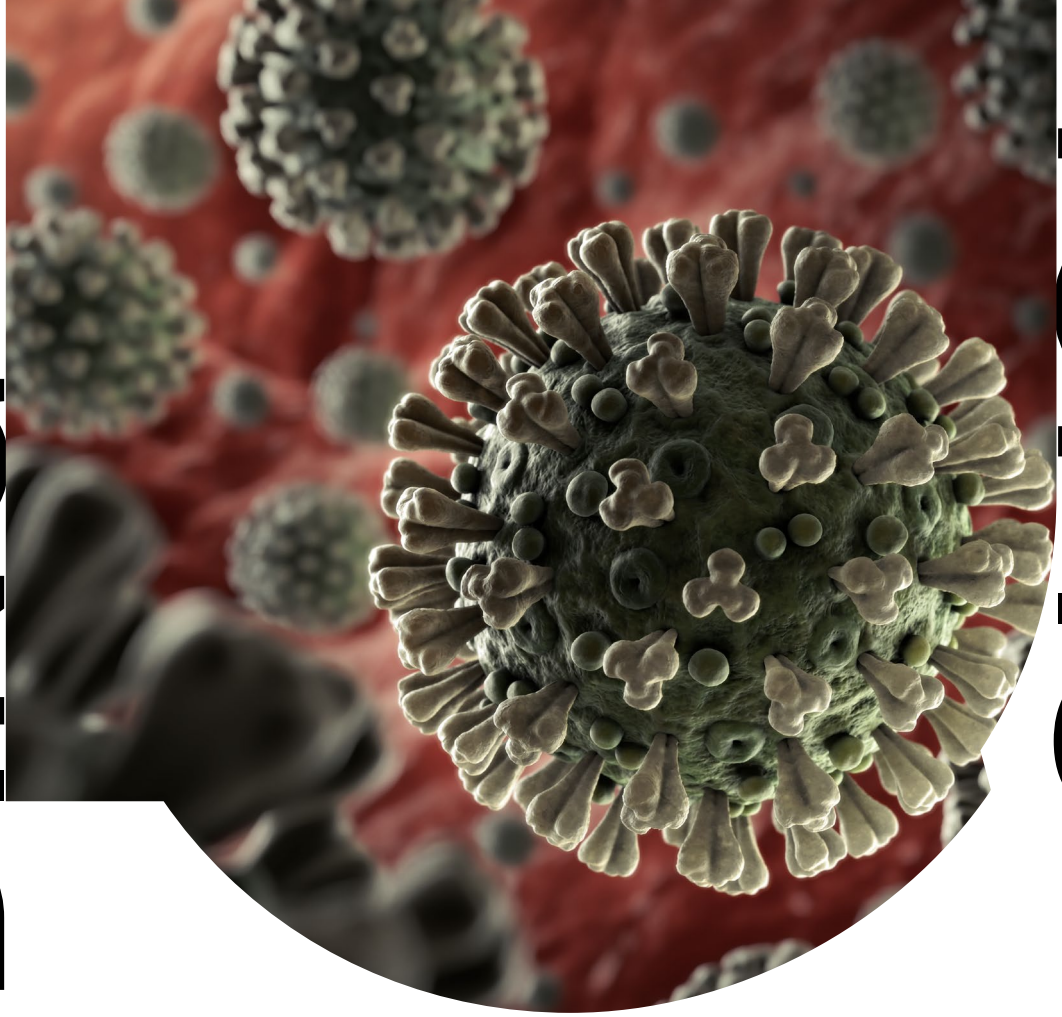
TRENDING TOPIC



13 ABR. 20

TECNOLOGIA, MOBILIDADE E COMUNICAÇÕES

Coronavírus: Privacidade e segurança no teletrabalho, *e-learning* e lazer

Os números recentemente publicados pela ANACOM são inequívocos: em consequência da propagação do COVID-19, as medidas de proteção individual e comunitária conduziram a um aumento de 50% do tráfego de comunicações eletrónicas, em Portugal.

PLMJ

Pedro Lomba
Jorge Silva Martins
Carolina Sousa Guerreiro
Rita de Sousa Costa

O tráfego de dados teve um acréscimo de 54%, na rede fixa, e de 24%, na rede móvel, sendo também particularmente significativo o aumento de 94% do tráfego de voz na rede fixa. A utilização massificada e a partir de casa de meios tecnológicos ganhou uma relevância nova.

Na verdade, o aumento do tráfego de comunicações eletrónicas é uma realidade à escala europeia, tendo, por isso, a Comissão Europeia e o BEREC sugerido, em caso de congestionamento da rede, a adoção de medidas absolutamente excecionais em matéria de gestão de tráfego – e.g. a redução da velocidade de conexão, a redução da qualidade de disponibilização dos conteúdos, etc – aos operadores de telecomunicações e às plataformas OTT de *streaming*.

> "Aliado ao aumento do tráfego das comunicações eletrónicas, designadamente por força das novas formas de trabalho e prestação de serviços à distância, bem como de lazer, está também um conhecido conjunto de riscos para a privacidade das pessoas e para a segurança da informação e segredos comerciais das organizações."

Aliado ao aumento do tráfego das comunicações eletrónicas, designadamente por força das novas formas de trabalho e prestação de serviços à distância, bem como de ensino e lazer, está também um conhecido conjunto de riscos para a privacidade das pessoas e para a segurança da informação e segredos comerciais das organizações. A título ilustrativo, ao nível do *e-learning*, a CNPD, ciente desta realidade, emitiu recentemente umas Orientações sobre a utilização de tecnologias de suporte ao ensino à distância, as quais estabelecem um conjunto de recomendações, dirigidas ao Ministério da Educação e aos diretores dos estabelecimentos de ensino relativas à escolha das plataformas, assim como um conjunto de recomendações gerais de privacidade dirigidas a toda a comunidade educativa.

Nos parágrafos subsequentes identificamos alguns aspetos fundamentais, do ponto de vista jurídico, que pessoas e organizações devem ter em conta de forma a proteger-se.

Algumas ideias-chave para a proteção dos dados pessoais e para a segurança da informação, em contexto de teletrabalho, *e-learning* e lazer

De acordo com os dados do Eurobarómetro relativo à atitude dos europeus perante a cibersegurança, publicado em janeiro de 2020, previamente, portanto, à situação de emergência sanitária que tem assolado o país e o mundo, 54% dos portugueses inquiridos – um valor 8 pontos percentuais acima da média europeia – concordou com a afirmação segundo a qual a principal preocupação subjacente à utilização de serviços através da internet está relacionada com a possibilidade de serem efetuados tratamentos abusivos dos respetivos dados pessoais. Num outro Eurobarómetro também publicado em janeiro de 2020 – neste caso, sobre a atitude dos europeus perante a digitalização no seu quotidiano –, mais de 40% dos europeus declarou que gostaria de ter um papel mais ativo no controlo sobre os respetivos dados pessoais.

Num contexto em que a maioria da população ativa está em teletrabalho, as crianças e jovens estão em casa, dando o seguimento possível às atividades letivas por meios telemáticos, e num contexto em que crianças, jovens e adultos têm oportunidade de visualizar mais conteúdos de lazer, como filmes e séries, ou participar mais amiudamente em iniciativas de *webinars*, destacamos quatro ideias-chave, no que concerne à confidencialidade, à privacidade e à segurança da informação de pessoas e organizações, em tempos de emergência sanitária.

1. Esteja especialmente atento(a) a situações de fraude e, quando aplicável, reporte ao Centro Nacional de Cibersegurança e/ou aos órgãos de polícia criminal competentes

O Centro Nacional de Cibersegurança (CNCS) e a ENISA têm alertado para um conjunto de ciberameaças que têm surgido, no contexto da pandemia, e que aproveitam a fragilidade das pessoas e organizações. São destacados, entre outros, os ataques de *phishing* através de SMS e das redes sociais, *ransomware* e outros *malwares* contidos em determinadas aplicações, bem como a proliferação de emails e websites fraudulentos.

O regime jurídico da segurança do ciberespaço estabelece um regime de notificação obrigatória de incidentes dirigido às entidades da Administração Pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais e aos prestadores de serviços digitais.

O mesmo regime estabelece, ainda, um regime de notificação voluntária de incidentes que pode ser utilizado por qualquer entidade que tenha tido um incidente com impacto importante na continuidade dos serviços por si prestados.

A notificação de incidentes efetua-se através do website do CNCS. No entanto, esta notificação não preclude a competente participação aos órgãos de polícia criminal, uma vez que muitos dos incidentes de segurança resultam de atividades criminosas previstas e puníveis nos termos da lei penal, do cibercrime e/ou da proteção de dados.

> "O regime jurídico da segurança do ciberespaço estabelece um regime de notificação obrigatória de incidentes dirigido às entidades da Administração Pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais e aos prestadores de serviços digitais."

2. Enquanto titular dos dados ou na qualidade de representante de uma organização, leia sempre as Políticas ou Declarações de Privacidade das plataformas em que se inscrever ou das subscrições que adquirir

A disponibilização de políticas ou declarações de privacidade é uma das obrigações de transparência relativamente ao tratamento dos dados do titular que o RGPD impõe aos responsáveis pelo tratamento. Quando os dados do titular são recolhidos junto do mesmo ou de terceiro, o RGPD estabelece um conjunto de informações obrigatórias que o responsável pelo tratamento terá de fornecer. As políticas ou declarações de privacidade constituem uma das formas de o responsável pelo tratamento cumprir essa obrigação legal de transparência.

Por isso, a leitura do documento permite que uma pessoa que pretenda proceder à respetiva inscrição numa plataforma, ou uma organização que pretenda subscrever um serviço, conheça os aspetos fundamentais do tratamento dos dados efetuado pela plataforma e em que medida esta institui mecanismos de *privacy by design* e *by default*, o que permitirá igualmente, entre outras coisas, comparar os standards de privacidade entre diferentes concorrentes, na hora de optar pelo (melhor) serviço.

Algumas informações úteis que as políticas ou declarações de privacidade fornecem são, a título exemplificativo, e entre outras, as seguintes:

- **Para que finalidades os dados são tratados.** É nesta secção que poderá ficar a conhecer todos os (outros) usos que a plataforma dá aos seus dados para além da mera prestação do concreto serviço que subscreveu. Em casos extremos, poderá inclusivamente perceber se os seus dados são "vendidos" a terceiros.

- **Os tipos de dados pessoais recolhidos.** Nesta secção, poderá ficar a par de todos os dados que a plataforma recolhe. Note que os dados recolhidos devem limitar-se ao necessário para o cumprimento das finalidades, não sendo boa prática a exigência de múltiplos dados sem conexão com o funcionamento do serviço.

- **Os destinatários ou categorias de destinatários dos dados.** Esta secção permite conhecer as entidades ou categorias de entidades que poderão ter acesso aos seus dados, permitindo ter algum rasto sobre os mesmos. Tal abrange eventuais subcontratantes da plataforma, i.e., entidades que tratam os dados por conta desta e com quem a mesma celebrou um Contrato de Tratamento de Dados Pessoais.

- **As interconexões com redes sociais terceiras.** Esta secção permite aferir os dados que são partilhados com as redes sociais, quer através de uma opção do próprio titular (por exemplo, através da autenticação com recurso a uma conta de uma rede social) quer, eventualmente, através de outras interconexões.

- **A localização dos dados e das operações de tratamento.** O local onde os dados estão a ser tratados também poderá ser um critério relevante para a escolha de uma plataforma, atendendo a que muitos Estados situados fora do Espaço Económico Europeu (EEE) não têm legislação aprovada em matéria de proteção de dados ou têm legislação aprovada sem os *standards* aproximados aos que vigoram no EEE.

3. Enquanto trabalhador ou prestador de serviços de uma organização, leia cuidadosamente os regulamentos internos de utilização de dispositivos e plataformas elaborados pelo seu empregador ou cliente

Há cada vez mais organizações, incluindo aquelas que não detêm certificações ISO 27001, a adotar regulamentos internos em matéria de segurança da informação, que podem incluir, entre muitas outras coisas, a regulação da utilização de dispositivos e plataformas, quer na rede da própria organização quer noutras redes privadas a partir de casa, a regulação de B.Y.O.D., nos casos em que o trabalhador utilize o seu próprio dispositivo. Trata-se de boas práticas em matéria de segurança da informação ou até de *accountability* do responsável pelo tratamento, embora não haja qualquer obrigação legal expressa que determine a obrigatoriedade da elaboração de tais documentos.

Os trabalhadores ou os prestadores de serviços de uma organização que tenha aprovado um regulamento ou política interna dessa natureza devem proceder à respetiva leitura, identificar dúvidas e, neste caso, questionar o empregador/cliente, quando possível.

"Os trabalhadores ou os prestadores de serviços de uma organização que tenha aprovado um regulamento ou política interna dessa natureza devem proceder à respetiva leitura, identificar dúvidas e, neste caso, questionar o empregador/cliente, quando possível."

Por força da relação laboral, os trabalhadores estão adstritos a um conjunto de deveres de zelo, cuidado e lealdade relativamente ao empregador, bem como estão obrigados a cumprir as ordens e instruções do mesmo.

O não cumprimento das normas do regulamento ou política de segurança da informação pode, em certos casos, ter consequências muito gravosas para a organização, como, por exemplo, constituir a causa de um incidente de violação de dados pessoais ou de outras infrações ao RGPD, pelas quais a organização, enquanto responsável pelo tratamento, terá de responder. Por outro lado, situações como, por exemplo, a utilização de *software* não autorizado pela organização podem acarretar não só problemas em matéria de segurança da informação e proteção de dados pessoais, mas também problemas de propriedade intelectual. Ora, tais condutas em violação das normas internas da organização e, por conseguinte, dos deveres do trabalhador acima expendidos, podem, num determinado caso concreto, dar origem à instauração de um procedimento disciplinar.

O mesmo racional do parágrafo anterior também se pode aplicar, com as devidas adaptações, aos prestadores de serviços. Neste caso, não está em causa a aplicação do poder disciplinar, mas a possibilidade, no limite, de resolução do contrato de prestação de serviços ou até mesmo a instauração de uma ação de responsabilidade civil.

4. Tenha especial atenção à divulgação fortuita de segredos comerciais da organização que representa ou na qual trabalha

O conceito de segredo comercial remete para informações empresariais que são confidenciais e que se pretende que permaneçam confidenciais. Os segredos comerciais são um dos principais *assets* das organizações, em particular daquelas que assumem um perfil inovador, incluindo PMEs e *startups*.

O regime jurídico dos segredos comerciais resulta da transposição, no novo Código da Propriedade Industrial, da Diretiva relativa à proteção de *know-how*. De acordo com este regime, são objeto de proteção, *grosso modo*, as informações que, cumulativamente, (i) sejam secretas; (ii) tenham valor comercial pelo facto de serem secretas; e (iii) tenham sido objeto de diligências razoáveis no sentido de as manter secretas. Trata-se, como se pode constatar, de um conceito bastante amplo, que pretende conferir uma proteção consistente da informação.

As empresas devem por isso ter a capacidade de identificar que segredos comerciais são suscetíveis de ficar mais expostos num contexto de teletrabalho, e tomar medidas adicionais para protegerem tal informação, nomeadamente, através da restrição dos direitos de acesso dos utilizadores que se conectam à rede corporativa.

Adicionalmente, a lei estabelece um elenco típico de atos ilícitos de obtenção, utilização ou divulgação, sem consentimento, de segredos comerciais, destacando-se, entre outros, o acesso ou a cópia não autorizada de documentos que contenham o segredo e que estejam sob o controlo do respetivo titular, bem como a violação de acordos de confidencialidade.

Neste período de emergência sanitária, alguns dos riscos associados à utilização de dispositivos e plataformas em contexto de teletrabalho já elencados neste texto, designadamente as ciberameaças ou o recurso a aplicações e/ou plataformas que não priorizem a segurança da informação (e, por conseguinte, a confidencialidade) das informações obtidas, pode expor segredos comerciais das organizações.

Esta nota foi redigida a 03 de abril de 2020 e atualizada a 13 de abril de 2020, não tem pretensão de completude nem dispensa aconselhamento jurídico. ■