
CYBERLAW
by CIJIC

# CYBERLAW by CIJIC

**EDIÇÃO N.º VIII – SETEMBRO DE 2019**

**REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA**


CYBERLAW
by CIJIC

# CYBERLAW by CIJIC



**ISSN 2183-729**

## NOTAS DO EDITOR:

Nesta nova edição da revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa, dada a pertença do CIJIC ao grupo do Network of Centers (https://networkofcenters.net/center/cyberlaw-research-centre-university-lisbon-school-law-cijic ), a obrigação identitária desta comunidade, persuade-nos a publicar artigos em inglês. Traremos, portanto, duas investigações em anglo-saxónico.

Na oportunidade presente da publicação desta VIII Edição e dos actos legislativos nacionais em curso, foi nossa opção trazer uma visão jurídica sobre o poder, eventualmente, manipulativo da democracia através das redes sociais.

O contexto é o da eleição presidencial de 2018, no Brasil, mas o modo como se desenvolve, desde uma engenharia social mais dissimulada a uma difusão de *fake news* ou *deep fakes*, permitem utilizar tais distorção de forma globalizada. Sendo certo que carece de maior investigação o real efeito da *realidade* das redes sociais *versus* o do "*quotidiano não digitalizado*" e o resultado concreto disto em sede de apuramento final dos resultados de eleições livres e universais, parece já possível concluir que, mesmo ante esta condicionante ainda não determinada, a realidade democrática pode, efectivamente, ser *hackeavel*.

Não obstante, por princípio, a clarificação dos conceitos de *fake news* e *deep fakes*, deveria afastar-se do radical "notícia" que lhe dá a alma. Porque uma notícia corresponde a um acto jornalístico, exercício com tutela constitucional, que conclui um dado conteúdo factual, relatando acontecimentos de interesse geral da comunidade com

o maior grau de objectividade possível. Uma notícia identifica-se pela clareza, simplicidade, exatidão, e pelo bom uso da língua em que é escrita. Compreende contraditório, ou a possibilidade deste, suporta-se em fontes credíveis. Há todo um ónus ético e deontológico que sopesa uma notícia assinada por um jornalista. Toda esta súmula é uma notícia. Comentário, mesmo televisivo, liberdade de opinião, todos os outros "*fenómenos*", não se identificam com este radical conceptual. Logo, porque continuamos a insistir em querer colar uma qualquer liberdade opinativa ao conceito de "notícia"?

Não vos soa ridículo o exercício de contínuo *fact-check* a exercícios de liberdade de opinião? Desde quando é que mentira foi legalmente proibida? Mas, pelo contrário, uma notícia que veicule um facto falacioso, de cariz subjectivo, não é fortemente sancionável? Desde logo pelos poderes de regulação, pela sindicância da própria classe, pelo público?

Será assim tão difícil perceber as diferenças?

Noutro plano, em efeméride do décimo aniversário da Lei do Cibercrime portuguesa, a Lei n.º 109/2009, de 15 de Setembro, olhamos para a perspectiva da aptidão do enquadramento legal, num contexto nada fácil, de obtenção de resultados eficazes em tempos, da acção *contra-legem versus* investigação, demasiado assíncronos. Qual a razão que explica a falta de enquadramento legal nacional para o agente (digital) encoberto, quando dezenas de outras polícias de investigação, congéneres, já o fazem?

Se há disciplina onde a soberania das fronteiras físicas acabou é no digital. Outrossim, pela fragilidade dos "muros" digitais e das deficiências do enquadramento jurídico-penal nacional, abordaremos ainda o fenómeno do *Ransomware*. Dez anos volvidos da Lei do Cibercrime, e em apologia à vanguarda em que já estivemos nos idos do início da década de 90 do século passado, impõe-se no presente, em 2019, o revisitar a especialidade da lei do cibercrime. O contexto presente de *leaks* de índole variada e processos mais ou menos mediáticos, reclamam prudência. A digitalização do Estado, por outro lado, impõem mudanças assertivas. Ademais, quer a falta da criminalização do roubo de identidade digital[1], quer a complexidade jurídico-penal do

1 Atente-se por exemplo no Considerando (14) da Directiva: "(…) *A adoção de medidas eficazes contra a usurpação de identidade e outras infrações relacionadas com a identidade constitui outro elemento importante de uma abordagem integrada contra a cibercriminalidade. A necessidade de intervenção da*

*Ransomware*, quer a própria transposição da Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013 (esgotado o prazo de transposição no ano de 2015), quer a protecção do Estado digital (e não só) reivindicam melhores ferramentas, desde logo legais, que bem que poderiam servir de impulso necessário ao dormente legislador nacional.

Por fim, tema que não sai das agendas, o Regulamento geral de protecção de dados. Desta vez, as fricções que a ferramenta *blockchain*, cada vez mais usada no contexto das relações entre particulares e organizações, compreende face ao RGPD mas, e também, a melhor consecução dos objectivos proclamados pelo RGPD que esta ferramenta pode ajudar a alcançar.

Por fim, mas antecipando o futuro, atendendo ao propósito identitário da revista, passaremos nas próximas edições a publicar artigos de investigação dos alunos do Mestrado em Segurança da Informação e Direito do Ciberespaço, trabalhos estes desenvolvidos nas cadeiras que frequentarem.

Resta-me, neste final, agradecer a todos quantos contribuíram para mais uma edição da Revista, pelo esforço e pelo trabalho, enereçando, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um reconhecido:

- Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

**Boas leituras.**

Lisboa, FDUL, 29 de Setembro de 2019

Nuno Teixeira Castro

*União contra este tipo de comportamento criminoso poderá também ser ponderada no contexto da avaliação da necessidade de um instrumento transversal e abrangente da União."*

CYBERLAW

by CIJIC

# OPINIÃO

# A GESTÃO DOCUMENTAL COMO A ALAVANCA À CONFORMIDADE DO REGULAMENTO GERAL DE PROTECÇÃO DE DADOS (RGPD)

**SOFIA PINA** [1]

1 Arquivista. Contactos:. sofia.opina@gmail.com

*O RGPD e a gestão documental são alavancas mútuas porque "arquivar, preservar e controlar dados pessoais" é o mesmo processo que "arquivar, reter e controlar documentos relevantes": precisamos de conhecer a vida útil da informação e justificar a sua duração, caso contrário, vamos eliminá-los indiscriminadamente. Irrecuperavelmente.*

De um lado apresenta-se-nos o RGPD, como baluarte da Protecção de dados de carácter pessoal dos cidadãos do espaço europeu; do outro lado, a gestão documental e a abordagem empresarial para o controlo da informação ao longo do tempo. Entre ambos existe a ténue linha da recuperação de informação.

Foquemo-nos **nos prazos de conservação**.

Tudo começa na recolha.

O RGPD contém disposições específicas sobre a documentação das atividades em processamento. Os dados pessoais incluem dados recolhidos diretamente através de formulários, bem como todos aqueles que cedemos. Mesmo que de forma involuntária. O RGPD requer uma recolha de dados pessoais "lícita e legal". A recolha "lícita" é baseada no consentimento prévio e na explicação da legitimidade dessa mesma recolha (prospeção comercial, marketing, estudo, estatística, etc. ...). A documentação RGPD deve registar o consentimento, como garantia de rastreabilidade ao longo do tempo, e o princípio da proporcionalidade de recolha apresentado é o de manter a necessidade estrita. Os registos das atividades devem manter-se como fins do processamento, de partilha de dados e de retenção, uma vez que a entidade reguladora, se assim o entender, poderá requerer a sua disponibilização.

A gestão documental é, aqui, precursora na definição dos prazos de conservação ao considerar os dados a partir do seu momento de produção e não de registo. O RGPD enuncia

períodos de retenção de dados, mas não refere que estes mesmos prazos estejam associados aos processos de negócio.

Se nos focarmos apenas na duração da utilização operacional, corremos o risco de nos esquecermos da salvaguarda dos requisitos de evidências! O mesmo é dizer que os dados individuais também pertencem a bases de dados com valor de evidência de longo prazo.

Com a promulgação da Lei n.º 58/2019 de 8 de Agosto, que assegura a execução na ordem jurídica nacional do Regulamento 2016/679 do Parlamento e do Conselho Europeus, o prazo de conservação de dados pessoais é fixado no artigo 21.º. Tal como a gestão documental já o executava, o prazo de conservação de dados pessoais é fixado por norma legal ou regulamentar, e na sua falta, a finalidade será justificada pela necessidade.

Desde que as organizações adoptem medidas técnicas e organizativas adequadas às garantias dos titulares dos dados, o fim justificará a conservação permanente ou num espaço de tempo mais dilatado, desde que o arquivo seja de interesse público, para investigação científica, histórica ou estatística[1].

O artigo 26.º da Lei n.º 58/2019, *glosou* a redação da *L.A.D.A. – Lei de Acesso aos Documentos Administrativos* – Lei n.26/2016 de 22 de Agosto, no que concerne aos documentos administrativos com dados pessoais.

O artigo 31.º da Lei n.º 58/2019 garante ao arquivo de interesse público para os fins de investigação identificados, a conservação de dados, salvaguardando os interesses dos titulares, através de técnicas de minimização, de anonimização ou ainda de pseudonimização. Ou seja, *mantem-se em vigor* a redação atual do Decreto-Lei 16/93 de 23 de Janeiro, no que se refere ao tratamento de dados pessoais para fins de arquivo de interesse público.

Os processos de documentação permitem cumprir vários requisitos do RGPD, além de melhorar a gestão de dados, já que são essas as obrigações do responsável pelo tratamento de dados (*Data Controller)* e do processador *(Data Processor*).

1 Ver *Orientações sobre Protecção de Dados nos Arquivos - Orientações do GEA sobre a implementação do Regulamento Geral de Proteção de Dados no setor dos arquivos, Título original: Guidance on data protection for archive services. EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector, Autor*: © European Archives Group, Tradução da autora.

Continuando no artigo 21º, sempre que houver a necessidade de comprovar a obrigação contratual, a conservação num prazo dilatado é permitida, desde que fundamentada, salvaguardando os direitos correspetivos.

A minimização e /ou a anonimização dos dados no momento da recolha é apenas um dos aspetos. Se considerarmos um serviço como a parte exposta de um conjunto de realizações de trabalho (definição de arquitetura empresarial), o exercício não se limita à catalogação dos serviços, mas à caracterização dos processos que os realizam. Por exemplo, a finalidade dos tratamentos é mais adequada se representada pelos processos (ou seja, as realizações de trabalho) do que se pelos serviços (a parte exposta). O documento faz parte de um processo e é segundo a MEF/LC *(Macroestrutura funcional / Lista Consolidada*), que os prazos e destinos da informação são definidos por processo, ou seja, é o contexto de negócio que determina as regras para gerir as peças de informação (o *documento).*

Em termos de ferramentas tecnológicas, a proteção de dados por *design* deverá fazer parte da transformação digital de uma empresa, além de permitir funcionar como garante, a quem gere as aplicações, que está a gerir dados recolhidos desde o início da sua produção.

A boa gestão da informação exige uma clara definição de perfis bem como a correta segmentação de processos de negócio, evitando o uso de dados recolhidos a um cliente num outro contexto, uma vez que a avaliação, e a posterior classificação de dados, só será válida caso os dados sejam recolhidos de forma lícita, nos termos do RGPD.

As auditorias e os exercícios de mapeamento de dados, suportam-se no processamento da documentação das atividades, e todos esses registos devem ser mantidos por escrito (ainda que em suporte digital), e atualizados de forma a refletirem sempre o processamento das atividades atuais. E em conformidade com a lei.

É importante que o sistema informático de gestão de dados pessoais se baseie em regras de arquivo (*a gestão documental*), de preferência actuais, cumprindo as leis em vigor e conhecidas pelos vários atores da empresa.

Os arquivistas / gestores documentais, por tudo isto, apresentam-se assim como os mais avalizados, se não os únicos, para fazer cumprir corretamente a legislação no tocante aos prazos de conservação dos dados pessoais.