Sabemos que a Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, está na iminência de discutir e votar os vários projetos de lei que procuram reforçar a proteção das vítimas de crimes de disseminação não consensual de conteúdos íntimos. Aproveitamos esta fase da iniciativa legislativa para partilhar consigo os nossos contributos.

1. **Necessidade de notificar a Comissão**

   O Projeto de Lei nº 347/XV, bem como as disposições nacionais sobre o bloqueio de sites contendo pornografia de menores introduzidas em Portugal em 2020, por força da Lei nº 40/2020, estão sujeitos a notificação à Comissão nos termos da Diretiva (UE) 2015/1535.

   O artigo 5.º, n.º 1, da Diretiva (UE) 2015/1535 exige que os Estados-Membros informem a Comissão de qualquer projeto de regulamento técnico, relativo a produtos e serviços da sociedade da informação antes da sua adoção. O que servirá os príncipios da transparência e do intercâmbio de informações entre os regulamentos dos Estados-Membros e, assim, o bom funcionamento do mercado interno.

   Os "regulamentos técnicos" abrangem, nomeadamente, as «regras relativas aos serviços» (artigo 1.º, alínea e, f), que incluem disposições relativas ao prestador intermediário de serviços em rede. Uma vez que o Projeto de Lei nº 347/XV introduz obrigações aplicáveis aos prestadores intermediários de serviços em rede, é considerado um "regulamento técnico". Assim, nos termos do artigo 5.º, n.º 1, da Diretiva (UE) 2015/1535, Portugal é obrigado a comunicar de imediato o Projeto de Lei à Comissão.

   Em todo o caso, os Estados-Membros são obrigados a notificar um novo projeto se o projeto de regulamento técnico sofrer alterações substanciais, como por exemplo alterações significativas ao âmbito de aplicação, acrescentar especificações ou requisitos ou torná-los mais restritivos, art. 5(1) Diretiva (UE) 2015/1535. Uma mudança substancial deste tipo acrescentaria uma categoria de conteúdo, como no caso em questão, uma vez que o número de sites que os prestadores intermediários de serviços em rede são obrigados a bloquear irá provavelmente aumentar significativamente.

   A necessidade de comunicação à Comissão do Projeto de Lei nº 347/XV é corroborada por processos de notificação prévia. Por exemplo, em 2021, a Alemanha notificou a Comissão de seu Projeto de Lei que altera a Lei de Execução de Redes, que introduziu obrigações adicionais aplicáveis aos prestadores de serviços de redes sociais e plataformas de partilha de vídeo. Em 2019, a França notificou a Comissão do projeto de lei destinado a combater o conteúdo de ódio na internet. Além disso, em 2009, a Alemanha notificou

Recebido por email na CACDLG em 05/12/2022
Distribuído à Comissão em 12/12/2022

a Comissão do seu projeto de lei de luta contra a pornografia infantil nas redes de comunicação, que previa o impedimento do acesso à pornografia infantil, nomeadamente através do bloqueio de determinados sites.

2. **Ajustar a Lei Nacional com a Lei dos Serviços Digitais (DSA) e a regulação europeia que estabelece as regras para prevenir e combater o abuso sexual de crianças (CSAM).**

   Alertamos para a necessidade do projeto de lei ser compatível com a Lei dos Serviços Digitais da Comissão Europeia e a futura regulação CSAM. De acordo com a atual redação do projeto de lei 347/XIV/I, o legislador, de um lado, parece não alcançar essa harmonia em relação ao DSA e parece também adiantar-se em relação às regras de CSAM, criando potenciais fragmentações entre a lei comunitária e a lei nacional.

3. **Compatibilidade com o DSA**

   As alterações propostas nos artigos 19-A e 19-B do projeto de lei 347/XIV/I são incompatíveis com o DSA.

   a. **DSA pretende criar "total harmonia" na Europa**

      O legislador europeu identificou um aumento na fragmentação a nível europeu por consequência das divergências entre as leis nacionais dos Estados-Membros, em particular, nos requisitos das diligências dos prestadores intermediários de serviços em rede, nomeadamente, na maneira como o combate ao conteúdo ilegal, à desinformação online e a outros riscos sociais, deve ser efetuado, o que impacta negativamente o Mercado Interno.[1]

      A Comissão afirma explicitamente que o DSA "será diretamente aplicável; substituindo as legislações nacionais com o mesmo objectivo que se sobrepunham, e, uma vez que é um instrumento para a plena harmonização, impedindo os Estados-Membros da UE de ir mais longe na sua legislação nacional."[2]

---

[1] Cf. Considerando 2 DSA.
[2] Cf. https://ec.europa.eu/commission/presscorner/detail/pt/QANDA_20_2348 e artigos 114, 288 TFUE.

Assim, o DSA pretende harmonizar por completo as regras aplicáveis aos intermediários de serviços na União Europeia. **Consequentemente, os Estados Membros estão fortemente restringidos na adoção ou manutenção de requisitos nacionais adicionais dentro da esfera do DSA,** a menos que uma justificação seja indicada explicitamente na legislação.[3]

Em particular, a DSA harmoniza o quadro para a isenção de responsabilidade e especialmente para a forma como os fornecedores devem lidar com o conteúdo ilegal, as diligências devidas e as regras sobre a implementação e execução do DSA.[4] Caso os Estados-Membros não cumpram o disposto no DSA, a Comissão tem o direito de instaurar um processo formal de infração nos termos dos artigos 258.º e seguintes. TFUE.

b. Harmonização de regras referentes a conteúdos ilegais

A partilha ilícita e não consensual de imagens privadas que se pretende que seja enquadrada pelo Projeto de Lei nº 347/XV, que reforça a proteção das vítimas de crimes de disseminação não consensual de conteúdos íntimos, já se encontra no âmbito do DSA e é expressamente referida como exemplo de conteúdos ilícitos.

De modo a harmonizar a forma como os prestadores intermediários de serviços em rede lidam com conteúdo ilegal, o legilsador europeu introduziu várias obrigações que se aplicam a diferentes tipos de prestadores intermediários de serviços.

Entre outras coisas,os prestadores intermediários de serviços em rede devem:

- Agir contra o conteúdo ilegal após receber ordens das autoridades nacionais[5];
- Cooperar com as autoridades nacionais e notificá-las sobre tipos especiais de ilegalidades[6];
- Implementar mecanismos que permitam a qualquer indivíduo ou entidade notificá-los sobre o presença de conteúdo; ilegal e agir em conformidade[7] e;
- Avaliar e enfrentar os riscos sistémicos decorrentes da disseminação de conteúdo ilegal por meio dos seus serviços.[8]

---

[3] Cf. Considerando 9 e Artigo 1(2) DSA.
[4] Cf. Artigo 1(2) DSA.
[5] Cf. Artigo 9(1) DSA.
[6] Cf. Artigos 10(1) e 18 DSA.
[7] Cf. Artigo 16 DSA.
[8] Cf. Artigos 34 e 35 DSA.

Embora o DSA não ofereça uma definição abrangente do conceito de "conteúdo ilegal" e se refira a informações que não estão em conformidade com a legislação da União ou de qualquer Estado-Membro[9], o legislador europeu delineou explicitamente "*exemplos ilustrativos*" de conteúdo ilegal que considera estarem na esfera do DSA. Entre esses exemplos, encontram-se a partilha de imagens que retratam abusos sexuais infantis e **a partilha ilegal e não consensual de imagens privadas**[10].

A imposição de obrigações adicionais aos prestadores intermediários de serviços em rede relativamente a tais conteúdos ilegais que estão no escopo do DSA contradiz a harmonização total que o DSA pretende.

c. Obrigações de informação e apuramento de factos - Artigo 19.º-A do Projeto de Lei nº 347/XV

Impor o dever de informar as autoridades nacionais sobre tipos específicos de conteúdos suscetíveis de constituir infrações penais, como crime de invasão de privacidade (Artigo 19.º-A do Projeto de Lei nº 347/XV), ao prestador intermediário de serviços online, contradiz a estrutura do DSA.

Com vista a equilibrar os interesses e direitos fundamentais de todas as partes envolvidas na prestação de serviços de intermediação online, o legislador europeu tomou uma decisão consciente ao limitar as obrigações dos fornecedores desses serviços de informar ativamente as autoridades policiais ou judiciais da presença de conteúdo ilegal nos seus serviços.

Tais obrigações são particularmente limitadas a (1) ofensas criminais que envolvam uma ameaça à vida ou à segurança de uma pessoa[11] e (2) para cumprir ordens de autoridades judiciais ou administrativas nacionais para fornecer informações sobre um ou mais destinatários individuais específicos do serviço[12]. Além dessas disposições, não há obrigações adicionais que exijam que os prestadores intermediários de serviços em rede avaliem ativamente se um tipo específico de conteúdo pode constituir um crime ou informem as autoridades sobre os seus utilizadores.

Exigir que prestadores intermediários de serviços em rede avaliem proativamente se o conteúdo disponibilizado pelos seus serviços constitui crime de invasão de privacidade contradiz esse equilíbrio de interesses ilustrado nas disposições.

---

[9] Cf. Artigo 3(h) DSA.
[10] Cf. Considerando 12 DSA.
[11] Cf. Artigo 18 DSA.
[12] Cf. Artigo 10(1) DSA.

Além disso, avaliar se o conteúdo pode configurar crime de devassa da vida privada, impõe necessariamente a obrigação de procurar ativamente factos ou circunstâncias que indiquem atividade ilegal, o que contraria diretamente o artigo 8 do DSA.

d. Inexistência de obrigação de bloquear o acesso a sites

Obrigar os prestadores intermediários de serviços em rede a agir contra tipos específicos de conteúdos ilegais, nomeadamente garantindo que os sites que contenham a divulgação não consensual de conteúdos íntimos sejam bloqueados no prazo de 48 horas (artigo 19.º-B do Projeto de Lei nº 347/XV), contradiz o quadro harmonizado apresentado pelo DSA.

O legislador da UE tomou uma decisão consciente de não introduzir uma obrigação geral de agir contra tipos específicos de conteúdo ilegal sem uma ordem e, em particular, de não introduzir uma obrigação de bloquear o acesso a sites que contenham conteúdo ilegal.

Pelo contrário, a DSA exige que os prestadores intermediários de serviços em rede atuem apenas contra um ou mais objetos específicos de conteúdo ilegal mediante a receção de uma ordem específica para agir contra um ou mais objetos de informação emitidos pela autoridade judicial ou administrativa nacional relevante.[13] Exigir que prestadores intermediários de serviços em rede bloqueiem o acesso a sites identificados que contenham disseminação não consensual de conteúdo íntimo, sem ordem específica das autoridades competentes, está a contradizer esse mesmo quadro.

4. Propostas de alteração ao Dever de Informar e ao Dever de Suprimir

Pelas razões acima expostas, entendemos que a alteração proposta, se aprovada, poderá prejudicar gravemente os esforços de harmonização da UE nestas matérias. No entanto, e caso a Assembleia da República decida avançar e aprovar o projeto de lei, gostaríamos de apresentar as seguintes sugestões e comentários ao texto proposto:

Proposta no Projeto de Lei 347/XIV	Alteração Proposta

[13] Cf. Artigo 9(1) DSA.

Artigo 19.º- Dever de Informar Os prestadores intermediários de serviços em rede, conforme definidos neste Decreto-Lei, devem informar imediatamente o Ministério Público da identificação de conteúdos disponibilizados através dos serviços que prestam, sempre que a disponibilização ou acesso a tais conteúdos possa constituir uma crime, designadamente crime de pornografia infantil, crime de discriminação e incitação ao ódio e à violência, crime de invasão de privacidade ou crime de invasão de privacidade informática.	**Artigo 19.º- Dever de Informar** Os prestadores intermediários de serviços em rede, conforme definidos neste Decreto-Lei, devem informar o Ministério Público imediatamente ao tomarem conhecimento da detecção de conteúdos disponibilizados através dos serviços que prestam sempre que a disponibilização ou o acesso a , tais conteúdos podem constituir crime, nomeadamente crime de pornografia infantil, ou crime de discriminação e incitação ao ódio e à violência, ~~crime de invasão de privacidade ou crime de invasão de privacidade informática.~~

Argumentos jurídicos para a primeira alteração sugerida

1. **A privacidade está expressamente excluída do âmbito de aplicação da lei do comércio eletrónico**: O artigo 2.º da lei alterada (Lei do Comércio Eletrónico - Decreto-Lei n.º 7/2004, de 7 de janeiro) dispõe expressamente que, "*o enquadramento relativo ao tratamento de dados pessoais e à **proteção da privacidade** não se enquadra no âmbito desta lei*". Isso significa que a lei de comércio eletrónico não se destina a fornecer uma estrutura sobre questões gerais de "proteção da privacidade". No entanto, e ao prever uma obrigação específica de informar o Ministério Público sobre factos que possam constituir "crime de invasão de privacidade", a disposição colide com o âmbito de aplicação inicial da lei, uma vez que pretende incluir matérias expressamente fora do âmbito de aplicação .

2. **Inexistência de obrigação legal de denúncia**: Nos termos do artigo 242.º do Código de Processo Penal (CPC), "*É obrigatória a denúncia, ainda que se desconheça a autoria do crime: (a) Para as entidades policiais, quanto a todos os crimes de que tomem conhecimento; e (b) Para todos os funcionários, na aceção do artigo 386.º do Código Penal, relativamente a crimes de que tenham conhecimento no exercício das suas funções e por causa delas.*"

   Isto significa que não existe qualquer obrigação legal de qualquer outra entidade/pessoa de denunciar às autoridades crimes de que tenham conhecimento. No entanto, ao exigir que os prestadores intermediários de serviços em rede informem o Ministério Público de qualquer conteúdo com que se depare e que possa constituir um "crime de devassa da privacidade", a proposta viola o artigo 242.º do Código de Processo Penal português.

   Como acima mencionado, a DSA limita estas obrigações a (1) infracções penais que envolvam uma ameaça à vida ou à segurança de uma

pessoa[14] e (2) ao cumprimento de ordens das autoridades judiciais ou administrativas nacionais para fornecer informações sobre um ou mais destinatários individuais específicos do serviço[15].

3. **Violação da regra da denúncia voluntária**: O artigo 244.º do Código de Processo Penal (CPC) dispõe, como regra geral, que "**Quem** *tiver notícia de um crime* ***pode*** *denunciá-lo ao Ministério Público, a outra autoridade judiciária ou à autoridade policial criminal, salvo se o respectivo procedimento depender de queixa ou acusação particular*". Por outro lado, crimes como "violação da privacidade", em que o procedimento depende de queixa ou acusação privada, a denúncia só pode ser validamente apresentada às autoridades pela vítima: "*a proprietária dos interesses que a lei especialmente queria proteger com a incriminação*". Isto significa que, nesses casos, a denúncia do crime não pode ser apresentada por "qualquer um", mas apenas pela vítima (ou os seus representantes). No entanto, e ao permitir que os intermediários prestadores de serviços apresentem denúncia às autoridades públicas sobre factos que possam constituir crime, a disposição viola a regra prevista no artigo 244.º do Código de Processo Civil.

   Esta questão não se coloca relativamente aos demais crimes já previstos no artigo (pornografia infantil e crime de discriminação e incitação ao ódio e à violência), uma vez que ambos os crimes, ao contrário do crime de violação da privacidade, são considerados "crimes públicos " e como tal, nos termos do artigo 244.º do CPC, "**quem** *tiver notícia de um crime* ***pode*** *denunciá-lo ao Ministério Público*".

4. **Inexistência de direito legal de informar**: O artigo 198.º do Código Penal, prevê que o crime de violação da privacidade depende da apresentação de queixa pela vítima (ou seus representantes). Nos termos do artigo 113.º do Código Penal, quando o processo penal dependa de queixa, apenas a vítima tem direito a apresentar queixa. Isso significa que o Google não tem o direito de denunciar a existência de crimes ao Ministério Público.

   Novamente, esta questão não se coloca no que diz respeito aos demais crimes já previstos no artigo (pornografia infantil e crime de discriminação e incitação ao ódio e à violência), uma vez que ambos os crimes, ao contrário do crime de violação da privacidade, são considerados " crimes públicos" e como tal, nos termos do artigo 244.º do CPC, "**quem** *tiver notícia de um crime* ***pode*** *denunciá-lo ao Ministério Público*".

5. **Impossibilidade legal de instauração de inquérito por parte do Ministério Público**: Nos termos do artigo 49.º do CPC, "*Quando o processo penal depender de denúncia da vítima, é necessário que esta apresente queixa ao Ministério Público, para que possa promover o processo*." Isto significa que o Ministério Público não pode investigar um "crime de violação da privacidade", ainda que tome conhecimento dos factos através do "dever de informar", salvo se a vítima (ou os seus representantes) tiver formalmente apresentado queixa e manifestado a intenção de avançar com um procedimento.

[14] Cf. Artigo 18 DSA.

[15] Cf. Artigo 10(1) DSA

De acordo com a lei portuguesa, o Ministério Público está legalmente proibido de iniciar uma investigação de factos relativos a "violação de privacidade" com base exclusivamente em informações enviadas por prestadores intermediários de serviços em rede no âmbito do "dever de informar".

6. **Nulidade da investigação criminal**: No entanto, e se o Ministério Público instaurar uma investigação sobre a violação da privacidade, com base no conhecimento dos factos apurados através do "Dever de Informar", a investigação seria considerada nula, nos termos dos artigos 48.º, 49.º, 118 e 119 b) do Código de Processo Penal Português.

7. **Violação do RGPD (Tratamento de informação sensível)**:O dever de informar o Ministério Público da existência de conteúdos relacionados com a violação da privacidade seria considerado um tratamento de dados pessoais nos termos do artigo 4 (2) do RGPD. Nos termos do nº 1 do artigo 9º do Regulamento, o tratamento de "dados relativos à vida sexual ou orientação sexual de uma pessoa singular é proibido", a menos que se enquadre numa das justificações previstas no nº 2, o que não será o caso, o que significa que, ao fornecer esta informação ao Procurador da República, os prestadores intermediários de serviços, poderão estar a violar o RGPD.

   Além disso, ao prever a obrigação de informar sobre estes conteúdos, a lei estará em violação direta do artigo 9.º do RGPD.

8. **Violação do RGPD (Ausência de fundamento legal)**: Nos termos do artigo 6 da GDPR, o tratamento de dados pessoais "só será legal se e na medida em que se aplique pelo menos uma das seguintes disposições: (a) a pessoa em causa tiver dado consentimento para o tratamento dos seus dados pessoais para um ou mais fins específicos; b) o tratamento for necessário para a execução de um contrato no qual a pessoa em causa é parte ou para tomar medidas a pedido da pessoa em causa antes da celebração de um contrato; c) o tratamento for necessário para o cumprimento de uma obrigação legal a que o responsável pelo tratamento esteja sujeito; d) o tratamento for necessário para proteger os interesses vitais da pessoa em causa ou de outra pessoa singular; (e) o tratamento for necessário para o cumprimento de uma missão de interesse público ou para o exercício da autoridade pública de que é investido o responsável pelo tratamento; f) o tratamento for necessário para os fins dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, excepto se esses interesses forem ultrapassados pelos interesses ou direitos e liberdades fundamentais da pessoa em causa que exijam a protecção de dados pessoais, em especial se a pessoa em causa for uma criança. "

   Os prestadores intermediários de serviços em rede não teriam base legal para tratar dados pessoais para fins de processo criminal ou iniciar investigações criminais, uma vez que nenhum dos casos acima mencionados se aplicaria.

   Isto significa que o dever de informar o Ministério Público sobre estes conteúdos específicos, seria uma violação direta do artigo 6.º do RGPD.

   Mesmo que com esta alteração a lei expressasse uma "autorização" para os prestadores intermediários de serviços em rede informarem o Ministério Público, isso estaria em conflito direto com o artigo 113.º do Código Penal acima mencionado, que prevê que, nestes casos, apenas

as vítimas teriam esse direito.

9. **Exercício da função judicial penal:** O artigo 202.º da Constituição da República Portuguesa prevê que compete aos tribunais "*assegurar a defesa dos direitos e interesses legalmente protegidos dos cidadãos, reprimir a violação da legalidade democrática e dirimir conflitos de interesse público e privado.*" e o artigo 9º do CPC, inclui disposição igual. No entanto, e ao impor aos prestadores intermediários de serviços em rede a obrigação de apurar se um determinado conteúdo constitui "crime de devassa da vida privada", a lei obriga os prestadores a assumirem uma função que legalmente cabe aos Tribunais.

   O facto é que um determinado conteúdo só será considerado como "crime de violação da privacidade", quando e se tiver sido partilhado: "*sem consentimento e "com intenção de se intrometer na vida privada das pessoas, nomeadamente na intimidade das vida familiar ou sexual*".

   Os prestadores intermediários de serviços em rede não têm o contexto necessário para identificar se um determinado conteúdo constitui um "crime de violação de privacidade", porque não conseguem determinar se houve "*consentimento*" dos sujeitos ou, mais difícil ainda, se houve uma "*intenção de intrometer-se na vida privada das pessoas"*.

   No quadro legal português, se o conteúdo foi recolhido (partilhado, disponibilizado, etc.) com consentimento **ou** sem a motivação específica prevista na lei (para *"intrometer-se na vida privada de uma pessoa"*), o conteúdo não deve ser considerado um " crime de devassa da vida privada".

   Ou seja, não bastará determinar que qualquer conteúdo que se enquadre no crime de "devassa da vida privada" esteja sujeito ao dever de informar, pois o "consentimento" é considerado um elemento negativo deste tipo específico de crime, ou seja, os factos só serão considerados crime se este elemento específico não estiver presente.

   Ao atribuir esta obrigação aos prestadores intermediários de serviços em rede, a lei viola o artigo 202.º da Constituição Portuguesa e o artigo 9.º do CPC.

10. **Conflito de direitos**: O quadro penal em vigor prevê que o crime de "violação da intimidade" pode ser cometido quando alguém, *sem consentimento e com intenção de se intrometer na vida privada de uma pessoa:*

    (a) intercetar, registar, utilizar, transmitir ou divulgar conversas, comunicações telefónicas, mensagens de correio eletrónico ou dados de faturação detalhados;
    (b) Capture, fotografe, filme, grave ou divulgue imagens de pessoas ou objetos ou espaços íntimos;
    (c) observar ou escutar pessoas secretamente em locais privados; ou
    (d) Divulgar factos relativos à vida privada ou doença grave de outra pessoa;"

    Em muitos casos, a divulgação do conteúdo acima pode ser legitimada por outro direito igualmente fundamental, como por exemplo, o

direito à informação ou liberdade de imprensa. No entanto, e não tendo os prestadores intermediários de serviços em rede qualquer contexto ou informação sobre um conteúdo específico, não conseguem determinar se esse conteúdo específico constitui um crime de violação da privacidade ou o exercício legítimo de um Direito Constitucional.

Por exemplo, se um jornalista publicou uma imagem de um político sem o seu consentimento ou conhecimento, mas essa imagem é importante para provar que, ao contrário do que ele havia afirmado publicamente, ele realmente conhecia alguém ou esteve num local específico, ou compareceu em determinado restaurante com alguém, as imagens poderiam ser protegidas pelo direito à liberdade de imprensa, previsto nos artigos 37.º e 38.º da Constituição da República Portuguesa e no n.º 1 do artigo 10.º da Convenção Europeia dos Direitos do Homem.

O artigo 18.º da Constituição da República Portuguesa estabelece que "*a lei só pode restringir direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos*".

A jurisprudência portuguesa é unânime ao considerar que a colisão de direitos, ainda que de natureza diversa, deve ser resolvida pelo princípio da concordância prática consagrado no art. 18, n. 2º da Constituição Portuguesa, que exige uma ponderação judicial casuística, tendo também em consideração o princípio da proporcionalidade e a intensidade e relevância da lesão à personalidade.

Isso significa que a simples determinação de que todos os conteúdos que eventualmente constituam "violação de privacidade" devem ser fornecidos ao Ministério Público e sujeitos ao dever de informação, pode levar à violação dos princípios da proporcionalidade e da ponderação.

11. Ao contrário da "pornografia infantil", o conteúdo que constitua *"invasão de privacidade ou crime de invasão de privacidade por meio de computador*" é difícil de determinar sem contexto e informações complementares. A implementação do "dever de informar" para um conceito tão amplo e indeterminado envolve múltiplos desafios legais que podem impedir a sua aplicação.

Considerando a dificuldade proporcionada pela amplitude e incerteza dos conceitos utilizados na emenda, sugerimos enfaticamente a retirada de quaisquer conceitos indeterminados.

12. Como acima mencionado, exigir aos prestadores intermediários de serviços que avaliem proactivamente se o conteúdo pode constituir um crime de devassa da vida privada, impõe necessariamente a obrigação de procurar activamente factos ou circunstâncias que indiquem uma actividade ilegal, o que contradiz directamente o Artigo 8 da DSA.

Artigo 19.º-B **(Dever de remoção)**	**Artigo 19.º-B** **(Dever de remoção)**

(1) Sem prejuízo do disposto no artigo anterior, os prestadores intermediários de serviços em rede devem assegurar, no prazo de 48 horas, o bloqueio de sites identificados como de acolhimento de pornografia infantil, difusão não consentida de conteúdos íntimos ou material conexo, através de um procedimento transparente e com salvaguardas adequadas, nomeadamente assegurando que o bloqueio se limita ao necessário e proporcional, e que os utilizadores são informados do motivo do bloqueio.	(1) Sem prejuízo do disposto no artigo anterior, os prestadores intermediários de serviços em rede devem assegurar, no prazo de 48 horas, o bloqueio dos ~~sites~~ conteúdos identificados como contendo pornografia infantil, não consensual de ~~divulgação~~conteúdo sexuamente explícito ou material conexo, através de um procedimento transparente e com salvaguardas adequadas, nomeadamente assegurando que o bloqueio se limita ao necessário e proporcional, e que os utilizadores são informados do motivo do bloqueio.
(2) Para efeitos do número anterior, os sites identificados como contendo pornografia infantil, difusão não consensual de conteúdos íntimos ou material conexo são todos aqueles que constam das listas elaboradas para o efeito pelas entidades nacionais e internacionais competentes na área da prevenção e combate ao crime, nos termos previstos no número seguinte.	(2) Para efeitos do número anterior, os ~~sites~~ conteúdos identificados como contendo pornografia infantil, não consensual de ~~divulgação~~ conteúdo sexuamente explícito ou material conexo são todos aqueles que constam das listas elaboradas para o efeito pelas entidades nacionais e internacionais competentes na área da prevenção e combate ao crime, nos termos previstos no número seguinte.

Argumentos legais para a alteração

1. **Proposta de substituição de "site" por "conteúdo":** O bloqueio de um site (ao invés de um "conteúdo" específico) terá como efeito a indisponibilidade de todo o conteúdo existente naquele determinado site independentemente da sua natureza ou licitude. Isso significa que um site pode ser totalmente bloqueado por ter conteúdo que pode constituir "*divulgação não consensual de conteúdo íntimo*".

   Podem existir sites que são legais, mas hospedam esse conteúdo sem saber. No entanto, a decisão de bloquear todo o site entraria em conflito com outros direitos existentes, como o direito à informação ou o direito de realizar um negócio em que não existe uma regra geral, no quadro português, que determine que qualquer um dos direitos mencionados é mais valioso do que outros ou que um deva compensar o outro.

   Ao bloquear automaticamente sites inteiros, os prestadores intermediários de serviços em rede podem estar a afetar o direito à liberdade de imprensa, previsto nos artigos 37.º e 38.º da Constituição da República Portuguesa e no n.º 1 do artigo 10.º da Convenção Europeia dos Direitos do Homem.

O artigo 18.º da Constituição da República Portuguesa estabelece que "*a lei só pode restringir direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos*".

No mesmo sentido, o artigo 335 do Código Civil dispõe que "*Em caso de colisão de direitos iguais ou da mesma espécie, os titulares devem ceder o quanto for necessário para que produzam seus efeitos de forma igualitária, sem maior prejuízo para qualquer das partes.*"

No entanto, o facto é que, ao bloquear sites inteiros (em vez de apenas o conteúdo "ilegal") a lei não está limitando o direito de acesso à informação ao estritamente necessário.

Isso significa que a aplicação do dever de bloqueio quando aplicada a sites inteiros (em vez de conteúdo específico) constituirá uma violação da
concordância prática consagrada no art. 18, n. 2º da Constituição Portuguesa, que exige uma ponderação judicial casuística, tendo também em consideração o princípio da proporcionalidade e a intensidade e relevância da lesão à personalidade.

2. O DSA exige que os prestadores intermediários de serviços apenas actuem contra um ou mais itens específicos de conteúdo ilegal após a recepção de uma ordem específica emitida pela autoridade judicial ou administrativa[16] nacional relevante que deve conter informações específicas e claras, permitindo ao prestador intermediário de serviços identificar e localizar o conteúdo ilegal em causa, tais como um ou mais URL's e, quando necessário, informações adicionais.

Exigir aos prestadores intermediários de serviços que bloqueiem o acesso a sítios web inteiros identificados como contendo difusão não consensual de conteúdo íntimo sem fornecerem as informações necessárias para a identificação do conteúdo específico, comprometerá todos os esforços de harmonização no sentido de um quadro comum da UE[17].

3. Sugestão de alteração da emenda: [substituição de "divulgação não consensual de conteúdo íntimo" por "divulgação não consensual de conteúdo sexual"]:

Considerando a dificuldade proporcionada pela amplitude e incerteza do conceito de "conteúdo íntimo" (que depende de questões como cultura, religião e hábitos sociais), o uso de uma redação mais objetiva como "**conteúdo sexualmente explícito"** permitiria uma melhor interpretação e aplicabilidade da lei.

[16] Cf. Artigo 9(1) DSA.
[17] Cf. Artigo 9(1) DSA.

(3) As listas referidas no número anterior são comunicadas aos prestadores intermediários de serviços em rede e à Procuradoria-Geral da República pelas entidades que as elaboram, com a colaboração das autoridades sectoriais competentes, que, para o efeito, também devem fornecer à Procuradoria-Geral da República todos os elementos identificativos dos prestadores intermediários de serviços em rede e informar sobre quaisquer alterações que ocorram a esse respeito.	N/A
	(4) A lista referida no parágrafo (3) deve fornecer informações claras que permitam ao Ministério Público e aos prestadores intermediários de serviços em rede identificar e localizar o conteúdo ilegal em questão, como um ou mais localizadores uniformes de recursos exatos (URL) e, quando necessário, informações adicionais.

Sugestão de alteração da emenda: [Acrescentar ponto 4]:

Argumentos jurídicos para a alteração sugerida

1. O artigo 18.º da Constituição da República Portuguesa dispõe que "*a lei só pode restringir direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou direitos constitucionalmente protegidos interesses*".

O artigo 335.º do Código Civil prevê ainda que "*Em caso de colisão de direitos iguais ou da mesma natureza, os titulares devem ceder o quanto for necessário para que produzam os seus efeitos de forma igualitária, sem maior prejuízo para qualquer um dos lados.*"

Como mencionado anteriormente, o bloqueio de sites inteiros (em vez de conteúdos específicos considerados ilegais) pode ter um efeito desproporcional, pois bloqueará indiscriminadamente conteúdos lícitos e legítimos, e por isso tal obrigação pode configurar uma violação do artigo 18 da Constituição portuguesa, que exige uma ponderação judicial casuística, tendo também em consideração o princípio da proporcionalidade e a intensidade e relevância da lesão à personalidade.

Considerando esta necessidade de proporcionalidade e para limitar a violação desnecessária de direitos de terceiros, quaisquer listas de bloqueio devem fornecer um URL específico e outras informações para que o conteúdo específico possa ser rapidamente identificado.

2. O DSA exige que os prestadores intermediários de serviços apenas actuem contra um ou mais itens específicos de conteúdo ilegal após a recepção de uma ordem específica emitida pela autoridade judicial ou administrativa nacional relevante que deve conter elementos específicos relativos ao conteúdo, e informações claras que permitam ao prestador intermediários de serviços identificar e localizar o conteúdo ilegal em questão, tais como um ou mais URL's e, quando necessário, informações adicionais. Exigir aos prestadores intermediários de serviços que bloqueiem o acesso a sítios web inteiros identificados como contendo difusão não consensual de conteúdos íntimos sem fornecer as informações necessárias à identificação do conteúdo específico comprometerá todos os esforços de harmonização no sentido de um quadro comum da UE.	
(4) O bloqueio efetuado nos termos do n.º 1 pode ser impugnado perante o juiz competente, nos termos gerais da lei.	~~(4)~~ (5) O bloqueio efetuado nos termos do n.º 1 pode ser impugnado perante o juiz competente, nos termos gerais da lei.

5. Processo de notificação do NCMEC

Quando identificamos conteúdo que contém abuso e exploração sexual infantil, removemos esse mesmo conteúdo e o denunciamos ao Centro Nacional para Crianças Desaparecidas e Exploradas (NCMEC)

a. Conforme exigido pela lei dos EUA, denunciamos todas as ocorrências relacionadas com pornografia de menores nas nossas plataformas ao CNCDE , que por sua vez relata o incidente às autoridades policiais de todo o mundo.
b. O Centro Nacional para Crianças Desaparecidas e Exploradas (NCMEC) é uma ONG que funciona como centro de informações e relatórios para todas as questões relacionadas com a prevenção e recuperação de vitimização infantil.
c. O NCMEC mantém um banco de dados – servindo como impressões digitais de conteúdo CSAM identificado – que é disponibilizado aos prestadores intermediários de serviços em rede para que o conteúdo identificado numa plataforma possa ser rapidamente removido de todas as plataformas.
d. O NCMEC estabeleceu VPNs em conjunto com mais de 150 autoridades policiais em todo o mundo. Quando identificam que uma denúncia se refere a uma vítima ou perpetrador noutra jurisdição, o NCMEC partilha essas informações com as autoridades competentes.

O nosso último relatório de transparência do CSAM mostra que, de janeiro a junho de 2022, fizemos:

1. Mais de 1 milhão de relatórios ao NCMEC;
2. Contendo cerca de 6,7 milhões de conteúdos; e
3. Indexando cerca de 485.000 URLs

O relatório de transparência do NCMEC demonstra que 34.415 incluíram indicadores geográficos relativos a Portugal e foram partilhados com as autoridades portuguesas competentes.