Campos Ferreira
Sá Carneiro
CS ASSOCIADOS

Tecnologia, Dados e Inovação Digital

Round-up mensal • Fevereiro 2021 • N.º 2

Os destaques do mês de fevereiro

O *round-up* do mês de fevereiro volta a dar maior destaque a temas de # privacidade e dados pessoais, assumindo aí particular relevância a circunstância de Portugal, ocupando atualmente a Presidência do Conselho da União Europeia, ter sido mandatado pelos Estados-Membros para iniciar conversações com o Parlamento Europeu, tendo em vista a discussão da proposta de texto do que se espera que venha a ser o futuro Regulamento ePrivacy (link mais à frente).

No que respeita a temas de # propriedade intelectual (aliás, é por eles que iniciamos o *round-up* deste mês), começamos por fazer referência às novas regras de registo de nomes de domínio .pt que entraram em vigor no passado dia 2 de fevereiro, analisando, em seguida, duas decisões inéditas do *High Court of Justice* do Reino Unido em matéria de bloqueio de websites.

Damos ainda destaque a um (muito completo) estudo divulgado pelo Parlamento Europeu dedicado ao importantíssimo tema da responsabilidade das plataformas digitais, as quais desempenham um papel central na # economia digital em que vivemos.

A intersecção das temáticas da # cibersegurança e # inteligência artificial surge evidenciada em dois documentos que também destacamos: por um lado, o estudo publicado pela ENISA sobre os desafios da cibersegurança relacionados com a utilização de inteligência artificial na condução inteligente; por outro, o novo regime aprovado na Alemanha (ainda apenas o projeto) sobre condução autónoma.

Finalmente, terminaremos o presente *round-up* no domínio das # comunicações eletrónicas, fazendo um breve ponto de situação sobre o leilão do 5G.

Para mais informações, por favor contactar:
Jorge Silva Martins (jorge.silvamartins@csassociados.pt) • João Carminho (joao.carminho@csassociados.pt)

Propriedade Intelectual

Novas regras de registo de nomes de domínio sobre o TLD .pt entram em vigor

No passado dia 2 de fevereiro, entraram em vigor as novas regras de registo de nomes de domínio sobre o TLD (*Top Level Domain*) .pt, cuja gestão, registo e manutenção se encontra a cargo da Associação DNS.PT.

Estas novas regras surgem em resultado de um processo largamente participado, que teve início com uma consulta ao público realizada entre 22 de maio e 5 de junho de 2020.

Entre as principais novidades, destacamos as seguintes:

- Ampliação do catálogo de nomes de domínio admissíveis para registo;
- Impossibilidade de novos registos sob os classificadores "org.pt" e "edu.pt";
- Obrigatoriedade de divulgação dos dados das pessoas coletivas responsáveis por um nome de domínio no diretório "WHOIS", eliminando-se, assim, o mecanismo (facultativo) de confidencialidade existente até ao momento;
- Possibilidade dada aos responsáveis por um nome de domínio de indicar um número de identificação alternativo ao NIF no âmbito do processo de registo e manutenção do nome de domínio, desde que aquele contenha um fim e valor legal iguais aos do NIF (importante para pessoas singulares ou coletivas estrangeiras que não tenham NIF ou outro);
- Possibilidade de a DNS.PT solicitar ao *registrant* e à entidade gestora que apresentem, no prazo máximo de 2 dias, prova do cumprimento das regras aplicáveis ao registo de nomes de domínio;
- Imposição da transferência da gestão de um nome de domínio por via online;
- Sujeição do registo de nomes de domínio com 2 caracteres às mesmas condições (incluindo preço) aplicáveis aos restantes nomes de domínio sob .pt;
- Fim da obrigatoriedade de a DNS.PT informar a entidade gestora, com a devida antecedência, da data de expiração do nome de domínio;
- Fim da possibilidade de a DNS.PT poder suspender ou remover, por sua própria iniciativa e a qualquer momento, nomes de domínio registados com finalidades especulativas e abusivas (sem prejuízo de o poder fazer no âmbito do processo de verificação da conformidade do nome de domínio, de acordo com os critérios de admissibilidade definidos, e dentro do prazo estabelecido para o efeito).

Por fim, importa referir que as novas regras não se aplicam aos processos pendentes à data da sua entrada em vigor, nem afetam as condições de atribuição dos nomes de domínio já registados.

As novas regras poderão ser consultadas aqui.

High Court of Justice ordena bloqueio de websites de *cyberlocker* e *stream ripping*

O *High Court of Justice (England and Wales)* emitiu, no passado mês de fevereiro, duas ordens de bloqueio de websites consideradas históricas, ambas por violação de direitos de autor.

A primeira decisão assentou na queixa apresentada pela *British Phonographic Industry* (representando um conjunto de editoras discográficas com uma quota de mercado de cerca de 99%) contra os 6 maiores prestadores de serviços de internet do Reino Unido. Nessa queixa, era solicitado o bloqueio do website nitroflare.com, um *cyberlocker* que, de acordo com os queixosos, era utilizado para cometer violações em larga escala dos direitos de autor dos seus representados.

O Tribunal, de forma inédita, deu provimento a um pedido desta natureza e ordenou o bloqueio do referido website. O que é interessante nesta decisão é a conclusão alcançada pelo tribunal de que os operadores do *cyberlocker* em questão violaram diretamente direitos de autor de terceiros ao praticar atos de comunicação ao público nos termos da secção 20 do *Copyright, Designs and Patents Act* de 1988 (CDPA), equivalente ao artigo 3.º da Diretiva Infosoc 2001, relativa à harmonização de certos aspetos do direito de autor e dos direitos conexos na sociedade da informação. Este entendimento, porém, vai em sentido exatamente contrário à posição do Advogado-Geral Saugmandsgaard Øe (nos processos apensos Youtube/Cyando), que concluiu que nem o Youtube nem o *cyberlocker* Uploaded estariam, nas respetivas operações, diretamente a praticar atos de comunicação ao público (nos termos do referido artigo 3.º da Diretiva Infosoc).

A segunda decisão, por sua vez, assenta também numa queixa apresentada pela *British Phonographic Industry*, tendo em vista o bloqueio de vários sites de *stream ripping*.

Também aqui o Tribunal deu provimento aos pedidos apresentados, invocando a violação das disposições do CDPA equivalentes aos artigos 2.º e 3.º da Diretiva Infosoc.

O texto da primeira decisão pode ser encontrado aqui. A segunda decisão pode ser lida aqui.

Economia Digital

Parlamento Europeu divulga estudo sobre responsabilidade das plataformas digitais

No passado dia 5 de fevereiro, o Parlamento Europeu divulgou um importante estudo intitulado "*Liability of online platforms*". Tendo em conta a importância central e crescente das plataformas online no contexto da economia digital, um dos temas que maior debate tem suscitado diz respeito à responsabilidade dessas plataformas relativamente a conteúdos ou produtos ilegais/lesivos gerados e/ou divulgados no quadro das suas operações.

Em traços gerais, e desde logo perante a falta de consenso em torno de uma definição única de "plataforma online", este estudo começa por avançar com uma proposta de classificação de plataformas, recorrendo, para o efeito, a seis critérios:

i) tipo de atividades desenvolvidas e serviços disponibilizados ("*activities*");
ii) setor relevante de atuação ("*sector of relevance*");
iii) participantes ("*actors*");
iv) tipo de utilização de dados ("*data usage*");
v) fonte de receitas ("*sources of revenues*");
vi) nível de controlo sobre os comportamentos dos utilizadores ("*level of control*").

Feita essa classificação, o estudo procede em seguida à identificação, descrição e avaliação de um conjunto de regimes de responsabilidade potencialmente operativos nos casos em que conteúdos ou produtos ilegais/lesivos sejam postos em circulação em plataformas online. Desse amplo catálogo consta, designadamente, a análise da Diretiva sobre o Comércio Eletrónico (em particular, do regime constante dos seus artigos 12.º a 14.º), da Diretiva Serviços de Comunicação Social Audiovisual (destacando, em particular, a dualidade regulatória serviços lineares *versus* serviços não lineares), da Diretiva (de 2019) relativa aos direitos de autor e direitos conexos no mercado único digital (em particular, do seu amplamente debatido artigo 17.º e da definição das suas fronteiras face ao disposto no artigo 14.º da Diretiva do Comércio Eletrónico) e, bem assim, da Decisão-Quadro do Conselho (de 2008) relativa à luta por via do direito penal contra certas formas e manifestações de racismo e xenofobia.

Fechado o mapeamento (e a análise crítica) de um conjunto de regimes potencialmente aplicáveis, o estudo elenca em seguida um conjunto de opções de *policy*, essencialmente assentes em duas abordagens complementares: por um lado, enfatizando que a responsabilidade das plataformas online constitui apenas um dos elementos (e não o único elemento) de um quadro europeu mais alargado, tendente a garantir um ambiente digital seguro; por outro, salientando que a responsabilidade deve ser adaptada à tecnologia ("*technology specific*" e não "*technology-neutral*", usando as expressões do estudo), devendo a regulação ser desenhada em função de tipologias de riscos e danos e das diferentes características das plataformas envolvidas.

Este estudo encontra-se disponível aqui.

Privacidade e dados pessoais

Conselho da UE anuncia acordo sobre texto da proposta de Regulamento *ePrivacy*

No passado dia 10 de fevereiro, o Conselho da UE anunciou que os Estados-Membros acordaram num mandato de negociação do projeto final do Regulamento *ePrivacy*, o qual permite à Presidência Portuguesa iniciar conversações com o Parlamento Europeu sobre o texto final daquele regulamento.

Tal como se pode ler no comunicado de imprensa oficial, disponibilizado no **website** do Conselho Europeu, as novas regras aplicar-se-ão: *(i)* ao conteúdo das comunicações eletrónicas transmitido através de serviços e redes acessíveis ao público e aos metadados relacionados com a comunicação, sendo igualmente extensivas aos dados máquina-a-máquina transmitidos através de uma rede pública; *(ii)* quando os utilizadores finais se encontrem na UE, incluindo-se aqui os casos em que o tratamento ocorra fora da UE ou em que o prestador de serviços esteja estabelecido ou localizado fora da UE.

De acordo com o mesmo comunicado, o projeto de Regulamento aprovado pelo Conselho mantém a regra de que os dados de comunicações eletrónicas são confidenciais, prevê que os utilizadores finais devem poder escolher verdadeiramente se aceitam ou não a utilização de cookies ou identificadores semelhantes, incluindo ainda regras em matéria de identificação em linha, listas públicas, comunicações não solicitadas e marketing direto.

Caso venha a ser aprovado, o referido projeto, que poderá ser consultado aqui, entrará em vigor 20 dias após a sua publicação no Jornal Oficial da UE, estando previsto um período transitório de 2 anos até ao início da sua aplicação.

Autoridade de Proteção de Dados Sueca aplica coima por utilização ilícita de software de reconhecimento facial

No passado dia 10 de fevereiro, a Autoridade de Proteção de Dados Sueca ("IMY") proferiu uma decisão condenatória na qual aplicou uma coima no montante de, aproximadamente, € 250.000 à autoridade policial daquele país pela utilização ilícita do "Cleaview AI", um software de reconhecimento facial (e tratamento de dados biométricos associado), em violação das disposições legais aplicáveis em matéria de tratamento de dados pessoais (em especial, dados criminais).

De acordo com a IMY, a autoridade policial não cumpriu com as suas obrigações enquanto responsável pelo tratamento daqueles dados, uma vez que: (i) não implementou as medidas técnicas e organizativas destinadas a assegurar (e demonstrar) um nível de segurança adequado, tendo em conta a legislação aplicável (p.e., ficou demonstrado que vários funcionários utilizaram o referido software sem qualquer autorização para o efeito); e (ii) não procedeu à realização de um DPIA antes de iniciar o tratamento, conforme era exigido no presente caso.

Para além da coima propriamente dita, a IMY ordenou ainda, no âmbito dos seus poderes de correção, a autoridade policial a: *(i)* formar os seus trabalhadores, tendo em vista evitar a ocorrência de situações semelhantes no futuro; e *(ii)* informar os titulares dos dados afetados, na medida em que as regras de confidencialidade o permitam.

A decisão pode ser consultada aqui (disponível em sueco).

Pós-Brexit: Comissão Europeia publica dois projetos de decisão de adequação em relação ao Reino Unido

No passado dia 19 de fevereiro, a Comissão Europeia publicou dois projetos de decisão de adequação em matéria de transferências de dados pessoais para o Reino Unido: um primeiro, ao abrigo do RGPD; um segundo, ao abrigo da Diretiva (UE) 2016/680, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa ao tratamento de dados pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais (a denominada "*Law Enforcement Directive*").

A publicação destes dois projetos marca o pontapé de saída do processo tendo em vista a sua futura adoção. Os dois projetos serão agora objeto de parecer do Comité Europeu para a Proteção de Dados e, posteriormente, sujeitos a aprovação por um comité composto por representantes dos Estados-Membros.

Tal como referido no *round-up* n.º 1 (relativo ao mês de janeiro), caso estes projetos venham a ser adotados, as transferências de dados pessoais para o Reino Unido continuarão a seguir um princípio geral de liberdade (como acontece atualmente, em virtude do acordo transitório pós-Brexit, celebrado entre a União Europeia e o Reino Unido), podendo, portanto, realizar-se em moldes idênticos aos que seriam aplicáveis caso o importador dos dados se situasse num Estado-Membro. Caso contrário, após a cessação do mencionado acordo, as transferências de dados para aquele país ficarão sujeitas ao regime aplicável às transferências de dados pessoais para países terceiros (constante do Capítulo V do RGPD).

Por fim, importa referir que as decisões de adequação que estão na base destes projetos serão válidas por um período de 4 anos, com possibilidade de renovação, caso o Reino Unido continue a assegurar um nível de proteção adequado no que respeita ao tratamento de dados pessoais.

O projeto de decisão de adequação ao abrigo do RGPD pode ser consultado aqui. O projeto de decisão de adequação ao abrigo da Diretiva (UE) 2016/680 pode ser acedido aqui.

CNIL publica recomendações sobre utilização de *chatbots*

No passado dia 19 de fevereiro, a Autoridade de Proteção de Dados Francesa ("CNIL") publicou um conjunto de recomendações acerca da utilização de *chatbots* (sistemas de comunicação baseados em inteligência artificial, muitas vezes utilizados em websites e aplicações para responder às perguntas mais frequentes dos utilizadores), tendo em vista a salvaguarda dos direitos de todos aqueles que com eles interagem.

De acordo com as referidas recomendações, para além dos princípios gerais em matéria de tratamento de dados pessoais (naturalmente aplicáveis neste contexto), os responsáveis pelo tratamento e/ou os subcontratantes que disponibilizem *chatbots* no âmbito dos seus serviços (os "Operadores"), devem dar especial atenção a um conjunto de aspetos.

Em primeiro lugar, à utilização de *cookies*, destinada a assegurar a continuidade técnica do *chatbot* ou a manter um histórico da conversação entre as diferentes páginas do website ou da aplicação em causa. De acordo com a CNIL, os Operadores têm, nestes casos, uma de duas opções: ou utilizam esses *cookies* antes de o utilizador ativar o *chatbot*, caso em que devem obter previamente o seu consentimento; ou utilizam esses cookies apenas quando o utilizador ativa o *chatbot*, caso em que os mesmos se consideram como "estritamente necessários" para a prestação do serviço de comunicação solicitado, dispensando-se, assim, o consentimento do utilizador.

Em segundo lugar, aos prazos de conservação dos dados dos utilizadores. Quanto a este aspeto, deve ser feita uma distinção entre: *(i)* situações em que os dados devem ser apagados assim que a conversa termina (p.e., *chatbot* auxilia num ato de compra); e *(ii)* situações em que o Operador pode legitimamente conservá-los durante um período de tempo mais longo (p.e., o utilizador apresenta uma reclamação sobre um produto comprado).

Por fim, e em terceiro lugar, ao tratamento de dados "sensíveis".

Tal como no ponto anterior, também aqui deve ser feita uma distinção entre:

(i) situações em que a sua recolha é previsível (p.e., *chatbot* de serviço de apoio a minorias sexuais ou relacionado com a saúde), caso em que o Operador deve assegurar que tal tratamento se enquadra numa das exceções previstas no artigo 9.º, n.º 2 do RGPD (e, eventualmente, proceder à realização de um DPIA antes de iniciar o tratamento); e

(ii) situações em que a sua recolha não é previsível (tendo apenas ocorrido por iniciativa do utilizador), caso em que o Operador deve adotar mecanismos de prevenção e minimização dos riscos, tais como a disponibilização de avisos para que os utilizadores se abstenham de fornecer este tipo de informação ou a implementação de um sistema de eliminação (imediata ou, pelo menos, regular) dos respetivos dados.

Estas recomendações podem ser consultadas aqui (disponíveis em francês).

Cibersegurança e Inteligência Artificial

ENISA e JRC publicam relatório conjunto sobre desafios de cibersegurança relacionados com a utilização de inteligência artificial na condução inteligente

No passado dia 11 de fevereiro, a Agência da União Europeia para a Cibersegurança (ENISA) e o Centro Comum de Investigação da Comissão Europeia (JRC) publicaram um relatório conjunto no qual analisam um conjunto de riscos de cibersegurança relacionados com a utilização de Inteligência Artificial (IA) na condução inteligente, apresentando recomendações para a sua mitigação.

Subjacente a esta publicação encontra-se a ideia de que os veículos inteligentes, baseados em sistemas de inteligência artificial que permitem tomar decisões tradicionalmente tomadas por seres humanos, tal como todos os outros sistemas desta natureza, apresentam vulnerabilidades que podem comprometer o seu bom funcionamento e, em última instância, colocar em risco os seus condutores, passageiros e peões.

Para além dos problemas técnicos que podem surgir (p.e., avarias repentinas), estes veículos podem ser afetados por diversas condutas (que, em alguns casos, poderão consubstanciar verdadeiros ataques), tais como a colocação de tinta na estrada ou autocolantes em sinais, suscetíveis de interferir com o seu sistema de inteligência artificial e, em particular, com a sua segurança.

Por fim, o relatório apresenta diversas recomendações que visam a atenuação destes riscos, de onde se destaca a realização de processos de avaliação e testes de segurança contínuos, por forma a identificar potenciais riscos e corrigir riscos já existentes, bem como a adoção de uma cultura e políticas de segurança de inteligência artificial, as quais devem estar presentes em toda a cadeia de distribuição do setor automóvel ("*security by design approach*").

Este relatório encontra-se disponível para download aqui.

Projeto de diploma sobre condução inteligente aprovado na Alemanha

No passado dia 10 de fevereiro, o Ministério Alemão dos Transportes e Infraestruturas Digitais alemão publicou um projeto de lei sobre condução inteligente, o qual visa completar a legislação existente em matéria rodoviária, adaptando-a aos veículos altamente automatizados (*i.e.*, sem condutor, embora seja exigido um técnico supervisor, que poderá estar dentro do veículo ou a trabalhar remotamente).

De acordo com o referido projeto, estes veículos necessitarão de uma licença especial para circular e só poderão fazê-lo em áreas determinadas, devidamente aprovadas para o efeito. Reunidas estas condições, estes veículos poderão, por exemplo, deslocar pessoas e mercadorias em rotas pré-estabelecidas.

A sua aplicabilidade a veículos de passageiros será, no entanto, muito limitada.

Em primeiro lugar, devido à limitação existente quanto às áreas de circulação; em segundo lugar, porque esta matéria encontra-se regulada a nível europeu, mais concretamente, pelo Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, relativo à homologação e à fiscalização do mercado dos veículos a motor e seus reboques, e dos sistemas, componentes e unidades técnicas destinados a esses veículos, embora estejam previstas isenções para novas tecnologias e homologações nacionais de veículos produzidos em pequenas séries. Um exemplo de potencial aplicação a este tipo de veículos poderá ser no âmbito do estacionamento, em que o condutor deixa o veículo à entrada de um parque de estacionamento e este, com base em sensores, procura um lugar livre, onde acaba por estacionar.

Por fim, importa referir que a utilização destes veículos irá originar um tratamento de dados considerável, os quais deverão ser devidamente protegidos e, no caso de dados pessoais, devidamente articulados com o RGPD.

O projeto de lei, que pode ser consultado aqui (disponível em alemão), será agora submetido ao parlamento alemão, estimando-se que o mesmo venha a ser aprovado dentro do horizonte temporal dos próximos meses.

Comunicações Eletrónicas

Prossegue o leilão do 5G

A fase de licitação principal do leilão para a atribuição de direitos de utilização de frequências nas faixas dos 700 MHZ, 900 MHz, 2,1 GHz, 2,6 GHz e 3,6 GHz prosseguiu no mês de fevereiro, com a realização de 20 dias de licitação.

A duração da fase principal do leilão do 5G já ultrapassou o período de um mês, num processo que está a superar largamente a duração da fase reservada a novos entrantes no mercado móvel nacional e que, inevitavelmente, tornará impossível cumprir o calendário proposto pela ANACOM (que havia manifestado a sua intenção de garantir a disponibilização de serviços comerciais ainda no primeiro trimestre de 2021).

No último dia de licitação do mês de fevereiro (26 de fevereiro) realizaram-se seis rondas, tendo as licitações atingido o valor de 239,06 milhões de euros.

O leilão prossegue no mês de março.

A ANACOM disponibiliza informação diária (e detalhada) sobre o leilão 5G aqui.

CS ASSOCIADOS