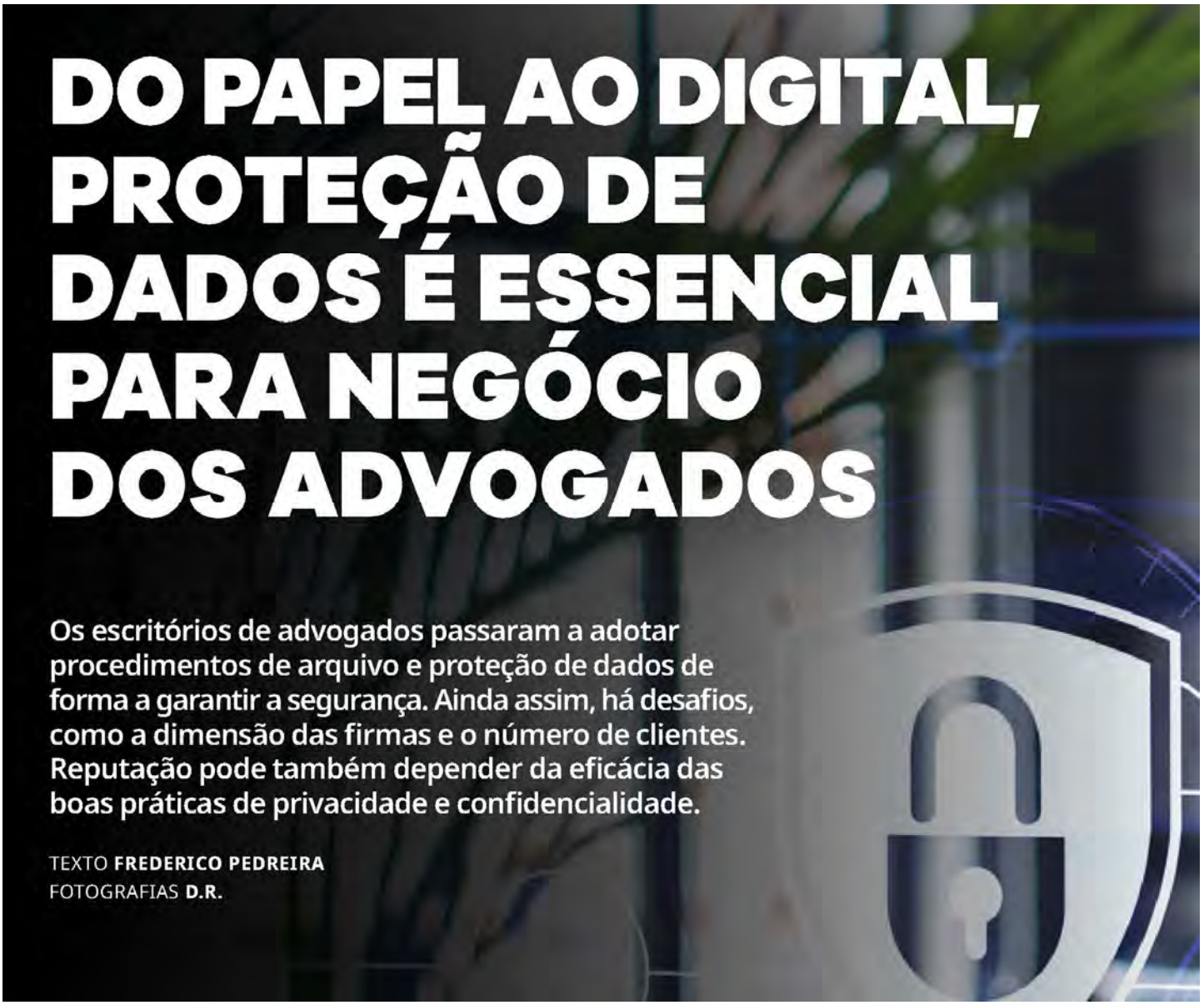
DO PAPEL AO DIGITAL, PROTEÇÃO DE DADOS É ESSENCIAL PARA NEGÓCIO DOS ADVOGADOS

Os escritórios de advogados passaram a adotar procedimentos de arquivo e proteção de dados de forma a garantir a segurança. Ainda assim, há desafios, como a dimensão das firmas e o número de clientes. Reputação pode também depender da eficácia das boas práticas de privacidade e confidencialidade.

TEXTO **FREDERICO PEDREIRA**
FOTOGRAFIAS **D.R.**



A proteção dos dados físicos e digitais nas empresas é essencial para a prossecução do negócio quer para a segurança dos clientes e da própria empresa.

No setor da advocacia, as firmas passaram a adotar procedimentos de arquivo e proteção de dados, físicos e digitais, através de diversas ferramentas. Assim, começaram também a delinear planos de risco. O objetivo? Garantir a segurança e reputação.

Por exemplo, a Abreu Advogados tem diversas medidas técnicas e organizativas que asseguram a segurança dos dados pessoais e outras informações, como a política de gestão de acessos e o sistema de gestão documental que permite a centralização, proteção e classificação da informação, com todas as medidas de segurança associadas.

"Relativamente ao arquivo físico, a Abreu tem contratado um serviço com um parceiro de referência que garante toda a confidencialidade no âmbito do manuseamento e tratamento da documentação", asseguraram o sócio Ricardo Henriques e o *head of IT* Paulo Nunes.

Já na PRA - Raposo, Sá Miranda & Associados o investimento em *softwares*, independentemente da sua finalidade, é feito a pensar na necessidade de manter todos os documentos em segurança e no cumprimento do princípio da proteção de dados desde a conceção e por defeito. "A *due diligence* nestas contratações tem muita relevância e é levada muito a sério, internamente", explicou o sócio Gonçalo Gil Barreiros.

No que concerne a documentos físicos, a firma liderada por Miguel Miranda contratou uma empresa certificada para destruição de papel.

Outra das firmas do mercado de advocacia portuguesa, a CCA Law Firm, também tem vindo a adotar um conjunto de medidas técnicas e organizativas que garantem a segurança dos dados e informação que trata. "Utilizamos sistemas físicos e lógicos com capacidade para assegurar a confidencialidade, a integridade e a resiliência da informação tratada, prevenindo violações ou incidentes de segurança e que incorporam processos para avaliar regularmente a respetiva eficácia", referiu a associada sénior Rita Serrano.

À *Advocatus*, a advogada explicou ainda que no escritório promovem formações específicas de sensibilização para a segurança cibernética. "Estamos cientes de que o erro humano é o mais frequente causador de violações de segurança. Por exemplo, os emails de *phishing* são uma técnica muito popular para atacar uma organização, pelo que mantemos, o mais possível, os nossos colaboradores informados e cooperantes", acrescentou.

Na Antas da Cunha Ecija também tem vindo a ser desenvolvido um plano de risco detalhado, com medidas de mitigação específicas no âmbito da efetiva concretização de cibersegurança. Formação dos colaboradores, auditorias de cibersegurança, designação de um Encarregado de Proteção de Dados, desenvolvimento de documentação pré-contratual, ações de auditoria de cumprimento do Regulamento Geral sobre a Proteção de Dados (RGPD) e cibersegurança são algumas dessas medidas.

"Do ponto de vista mais técnico, a sociedade tem presente os requisitos da ISO 27001 e caminha para a certificação através de parceiros tecnológicos e de uma jurista que obteve a certificação ISO 27001 Lead Implementer. Em especial, a sociedade está a seguir as diretrizes para a gestão de segurança da informação e a criar o espólio documental necessário para obter a certificação da norma internacional", explicou Ana Catarina Silva, *of counsel* da Antas da Cunha Ecija.

DA DIMENSÃO ÀS BOAS PRÁTICAS, DESAFIOS AUMENTAM

A dimensão do escritório e o número de clientes é um desafio na proteção de dados, pelo menos para os quatro escritórios contactados pela *Advocatus*. "Obviamente que o volume de dados contribui para a necessidade de implementar medidas de maior complexidade", sublinharam Ricardo Henriques e Paulo Nunes.

Os profissionais da Abreu consideram que a possibilidade de os trabalhadores da firma poderem trabalhar remotamente e terem presença em locais geograficamente distintos constituem "desafios acrescidos" e que "exigem a aplicação de medidas adicionais". "Como forma de lidar com estes desafios, assinalamos a existência do Security Operations Center (SOC) da Abreu, o qual tem contribuído para uma constante monitorização da segurança de todos os dados pessoais e informação tratada", acrescentaram.

Por outro lado, Ana Catarina Silva sublinhou que, acima de tudo, o desafio na proteção de dados é "transversal" a uma organização, quer pelo número de clientes quer pela sua dimensão. Ainda assim, considera que o maior desafio é a mudança de hábitos ou de procedimentos internos e a proliferação de uma cultura de proteção de dados e segurança da informação.

"Numa sociedade com maior dimensão a alteração nos procedimentos internos de segurança e de proteção de dados pessoais pode tornar-se mais difícil de concretizar, exatamente pela dimensão e volume de informação existente", disse.

A *of counsel* relembrou que a firma inclui-se grupo Ecija e Taylor Wessing que integra profissionais localizados em diversos países, pelo que é "especificamente exigente" neste tema relativamente a todos os associados. Assim, implementaram "rigorosas" regras no que diz respeito à proteção de dados e às respetivas transferências internacionais internas e de clientes.

"O cumprimento das obrigações que advêm do RGPD, e não o cumprimento com o direito à proteção de dados pessoais que remonta a 1998, é um desafio no que toca à consciencialização dos colaboradores e dos órgãos de administração para a mudança dos procedimentos internos e, como será expectável, para o investimento financeiro na contratação de recursos tecnológicos, sistemas de informação seguros e de softwares que ajudem a cumprir com as medidas de segurança adequadas", referiu.

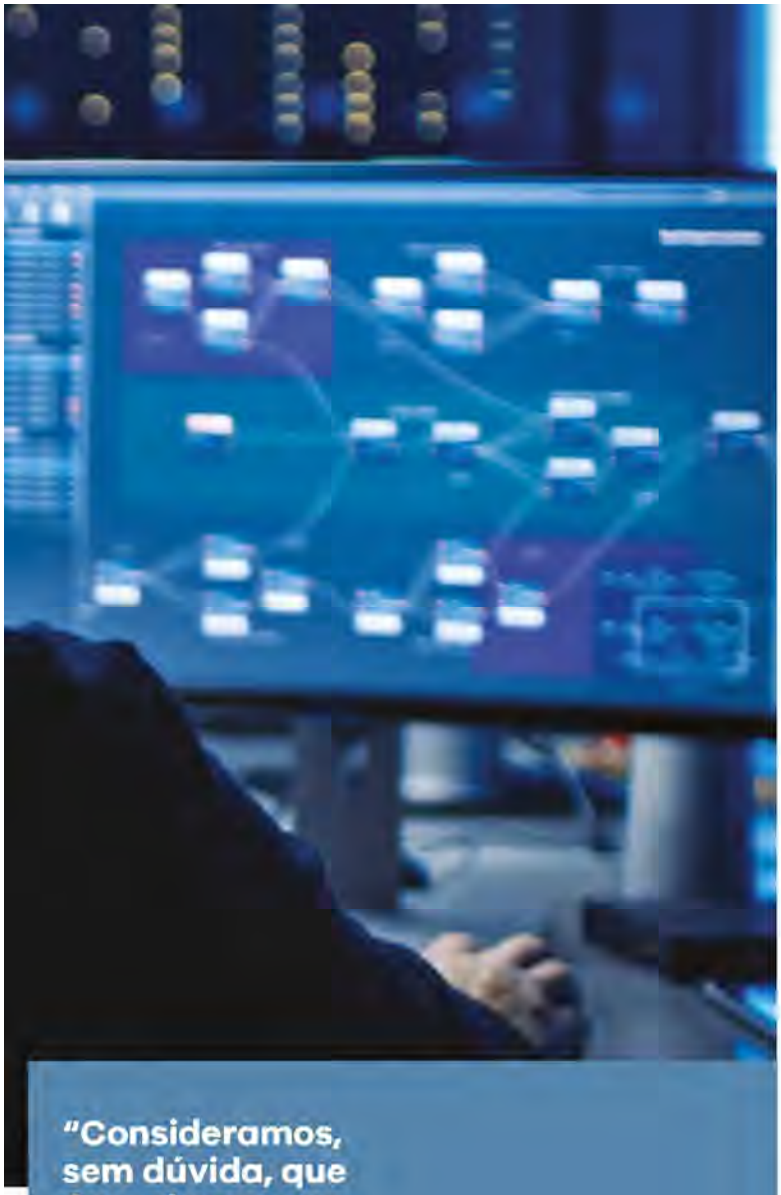
"A complexidade crescente dos Sistemas de Informação e a dispersão da informação pelas novas tecnologias de colaboração é outro dos desafios que deve ser considerado"

Ricardo Henriques e Paulo Nunes
Sócio e *head of IT* da Abreu Advogados

Gonçalo Gil Barreiros defendeu ainda que os maiores desafios prendem-se com a minimização dos dados pessoais e com a conservação dos mesmos. O sócio e coordenador de Propriedade Intelectual e Privacidade da PRA explicou que existe um maior cuidado com os dados pessoais que hoje são recolhidos, tendo que se responder a questões primordiais como: Porque temos os dados? Quem pode aceder aos dados? Quanto tempo temos os dados? Ou como mantemos a segurança dos dados?

"Importa, pois, responder, de forma correta, a tais questões e encetar as melhores ações no manuseamento destes dados pessoais por forma a cumprir com o RGPD e com a demais legislação aplicável a estas matérias", disse.

Para Rita Serrano o maior desafio é o de "uniformizar as boas práticas internas" e garantir que essas práticas e respetivas medidas de segurança são "respeitadas igualmente por todos dentro da organização".



"Consideramos, sem dúvida, que é um dos pontos relevantes para a boa imagem e reputação de uma sociedade de advogados e de como isso é um fator decisivo na escolha por parte dos clientes, que valorizam a capacidade de o escritório guardar a sua informação"

Gonçalo Gil Barreiros
Sócio da PRA

Já Ricardo Henriques e Pedro Nunes apontaram a evolução tecnológica com o novo paradigma da Inteligência Artificial como o principal desafio, uma vez que obriga a um aumento da complexidade dos sistemas de proteção de dados e serviços de segurança e à necessidade de investimento em tecnologias de proteção mais recentes.

"A complexidade crescente dos Sistemas de Informação e a dispersão da informação pelas novas tecnologias de colaboração é outro dos desafios que deve ser considerado, gerando uma necessidade de uma maior monitorização, controlo e gestão dos fluxos de informação, quer da organização, quer dos seus parceiros tecnológicos", acrescentaram.

Por outro lado, Ana Catarina Silva considera que os maiores desafios para os clientes e profissionais é utilização adequada dos dados que não comprometa a segurança dos mesmos, o risco de ciberataques, a adoção de tecnologias seguras e de confiança para o armazenamento da informação e a implementação de práticas de boa governança e consciencialização dos colaboradores.

BOAS PRÁTICAS MELHORAM REPUTAÇÃO

A reputação pode ser uma ferramenta essencial para impulsionar os negócios, mas também os pode arruinar, caso seja negativa. Assim, os escritórios de advogados consideram que a sua reputação pode também depender da eficácia das boas práticas de privacidade e confidencialidade.

"Consideramos, sem dúvida, que é um dos pontos relevantes para a boa imagem e reputação de uma sociedade de advogados e de como isso é um fator decisivo na escolha por parte dos clientes, que valorizam a capacidade de o escritório guardar a sua informação", sublinhou Gonçalo Gil Barreiros.

Também Ana Catarina Silva partilha desta posição, acrescentando que as firmas de advogados são "fontes" e "locais" de armazenamento de informação confidencial e privada de clientes, pelo que "indubitavelmente a reputação dos mesmos depende da eficácia das medidas de proteção de dados pessoais e confidencialidade".

"Para além de ser algo que está associado às exigências da atividade, os escritórios de advogados não conseguem ser confiáveis para os seus clientes e competitivos face aos seus concorrentes se não implementarem medidas efetivamente robustas de segurança da informação, encriptação, *firewalls*, sistemas de deteção de intrusões e a consciencialização dos utilizadores das práticas seguras", referiu a *of counsel* da Antas da Cunha Ecija.

Por outro lado, Rita Serrano assegurou que é "óbvio" que a eficácia de boas práticas contribui "inevitavelmente" para a reputação de qualquer organização. "O dever de sigilo profissional corresponde a uma concretização da tutela da confiança, sem a qual não haverá base para estabelecer qualquer relação com clientes. O fundamento ético do sigilo profissional radica, pois, no princípio da confiança, princípio que está também na génese do conceito de privacidade", disse. ■