

RECOMENDAÇÕES

RECOMENDAÇÃO (UE) 2018/334 DA COMISSÃO

de 1 de março de 2018

sobre medidas destinadas a combater eficazmente os conteúdos ilegais em linha

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 292.º,

Considerando o seguinte:

- (1) A Internet e os prestadores de serviços ativos na Internet contribuem de forma significativa para a inovação, o crescimento económico e a criação de emprego na União. Muitos desses prestadores de serviços desempenham um papel essencial na economia digital, ligando empresas e cidadãos e facilitando o debate público e a distribuição e receção de informações factuais, de opiniões e de ideias. No entanto, em determinados casos, os seus serviços são utilizados de forma abusiva por terceiros para atividades ilegais em linha, por exemplo para divulgação de determinadas informações relacionadas com o terrorismo, o abuso sexual de crianças, o incitamento ilegal ao ódio em linha ou infrações à legislação de defesa do consumidor, o que pode prejudicar a confiança dos utilizadores e lesar os seus modelos de negócio. Em determinados casos, os prestadores de serviços podem inclusivamente extrair algumas vantagens desse tipo de atividades, por exemplo como consequência da disponibilidade de conteúdos protegidos por direitos de autor sem autorização dos titulares dos direitos.
- (2) A presença de conteúdos ilegais em linha tem sérias consequências negativas para os utilizadores, para outras empresas e cidadãos afetados e para a sociedade em geral. Tendo em conta o papel central que desempenham e as capacidades e meios tecnológicos relacionados com os serviços que fornecem, os prestadores de serviços em linha têm uma responsabilidade social particular de ajudar a combater os conteúdos ilegais difundidos através da utilização dos seus serviços.
- (3) Uma vez que a remoção rápida ou a impossibilitação do acesso a conteúdos ilegais é muitas vezes essencial para limitar uma mais ampla difusão e maiores danos, essas responsabilidades implicam, designadamente, que os prestadores dos serviços possam tomar decisões rápidas quanto a eventuais ações no que respeita aos conteúdos ilegais em linha. Estas responsabilidades implicam também que os prestadores de serviços devam pôr em prática salvaguardas eficazes e apropriadas, sobretudo tendo em vista assegurar que atuam de forma diligente e proporcionada e impedir a remoção não intencional de conteúdos que são legais.
- (4) Muitos prestadores de serviços em linha tomaram conhecimento dessas responsabilidades e agiram em conformidade. A nível coletivo, registaram-se importantes progressos graças a acordos voluntários de vários tipos, incluindo o Fórum Internet da UE sobre os conteúdos terroristas em linha, o Código de Conduta sobre incitação ilegal ao ódio na Internet e o Memorando de Entendimento sobre a venda de produtos de contrafação na Internet. Contudo, não obstante este empenhamento e os progressos registados, os conteúdos ilegais em linha continuam a ser um grave problema na União.
- (5) Preocupado com uma série de atentados terroristas na UE e com a proliferação de propaganda terrorista em linha, o Conselho Europeu de 22 e 23 de junho de 2017 declarou que «espera que o setor ... desenvolva novas tecnologias e novos instrumentos a fim de melhorar a deteção automática e a supressão de conteúdos que incitem a atos terroristas. ...». O Parlamento Europeu, na sua Resolução de 15 de junho de 2017, instou as outras plataformas em linha «a reforçarem as medidas destinadas a combater os conteúdos ilegais e lesivos em linha». O convite às empresas no sentido de adotarem uma abordagem mais proativa para proteger os seus utilizadores de conteúdos terroristas foi reiterado pelos Ministros dos Estados-Membros, no âmbito do Fórum Internet da UE. No que diz respeito aos direitos de propriedade intelectual, nas suas Conclusões de 4 de dezembro de 2014 sobre a aplicação desses direitos, o Conselho convidou a Comissão a ponderar a utilização dos instrumentos disponíveis para identificar os autores de violações dos direitos de propriedade intelectual e o papel dos intermediários na colaboração na luta contra as violações dos direitos de propriedade intelectual.

- (6) Em 28 de setembro de 2017, a Comissão adotou uma Comunicação com orientações sobre a responsabilidade dos prestadores de serviços em linha de conteúdos ilegais em linha ⁽¹⁾. Nessa comunicação, a Comissão explicou que iria apreciar se eram necessárias medidas suplementares, nomeadamente através do acompanhamento dos progressos com base em medidas voluntárias. A presente recomendação dá seguimento a essa comunicação, refletindo o nível de ambição indicado na mesma e dando-lhe execução, tendo simultaneamente em conta e baseando-se nos importantes progressos alcançados graças a essas medidas voluntárias.
- (7) A presente recomendação reconhece que devem ser tidas em conta as especificidades de tratamento dos diferentes tipos de conteúdos ilegais em linha, bem como as respostas específicas que podem ser necessárias, inclusivamente através de medidas legislativas específicas. A título de exemplo, reconhecendo a necessidade de adotar medidas legislativas específicas, em 25 de maio de 2016 a Comissão adotou uma proposta de alteração da Diretiva 2010/13/UE do Parlamento Europeu e do Conselho ⁽²⁾, para a adaptar à evolução das realidades do mercado. Em 14 de setembro de 2016, a Comissão adotou igualmente uma proposta de diretiva relativa aos direitos de autor no mercado único digital ⁽³⁾, que prevê a obrigação para determinados prestadores de serviços, em cooperação com os titulares de direitos, de tomar medidas que assegurem o funcionamento dos acordos celebrados com esses titulares relativos à utilização das suas obras ou outro material protegido, ou que impeçam a colocação à disposição nos seus serviços de obras ou outro material protegido identificado pelos titulares de direitos através da cooperação com os prestadores de serviços. A presente recomendação não afeta essas propostas e medidas legislativas.
- (8) A Diretiva 2000/31/CE do Parlamento Europeu e do Conselho ⁽⁴⁾ prevê algumas isenções de responsabilidade que, em determinadas condições, de que podem beneficiar alguns prestadores de serviços em linha, incluindo os prestadores de serviços de armazenagem em servidor, na aceção do artigo 14.º. A fim de beneficiar da isenção de responsabilidade, os prestadores de serviços de armazenagem em servidor devem proceder com diligência no sentido de remover ou impossibilitar o acesso às informações ilegais que tenham armazenado a partir do momento em que tenham conhecimento efetivo desse facto e, no que diz respeito a ações de indemnização, a partir do momento em que a informação ou a atividade ilegal seja evidente. Podem ter conhecimento e sensibilidade desse facto, nomeadamente através de notificações que recebam. A Diretiva 2000/31/CE constitui, enquanto tal, a base para a elaboração de procedimentos destinados a retirar e impossibilitar o acesso às informações ilegais. A diretiva prevê igualmente a possibilidade de os Estados-Membros exigirem que os prestadores de serviços em causa observem um dever de diligência no que respeita aos conteúdos ilegais que possam armazenar.
- (9) Ao tomar medidas em matéria de conteúdos ilegais em linha, os Estados-Membros devem respeitar o princípio do país de origem previsto na Diretiva 2000/31/CE. Por conseguinte, os Estados-Membros não podem, por razões que relevem do domínio coordenado, como especificado na diretiva, restringir a liberdade de prestação de serviços da sociedade da informação pelos prestadores estabelecidos noutro Estado-Membro, sob reserva de eventuais derrogações ao abrigo de determinadas condições estabelecidas nessa diretiva.
- (10) Além disso, vários outros atos do direito da União preveem um quadro jurídico para alguns tipos de conteúdos ilegais que estão acessíveis e são divulgados em linha. Em especial, a Diretiva 2011/93/UE do Parlamento Europeu e do Conselho ⁽⁵⁾ requer que os Estados-Membros tomem medidas para retirar páginas Web que contenham ou difundam pornografia infantil, e permitindo-lhes bloquear o acesso a essas páginas Web, sob reserva de determinadas garantias. A Diretiva (UE) 2017/541 do Parlamento Europeu e do Conselho, ⁽⁶⁾ que deve ser transposta para os direitos nacionais até 8 de setembro de 2018, inclui disposições semelhantes em matéria de conteúdos em linha que constituem um incitamento público à prática de infrações terroristas. A Diretiva (UE) 2017/541 também estabelece normas mínimas para a definição de infrações penais no domínio de infrações terroristas, infrações relacionadas com um grupo terrorista e infrações relacionadas com atividades terroristas. Nos

⁽¹⁾ COM(2017) 555 final de 28 de setembro de 2017.

⁽²⁾ Diretiva 2010/13/UE do Parlamento Europeu e do Conselho de 10 de março de 2010, relativa à coordenação de certas disposições legislativas, regulamentares e administrativas dos Estados-Membros respeitantes à oferta de serviços de comunicação social audiovisual (Diretiva Serviços de Comunicação Social Audiovisual) (JO L 95 de 15.4.2010, p. 1). COM(2016) 287 final.

⁽³⁾ COM(2016) 593 final de 14 de setembro de 2016.

⁽⁴⁾ Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio eletrónico») (JO L 178 de 17.7.2000, p. 1).

⁽⁵⁾ Diretiva 2011/93/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho (JO L 335 de 17.12.2011, p. 1).

⁽⁶⁾ Diretiva (UE) 2017/541 do Parlamento Europeu e do Conselho, de 15 de março de 2017, relativa à luta contra o terrorismo e que substitui a Decisão-Quadro 2002/475/JAI do Conselho e altera a Decisão 2005/671/JAI do Conselho (JO L 88 de 31.3.2017, p. 6).

termos da Diretiva 2004/48/CE do Parlamento Europeu e do Conselho ⁽¹⁾, é possível as autoridades judiciais competentes decretarem medidas inibitórias contra intermediários cujos serviços estejam a ser utilizados por um terceiro para violar um direito de propriedade intelectual.

- (11) Em especial neste contexto, para além das medidas voluntárias tomadas por determinados prestadores de serviços em linha, alguns Estados-Membros adotaram normas sobre os mecanismos de notificação e ação desde a adoção da Diretiva 2000/31/CE. Outros Estados-Membros estão a considerar a hipótese de adotar normas dessa natureza. Esses mecanismos, de um modo geral, procuram facilitar a notificação de conteúdos, que a parte notificante considera ilegais, ao fornecedor de serviços de armazenagem em servidor em causa («notificação»), por força da qual o fornecedor pode decidir se concorda ou não com a avaliação e se pretende remover ou impossibilitar o acesso a esse conteúdo («ação»). Há cada vez mais diferenças entre as normas nacionais neste domínio. Em consequência, os prestadores de serviços em questão podem ser sujeitos a uma série de requisitos legais que são diferentes em termos de conteúdo e de âmbito de aplicação.
- (12) No interesse do mercado interno e da eficácia do combate aos conteúdos ilegais em linha, e a fim de garantir a abordagem equilibrada que a Diretiva 2000/31/CE visa garantir, é necessário definir determinados princípios de base que devem orientar a ação dos Estados-Membros e dos prestadores de serviços em causa a este respeito.
- (13) Esses princípios devem ser definidos e aplicados no pleno respeito dos direitos fundamentais protegidos na ordem jurídica da União e, em especial, os garantidos na Carta dos Direitos Fundamentais da União Europeia (a seguir designada «Carta»). Os conteúdos ilegais em linha devem ser combatidos com garantias sólidas e adequadas, de modo a proteger os diferentes direitos fundamentais em causa de todas as partes envolvidas. Estes direitos incluem, consoante o caso, a liberdade de expressão, nomeadamente a liberdade de receber e partilhar informações, o direito ao respeito da vida privada e à proteção dos dados pessoais, bem como o direito a uma proteção judicial efetiva dos utilizadores dos serviços em causa. Podem ainda incluir a liberdade de empresa, incluindo a liberdade contratual, de prestadores de serviços de armazenagem em servidor, bem como os direitos da criança e os direitos de proteção da propriedade, incluindo a propriedade intelectual, a dignidade do ser humano e a não discriminação de determinadas outras partes afetadas. Em especial, as decisões adotadas pelos prestadores de serviços de armazenagem em servidor para remover ou impossibilitar o acesso a conteúdos que armazenam devem ter devidamente em conta os direitos fundamentais e os interesses legítimos dos seus utilizadores, bem como o papel central que os prestadores normalmente desempenham no sentido de facilitar o debate público e a divulgação e receção de factos, opiniões e ideias em conformidade com a lei.
- (14) Em conformidade com a abordagem horizontal subjacente à isenção de responsabilidade prevista no artigo 14.º da Diretiva 2000/31/CE, a presente recomendação deve ser aplicada a qualquer tipo de conteúdos não conformes com o direito da União ou dos Estados-Membros, independentemente do objeto concreto ou da natureza dessas legislações. Basta ter em conta as legislações dos Estados-Membros relativas à prestação de serviços em causa, designadamente as legislações dos Estados-Membros em cujo território está estabelecido o fornecedor de serviços de armazenagem em servidor ou no qual os serviços são prestados. Além disso, ao dar execução à presente recomendação, devem ser tidos em conta a gravidade e qualquer tipo de danos potenciais causados por conteúdos ilegais, que podem estar estreitamente relacionados com a celeridade das medidas tomadas e do que pode ser razoavelmente esperado dos prestadores de serviços de armazenagem em servidor, considerando, se for caso disso, o estado de desenvolvimento e a possível utilização de tecnologias. Devem também ser tidas em devida conta as diferenças que possam existir entre os diferentes tipos de conteúdos ilegais e as medidas a tomar para os contrariar.
- (15) Os prestadores de serviços de armazenagem em servidor desempenham um papel particularmente importante no combate aos conteúdos ilegais em linha, na medida em que armazenam informação fornecida pelos seus utilizadores e a pedido dos mesmos, e autorizam outros utilizadores a aceder a essa informação, muitas vezes em grande escala. Por conseguinte, a presente recomendação refere-se sobretudo às atividades e responsabilidades desses prestadores. No entanto, se for caso disso, as recomendações feitas podem igualmente ser aplicadas, *mutatis mutandis*, a outros prestadores de serviços em linha afetados. Uma vez que o objetivo da presente recomendação consiste em abordar os riscos relacionados com conteúdos ilegais em linha que afetam os consumidores na União, a mesma está relacionada com as atividades de todos os prestadores de serviços de armazenagem em servidor, independentemente de estarem ou não estabelecidos na União ou num país terceiro, desde que as suas atividades se destinem aos consumidores que residem na União.
- (16) Os mecanismos de notificação aos prestadores de serviços de armazenagem em servidor de conteúdos considerados ilegais são um instrumento importante para combater os conteúdos ilegais em linha. Esses

⁽¹⁾ Diretiva 2004/48/CE do Parlamento Europeu e do Conselho de 29 de abril de 2004 relativa ao respeito dos direitos de propriedade intelectual (JO L 157 de 30.4.2004, p. 45).

mecanismos devem facilitar a notificação por parte de todas as pessoas e entidades que pretendam fazê-lo. Por conseguinte, devem ser de fácil acesso e utilização por todos os utilizadores. No entanto, os prestadores de serviços de armazenagem em servidor devem ser flexíveis, por exemplo quanto ao formato ou tecnologia a utilizar, a fim de permitir soluções eficazes e evitar encargos desproporcionados a esses prestadores de serviços.

- (17) Em conformidade com a jurisprudência do Tribunal de Justiça relativa ao artigo 14.º da Diretiva 2000/31/CE, as notificações devem ser suficientemente precisas e devidamente fundamentadas de modo a permitir ao prestador de serviços de armazenagem em servidor que as recebe tomar uma decisão informada e diligente no que respeita ao seguimento a dar à notificação. Por conseguinte, e na medida do possível, há que garantir que este requisito é preenchido. No entanto, se determinada notificação tiver como resultado o conhecimento ou alerta para uma ilicitude, na aceção do artigo 14.º dessa diretiva, deve ser apreciada em função das especificidades do caso em apreço, tendo em conta que esse conhecimento também pode ser obtido de outras formas que não sejam notificações.
- (18) Em geral, não é necessário ter os dados de contacto do autor da notificação para que o prestador de serviços de armazenagem em servidor possa tomar uma decisão informada e diligente sobre o seguimento a dar à notificação recebida. Tornar obrigatório o fornecimento dos dados de contacto para a apresentação de uma notificação implicaria um entrave a esta última. No entanto, a inclusão dos dados de contacto é necessária para que o prestador de serviços possa dar informações de retorno. Por conseguinte, deve ser ponderada a possibilidade de incluir os dados de contacto do autor da notificação, sem que tal seja exigível.
- (19) A fim de aumentar a transparência e a exatidão dos mecanismos de notificação e ação, bem como permitir a correção quando tal seja necessário, os prestadores de serviços de armazenagem em servidor, quando estão na posse de informações de autores de notificações e/ou fornecedores de conteúdos, devem informar atempada e adequadamente essas pessoas sobre as medidas tomadas no âmbito dos referidos mecanismos, em especial no que respeita às suas decisões sobre o pedido para remover ou impossibilitar o acesso ao conteúdo em causa. As informações a fornecer devem ser proporcionadas, o que significa que devem corresponder aos contributos feitos pelas pessoas em causa nas suas notificações ou contranotificações, permitindo simultaneamente encontrar soluções adequadas e diferenciadas sem constituir um encargo excessivo para os fornecedores.
- (20) A fim de garantir a transparência e a equidade e evitar a remoção involuntária de conteúdos que são legais, os fornecedores de conteúdos devem, por uma questão de princípio, ser informados da decisão de remover ou impossibilitar o acesso a conteúdos armazenados a seu pedido, devendo ser-lhes dada a possibilidade de contestar a decisão através de uma contranotificação com vista à anulação da referida decisão quando tal for adequado, independentemente do facto de essa decisão ter sido tomada com base numa notificação ou numa sinalização, ou em conformidade com medidas proativas pelo prestador de serviços de armazenagem em servidor.
- (21) No entanto, tendo em conta a natureza do conteúdo em causa, o objetivo desse procedimento de contranotificação e os encargos adicionais que tal implica para os prestadores de serviços de armazenagem em servidor, não há justificação para recomendar a prestação de informação sobre essa decisão e a possibilidade de contestar a decisão sempre que é manifesto que o conteúdo em questão é um conteúdo ilegal e diz respeito a infrações penais graves que envolvem uma ameaça para a vida ou a segurança de pessoas, como é o caso das infrações especificadas na Diretiva (UE) 2017/541 e na Diretiva 2011/93/UE. Além disso, em determinados casos, razões de ordem pública e de segurança pública, nomeadamente motivos relacionados com a prevenção, investigação, deteção e repressão de infrações penais, podem justificar o facto de não serem prestadas diretamente essas informações ao fornecedor de conteúdos em causa. Por conseguinte, os prestadores de serviços de armazenagem em servidor não devem fazê-lo quando a autoridade competente tiver apresentado um pedido nesse sentido, com base em razões de ordem pública e de segurança pública, desde que a autoridade o tenha feito por esses motivos. Na medida em que este procedimento comporta uma limitação do direito de ser informado em relação ao tratamento de dados pessoais, as condições aplicáveis estabelecidas no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ⁽¹⁾ devem ser respeitadas.
- (22) Os mecanismos de notificação e ação não devem de modo algum afetar os direitos das partes envolvidas de intentar uma ação judicial, em conformidade com a legislação aplicável, no que diz respeito a conteúdos considerados ilegais ou a medidas tomadas a este respeito pelos prestadores de serviços de armazenagem em servidor. Os mecanismos de resolução extrajudicial de litígios que surjam neste contexto podem ser um importante complemento dos processos judiciais, nomeadamente quando permitem uma resolução efetiva, acessível e célere desses litígios. Por esse motivo, deve ser incentivada a resolução extrajudicial de litígios, desde que os mecanismos em causa satisfaçam determinados critérios, nomeadamente em termos de equidade processual, que o acesso das partes aos tribunais não seja afetado e que sejam evitados abusos.

⁽¹⁾ 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 (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

- (23) A fim de avaliar melhor a eficácia dos mecanismos de notificação e ação e de outras atividades dos prestadores de serviços de armazenagem em servidor em relação a conteúdos considerados ilegais e de garantir a responsabilização, deve ser assegurada a transparência perante o público em geral. Por conseguinte, os prestadores de serviços de armazenagem em servidor devem publicar regularmente relatórios sobre estes mecanismos e sobre outras atividades, que devem ser suficientemente completos e detalhados para permitir um conhecimento adequado da questão. Devem também prever clareza *ex ante*, nas suas condições de utilização, sobre as respetivas disposições para remover ou impossibilitar o acesso a quaisquer conteúdos que armazenam, incluindo conteúdos ilegais.
- (24) Para além dos mecanismos de notificação e ação, as medidas proporcionadas e específicas proativas tomadas voluntariamente pelos prestadores de serviços de armazenagem em servidor, incluindo através da utilização de meios automatizados em determinados casos, podem também ser um elemento importante na luta contra os conteúdos ilegais em linha, sem prejuízo do disposto no artigo 15.º, n.º 1, da Diretiva 2000/31/CE. Em ligação com essas medidas proativas, deve ser tida em conta a situação dos prestadores de serviços de armazenagem em servidor que, em virtude da dimensão ou da escala em que operam, dispõem de recursos e conhecimentos especializados limitados, bem como a necessidade de garantias efetivas e adequadas subjacentes a essas medidas.
- (25) Pode ser adequado tomar tais medidas proativas, em especial nos casos em que o caráter ilegal dos conteúdos já tenha sido estabelecido ou em que o tipo de conteúdo seja tal que essa contextualização não seja essencial. Pode também depender da natureza, dimensão e finalidade das medidas previstas, do tipo de conteúdo em questão, de o conteúdo ter sido ou não notificado às autoridades responsáveis pela aplicação da lei ou à Europol, de já terem sido tomadas medidas no que respeita ao conteúdo, bem como de já terem sido tomadas medidas em relação ao conteúdo por se considerar que se trata de um conteúdo ilegal. No que diz particularmente respeito a material de pornografia infantil, os prestadores de serviços de armazenagem em servidor devem tomar medidas proativas para detetar e impedir a difusão desse tipo de material, em conformidade com os compromissos assumidos no âmbito da Aliança Mundial contra o Abuso Sexual de Crianças na Internet.
- (26) Neste contexto, na sua Comunicação de 28 de setembro de 2017 relativa ao combate aos conteúdos ilegais em linha, a Comissão expôs o seu ponto de vista segundo o qual a adoção dessas medidas proativas voluntárias não implica automaticamente para o prestador de serviços de armazenagem em servidor a perda do benefício da isenção de responsabilidade prevista no artigo 14.º da Diretiva 2000/31/CE.
- (27) É essencial que as eventuais medidas para combater os conteúdos ilegais em linha estejam sujeitas a garantias efetivas e adequadas, a fim de assegurar que os prestadores de serviços de armazenagem em servidor atuam de forma diligente e proporcionada ao definir e aplicar as suas disposições relativamente a quaisquer conteúdos que armazenam, incluindo conteúdos ilegais, de forma a garantir, em particular, que os utilizadores podem livremente receber e partilhar informações em linha, em conformidade com a legislação aplicável. Para além das garantias previstas na legislação aplicável, por exemplo no que diz respeito à proteção dos dados pessoais, devem ser previstas e aplicadas garantias especiais, nomeadamente controlos e verificações humanos, sempre que necessário em relação à utilização de dispositivos automatizados, a fim de evitar decisões involuntárias e erradas.
- (28) Deve ser assegurada uma cooperação harmoniosa, efetiva e adequada entre as autoridades competentes e os prestadores de serviços de armazenagem em servidor na luta contra os conteúdos ilegais em linha. Essa cooperação deve beneficiar da assistência da Europol quando for adequado, por exemplo no âmbito do combate ao terrorismo, aos abusos sexuais e à exploração sexual de crianças, à pornografia infantil e ao aliciamento de crianças. Tendo em vista facilitar essa cooperação, os Estados-Membros e os prestadores de serviços de armazenagem em servidor devem designar pontos de contacto, devendo igualmente ser estabelecidos procedimentos para o processamento de notificações apresentadas por essas autoridades como uma questão prioritária e com um nível adequado de confiança quanto à sua exatidão, tendo em conta as competências específicas e as responsabilidades dessas autoridades. A fim de lutar eficazmente contra determinadas infrações penais particularmente graves, como as especificadas na Diretiva (UE) 2017/541 e na Diretiva 2011/93/UE, que podem chegar à atenção dos prestadores de serviços de armazenagem em servidor no decorrer das suas atividades, os Estados-Membros devem ser incentivados a fazer uso da possibilidade prevista no artigo 15.º, n.º 2, da Diretiva 2000/31/CE, de estabelecer obrigação legal de prestação de informações, em conformidade com a legislação aplicável, designadamente o Regulamento (UE) 2016/679.
- (29) Para além das autoridades competentes, determinadas pessoas ou entidades, incluindo organizações não governamentais e associações comerciais, podem igualmente ter competências específicas e querer assumir, numa base voluntária, determinadas responsabilidades relacionadas com a luta contra os conteúdos ilegais em linha. Tendo em conta o seu valor acrescentado e o número, por vezes elevado, de notificações, deve ser incentivada a cooperação entre os prestadores de serviços de armazenagem em servidor e os sinalizadores de confiança, em especial tratando prioritariamente as notificações que estes apresentam e com um grau adequado de confiança no que se refere à sua exatidão. No entanto, em conformidade com o seu estatuto especial, essa cooperação deve

estar aberta apenas a pessoas e entidades que respeitem os valores em que se funda a União Europeia, tal como enunciados no artigo 2.º do Tratado da União Europeia, e que preencham determinadas condições adequadas, que devem também ser claras e objetivas e colocadas à disposição do público.

- (30) A luta contra os conteúdos ilegais em linha requer uma abordagem abrangente, uma vez que esses conteúdos muitas vezes migram facilmente de um prestador de serviços de armazenagem em servidor para outro e tendem a explorar os elos mais fracos da cadeia. Por conseguinte, é essencial que haja cooperação, numa base voluntária, em matéria de partilha de experiências, soluções tecnológicas e melhores práticas. Essa cooperação é particularmente importante em relação aos prestadores de serviços de armazenagem em servidor que, em virtude da sua dimensão ou da escala em que operam, dispõem de recursos e conhecimentos especializados limitados.
- (31) O terrorismo envolve a utilização ilegal e indiscriminada de violência e a intimidação dos cidadãos. Os terroristas estão cada vez mais dependentes da Internet para divulgar propaganda terrorista, utilizando frequentemente métodos sofisticados para garantir a sua rápida e ampla difusão. Apesar dos progressos registados, em particular no contexto do Fórum Internet da UE, continua a haver a necessidade urgente de uma resposta mais rápida e mais eficaz aos conteúdos terroristas em linha, para além da necessidade de os prestadores de serviços de armazenagem em servidor que participam no Fórum Internet da UE cumprirem integralmente os seus compromissos relativos à comunicação efetiva e exaustiva de informações.
- (32) Tendo em conta as especificidades inerentes à luta contra os conteúdos terroristas em linha, as recomendações relativas à luta contra os conteúdos ilegais em geral deve ser complementada por determinadas recomendações que dizem especificamente respeito ao combate aos conteúdos terroristas em linha, baseando-se nos esforços empreendidos e consolidados no contexto do Fórum Internet da UE.
- (33) Considerando os riscos particularmente graves associados a conteúdos terroristas e ao papel central dos prestadores de serviços de armazenagem em servidor na difusão de tais conteúdos, esses prestadores devem tomar todas as medidas razoáveis para impedir os conteúdos terroristas e, se possível, impedir a sua armazenagem, sob reserva da possibilidade de definir e impor as suas condições de prestação dos serviços e a necessidade de assegurar garantias efetivas e adequadas, sem prejuízo do disposto no artigo 14.º da Diretiva 2000/31/CE.
- (34) Essas medidas devem, em especial, consistir na cooperação com as autoridades competentes e a Europol em matéria de sinalizações, que são um método específico de notificação dos prestadores de serviços de armazenagem em servidor adaptado à especificidade da luta contra os conteúdos terroristas. As autoridades competentes e a Europol, ao apresentarem sinalizações, devem poder solicitar a remoção ou a impossibilitação do acesso a conteúdos que considerem de natureza terrorista, quer com referência à legislação aplicável relevante ou às condições de serviço do prestador de serviços de armazenagem em servidor em causa. Esses mecanismos de sinalização devem existir juntamente com os mecanismos para a apresentação de notificações, incluindo por parte dos sinalizadores de confiança, podendo igualmente ser utilizados para notificar conteúdos considerados de natureza terrorista.
- (35) Tendo em conta que os conteúdos terroristas são geralmente mais prejudiciais na primeira hora em que estão em linha, e dados os conhecimentos especializados e as responsabilidades específicas das autoridades competentes e da Europol, as sinalizações devem, regra geral, ser avaliadas e executadas no prazo de uma hora, se for apropriado.
- (36) Essas medidas para combater conteúdos terroristas devem também consistir em medidas proativas proporcionadas e específicas, incluindo o recurso a meios automatizados, a fim de detetar, identificar e remover ou impossibilitar rapidamente o acesso a tais conteúdos e garantir que não reaparecem, sem prejuízo do disposto no artigo 15.º, n.º 1, da Diretiva 2000/31/CE. Neste contexto, deverá ser tida em conta a necessidade de garantias apropriadas e eficazes de acompanhamento de tais medidas, nomeadamente as recomendadas no capítulo II da presente recomendação.
- (37) A cooperação entre os prestadores de serviços de armazenagem em servidor, bem como entre estes e as autoridades competentes, é da maior importância quando se procura combater conteúdos terroristas em linha. Em especial, as ferramentas tecnológicas que permitem a deteção automática de conteúdos, tais como a base de dados de valores de dispersão (*database of hashes*), podem ajudar a alcançar o objetivo de impedir a difusão de conteúdos terroristas em diferentes serviços de armazenagem em servidor. Tal cooperação, bem como o desenvolvimento, a exploração e a partilha dessas ferramentas tecnológicas, devem ser incentivados, recorrendo aos conhecimentos especializados da Europol quando tal for pertinente. Esses esforços de cooperação são particularmente importantes para ajudar os prestadores de serviços de armazenagem em servidor que, em virtude da sua dimensão ou da escala em que exercem a sua atividade, têm recursos e conhecimentos especializados limitados para responder de forma eficaz e urgente a sinalizações e tomar medidas proativas, como recomendado.

- (38) O maior número possível de prestadores de serviços de armazenagem em servidor deve aderir a estes esforços de cooperação e todos estes prestadores devem contribuir para otimizar e maximizar a utilização dessas ferramentas. Deve também ser incentivada a celebração de acordos de cooperação entre todas as partes interessadas, incluindo, se for caso disso, a Europol, uma vez que tais acordos podem ajudar a garantir uma abordagem coerente e efetiva e permitir o intercâmbio de experiências e de conhecimentos especializados.
- (39) A fim de garantir o respeito pelo direito fundamental à proteção das pessoas singulares relativamente ao tratamento de dados pessoais, bem como à livre circulação desses dados, o tratamento de dados pessoais no contexto das medidas tomadas para dar cumprimento à presente recomendação deve estar em plena conformidade com as normas relativas à proteção dos dados, nomeadamente com o Regulamento (UE) 2016/679 e a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho ⁽¹⁾, devendo esse tratamento de dados ser acompanhado pelas autoridades de supervisão competentes.
- (40) A presente recomendação respeita os direitos fundamentais e observa os princípios reconhecidos em particular pela Carta. Em especial, a presente recomendação procura assegurar o respeito integral dos artigos 1.º, 7.º, 8.º, 10.º, 11.º, 16.º, 17.º, 21.º, 24.º e 47.º da Carta.
- (41) A Comissão tenciona acompanhar de perto as medidas tomadas em resposta à presente recomendação. Os Estados-Membros e os prestadores de serviços de armazenagem em servidor devem, por conseguinte, estar preparados para apresentar à Comissão, a pedido desta, todas as informações pertinentes que se espera possam fornecer com o objetivo de possibilitar esse acompanhamento. Com base nas informações assim obtidas, bem como em todas as outras informações disponíveis, incluindo a elaboração de relatórios baseados em vários acordos voluntários, a Comissão irá avaliar os efeitos da presente recomendação e determinar a necessidade de tomar medidas adicionais, inclusive propondo atos jurídicos vinculativos da União. Dadas as especificidades e a urgência de combater conteúdos terroristas em linha, o acompanhamento e a avaliação devem ser efetuados com base em informações pormenorizadas e de forma particularmente rápida, no prazo de três meses a contar da data de publicação da presente recomendação, enquanto para outros conteúdos ilegais é conveniente fazê-lo no prazo de seis meses após a referida publicação,

ADOTOU A PRESENTE RECOMENDAÇÃO:

CAPÍTULO I

Objetivo e terminologia

1. Os Estados-Membros e os prestadores de serviços de armazenagem em servidor, em relação a conteúdos fornecidos por fornecedores de conteúdos que aqueles armazenam a pedido destes últimos, são incentivados a tomar medidas efetivas, adequadas e proporcionadas para combater os conteúdos ilegais em linha, de acordo com os princípios estabelecidos na presente recomendação e em plena conformidade com a Carta, em especial o direito à liberdade de expressão e de informação, e com outras disposições aplicáveis do direito da União, em particular no que respeita à proteção dos dados pessoais, à concorrência e ao comércio eletrónico.
2. A presente recomendação tem por base e consolida os progressos realizados no âmbito dos acordos voluntários entre prestadores de serviços de armazenagem em servidor e outros prestadores de serviços em causa no que se refere aos diferentes tipos de conteúdos ilegais. No domínio do terrorismo, tem por base e consolida os progressos realizados no âmbito do Fórum Internet da UE.
3. A presente recomendação não prejudica os direitos e as obrigações dos Estados-Membros de adotarem medidas em matéria de conteúdos ilegais em linha, em conformidade com o direito da União, incluindo a possibilidade de os tribunais ou as autoridades administrativas dos Estados-Membros, em conformidade com as respetivas ordens jurídicas, exigirem que os prestadores de serviços de armazenagem em servidor removam ou impossibilitem o acesso a conteúdos ilegais. A presente recomendação não prejudica a posição dos prestadores de serviços de armazenagem em servidor nos termos da Diretiva 2000/31/CE e a sua possibilidade de estabelecer e fazer aplicar as suas condições de utilização, em conformidade com o direito da União e a legislação dos Estados-Membros.

⁽¹⁾ Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO L 119 de 4.5.2016, p. 89).

4. Para efeitos da presente recomendação, entende-se por:
- (a) «Prestador de serviços de armazenagem em servidor», um prestador de serviços da sociedade da informação cuja atividade consiste em armazenar informações prestadas pelo destinatário do serviço, a seu pedido, na aceção do artigo 14.º da Diretiva 2000/31/CE, independentemente do seu local de estabelecimento, que dirige as suas atividades aos consumidores que residem na União;
 - (b) «Conteúdo ilegal», qualquer informação que não esteja em conformidade com a legislação da União ou a legislação do Estado-Membro em questão;
 - (c) «Utilizador», qualquer pessoa singular ou coletiva que seja o destinatário dos serviços prestados por um prestador de serviços de armazenagem em servidor;
 - (d) «Fornecedor de conteúdos», um utilizador que tenha apresentado informação que é ou tenha sido armazenada a seu pedido por um prestador de serviços de armazenagem em servidor;
 - (e) «Notificação», qualquer comunicação dirigida a um prestador de serviços de armazenagem em servidor apresentada pelo autor de uma notificação em relação a conteúdos armazenados por esse prestador que o autor da notificação considere ilegais, solicitando a sua remoção ou impossibilitação por esse prestador de serviços de armazenagem em servidor numa base voluntária;
 - (f) «Autor da notificação», a pessoa singular ou entidade que tenha apresentado uma notificação a um prestador de serviços de armazenagem em servidor;
 - (g) «Sinalizador de confiança», a pessoa singular ou entidade considerada pelo prestador de serviços de armazenagem em servidor com competências específicas e responsabilidades para efeitos de luta contra os conteúdos ilegais em linha;
 - (h) «Conteúdo terrorista», qualquer informação cuja difusão constitua uma infração especificada na Diretiva (UE) 2017/541, ou uma infração terrorista definida na legislação do Estado-Membro em causa, incluindo a difusão de informações pertinentes emitidas por, ou imputáveis a, grupos terroristas ou entidades incluídas nas listas pertinentes estabelecidas pela União ou pelas Nações Unidas;
 - (i) «Autoridades de aplicação da lei», as autoridades competentes designadas pelos Estados-Membros, em conformidade com o seu direito nacional, para desempenhar missões de aplicação da lei para fins de prevenção, investigação, deteção ou repressão de infrações penais em relação a conteúdos ilegais em linha;
 - (j) «Autoridades competentes», as autoridades competentes designadas pelos Estados-Membros, em conformidade com o seu direito nacional, para desempenhar missões que incluem combater os conteúdos ilegais em linha, incluindo as autoridades de aplicação da lei e as autoridades administrativas encarregadas de fazer cumprir a lei, independentemente da natureza ou do objeto específico dessa lei, aplicável em determinados domínios específicos;
 - (k) «Sinalização», qualquer comunicação dirigida a um prestador de serviços de armazenagem em servidor apresentada por uma autoridade competente ou pela Europol em relação a conteúdos armazenados por esse prestador de serviços e que essa autoridade ou a Europol considere como conteúdos terroristas, solicitando a sua remoção ou impossibilitação do acesso por esse prestador de serviços numa base voluntária.

CAPÍTULO II

Recomendações gerais relativas a todos os tipos de conteúdos ilegais

Apresentação e tratamento das notificações

5. Devem ser previstos mecanismos para a apresentação de notificações. Esses mecanismos devem ser de fácil acesso, conviviais, e permitir a apresentação de notificações por meios eletrónicos.
6. Tais mecanismos devem prever e incentivar a apresentação de notificações que sejam suficientemente precisas e devidamente fundamentadas para que o prestador de serviços de armazenagem em causa possa tomar uma decisão informada e diligente no que respeita ao conteúdo da notificação, em especial se o conteúdo deve ser ou não considerado ilegal e ser removido ou impossibilitado o seu acesso. Esses mecanismos devem facilitar a apresentação de notificações com uma explicação das razões pelas quais o autor da notificação considera que o conteúdo é ilegal e uma indicação clara da localização desse conteúdo.

7. Os autores da notificação devem ter a possibilidade, mas não a obrigação, de incluir os respetivos dados de contacto na notificação. Caso decidam fazê-lo, deve ser garantido o seu anonimato face ao fornecedor de conteúdos.
8. Se os dados de contacto do autor da notificação forem do conhecimento do prestador de serviços de armazenagem em servidor, este deve enviar uma confirmação de receção ao autor da notificação e informá-lo sem demora e de forma proporcionada da sua decisão relativa ao conteúdo a que a notificação se refere.

Informação aos fornecedores de conteúdos e contranotificações

9. Sempre que um prestador de serviços de armazenagem em servidor decida remover ou impossibilitar o acesso a qualquer conteúdo que armazena por considerar que o mesmo é ilegal, independentemente dos meios utilizados para detetar, identificar, remover ou impossibilitar o acesso a esse conteúdo, e se os dados de contacto do fornecedor de conteúdos forem do conhecimento do prestador de serviços de armazenagem em servidor, o fornecedor de conteúdos deve ser informado sem demora e de forma proporcionada dessa decisão e dos motivos para a mesma, bem como da possibilidade de contestar a decisão referida no ponto 11.
10. Contudo, o ponto 9 não se aplica quando é manifesto que o conteúdo em causa é ilegal e diz respeito a infrações penais graves que envolvem uma ameaça contra a vida ou a segurança das pessoas. Além disso, os prestadores de serviços de armazenagem em servidor não devem fornecer as informações referidas nesse ponto quando e se uma autoridade competente o solicitar por razões de ordem pública e de segurança pública, nomeadamente para efeitos de prevenção, investigação, deteção e repressão de infrações penais.
11. Os fornecedores de conteúdos devem ter a possibilidade de contestar a decisão do prestador de serviços de armazenagem em servidor a que se refere o ponto 9 dentro de um prazo razoável, mediante transmissão de uma contranotificação a esse prestador de serviços. O mecanismo de transmissão de contranotificações deve ser de fácil utilização e permitir a transmissão por via eletrónica.
12. Os prestadores de serviços de armazenagem em servidor devem ter devidamente em conta eventuais contranotificação que recebam. Nos casos em que a contranotificação inclui motivos que levem o prestador de serviços de armazenagem em servidor a considerar que o conteúdo em causa não é ilegal, deve anular a sua decisão de remover ou impossibilitar o acesso a esse conteúdo sem demora injustificada, sem prejuízo da possibilidade de definir e aplicar as suas condições de utilização em conformidade com o direito da União e as legislações dos Estados-Membros.
13. O fornecedor de conteúdos que apresentou uma contranotificação, bem como o autor da notificação em questão, devem, sempre que os seus dados de contacto sejam do conhecimento do prestador de serviços de armazenagem em servidor em causa, ser informados, sem demora injustificada, da decisão que este prestador tiver tomado em relação a esse conteúdo.

Resolução extrajudicial de litígios

14. Os Estados-Membros são encorajados a facilitar, se for caso disso, a resolução extrajudicial de litígios relacionados com a remoção ou a impossibilitação do acesso a conteúdos ilegais. Quaisquer mecanismos de resolução extrajudicial de litígios deste tipo devem ser facilmente acessíveis, eficazes, transparentes e equitativos, assegurando uma resolução justa e conforme com o direito aplicável. As tentativas de resolução extrajudicial desse tipo de litígios não devem afetar o acesso aos tribunais das partes em causa.
15. Se estiverem disponíveis no Estado-Membro em causa, os prestadores de serviços de armazenagem em servidor são incentivados a autorizar o recurso a mecanismos de resolução extrajudicial de litígios.

Transparência

16. Os prestadores de serviços de armazenagem em servidor devem ser incentivados a publicar de forma clara, facilmente compreensível e suficientemente detalhada, explicações sobre as suas disposições no que respeita à remoção ou à impossibilitação do acesso aos conteúdos que armazenam, incluindo conteúdos considerados ilegais.
17. Os prestadores de serviços de armazenagem em servidor devem ser incentivados a publicar periodicamente, de preferência pelo menos uma vez por ano, relatórios sobre as suas atividades relativas à remoção e à impossibilitação de conteúdos considerados ilegais. Esses relatórios devem incluir, em especial, informações sobre a quantidade e o tipo de conteúdos removidos, sobre o número de notificações e contranotificações recebidas e o tempo necessário para tomar medidas.

Medidas proativas

18. Os prestadores de serviços de armazenagem em servidor devem ser encorajados a tomar, se for caso disso, medidas proporcionadas e específicas no que respeita aos conteúdos ilegais. Essas medidas podem incluir a utilização de dispositivos automatizados para a deteção de conteúdos ilegais somente quando seja necessário e proporcionado e sujeitas a garantias eficazes e adequadas, em especial as previstas nos pontos 19 e 20.

Garantias

19. A fim de evitar a remoção de conteúdos que não são ilegais, sem prejuízo da possibilidade de os prestadores de serviços de armazenagem em servidor definirem e aplicarem as suas condições de utilização em conformidade com o direito da União e as legislações dos Estados-Membros, devem ser previstas garantias efetivas e adequadas para assegurar que esses prestadores atuam de forma diligente e proporcionada em relação aos conteúdos que armazenam, em particular no que se refere ao tratamento de notificações e contranotificações e à decisão sobre a eventual remoção ou impossibilitação do acesso a conteúdos considerados ilegais.
20. Sempre que os prestadores de serviços de armazenagem em servidor utilizem dispositivos automatizados no que diz respeito aos conteúdos que armazenam, devem ser previstas garantias efetivas e adequadas para assegurar que as decisões tomadas relativamente a esses conteúdos, em especial as decisões de remover ou impossibilitar o acesso a conteúdos considerados ilegais, são exatas e devidamente fundamentadas. Essas salvaguardas devem consistir, nomeadamente, em controlos e verificações humanos, quando tal for adequado e, em todo o caso, quando é necessária uma avaliação pormenorizada do contexto pertinente para determinar se os conteúdos devem ser considerados ilegais.

Proteção contra comportamentos abusivos

21. Devem ser previstas disposições efetivas e adequadas para evitar a comunicação ou a tomada de medidas em relação a notificações ou contranotificações que tenham sido comunicadas de má-fé, bem como em relação a outras formas de práticas abusivas relacionadas com as medidas recomendadas para combater os conteúdos ilegais em linha como enunciado na presente recomendação.

Cooperação entre prestadores de serviços de armazenagem em servidor e Estados-Membros

22. Os Estados-Membros e os prestadores de serviços de armazenagem em servidor devem designar pontos de contacto para as questões relativas aos conteúdos ilegais em linha.
23. Devem ser previstos procedimentos acelerados para o tratamento das notificações enviadas pelas autoridades competentes.
24. Os Estados-Membros são incentivados a estabelecer obrigações jurídicas para que os prestadores de serviços de armazenagem em servidor informem rapidamente as autoridades de aplicação da lei, para efeitos de prevenção, investigação, deteção ou repressão de infrações penais, de quaisquer elementos de prova de alegadas infrações penais graves que envolvam uma ameaça contra a vida ou a segurança das pessoas, elementos esses obtidos no contexto das suas atividades com vista a remover ou a impossibilitar o acesso a conteúdos ilegais, em conformidade com os requisitos legais aplicáveis, em particular no que respeita à proteção de dados pessoais, nomeadamente o Regulamento (UE) 2016/679.

Cooperação entre prestadores de serviços de armazenagem em servidor e sinalizadores de confiança

25. Deve ser incentivada a cooperação entre prestadores de serviços de armazenagem em servidor e sinalizadores de confiança. Em especial, devem ser previstos procedimentos acelerados para tratar as comunicações enviadas por sinalizadores de confiança.
26. Os prestadores de serviços de armazenagem em servidor devem ser incentivados a publicar condições claras e objetivas para determinar quais as pessoas ou entidades que consideram serem sinalizadores de confiança.
27. Essas condições devem ter como objetivo garantir que as pessoas ou as entidades em causa possuem os conhecimentos especializados necessários e exercem as suas atividades como sinalizadores de confiança de forma diligente e objetiva, com base no respeito pelos valores em que se funda a União.

Cooperação entre os prestadores de serviços de armazenagem em servidor

28. Os prestadores de serviços de armazenagem em servidor devem, quando for apropriado, partilhar entre si experiências, soluções técnicas e boas práticas para combater os conteúdos ilegais em linha e, em especial, com prestadores de serviços de armazenagem em servidor que, em virtude da sua dimensão ou da escala em que exercem a sua atividade, têm recursos e conhecimentos especializados limitados, incluindo no contexto da cooperação já criada entre prestadores de serviços de armazenagem em servidor, através de códigos de conduta, de memorandos de entendimento e de outros acordos voluntários.

CAPÍTULO III**Recomendações específicas relativas a conteúdos terroristas***Generalidades*

29. As recomendações específicas relacionadas com conteúdos terroristas enunciadas no presente capítulo aplicam-se para além das recomendações gerais referidas no capítulo II.
30. Os prestadores de serviços de armazenagem em servidor devem indicar expressamente nas suas condições de utilização que não armazenam conteúdos terroristas.
31. Os prestadores de serviços de armazenagem em servidor devem prever disposições para não armazenarem conteúdos terroristas, em especial disposições relativas a sinalizações, medidas proativas e de cooperação, em conformidade com os pontos 32 a 40.

Comunicação e tratamento de sinalizações

32. Os Estados-Membros devem garantir que as suas autoridades competentes dispõem de capacidade e meios suficientes para detetar e identificar eficazmente conteúdos terroristas e comunicar sinalizações aos prestadores de serviços de armazenagem em servidor em causa, em especial através de unidades nacionais de sinalização de conteúdos na Internet e em cooperação com a Unidade da UE de Sinalização de Conteúdos na Internet da Europol.
33. É necessário prever mecanismos que permitam a comunicação de sinalizações. Devem ser previstos procedimentos acelerados para tratar as sinalizações, nomeadamente as comunicadas pelas unidades nacionais de sinalização de conteúdos na Internet e pela Unidade da UE de Sinalização de Conteúdos na Internet da Europol.
34. Os prestadores de serviços de armazenagem em servidor devem enviar sem demora indevida a confirmação da receção de sinalizações e informar a autoridade competente ou a Europol das suas decisões no que respeita ao conteúdo a que as sinalizações se referem, indicando, se for caso disso, quando o conteúdo foi retirado ou o seu acesso foi impossibilitado ou por que motivo foi decidido não remover ou não impossibilitar esse acesso.
35. Os prestadores de serviços de armazenagem em servidor devem avaliar e, se for caso disso, remover ou impossibilitar o acesso a conteúdos identificados nas sinalizações, em geral no prazo de uma hora a contar do momento em que receberam a sinalização.

Medidas proativas

36. Os prestadores de serviços de armazenagem em servidor devem tomar medidas proativas proporcionadas e específicas, incluindo através de meios automatizados, a fim de detetar, identificar e remover ou impossibilitar rapidamente o acesso a conteúdos terroristas.
37. Os prestadores de serviços de armazenagem em servidor devem tomar medidas proativas proporcionadas e específicas, inclusivamente através de meios automatizados, a fim de impedir imediatamente que os fornecedores de conteúdos insiram novamente conteúdos que já tenham sido retirados ou cujo acesso tenha sido removido ou impossibilitado por se considerar que se trata de conteúdos terroristas.

Cooperação

38. A fim de impedir a difusão de conteúdos terroristas entre os diferentes serviços de armazenagem em servidor, os prestadores deste tipo de serviços devem ser incentivados a cooperar através da partilha e otimização de ferramentas tecnológicas efetivas, adequadas e proporcionadas, incluindo ferramentas que permitem a deteção automática de conteúdos. Sempre que tal for tecnicamente possível, devem ser detetados todos os formatos pertinentes através dos quais os conteúdos terroristas são difundidos. Essa cooperação deve incluir, em especial, prestadores de serviços de armazenagem em servidor que, em virtude da sua dimensão ou da escala em que exercem a sua atividade, têm recursos e conhecimentos especializados limitados.

39. Os prestadores de serviços de armazenagem em servidor devem ser encorajados a tomar as medidas necessárias para assegurar o bom funcionamento e a melhoria das ferramentas a que se refere o ponto 38, nomeadamente disponibilizando identificadores relativos a todos os conteúdos considerados terroristas e explorando plenamente as possibilidades dessas ferramentas.
40. As autoridades competentes e os prestadores de serviços de armazenagem em servidor devem celebrar acordos de trabalho, e igualmente com a Europol quando tal for pertinente, sobre matérias relacionadas com conteúdos terroristas em linha, nomeadamente para melhorar os conhecimentos das atividades terroristas em linha, reforçar os mecanismos de sinalização, evitar a duplicação inútil de esforços e facilitar os pedidos das autoridades de aplicação da lei para efeitos de investigações penais em matéria de terrorismo.

CAPÍTULO IV

Prestação de informações

41. Os Estados-Membros devem, com regularidade e preferencialmente de três em três meses, apresentar um relatório à Comissão sobre as sinalizações comunicadas pelas respetivas autoridades competentes e sobre as decisões adotadas pelos prestadores de serviços de armazenagem em servidor em relação a essas sinalizações, bem como sobre a sua cooperação com estes prestadores de serviços relativa à luta contra os conteúdos terroristas.
42. A fim de permitir o acompanhamento dos efeitos da presente recomendação no que respeita aos conteúdos terroristas, o mais tardar três meses a contar da data da sua publicação, os prestadores de serviços de armazenagem em servidor devem apresentar à Comissão, a pedido desta, todas as informações necessárias para permitir esse acompanhamento. Estas informações podem incluir, em especial, dados sobre a quantidade de conteúdos que tenham sido removidos ou cujo acesso tenha sido impossibilitado, tanto com base em sinalizações ou notificações como na sequência da adoção de medidas proativas e de utilização de meios automatizados. Podem igualmente incluir o número de sinalizações recebidas, bem como o tempo necessário para a tomada de medidas e a quantidade de conteúdos impedidos de serem apresentados ou repetidos, através do recurso à deteção automática de conteúdos e de outras ferramentas tecnológicas.
43. A fim de permitir o acompanhamento dos efeitos da presente recomendação no que respeita a conteúdos ilegais, com exceção dos conteúdos terroristas, o mais tardar seis meses a contar da data da sua publicação, os Estados-Membros e os prestadores de serviços de armazenagem em servidor devem apresentar à Comissão, a seu pedido, todas as informações necessárias para permitir esse acompanhamento.

Feito em Bruxelas, em 1 de março de 2018.

Pela Comissão
Andrus ANSIP
Vice-Presidente
