Processos da Privacy International, La Quadrature du Net e outros

País: Reino Unido

Região: Europa e Ásia Central

Número do caso: Processo C-623/17, Processos C-511/18, C-512/18, C-520/18

Data da decisão: 6 de outubro de 2020

Desfecho: Lei ou ação indeferida ou considerada inconstitucional. Parecer consultivo/Decisão preliminar.

Órgão judicial: Tribunal de Justiça da União Europeia

Área do direito: Direito Civil, Direito Constitucional

Temas: Privacidade / Proteção e Retenção de Dados

Palavras-chave: Proteção e Retenção de Dados / Direito à Privacidade

ANÁLISE DO CASO

Resumo do caso e desfecho

O Tribunal de Justiça da União Europeia (TJUE), em duas decisões proferidas pelo pleno, considerou que o direito da União Europeia impedia que a legislação nacional exigisse aos prestadores de serviços de comunicações eletrônicas a transmissão geral e indiscriminada de dados de tráfego e localização às agências de segurança e inteligência, com o objetivo de salvaguardar a segurança nacional. Em pedidos conjuntos elaborados pelo Reino Unido, França e Bélgica, o TJUE procurou determinar a legalidade da legislação nacional que estabelecia a obrigação de os prestadores de serviços de comunicações eletrônicas encaminharem os dados de tráfego e localização dos usuários para uma autoridade pública, ou reter esses dados de uma forma geral ou indiscriminada por motivos de prevenção do crime e segurança nacional. O Tribunal considerou que essa obrigação não só interferia com a proteção da privacidade e dos dados pessoais, como era incompatível com o princípio da liberdade de expressão consagrado no artigo 11 da Carta da União Europeia. Entretanto, o Tribunal estabeleceu que, quando tal retenção for justificada nos processos em que houver uma grave ameaça à segurança nacional ou pública, a natureza da medida deve ser "estritamente" proporcional ao objetivo pretendido. Além disso, o Tribunal também esclareceu o âmbito dos poderes conferidos aos Estados-Membros pela Diretiva sobre Privacidade e Comunicações Eletrônicas no que diz respeito à retenção de dados para os fins supracitados.

Fatos

Em toda a UE, a retenção e o acesso a dados pessoais no domínio das comunicações eletrônicas para salvaguardar a segurança nacional e combater a criminalidade têm sido uma prática generalizada entre as agências de segurança nacionais. Em particular, o TJUE, no processo Tele2Sverige, Watson e outros (C-203/15 e C-698/15, doravante "Tele2"), decidiu que os Estados-Membros não podem impor aos prestadores de serviços de comunicações eletrônicas uma obrigação de retenção geral e indiscriminada de dados. Isto foi problemático para os Estados-Membros que foram privados de um instrumento para salvaguardar a segurança nacional. Nesta toada, foram instaurados quatro processos distintos contra as legislações nacionais do Reino Unido, França e Bélgica relativamente à legalidade de uma obrigação geral e indiscriminada de retenção imposta aos prestadores de serviços de comunicações eletrônicas. Os detalhes destes procedimentos estão descritos a seguir:

Processo C-623/17 (Reino Unido)

No dia 5 de junho de 2015, foi proposta uma ação junto ao Tribunal de Poderes de Investigação (Investigatory Powers Tribunal, IPT) (Reino Unido) pelo Privacy International, um grupo de defesa sediado no Reino Unido, discutindo a legalidade da legislação que autoriza a aquisição e utilização de dados de comunicações em massa por agências de segurança e inteligência (nomeadamente GCHQ, MI5 e MI6). Especificamente, em uma decisão do dia 17 de outubro de 2016, os réus tinham reconhecido a utilização de dados pessoais em massa (como dados biográficos, de viagem, financeiros, comerciais e de comunicação) para análise por meio de verificação

cruzada e processamento automatizado, bem como a divulgação a outras pessoas/autoridades e parceiros estrangeiros. Estes dados, adquiridos de redes públicas de comunicações eletrônicas, eram utilizados pela GCHQ e MI5 desde 2001 e 2005, respectivamente.

Ao analisar a legalidade destas práticas, o tribunal considerou que as medidas para aquisição e utilização de dados eram compatíveis com o direito nacional [p. 6 da decisão 1]. Especificamente, as redes de comunicação eletrônica tinham a obrigação de enviar às agências de segurança e inteligência os dados coletados no curso de sua atividade econômica, mas o mesmo não acontecia com relação à aquisição de outros dados obtidos por essas agências sem o uso de poderes vinculantes. Portanto, o Tribunal considerou conveniente consultar o TJUE se (a) o regime jurídico nacional se enquadrava no âmbito da legislação da UE e (b) se e de que forma as exigências do Tele2 se aplicavam a esse regime.

Processo C-511/18 (França)

Mediante pedidos de 30 de novembro de 2015 e 16 de março de 2016, diversos grupos de defesa e organizações sem fins lucrativos propuseram pedidos de anulação de decretos junto ao Conselho de Estado [da França], que exigiam aos operadores de comunicações eletrônicas e aos prestadores de serviços técnicos que "implementassem nas suas redes práticas de processamento automatizado de dados concebidos [...] para detectar links que pudessem constituir uma ameaça terrorista", nos termos do ordenamento francês [p. 25]. Os autores alegaram que os decretos violavam a Constituição da França, a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais (CEDH) e as Diretivas 2000/31 e 2002/58 (relativas à proteção de dados pessoais e da privacidade).

Embora o órgão tenha concluído que a obrigação de reter os dados e o acesso das autoridades administrativas a esses dados se enquadra no âmbito da legislação da UE, considerou que não era aplicável as disposições do direito nacional relacionadas diretamente com as técnicas de coleta de inteligência aplicadas diretamente pelo Estado. Dessa maneira, o Tribunal considerou conveniente suspender o processo e enviou ao TJUE três questões para interpretação.

Processo C-512/18 (França)

Mediante um pedido de 15 de setembro de 2016, os grupos de defesa acima mencionados propuseram uma ação apartada contra uma decisão implícita de rejeição do pedido de revogação de textos legislativos, que segundo os autores violavam a privacidade ao impor uma obrigação de retenção geral e indiscriminada de dados de comunicação para fins judiciais. O órgão considerou que a obrigação de reter e conservar dados, tal como aplicada ao presente caso, não se enquadrava no âmbito da legislação da UE, uma vez que seu âmbito se limitava à prestação de serviços de comunicações eletrônicas publicamente disponíveis em redes de comunicações públicas na UE. Como a legislação da UE não estabeleceu uma proibição expressa à retenção de tais dados, também considerou adequado enviar o processo ao TJUE.

Processo C-520/18 (Bélgica)

Mediante pedidos protocolados em janeiro de 2017, foram propostas diversas ações junto ao Tribunal Constitucional da Bélgica para anulação da lei belga que exige a retenção de dados. Os autores alegaram que a lei não fornecia garantias adequadas de proteção dos dados retidos e isso implicou no risco de que os perfis de personalidade pudessem ser compilados e utilizados indevidamente pelas autoridades competentes. Alegaram que as disposições violavam a Constituição da Bélgica, diversas disposições da CEDH, o Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP) e o Tratado da União Europeia (TUE). Com semelhanças entre o direito nacional belga e a legislação da UE sobre a retenção de dados gerados em conexão com as redes públicas de comunicação, o Tribunal Constitucional da Bélgica decidiu enviar o processo ao TJUE para uma decisão preliminar.

Mediante decisões de 25 de setembro de 2018 e 9 de julho de 2020, o Tribunal combinou os processos C-511/18, C-512/18 e C-520/18. O processo C-623/17 foi julgado em separado. Em três entendimentos doutrinários distintos proferidos pelo procurador-geral Campos Sánchez-Bordona, de 15 de janeiro de 2020, o procurador-geral decidiu que as atividades desenvolvidas pelas autoridades públicas dos Estados-Membros por motivos de segurança nacional que exigem a cooperação de entidades privadas estão abarcadas no âmbito da Diretiva 2002/58 em relação à privacidade e às comunicações eletrônicas. Portanto, quando os prestadores de serviços de comunicações eletrônicas forem obrigados por lei a reter dados e a permitir que as autoridades públicas tenham acesso a esses dados, serão aplicáveis as disposições da Diretiva (especificamente o princípio da confidencialidade das comunicações nos termos do Artigo 5(1)). De acordo com a AG, os regimes nacionais devem se alinhar às normas do TJUE estabelecidas no Tele2 e no Digital Rights Ireland e Outros, processos C-293/12 e C-594/12 (“Digital Rights Ireland”), mesmo em casos relacionados à segurança nacional.

Embora os Estados-Membros possam adotar medidas legislativas no interesse da segurança nacional, o procurador-geral também decidiu que as limitações previstas no artigo 5(1) devem ser interpretadas “estritamente”. Ele recomendou retenção e acesso limitados aos dados para a prevenção eficaz da criminalidade e a salvaguarda da segurança nacional, mas acrescentou também que, nos casos que apontassem uma ameaça iminente ou um risco extraordinário, a legislação nacional tinha autorização de impor obrigações gerais e amplas de retenção de dados [p. 16 do Voto C 511/18 e C 512/18]. O procurador-geral indicou que as obrigações de retenção de dados de forma geral ou indiscriminada devido a ameaças graves ou persistentes à segurança nacional interferem com os direitos fundamentais consagrados na Carta dos Direitos Fundamentais da UE. Argumentando que o combate contra o terrorismo não era uma questão de eficácia prática, mas de eficácia jurídica [p. 5 do Voto no processo C 623/17], ele decidiu que a notificação aos titulares dos dados era uma condição prévia necessária à retenção dos dados, a menos que isso comprometesse a ação das autoridades nacionais.

O procurador-geral também declarou que a coleta em tempo real de dados de tráfego e localização não estava excluída nos termos da Diretiva, desde que seja realizada considerando os procedimentos estabelecidos e as salvaguardas acima mencionadas. Também foi decidido que esta obrigação não é aplicável apenas a crimes graves, mas também a crimes menos graves, conforme previsto no Artigo 23(1) do RGPD [p. 9 do Voto no processo C-520/18]. Quanto à possibilidade de o tribunal nacional manter os efeitos de uma lei nacional em caso de incompatibilidade com a legislação da UE, o procurador-geral considerou que isso é possível apenas se a manutenção desses efeitos for justificada e enquanto for estritamente necessário para corrigir a incompatibilidade com a legislação da UE.

Visão geral da decisão

O pleno do Tribunal de Justiça proferiu um parecer preliminar em dois processos no dia 6 de outubro de 2020.

A principal questão para o Tribunal era a aplicação da Diretiva sobre a privacidade, as comunicações eletrônicas, as atividades relacionadas com a segurança nacional e o combate ao terrorismo.

Diante disso, o TJUE formulou cinco perguntas para consideração:

(a) Uma legislação nacional que permita a uma autoridade estatal exigir aos provedores de serviços de comunicações eletrônicas o envio de dados a agências de segurança e inteligência para segurança nacional se enquadra no âmbito de aplicação da Diretiva 2002/58?

(b) O Artigo 15(1) da Diretiva 2002/58 deve ser interpretado no sentido de impedir a aplicação da legislação nacional que impõe aos prestadores de serviços de comunicações eletrônicas, para os fins previstos no Artigo 15(1), uma obrigação de retenção geral e indiscriminada de dados de tráfego e localização?

(c) O Artigo 15(1) da Diretiva 2002/58 deve ser interpretado no sentido de impedir a aplicação da legislação nacional que exige que os prestadores de serviços de comunicações eletrônicas implementem, em suas redes, medidas que permitam, por um lado, a análise automatizada e a coleta em tempo real de dados de tráfego e localização e, por outro, a coleta em tempo real de dados técnicos relativos à localização do equipamento terminal utilizado, mas que não prevê que as pessoas envolvidas nesse processamento e nessa coleta sejam notificadas? [p. 45]

(d) As disposições da Diretiva 2000/31 devem ser interpretadas no sentido impedir a aplicação da legislação nacional que exige que os fornecedores de acesso aos serviços de comunicações públicas online e os provedores de serviços de hospedagem retenham, em geral e indiscriminadamente, os dados pessoais relativos a esses serviços? [p. 49]

(e) Um tribunal nacional pode aplicar uma disposição de direito nacional que exige a retenção geral e indiscriminada de dados de tráfego e localização, de forma a alcançar os objetivos de segurança nacional/combate ao crime – apesar de a legislação ser incompatível com o artigo 15(1) da Diretiva 2002/58? [p. 52]

(f) O artigo 15(1) da Diretiva 2002/58 sobre privacidade e comunicações eletrônicas consagra o princípio da confidencialidade das comunicações eletrônicas e respectivos dados de tráfego e prevê que outras pessoas, além dos usuários, sejam proibidas de armazenar, sem o consentimento dos usuários, tais comunicações e dados. Entretanto, o artigo 15(1) da Diretiva permite que os Estados-Membros introduzam exceções ao princípio previsto no artigo 15(1), quando tal restrição for necessária para salvaguardar a segurança nacional.

Quanto à primeira questão, o Tribunal decidiu inicialmente que a Diretiva 2002/58 sobre privacidade e comunicações eletrônicas é aplicável à legislação nacional que exige a coleta e retenção de dados pessoais. Respondendo negativamente à alegação dos réus de que as atividades das agências de segurança e inteligência são funções essenciais do Estado e, por conseguinte, responsabilidade exclusiva dos Estados-Membros fora do âmbito da Diretiva, o TJUE considerou que o âmbito da Diretiva afeta não apenas as medidas legislativas que exigem a coleta e retenção de dados, mas também as medidas legislativas que exigem que os prestadores de serviços concedam acesso a esses dados. Isto porque tais medidas legislativas exigiam necessariamente o processamento de dados pelos provedores de comunicações eletrônicas e, portanto, não podem ser consideradas como atividades características dos Estados. O Tribunal mencionou o RGPD para ressaltar que a divulgação de dados pessoais por transmissão (como o armazenamento ou a disponibilização de dados de outra forma) constituía "processamento" (o RGPD designa o conceito de "processamento de dados pessoais" como qualquer operação sobre dados pessoais que constitua coleta, armazenamento, utilização, consulta, divulgação por transmissão, difusão ou disponibilização de dados de outra forma). [p. 15 do Processo C-623/17].

Em contrapartida, o TJUE declarou que a única circunstância em que a proteção dos dados das pessoas não é coberta no âmbito da legislação da UE é quando os Estados-Membros implementam diretamente medidas sem impor obrigações de processamento aos prestadores de serviços de comunicações eletrônicas.

Após decidir sobre a aplicabilidade da Diretiva 2002/58 no presente conjunto de processos, o Tribunal analisou o impacto do direito à segurança consagrado no artigo 15(1) da Diretiva 2002/58 e na Carta dos Direitos Fundamentais da UE (Artigo 6 – Direito à Liberdade e à Segurança). Especificamente, os órgãos não sabiam se a retenção de dados prevista nas legislações nacionais interferia com os artigos 7 (Respeito à vida privada e familiar) e 8 (Proteção dos dados pessoais) da Carta. Ao confirmar a decisão no processo Tele2, Watson e outros, o TJUE decidiu que a Diretiva 2002/58 não permite que a exceção à obrigação do princípio de garantir a confidencialidade das comunicações eletrônicas e dos dados associados e à proibição de armazenamento de tais dados se torne a regra (conforme estabelecido no artigo

5(1)). Consequentemente, o Tribunal concluiu que a Diretiva não autoriza os Estados-Membros a adotarem medidas legislativas que restrinjam o âmbito dos direitos para efeitos de segurança nacional, a menos que tais medidas respeitem os princípios gerais da legislação da UE, como o princípio da proporcionalidade e os direitos fundamentais garantidos pela Carta. [p. 35]

É importante ressaltar que o Tribunal concordou que a imposição de obrigações, por meio de legislações nacionais, aos prestadores de serviços de comunicações eletrônicas de reter dados de tráfego não apenas interferia na proteção da privacidade e dos dados pessoais, mas também era incompatível com o princípio da liberdade de expressão, nos termos do artigo 11 da Carta da UE. O Tribunal não apenas reiterou a importância da privacidade e da liberdade de expressão na interpretação do artigo 11 da Diretiva, como também considerou que a retenção de dados, *per se*, constituía uma derrogação do princípio de confidencialidade previsto no artigo 5(1), pois impedia qualquer outra pessoa além do usuário de armazenar esses dados. O Tribunal não considerou relevante fazer uma distinção entre dados confidenciais e não confidenciais ou o fato de os dados retidos terem sido utilizados posteriormente ou não.

De notável importância para o Tribunal foi o risco de criar perfis – a possibilidade do uso de dados de tráfego e localização para obter informações sobre aspectos da vida privada (como posições políticas, orientação sexual, crenças religiosas, condição de saúde, relações sociais, etc.) e tirar conclusões precisas sobre a vida privada de pessoas cujos dados foram retidos constituiu uma ameaça direta ao direito à privacidade. Como resultado, em primeiro lugar, a retenção de dados para fins de policiamento foi, *per se*, uma violação do direito de respeito às comunicações e, em segundo lugar, a mera retenção de dados em quantidades significativas por parte dos provedores de comunicações eletrônicas acarretou um risco de abuso e acesso ilegal.

Neste contexto, o Tribunal de Justiça respondeu afirmativamente à segunda questão, e decidiu que a Diretiva da UE impedia que a legislação nacional exigisse aos prestadores de serviços de comunicações eletrônicas a transmissão geral e indiscriminada de dados de tráfego e localização às agências de segurança e inteligência, com o objetivo de salvaguardar a segurança nacional. Além disso, declarou também que fazer isso, mesmo como medida preventiva, não é permitido nos termos da legislação da UE, especialmente no caso das obrigações que retêm dados de forma geral ou indiscriminada e quando não existe qualquer vínculo entre o comportamento das pessoas cujos dados são afetados e o objetivo visado pela legislação em questão.

Entretanto, o Tribunal estabeleceu que, quando tal retenção for justificada nos processos em que houver uma grave ameaça à segurança nacional ou pública, a natureza da medida deve ser "estritamente" proporcional ao objetivo pretendido. É possível ter um objetivo de medida geral apenas se for conciliado com os direitos fundamentais (interpretação do artigo 15(1)). Mais importante ainda, o Tribunal especificou que uma decisão que imponha tal ordem deve estar sujeita à revisão efetiva pelo Tribunal ou por um órgão administrativo independente com autoridade vinculante. O Tribunal também solicitou uma regulamentação clara e precisa em nível nacional que regule o âmbito e a aplicação da retenção de dados para salvaguardar

contra o risco de abuso.

Entretanto, o Tribunal fez um ponto de distinção em relação à retenção de dados relativos à identidade civil dos usuários de sistemas de comunicação eletrônica. Como não é possível determinar a data, hora, duração e destinatários em tais casos, não é possível traçar um perfil da vida privada. Para essa retenção orientada com base em fatores objetivos ou não discriminatórios (de acordo com categorias de pessoas envolvidas ou um critério geográfico), é permitida uma medida legislativa que exija que os provedores de comunicações eletrônicas retenham tais dados, mesmo na ausência de uma conexão entre todos os usuários de sistemas de comunicações eletrônicas e os objetivos visados [p. 42]. Da mesma forma, a retenção dos endereços IP atribuídos à fonte da comunicação também é permitida se for limitada ao estritamente necessário. Por último, quando a retenção de dados para além dos períodos legais de retenção for necessária e as infrações já tiverem sido estabelecidas ou a sua existência for razoavelmente suspeita, a Diretiva não impede a adoção de uma medida legislativa.

Na terceira questão, o órgão de envio observou que as técnicas de coleta automatizada de inteligência e coleta de dados técnicos em tempo real eram legais apenas com a intenção de prevenir o terrorismo e não de outra forma. Como ponto preliminar, o TJUE observou que os dados em relação aos quais é feita uma análise automatizada para fins de rastreio de terrorismo constituem "dados pessoais" ao abrigo do RGPD, uma vez que as informações ainda pode ser identificáveis a uma pessoa específica. Nesta base, o Tribunal concluiu que essa análise automatizada dos dados de tráfego e localização era contrária ao princípio da confidencialidade da Diretiva 2002/58, bem como aos direitos fundamentais previstos na Carta da UE, e provavelmente desencorajaria o exercício da liberdade de expressão.

Mesmo aqui, a doutrina da proporcionalidade “estrita” seria aplicável, se uma interferência fosse considerada necessária em relação a uma grave ameaça à segurança nacional. As ressalvas para cumprir o teste de proporcionalidade incluíram: (a) a ameaça à segurança nacional deve ser genuína e presente ou previsível e (b) a duração da retenção deve ser limitada ao estritamente necessário. Modelos ou critérios pré-estabelecidos para fins de análise automatizada (como origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical ou informações sobre a saúde ou vida sexual de uma pessoa) com a intenção de prevenir o terrorismo, portanto, não podem ser baseados em dados confidenciais isoladamente [p. 47]. O Tribunal aplicou um raciocínio semelhante à coleta de dados pessoais em tempo real. A coleta de tais dados não é proibida pela Diretiva apenas se for limitada às pessoas em relação às quais exista um motivo válido para suspeitar que estão envolvidas em uma atividade terrorista e estão sujeitas a uma análise prévia por parte de um tribunal ou de uma autoridade administrativa independente vinculante.

Em relação à quarta questão, o Tribunal interpretou o artigo 23(1) do RGPD (que prevê restrições ao processamento de dados pessoais), juntamente com a Carta, para excluir a legislação nacional que exige que os fornecedores de acesso aos serviços de comunicação online e os provedores de serviços de hospedagem retenham, em geral e indiscriminadamente, os dados pessoais relativos a esses serviços. O Tribunal aplicou

as conclusões no contexto das questões acima mencionadas também ao artigo 23 do RGPD.

Por último, o TJUE decidiu sobre a última questão, em relação à situação da manutenção dos efeitos temporários da legislação nacional considerada incompatível com a legislação da UE. Decidiu que os tribunais nacionais não podem aplicar uma disposição no direito nacional que os habilite a limitar os efeitos temporários de uma declaração de ilegalidade exigida nos termos deste direito. Isto foi com base no princípio da prevalência da UE, que estabelece a superioridade da legislação da UE sobre as leis dos Estados-Membros. Entretanto, o TJUE também decidiu que cabe ao direito nacional determinar as regras relativas à admissibilidade e avaliação das informações obtidas por meio da retenção de dados em violação da legislação da UE, em processos penais contra pessoas suspeitas [p. 53]. Ainda, os tribunais penais nacionais têm a obrigação de ignorar informações ou provas obtidas por meio da retenção geral ou indiscriminada de dados de tráfego e localização em violação da legislação da UE, quando pessoas suspeitas de terem cometido crimes não podem comentar de maneira eficaz em relação a tais informações (com base no princípio da eficácia). Desta forma, o TJUE também respondeu à pergunta final de forma negativa.

ORIENTAÇÃO DA DECISÃO

Expansão da liberdade de expressão

A vigilância em massa tem um efeito intimidador sobre a liberdade de expressão. A decisão do TJUE neste processo é um passo significativo nos esforços de proteção dos direitos fundamentais à liberdade de expressão e manifestação na União Europeia. Nos quatro processos, o Tribunal utilizou a análise "rigorosa" como norma para a ação legislativa, o que exige que os Estados-Membros realizem a coleta e retenção de dados para atender apenas a interesses estatais imperiosos, sem qualquer relação com a supressão de ideias. O processo reafirma que a troca de ideias e o livre exercício da expressão são valores positivos e importantes, não apenas para aqueles que exercem os direitos, mas para toda a sociedade.

PERSPECTIVA GLOBAL

Leis internacionais e regionais correlatas

- **TJUE, Tele2 Sverige AB vs. Post-och telestyrelsen, Secretaria de Estado do Ministério do Interior vs. Watson, Processos apensos C 203/15 e C 698/15 (2016)**
- **TEDH, Comissão vs. Hungria (Transparência das Associações) (2020), C-78/18.**
- **TEDH, K.U. vs. Finlância (2008), pedido nº 2872/02.**

- **TEDH, Von Hannover vs. Alemanha (2004), pedido nº 59320/00.**
- **TEDH, M.C. vs. Bulgária (2004), pedido nº 39272/98.**
- **TEDH, Osman vs. Reino Unido (1998), pedido nº 87/1997/871/1083.**
- **TEDH, El-Masri vs. "A antiga República Jugoslava da Macedónia" (2012), pedido nº 39630/09.**
- **TEDH, Medvedye vs. França (2010), pedido nº 3394/03.**
- **TEDH, Ladent vs. Polônia (2008), pedido nº 11036/03.**
- **TJUE, Comissão vs. Hungria (Direitos de usufruto sobre terras agrícolas) (2019), C-235/17, EU:C:2019:432.**
- **TJUE, Rayonna prokuratura Lom (2019), C-467/18, EU:C:2019:765.**
- **TJUE, Direitos Digitais (2014), C-293/12 e C-594/12, EU:C:2014:238.**
- **TJUE, Volker und Markus Schecke e Eifert (2010), C-92/09 e C-93/09, EU:C:2010:662.**
- **TJUE, Satakunnan Markkinapörssi e Satamedia (2008), C-73/07, EU:C:2008:727.**
- **TJUE, Ministério Fiscal (2018), C-207/16, EU:C:2018:788.**
- **TJUE, Facebook Irlanda e Schrems (2020), C-311/18, EU:C:2020:55.**
- **TEDH, Ben Faiza vs. França (2018), pedido nº 31446/12.**
- **TJUE, SNB-REACT (2018), C-521/17, EU:C:2018:639.**
- **TJUE, Mc Fadden (2016), C-484/14, EU:C:2016:689.**
- **TJUE, SABAM (2012), C-360/10, EU:C:2012:85.**
- **TJUE, Scarlet Extended (2011), C-70/10, EU:C:2011:771.**
- **TJUE, Österreichischer Rundfunk e outros (2003), C-465/00, C-138/01 e C-139/01, EU:C:2003:294.**
- **TJUE, Skype Communications (2019), C-142/18, EU:C:2019:460.**
- **TJUE, Popławski (2019), C-573/17,EU:C:2019:530.**
- **TJUE, Melki e Abdeli (2010), C-188/10 e C-189/10, EU:C:2010:363.**
- **TJUE, A. K. e outros (Independência da Câmara Disciplinar do Tribunal Superior) (2019), C-585/18, C-624/18 e C-625/18, EU:C:2019:982.**
- **TJUE, Flaminio Costa vs. E.N.E.L. (1964), Processo 6/64, EU:C:1964:66.**
- **TJUE, Inter-Environnement Wallonie e BeterLeefmilieu Vlaanderen (2019), C-411/17, EU:C:2019:622.**
- **TJUE, A e outros (Turbinas eólicas em Aalter e Nevele) (2020), C-24/19, EU:C:2020:503.**
- **TJUE, Nelson e outros (2020), C-581/10 e C-629/10, EU:C:2012:657.**

SIGNIFICÂNCIA DO CASO

A decisão estabelece um precedente vinculante ou persuasivo dentro de sua jurisdição

Decisão (incluindo votos vencedores e vencidos) estabelece influente ou persuasivo precedente fora de sua jurisdição

DOCUMENTOS OFICIAIS DO CASO

Documentos oficiais do caso:

- **Sentença (inglês)**
- **Parecer do AG sobre o C-511/18 - 512/18 15 de janeiro de 2020**
- **Parecer do AG sobre o C-520/18 15 de janeiro de 2020**
- **Parecer do AG sobre o C-623/17**

ANEXOS

Reportagens, análises e artigos jornalísticos:

- **EU's top court blocks states from gathering user data for surveillance**
- **Press release: Ruling by EU's highest court finds that UK, French and Belgian mass surveillance regimes must respect privacy, even in the context of national security**
- **Q&A: EU's top court rules that UK, French and Belgian mass surveillance regimes must respect privacy**