

ADVISORY AVOGADOS, CONSULTORES E BANCOS DE INVESTIMENTO

ENTREVISTA

Lei dispersa é o *malware* da busca criminal

Ataques informáticos e escutas são realidades na investigação criminal. Mais cedo ou mais tarde, o quadro legal português terá de se adaptar.

MARIANA BANDEIRA
mbandeira@jornaleconomico.pt

A cibersegurança tem preocupado as empresas e não deixou de parte os operadores do sistema jurídico. A aposta na tecnologia faz com que provas oriundas de câmaras de videovigilância possam ludibriar as garantias de proteção dos arguidos se não forem autorizadas. Rui Soares Pereira e David Silva Ramalho defendem uma adaptação da lei à era digital.

Quais os principais desafios da investigação criminal portuguesa na era digital?

Os desafios que a investigação criminal enfrenta em Portugal são essencialmente de três ordens: técnica, jurídica e prática. A técnica é, em geral, comum aos demais ordenamentos jurídicos. Além dos crimes que se passam em zonas escondidas da Internet, muitas vezes debaixo do radar das autoridades, verifica-se ser muitas vezes quase impossível descobrir os autores dos crimes. A investigação criminal precisa de um quadro normativo claro e coeso, apto a fazer face à evolução das tecnologias e construir um quadro de aplicação legislativa que não se preste a dúvidas perante os operadores judiciais. Em Portugal temos legislação dispersa, com âmbitos de aplicação sobreponíveis e pouco adaptada à realidade digital.

Em Portugal é legalmente admissível o recurso a técnicas de *hacking* ou a *malware* pela polícia?

Entendemos que não. Apesar de ser possível, para alguns, encontrar um vislumbre de previsão legal para o efeito, a verdade é que os termos em que esse meio de obtenção de prova se encontra previsto afrontam os princípios da legalidade e da proporcionalidade. A



RUI SOARES PEREIRA
consultor PLMJ

"A ideia de que *quem não deve não teme* é perigoso na privacidade"



DAVID SILVA RAMALHO
investigador CIPDC

"O recurso a escutas deve ser feito apenas em condições de absoluta necessidade"

possibilidade de as autoridades ordenarem a infiltração informática em sistemas para monitorizarem a atividade do utilizador e ativarem remotamente e de forma sub-reptícia os microfones e *webcams*, deve considerar-se proibida no nosso ordenamento jurídico. O que não significa que não devesse ser admitida, como sucedeu recentemente em Espanha.

Até que ponto a maior videovigilância pode violar os direitos e garantias pessoais?

Existe a ideia de que mais videovigilância equivale a mais segurança e que mais segurança é sempre algo de positivo. Não está demonstrado que a videovigilância apresente um efeito determinante na redução significativa da prática de crimes. É importante reter que a procura de segurança à custa da privacidade de todos cidadãos pode ser um sacrifício desproporcional de interesses. É a ideia de que "quem não deve não teme" é um caminho perigoso da privacidade.

Que opinião têm sobre a colocação de GPS em viaturas de suspeitos e arguidos?

O recurso a meios de obtenção de prova ocultados do visado (escutas, ações encobertas, interceções de comunicação...) deve ser feito apenas em condições de absoluta necessidade e mediante apertado controlo judicial. A colocação de GPS na viatura de um suspeito ou arguido, independentemente da sua utilidade, deve ser considerada um meio oculto de obtenção de prova que não está previsto na lei. A doutrina e os tribunais têm avançado soluções diferentes, mas algumas representam um claro desvio relativamente à tradicional forma de encarar a reserva de lei. Então, surge a pertinente questão de saber se é necessária uma intervenção legislativa nesta matéria.

CONFERÊNCIA "A PROVA DIGITAL EM PROCESSO PENAL"

Os advogados consideram que existe um certo desconhecimento, por parte das autoridades e dos colegas de profissão, do quadro legal aplicável à prova digital, o que resulta em decisões diferentes para casos semelhantes. No próximo dia 24 de maio, o Centro de Investigação de Direito Penal e Ciências Criminais da Faculdade de Direito da Universidade de Lisboa organiza o evento "A Prova Digital em Processo Penal" para debater o assunto e dar um novo impulso à discussão da tecnologia no panorama jurídico atual.



OPINIÃO

Os media e o regulamento de dados pessoais



JORGE SILVA MARTINS
Advogado, DLA Piper ABCC

A pouco mais de um ano do início de aplicação do novo Regulamento, a névoa parece finalmente começar a assentar e as dúvidas dão já lugar a algumas certezas. Uma delas surge antes de todas as outras: o GDPR não é apenas um conjunto de (muitos) considerandos e de (muitos) artigos. Corporiza, pelo contrário, uma revolução sem precedentes a

nível europeu nos domínios da privacidade e da proteção de dados pessoais, trazendo agarrado a si uma nova cultura "datocêntrica" (chamemo-lhe assim), nos termos da qual os dados pessoais e o seu titular ocupam o centro da moderna cosmologia digital.

As empresas de media não escapam a esta revolução. Encontram nesta fase, porém, uma dificuldade que lhes é específica e uma outra que é comum a muitos setores.

A primeira diz respeito à enorme margem de abertura que o legislador comunitário deixou ao legislador nacional para afastar a aplicação do Regulamento quando pretenda dirimir, por via de lei, o conflito intra-sistemático entre o direito à proteção de dados pessoais e o direito à liberdade de expressão e de in-



SÉRVULO PROMOVE SEMINÁRIO PARA ASSINALAR ARRANQUE DE NOVO SERVIÇO NA ÁREA DA RESPONSABILIDADE NA SAÚDE

A Sérvulo & Associados organiza no dia 25 de maio, a partir das 15:45, um seminário dedicado ao tema "Responsabilidade na Saúde". O evento constitui uma "iniciativa multidisciplinar que assinala o lançamento do serviço integrado de apoio jurídico à responsabilidade na saúde", refere a Sérvulo em comunicado. Este serviço está especialmente vocacionado para os intervenientes no setor da Saúde, incluindo utentes, profissionais da saúde, estabelecimentos prestadores de cuidados de saúde públicos e privados, indústria farmacêutica e entidades seguradoras, contando com as participações das equipas da Sérvulo nas áreas de Responsabilidade Civil, Direito dos Seguros, Direito Penal, Direito do Trabalho, Direito Público, Proteção de Dados e Tecnologias da Informação, Direito Europeu e da Concorrência, referiu ainda o escritório liderado por Paulo Câmara. As inscrições decorrem até 22 de maio e estão limitadas ao espaço existente.

formação. Sendo uma concretização do princípio da subsidiariedade, o certo é que, na prática, esta especificidade deixa um rasto de incerteza em redor de 7 dos 11 capítulos do Regulamento (de 73 dos seus 99 artigos), conduzindo ao paradoxo de as empresas saberem que têm de se adaptar mas não saberem ainda exatamente a quê.

A segunda dificuldade é sentida pelas empresas de media mas partilhada com empresas de diferentes setores: por onde devem iniciar a travessia do GDPR? Por onde se começa? O tema é complexo. Deixarmos, no entanto, quatro pistas para *kick-off*: primeiro, é necessário mapear o universo de dados pessoais tratados e, nesse âmbito, encontrar resposta para um conjunto nuclear de questões, entre elas a de saber para que finalidades são tratados esses dados (processamento de salários, concursos televisivos ou de rádio, assinaturas de publicações, etc.), se os mesmos ainda são necessários e se foram adotadas medidas que asseguram a sua integridade; em segundo lugar é preciso conhecer o fundamento

que legitima esse tratamento, designadamente, se foi consentido pelo titular dos dados, qual a extensão desse consentimento e em que medida as regras até agora seguidas cumprem com as disposições do GDPR (o que será relevante, por exemplo, para efeitos de realização de campanhas de marketing direto); depois, é fundamental assegurar uma adaptação dos procedimentos internos (e dos instrumentos que os corporizam, como as políticas de privacidade, os formulários de consentimento, etc.) à nova metódica de *accountability* do Regulamento, sem esquecer a importância da criação de mecanismos de resposta em caso de violação de dados pessoais; finalmente, é ainda necessário garantir que o processo de adaptação das empresas ao GDPR não toca apenas nos seus procedimentos mas, e essencialmente, na sua cultura: o tema da privacidade e da proteção de dados pessoais passa agora a estar "dentro" do negócio e já não apenas nas suas franjas.

Não há tempo a perder. Maio de 2018 está já no horizonte. ●