.

Está também atualmente em vigor uma diretiva relativa à proteção de infraestruturas críticas de cada país, diretiva esta já traduzida em lei dentro de cada país – em Portugal, a Lei 46/2018 de 13 de agosto. Esta Lei vem obrigar à adoção de um conjunto de medidas que garantam a resiliência e uma mitigação do risco de ataques em conjunto com a capacidade de responder adequadamente e repor os níveis de serviço num espaço de tempo definido e aceitável.

Este desafio externo vem colocar o repto às empresas de assumirem a decisão estratégica de serem inovadoras, proativas e apresentarem aos seus clientes as suas credenciais ou serem reativas perante os requisitos da regulação Europeia e Internacional.

Sintetizando, as empresas de maior dimensão, com outro grau de maturidade nas suas políticas e processos internos, mais poderosas financeiramente, estão progressivamente a incrementar o grau de exigência no processo de seleção dos seus parceiros e fornecedores.

Hoje, a decisão dos líderes já não é sobre "se", mas antes "como" e "quando..., porque o "hoje" já não é cedo. ■