PATRÍCIA DOS SANTOS RAMINHOS

O FUTURO DO *ePRIVACY*: OS DESAFIOS TRAZIDOS PELO ARTIGO 6.º DA PROPOSTA DE REGULAMENTO ÀS OPERADORAS DE TELECOMUNICAÇÕES

Dissertação com vista à obtenção do grau de
Mestre em Direito na especialidade de Direito Internacional e Europeu

Orientador:

Doutor Francisco Pereira Coutinho, Professor da Faculdade de Direito da Universidade Nova de Lisboa

Julho de 2021

PATRÍCIA DOS SANTOS RAMINHOS

O FUTURO DO *ePRIVACY*: OS DESAFIOS TRAZIDOS PELO ARTIGO 6.º DA PROPOSTA DE REGULAMENTO ÀS OPERADORAS DE TELECOMUNICAÇÕES

Dissertação com vista à obtenção do grau de
Mestre em Direito na especialidade de Direito Internacional e Europeu

Orientador:

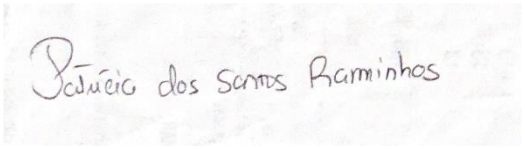
Doutor Francisco Pereira Coutinho, Professor da Faculdade de Direito da Universidade Nova de Lisboa

Julho de 2021

DECLARAÇÃO ANTIPLÁGIO

Declaro por minha honra que o trabalho que apresento é original e de minha exclusiva autoria. Declaro ainda que todas as citações estão corretamente identificadas. Tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta ética e disciplinar.

Lisboa, 09 de julho de 2021.



DECLARAÇÃO DE CONFORMIDADE DO NÚMERO DE CARACTERES

Declaro que o corpo da presente dissertação de mestrado é composto por 167 121 caracteres, incluindo espaços e notas de rodapé.

Declaro, ainda, que o Resumo é composto por 1407 caracteres e o Abstract por 1365 caracteres.

AGRADECIMENTOS

Não posso deixar de aqui expressar os meus mais sinceros agradecimentos a quem sempre me acompanhou não apenas durante esta dissertação, mas ao longo da vida: aos meus pais, que nunca me deixaram desistir e que me incentivaram sempre a seguir os meus sonhos. Este é mais um. Um dos mais importantes.

Depois quero também agradecer ao Gonçalo Moreira, por me ter apoiado nos piores momentos, e por me ter feito encontrar forças onde eu já nem sabia que existia para concluir esta tarefa. Obrigada pelo companheirismo e por todos os "tu consegues".

Aos meus amigos, que por não querer deixar ninguém excluído não irei nomeá-los, até porque eles sabem quem são e o lugar que ocupam na minha vida.

À minha família, por torcer pelo meu sucesso, tal como uma claque de futebol torce pelo seu clube, de forma incondicional, acompanhando-o para qualquer lugar, chorando nas derrotas e comemorando nas vitórias.

Por último, mas não menos importante, deixo um especialmente agradecimento ao meu orientador, o professor Francisco Pereira Coutinho, por ter visto em mim, há já seis anos que levo de Nova School of Law, talento para o Direito e por me ter apoiado e ajudado ao longo desta tarefa árdua que é a elaboração de uma dissertação de mestrado.

O meu mais sincero agradecimento a todos!

MODO DE CITAÇÃO E OUTROS ESCLARECIMENTOS

- As referências bibliográficas serão feitas nas notas de rodapé, de acordo com a Norma Portuguesa 405-1 e 405-4 do Instituto Português de Qualidade.
- As expressões em língua estrangeira ou latinismos encontram-se a itálico.
- Os textos em língua estrangeira foram traduzidos para a língua portuguesa. A tradução dos mesmos é da responsabilidade da autora.
- A presente dissertação foi redigida ao abrigo do novo Acordo Ortográfico.

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

AEPD – Autoridade Europeia para a Proteção de Dados

APD – Autoridade para a Proteção de Dados

CARTA/CDFUE – Carta dos Direitos Fundamentais da União Europeia

CEPD – Comité Europeu para a Proteção de Dados

CE – Comissão Europeia

CEDH – Convenção Europeia dos Direitos do Homem

CECE – Código Europeu das Comunicações Eletrónicas

Diretiva/Diretiva *ePrivacy* – Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002

GT29/WP29 – Grupo de Trabalho do Artigo 29.º/WP 29

IOT – Internet of Things

M2M – Machine-to-Machine

OTT – Over-The-Top

p. – página

pp. – páginas

Para. – Paragrafo

PE – Parlamento Europeu

RGPD – Regulamento Geral de Proteção de Dados

Regulamento/ Regulamento *ePrivacy* – Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE

TJ/TJUE – Tribunal de Justiça da União Europeia

TEDH – Tribunal Europeu dos Direitos do Homem

TUE – Tratado da União Europeia

UE – União Europeia

RESUMO

A presente dissertação de mestrado incidirá sobre a proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas, também designado por Regulamento *e-Privacy*. O foco da minha investigação será o artigo 6.º da proposta de Regulamento, referente ao tratamento do conteúdo e dos metadados das comunicações eletrónicas. O artigo 6.º nas suas sucessivas alterações, primeiro pelo Parlamento Europeu e, posteriormente, pelas sucessivas presidências do Conselho Europeu, constituía um impedimento ao desenvolvimento tecnológico num setor primordial para a economia digital, como é o setor das comunicações eletrónicas, uma vez que previa uma abordagem baseada numa proibição geral do tratamento de dados de comunicações eletrónicas, com exceções bastantes restritas. Volvidos quatro anos e sob a égide da presidência portuguesa, o texto ePrivacy foi finalmente aprovado no Conselho Europeu, dando-se agora início a negociações com o Parlamento Europeu e com o Comissão Europeia, com vista à aprovação do texto final. Este novo texto, ainda que não totalmente alinhado com o RGPD e com as expectativas da indústria é, quando comparado com os seus antecessores, o texto que melhor equilibra um nível elevado de proteção dos dados e metadados das comunicações eletrónicas com o tão desejado desenvolvimento tecnológico.

Palavras-Chave: Dados Pessoais, Comunicações Eletrónicas, Metadados, Privacidade, RGPD, Tratamento de dados, Desenvolvimento Tecnológico, Economia Digital, Confidencialidade.

ABSTRACT

The present master´s dissertation will focus on the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications, also known as *ePrivacy* Regulation. The cornerstone of my dissertation will rely on article 6 of the Proposed Regulation, inciding on the processing of eletronic comunications content and metadata. Article 6, after several amendments, firts by the European Parliament and then by the succesives European Council presidencies, had constitute an obstacle to technological development in a vital sector of the digital economy, such as the eletronic communications sector, once it was based on an approach which established a general prohibition for processing of eletronic communications data, with very strict exceptions. After four years of discussion and under the portuguese presidency, the ePrivacy text was finally aproved in the European Council, starting now the negotiations with the European Parliament and with the European Comission. This new text, even if not fully aligned with GDPR and with industry expectations is, when compared with its predecessors, the text that better accomplishes the balance between a high level of protection of electronic communication data and metadata with the desired technological development.

Keywords: Personal data, eletronic comunications, metadata, privacy, GDPR, Data Processing, Technological Development, Digital Economy, Confidentiality.

INTRODUÇÃO

I. Com a entrada em vigor do Regulamento Geral de Proteção de Dados, a 25 de maio de 2018, tornou-se da máxima importância reformar outro instrumento jurídico essencial para a proteção de dados na União Europeia. Assim, a 10 de janeiro de 2017, é apresentada a tão aguardada Proposta da Comissão Europeia relativa ao novo Regulamento *ePrivacy*, que veio substituir a Diretiva 2002/CE/EC, que não é alvo de revisão desde 2009.

A Proposta de Regulamento *ePrivacy*, tem como principal objetivo assegurar a proteção dos direitos e liberdades fundamentais, em especial, o respeito pela vida privada, a confidencialidade das comunicações e a proteção dos dados pessoais no setor das comunicações eletrónicas. Assegura também a livre circulação de dados, equipamentos e serviços de comunicações eletrónicas ao nível da União Europeia. A Proposta de Regulamento *ePrivacy* concretiza o direito fundamental ao respeito pela vida privada, no setor das comunicações eletrónicas, tal como previsto no artigo 7.º da Carta dos Direitos Fundamentais da União Europeia.

A escolha deste tema está relacionada com o facto de, atualmente, estar a exercer funções numa das maiores operadoras de comunicações do pais, que pertence à ETNO – *European Telecommunications Network Association* - e ter tido a oportunidade de, ao longo do último ano, ter assistido *"in loco"* ao debate intenso que tem sido levado a cabo acerca da Proposta de Regulamento *ePrivacy*, nomeadamente no que diz respeito ao artigo 6.º relativo ao "Tratamento Permitido de Dados de Comunicações Eletrónicas." No fundo, este é o artigo que irá estabelecer os fundamentos de licitude de tratamento dos dados de comunicações eletrónicas, seja do conteúdo, seja dos metadados, por parte dos prestadores de serviços de comunicações eletrónicas.

Desta forma, a primeira paragem no caminho desta dissertação será sobre a necessidade de reforma da atual *Diretiva ePrivacy*, perante o novo quadro jurídico europeu para a proteção dados, mencionando o que se alterou desde 2009, nomeadamente de que forma é que a entrada de novos intervenientes no setor das comunicações, os chamados provedores de serviços *Over-The-Top*, como o Gmail, o WhatsApp, o Facebook Messenger, impactaram a elaboração da Proposta de Regulamento *ePrivacy*. De seguida, debruçar-me-ei sobre as principais alterações entre a Diretiva ePrivacy e a

Proposta de Regulamento: o porquê da escolha de um regulamento, o alargamento do âmbito de aplicação material e territorial, a distinção entre conteúdo e metadados, novas normas aplicadas a *cookies*, a regulação das definições de privacidade, as comunicações não solicitadas e a aplicação do mecanismo de coerência e das sanções replicadas do RGPD.

II. Já no âmbito do capítulo II, o que me interessou esmiuçar foi de que forma é que o RGPD e o futuro Regulamento *ePrivacy* se irão articular na sua relação entre Lei Geral – Lei Especial, respetivamente, primeiro debruçando-me sobre se não bastaria a regulação do RGPD e depois sobre a relação entre o RGPD e a atual Diretiva ePrivacy.

III. No capítulo III, começa a pedra angular da minha dissertação: a eterna questão, que não foi respondida ao longo dos último quase quatro anos e que tem sido um dos principais motivos de debate desde a publicação da Proposta da Comissão Europeia: afinal, o artigo 6.º configura-se como sendo um bastião da proteção da privacidade nas comunicações eletrónicas ou, pelo contrário, é um impedimento ao desenvolvimento tecnológico? No meu entender, a resposta a esta questão, seja num ou noutro sentido, será determinante para determinar o futuro da Europa enquanto exportador de produtos e serviços da economia digital. Embora o artigo 6.º não se debruce apenas sobre o tratamento de metadados, estes têm tido um papel central no debate sobre este artigo, provocando sentimentos totalmente antagónicos entre as instituições europeias e respetivos organismos e a indústria, no fundo, estamos perante um daqueles casos em que a prática ultrapassa em muito a teoria, o que se poderá verificar através dos exemplos que darei na presente dissertação.

Posteriormente, irei tentar explicar o caminho que foi traçado desde a publicação da Proposta de Regulamento pela Comissão, passando pelas alterações do Parlamento Europeu e pelas sucessivas alterações no Conselho Europeu, até à aprovação do texto final pelo Conselho Europeu, no âmbito da presidência portuguesa, iniciando-se agora um longo caminho de negociações com o Parlamento Europeu e com a Comissão Europeia.

Por último, no âmbito do artigo 6.º, uma das questões que mais tem suscitado duvidas é a questão dos metadados e do tratamento dos mesmos para outros fins compatíveis, tal como previsto no RGPD. Explicarei, na presente dissertação, porque é que o tratamento de metadados para outros fins compatíveis, com recurso a salvaguardas

como a pseudonimização ou a cifragem é o caminho que deverá ser seguido para estabelecer um equilíbrio entre um elevado nível de proteção de dados e metadados desejado pelas autoridades europeias e o desenvolvido tecnológico desejado pelos intervenientes no mercado das comunicações.

Capítulo 1: A atual Diretiva *ePrivacy* e a Proposta de um novo Regulamento

1.1– Da necessidade de propor um novo regulamento para o setor das comunicações eletrónicas

A 10 de janeiro de 2017, a Comissão Europeia comunicou a intenção de substituir a atual Diretiva relativa ao respeito pela vida privada e à proteção de dados pessoais nas comunicações eletrónicas, também designada por Diretiva 2002/58/EC[1] ou Diretiva *ePrivacy*, por um novo Regulamento[2], dado que a mesma não é alvo de um processo de revisão desde 2009. No entanto, a identificação da necessidade de elaborar um novo quadro jurídico que protegesse a privacidade das comunicações eletrónicas no seio da União Europeia encontra-se há muito identificada.

A Estratégia para o Mercado Único Digital ou "Estratégia MUD"[3] que veio demonstrar a urgência de uma reforma no quadro dos dados pessoais na União Europeia, datada de 2015, é clara quanto à necessidade, no contexto deste novo quadro jurídico relativo à proteção de dados pessoais, de iniciar um processo de revisão da Diretiva *ePrivacy*, uma vez que a mesma se encontra desatualizada face ao atual contexto tecnológico e jurídico.

Encontra-se desatualizada face ao atual contexto tecnológico, uma vez que a Diretiva não abrange os chamados serviços *Over-The-Top*, aplicando-se, em exclusivo, às operadoras de telecomunicações, numa visão tradicional daquilo que se considera um provedor de comunicações eletrónicas, ignorando que os *OTTs* utilizam as infraestruturas de Internet disponibilizadas pelas operadoras tradicionais para poderem fornecer serviços "funcionalmente equivalentes", sem que sobre estes recaia qualquer onerosidade. É o caso de prestadores de serviços da sociedade de informação, tais como o WhatsApp, o Gmail, o Skype, e os serviços *VOIP (Voice over Internet Protocol)*.

[1] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas.
[2] Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE.
[3] «Estratégia para o Mercado Único Digital na Europa» Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, 6 de maio de 2015, disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

Também ao nível jurídico, a Diretiva *ePrivacy* não acompanhou a evolução dentro do atual quadro jurídico europeu para a proteção de dados, nomeadamente, no que foi o seu maior ato normativo, a entrada em vigor do Regulamento Geral de Proteção de Dados[4], a 25 de maio de 2018, que veio substituir a Diretiva 95/46/CE do Parlamento Europeu e do Conselho e que devia ter sido acompanhada por uma revisão simultânea da Diretiva *ePrivacy*, uma vez que esta clarificava e complementava a diretiva, agora substituída pelo RGPD, atuando em relação a esta como *"lex specialis"*[5], prevendo normas específicas para o tratamento dos dados pessoais no domínio das comunicações eletrónicas e, contrariamente ao RGDP, aplicando-se não só a pessoas singulares, mas também a pessoas coletivas.

A importância da revisão da Diretiva *ePrivacy* é demonstrada através deste excerto da "Estratégia MUD": *"*Uma vez adotadas as novas normas da UE em matéria de proteção de dados, previstas para o final de 2015, a Comissão procederá à revisão da Diretiva Privacidade e Comunicações Eletrónicas com o objetivo de assegurar um elevado nível de proteção para os titulares dos dados e condições equitativas para todos os intervenientes no mercado."[6]

Também a Autoridade Europeia para a Proteção de Dados, enquanto entidade de supervisão e órgão consultivo independente foi chamada a pronunciar-se, em 2016, pela Comissão Europeia, sobre a revisão da Diretiva.

Neste parecer preliminar, a AEPD é clara quanto à necessidade de proceder à modernização da atual Diretiva: "A revisão visa a modernização e a atualização da Diretiva Privacidade e Comunicações Eletrónicas (*ePrivacy*), como parte de um esforço mais amplo com vista ao estabelecimento de um quadro jurídico coerente e harmonizado para a proteção de dados na Europa."[7]

---

[4] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

[5] O art.º1, n.º1, da Diretiva 2002/58/CE é claro quanto à relação de complementaridade da mesma em relação à Diretiva 95/46/CE, prevendo que: "Para os efeitos do n.º1, as disposições da presente diretiva especificam e complementam a Diretiva 95/46/CE."

[6] Ver "Estratégia MUD", p.15.

[7] Síntese do parecer preliminar da Autoridade Europeia para a Proteção de Dados sobre a revisão da Diretiva Privacidade e Comunicações Eletrónicas (ePrivacy) (2002/58/CE). 14.10.2016. Disponível em: https://edps.europa.eu/sites/edp/files/publication/16-07-22_opinion_eprivacy_en.pdf

Este parecer foi requerido à AEPD em simultâneo com uma consulta publica[8] cujo objetivo seria recolher diferentes perspetivas sobre a efetividade, a eficácia e a coerência das atuais normas da UE e a melhor abordagem para a revisão da Diretiva, lançada pela Comissão no período compreendido entre 12 de abril e 5 julho de 2016, contando com a colaboração de 421 intervenientes[9]. Os resultados desta consulta pública revelaram falta de consenso entre os cidadãos, as autoridades e os representantes da indústria quanto à melhor abordagem para revisão da Diretiva.

De acordo com a iniciativa "Legislar Melhor", a Comissão Europeia levou a cabo um programa de avaliação *ex-post* do desempenho da Diretiva *ePrivacy*, denominado *Regulatory Fitness and Performance Programme, (Refit Evaluation)*[10]. O que resultou desta avaliação foi a confirmação de que os objetivos principais da Diretiva permanecem válidos: **1)** Garantir um nível equivalente de proteção na UE do direito à privacidade e confidencialidade no que respeita ao tratamento de dados pessoais no setor das comunicações eletrónicas, e **2)** assegurar a livre circulação de dados pessoais e de equipamentos e serviços de comunicações eletrónicas na União. Algo que ficou amplamente demonstrado no âmbito da avaliação *REFIT* é que, tanto ao nível das empresas, como ao nível dos consumidores existe um acréscimo significativo de utilização dos serviços *OTT*. Por outro lado, a avaliação demonstra também que, com a entrada em vigor do RGPD, algumas disposições da Diretiva tornaram-se redundantes. É, a título de exemplo, o caso dos requisitos de segurança e do dever de notificação das violações de dados pessoais, que se encontram, atualmente, previstas no RGPD.

A avaliação REFIT também considerou que certas provisões da Diretiva geram ambiguidade, não contribuindo, como seria desejável, para uma harmonização legislativa entre os Estados-Membros, principalmente se tivemos em conta que o que interessa e à indústria é poder operar a um nível transfronteiriço.[11]

8 Synopsis Report of the Public Consultation on The Evaluation And Review of the Eprivacy Directive. 2016. Disponível em: https://ec.europa.eu/digital-single-market/en/news/full-report-public-consultation-eprivacy-directive

9 162 contribuições de cidadãos, 33 de organizações de sociedade civil e de consumidores; 186 da indústria e 40 das autoridades públicas, incluindo as autoridades responsáveis pela aplicação da Diretiva Privacidade e Comunicações Eletrónicas.

10 COMMISSION STAFF WORKING DOCUMENT. Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC. 10.1.2017. Disponível em: file:///C:/Users/drara/Downloads/2-Ex-postREFITevaluationoftheePrivacyDirective200258EC.pdf

11 Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC, pp.62-63.

A proposta de regulamento foi, ainda, alvo de uma Avaliação de Impacto[12], tendo o Comité de Controlo da Regulamentação emitido, a 28 de setembro de 2016, um parecer positivo. Entre as várias opções abordadas na avaliação de impacto, no sentido de garantir uma efetiva confidencialidade das comunicações eletrónicas e uma uniformização/modernização do quadro jurídico da Diretiva, a opção escolhida num total de cinco (tendo em conta as opiniões dos diferentes intervenientes) foi no sentido de reforçar as normas respeitantes à privacidade e à confidencialidade das comunicações, sem, todavia, colocar impedimentos excessivos à industria (seja através da prestação de serviços pelas operadoras de telecomunicações tradicionais, ou dos OTT).

Adicionalmente, a Comissão baseou-se, para elaborar a proposta de um novo Regulamento, em aconselhamento especializado externo[13], nomeadamente:

-Consultas específicas a grupos de peritos da UE: parecer do Grupo de Trabalho do artigo 29.º; o já referido parecer da AEPD; parecer da Plataforma REFIT; pareceres do ORECE; pareceres da ENISA e dos membros da Rede de Cooperação no Domínio da Defesa do Consumidor.

- Estudo "Diretiva Privacidade e Comunicações Eletrónicas: avaliação da transposição, da eficácia e da compatibilidade com a proposta de Regulamento sobre a Proteção de Dados" (SMART 2013/007116).

- Estudo «Avaliação e revisão da Diretiva 2002/58 relativa à privacidade e ao setor das comunicações eletrónicas» (SMART 2016/0080).

No fundo, todos estes todos apontam numa direção: é essencial uma regulação especifica que regule a privacidade e a confidencialidade no setor das comunicações eletrónicas, sendo urgente uma atualização da Diretiva, perante os novos desenvolvimento tecnológicos da industria e o aparecimento de novos produtos e serviços, bem como de novos intervenientes.

[12] COMMISSION STAFF WORKING DOCUMENT. EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT. 10.1.2017. Disponível em: file:///C:/Users/drara/Downloads/7-SummaryoftheImpactAssessment%20(3).pdf

[13] Ver Proposta de Regulamento *ePrivacy*. p.7

1.2– A Diretiva ePrivacy e a Proposta de Regulamento ePrivacy: Principais alterações

1.2.1 – Um regulamento e não uma diretiva

A Comissão decidiu utilizar o instrumento jurídico do regulamento para substituir o atual quadro jurídico em matéria de privacidade nas comunicações eletrónicas, uma vez que é através da figura do regulamento que se garante uma verdadeira uniformização legislativa, sendo que ao contrário do que acontece com as diretivas, os regulamentos são diretamente aplicáveis aos Estados Membros.[14]

A opção por um regulamento vem na senda da escolha da Comissão aquando da substituição da diretiva 95/46/CE pelo atual RGPD. Assim sendo e, tal como explicado no ponto anterior, a Diretiva *ePrivacy* complementava e especificava a diretiva 95/46/CE, o objetivo da criação de um Regulamento *ePrivacy* seria também o de complementaridade face ao RGPD. O Regulamento pretende-se ser coerente com o RGPD, bem como assegurar que existe, tanto para os utilizadores finais, como para a indústria, certeza jurídica, evitando interpretações divergentes quanto às suas normas, apesar de alguma flexibilidade ser desejável. É por este motivo que o art.º 11 da Proposta de Regulamento, comtempla a possibilidade de os Estados Membros restringirem, através de medidas legislativas, o âmbito das obrigações e dos direitos garantidos na proposta, desde que essas medida sejam necessárias, adequadas e proporcionais e sempre que essa restrição não atente contra a essência dos direitos e liberdades fundamentais, com o objetivo de salvaguardar um ou mais dos interesses públicos gerais referidos no art.º 23 do RGPD.[15]

1.2.2– Âmbito de aplicação alargado

Em relação ao conteúdo da proposta, uma das grandes alterações relativamente à anterior Diretiva, tem que ver com o alargamento do âmbito material e territorial das normas *ePrivacy*, que, à luz dos novos intervenientes no mercado e da nova realidade tecnológica, cobrem um espectro muito abrangente de serviços que implicam o

[14] Os regulamentos são atos jurídicos que se aplicam de forma automática e uniforme em todos os países da UE a partir do momento em que entram em vigor, sem terem de ser incorporados no direito nacional. Os regulamentos são vinculativos em todos os seus elementos em todos os países da UE. Disponível em: https://ec.europa.eu/info/law/law-making-process/types-eu-law_pt

[15] É o exemplo da segurança nacional, defesa, segurança pública, prevenção, investigação criminal.

tratamento de dados. No que toca ao âmbito de aplicação material, o art.º 2 da Proposta prevê que a mesma "se destina a ser aplicada sempre que haja tratamento de dados de comunicações efetuado no contexto da prestação e da utilização de serviços de comunicações eletrónicas e às informações relativas ao equipamento terminal dos utilizadores finais." Este artigo é particularmente importante porque concretiza um dos objetivos primordiais desta proposta: estabelecer um quadro normativo equivalente para prestadores de serviços de comunicações tradicionais, mas também para os prestadores de serviços *Over-The-Top* (OTTs), já mencionados no ponto anterior.

Da mesma forma, também o âmbito de aplicação territorial foi alargado, uma vez que o Regulamento passa a abranger todos os serviços de comunicações eletróncias prestados a utilizadores finais na União, independentemente da onerosidade da prestação desses serviços, aplicando-se também a um prestador fora da União, ainda que este não esteja estabelecido na mesma, devendo, nesse caso, nomear um representante.

1.2.3– Conteúdo e metadados

Diferentemente do que sucede com a Diretiva *ePrivacy*, o Regulamento irá aplicar-se tanto ao conteúdo, como aos metadados resultantes de comunicações eletrónicas. Com o avanço e a sofisticação das novas tecnologias relacionadas com as comunicações eletrónicas, os metadados, que são comummente considerados como dados externos às comunicações, são capazes de revelar cada vez mais informação sobre os indivíduos, tais como as suas preferências, os seus hábitos, ou os seus estilos de vida. É de notar que dados de tráfego e de localização configuram tipos de metadados[16] que, no que respeita aos novos tipos de comunicações eletrónicas, podem revelar informação sobre a vida pessoal de cada um de nós, a um nível nunca antes registado. Assim, o art. º6, n. º2 da Proposta de Regulamento *ePrivacy* prevê que os metadados possam ser alvo de tratamento, nomeadamente, para efeitos de prestação de serviços, garantia de segurança das comunicações ou faturação. Na ausência de qualquer outra condição de

[16] O art.º 4, n.º 3, al. c) da Proposta de Regulamento *ePrivacy* define «Metadados das Comunicações Eletrónicas» como sendo: "Os dados tratados numa rede de comunicações eletrónicas para efeitos de transmissão, distribuição ou intercâmbio de conteúdo de comunicações eletrónicas, incluindo os dados utilizados para detetar uma comunicação e identificar a sua fonte e destino, a localização do dispositivo no contexto da comunicação e a data, hora, duração e tipo de comunicação."

licitude prevista no Regulamento, o tratamento de metadados está sujeito ao consentimento, tal como previsto pelo RGPD.

1.2.4 – Novas normas aplicáveis a dispositivos de rastreio (Cookies)

Cada vez mais os equipamentos terminais dos utilizadores finais de serviços de comunicações eletrónicas contêm informações relativas à utilização desses equipamentos, seja através da informação armazenada nos referidos equipamentos, ou quando é solicitado o acesso ao equipamento para permitir a sua ligação a outros dispositivos ou rede, por exemplo, via *Wi-Fi*.

É de notar que os equipamentos terminais permitem o acesso a um número infindável de informação relativa a um determinado individuo, inclusive permitem o acesso ao conteúdo das comunicações armazenadas no equipamento, a listas de contactos, a serviços de localização, de que é exemplo o GPS, permitindo, através das informações referidas, criar um retrato completo relativo à vida pessoal de qualquer pessoa singular.

Além do exposto, temos que ter em atenção que existem dispositivos de rastreio que se introduzem no equipamento terminal do utilizador final sem o seu consentimento, tais como, os programas espiões, os pixéis espiões, os identificadores ocultos, os testemunhos persistentes, com as finalidades de recolha de informação ou de rastreamento de atividades.[17]

A questão dos dispositivos de rastreamento é particularmente grave se considerarmos que existem técnicas de rastreamento à distância, como por exemplo, a recolha da "impressão digital do aparelho".[18] Estas técnicas, além de permitem o rastreamento de atividades e a localização do equipamento, permitem também alterar as suas funcionalidades.

Perante esta nova realidade tecnológica a Proposta de Regulamento *ePrivacy* prevê que a recolha de informação obtida através do equipamento terminal do utilizador final passa a ser permitida sobre condições bastante restritas, previstas no **art.º 8, n.º 1** da Proposta de Regulamento, tais como: se forem necessárias exclusivamente para assegurar a transmissão de uma comunicação eletrónica através de uma rede de comunicações

[17] Ver considerando 20 da Proposta de Regulamento *ePrivacy*.
[18] Idem.

eletrónicas (alínea a), se o utilizador final tiver dado o seu consentimento (alínea b), se forem necessárias para prestar um serviço da sociedade de informação solicitado pelo utilizador (alínea c), ou se forem necessárias para uma medição de audiência da web, desde que tal medição seja efetuada pelo prestador do serviço da sociedade de informação solicitado pelo utilizador final (alínea d).

Também a recolha de informações emitidas pelos equipamentos terminais para permitir a sua ligação a outro dispositivo e/ou equipamento de rede é proibida, salvaguardando-se quando for exclusivamente efetuada para estabelecer uma ligação e durante o tempo necessário para o efeito, ou se for afixado um aviso claro e visível que contenha as informações exigidas ao abrigo do art.º 13 do RGPD. A recolha dessas informações estará subordinada à aplicação de medidas técnicas e organizativas, nos mesmos moldes exigidos pelo art.º 32 do RGPD.

1.2.5 – Definições de Privacidade

Em linha com o RGPD, o consentimento do titular dos dados deverá ser dado através de um ato positivo inequívoco que manifeste o seu acordo livre, específico, informado e explícito. Nesse sentido, o **artigo 9.º** da Proposta prevê a possibilidade de o consentimento poder ser expresso, sempre que for tecnicamente possível e exequível, utilizando as definições técnicas adequadas de uma aplicação de software que permita o acesso à Internet.

Esta questão é particularmente importante no caso dos chamados "testemunhos de conexão", vulgarmente denominados ***Cookies***. Os *Cookies* são pequenos ficheiros de texto que se instalam no equipamento terminal, seja no computador ou no dispositivo móvel, sempre que o utilizador final "navega" por uma página *Web*. Estes ficheiros de texto têm a capacidade de sempre que o utilizador revisite a página armazenar informações acerca das suas ações e preferências. Alguns tipos de *Cookies* têm a faculdade de melhorar a navegação e utilização quando um utilizador acede a uma determinada página Web, não sendo nocivos para a privacidade do utilizador. Falamos, a este propósito, dos Cookies de sessão, que desaparecem após o utilizador fechar a página do navegador *(Browser)*. Por outro lado, os *Cookies* persistentes são utilizados para permitir saber quando um utilizador volta a aceder a um *Website* e não desaparecem após o término da sessão.

Como referido no ponto acima, os *Cookies* têm a capacidade de armazenar um recolher um acervo bastante significativo de dados. Acontece que a os navegadores estão configurados para aceitar os *Cookies* por defeito, enquanto o utilizador navega e fornece informações sobre si.

A grande questão coloca-se com os chamados *"Tracking Cookies"* ou *Cookies* de Publicidade, que podem servir para monitorizar o comportamento de navegação do utilizador, estabelecer perfis, tendo geralmente como objetivo a publicidade endereçada *(marketing)*.

Ora, na prática, a maioria dos *Websites* requerem um consentimento em bloco, não diferenciando os tipos de *Cookies* que não necessitam de consentimento daqueles que necessitam, como é o caso dos *Cookies* de Publicidade. Na prática, ou o utilizador aceita a política de *Cookies* do *Website*, muitas vezes através de um *pop-up*, ou é impedido de aceder aos conteúdos dos mesmos. Este fenómeno designa-se por *Cookie Walls*.

No fundo, a questão em relação aos *Cookies* ou "testemunhos de conexão" resume-se, em grande parte, ao consentimento. É inegável que a esmagadora maioria dos *websites* a que acedemos diariamente nos pede constantemente a aceitação de *Cookies*, criando-se, no utilizador final, uma verdadeira "fadiga de consentimento".

O que a Proposta de Regulamento *ePrivacy* propõe é que o utilizador possa escolher as predefinições de privacidade no navegador que utiliza ou numa aplicação. Tal como indicado no considerando 22 da Proposta: "Os programas de navegação atuam como mediador em muito do que acontece entre o utilizador final e o sítio web." No fundo, é ao próprio utilizador do equipamento terminal, que deverá caber, em última análise, por exemplo, através da escolha de opções de privacidade no seu *browser*, escolher o tipo de acesso ou armazenamento que é gerado a partir do seu equipamento terminal, ou até impedi-lo.

Idealmente, os utilizadores finais deveriam poder escolher entre vários tipos de opções de privacidade, podendo aceitar todos os tipos de *Cookies*, rejeitar todos os tipos de *Cookies*, aceitar apenas os *Cookies* dos websites visitados ou rejeitar os *Cookies* de terceiros.[19]

[19] Ver considerando 23 da Proposta de Regulamento *ePrivacy*.

Esta ideia encontra-se expressa no art.º 10, n.º 1 da Proposta: "O software colocado no mercado que permite efetuar comunicações eletrónicas, incluindo a recuperação e a apresentação de informações da Internet, deve oferecer a possibilidade de impedir que terceiros armazenem informações no equipamento terminal de um utilizador final ou tratem as informações já armazenadas nesse equipamento." Adicionalmente, o software terá de informar o utilizador acerca das opções privacidade, não concluindo a sua instalação, enquanto o utilizador final não der o seu consentimento em relação a uma dessas opções.[20]

No fundo, o consentimento aplicável deverá traduzir-se, em linha do já previsto pelo RGPD[21], num ato positivo inequívoco que manifeste um acordo livre, específico, informado e explicito em relação ao acesso e armazenamento dos testemunhos de conexão no e partir dos equipamentos dos utilizadores finais.

A *"ratio legis*" presente nesta norma, tal como explicitado no considerando 24 da Proposta, é de conferir a opção de o utilizador predefinir, inclusive, a opção de privacidade mais elevada, indicando os riscos inerente à permissão dos testemunhos de conexão, principalmente no que toca aos testemunhos de conexão de terceiros, no seu equipamento terminal[22]. O utilizador deve poder ainda, a qualquer momento, alterar as definições de privacidade no navegador[23].

1.2.6– Comunicações não solicitadas

Para aumentar a proteção contra comunicações não solicitadas (*spam*) o princípio é o de que o envio de comunicações que se destinem a *marketing* direto só são permitidas a pessoas singulares que tenham dado o seu consentimento (*opt-in*).[24]

[20] Ver art.º 10, n. º2 da Proposta de Regulamento ePrivacy.
[21] Ver art.º 4, n.º 11 do RGPD e art.º 7.º.
[22] O considerando 24 da Proposta prevê acerca desta matéria: "As informações prestadas não devem dissuadir os utilizadores finais de selecionar as predefinições de privacidade mais elevadas e devem incluir informações sobre os riscos associados à permissão do armazenamento de testemunhos de conexão de terceiros no computador, incluindo a compilação a longo prazo de registos do histórico de navegação das pessoas singulares e a utilização desses registos para enviar publicidade orientada."
[23] BORGESIUS, Zuiderveen et, al. *Tracking Walls, Take-It-Or-Leave-It Choices, and the ePrivacy Regulation,* March 15, 2018, European Data Protection Law Review, Volume 3, Issue 3, pp. 353-368.
[24] Ver art.º 16, n. º1 da Proposta de Regulamento *ePrivacy*.

Existe, todavia, uma exceção: se existir uma relação prévia entre cliente e fornecedor, é permitido o envio de comunicações com oferta de produtos ou serviços de cariz semelhante. Adicionalmente, os utilizadores finais devem poder, a qualquer momento, retirar o seu consentimento à receção de comunicação não solicitadas de marketing direto (opt-out).[25] Deverão poder fazê-lo através de uma ligação, ou endereço de correio eletrónico, disponibilizado pelo fornecedor de produtos e/ou serviços e que seja facilmente acedível pelo utilizador final.

Ainda, em relação ao marketing direto realizado através de chamadas vocais (*voice-to-voice calls*), ou por qualquer outro meio de comunicação automatizado, as pessoas singulares ou coletivas devem identificar uma linha para a qual possam ser contactas, ou apresentar um código específico que indique que se trata de uma chamada com intuito comercial.[26]

Por fim, em relação a chamadas vocais de marketing direto, os Estados-Membros devem prever, na sua legislação interna, que a sua receção pelos utilizadores finais que sejam pessoas singulares só poderá ocorrer caso estes não tenham expressado a sua objeção.[27]

1.2.7 - Aplicação coerente ao nível da União e sanções previstas

O objetivo da Proposta de Regulamento *ePrivacy* é aplicar-se de forma uniforme a todos os Estados-Membros da União, contrariamente ao que se sucede com a atual Diretiva, daí a escolha óbvia, no que ao instrumento legislativo diz respeito, com a adoção de um regulamento e não de uma diretiva.[28]

Adicionalmente, a Comissão deseja atingir uma maior coerência na aplicação das normas relativas ao *ePrivacy*, atribuindo a execução das disposições presentes no Regulamento às mesmas autoridades responsáveis pela execução das normas do RGPD[29]. Aplica-se também ao Regulamento *ePrivacy*, o mesmo procedimento de controlo de coerência previsto no RGPD.[30]

[25] Cfr. Art.º 16, n. º2.
[26] Cfr. Art.º 16, n. º3, alíneas a) e b).
[27] Cfr. Art.º 16, n.º 4.
[28] A este propósito ver o subcapítulo 1.2.1 da presente dissertação.
[29] Cfr. Art.º18 da Proposta.
[30] Cfr. Art.º 20 da Proposta.

Até agora, a autoridade responsável pela execução das normas relativas à *ePrivacy* podem diferir de Estado-Membro para Estado-Membro, cabendo, em alguns casos, à autoridade competente para a proteção de dados, e noutros, ao regulador do setor das comunicações.[31]

Ao nível das sanções pelo incumprimento previsto numa norma do Regulamento *ePrivacy*, as mesmas poderão atingir até 4% do volume de negócio anual, a nível mundial, à semelhança das coimas existentes por incumprimento das disposições previstas no RGPD.

Capítulo 2: A interação entre o Regulamento Geral de Proteção de Dados e o Futuro Regulamento *ePrivacy*

2.1 – Porquê um Regulamento ePrivacy, quando já existe um RGPD?

Não era claro que com entrada em vigor do novo RGPD[32] houvesse necessidade de regras especiais para o setor das comunicações eletrónicas em matéria de confidencialidade das comunicações eletrónicas.[33]

Contudo, o Direito da União, de acordo com o artigo 7.º da Carta dos Direitos Fundamentais da União Europeia, prevê que "todas as pessoas têm direito ao respeito pela sua privada, pelo seu domicílio e pelas comunicações." Além disso, a confidencialidade e a privacidade das comunicações têm de ser protegidas, mesmo não estando em causa dados pessoais.

Assim, o RGPD, que apenas estabelece normas relativas aos dados pessoais, não é suficiente para assegurar a confidencialidade das comunicações. A "Carta" prevê o direito à proteção de dados pessoais, no Artigo 8.º, estabelecendo que "Todas as pessoas têm direito à proteção dos dados de caracter pessoal que lhes digam respeito." O RGPD

[31] No caso português, a Lei n.º46/2012, de 29 de agosto que transpõe para ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, já prevê uma competência bipartida entre a CNPD e a ANACOM. Ver artigo 13.º-D.

[32] Ver Voss, W. Gregor, First the GDPR, *Now the Proposed ePrivacy Regulation (July 25, 2017)*. *Journal of Internet Law,* Vol. 21, No. 1, pp. 3-11 (July 2017).

[33] Por exemplo, 63,4% dos inquiridos na Consulta Publica, levada a cabo pela Comissão, entre 12 de abril a 5 de julho de 2016, não concordaram com a necessidade de regras especiais para o setor das comunicações eletrónicas em matéria de confidencialidade das comunicações eletrónicas. Ver "Exposição de Motivos" da Proposta de ePrivacy, p.6, secção 3.2.

não pretende proteger o direito à confidencialidade das comunicações, nem o direito à privacidade em geral.[34] Como mencionado na Avaliação de Impacto à Proposta de Regulamento *ePrivacy*: "As normas relativas a dados pessoais, não protegem, em regra, a confidencialidade da informação respeitante às pessoas coletivas, como por exemplo, segredos comerciais.".[35]

Por exemplo, as empresas podem enviar emails entre si, cujo conteúdo diz respeito a informações confidenciais, como segredos comerciais, dados contabilísticos, uma instrução para a adquirir ações numa determinada bolsa de valores. As empresas são pessoas coletivas (não protegidas pelo RGPD[36]) e nem sempre as suas comunicações estão relacionadas com dados pessoais. A título de exemplo: "Suponhamos que a info@large-company.com envia um email com segredos comerciais (sem que esse email contenha dados pessoais) à info@big-company.com. Neste cenário hipotético, o RGPD não se aplicaria. Contudo, muitas empresas desejam que as suas comunicações permaneçam confidenciais".[37]

Em relação ao âmbito de aplicação do art.º 7 da Carta, tanto a jurisprudência do Tribunal de Justiça da União Europeia (TJUE)[38], como do Tribunal Europeu dos Direitos do Homem (TEDH)[39] confirmam que as atividades profissionais das pessoas coletivas não podem ser excluídas da proteção dos direitos garantidos pelo art.º7 da Carta e pelo art.º8 da Convenção Europeia dos Direitos do Homem (CEDH)[40].

Outra razão pela qual faz sentido a existência de normas separadas relativas à *ePrivacy* prende-se com a concretização do mercado interno. O objetivo da proposta é uniformizar as normas relativas ao direito à privacidade e à confidencialidade das

[34] Ver BUTARELLI, Giovanni, : *The Commission Proposal for a Regulation on ePrivacy: Why Do We Need a Regulation Dedicated to ePrivacy in the European Union?* European Data Protection Law Review, Volume 3 (2017) p.156.
[35] Avaliação de Impacto da Proposta de Regulamento ePrivacy, 2017, parte 1, p.8. Disponível em: file:///C:/Users/drara/Downloads/4-ImpactAssessment-part1%20(1).pdf
[36] Considerando 14 do RGPD.
[37] BORGESIUS, Zuiderveen *et al.*, *An Acessement of the Comission´s Proposal on Privacy and Eletronic Communications*, Directorate-General for International Policies, Policy Department C: Citizen´s Rights and Constitucional Affairs, June 7, 2017, p.20. ISBN: 978-92-846-1101-0.
[38] Ver Processo C- 450/06 *Varec SA*, ECLI:EU: C: 2008:91, ponto 48.
[39] Ver, por exemplo, acórdão *Niemietz/Alemanha*, de 16 de dezembro de 1992, Série A, n.º 251-B, ponto 29.
[40] Ver Zuiderveen Borgesius, Frederik and Steenbruggen, Wilfred, *The Right to Communications Confidentiality in Europe: Protecting Trust, Privacy, and Freedom of Expression* (August 31, 2018). Theoretical Inquiries in Law, Forthcoming.

comunicações eletrónicas de forma a contribuir para a concretização do Mercado Único Digital.[41] Se, ao nível da União não forem criadas normas que regulem o direito à privacidade e à confidencialidade no setor das comunicações eletrónicas, existe uma grande probabilidade de os próprios Estados-Membros legislarem, ao nível interno, sobre essa matéria, criando uma fragmentação legislativa ao nível da União, que em nada contribuirá para a implementação do MUD, criando uma situação em tudo semelhante à que existe atualmente com a Diretiva.[42]

Adicionalmente, normas separadas de *ePrivacy* contribuem para uma maior certeza jurídica. O RGPD contém várias normas que necessitam de uma concretização específica, uma vez que foi pensado com o intuito de ser um regime geral, tendo um âmbito de aplicação extenso, que regula diferentes matérias. Assim, as normas previstas no RGPD são demasiado vagas para o tipo de dados e de matérias que o *ePrivacy* pretende regular.

Tal como no exemplo acima demonstrado, a Proposta de Regulamento aplica-se ao conteúdo das comunicações e aos dados armazenados nos nossos equipamentos telefónicos. Uma vez que estes podem revelar um acervo de informação com um elevado grau de sensibilidade sobre um determinado individuo, as normas previstas no RGPD, não são, *per se*, suficientes.

Ainda, a Proposta de Regulamento *ePrivacy* regula, à semelhança do que acontece com a presente Diretiva, situações que apenas dizem respeito ao setor das comunicações eletrónicas e que não se encontram previstas no RGPD. O RGPD só protege parcialmente os equipamentos terminais dos utilizadores finais[43], o mesmo ocorrendo contra comunicações não solicitadas.[44]

Ademais, a necessidade de normas relativas à *ePrivacy* tornou-se inquestionável, na sequência da Consulta Pública levada a cabo pela Comissão[45], conclui-se quanto "[…] à necessidade de regras especiais para o setor das comunicações em matéria de confidencialidade das comunicações eletrónicas: 83,4% dos cidadãos, consumidores, e

[41] Ver subcapítulo 1.1 da presente dissertação de mestrado.
[42] Ver Opinião 5/2016 da AEPD, p.7.
[43] Ver o Art.º 8 da Proposta de Regulamento *ePrivacy*. O RGPD aplica-se aos dados pessoais que se encontrem armazenados nos equipamentos terminais dos utilizadores finais e, nesse caso, poderá ser aplicável.
[44] Ver o Art.º 16 da Proposta de Regulamento *ePrivacy*.
[45] Ver ponto 1.1 da presente dissertação de mestrado.

organizações da sociedade civil e 88,9% das autoridades públicas que responderam concordam, ao passo que 63,4 % dos inquiridos da indústria não concordam."[46] Logo, a conclusão é a de que regras específicas que assegurem a confidencialidade no setor das comunicações eletrónicas são essências, em complemento do RGPD.

2.2 – A interação entre a atual Diretiva ePrivacy e o RGPD

A 12 de março de 2019, o Comité Europeu para a Proteção de Dados ("CEPD") adotou uma opinião, no sentido de clarificar a relação entre a Diretiva *ePrivacy* e o RGPD. Em resposta a um pedido da Autoridade para Proteção de Dados Belga, o CEPD deu o seu parecer em relação às seguintes questões:[47]

- Se as competências, atribuições e poderes das autoridades para a proteção de dados conferidos pelo RGPD estão limitados quando o tratamento de dados pessoais cai no âmbito de aplicação do RGPD e da Diretiva *ePrivacy*.
- Se as autoridades para a proteção de dados devem ter em consideração as previsões da Diretiva *ePrivacy* ao exercerem as suas competências, atribuições e poderes conferidos pelo RGPD, ao depararem-se com possíveis incumprimentos de normas nacionais que implementem a Diretiva *ePrivacy*.
- Se os mecanismos de cooperação e coerência, plasmados no RGPD, se aplicam ao tratamento de matérias que caiam, simultaneamente, no âmbito de aplicação do RGPD e da Diretiva *ePrivacy*.

Na referida Opinião, o CEPD, indica de forma clara, que o facto de uma parte do tratamento cair no âmbito de aplicação material da Diretiva *ePrivacy* não limita as competências das autoridades para a proteção de dados no âmbito do RGPD; que uma violação de uma norma prevista no RGPD pode, simultaneamente, constituir uma violação de normas nacionais da Diretiva *ePrivacy*, e que as autoridades para a proteção de dados podem ter estes fatores em consideração, ao aplicarem o RGPD, por exemplo, ao avaliarem a conformidade com os princípios da licitude e da lealdade.

[46] Ver Exposição de Motivos da Proposta de Regulamento *ePrivacy*, ponto 3.2, p.6.
[47] Ver Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks, and powers of data protection authorities, European Data Protection Board, Adopted on 12 March 2019, p. 4.

Em princípio, o âmbito de aplicação material do RGPD é extensível a qualquer tratamento de dados pessoais, independentemente da tecnologia utilizada. De acordo com o artigo 3.º da Diretiva *ePrivacy*: "A presente diretiva é aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas publicamente disponíveis nas redes públicas de comunicações da Comunidade."

Existem vários exemplos de atividades de tratamento que despoletam o âmbito de aplicação material tanto do RGPD, como da Diretiva *ePrivacy*. Um exemplo óbvio relaciona-se com o tema já abordado dos testemunhos de conexão ou *Cookies.* O Grupo de Trabalho do Artigo 29.º (GT29), antecessor do CEPD, clarificou esta questão no seu Parecer 2/2010 sobre publicidade comportamental em linha indicando que: "Se as informações recolhidas através da instalação do testemunho ou de um dispositivo análogo forem consideradas dados pessoais, é também aplicável, para além do artigo 5.º, n.º 3, a Diretiva 95/46/CE.[48]"

Recentemente, na apreciação do caso *Fashion ID*, do Tribunal de Justiça da União Europeia, o Advogado-Geral Michal Bobek, nas suas conclusões[49], refere o seguinte: "Concordo com a Comissão em relação ao facto de que a Diretiva Privacidade e Comunicações Eletrónicas (que, nos termos do seu artigo 1.º, n.º 2, precisa e complementa a Diretiva 95/46 no setor das comunicações eletrónicas) se afigura aplicável ao caso em apreço, na medida em que foram colocados *cookies* nos dispositivos dos utilizadores. Além disso, o artigo 2.º, alínea f), e o considerando 17 da Diretiva Privacidade e Comunicações Eletrónicas definem o consentimento tendo por referência o conceito de consentimento que consta da Diretiva 95/46." Podemos daqui depreender qua quando estamos perante *cookies* ou *social plug-ins*, tanto as normas decorrentes da Diretiva *ePrivacy*, como as normas previstas no RGPD poderão ser simultaneamente aplicáveis.

Adicionalmente, o considerando 30 do RGPD, indica que identificadores como o endereço de IP (protoloco Internet) e os *cookies "*[…] podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas

[48] Parecer 2/2010 sobre publicidade comportamental em linha, Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, Adotado em 22 de junho de 2010, p.10.
[49] Conclusões do Advogado Geral MICHAEL BOBEK *in Fashion ID*, C-40/17, ECLI:EU:C:2018:1039, para.114.

pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares."

Além disso, tal como explicado na Opinião, o próprio RGPD refere-se especificamente, ao clarificar o seu âmbito de aplicação material, a atividades de tratamento que também caiem, pelo menos parcialmente, no âmbito de aplicação material da Diretiva *ePrivacy*.[50]

Dados de tráfego e de localização gerados por serviços de comunicações eletrónicas poderão envolver tratamento de dados pessoais, na medida em que em que estejam relacionados com pessoas singulares.[51]

O artigo 1.º, n. º2 da Diretiva *ePrivacy* prevê expressamente que: "Para os efeitos do n.º 1, as disposições da presente diretiva especificam e complementam a Diretiva 95/46/CE." No sentido de clarificar o significado de "complementaridade", o CEPD, refere-se ao artigo 5, n. º3 da Diretiva *ePrivacy,* relativo ao consentimento de *Cookies*. O artigo 5, n.º3, prevê que, salvo algumas exceções […]"a utilização de redes de comunicações eletrónicas para a armazenagem de informações ou para obter acesso à informação armazenada no equipamento terminal de um assinante ou utilizador só seja permitida na condição de serem fornecidas ao assinante ou ao utilizador em causa informações claras e completas, nomeadamente sobre os objetivos do processamento, em conformidade com a Diretiva 95/46/CE, e de lhe ter sido dado, pelo controlador dos dados, o direito de recusar esse processamento.[52]" Como é explicado pelo CEPD, na medida em que a informação armazenada num equipamento terminal de um utilizador final, constituir dados pessoais, o artigo 5, n.º3, da Diretiva *ePrivacy* "deverá ter precedência" sobre o artigo 6.º do RGPD em relação à atividade de armazenamento ou obtenção de acesso a essa informação, mas apenas na medida em que a norma especial do artigo 5, n.º 3, seja aplicável.

O CEPD dá o seguinte exemplo:

"Um corretor de dados pessoais ("data broker") dedica-se à perfilagem, baseando-se na informação contida no histórico de navegação dos indivíduos, recolhida com recurso

[50] Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks, and powers of data protection authorities, European Data Protection Board, Adopted on 12 March 2019, para. 33.
[51] Ibidem, para. 34.
[52] Ibidem, para. 40.

a *cookies*, mas que também pode conter informação recolhida através de outras fontes (por exemplo, "parceiros comerciais"). Neste caso, uma parte desse tratamento, nomeadamente a colocação ou a leitura dos *cookies*, deverão estar em conformidade com a norma nacional de transposição do artigo 5.º, n.º 3 da Diretiva *ePrivacy*. O tratamento subsequente de dados pessoais, incluindo os dados obtidos através de *cookies*, deve assentar numa das bases de licitude do artigo 6.º do RGPD, de forma a que seja lícito."[53]

Por outras palavras, quando existam normas especificas que regulem uma determinada operação de tratamento ou várias operações, essas normas especificas deverão aplicar-se *("lex specialis")*, em todos os restantes casos, a normas gerais aplicam-se ("*lex generalis*"). Um fornecedor de uma rede pública de comunicações ou de um serviço de comunicações eletrónicas publicamente disponíveis deverá, por exemplo, atuar em conformidade com as normas nacionais de transposição do artigo 6.º, número 2, da *Diretiva ePrivacy*, relativo ao tratamento de dados de tráfego necessários para efeitos de faturação dos assinantes e de pagamento de interligações. Todavia, devido à falta de normas especificas na Diretiva em relação ao direito de acesso, por exemplo, as normas previstas no RGPD também serão aplicáveis.

O CEPD também aborda especificamente o artigo 95.º do RGPD, que estabelece: "O presente regulamento não impõe obrigações suplementares a pessoas singulares ou coletivas no que respeita ao tratamento no contexto da prestação de serviços de comunicações eletrónicas disponíveis nas redes públicas de comunicações na União em matérias que estejam sujeitas a obrigações específicas com o mesmo objetivo estabelecidas na Diretiva 2002/58/CE."

Como explicado pelo CEPD, o objetivo do artigo 95.º do RGPD é "evitar a imposição de ônus administrativos desnecessários sobre os responsáveis pelo tratamento, que, de outra forma, estariam sujeitos a ônus administrativos semelhantes, mas não totalmente idênticos."[54] A título de exemplo: os prestadores de serviços de comunicações eletrónicas que notificarem uma violação de dados pessoais ao abrigo das normas nacionais de transposição da Diretiva *ePrivacy*, não estão obrigados a notificar, separadamente, as autoridades de proteção de dados, dessa mesma violação, como exigido pelo artigo 33.º do RGPD.

[53] Ibidem, para. 41.
[54] Ibidem, para. 44.

As autoridades de proteção de dados não podem, de forma automática, basear-se nos poderes que lhes são conferidos pelo RGPD para aplicarem as normas presentes na Diretiva *ePrivacy*. Na eventualidade de o tratamento desencadear, simultaneamente, o âmbito de aplicação material do RGPD e da Diretiva, as autoridades de proteção de dados só poderão aplicar as normas presentes na Diretiva no caso de a legislação nacional lhes atribuir especificamente essa competência. Contudo, como esclarecido pelo CEPD[55], o mero facto de um subconjunto do tratamento recair sobre o âmbito de aplicação material da Diretiva *ePrivacy* não limita a competência das autoridades de proteção de dados atribuída pelo RGPD. Isto significa que permanecem totalmente competentes relativamente a qualquer tratamento que envolva dados pessoais que não esteja sujeito a normas especificas previstas na Diretiva *ePrivacy*. Adicionalmente, quando um incumprimento do RGPD constitua, ao mesmo tempo, um incumprimento da Diretiva, a APD poderá levar esse aspeto em consideração na aplicação do RGPD, por exemplo, ao avaliar a conformidade com os princípios da licitude e da lealdade, de acordo com o artigo 5.º, n. º1, alínea a) do RGPD[56].

Por último, o CEPD confirma que os mecanismos de cooperação e coerência disponibilizados às APD no RGPD, referindo-se, a esse respeito, ao controlo da aplicação das normas previstas no RGPD, não se aplicam à execução das normas nacionais que implementam a Diretiva *ePrivacy*. No entanto, os mecanismos de cooperação e coerência permanecem totalmente aplicáveis, na medida em que o tratamento esteja sujeito a normas gerais previstas no RGPD (e não a uma "norma especial" prevista na Diretiva *ePrivacy)*.[57]

De ressalvar que a Opinião do CEPD não aborda a Proposta de Regulamento *ePrivacy*. Adicionalmente, o CEPD emitiu uma declaração no dia posterior, pedindo aos legisladores da UE para que "intensifiquem os seus esforços com vista à adoção de um regulamento relativo à privacidade e às comunicações eletrónicas, necessário para completar o quadro da UE relativo à proteção de dados e à confidencialidade das comunicações". Esta declaração reitera posições previamente adotadas pelo GT29 e pelo CEPD no sentido em que a Proposta de Regulamento *ePrivacy* "não deve, em circunstância alguma, reduzir o nível de proteção concedido pela atual Diretiva

[55] Ibidem, para. 69.
[56] Ibidem, para. 76.
[57] Ibidem, para. 80 e 84.

2002/58/CE relativa à privacidade e às comunicações eletrónicas e deve complementar o Regulamento Geral sobre a Proteção de Dados, fornecendo garantias adicionais sólidas para todos os tipos de comunicações eletrónicas."[58]

Capítulo 3: O artigo 6.º: necessário para a proteção da privacidade ou um impedimento ao desenvolvimento tecnológico?

3.1 – O artigo 6.º: divergências entre as operadoras de telecomunicações e as instituições europeias

O artigo 5.º da Proposta de Regulamento *ePrivacy* estabelece a regra geral que prevê que os dados das comunicações eletrónicas devem ser confidenciais. A importância do artigo 5.º prende-se com o facto de este prever uma proibição geral de qualquer interferência com os dados das comunicações eletrónicas, exceto quando o Regulamento o permitir. As derrogações a este princípio geral estão, em larga medida, presentes nos artigos 6.º e 7.º da Proposta.

O artigo 6.º da Proposta de Regulamento *ePrivacy* tem sido, desde o início, um dos grandes responsáveis pelo facto de que quase quatro anos volvidos da apresentação da proposta de Regulamento, pela Comissão Europeia, ainda não ter sido possível definir uma versão final do mesmo para aprovação.

O artigo 6.º estabelece uma proibição geral respeitante ao tratamento de dados pessoais de comunicações eletrónicas, exceto quando esse tratamento recai sobre uma das suas bases de licitude, variando entre o conteúdo das comunicações eletrónicas e os metadados resultantes das mesmas.

Na proposta original da Comissão Europeia, essas exceções, dependendo do tipo de dados objeto do tratamento, estavam essencialmente relacionadas com:

1 - A transmissão das comunicações (artigo 6, (1) (a));

2- Manter ou restabelecer a segurança das redes e serviços de comunicações eletrónicas (artigo 6 (1) (b));

[58] Declaração 3/2019 sobre um regulamento relativo à privacidade e às comunicações eletrónicas, Comité Europeu para a Proteção de Dados, adotada em 13 de março de 2019.

3- Cumprir as obrigações em matéria de qualidade do serviço previstas na [Diretiva que estabelece o Código Europeu das Comunicações Eletrónicas] ou no Regulamento (UE) 2015/212011 (artigo 6 (2) (a));

4 - Para proceder à faturação, calcular o pagamento das interligações, detetar ou impedir a utilização abusiva ou fraudulenta de serviços de comunicações eletrónicas ou a subscrição desses serviços (artigo 6 (2) b));

Isto significa que, à exceção das condições de licitude para o tratamento de dados de comunicações eletrónicas acima referidas, apenas é permitido aos prestadores de serviços de comunicações eletrónicas o tratamento desses dados mediante consentimento do utilizador final.

Neste sentido, o Grupo de Trabalho do Artigo 29.º[59], no seu parecer sobre a Proposta de Regulamento *ePrivacy* sugere que se deva adotar uma abordagem ainda mais restritiva quanto à aplicação do critério da necessidade relativamente às exceções previstas no artigo 6.º do Regulamento, vejamos: "O grupo de trabalho sugere, por conseguinte, que, no que diz respeito a todas as exceções previstas nos artigos 6.º e 8.º, n.º 1, da proposta de regulamento, o termo «estritamente» deva ser aditado antes de «necessário/necessárias»."

No mesmo Parecer, o GT29 prevê ainda que: "O regulamento relativo à privacidade e às comunicações eletrónicas deve garantir exceções aos requisitos de consentimento redigidas de forma precisa e estrita."[60]

Também a AEPD concorda que o Artigo 6.º deveria conter a expressão "estritamente necessário" e não apenas "necessário".[61]

Por outro lado, as principais associações de telecomunicações, tais como a ETNO, a GSMA ou a CABLE EUROPE[62] consideram que o artigo 6.º constitui um verdadeiro impedimento ao desenvolvimento tecnológico do setor, uma vez que, como já

[59] Parecer 1/2017 sobre a proposta de regulamento relativo à privacidade e às comunicações eletrónicas (2002/58/CE), Grupo de Trabalho sobre a Proteção de Dados do Artigo 29.º, Adotado em 4 de abril de 2017, para. 26. Ver também, a este propósito, o para. 18.
[60] Ibidem.
[61] Opinion 6/2017, EDPS on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), European Data Protection Supervisor, 24 April 2017.
[62] Ver ETNO's views on the Proposal for an ePrivacy Regulation, março de 2017, RD440 (2017/03).

mencionado, além de estabelecer uma proibição geral no que toca do tratamento de dados de comunicações eletrónicas, as bases de licitude, além do consentimento do utilizador final, que aí se encontram previstas, excluem inúmeros fundamentos que poderiam servir de base a esse tratamento, com um impacto mínimo ou nulo na privacidade dos utilizadores finais.

Senão, vejamos os seguintes exemplos:

Exemplo 1

- Tratamento de dados de comunicações eletrónicas para cumprimento de obrigações legais (como por exemplo, obrigações de conservação de dados impostas pela legislação nacional ou interceções lícitas de comunicações eletrónicas) não está explicitamente abrangido pelo artigo 6.º. Enquanto que o artigo 11.º prevê que o direito da União ou o direito dos Estados-Membros possam restringir, através de medidas legislativas, o âmbito das obrigações e dos direitos previstos nos artigos 5.º a 8.º, ainda assim, deveria ser incluída uma referencia expressa no artigo 6.º em relação ao "cumprimento de uma obrigação legal"[63].

Exemplo 2

- A prestação de serviços de emergência para a proteção de interesses vitais.[64]

Exemplo 3

- A utilização de dados de comunicações eletrónicas para a gestão e melhoramento/implementação das redes de comunicações eletrónicas, que não se encontra especificamente prevista no artigo 6.º.[65]

Tal como apontado pelo parecer da ETNO relativo à Proposta de Regulamento *ePrivacy*: na prática, os engenheiros de telecomunicações devem poder monitorizar metadados (por exemplo, para medir a utilização ou capacidade por equipamento móvel ou os hábitos de uso numa certa área coberta por rede fixa) e, em certa medida, o mesmo se aplica também ao conteúdo das comunicações (por exemplo, para medir que tipo de aplicações têm impacto na produtividade) para que seja possível gerir o tráfego de forma eficiente e tomar decisões racionais respeitantes a investimento e implementação.

[63] Ibidem, p.3.
[64] Ibidem, p.4.
[65] Ibidem, p.4.

Enquanto que a pseudonimização dos dados analisados pode ser possível, a monitorização ou o planeamento das redes não pode ser feita com dados anonimizados. Informações do usuário ou de localização são precisamente o tipo de dados que são essenciais para esses propósitos.[66]

Exemplo 4

O artigo 6.º não permite especificamente o uso de dados de comunicações eletrónicas para o desenvolvimento de produtos e serviços.[67]

De forma a desenvolverem de forma eficiente produtos e serviços que correspondam às necessidades dos clientes os operadores de telecomunicações utilizam dados agregados baseando-se, por exemplo, no uso de metadados (percentagem de roaming, divida em várias localizações, percentagem de chamadas para números móveis ou fixos, ou desenvolvimento da utilização de dados móveis).

Exemplo 5[68]

O artigo 6.º não permite a utilização de metadados para efeitos de marketing direto ou para efeitos de apoio ao cliente.

O que significa que as operadoras de telecomunicações não poderão, sem o consentimento explicito do utilizador final, propor um tarifário mais adequado a um cliente cujos metadados demonstrem que o seu tarifário não está adaptado ao serviço que o cliente efetivamente utiliza, por exemplo, quando utiliza a maioria do seu tráfego no estrangeiro.

Exemplo 6[69]

O artigo 6.º confere extrema importância à anonimização e os considerandos (nomeadamente o considerando 17[70]) da Proposta recomendam a adoção de uma posição bastante restrita relativa à anonimização. Uma posição de tal forma restritiva que irá impossibilitar que as operadoras de telecomunicações façam análises de localização com interesse e valor para a sociedade que digam respeito a grandes períodos, beneficiando, por exemplo, setores como o turismo ou a mobilidade. De ressalvar, todavia, que essas

[66] Ibidem, p.4.
[67] Ibidem, p.4.
[68] Ibidem, p.4.
[69] Ibidem, pp. 4-5.

análises de localização poderão continuar a ser feitas por criadores de aplicações que tratam de dados de localização com um nível de precisão que é, frequentemente, mais detalhado do que os dados de localização recolhidos através de uma rede de comunicações eletrónicas.

A meu ver, todos estes exemplos práticos[71] em que é necessário o tratamento de dados de comunicações eletrónicas, quer ao nível dos conteúdos, quer ao nível dos metadados, são bastante exemplificativos de que o artigo 6.º da Proposta, exclui, à partida, vários tipos de tratamento que, além de serem essenciais para que as operadoras possam, de uma forma bem sucedida, prestar os seus serviços aos seus clientes, são também necessários ao desenvolvimento da tecnologia inerente ao setor das telecomunicações, de forma a estimular a competição e a diversificação de ofertas entre os vários operadores que atuam no mercado europeu.

3.2 – As alterações do Parlamento Europeu à Proposta na redação original da Comissão do artigo 6.º

Como referido no ponto anterior, o art.º6, n.º1, permitia o tratamento de dados de comunicações eletrónicas, essencialmente, para dois pressupostos: i) Se tal fosse necessário para assegurar a transmissão da comunicação; ii) Se tal fosse necessário para manter ou restabelecer a segurança das redes e serviços de comunicações eletrónicas, ou detetar falhas técnicas e/ou erros na transmissão das comunicações eletrónicas. Neste último caso, o PE introduziu a possibilidade de os dados poderem ser tratados pelos fornecedores de serviços de comunicações eletrónicas ou por terceiros que atuem por conta destes. Poderá ser o caso, de uma operadora de telecomunicações ou de um prestador de serviços OTT que subcontratem uma empresa externa de segurança de forma a assegurar que a transmissão da comunicação é feita sem falhas técnicas ou erros.[72]

Adicionalmente, e na senda das opiniões emitidas pela AEPD e pelo GT29, o PE estabeleceu um limite ainda mais restrito para o tratamento de dados de comunicações

[71] Ver a este propósito alguns casos práticos apresentados pela ETNO e pela GSMA no documento: The Proposed European ePrivacy Regulation, Use Cases for enabling privacy-protection inovative products and services, April 2018. Disponível em: https://www.gsma.com/gsmaeurope/wp-content/uploads/2018/04/GSMA-ETNO-ePR-Use-Cases-April-2018.pdf

[72] Elena Gil González et. al, *The Proposed ePrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads? In* Brussels Privacy Hub, Working Paper Vol.6, n. º20 (March 2020), P. 12.

eletrónicas, alterando a redação original da CE, substituindo a expressão "necessário" por "tecnicamente necessário".

Em relação ao artigo 6.º, n. º2, relativo ao tratamento de metadados, o PE, substituiu novamente a expressão "necessário", que constava na redação original da Proposta da CE, por "estritamente necessário". As situações em que o tratamento de metadados é permitido são as seguintes: Primeiramente, para efeitos de faturação[73], por exemplo para assegurar que alguém que beneficie dos serviços não envie, de forma fraudulenta, a fatura a outrem, bem como para prevenir o uso e a subscrição abusivos de serviços de comunicações eletrónicas.[74] Neste último caso, apenas serão conservados os metadados estritamente necessários e pelo período correspondente ao qual uma faturação ou um pagamento indevido possam ser legalmente contestados, ou quando forem tecnicamente necessários pelos motivos de segurança acima descritos.[75]

Em segundo lugar, os metadados poderão ser tratados quando for necessário para cumprir as obrigações em matéria de qualidade do serviço, de acordo com legislação especifica.[76] Um exemplo seria uma situação em que o prestador necessita de adaptar a qualidade de uma imagem às definições do ecrã.[77] Em terceiro lugar, os metadados apenas poderão ser utilizados com o consentimento do utilizador para a prestação de finalidades ou serviços específicos, desde que esses serviços não possam ser prestados sem o tratamento desses metadados. Por exemplo, um serviço em que é mostrado ao utilizador os pontos de abastecimento mais económicos na área onde se encontra, através do rastreamento da sua localização.[78] A este respeito, as emendas do Parlamento à Proposta da Comissão, tentam limitar, ainda mais, o recurso ao consentimento como exceção, permitindo apenas o consentimento dos utilizadores (i.e de pessoas singulares) e não de todos os utilizadores finais (exclui-se o consentimento relativo às pessoas coletivas) e pela obrigação de conduzir uma avalização de impacto e de notificar previamente a autoridade de controlo sempre que o tratamento implique um risco elevado para os titulares dos dados, tal como previsto nos artigos 35.º e 36.º do RGPD. Nestes dois últimos

[73] Art. 6.2.b) do Regulamento ePrivacy, tal como reformulado pela Proposta doParlamento Europeu.
[74] Ibidem, p.13.
[75] Art. 7.3 do Regulamento ePrivacy, tal como reformulado pela Proposta do Parlamento Europeu.
[76] Art. 6.2.a) do Regulamento ePrivacy, tal como reformulado pela Proposta do Parlamento Europeu.
[77] Ibidem, p.13.
[78] Ibidem. p.13.

casos (cumprir as obrigações em matéria de qualidade do serviço e prestação para finalidades ou serviços específicos) os metadados deverão ser apagados ou anonimizados quando deixem de ser necessários para um determinado propósito.

À luz destas emendas do PE, um prestador poderá conservar metadados anonimizados para outras finalidades que não acarretem riscos para os utilizadores, dando a possibilidade aos prestadores de desenvolverem novas soluções com recurso à tecnologia *Big Data*. Um exemplo do uso desta tecnologia é o projeto *Smart Steps* da Operadora de Telecomunicação espanhola – *Telefonica* – que consiste no tratamento de dados agregados anonimizados provenientes da sua rede de comunicações para detetar tendências e comportamentos de grupo. Permitindo, desta forma, ter um conhecimento preciso acerca de quantos turistas chegam a uma cidade, a sua proveniência, e como se movem pelo território, o que constituiu um enorme valor para o setor do turismo. Este novo serviço, concretizado pela *Telefonica*, permite um conhecimento muito mais aprofundado para os comerciantes locais, que poderão criar descontos, a certas horas do dia, para serviços culturais, gastronómicos ou de retalho.[79]

Em relação ao conteúdo das comunicações, na Proposta de Regulamento *ePrivacy*, nas emendas do Parlamento Europeu à Proposta da Comissão, o consentimento tornou-se o único fundamento lícito para o tratamento, devido ao facto de os conteúdos das comunicações serem sensíveis por inerência, e o facto de que nenhuma razão técnica é suficiente para justificar uma interferência desta dimensão na privacidade. [80]

À semelhança do tratamento de metadados, o consentimento para tratamento de conteúdo é permitido apenas para os utilizadores finais, na Proposta original da Comissão, sendo permitido apenas para os utilizadores, na versão mais restritiva do Parlamento Europeu. Primeiramente, o consentimento do utilizador pode ser requisitado para efeitos da prestação de um serviço solicitado pelo próprio utilizador, desde que a prestação desse serviço não possa ser efetuada sem o tratamento desse conteúdo, "pelo fornecedor", tendo esta última parte sido acrescentada na versão do Parlamento Europeu. Segundo esta disposição, os fornecedores não poderão tentar obter o consentimento para o tratamento de dados de conteúdo em número superior aos que são necessários para a prestação dos serviços, que necessitam de ser específicos. Adicionalmente, a especificação de que os

[79] Ibidem,p .14. Ver, a este respeito, o Projeto Smart Steps da Telefonica. Disponível em: https://www.telco4telco.business-solutions.telefonica.com/smart_steps/index.php

[80] Art. 6.3 do Regulamento ePrivacy, tal como reformulado pela Proposta do Parlamento Europeu.

dados necessários só poderão ser tratados "pelo fornecedor", limita, de forma ainda mais incisiva, o âmbito de aplicação do artigo, uma vez que exclui a possibilidade desses dados puderem ser tratados por entidades terceiras. Esta norma irá impedir, por exemplo, que o fornecedor de email transfira dados para uma entidade terceira que seja especialista em algoritmos de processamento de linguagem natural e que poderão estar interessados em aceder ao conteúdo dos emails para desenvolverem os seus serviços.[81]

Em segundo lugar, o consentimento para tratamento do conteúdo das comunicações eletrónicas pode ser também requerido por todos os utilizadores para uma ou mais finalidades especificas e desde que essas finalidades não possam ser atingidas através do recurso à anonimização dos dados, e na condição de o fornecedor consultar a autoridade de controlo, de acordo com o previsto nos artigos 36.º, n.º 2 e 3 do RGPD. Este artigo aplicar-se-á nos casos em que os serviços não são requeridos pelo utilizador, e sim disponibilizados pelo fornecedor. Um exemplo desta situação seria se uma rede social disponibilizasse uma funcionalidade que permitisse examinar as fotografias dos utilizadores identificando-os de forma automática, ou emitindo um alerta cada vez que alguém efetuasse o *download* de fotografias em que o utilizador estivesse identificado.[82] A este respeito, o Parlamento Europeu introduziu uma exceção segundo a qual deixa de ser necessário o consentimento de todos os utilizadores para a prestação de um serviço explicitamente solicitado por um utilizador, para uso puramente pessoal e apenas durante o período necessário para esse efeito, desde que o tratamento efetuado não prejudique os direitos fundamentais e os interesses de outros utilizadores. Esta exceção facilita a obtenção do consentimento para o tratamento de dados pessoais no exercício de atividades exclusivamente pessoais ou domésticas.

Por fim, em relação ao tempo de conservação e apagamento dos dados, a Proposta da Comissão previa que o prestador do serviço de comunicações eletrónicas deveria apagar o conteúdo das comunicações eletrónicas ou tornar os dados anónimos, após a receção dos conteúdos das comunicações eletrónicas pelos destinatários, independentemente desses dados poderem ser registados ou armazenados pelo utilizador final ou por terceiros por ele designados. O Parlamento Europeu emendou esta disposição, prevendo que o prestador do serviço de comunicações eletrónicas deverá apagar o conteúdo das comunicações eletrónicas quando o mesmo deixar de ser necessário para

[81] Ibidem, p.14.
[82] Ibidem, p.14.

prestar desse serviço. Mais uma vez, o Parlamento optou por uma opção mais restritiva, eliminando a possibilidade de os prestadores de serviços de comunicações eletrónicas conservarem dados anonimizados.[83] Por exemplo, quando um utilizador partilha uma fotografia, através de uma aplicação de mensagens, o fornecedor da aplicação deverá apagar a fotografia nos seus servidores, assim que esta seja entregue ao destinatário.

Todavia, ambos os utilizadores podem decidir armazenar a fotografia, recorrendo a um fornecedor de *cloud*, que está sujeito às obrigações do RGPD. Isto significa que o fornecedor de serviços de *cloud* irá necessitar de um fundamento de licitude para tratar esses dados, estará obrigado a respeitar o princípio da limitação das finalidades, fornecer informação transparente, cumprir com as obrigações junto dos titulares dos dados ou aplicar medidas técnicas e organizativas.[84]

3.3 – Principais diferenças entre o artigo 6.º na versão original da Proposta da Comissão e as sucessivas alterações propostas pelo Conselho

Como referido no capítulo anterior, o artigo 6.º da Proposta, na sua versão original, permitia o tratamento de dados de comunicações eletrónicas para um conjunto bastante limitado de finalidades.

Este artigo, nas sucessivas alterações que foram sendo propostas pelas várias presidências do Conselho Europeu ao longo de quase quatro anos, foi-se tornando cada vez mais complexo, à medida que os legisladores tentavam evitar situações em que casos práticos específicos pudessem ser identificados, mas que não pudessem ser acomodados na versão original do artigo 6.º, tal como demonstrado nos exemplos acima mencionados.

Não existe duvidas em relação à existência de um impasse no Conselho, entre os vários Estados-Membros. Desde setembro de 2017, foram publicadas inúmeras redações que estabelecem alterações à proposta inicial da Comissão e do Parlamento. Na presente dissertação, debruçar-me-ei sobre as que considero mais significativas.

A **5 de dezembro de 2017**[85], a presidência Estónia do Conselho propôs algumas alterações à proposta inicial da Comissão e do Parlamento:

[83] Art. 7.1 do Regulamento ePrivacy, tal como reformulado pela Proposta do Parlamento Europeu.
[84] Ibidem, p.15.
[85]Doc.ST_15333_2017_INIT do Conselho da União Europeia. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_15333_2017_INIT&from=PT

1. **Artigo 6(2) (b):** Esta norma foi alterada para permitir o tratamento necessário para efeitos de execução contratual com o utilizador final. Inspirado no artigo 6(1) (b) do RGPD.
2. **Artigo 6(2) (ba):** A Presidência adicionou como base de licitude o tratamento de dados pessoais para efeitos de cumprimento de uma obrigação legal. Inspirado no artigo 6(1) (c) do RGPD.
3. **Artigo 6(2) (c):** Esta norma foi alterada para refletir o facto de que o utilizador final poderá ser uma pessoa singular ou coletiva.
4. **Artigo 6(2) (d):** A presidência incluiu como base de licitude o tratamento de dados pessoais para proteção do interesse vital do utilizador. Esta norma foi inspirada no artigo 9 (2) (c) do RGPD. Esta alteração foi acompanhada por um novo **considerando 17a.**
5. **Artigo (6)(2) (e):** A presidência incluiu como base de licitude o tratamento de dados pessoais para efeitos de investigação científica e estatísticos, inspirando-se, claramente, no artigo (9) (2) (j) do RGPD. Esta alteração é acompanhada por um novo **considerando 17b.**
6. **Artigo 6(3) (a):** Esta norma foi alterada para refletir o facto de que o utilizador final poderá ser uma pessoa singular ou coletiva.
7. **Artigo 6 (3) (aa):** Esta nova disposição permite o tratamento de dados quando existe, por parte do utilizador final, um pedido específico para o fornecimento de um determinado serviço, baseado no consentimento do utilizador que requereu esse mesmo serviço, desde que os direitos fundamentais e os interesses dos outros utilizadores sejam alvo de proteção adequada. Esta alteração é acompanhada com um **considerando 19a**, que explica que tipo de serviços é que são abrangidos por esta exceção.
8. **Artigo 6(3) (b):** A presidência incluiu, como uma das condições para esta exceção, a obrigação de conduzir uma avaliação de impacto das atividades de tratamento, de acordo com o RGPD. (art.36(2)(e)).
9. **Artigo 6(4):** Esta nova provisão permite o tratamento de dados de comunicações eletrónicas por uma entidade terceira por conta de um fornecedor de serviços de comunicações eletrónicas.

A segunda grande modificação ao artigo 6.º, já sobre a alçada da presidência austríaca do Conselho, foi publicada, a 10 de julho de 2018[86], com a introdução de um novo **artigo 6(2) (a),** que introduziu a possibilidade de o tratamento de metadados resultantes de comunicações eletrónicas poder ser efetuado pelos provedores de serviços de comunicações eletrónicas para outras finalidades compatíveis com as quais os metadados foram inicialmente recolhidos, simplificando: para "outros tratamento compatíveis"**.** Tal como mencionado pelo Conselho, este novo artigo foi inspirado no **artigo 6(4)** do RGPD. Este artigo foi inserido numa tentativa por parte do Conselho de fazer com o Regulamento continue aplicável no futuro, acompanhando a constante evolução tecnológica do setor, nomeadamente, com o desenvolvimento da Inteligência Artificial e da Internet das Coisas.

Simultaneamente, o Conselho procurou, ao introduzir esta alteração, assegurar que é levado a cabo por parte dos prestadores de serviços de comunicações eletrónicas um tratamento lícito e responsável dos dados dos cidadãos, introduzindo, juntamente com a possibilidade de efetuar o tratamento de metadados de comunicações eletrónicas "para outros fins compatíveis", inúmeros procedimentos e salvaguardas, que são, essencialmente, os mesmos que estão presentes no artigo 6 (4) do RGPD, complementando-as com salvaguardas especificas inerentes ao âmbito de aplicação material do Regulamento.

Essas salvaguardas foram incluídas no primeiro e segundo subparágrafos do **artigo 6(2) (a)** e são as seguintes: 1) os metadados só podem ser tratados para "outros fins compatíveis", desde que o tratamento não possa ser efetuado com recurso a informação anonimizada, e desde que esses metadados sejam apagados ou anonimizados, assim que deixem de ser necessários para cumprir com uma determinada finalidade; 2) o tratamento seja limitado a dados pseudonimizados e 3) os metadados não sejam usados para determinar a natureza ou as características do utilizador ou para estabelecer um perfil.

Adicionalmente, as salvaguardas já presentes no artigo 6(3a) (renumerado como **artigo 6(2aa))** foram também mantidas, isto é os fornecedores de serviços e redes de comunicações eletrónicas podem proceder ao tratamento de metadados: a) desde que não

[86] Doc. ST_10975_2018_INIT do Conselho da União Europeia, Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=consil%3AST_10975_2018_INIT

partilhem esses dados com entidades terceiras, excetuando se os dados forem anonimizados; b) antes de iniciarem o tratamento deverão efetuar uma avaliação de impacto das operações de tratamento e consultar as autoridades de controlo, em conformidade com os artigos 36 (2) e (3) do RGPD e c) informar o utilizador final, conferindo-lhe o direito de oposição ao tratamento, sem custos, a qualquer momento, e de forma simples e eficaz.

Além do exposto, a presidência introduziu, ainda, uma alteração no artigo 6(2) (b) no sentido de clarificar que o tratamento de metadados para efeitos de faturação e de pagamentos de interligação (relacionados com o quotidiano empresarial dos prestadores de serviços de comunicações eletrónicas) é permitido.

A terceira grande modificação da Proposta de Regulamento *ePrivacy* ocorreu a 26 de julho de 2019[87], durante a presidência finlandesa do Conselho.

Neste rascunho, a presidência propôs dividir o Artigo 6.º em quatro artigos:

- O artigo 6.º regula o tratamento de dados de comunicações eletrónicas
- O artigo 6a regula o tratamento do conteúdo das comunicações eletrónicas
- O artigo 6b regula o tratamento dos metadados das comunicações eletrónicas
- O artigo 6c que regula o tratamento de metadados para outros fins compatíveis.

No rascunho de 4 de outubro de 2019[88], foi introduzido um artigo 6d, relativo ao tratamento de dados de comunicações eletrónicas para deteção, apagamento e reporte de material que constitui pornografia infantil.

Nesta fase de discussão no Conselho Europeu, e após inúmeras propostas publicadas por cinco diferentes presidências (maltesa, estónia, búlgara, austríaca e romena), e após a publicação de oito textos de compromissos da presidência finlandesa, o que só evidencia diferentes pontos de vista e diferentes prioridades dos Estados-Membros em relação à Proposta de Regulamento *ePrivacy*,[89]a presidência finlandesa

[87] Doc. ST_11291_2019_INIT do Conselho da União Europeia. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_11291_2019_INIT&from=PT

[88]Doc. ST 12633 2019 INIT. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_12633_2019_INIT&from=PT

[89] Docs. 11001/19, 11291/19, 12293/19, 12633/19, 13080/19, 13632/19, 13808/19, 14054/19.

apresentou um novo texto de compromisso[90] ao Comité de Representantes Permanentes com vista à adoção de uma orientação geral. Todavia, este texto de compromisso foi rejeitado pelo Comité.[91]

A 21 de fevereiro de 2020, a presidência Croata[92] da presidência publicou uma nova Proposta com alterações de vulto relativas ao artigo 6.º. A maior alteração incluída neste rascunho, que pretendia ultrapassar o impasse de cerca de quatro anos de discussão da Proposta de Regulamento no Conselho, foi a introdução do interesse legitimo como base de licitude para o tratamento de metadados de comunicações eletrónicas. De acordo com o texto proposto pela presidência Croata, o artigo 6b(1)(d), será acompanhado, em linha do que ocorre com o RGPD, por um número de condições e salvaguardas previstas num novo artigo 6b (2). Estas salvaguardas são em tudo semelhantes às já mencionadas para o tratamento para "outros fins compatíveis": os metadados utilizados para efeitos de interesses legítimos não poderão ser transmitidos a entidades terceiras, a não ser que sejam anonimizados; deverá implementar-se uma avaliação de impacto na confidencialidade e na privacidade dos utilizadores finais, de acordo com o art. 35.º do RGPD, podendo ser necessária uma consulta prévia à autoridade de supervisão, em conformidade com o artigo 36.º do RGPD; deverá informar-se o utilizador final do direito de oposição ao tratamento, sem custos, a qualquer momento, de forma simples e eficaz e, por fim, deverão ser implementadas medidas técnicas e organizativas, com recurso à pseudonimização e à encriptação dos dados.

Todavia, o que parecia ser um enorme avanço no sentido de compatibilizar as condições de licitude previstas na Proposta de Regulamento *ePrivacy* e no RGPD, introduzindo a possibilidade de as operadoras de telecomunicações poderem tratar metadados de acordo com o interesse legítimo, ficou parcialmente gorada com a eliminação do artigo 6b c), relativo aos "outros tratamentos compatíveis" e com a eliminação do artigo 6b f), correspondente ao tratamento de metadados para efeitos estatísticos ou de investigação cientifica, uma vez que a presidência Croata considerou que a manutenção destes artigos seria redundante.

[90] 14068/19 + COR 1
[91] Doc. ST_14447_2019_INIT. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=consil%3AST_14447_2019_INIT
[92] Doc. ST 5979 2020 INIT. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5979_2020_INIT&from=PT

A última grande alteração no que ao artigo 6.º diz respeito, foi publicada a 4 de novembro de 2020[93], sob a égide da presidência alemã, e constituiu uma enorme surpresa para a indústria das telecomunicações, uma vez que vai contra muitos dos compromissos alcançados em versões anteriores da Proposta.

Por um lado, a Proposta da presidência alemã, introduz a possibilidade de tratamento de metadados para "monitorização de surtos epidémicos ou pandémicos", numa clara alusão ao atual surto da pandemia COVID-19, ou para auxílio em caso desastres naturais ou humanos. Estes dois exemplos são incluídos no tratamento para a proteção dos interesses vitais do utilizador final, tal como acontece no artigo correspondente no RGPD.[94] Apesar disto, a grande novidade foi a eliminação do tratamento para efeitos da prossecução de interesses legítimos, introduzida pela presidência Croata. Algumas dos exemplos anteriormente dados a propósito do tratamento para efeitos legítimos incluía o tratamento de metadados para efeitos de deteção de comportamentos abusivos ou fraudulentos na utilização de serviços de comunicações eletrónicas, ou para efeitos de faturação. A investigação científica também já havia sido citada como sendo um exemplo de tratamento de dados para fins de "interesse legitimo".

3.4 – O novo texto da presidência portuguesa do Conselho: finalmente a caminho da aprovação de um novo Regulamento ePrivacy?

A 5 de janeiro de 2021[95], no âmbito da presidência portuguesa do Conselho Europeu, foi publicado um novo texto ePrivacy que alterou por completo o caminho que vinha sendo seguido no quadro regulatório ePrivacy, em especial quando comparado com a última proposta publicada pela presidência alemã, que impunha duras restrições ao tratamento de metadados por parte das operadoras das telecomunicações. A grande modificação introduzida no texto da presidência portuguesa é precisamente a possibilidade de tratar metadados para "outros fins compatíveis", em linha com o que já sucede com o RGPD, vejamos:

[93] Doc. ST 9931 2020 INIT. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9931_2020_INIT&from=PT
[94] Artigo 6, n. º1, al. d) do RGPD.
[95] Doc. ST 5008 2021 INIT. Disponível em: https://www.statewatch.org/media/1649/eu-council-e-privacy-presidency-proposal-5008-21.pdf

- O artigo 6 (1) (a) (Tratamento permitido de dados de comunicações eletrónicas), foi alinhado com o artigo 6 (1) (b) do RGPD, relativo ao tratamento de dados para efeitos de execução contratual, tendo sido substituída a base legal demasiado restritiva que vinha do texto da presidência alemã: "**Para concretizar a transmissão da comunicação"** para uma base legal mais abrangente: **"Para fornecer um serviço de comunicações eletrónicas"** com todas as atividades de tratamento que fazem parte do fornecimento de um serviço de comunicações eletrónicas. Esta alteração é também consistente com a expressão utilizada na base legal prevista no artigo 6b (1) (b) (Tratamento permitido de metadados de comunicações eletrónicas), **"execução de um contrato de serviços de comunicações eletrónicas".**
- **O artigo 6 (1) (d) (Tratamento permitido de dados de comunicações eletrónicas)** voltou à versão constante no texto da presidência finlandesa para assegurar certeza jurídica sobre a base legal para o tratamento **"cumprimento de uma obrigação legal",** em linha com o previsto no artigo 6(1) (c) do RGPD.
- **O artigo 6b (1) (b) (Tratamento permitido de metadados de comunicações eletrónicas)** encontra-se em linha com o artigo 6(1) (b) do RGPD ("execução contratual"), tendo sido alterado de forma a identificar claramente a base legal para o tratamento de metadados, **"execução contratual"**, e outras atividades de tratamento permitidas, se tal for necessário, como por exemplo, para efeitos de faturação, cálculo de pagamentos de interconexão, detetar/impedir usos fraudulentos ou abusivos de serviços de comunicações eletrónicas.
- **O artigo 6b (1) (e) e (f) (tratamento para fins estatísticos)** está em linha com a expressão menos restritiva constante no artigo 89 (1) do RGPD (tratamento para efeitos estatísticos), tendo sido alterada a expressão: "contagem estatística" (uma única atividade) para uma expressão mais abrangente: "efeitos estatísticos".
- **O artigo 6b (2a)** sobre efeitos estatísticos, em relação à expressão "estatísticas oficiais nacionais e europeias", foram introduzidas alterações para incluir situações futuras, alterando-se a expressão: "com a legislação

nacional e o Regulamento 223/2009/EC para "com o direito nacional da União".

- **O artigo 6b, (2) (a), (b) e (c)** relativo à partilha de metadados estatísticos anonimizados com entidades terceiras foi reintroduzido em linha com o RGPD (que deixam de ser considerados dados pessoais de acordo com o artigo 4 (1) do RGPD) e com as salvaguardas adicionais de proceder a uma avaliação de impacto sobre a proteção de dados e à consulta prévia da autoridade de controlo de acordo com os artigos 35 e 36 do RGPD. Este artigo está também alinhado com o reintroduzido artigo 6c (3) (Tratamento compatível de metadados de comunicações eletrónicas).
- **Artigo 6c (Tratamento compatível de metadados de comunicações eletrónicas)** foi reintroduzido, em linha com a base legal de tratamento prevista no artigo 6 (4) do RGPD, sem necessidade de impor duras restrições ao setor das comunicações eletrónicas. Com esta base legal, as atividades de tratamento têm de estar em conformidade com os requisitos elencados no n.º 4 do artigo 6 do RGPD. Adicionalmente, o fornecedor do contrato de serviços de comunicações eletrónicas deverá cumprir com o princípio da responsabilidade enunciado no artigo 5 (2) do RGPD. (**Ver Anexo I).**

Assim, se compararmos as alterações ao artigo 6.º que foram introduzidas na Proposta de Regulamento ePrivacy, com o anterior texto da presidência alemã, é notório o esforço que foi encetado pela presidência portuguesa para encontrar o equilíbrio entre um elevado nível de proteção dos direitos fundamentais à vida privada e à proteção dos dados pessoais das comunicações eletrónicas, assegurando a livre circulação de dados e serviços de comunicações eletrónicas e impulsionando, simultaneamente, o desenvolvimento de novas tecnologias e a inovação no setor.

A 10 de fevereiro[96], e após quatro anos de negociações no Conselho, é aprovado pelos Estados Membros o texto da presidência portuguesa sobre o novo Regulamento ePrivacy no Comité de Representantes Permanentes do Conselho (COREPER), tendo sido o texto remetido para o Parlamento Europeu como parte do processo de "triálogo". De momento, tanto Conselho como o Parlamento Europeu e a Comissão terão de chegar

[96] Doc. ST 6087 2021 INIT. Disponível em: https://eur-lex.europa.eu/legal content/EN/HIS/?uri=CELEX:52017PC0010

a um consenso sobre o texto final, pelo que o caminho para a aprovação de um novo Regulamento ePrivacy se avizinha longo, principalmente tendo em conta a anterior posição do Parlamento Europeu, bastante pró-privacidade, aquando da publicação do texto da Comissão Europeia.

A reação do CEPD[97] ao acordo sobre o mandato de negociação adotado pelo Conselho, no sentido da adoção de um novo Regulamento ePrivacy não se fez esperar. À semelhança do que havia sucedido em versões anteriores, o CEPD alerta para o facto de que: "(…) o Regulamento Privacidade Eletrónica não deve, em caso algum, reduzir o nível de proteção proporcionado pela atual Diretiva Privacidade Eletrónica, devendo antes complementar o RGPD, proporcionando garantias adicionais sólidas de confidencialidade e proteção para todos os tipos de comunicações eletrónicas. O Regulamento Privacidade Eletrónica não pode, de modo algum, ser utilizado para alterar de facto o RGPD." Especificamente em relação ao artigo 6.º, a preocupação do CEPD é a que as exceções presentes nos artigos 6 (1) (c), artigo 6b (1) (e), artigo 6b (1) (f) e artigo 6c introduzidos pelo Conselho permitam tipos de tratamento demasiado abrangentes, devendo ser restringidas. Na opinião do CEPD, as exceções presentes nos artigos 6 (1) (b), no Artigo 6(1) (c) e no Artigo 6(1)(d) poderão permitir que o fornecedor de serviços de comunicações eletrónicas possa ter acesso irrestrito ao conteúdo dos dados dos utilizadores de serviços de comunicações eletrónicas. Por último, o CEPD enfatiza a importância do papel da anonimização e da cifragem.

Ainda, em relação ao "Tratamento para outros fins compatíveis", o CEPD argumenta que "O tratamento posterior para finalidades compatíveis comporta o risco de comprometer a proteção conferida pelo Regulamento Privacidade Eletrónica, especialmente no tratamento de metadados de comunicações eletrónicas, ao permitir o tratamento para qualquer finalidade que o prestador de serviços considere cumprir a cláusula de «compatibilidade», apesar de o legislador ter claramente procurado restringir a sua utilização a finalidades específicas na ausência de consentimento".

[97] Ver Declaração 03/2021 sobre o Regulamento Privacidade Eletrónica. Comité Europeu para a Proteção de Dados. Adotada em 9 de março de 2021. Disponível em: https://edpb.europa.eu/system/files/**202106**/edpb_statement_032021_eprivacy_regulation_pt.pdf

Por outro lado, apesar de as principais associações de comunicações, como a ETNO ou a GSMA[98] reconhecerem os esforços significativos levados a cabo pela Presidência Portuguesa, nomeadamente através da reintrodução do tratamento de metadados para outros fins compatíveis, e de uma abordagem baseada no risco, aproximando as normas constantes do RGPD com as normas constantes no ePrivacy, continua a existir uma discrepância no texto entre as operadoras de telecomunicações tradicionais e os OTTs, sendo, para isso, imprescindível, uma regulação que permita uma abordagem flexível e baseada no risco quanto ao tratamento de metadados de comunicações eletrónicas, sem comprometer o principio da confidencialidade das comunicações eletrónicas, essencial a este setor. Considerando, por último, que este é um bom ponto de partida para encetar negociações com o Parlamento Europeu e com a Comissão Europeia.

3.5. – A importância do tratamento dos metadados para as operadoras de telecomunicações

3.5.1 – A necessidade urgente de revisão do conceito "serviço de comunicações eletrónicas"

Há muito que as operadoras de telecomunicações deixaram de exercer a atividade clássica de fornecer infraestruturas para permitir a comunicação à distância entre pessoas localizadas em diferentes partes. Pensar que a atividade de uma operadora de telecomunicações em 2021 é apenas a de assegurar as comunicações, independente do meio, é, na minha opinião, uma perceção redutora e é, na minha perspetiva, o que tem estado na origem do debate relativo ao artigo 6.º, principalmente no que toca à diferente perceção, no que ao tratamento de metadados diz respeito, e à possibilidade de tratar os mesmos para "outros fins compatíveis", em linha com o que acontece com o RGPD. As autoridades europeias parecem partir de uma perspetiva em que a atividade de uma operadora de telecomunicações se deve cingir à prestação de serviços de telecomunicações. Ora, na realidade, o leque de soluções que a indústria das telecomunicações apresenta hoje em dia, quer no segmento do consumo, quer no

[98] Ver "ePrivacy: European telcos support a strong alignment with GDPR". 10 February 2021. Disponível em: https://etno.eu/news/all-news/696:eu-telcos-eprivacy.html

segmento empresarial vai muito além dos serviços básicos de provedor de acesso à internet e a comunicações de voz.

Ver, um provedor de serviços de comunicações eletrónicas, desta forma clássica, é criar um fosso já existente entre as operadoras tradicionais e os novos OTTs, que fornecem os mesmos serviços de comunicações utilizando as infraestruturas de internet das operadoras tradicionais, mas estando, atualmente, não sujeitas ao cumprimento de muitas das obrigações que lhes são impostas pela atual Diretiva ePrivacy. Isto, porque, se atentarmos ao artigo 3.º da Diretiva ePrivacy, o mesmo prevê que: "A presente diretiva é aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas publicamente disponíveis nas redes públicas de comunicações da Comunidade", enquanto o artigo 2.º da Diretiva remete para outros diplomas legais[99] a definição exata do que são "serviços de comunicações eletrónicas".[100] É possível inferir, através desses diplomas legais, que a intenção do legislador foi excluir do âmbito de aplicação material da Diretiva ePrivacy os OTTs.

Contudo, em dezembro de 2018, houve uma alteração significativa, uma vez que os diplomas legais para os quais o artigo 2.º da Diretiva ePrivacy remetiam foram substituídos pela entrada em vigor do Código Europeu das Comunicações das Comunicações Eletrónicas[101]. Ora, o novo Código Europeu das Comunicações Eletrónicas deixou de excluir os OTTs do seu âmbito de aplicação material. Pelo contrário, expandiu o conceito de "serviços de comunicações eletrónicas" para incluir também o conceito de "serviço de comunicações interpessoais".[102] Na prática, e tal como explicado no próprio texto do CECE: "(…) os serviços de comunicações eletrónicas, tais

[99] Diretiva 95/46/EC e Diretiva 2002/21/EC.

[100] Neste caso, a definição de "Serviço de Comunicações Eletrónicas" **encontrava-se no artigo 2.º, alínea c) da Diretiva 2002/21/EC,** cuja definição era a seguinte: "o serviço oferecido em geral mediante remuneração, que consiste total ou principalmente no envio de sinais através de redes de comunicações eletrónicas, incluindo os serviços de telecomunicações e os serviços de transmissão em redes utilizadas para a radiodifusão, excluindo os serviços que prestem ou exerçam controlo editorial sobre conteúdos transmitidos através de redes e serviços de comunicações eletrónicas; **excluem-se igualmente os serviços da sociedade da informação, tal como definidos no artigo 1.º da Diretiva 98/34/CE que não consistam total ou principalmente no envio de sinais através de redes de comunicações eletrónicas**."

[101] Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2018, que estabelece o Código Europeu das Comunicações Eletrónicas.

[102] Ver os artigos 2(4) e (5) do CECE no que diz respeito à definição de "serviço de comunicações interpessoais".

como os serviços de telefonia vocal, os serviços de mensagens e os serviços de correio eletrónico estão abrangidos pela presente diretiva."[103]

Como referido acima, um provedor de serviços de comunicações eletrónicas oferece muito mais aos seus consumidores do que apenas o serviço de acesso à internet e serviços de voz. Nos últimos 20 anos[104], assistiu-se a duas grandes revoluções, uma tecnológica e outra empresarial. Do ponto de vista tecnológico, a internet de banda larga permitiu a comunicação por voz através da internet, ou o chamado "*voice over internet protocol.*"[105] Este ponto explica o crescimento exponencial dos OTTs, que passaram também a prestar serviços tradicionalmente ligados às operadoras tradicionais. Por outro lado, assistiu-se, simultaneamente, a uma mudança no modo de operar das próprias operadoras que, apercebendo-se de uma redução drástica nas quotas de mercado, pelo desenvolvimento tecnológico acima mencionado, começaram a apostar em serviços de valor acrescentado.[106]

Todavia, apesar de assistirmos a uma clara aposta da indústria nos serviços de valor acrescentado em detrimento dos serviços básicos ou essenciais, de forma a aumentar a sua quota de mercado e a sua competitividade perante os OTTs, este tem sido um mercado praticamente ignorado do ponto de vista regulatório. Isto, porque, tal como explicado acima, a Diretiva ePrivacy, remete para outros instrumentos regulatórios a definição de "serviços de comunicações eletrónicas". Em 2009, remetia para a Diretiva 2002/21/EC, cabendo agora essa tarefa ao CECE. Esta opção foi também mantida na atual proposta de Regulamento ePrivacy.[107] Se o objetivo da Proposta de Regulamento ePrivacy é a de complementar e particularizar o RGPD, aplicando-se especificamente ao

[103] Ver o Considerando 10 do CECE.
[104] A primeira diretiva ePrivacy foi a DIRECTIVA 97/66/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 15 de dezembro de 1997 relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações.
[105]Vagelis Papakonstantinou & Paul de Hart, "Big Data Analytics in eletronic communications: A reality in need of ganular regulation (even if this includes na interim period of no regulation al all)", Brussels Privacy Hub, Working Paper, Vol.5, N.º16, June 2019. P.7. Disponível em: https://brusselsprivacyhub.eu/publications/BPH-Working-Paper-VOL5-N16.pdf
[106] O artigo 2, alínea g, da Diretiva ePrivacy define "Serviço de Valor Acrescentado" como: "qualquer serviço que requeira o tratamento de dados de tráfego ou dados de localização que não sejam dados de tráfego, para além do necessário à transmissão de uma comunicação ou à faturação da mesma". Na mesma linha, o considerando 18 da Diretiva exemplifica o que podem ser considerados serviços de valor acrescentado: os conselhos sobre as tarifas menos dispendiosas, a orientação rodoviária, as informações sobre o trânsito, as previsões meteorológicas e a informação turística.
[107] Ver o artigo 4(1) (b), que expressamente refere o CECE.

setor das comunicações eletrónicas, seria desejável que a Proposta de Regulamento regulasse casos muito mais detalhados e complexos, como o caso da utilização dos metadados provenientes das comunicações eletrónicas com recurso à inteligência artificial, ao *big data analytics* à IOT. Esta abordagem não pode ser simplesmente remetida para outro tipo de instrumentos jurídicos, que têm como objetivo regular outro tipo de situações.[108]

Ora, se verificarmos, a Proposta de Regulamento ePrivacy, parece apenas distinguir entre serviços de comunicações eletrónicas "essenciais" ou "básicos", referindo-se "aos serviços de acesso à Internet de banda larga básica e às comunicações de voz."[109] Poderá argumentar-se que a *ratio legis* do legislador em qualificar estes serviços como essenciais é que o consentimento para o tratamento de dados nestes dois serviços "não será válido se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado.[110]"

Todavia, parece que com esta opção, o legislador europeu deixou de fazer referência aos serviços de valor acrescentado na Proposta de Regulamento, cuja definição já consta da Diretiva ePrivacy,[111] Se tivermos em conta o atual mercado das comunicações, esta opção legislativa não parece fazer sentido, devido à multiplicidade de serviços que hoje são oferecidos pelo mercado.

No fundo, e tendo em conta a forma como o mercado das telecomunicações atua, devia existir, do ponto de vista regulatório, na Proposta de Regulamento ePrivacy, uma clara distinção entre os diversos serviços prestados, como pode ser demonstrado através da tabela infra:[112]

Serviços	Características
Básicos/Essenciais	Acesso à Internet e a comunicações de voz
Serviços Necessários	A título de exemplo: serviços de segurança, deteção de fraude, melhoria do sinal, apoio ao cliente, suporte técnico.

[108] Ibidem p.8.
[109] Ver o Considerando 18 da Proposta de Regulamento ePrivacy (e também os Considerandos 213 e 237 do CECE).
[110] Ver o Considerando 18 da Proposta de Regulamento ePrivacy.
[111] Ver o artigo 2 (g) da Diretiva ePrivacy.
[112] Ibidem p. 9

	Todos os que estão relacionados e que são necessários para o fornecimento dos serviços básicos.
Serviços de Valor Acrescentado	Todo e qualquer serviço não incluído nas duas categorias acima.

Este tipo de classificação iria trazer uma desejada flexibilidade, a um instrumento regulatório que pretende regular um mercado tão vasto e dinâmico, como é o mercado das comunicações eletrónicas. Esta classificação deverá ser feita dentro do quadro regulatório ePrivacy, isto porque o nível de especificidade necessário para efeitos de proteção de dados não deverá ser remetido para normas gerais europeias aplicáveis às telecomunicações.[113]

3.5.2 – Afinal, que tipo de dados pessoais é que são tratados no setor das comunicações eletróncias?

A classificação e o contexto do tratamento de dados pessoais no setor das telecomunicações constitui outro dos pontos em que o quadro regulatório ePrivacy tem falhado em acompanhar o desenvolvimento tecnológico no setor. No que toca às operadoras de telecomunicações tradicionais, apesar das alterações que se têm vindo assistir com a entrada no mercado dos OTTs, o modelo de negócio permanece praticamente intacto: Os clientes subscrevem contratos de longa duração para o fornecimento de serviços de internet, voz e serviços de valor acrescentado. Já os OTTs têm por base um modelo de negócio "livre", cujos serviços são prestados gratuitamente, tendo como contrapartida o tratamento de dados pessoais cada vez mais significativo.[114]

As categorias de dados pessoais tratados sob o quadro regulatório ePrivacy podem ser divididas de acordo com a seguinte tabela:

Categorias de Dados Pessoais	Características
Dados de Subscrição	Dados pessoais requisitados e fornecidos pelos subscritores aquando da celebração e durante a execução de um novo contrato.

[113] Ibidem p.9-10.
[114] Ibidem. p.10.

Metadados	Dados resultantes da utilização dos serviços, que podem ser incluídos nas seguintes categorias: - Números marcados; -Websites visitados: Dados relacioandos com o URL; - Dados de localização/ dados relacionados com o ponto de conexão de um equipamento terminal; - Dados de utilização dos serviços; - Canais de televisão visualizados; - Data, local, duração das comunicações; -Tipo de comunicação (voz/dados)
Conteúdo das comunicações	Conteúdo de uma chamada telefónica; texto de um SMS; mensagem de um *voice mail*; conteúdo de um email.

O que é relevante, além da distinção entre as diferentes categorias de dados pessoais presente na tabela supra, é perceber que o tipo de tratamento levado a cabo pelas operadoras tradicionais de telecomunicações difere, em muito, do tratamento levado a cabo pelos OTTs, tal como demonstrado na tabela infra:

Categorias de dados pessoais	**Operadoras de Telecomunicações**	**OTTs**
Dados de Subscrição	Detalhados (de forma a fazerem parte de um contrato para efeitos de fornecimento de serviços de telecomunicações)	Limitados (frequentemente, apenas nome e email)
Metadados	Variam consideravelmente, dependendo do caso em apreço, por exemplo:	

	- As operadoras de telecomunicações detêm dados detalhados como os números marcados/data/local/duração de uma chamada telefónica; - Os OTTs detêm dados de geolocalização mais precisos, uma vez que recorrem ao GPS, por oposição a torres móveis ou antenas.	
Conteúdo	Em princípio, não são alvo de tratamento (a não ser por força do cumprimento de uma obrigação legal)	Em princípio existe tratamento (por exemplo, em serviços de email gratuitos)

Na fundo, a qualidade do tratamento difere devido aos diferentes modelos de negócio que estão subjacentes às operadoras de telecomunicações tradicionais e aos OTTs. Enquanto as operadoras de telecomunicações funcionam com um modelo de negócio baseado no pagamento fixo em contratos de longa duração que se baseiam na utilização de um determinado serviço, os OTTs tendem a prestar os seus serviços gratuitamente, o que implica a contrapartida de tratar os dados dos seus utilizadores de forma mais significativa, nomeadamente para serem usados em publicidade.[115]

3.5.3 – A fusão dos conceitos de dados de tráfego e de dados de localização em metadados

A Diretiva *ePrivacy* prevê que as os Estados-Membros garantirão a confidencialidade das comunicações e respetivos dados de tráfego e de localização realizadas através de redes publicas de comunicações e serviços de comunicações eletrónicas. Assim, a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de interceção ou vigilância de comunicações e dos respetivos dados de tráfego, sem o consentimento dos utilizadores em causa, é proibido, exceto quando existe autorização legal para o efeito. De notar que esta esta obrigação se aplica tanto ao conteúdo das comunicações, como aos dados de tráfego. Estes dados podem ser utilizados com o consentimento do utilizador, ou se forem anonimizados.[116]

[115] Ibidem p. 11.
[116] Artigo 5.º, número 1, da Diretiva *ePrivacy*.

A este respeito, a Diretiva *ePrivacy*, define dados de tráfego, no Art.º 2, al. c) como: "quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações electrónicas ou para efeitos da facturação da mesma", como por exemplo, o tempo de duração de uma chamada. De acordo com o artigo 6.º da Diretiva *ePrivacy* os dados de tráfego só podem ser tratados se anonimizados, quando necessários para efeitos de faturação dos assinantes e de pagamento de interligações, ou para efeitos de comercialização dos serviços de comunicações eletrónicas ou para o fornecimento de serviços de valor acrescentado, desde que o consentimento dos utilizadores tenha sido previamente obtido.

Da mesma forma, a Diretiva define dados de localização, no Art.º 2, al.c), como: "quaisquer dados tratados numa rede de comunicações electrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações electrónicas publicamente disponível." Os dados de localização podem ser tratados quando anonimizados, ou com o consentimento dos utilizadores para a prestação de um serviço de valor acrescentado, como por exemplo o recurso ao GPS nos telemóveis[117].

A avaliação "REFIT" alertou para o facto de estas normas não serem replicadas noutros instrumentos, como o RGPD, sendo necessária uma regulação especifica na Proposta de Regulamento. Todavia, as disposições constantes da atual Diretiva não são suficientes para proteger a confidencialidade das comunicações. Algumas razões prendem-se, por exemplo, com a exclusão dos serviços prestados pelos OTT, ou com conceitos obsoletos de dados de tráfego e de localização (que não incluem, por exemplo, decisões automatizadas).[118] Num ambiente digital, os mesmos dados poderão definir-se como conteúdo para um prestador, e dados de tráfego para outro prestador. A Diretiva *ePrivacy* não reflete esta situação. A este respeito a AEPD menciona que deverá ser atribuído um elevado nível de proteção tanto aos metadados como aos conteúdos das comunicações eletrónicas, uma vez que, atualmente, os metadados, como é o caso dos

[117] Elena Gil González et. al, The Proposed ePrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads? In Brussels Privacy Hub, Working Paper Vol.6, n. º20 (March 2020), P. 10.

[118] Comission Staff Working Document, Ex-Post REFIT Evaluation of the ePrivacy Diretive, *Accompanying the document* Proposal for a Regulation of the European Parliament and the Council on the protection of privacy and confidentiality in relation to electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10.01.2017 SWD (2017) 5 final.

URL dos *websites*, poderão ser tão reveladores da vida privada de um individuo quanto os conteúdos[119]. Além disso, enquanto o RGPD permite seis fundamentos legais para o tratamento de dados pessoais, a atual Diretiva apenas permite o tratamento baseado no requisito do consentimento, restringindo o tratamento ao fornecimento de serviços de valor acrescentado. Portanto, a Diretiva *ePrivacy* contem uma abordagem bastante mais restritiva do que o RGPD.[120] Perante todas estas questões, a avaliação REFIT conclui que a confidencialidade das comunicações eletrónicas deve ser protegida sob a alçada das normas *ePrivacy*, uma vez que estas aumentam os direitos dos indivíduos. Adicionalmente, considerou-se que os conceitos de confidencialidade das comunicações eletrónicas, de dados de tráfego e de dados localização deveriam continuar unos.[121]

Na sequência destas várias recomendações, a Proposta de Regulamento *ePrivacy*, protege tanto o conteúdo das comunicações como os metadados: tendo isto em conta, a Proposta abandona os conceitos de dados de tráfego e de localização e substituiu-os no conceito único de metadados[122]. Ainda, existe uma clara divisão entre conteúdo, por um lado, e metadados, por outro. Se atentarmos ao conceito de metadados, o futuro regulamento contem uma definição mais especifica do que a Diretiva, definindo-os como: "os dados tratados numa rede de comunicações eletrónicas para efeitos de transmissão, distribuição ou intercâmbio de conteúdo de comunicações eletrónicas, incluindo os dados utilizados para detetar uma comunicação e identificar a sua fonte e destino, a localização do dispositivo no contexto da comunicação e a data, hora, duração e tipo de comunicação.[123]"

A definição de metadados acima referida, incorpora os conceitos de dados de localização e de tráfego provenientes da Diretiva *ePrivacy*. A razão desta fusão reside num aumento cada vez mais visível de dados gerados e do correspondente aumento da

[119] Opinion 5/2016, Preliminary EDPS on the review of the ePrivacy Directive (2002/58/EC), European Data Protection Supervisor, 22 July 2016, p.13.
[120] Estudo da Avaliação REFIT, p.38.
[121] No mesmo sentido vai o Parecer 03/2016 sobre a avaliação e revisão da Diretiva Privacidade Eletrónica (2002/58/CE), Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, adotado em 19 julho de 2016, p. 14. A este propósito o GT 29 alerta para o de que: "Estes dados já não são recolhidos apenas pelos fornecedores de serviços da Internet e fornecedores de serviços de telefonia tradicionais, mas também por diversas organizações, inclusive fora da UE."
[122] A AEPD considerou que se devia adotar o conceito de metadados na sua Opinion 5/2016, Preliminary EDPS on the review of the ePrivacy Directive (2002/58/EC), European Data Protection Supervisor, 22 July 2016, p.13.
[123] Art. 4.3 d) do Regulamento ePrivacy, tal como formulado pela Proposta do Parlamento Europeu.

sua capacidade de armazenamento e de análise. A evolução tecnológica fez com que, mesmo quando os dados de comunicações eletrónicas são apagados, a análise de dados de tráfego e de localização provenientes de várias fontes possa demonstrar padrões imergentes, que poderão levar à criação de perfis, aumentando um potencial impacto na privacidade. Além deste fator, há ainda que ter em conta as variadas formas de recolha e análise massiva de dados. Portanto, a fusão das normas relativas aos dados de tráfego e de localização em metadados deverá providenciar uma elevada proteção e definir regras claras para todas as partes envolvidas no tratamento.[124]

Por outro lado, a definição de conteúdo das comunicações eletrónicas foi definida pela Comissão como: "o conteúdo trocado através de serviços de comunicações eletrónicas, sob a forma de texto, voz, vídeos, imagens e som. Quando os metadados de outros serviços de comunicações eletrónicas ou protocolos são transmitidos, distribuídos, ou alterados, pela utilização do respetivo serviço, deverão ser considerados conteúdo de comunicações eletrónicas pelo respetivo serviço"[125]. A título de exemplo, ao tirar uma fotografia, a fotografia em si qualifica-se como conteúdo, já as definições da camara, a hora e a data da fotografia, qualificam-se como metadados. O mesmo aconteceu aquando do envio de um email, o corpo do email, o assunto e os documentos em anexo, são considerados conteúdo, enquanto que o emissor e o recetor do email são metadados.[126] Em relação a tipos de informações mais complexas, também podem ser qualificadas como metadados, tais como aquelas que podem ser analisadas a partir do tráfego IP, como *websites* navegados ou origem e destino de endereços. Contudo, a distinção entre conteúdo e metadados pode ser, em certos casos, bastante ténue. No geral, poderá concluir-se que a Proposta de Regulamento *ePrivacy* admite que os mesmos dados possam ser considerados conteúdo ou metadados dependendo do prestador de serviços. Tome-se o caso do email, por exemplo. O que foi dito anteriormente é verdadeiro para o fornecedor do email. No entanto, para o fornecedor de internet, o corpo do email, o

[124] Parecer 03/2016 sobre a avaliação e revisão da Diretiva Privacidade Eletrónica (2002/58/CE), Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, adotado em 19 julho de 2016, p.15.
[125]Art. 4.3 b) do Regulamento ePrivacy, tal como formulado pela Proposta do Parlamento Europeu.
[126] Elena Gil González et. al, The Proposed ePrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads? In Brussels Privacy Hub, Working Paper Vol.6, n. º20 (March 2020), P. 12.

assunto, os documentos anexos, o emissor e o recetor qualificam-se como conteúdo dos pacotes IP encaminhados pelo fornecedor.[127]

3.6 – A necessidade do Tratamento de Metadados de Comunicações Eletrónicas para "Outros fins compatíveis"

O artigo 6.º, n.º4 do RGPD prevê o tratamento para outros fins compatíveis como um mecanismo que permite aos responsáveis pelo tratamento reutilizar dados pessoais para uma finalidade diferente daquela para a qual os dados foram inicialmente recolhidos, sob condição de que essas duas finalidades sejam compatíveis. O responsável pelo tratamento deverá verificar a existência dessa compatibilidade, baseando-se em vários fatores:

a) Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;

b) O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento;

c) A natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9.o, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.o;

d) As eventuais consequências do tratamento posterior pretendido para os titulares dos dados;

e) A existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização.

Se a operação de tratamento pretendida passar o "teste da compatibilidade" não será necessária qualquer outra base legal além da que foi usada para a recolha inicial de dados pessoais.

Assim, o tratamento para outros fins compatíveis não serve como base legal primária para a recolha e tratamento de dados; é um mecanismo que permite aos responsáveis pelo tratamento, em casos específicos, reutilizar os dados pessoais que

[127] Ibidem. p.13.

foram recolhidos ao abrigo de uma base legal, claramente identificada, caso as condições que permitem auferir essa compatibilidade se encontrem preenchidas e as salvaguardas exigidas forem aplicadas.

O mandato de negociação do Conselho para o Regulamento ePrivacy introduziu o tratamento de metadados de comunicações eletrónicas para outros fins compatíveis no Artigo 6c, que foi redigido e opera da mesma forma que o tratamento de dados pessoais para outro fins compatíveis presente no artigo 6(4) do RGPD, estando sujeito, no entanto, a salvaguardas adicionais e mais restritas do que as que estão previstas no RGPD.

Poderá afirmar-se que as disposições introduzidas no texto do Conselho no que toca ao tratamento de metadados para outros fins compatíveis exige salvaguardas adicionais que são mais restritas do que aquelas que podemos encontrar no RGPD. Em particular, de acordo com o texto do Conselho, o tratamento de metadados para outros fins compatíveis, só poderá ocorrer nas seguintes condições:

(a) O tratamento não possa ser efetuado com recurso a metadados anonimizados;
(b) Os metadados que são usados para o tratamento têm de ser pseudonimizados;
(c) Os metadados não podem ser usados para determinar a natureza ou as características de um utilizador ou para criar perfis, de forma a que sejam produzidos efeitos jurídicos em relação aos mesmos ou que, de outra forma, os afete significativamente.

Outra diferença é que qualquer tratamento de metadados para outros fins compatíveis só poderá ocorrer se os dados em questão tiverem sido recolhidos de acordo com uma das bases legais previstas nos artigos 6 (1) e 6b (1) do texto do Conselho, sendo, elas próprias, mais restritas do que as bases legais previstas no RGPD.

Além do exposto, cabe também afirmar que os principais casos em que é necessário que as operadoras de telecomunicações recorram ao tratamento de metadados para outros fins compatíveis têm como objetivo estabelecer padrões de mobilidade a um nível agregado, respondendo a desafios práticos colocados pelas autoridades publicas, fornecedores de energia, organizações de transportes, entre outros. Os metadados tratados para outros fins compatíveis para este tipo de soluções seriam tipicamente atingidos através da análise de dados agregados de forma a criar mapas de fluxos, de maneira a visualizar padrões de movimento ou para ajudar à tomada de processos de decisão baseados em informação mais detalhada.

Assim, tendo em conta a realidade prática do setor, pedir o consentimento aos utilizadores para a utilização dos seus dados, como alternativa ao tratamento de metadados para outros fins compatíveis torna-se impraticável em casos como os acima descritos, ou porque as taxas de *opt-in* seriam bastante reduzidas, ou porque as tendências de *opt-in* seriam irregulares, destruindo-se assim o valor acrescentado que só se consegue, nestes casos, com recurso a vastas quantidades de dados.

Além do mais, o recurso à anonimização poderá ser impraticável nestes casos. Isto porque, para estabelecer padrões de mobilidade, os fornecedores de serviços de comunicações necessitam de ter acesso aos serviços de geolocalização que se encontram nos dispositivos dos utilizadores para entender a sua movimentação no espaço e no tempo. Este processo requere um indentificador que ligue a informação de localização obtida a um determinado dispositivo, sem que seja revelada a identidade do utilizador. Com recurso à anonimização dos dados, deixa de ser possível a ligação desse identificador ao dispositivo e, consequentemente, à localização do utilizador, não sendo possível estabelecer padrões de movimentação em tempo e espaço real.

Por outro lado, a pseudonimização permite analisar padrões de mobilidade, enquanto se salvaguarda a privacidade individual tornando impossível a correspondência dos dados a uma pessoa especifica sem o recurso a informação adicional, que deve ser tratada separadamente e sujeita a medidas técnicas e organizativas para prevenir a associação dos dados a uma pessoa. Se utilizadas em conjunto com outras medidas como a implementação de controlos de segurança e acesso, a pseudonimização torna-se uma medida extremamente eficaz e reconhecida pelo RGPD.

Por último, o Tribunal de Justiça da União Europeia (TJUE), no caso Tele2 & Watson[128] também considerou que os metadados não são inerentemente sensíveis. Na verdade, o TJUE afirmou que a retenção geral, sistemática e indiscriminada de metadados para efeitos de prevenção de criminalidade é desproporcionada.

Concluindo, o que importa, no entendimento do TJUE, não é apenas a natureza dos dados, mas também o objetivo, a finalidade, o contexto do tratamento e as salvaguardas ou a falta das mesmas. O mecanismo do tratamento para outros fins

[128] Processos apensos C-203/15 e C-698/15 Tele2 Sverige AB e Secretary of State for the Home Department, ECLI: EU: C:2016:970.

compatíveis, tendo em conta as salvaguardas que exige e porque não requere uma retenção geral de dados está, portanto, em conformidade com a jurisprudência do TJUE.

3.7 – Um possível paralelismo entre o artigo 6.º do RGPD e o artigo 6.º da Proposta da Regulamento ePrivacy?

O RGPD não regula, pelo menos não de forma direta, metadados, dados de localização e dados de tráfego no contexto das comunicações eletrónicas. Contudo, se atentarmos ao considerando 49 do RGPD o mesmo prevê: "O tratamento de dados pessoais, na medida estritamente necessária e proporcionada para assegurar a segurança da rede e das informações, […] bem como a segurança dos serviços conexos oferecidos ou acessíveis através destas redes e sistemas, pelas autoridades públicas, equipas de intervenção em caso de emergências informáticas (CERT), equipas de resposta a incidentes no domínio da segurança informática (CSIRT), fornecedores ou redes de serviços de comunicações eletrónicas e por fornecedores de tecnologias e serviços de segurança, constitui um interesse legítimo do responsável pelo tratamento." Sendo que estes tipos de tratamentos, necessários para assegurar a segurança das redes, envolvem, por inerência, o tratamento de metadados no contexto das comunicações eletrónica, é claro que o RGPD reconhece, implicitamente, os metadados, categorizando-os como o tipo de informação que pode ser tratada de acordo com os requisitos do interesse legitimo do artigo 6.º, n.º1, alínea f) do RGPD.[129]

Poderá ter-se em consideração inúmeros outros exemplos que demonstram que o RGPD não é alheio ao impacto dos metadados, dos dados de tráfego ou de localização. Primeiramente, é de notar que o RGPD (à semelhança do que sucedia com a Diretiva da Proteção de Dados) contem uma lista especifica de "categorias especiais de dados pessoais", presente no artigo 9.º. Este artigo aplica-se ao tratamento de dados pessoais que "revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa." Adicionalmente, o artigo 10.º contém normas especificas para o tratamento de outros tipos de dados

[129] Ver a este respeito*: Legal Memo with respect to the concept of metadata and its degree of sensitivity under future European e-privacy law*, Timelex, 29 de janeiro de 2018.

sensíveis, nomeadamente, para o tratamento de dados pessoais relacionados com condenações penais e infrações.

Perante o exposto, podemos observar que, o legislador europeu, não incluiu nas categorias especiais de dados pessoais, os metadados. Se atentarmos à lista de categorias especiais de dados pessoais que estava presente na Diretiva da Proteção de Dados e à atual lista que se encontra no RGPD, conclui-se que houve um acrescento com a inserção de dados genéticos e biométricos aos dados pessoais considerados sensíveis. Tendo este facto em conta, podemos concluir que se o legislador europeu tivesse desejado incluir, aquando da discussão do RGPD, os metadados, na categoria de dados sensíveis, poderia tê-lo feito, conjuntamente, com os dados genéticos e biométricos, o que não aconteceu. Também não se pode considerar que a não inclusão dos metadados como dados sensíveis tenha sido um lapso, uma vez que os dados de localização são um dos exemplos presente no artigo 4.º do RGPD, que incide sobre o conceito de dados pessoais. Poderá concluir-se que, contrariamente aos dados elencados no artigo 9.º e 10.º do RGPD, que são inerentemente sensíveis, a avaliação sobre a sensibilidade dos metadados só poderá ser feita mediante análise do contexto do tratamento dos metadados em questão, e numa base casuística. Além disso, também a proposta de Regulamento *ePrivacy* não contem qualquer referência ao artigo 9.º do RGPD, nem prevê que os metadados tenham de ser incluídos como outra categoria especial de dados ao referido artigo.

Adicionalmente, o RGPD prevê outros mecanismos, além do consentimento, para avaliar os potenciais riscos decorrentes das atividades de tratamento. A grande inovação trazida pelo RGPD reside, precisamente, na transferência do risco de uma atividade de tratamento, para os responsáveis pelo tratamento, o que significa que cabe aos mesmos avaliarem os riscos inerentes às atividades de tratamento conduzidas, adotando medidas técnicas e organizativas de forma a mitigarem esses riscos, bem como todas as outras medidas constantes na legislação de proteção de dados.

Esta abordagem baseada no risco[130] tem a sua expressão máxima no princípio da responsabilidade, previsto no artigo 5.º, n. º2 do RGPD, segundo o qual: "O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder

[130] Neste sentido: *Study of Proposal for an ePrivacy Regulation*, Hogan Lovells, November 2019. Disponível em: https://www.hoganlovells.com/~/media/hoganlovells/pdf/2019/2019_11_25_study_eprivacy_regulation.pdf?la=en

comprová-lo". No fundo, através da imposição de uma análise de eventuais riscos para os titulares dos dados e do cumprimento dos princípios enunciados no artigo 5.º, n. º1, o legislador europeu legitima a tomada de decisões pelo responsável pelo tratamento, imputando-lhe a responsabilidade das mesmas.

Ademais, se a linha de argumentação anteriormente exposta não fosse suficiente para demonstrar a opção do legislador europeu por uma abordagem baseada no risco, bem como a sua aplicabilidade aos dados de localização, bastando, para isso, estarmos atentos aos considerandos 74 e 75 do RGPD.

Esta abordagem baseada no risco é ainda visível em várias outras normas do RGPD, nomeadamente:

- No artigo 6.º, n. º4 que elenca as condições segundo as quais o tratamento de dados pessoais para fins distintos para os quais foram recolhidos é permitido, tal como descrito no capítulo 3.6 da presente dissertação.
- As disposições relativas às decisões individuais automatizadas, incluído a definição de perfis (Artigo 22.º), estabelecendo que o titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar. Também em relação a este artigo são admitidas exceções, desde que o responsável pelo tratamento adote "medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão."
- As novas obrigações relativas à proteção de dados desde a conceção e por defeito (artigo 25.º) que impõe aos responsáveis pelo tratamento que tenham em conta: "os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares" no momento da definição dos meios de tratamentos e no momento do próprio tratamento.
- A condução de avaliações de impacto sobre a proteção de dados (Artigo 35.º), estabelecendo: "Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades,

for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais."

- A obrigatoriedade para o responsável pelo tratamento e para o subcontratante de designar um encarregado de proteção de dados (Artigo 37.º), sempre que o tratamento for efetuado por uma autoridade ou organismo publico, excetuando os tribunais; sempre que " as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou que consistam em operações de tratamento em grande escala de categorias especiais de dados […]."

Em cada um destes exemplos, a abordagem presente no RGPD é clara: as atividades de tratamento levadas a cabo pelos responsáveis pelo tratamento deverão basear-se no princípio da responsabilidade, serem efetuadas de forma casuística e atendendo ao contexto específico do tratamento. Exclui-se, *a contrario*, uma abordagem baseada em soluções-padrão que ignoram o contexto e as características particulares das atividades de tratamento, precisamente o que se pretende no âmbito da Proposta de Regulamento *ePrivacy*.

Todavia, ainda que os metadatados devessem ser considerados sensíveis, é bastante criticável reduzir as bases de licitude ao consentimento, como se de uma panaceia se tratasse, uma vez que o consentimento, *per se*, não resolve todos os riscos e desafios que possam surgir de um eventual tratamento de metadados[131]. O próprio RGPD é bastante claro quanto a este ponto, não estabelecendo qualquer hierarquia entre as seis condições de licitude elencadas no artigo 6.º. O GT29 já emitiu, a este propósito, vários pareceres, em específico em relação à definição de consentimento, o GT 29 alerta para o facto de que: "O consentimento é, por vezes, uma base pouco sólida para justificar o tratamento de dados pessoais e perde o seu valor quando o seu âmbito é alargado ou restringido para se adequar a situações para as quais nunca foi pensado. A utilização do

[131] *Legal Memo with respect to the concept of metadata and its degree of sensitivity under future European e-privacy law*, Timelex, 29 de janeiro de 2018.

consentimento «no contexto certo» é crucial. Se for utilizado em circunstâncias para as quais não é adequado, em virtude de, provavelmente, não estarem reunidos os elementos que constituem um consentimento válido, isto conduziria a uma grande vulnerabilidade, o que, na prática, enfraqueceria a posição da pessoa em causa[132].”

Na realidade, o consentimento torna-se inviável em vários contextos em que possa existir uma relação de desigualdade estrutural, como no contexto de relação de uma relação laboral, situações médicas, relação entre professor e aluno, relações entre pais e filhos e nas várias interações que ocorrem entre a administração publica e o cidadão. Em suma, quando se trata de dados sensíveis, o mero recurso ao consentimento não é a forma mais viável ou adequada de fundamentar certos tipos de tratamento de dados pessoais. Um recurso exaustivo e sistemático ao consentimento poderá levar à criação de fadiga de consentimento, levando a que o consentimento possa ser considerado inválido, uma vez que, deixa de ser informado. Desta forma, o recurso a outros fundamentos de licitude, conjuntamente com a aplicação de medidas técnicas e organizativa adequadas poderá revelar-se uma forma mais eficiente de proteger dados pessoais[133].

[132] Parecer 15/2011 sobre a definição de consentimento do Grupo de Trabalho para a Proteção de Dados do Artigo 29.º, adotado em 13 de julho de 2011, pp.11-12.

[133] A este propósito ver Harting *Study on the Impact f the Proposed ePrivacy Regulation*, 19 de outubro de 2017: “As condições de licitude restritas contradizem o Artigo 6.º do RGPD. Quando um cliente paga ao fornecedor do serviço para “tratar” conteúdo e/ou metadados, o consentimento não é necessário de acordo com o RGPD, e não é claro o motivo pelo qual deverá ser um requisito no *ePrivacy*.” P.2.

CONCLUSÕES

No que ao artigo 6.º diz respeito, existe, desde o início da discussão do Regulamento *ePrivacy*, a ideia de que a privacidade e a confidencialidade das comunicações eletrónicas só pode ser alcançada sacrificando o desenvolvimento tecnológico.

O artigo 6.º, na versão original na Comissão Europeia, partia de uma proibição geral do tratamento dos dados de comunicações eletrónicas, contendo exceções bastantes restritivas para os fornecedores de serviços de comunicações eletrónicas. As alterações do Parlamento Europeu vierem restringir de forma ainda mais evidente a utilização dessas exceções, tornando-as aplicáveis apenas se estritamente necessário.

Durante as sucessivas presidências do Conselho Europeu, foram feitas algumas alterações no sentido de ir ao encontro das expectativas da industria que, como demonstrado, através do recurso a vários exemplos, tentou demonstrar que é possível proteger a confidencialidade e a privacidade das comunicações eletrónicas, sem com isso asfixiar a inovação e o desenvolvimento, por exemplo, em projetos de Big Data, Machine Learning, ou Inteligência Artificial, que poderão envolver o tratamento de dados, na condição de serem anonimizados, ou caso não seja possível do ponto de vista prático, pseudonimizados, contribuindo para setores como o turismo ou a mobilidade, ou aplicadas às smart cities, ao nível da EU.

A sugestão patente nesta dissertação vai no sentido de, à semelhança do que ocorre com o RGPD, no que toca ao tratamento de dados de comunicações eletrónicas, partir de uma abordagem baseada no risco, imputando a responsabilidade pelo tratamento e respetivas consequências aos fornecedores dos serviços de comunicações eletrónicas e não numa proibição à *priori*. Uma abordagem baseada em condições de licitude pré-definidas também não se afigura útil, uma vez que existem sempre casos que saem fora do escopo dos casos previstos nas exceções do artigo.

Ainda, no que ao tratamento de metadados diz respeito, parte-se do princípio que todos os metadados são sensíveis. De facto, esta posição apenas se poderá compreender se analisada à luz do acórdão *Tele 2 Sverige and Watson*, referido na própria Proposta. A

meu ver, o que se pode retirar após análise do caso é que não é possível separar o tratamento dos metadados do contexto em que são utilizados. Os metadados quando utilizados de forma generalizada e indiscriminada, podem, de facto, revelar inúmeras informações pessoais acerca dos indivíduos, no entanto, isto não significa que todos os metadados sejam sensíveis por inerência, dependendo do contexto em que forem utilizados.

Adicionalmente, ter-se-á de ter em conta que, no âmbito da presidência portuguesa, foi feito um esforço notável para criar um regulamento da privacidade no setor das comunicações eletrónicas mais flexível, com uma abordagem baseada no risco, nomeadamente através da introdução da possibilidade do tratamento de metadados para outros fins compatíveis, tendo sido aprovado o texto no COREPER, o que permite agora encetar negociações com o Parlamento Europeu e com a Comissão Europeia, numa tentativa de aprovar o tão necessário Regulamento ePrivacy.

Ao contrário do que, desde o início, tem vindo a ser argumentado pelas autoridades europeias para a proteção de dados, o texto da presidência portuguesa, ainda que não totalmente alinhado com o RGPD, prova que é possível compatibilizar um nível elevado de proteção de dados e metadados de comunicações eletrónicas, sem prejudicar o desenvolvimento tecnológico.

BIBLIOGRAFIA

1) Publicações/Artigos/Estudos especializados/Comunicações institucionais

- Voss, W. Gregor, First the GDPR, Now the Proposed ePrivacy Regulation (July 25, 2017). Journal of Internet Law, Vol. 21, No. 1, pp. 3-11 (July 2017). Disponível em: https://ssrn.com/abstract=3008765
- Zuiderveen Borgesius, Frederik and Kruikemeier, Sanne and Boerman, Sophie and Helberger, Natali, Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation (March 15, 2018). European Data Protection Law Review, Volume 3, Issue 3, p. 353-368. Disponível em: https://ssrn.com/abstract=3141290
- Zuiderveen Borgesius, Frederik and Steenbruggen, Wilfred, The Right to Communications Confidentiality in Europe: Protecting Trust, Privacy, and Freedom of Expression (August 31, 2018). Theoretical Inquiries in Law, Forthcoming. Disponível em: https://ssrn.com/abstract=3152014 ou http://dx.doi.org/10.2139/ssrn.3152014
- Zuiderveen Borgesius, Frederik and van Hoboken, Joris V. J. and Fahy, Ronan P. and Irion, Kristina and Rozendaal, Max, An Assessment of the Commission's Proposal on Privacy and Electronic Communications (June 7, 2017). Directorate-General for Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs, ISBN: 978-92-846-1100-3. Disponível em: https://ssrn.com/abstract=2982290
- Buttarelli, Giovanni, The Comission Proposal for a Regulation on ePrivacy: Why Do We Need a Regulation Dedicated to ePrivacy in the European Union? European Data Protection Law Review, Volume 3 (2017), Issue 2, pp.155-159. Diponível em: https://edpl.lexxion.eu/article/EDPL/2017/2/5
- HÄRTING Rechtsanwälte PartGmbB, Study on the Impact of the Proposed ePrivacy Regulation. 19 october 2017. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/epr_-_gutachten-final-4.0_3_.pdf
- Hongan Lovells, Study of Proposal for an ePrivacy Regulation. November 2019. Disponível em: https://www.hoganlovells.com/en/news/hogan-lovells-calls-for-an-alternative-approach-to-regulating-privacy-in-the-digital-economy
- «Estratégia para o Mercado Único Digital na Europa» Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao

Comité das Regiões, 6 de maio de 2015, disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

- Synopsis Report of the Public Consultation on The Evaluation And Review of the ePrivacy Directive. Disponível em: https://ec.europa.eu/digital-single-market/en/news/full-report-public-consultation-eprivacy-directive
- Comission Staff Working Document, Ex-Post REFIT Evaluation of the ePrivacy Diretive, *Accompanying the document* Proposal for a Regulation of the European Parliament and the Council on the protection of privacy and confidentiality in relation to electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10.01.2017 SWD (2017) 5 final. Disponível em:https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2017:0005:FIN:EN:PDF
- COMMISSION STAFF WORKING DOCUMENT. EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT. 10.1.2017. Disponível em: file:///C:/Users/drara/Downloads/7-SummaryoftheImpactAssessment%20(3).pdf
- By FUHR, Lise; PATAKI, Daniel, Overcoming Europe´s data inferiority complex: *why ePrivacy must be reformed?* 10 de novembro de 2020. Disponível em: https://etno.eu/news/all-news/8-news/687-data-inferiority-eprivacy.html
- Joint Telecoms Industry Statement on the ePrivacy Regulation, 6 de novembro de 2020. Disponível em: https://etno.eu//downloads/news/etno_gsma_statement_eprivacy_nov.2020.pdf
- Elena Gil González et. al, The Proposed ePrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads? *In* Brussels Privacy Hub, Working Paper Vol.6, n. º20 (March 2020). Disponível em: https://brusselsprivacyhub.eu/publications/BPH-Working-Paper-VOL6-N20.pdf
- ETNO´S views on the Proposal for an ePrivacy Regulation (2017/03). Disponível em: *https://etno.eu/datas/positionspapers/2017/RD440_ETNO_views_eprivacy/RD440_ETNO_views_eprivacy.pdf*
- Legal Memo with respect to the concept of metadata and its degree of sensitivity under future European e-privacy law, Timelex, Disponível em: https://etno.eu/datas/positions-papers/2018/ETNO_Metadata_Memo.pdf
- The Proposed European ePrivacy Regulation, Use Cases for enabling privacy-protection inovative products and services, April 2018. Disponível em:

https://www.gsma.com/gsmaeurope/wp-content/uploads/2018/04/GSMA-ETNO-ePR-Use-Cases-April-2018.pdf

- Digital Single Market – Stronger rules for eletronic communications, Brussels, 10 January 2017, MEMO/17/17. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_17
- ePrivacy: European telcos support a strong alignment with GDPR. Brussels, 10 February 2021. Disponível em https://etno.eu/news/all-news/696:eu-telcos-eprivacy.html
- Vagelis Papakonstantinou & Paul de Hart, "Big Data Analytics in electronic communications: A reality in need of ganular regulation (even if this includes an interim period of no regulation al all)", Brussels Privacy Hub, Working Paper, Vol.5, N.º16, June 2019. Disponível em: https://brusselsprivacyhub.eu/publications/BPH-Working-Paper-VOL5-N16.pdf

2) Orientações e recomendações:

- Parecer 2/2010 sobre publicidade comportamental em linha, Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, Adotado em 22 de junho de 2010
- Parecer 15/2011 sobre a definição de consentimento do Grupo de Trabalho para a Proteção de Dados do Artigo 29.º, adotado em 13 de julho de 2011.
- Parecer 03/2016 sobre a avaliação e revisão da Diretiva Privacidade Eletrónica (2002/58/CE), Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, adotado em 19 julho de 2016.
- Parecer 1/2017 sobre a proposta de regulamento relativo à privacidade e às comunicações eletrónicas (2002/58/CE), Grupo de Trabalho sobre a Proteção de Dados do Artigo 29.º, Adotado em 4 de abril de 2017.
- Opinion 6/2017. EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (e-Privacy Regulation). European Data Protection Supervisor. 24 April 2017.
- Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. European Data Protection Board. 12 March 2019.
- Declaração 3/2019 sobre um regulamento relativo à privacidade e às comunicações eletrónicas, Comité Europeu para a Proteção de Dados, Adotada em 13 de março de 2019.

- Declaração 03/2021 sobre o Regulamento Privacidade Eletrónica, Comité Europeu para a Proteção de Dados, Adotada em 9 de março de 2021.

3) Legislação e Jurisprudencia:

- Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas.
- DIRECTIVA 97/66/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 15 de dezembro de 1997 relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações.
- Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2018, que estabelece o Código Europeu das Comunicações Eletrónicas.
- Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE.
- Processos apensos C-203/15 e C-698/15 Tele2 Sverige AB e Secretary of State for the Home Department, ECLI: EU: C:2016:970.
- DIRECTIVA 2006/24/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 15 de março de 2006 relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE.
- Processos apensos C-293/12 e C-594/12 *Digital Rights Ireland e Seitlinger e Outros*, ECLI:EU:C:2014:238.
- Lei n.º46/2012, de 29 de agosto que transpõe para ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas.
- Processo C- 450/06 *Varec SA*, ECLI:EU: C: 2008:91.
- Acórdão *Niemietz/Alemanha*, de 16 de dezembro de 1992, Série A, n.º 251- B.

Índice

Anexo I
Proposta de Regulamento ePrivacy: Tabela Comparativa

Artigo 6.º "Tratamento permitido de dados de comunicações eletrónicas"

Comissão	Parlamento	Conselho
Tratamento permitido de dados de comunicações eletrónicas	**Tratamento ~~permitido~~ legal de dados de comunicações eletrónicas**	**Tratamento permitido de dados de comunicações eletrónicas**
1. Os fornecedores de redes e de serviços de comunicações eletrónicas podem tratar dados de comunicações eletrónicas: (a) Se tal for necessário para assegurar a transmissão da comunicação, durante o período necessário para esse efeito; ou (b) Se tal for necessário para manter ou restabelecer a segurança das redes e serviços de comunicações eletrónicas, ou detetar falhas técnicas e/ou erros na transmissão das comunicações eletrónicas, durante o período necessário para esse efeito.	**1.** Os fornecedores de redes e de serviços de comunicações eletrónicas **apenas** podem tratar dados de comunicações eletrónicas **se tal for necessário em termos técnicos para assegurar a transmissão da comunicação durante o período necessário para esse efeito.** (a) Se tal for necessário para assegurar a transmissão da comunicação, durante o período necessário para esse efeito; ou (b) Se tal for necessário para manter ou restabelecer a segurança das redes e serviços de comunicações eletrónicas, ou detetar falhas técnicas e/ou	1. Aos fornecedores de redes e de serviços de comunicações eletrónicas **é permitido** o tratamento de dados de comunicações eletrónicas **apenas se:** (a) Se tal for necessário para ~~assegurar a transmissão da comunicação, durante o período necessário para esse efeito~~ **fornecer um serviço de comunicações eletrónicas**; ou (b) Se tal for necessário para manter ou restabelecer a segurança das redes e serviços de comunicações eletrónicas, ou detetar falhas técnicas, ~~e/ou erros na transmissão das comunicações eletrónicas, durante o período necessário para esse efeito,~~ **erros, riscos de segurança, ou ataques a redes e serviços de comunicações eletrónicas.** (c) **Se tal for necessário para detetar ou prevenir riscos de segurança ou ataques no equipamento**

	erros na transmissão das comunicações eletrónicas, durante o período necessário para esse efeito.	**terminal do utilizador final.** (d) **Se tal for necessário para o cumprimento de uma obrigação legal à qual o fornecedor esteja obrigado pelo direito da União ou de um Estado-Membro, desde que essa obrigação respeite a essência dos direitos e liberdades fundamentais e que constitua uma medida necessária e proporcionada numa sociedade democrática para assegurar a prevenção, investigação, deteção ou repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.**
	1b. Os fornecedores de redes e de serviços de comunicações eletrónicas ou outras partes agindo em nome do fornecedor ou do utilizador final apenas podem tratar dados de comunicações eletrónicas se tal for necessário em termos técnicos para manter ou restabelecer a disponibilidade, integridade, confidencialidade e segurança das redes ou dos serviços de comunicações eletrónicas, ou para detetar falhas técnicas e/ou erros na transmissão das	

	comunicações eletrónicas, durante o período necessário para esse efeito.	
	3.a O prestador do serviço de comunicações eletrónicas apenas pode tratar dados de comunicações eletrónicas para efeitos da prestação de um serviço explicitamente solicitado, para uso puramente pessoal e somente durante o período necessário para esse efeito, e apenas o pode fazer sem o consentimento de todos os utilizadores se esse tratamento não prejudicar os direitos fundamentais e os interesses de outro utilizador ou utilizadores.	**2. Os dados de comunicações eletrónicas só poderão ser tratados durante o período necessário para uma ou várias finalidades específicas, previstas nos artigos 6 a 6b e desde que a finalidade ou finalidades em causa não possam ser atingidas através do tratamento de informações tornadas anónimas.**
		3.Uma parte terceira que atue por conta de um prestador de serviços e redes de comunicações eletrónicas poderá tratar dados de comunicações eletrónicas de acordo com os artigos 6 a 6c desde que as condições previstas no artigo 28 do Regulamento (UE) 2016/679 estejam preenchidas.
2. Os prestadores de serviços de comunicações eletrónicas podem tratar metadados de comunicações eletrónicas:	2. Os prestadores de serviços **e redes** de comunicações eletrónicas podem tratar metadados de comunicações eletrónicas **apenas:** (a) Se tal for **estritamente**	**Artigo 6b** **Tratamento permitido de metadados de comunicações eletrónicas** **1.Sem prejuízo do disposto no artigo 6(1), os prestadores de serviços e redes de comunicações eletrónicas**

(a) Se tal for necessário para cumprir as obrigações em matéria de qualidade do serviço previstas na [Diretiva que estabelece o Código Europeu das Comunicações Eletrónicas] ou no Regulamento (UE) 2015/212011 durante o período necessário para esse efeito; ou (b) Se tal for necessário para proceder à faturação, ~~calcular~~ o pagamento das interligações, detetar ou impedir a utilização ~~abusiva ou~~ fraudulenta de serviços de comunicações eletrónicas ou a subscrição desses serviços; ou ~~(c)~~ Se o utilizador ~~final~~ em causa tiver consentido o tratamento dos metadados das suas comunicações para uma ou várias finalidades específicas, incluindo a prestação de serviços específicos a esses utilizadores ~~finais~~, desde que a finalidade ou finalidades em	necessário para cumprir as obrigações em matéria de qualidade do serviço previstas na [Diretiva que estabelece o Código Europeu das Comunicações Eletrónicas] ou no Regulamento (UE) 2015/2120 durante o período **tecnicamente** necessário para esse efeito; ou (b) Se tal for **estritamente** necessário para proceder à faturação, **determinar** o pagamento das interligações, detetar ou impedir a utilização fraudulenta de serviços de comunicações eletrónicas ou a subscrição desses serviços; ou (c) Se o utilizador em causa tiver consentido o tratamento dos metadados das suas comunicações para uma ou várias finalidades específicas, incluindo a prestação de serviços específicos a	**podem tratar metadados de comunicações eletrónicas apenas:** **(a) Se tal for necessário para efeitos de gestão ou otimização de redes, ou para cumprir os requisitos obrigatórios de qualidade técnica do serviço previstos na Diretiva (EU) 2018/1972 ou no Regulamento (EU) 2015/2120;ou** **(b) Se tal for necessário para a execução de um contrato de serviços de comunicações eletrónicas no qual o utilizador final é parte, ou se for necessário para faturar, calcular pagamentos de interligação, detetar ou parar usos fraudulentos, ou usos abusivos, ou para subscrever serviços de comunicações eletrónicas; ou** **(c) Se o utilizador final visado tiver dado o seu consentimento para o tratamento de metadados de comunicações eletrónicas para uma ou mais finalidades específicas; ou** **(d) Se tal for necessário para a defesa de interesses vitais de uma pessoa singular; ou** **(e) Em relação a metadados que constituam dados de**

causa não possam ser atingidas ~~através do~~ tratamento ~~de informações tornadas anónimas.~~	esses utilizadores, desde que a finalidade ou finalidades em causa não possam ser atingidas **sem o** tratamento **desses metadados;**	**localização, se tal for necessário para fins de investigação científica ou histórica ou para fins estatísticos, desde que:** **i) Os dados sejam pseudonimizados;** **ii) O tratamento não possa ser efetuado através de informação tornada anónima, e os dados de localização sejam apagados ou tornados anónimos quando já não sejam necessários para o cumprimento da finalidade; e** **iii) Os dados de localização não sejam utilizados para determinar a natureza ou as características de um utilizador final ou para criar um perfil do utilizador final.** **f) Em relação a outros metadados que não sejam dados de localização, se tal for necessário para investigação científica ou histórica ou para fins estatísticos, desde que o tratamento esteja de acordo com o Direito da União ou dos Estados-Membros e esteja sujeito a garantias adequadas, incluindo encriptação e pseudoanonimização, para proteger os direitos fundamentais e os interesses dos utilizadores finais e que esteja de acordo com o número 6, do artigo 21.º e com os n.os 1,**

		2 e 4 do artigo 89.º do Regulamento (EU) 2016/679. **2a. Os dados tratados previstos nas alíneas e) e f) do número 1 deste artigo também podem ser usados para o desenvolvimento, produção e disseminação de estatísticas oficiais nacionais e Europeias, na medida em que tal seja necessário para essa finalidade e de acordo, respetivamente, com o direito nacional ou com o Direito da União.** **2.Sem prejuízo do disposto no artigo 6.º(3), os metadados de comunicações eletrónicas tratados de acordo com o n. º1, alínea e) não podem ser partilhados pelo fornecedor com uma parte terceira a não ser que se tenham tornado anonimizados.**
	2a. Para efeitos do n.º 2, alínea c), sempre que um tipo de tratamento de metadados das comunicações eletrónicas, nomeadamente através da utilização de novas tecnologias, tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar riscos elevados para os direitos e liberdades das pessoas singulares, aplicam-se os artigos 35.º e 36.º do Regulamento (UE) 2016/679.	

3. Os prestadores de serviços de comunicações eletrónicas podem tratar o conteúdo das comunicações eletrónicas: (a) Exclusivamente para efeitos da prestação de um serviço ~~específico a um~~ utilizador ~~final~~, se o utilizador ~~final ou utilizadores finais~~ em causa ~~tiverem~~ dado o seu consentimento para o tratamento do conteúdo das suas comunicações eletrónicas e a prestação desse serviço não puder ser efetuada sem o tratamento desse conteúdo; ou (b) Se todos os utilizadores ~~finais~~ em causa tiverem dado o seu consentimento para o tratamento do conteúdo das suas comunicações eletrónicas para uma ou mais finalidades específicas que não possam ser	3. Os prestadores de serviços de comunicações eletrónicas podem tratar o conteúdo das comunicações eletrónicas: (a) Exclusivamente para efeitos da prestação de um serviço **solicitado pelo** utilizador, se o utilizador em causa **tiver** dado o seu consentimento para o tratamento do conteúdo das suas comunicações eletrónicas e a prestação desse serviço não puder ser efetuada sem o tratamento desse conteúdo **pelo fornecedor**; ou (b) Se todos os utilizadores em causa tiverem dado o seu consentimento para o tratamento do conteúdo das suas comunicações eletrónicas para uma ou mais finalidades específicas que não possam ser atingidas através do tratamento de informações tornadas anónimas e o fornecedor tiver consultado a	**Artigo 6a** **Tratamento permitido do conteúdo das comunicações eletrónicas** **1.Sem prejuízo do disposto no artigo 6 (1), os fornecedores de serviços de redes e serviços de comunicações eletrónicas poderão tratar dados de conteúdo de comunicações eletrónicas, apenas:** **(a) Para efeitos da prestação de um serviço solicitado por um utilizador final para uso estritamente pessoal se o utilizador final que o solicitou tiver dado o seu consentimento e quando o tratamento solicitado não afete, de forma adversa, os direitos fundamentais e os interesses de outra pessoa visada; ou** **(b) Se todos os utilizadores finais visados tiverem dado o seu consentimento para o tratamento do conteúdo dos seus dados de comunicações eletrónicas para uma ou mais finalidades especificas**. **2.Antes de iniciar o tratamento previsto na alínea b) do n. º1, o fornecedor deverá proceder a uma avaliação de impacto dos riscos das operações de tratamento previstas sobre a proteção dos dados de comunicações eletrónicas e consultar a autoridade de controlo se tal for necessário de acordo com o artigo 36 (1)**

atingidas através do tratamento de informações tornadas anónimas e o fornecedor tiver consultado a autoridade de controlo. O disposto no artigo 36.º, n.os 2 e 3, do Regulamento (UE) 2016/679 aplica-se à consulta da autoridade de controlo.	autoridade de controlo. O disposto no artigo 36.º, n.ºs 2 e 3, do Regulamento (UE) 2016/679 aplica-se à consulta da autoridade de controlo.	**do Regulamento (EU) 2016/679. O artigo 36(2) e (3) do Regulamento (UE) 2016/679 deverá aplicar-se à consulta da autoridade de controlo.**
		Artigo 6c **Tratamento compatível de metadados de comunicações eletrónicas**
		1. Quando o tratamento para fins que não sejam aqueles para os quais os metadados de comunicações eletrónicas foram recolhidos de acordo com o n.º 1 dos artigos 6 e 6b não seja baseado no consentimento do utilizador final ou no Direito da União ou dos Estado-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 11.º, o fornecedor de serviços de redes e serviços deve, a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual

		os metadados de comunicações eletrónicas foram inicialmente recolhidos, ter nomeadamente em conta: **(a) Qualquer ligação entre as finalidades para as quais os metadados de comunicações eletrónicas foram recolhidos e as finalidades do tratamento posterior;** **(b) O contexto em que os metadados de comunicações eletrónicas foram recolhidos, em particular no que respeita à relação entre os utilizadores finais visados e o fornecedor;** **(c)) A natureza dos metadados de comunicações eletrónicas, bem como as modalidades do tratamento posterior, em particular quando esses dados ou quando o tratamento posterior possa revelar categorias de dados de acordo com os artigos 9 e 10 do Regulamento (EU) 2016/679;** **(d) As eventuais consequências do tratamento posterior pretendido para os utilizadores finais;** **(e)) A existência de salvaguardas adequadas, que podem**

		ser a cifragem ou a pseudonimização. **2. Tal tratamento, se considerado compatível, só poderá ocorrer, desde que:** **(a) O tratamento não possa ocorrer através de informação anonimizada, e os metadados de comunicações eletrónicas sejam apagados ou anonimizados assim que deixarem de ser necessários para concretizar aquela finalidade, e** **(b) O tratamento seja limitado ao tratamento de metadados de comunicações eletrónicas que sejam pseudonimizados, e** **(c) Os metadados de comunicações eletrónicas não sejam usados para determinar a natureza ou as características de um utilizador final, ou para criar um perfil do utilizador final, que produza efeitos legais em relação a esse ou essa utilizadora ou que o ou a afete significativamente.** **3.Para efeitos do n.º1 deste artigo, os fornecedores de redes e serviços de comunicações eletrónicas não podem, sem prejuízo do artigo 6 (3), partilhar esses dados com**

		uma parte terceira, a não ser que sejam anonimizados.