Respeitar os direitos humanos e o Estado de Direito na utilização de tecnologia para deteção automática de conteúdos relativos à exploração e ao abuso sexual de crianças em linha

Relatório de peritos independentes

Direção Geral dos Direitos Humanos e do Estado de Direito
- DG I e Direção Geral da Democracia - DG II

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Junho de 2021

Este relatório foi preparado pelos seguintes peritos independentes:

Lazarus Liora, Le Toquin Jean-Christophe, Magriço Manuel Aires, Nunes Francisco, Staciwa Katarzyna (apoio também ao perito principal), Vermeulen Gert e Walden Ian, liderados por Sicilianos Linos-Alexandros, ex-presidente do Tribunal Europeu dos Direitos do Homem e assistido pelo Secretariado do Conselho da Europa.

As opiniões expressas neste relatório são da responsabilidade dos autores e não refletem necessariamente a política oficial do Conselho da Europa.

Ao longo do documento foram adicionadas três Notas Explicativas que podem ser encontradas no final do documento.

A tradução do presente documento é da responsabilidade da DGPJ, que agradece a revisão final efetuada pelo Dr. Manuel Aires Magriço.

DGPJ DIREÇÃO-GERAL DA POLÍTICA DE JUSTIÇA
REPÚBLICA PORTUGUESA
JUSTIÇA

Respeitar os direitos humanos e o Estado de Direito na utilização de tecnologia para deteção automática de conteúdos relativos à exploração e ao abuso sexual de crianças em linha

Relatório de peritos independentes

Direção Geral dos Direitos Humanos e do Estado de Direito - DG I e Direção Geral da Democracia - DG II

Junho de 2021

ÍNDICE

clique no número ou título para avançar até ao respetivo capítulo

clique no número ou título para avançar até ao respetivo capítulo

SUMÁRIO EXECUTIVO

A dimensão da exploração e do abuso sexual de crianças em linha tem vindo a aumentar a um ritmo alarmante. De acordo com o Relatório Relativo à Avaliação de Ameaça do Crime Organizado na Internet (Europol, 2020), a deteção de material de abuso sexual de crianças em linha (CSAM) tem vindo a aumentar de ano para ano, denotando um incremento acentuado durante a crise associada ao COVID-19.

Por exemplo, em 2020, as comunicações feitas para a linha direta de denúncia nos EUA, CyberTipline incluíram 33,6 milhões de imagens, das quais 10,4 milhões foram detetadas pela primeira vez e 31,6 milhões de vídeos, dos quais 3,7 milhões eram também originais. Em 2020, a CyberTipline recebeu 21,7 milhões de denúncias, o que representa um aumento de 28% em relação a 2019. Como descrito pela INHOPE, 60% de todos os URLs avaliados pelas linhas diretas de denúncia INHOPE em 2020, provinham de material previamente avaliado, o que indica que o mesmo conteúdo está a ser reproduzido e a ser repetidamente comunicado. Enquanto isso, as crianças são constantemente revitimizadas, mercê da circulação contínua das imagens dos abusos que sofreram.

Esta tendência alarmante exige técnicas inovadoras de deteção e eliminação deste tipo de material. Até à data, a resposta a este desafio assenta, em grande parte, em ações voluntárias que envolvem o uso de tecnologia de deteção automática por parte das empresas do setor privado, com o fim de detetar, comunicar e remover material de abuso sexual de crianças, incluindo o aliciamento através de mensagens escritas.

Para detetar automaticamente conteúdos e/ou comportamentos, suscetíveis de configurar uma ameaça para as crianças neste contexto, são utilizadas três famílias principais de tecnologias: a mais rudimentar é a tecnologia associada ao *File Hashing* (ficheiro de assinaturas digitais únicas), a categoria intermédia é a Visão Computacional e a mais inovadora e recente é a utilização de Inteligência Artificial, incluindo a sua versão mais avançada, designada como *Deep Learning* (aprendizagem profunda).

Embora tal seja vital para encontrar formas de identificar e ajudar a resgatar crianças vítimas, investigar crimes e deter a circulação de CSAM, a utilização de tecnologias automáticas é suscetível de ter impacto na confidencialidade do conteúdo das comunicações e dos dados de tráfego conexos, que os prestadores de serviços estão obrigados a garantir. Por conseguinte, a utilização deste tipo de tecnologias pode constituir uma interferência no direito à reserva da vida privada e familiar e à proteção dos dados pessoais das pessoas envolvidas.

Em setembro de 2020, a Comissão Europeia (CE) propôs uma derrogação temporária às disposições da Diretiva e-Privacy para permitir o tratamento de dados pessoais e outros com o objetivo de combater a exploração e o abuso sexual de crianças em linha (OCSEA). O debate gerado por esta proposta ilustra bem a complexidade das questões associadas à utilização deste tipo de tecnologias por parte das empresas privadas.

Sobre os Estados impende uma obrigação positiva de proteger as crianças do abuso e da exploração sexual. Para isso, devem, no entanto, considerar o ambiente complexo e em evolução, do ponto de vista tecnológico e jurídico. Em dezembro de 2020, os Estados Partes da Convenção de Lanzarote sobre a proteção das crianças contra a exploração e o abuso sexual, solicitaram ao Conselho da Europa que reunisse os conhecimentos especializados da organização, de forma a apoiá-los na procura de soluções adequadas para conciliar os vários direitos humanos em jogo, integrando salvaguardas nas ações levadas a cabo no interesse público.

Este relatório representa um primeiro momento de resposta do Secretário-Geral do Conselho da Europa ao apelo do Comité de Lanzarote.

O relatório baseia-se nas observações individuais e no trabalho conjunto de um grupo de peritos independentes, especializados nos domínios dos direitos humanos, da proteção das crianças, da proteção de dados e da luta contra a cibercriminalidade. O grupo foi liderado por Linos-Alexandros Sicilianos, ex-presidente do Tribunal Europeu dos Direitos do Humanos e auxiliado pelo Secretariado do Conselho da Europa.

Embora reconhecendo os benefícios que um regime obrigatório poderia trazer, este relatório centra-se na prática da deteção e da comunicação voluntária da OCSEA pelos prestadores de serviços, com fundamento principal em motivos de interesse público, tal como descrito nos ordenamentos jurídicos existentes. A escolha das soluções tecnológicas analisadas neste documento limitou-se, assim, a esse contexto.

Após referência ao enorme volume de conteúdos de abuso infantil em linha e ao valor acrescentado associado à utilização de tecnologias de deteção automática, os peritos descrevem as tecnologias utilizadas, as suas limitações e as suas potencialidades. A identificação de meios menos invasivos para detetar a OCSEA e proteger eficazmente as vítimas continua a ser um desafio de resposta complexa. Responder a este desafio requer uma compreensão muito precisa do objetivo e do ambiente relativamente aos quais uma determinada tecnologia é selecionada. Para orientar a escolha, os peritos propõem analisar a complexidade do objetivo, o ambiente e a tecnologia, incluindo a maturidade da tecnologia (uma tecnologia bem testada, bem documentada e estável é uma escolha mais segura para os decisores políticos, uma vez que é mais difícil definir o nível adequado de salvaguardas no caso de uma tecnologia que se encontra ainda numa fase inicial de desenvolvimento).

Os peritos descrevem igualmente o quadro jurídico aplicável, especificando as principais normas internacionais relevantes). De particular importância são:

- A Convenção das Nações Unidas sobre os Direitos da Criança e o Protocolo Facultativo relativo à Venda de Crianças, Prostituição Infantil e Pornografia Infantil;

- A Convenção do Conselho da Europa sobre os Direitos do Homem, a Carta Social Europeia e as Convenções relativas à proteção das crianças contra a exploração e o abuso sexual, sobre a cibercriminalidade e a proteção de dados (também conhecida como Convenção 108+);

- A Diretiva 2002/58/CE da UE do Parlamento Europeu e do Conselho (Diretiva e-Privacy) e o Código Europeu das Comunicações Eletrónicas.

A relevância da jurisprudência europeia é igualmente abordada através da análise de decisões do Tribunal Europeu dos Direitos Humanos e do Tribunal de Justiça da União Europeia.

O relatório contém nove recomendações, que abrangem várias questões, tais como a necessidade de acompanhar o ritmo da evolução tecnológica, de aumentar a transparência e a responsabilização, de coordenar esforços e de reforçar o diálogo entre o setor privado e os decisores políticos/reguladores, de incorporar salvaguardas nas fases iniciais do desenvolvimento da tecnologia, de dar a devida importância à obrigação positiva de proteger as crianças contra a violência sexual e de definir um quadro jurídico que proporcione segurança jurídica aos prestadores de serviços, abordando ainda os desenvolvimentos tecnológicos futuros. Os peritos apelam igualmente à criação de um quadro jurídico baseado no interesse público, alicerçado na Convenção de Lanzarote, que permita aos prestadores de serviços detetar, remover, comunicar e transferir automaticamente conteúdos de exploração e abuso sexual em linha, em conformidade com as condições e salvaguardas da proteção de dados e privacidade descritas no relatório.

O relatório é de "leitura obrigatória" para qualquer pessoa ativa e interessada na proteção das crianças contra a violência sexual. Os peritos tiveram um cuidado especial em tornar o conteúdo acessível à maioria dos leitores, apesar da complexidade das matérias abordadas.

O relatório foi igualmente preparado como um contributo para a consulta lançada pela CE em dezembro de 2020 sobre uma Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à deteção, remoção e comunicação de abusos sexuais de crianças em linha.

1. INTRODUÇÃO

1.1. Objetivo do documento

A dimensão da exploração e do abuso sexual de crianças em linha (OCSEA), tanto em termos absolutos como em termos de comunicação às autoridades responsáveis pela aplicação da lei e à sociedade civil, está a aumentar a um ritmo alarmante,[1] exigindo técnicas de combate inovadoras. Este apelo é ainda mais forte à luz do principal produto estratégico da Europol recentemente publicado, [2] o Relatório Relativo à Avaliação de Ameaça do Crime Organizado na Internet (IOCTA) 2020,[3] que assinala o facto de, embora as principais ameaças relacionadas com a OCSEA tenham permanecido estáveis nos últimos anos, verificou-se que a pandemia COVID-19 parece ter mudado esta avaliação. De acordo com as conclusões do IOCTA, a deteção de materiais de abuso sexual infantil em linha (CSAM) já estava a aumentar de ano para ano, mas notou-se um incremento significativo durante o pico da crise, refletindo o aumento na permuta de materiais de abuso infantil em linha que ocorreu durante o tempo em que se mantiveram as restrições de contacto e de viagens. Espera-se igualmente que a evolução em torno da pandemia e dos respetivos confinamentos e das restrições de viagem dê origem a um maior número de denúncias de OCSEA, uma vez que os abusos ocorridos durante a pandemia da COVID-19 podem ser comunicados às autoridades responsáveis pela aplicação da lei, como sejam as polícias, o Ministério Público e os Tribunais. Do mesmo modo, espera-se um aumento acentuado da quantidade de material relativo à exploração e ao abuso sexual de crianças auto gerado o que provavelmente conduzirá a um aumento correspondente no aliciamento/solicitação e exploração sexual de crianças em linha.[4]

Até à data, a resposta existente aos desafios colocados pela OCSEA consiste, em grande medida, em ações voluntárias que envolvem a utilização de tecnologias de deteção automatizadas[5], por entidades do setor privado, a fim de detetar, comunicar e remover o CSAM, incluindo ameaças baseadas em mensagens de texto como, por exemplo, as que se produzem durante um processo de aliciamento (grooming) de crianças. Há uma exceção a este

1 WePROTECT Global Alliance, Global Threat Assessment 2019, «Colaborando para acabar com a exploração sexual de crianças em linha», p. 2, (disponível em: https://www.endviolence.org/sites/default/files/paragraphs/download/Global%20Threat%20Assessment%202019.pdf).

2 A Agência da União Europeia para a Cooperação Policial, mais conhecida sob o nome de Europol, anteriormente Serviço Europeu de Polícia e Unidade de Droga da Europol, é a agência responsável por garantir o cumprimento da lei na União Europeia (UE), criada em 1998 para lidar com a informação criminal e combater a criminalidade organizada internacional grave e o terrorismo através da cooperação entre as autoridades competentes dos Estados-Membros da UE. Tem sede em Haia.

3 IOCTA 2020, p. 35, *(available at:* https://www.europol.europa.eu/activities-services/main-reports/internet- organised-crime-threat-assessment-iocta-2020).

4 Ibid, p.41.

5 Ver seção 2, "Visão técnica geral".

tipo de resposta nos EUA, onde uma lei federal exige que os prestadores de serviços[6] sedeados nos EUA reportem casos de aparente "pornografia infantil"[7] nos seus sistemas, de que tenham conhecimento, ao Centro Nacional para Crianças Desaparecidas e Exploradas (NCMEC), através da CyberTipline[8] Estes relatórios são posteriormente partilhados com as agências responsáveis pela aplicação da lei de todo o mundo [9], pelo NCMEC, e constituem uma parte significativa de casos objeto de investigação.

Embora os relatórios das entidades do setor privado sejam essenciais para ajudar a identificar as crianças vítimas e a resgatá-las dos abusos em curso, bem como para impedir a circulação de CSAM, subsistem duas questões. Em primeiro lugar, existe uma discrepância significativa entre o uso das tecnologias de deteção automática e o nível de informação acessível ao público sobre a sua adoção. Esta assimetria de informação torna difícil aos decisores políticos e aos reguladores desenvolverem uma abordagem coerente para regular estas tecnologias e garantir as salvaguardas legais adequadas. Em segundo lugar, o quadro legal que rege a conduta dos prestadores de serviços (PS) pode parecer insatisfatório, uma vez que a aplicação voluntária de tecnologias de deteção de OCSEA depende destes e, mesmo quando incluídos em regimes com características obrigatórias como nos EUA, não se exige que os PS procurem proativamente a OCSEA. A maioria dos países conta com o envio voluntário de comunicações às autoridades policiais e judiciárias, pois os volumes de dados envolvidos inviabilizam na prática, os pedidos oficiais obrigatórios. Consequentemente, a atual ausência de um quadro orientado para o interesse público, que permita aos agentes do setor privado participarem em práticas destinadas a responder eficazmente aos desafios colocados pela OCSEA, significa para estes agentes um enquadramento caracterizado pela insegurança jurídica e, muitas vezes, fragmenta e duplica os esforços para combater a OCSEA.

6 Entendido como "um prestador de serviços de comunicações eletrónicas ou um serviço de computação à distância" (18 USC § 2258E(6).

7 A lei federal dos Estados Unidos define "pornografia infantil" como "qualquer representação visual de conduta sexualmente explícita envolvendo um menor (uma pessoa com menos de 18 anos de idade)". O NCMEC opta por se referir a essas imagens como Material de Abuso Sexual Infantil (CSAM) de forma a refletir com mais precisão o que é retratado - o abuso sexual e a exploração de crianças. Mais informações estão disponíveis em: https://www.missingkids.org/theissues/csam

8 Gerido pelo Centro Nacional de Crianças Desaparecidas e Exploradas. O Centro Nacional de Crianças Desaparecidas e Exploradas (NCMEC) é uma empresa privada, sem fins lucrativos, cuja missão é ajudar a encontrar crianças desaparecidas, reduzir a exploração sexual infantil e prevenir a vitimização infantil. O NCMEC trabalha com famílias, vítimas, setor privado, autoridades de aplicação da lei e com o público para ajudar a prevenir os raptos de crianças, recuperar crianças desaparecidas e presta serviços para dissuadir e combater a exploração sexual de crianças. Ver secção 2.2.1, "Papel específico do Centro Nacional para Crianças Desaparecidas e Exploradas (NCMEC, EUA)".

9 Os relatórios 2019 & 2020 por país estão disponíveis em https://www.missingkids.org/gethelpnow/cybertipline.

O objetivo deste documento é, por conseguinte, dar orientações aos Estados Membros (EM) do Conselho da Europa[10] (CoE) no sentido de se assegurar o respeito pelos direitos humanos e pelo Estado de direito quando se utiliza tecnologia automatizada para detetar OCSEA. A necessidade de tais orientações foi expressa durante a 30.ª reunião do Comité de Lanzarote[11] (CtL), tendo o Secretariado do CtL sido convidado a verificar da viabilidade de emissão de um parecer abrangente ancorado nos direitos humanos que abordasse as dimensões acima referidas.[12] Espera-se igualmente que a apresentação destas orientações sirva de contributo para o trabalho da CE no sentido de uma proposta de solução a longo prazo no verão de 2021[13].

Parte do contexto destas orientações teve como referência a discussão na União Europeia sobre uma derrogação temporária[14] ao n.º 1 do artigo 5.º e do artigo 6.º da Diretiva 2002/58/CE (Diretiva e-Privacy),[15] no que respeita à utilização voluntária de tecnologias por prestadores de serviços de comunicações interpessoais independentes do número (NI-ICS), tal como voz sobre protocolo da Internet (IP), serviços de mensagens e serviços de correio eletrónico baseados na Web, para o tratamento de dados pessoais e outros para efeitos de combate ao abuso sexual de crianças em linha. Embora reconhecendo os benefícios que um regime obrigatório poderia trazer em termos de clareza e certeza jurídica, inclusive garantindo processos transparentes, bem como o reconhecimento e apoio generalizados, este relatório centra-se na prática da deteção e de comunicação voluntária da OCSEA por parte dos PS, principalmente com base em motivos de interesse público, tal como descrito pelos quadros jurídicos aplicáveis. Como consequência dessa abordagem, a escolha das soluções tecnológicas analisadas neste documento também se limitou a esse contexto.

Tendo em conta este contexto, é igualmente importante recordar que a terminologia utilizada nos instrumentos do CoE e da União Europeia (UE) nem sempre se encontra alinhada. Em especial, para efeitos do presente documento, importa salientar que as disposições pertinentes da

10 https://www.coe.int/en/web/portal/home

11 https://www.coe.int/en/web/children/lanzarote-committee

12 Lista das decisões tomadas pelo Comité de Lanzarote a 10 de dezembro 2020, (disponível em: https://rm.coe.int/list-of-decisions-30th-meeting-lanzarote-committee/1680a0b1eb)

13 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Fighting-child-sexual- abuse-detection-removal-and-reporting-of-illegal-content-online_en

14 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0568

15 Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas). Jornal Oficial da União Europeia, L 201, 31/07/2002 P. 0037-0047, (disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN).

Diretiva "e-Privacy" se referem aos prestadores de "serviços de comunicação eletrónica", conceito mais restrito do que o de um "prestador" utilizado na Convenção de Budapeste (CB).[16] [17]

Da mesma forma, enquanto os conceitos de privacidade e proteção de dados estão intimamente ligados ao abrigo da Convenção Europeia dos Direitos Humanos (CHR),[18] a Carta dos Direitos Fundamentais identifica-os como direitos separados. Esta distinção reflete-se, assim, no facto de a Diretiva e-Privacy assentar no direito à privacidade, enquanto o Regulamento Geral de Proteção de Dados (GDPR)[19] assentar no direito à proteção de dados. Estas distinções devem ser tidas em conta na leitura deste documento.

Como nota final, importa salientar que a questão do âmbito extraterritorial das obrigações positivas em matéria de combate contra a OCSEA não é exaustivamente tratada neste documento, uma vez que se trata de uma área de análise específica merecedora de um parecer separado.

1.2. Metodologia

O presente documento baseia-se num conjunto de propostas individuais de um grupo de peritos independentes convidado para esta tarefa pelo Secretariado do CoE: Liora Lazarus, Jean-Christophe Le Toquin, Manuel Aires Magriço, Francisco Nunes, Katarzyna Staciwa (que também apoiou o perito principal), Gert Vermeulen e Ian Walden, liderados por Linos -Alexandros Sicilianos, ex-presidente do Tribunal Europeu dos Direitos Humanos. Quando adequado, os seus respetivos contributos foram complementados com material público disponível no momento da redação, tais como informações provenientes de outras fontes especializadas, como sejam empresas do setor privado, organizações e instituições públicas e privadas.

O documento está dividido em duas partes: a primeira centra-se numa visão técnica geral e contém uma explicação sobre o papel atual da tecnologia para deteção automática de OCSEA, incluindo uma análise simplificada das soluções tecnológicas relevantes, bem como exemplos da sua aplicação prática. Na segunda parte, o documento apresenta uma panorâmica do quadro jurídico relevante: descreve o debate em torno da proposta da CE sobre uma derrogação temporária a certas disposições da Diretiva *e-Privacy*, explica o conceito e conduta de um "prestador de serviços", e familiariza os leitores com as propostas de regulamentos relevantes, anunciadas no processo de consulta pública pela CE. Em seguida, centra-se nas obrigações positivas específicas em relação à OCSEA, em especial nas obrigações

16 https://www.coe.int/en/web/cybercrime/the-budapest-convention

17 Ver secção 3.2.1, *O conceito de "prestador de serviços"*.

18 https://www.echr.coe.int/documents/convention_eng.pdf

19 https://eur-lex.europa.eu/eli/reg/2016/679/oj

relevantes desenvolvidas no âmbito da jurisprudência do Tribunal Europeu dos Direitos do Homem [20] (TEDH) e nas que decorrem das Convenções do CoE: sobre a proteção das crianças contra a exploração e o abuso sexual (também conhecida como Convenção de Lanzarote, (CL),[21] sobre o cibercrime (também conhecida como Convenção de Budapeste, (CB) e sobre a proteção de dados[22] (também conhecida como Convenção 108+).

1.3. Descrição do fenómeno

O fenómeno da exploração e do abuso sexual infantil (CSEA) está em constante evolução. Atualmente, existem mais do que o dobro de tipos de CSEA quando em comparação com o final da década de 1990. Naquela época, começaram a circular online cópias digitais de imagens comerciais anteriores retratando crianças vítimas e provas de produção familiar, bem como alguns vídeos produzidos para fins de comercialização.

A adoção de tecnologias de informação e de comunicação (TIC) no nosso dia-a-dia tem ligado inseparavelmente os ambientes *offline* e *online*, nos quais as crianças podem, com a maior facilidade, ser expostas a muitos perigos, tais como serem persuadidas a participar em condutas sexualmente explícitas (reais ou simuladas), ser recrutadas ou coagidas a participar em espetáculos pornográficos, ou forçadas a testemunhar situações de abuso sexual ou atividades sexuais. Muitas crianças são vítimas de exploração e abuso sexual em múltiplas formas: são vítimas dos infratores que abusam delas de forma física e, simultaneamente, dos infratores que produzem, distribuem, exigem, encomendam, vendem ou compram, trocam, descarregam ou transmitem conteúdos relacionados com a exploração e o abuso sexual de crianças, ou através de quaisquer outras TIC, que suportam e contribuem para a exploração sexual e o abuso sexual dessas crianças.[23] Uma pesquisa realizada demonstrou claramente que as infrações sexuais contra as crianças, incluindo as facilitadas pelo uso das TIC, têm um impacto duradouro nas vítimas. Este é, especialmente, o caso, quando materiais como imagens e vídeos que retratam a vítima estão em circulação por muito tempo no Ciberespaço após o abuso sexual físico ter sido praticado.

20 https://www.echr.coe.int/Pages/home.aspx?p=home

21 https://www.coe.int/en/web/children/lanzarote-convention

22 https://www.coe.int/en/web/data-protection

23 Parecer interpretativo sobre a aplicação da Convenção de Lanzarote aos crimes sexuais contra crianças, facilitados pela utilização das tecnologias da informação e da comunicação (TIC), adotada pelo Comité Lanzarote em 12 de maio de 2017, p. 5, (disponível em: https://rm.coe.int/t-es-2017-03-en-final-interpretative-opinion/168071cb4f)

As crianças são revitimizadas pela circulação contínua de imagens relativas aos abusos sofridos. A tecnologia utilizada para identificar essas imagens é, consequentemente, essencial para a sua proteção. Uma vez que as autoridades responsáveis pela aplicação da lei, em todo o mundo, são confrontadas com uma quantidade esmagadora de CSAM *online*, a implementação de soluções tecnológicas para combater eficazmente este fenómeno é necessária para uma resposta adequada ao desafio, em especial no sentido de conferir rapidez na priorização deste tipo de casos.

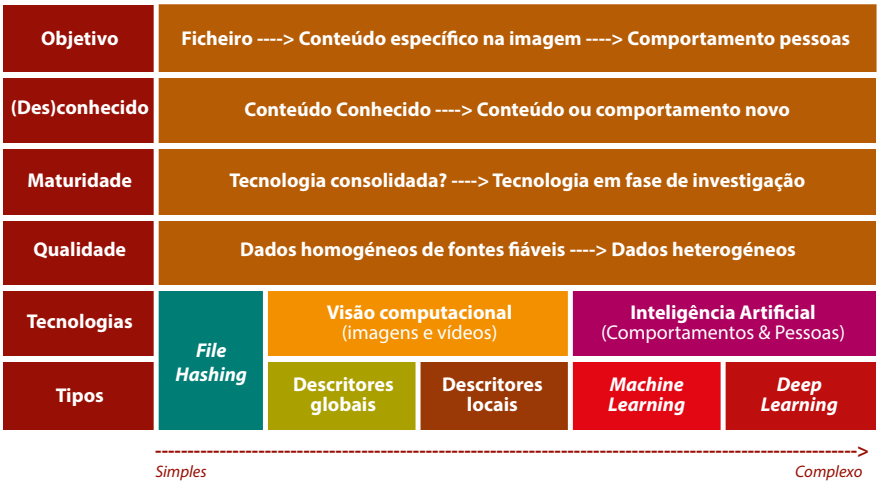
A prevenção e o combate bem-sucedidos à OCSEA exigem atualização e capacidade de respostas constantes aos desenvolvimentos nesta área, facilitados especialmente pela utilização predominante das TIC em constante transformação. Um dos pilares de tal abordagem, que é fundamental para a proteção competente das crianças contra a OCSEA, no mundo atual, é a adoção de soluções tecnológicas adequadas a tal desiderato, que poderiam - dependendo da sua escolha - apoiar ou ainda incluir a participação humana, ou substituir, em certa medida, o fator humano em áreas específicas. No entanto, esta escolha deve ser feita com o devido respeito pelos direitos fundamentais das crianças, tais como o direito à privacidade ou à liberdade de expressão.

2. VISÃO TÉCNICA GERAL

2.1. As três principais famílias de instrumentos de deteção automatizada de exploração e abuso sexual de crianças em linha[24]

A presente secção apresenta uma visão técnica simplificada sobre as principais tecnologias automáticas que podem ser utilizadas para detetar a OCSEA. Para detetar automaticamente conteúdos e/ou comportamentos, são aplicáveis três famílias principais de tecnologias: a mais rudimentar é designada *File Hashing* (FH), a categoria intermédia é a Visão Computacional (VC) e a mais inovadora é a Inteligência Artificial (IA), incluindo o Deep Learning (DL), que é o tipo mais avançado de inteligência artificial e que pode potencialmente lidar com cenários mais complexos.

O quadro apresentado a seguir apresenta uma visão geral das três principais famílias de deteção automática de conteúdos e/ou comportamentos e explica a sua complexidade.



As questões-chave em torno da escolha da tecnologia são definidas tendo em conta os objetivos e o ambiente para o qual vai ser utilizada. Estas questões são as seguintes:

- Fator relacionado com o objetivo - o que é que precisa de ser detetado: um ficheiro, um conteúdo ou uma pessoa? Por exemplo, identificar um ficheiro conhecido descrito como «csam1.jpg» é uma atividade de pesquisa elementar quando comparada com a atividade de identificação de uma pessoa através de tecnologias de reconhecimento facial;

24 A visão gráfica geral I sobre tecnologias de deteção de conteúdos visuais em imagens e vídeos é anexada ao presente documento no anexo.

• Fator conexo (des)conhecido - o que é que deve ser detetado: o conteúdo e/ou o comportamento, conhecido ou desconhecido? A tarefa mais difícil não é procurar conteúdo conhecido, é detetar conteúdos e/ou comportamentos anteriormente invisíveis, ou seja, a distribuição de CSAM que nunca antes foi observado ou a deteção de casos de um adulto que alicia uma criança. Por exemplo, um prestador de serviços ou um prestador de serviços cuja atividade consista no armazenamento de informações prestadas por um destinatário do serviço (*hosting*) de uma rede social, tanto pode decidir detetar o CSAM de forma reativa ao receber uma notificação, como pode agir proativamente analisando todo o conteúdo armazenado nos seus servidores. A tecnologia de deteção em ambos os casos permanece a mesma;

• Fator de maturidade - a tecnologia de deteção está consolidada ou em fase de investigação? Uma tecnologia consolidada pode ser definida como estável, bem documentada e testada ao longo dos anos; neste caso, a tecnologia é mais fácil de compreender e de regulamentar e os seus resultados serão muito mais previsíveis;

• Fator de qualidade - quão fiável é a base de dados de referência? A tecnologia de deteção automática muitas vezes depende de um conjunto inicial de dados: quanto mais fiável for a base de dados de referência, melhor será a compreensão da sua eficiência.

2.1.1. *File Hashing*

O *file hashing* é baseado num algoritmo matemático, onde um ficheiro é reduzido a uma assinatura, ou seja, 3CBCFDDEC145E3382D592266BE193E5BE53443138EE6AB6CA09FF-20DF609E268.[25] Esta tecnologia ajuda a detetar um ficheiro idêntico e é capaz de consultar grandes conjuntos de dados de assinaturas com recursos de computação limitados. Esta tecnologia, porém, não é compatível com alterações: a modificação de um *bit* ou de um *pixel* vai gerar uma assinatura diferente e não há maneira de entender se os dois ficheiros são idênticos ou não. Por vezes, afirma-se que este tipo de *file hashing* não gera falsos positivos, porquanto duas imagens diferentes não podem ter a mesma assinatura. A ser verdade, isso seria benéfico nas investigações e nos processos judiciais, principalmente quando as provas se baseiam apenas em *hashes* sem revisão humana. No entanto, já se defendeu a possibilidade mínima de dois ficheiros diferentes poderem resultar numa única imagem, o denominado fenómeno de "vulnerabilidade de colisão".[26]

25 https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/get-filehash?view=powershell-7.1

26 https://en.wikipedia.org/wiki/MD5#Collision_vulnerabilities and https://en.wikipedia.org/wiki/SHA-1

Os algoritmos mais frequentes são o MD5 e o SHA-1 adotados por muitas agências responsáveis pela aplicação da lei, por empresas e por algumas linhas diretas de denúncia, como CyberTipline (EUA), Internet Watch Foundation (IWF) (UK)[27] Expertisebureau Online Kindermisbruik (EOKM) (NL)[28] and Point de Contact[29] (FR).

2.1.2. Visão Computacional

Nesta categoria serão analisados dois modelos de técnicas: descritores globais e descritores locais.

Descritores globais

A tecnologia do descritor global é baseada num processo em que a imagem é transformada numa grade e, em seguida, cada quadrado da grade é traduzido numa assinatura. Esta tecnologia procede à comparação de imagens idênticas e pode também detetar as mesmas imagens ligeiramente recortadas (até 20%). Porém, não reconhece imagens significativamente modificadas: rodadas, viradas, alongadas, ampliadas, recortadas em mais do que 20%, inseridas noutra imagem ou vídeo, etc. Os algoritmos mais frequentes são as seguintes: *PhotoDNA* (Microsoft),[30] *pHash* (open source)[31] e *TMK PDQF* (Facebook).[32] A tecnologia assente em PhotoDNA é utilizada por algumas linhas de denúncia, como sejam a *CyberTipline*, *Cybertip*, IWF, bem como a *EOKM* e os seus parceiros.

Descritores locais

Esta tecnologia mede o número de pormenores partilhados entre 2 imagens ou vídeos, identificando pormenores com fortes semelhanças. Reconhece imagens, mesmo aquelas significativamente modificadas: rodadas, viradas, alongadas, ampliadas, cortadas em mais de 20%, inseridas noutra imagem ou vídeo. É também possível procurar uma correspondência exata ou parcial. Como opção, é possível reconhecer o conteúdo na imagem ou vídeo: o mesmo edifício, a mesma sala, o mesmo objeto, a mesma imagem inserida noutra imagem ou vídeo. O que pode ser considerado como limitação é o facto de ser baseada

27 https://www.iwf.org.uk/

28 https://www.eokm.nl/

29 https://www.pointdecontact.net/

30 https://www.youtube.com/watch?v=NORlSXfcWIo

31 https://www.phash.org/

32 https://about.fb.com/news/2019/08/open-source-photo-video-matching/

num algoritmo qualificado cujo processamento em escala pode ser complexo. O algoritmo mais frequente é o SIFT (domínio público) processado pela empresa tecnológica Videntifier [33] (patenteada). Entre os que utilizam esta tecnologia estão a INTERPOL,[34] o Facebook (para direitos de autor) e algumas linhas diretas de denúncia, como a CyberTipline (para vídeos) ou a Point de Contact.

Identificação de vídeos

Os princípios acima descritos (FH, CV utilizando descritores globais e CV utilizando descritores locais) aplicam-se à identificação de vídeos. No entanto, a principal diferença entre a identificação de imagens e vídeos é que esta última abordagem tecnológica é extremamente exigente em recursos computacionais. Se o algoritmo e o sistema da base de dados não forem projetados para a máxima eficiência, a tecnologia de deteção pode funcionar em pequena escala, mas não funcionará no caso de grandes volumes de dados.

O fluxograma apresentado a seguir explica a solução de vídeo PhotoDNA da Microsoft com base em descritores globais.[35]

2.1.3. Inteligência Artificial

A terceira, e até à data, tecnologia menos utilizada, mas ao mesmo tempo a mais promissora na luta contra a OCSEA, é a inteligência artificial (IA). Esta tecnologia foi desenvolvida na década de 1950 e desde então evoluiu na década de 1980 com a *Machine* Learning, onde os algoritmos podem ser "treinados" a partir de conjuntos de dados. Desde a década de 2010 que envolveu outro subconjunto de capacidades que é a denominada *Deep Learning*.[36]

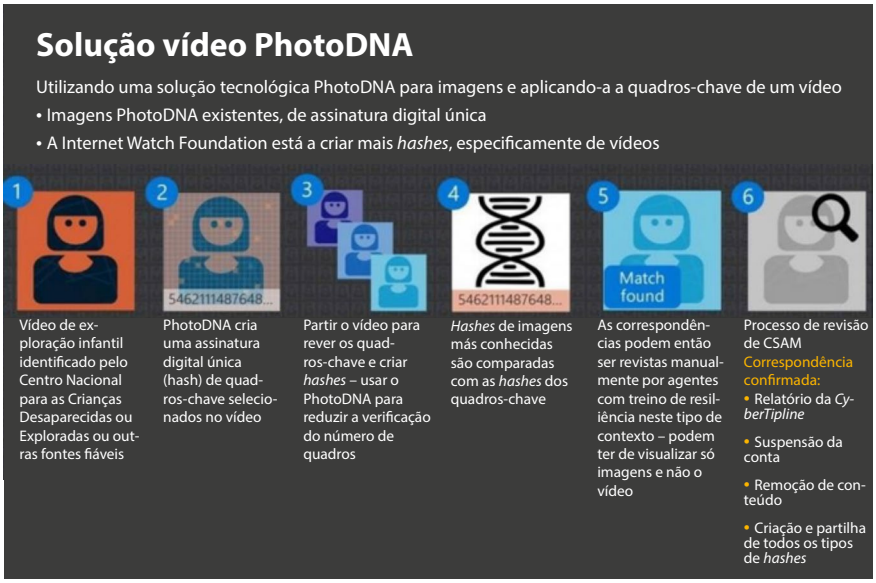
33 http://www.videntifier.com/

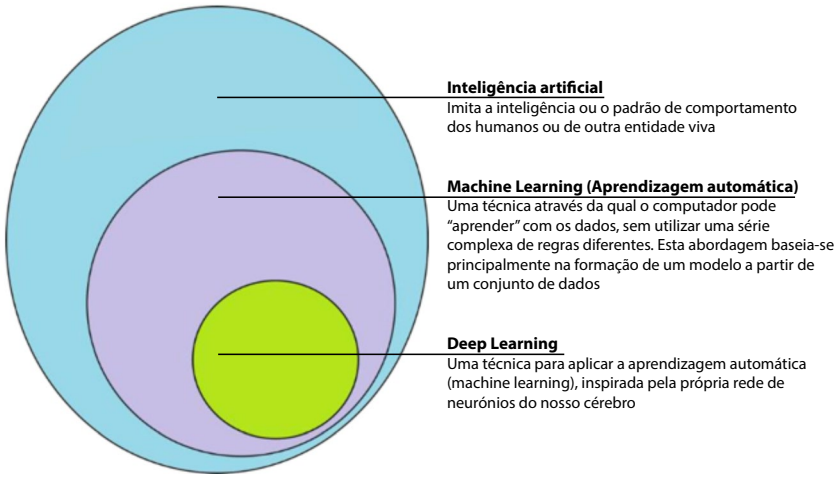
34 A Organização Internacional da Polícia Criminal (INTERPOL). É gerida pelo Secretário-Geral, e é composta por polícias e civis. Tem uma sede em Lyon, um complexo global de inovação em Singapura e vários escritórios satélites em diferentes regiões.

35 https://news.microsoft.com/on-the-issues/2018/09/12/how-photodna-for-video-is-being-used-to-fight- online-child-exploitation/

36 https://master-iesc-angers.com/artificial-intelligence-machine-learning-and-deep-learning-same-context- different-concepts/

O quadro apresentado a seguir dá uma visão geral simplificada das três famílias de IA.





37

Como a IA imita o cérebro humano, a sua utilização pode vir a gerar computadores capazes de detetar, por conta própria, situações de OCSEA e de as comunicar às autoridades com-

37 https://en.wikipedia.org/wiki/Deep_learning#Deep_learning_revolution

petentes. No entanto, a regulação do uso da IA constitui, neste momento, um vasto e complexo campo de pesquisa, que requer mecanismos diferentes dos utilizados para controlar a tecnologia CV.[38] Dois elementos devem ser considerados aqui:

- Qualidade do conjunto de dados – referimo-nos à origem do conjunto de dados em termos de metodologia da sua construção, ou seja, se envolveu a recolha de conversas públicas ou privadas, quais as organizações que estão envolvidas, ou se foi a indústria ou as autoridades de aplicação da lei a reunir e gerir, e de que forma, este conjunto de dados?

- Características do conjunto de dados – aqui são analisadas questões como quais os conteúdos em análise, apenas conversas de texto ou meta-dados, tais como a duração e frequência de comunicações, qual o idioma escolhido para o conjunto de dados, a existência de qualquer outra informação contextual incluída, como pode ser a data de criação da conta, a atividade da conta de utente, ou o uso de uma VPN para configurar uma conta.

2.1.4. Implicações para este relatório

O desafio crítico reside na identificação de meios de deteção de casos de OCSEA que sejam o menos restritivos possíveis, de forma a proteger efetivamente as vítimas. Responder a este desafio requer uma compreensão muito precisa do objetivo e do ambiente para os quais uma determinada tecnologia é selecionada.

Os seguintes elementos podem ser úteis na orientação deste processo:

- Complexidade do objetivo – a atividade de deteção de uma imagem idêntica previamente conhecida é menos complexa do que procurar imagens semelhantes. Detetar imagens semelhantes associadas a uma imagem conhecida, ou seja, retratar a mesma cena do crime, é menos complexo do que detetar a mesma pessoa. Quanto mais desafiante for o objetivo, mais complexa será a tecnologia envolvida;

- Complexidade da tecnologia - é possível aplicar tecnologias complexas a objetivos simples, sendo possível utilizar a tecnologia de *deep learning* para procurar imagens idênticas, ainda que também pudessem ser utilizadas soluções menos complexas nesses casos;

- Consolidação da tecnologia - quando se trata de definir salvaguardas, uma tecnologia bem testada, bem documentada e estável é a escolha mais segura para os

38 https://www.forbes.com/sites/cognitiveworld/2020/05/23/towards-a-more-transparent-ai/

decisores políticos. É mais difícil definir o nível adequado de salvaguardas no caso de tecnologias que estão na fase inicial de desenvolvimento;

• Complexidade do ambiente - o contexto da implantação tecnológica é significativamente importante, porquanto as salvaguardas vão depender de fatores chave. Estes estão relacionados com: o público-alvo do serviço, ou seja, por exemplo, destinado apenas a crianças, profissionais, público em geral, ou adultos; a utilização da tecnologia em ambientes públicos ou privados; a localização geográfica e o quadro legal aplicável nesse local.

2.2. Exemplos práticos da utilização de tecnologia automatizada para detetar a exploração e o abuso sexual de crianças em linha

Como já referido a utilização da tecnologia depende, em grande medida, do objetivo que se visa alcançar. No que se refere às formas conhecidas de OCSEA, a principal distinção reside na questão de saber se conteúdos, como o CSAM, e/ou comportamentos, como o aliciamento, são visados, bem como se a tecnologia é utilizada como uma medida proativa (prevenção) ou como uma medida reativa (deteção).

O quadro apresentado a seguir resume e simplifica a aplicabilidade das soluções tecnológicas anteriormente explicadas, suscetíveis de aplicação às principais formas de OCSEA. Tal mostra que a mesma série de soluções tecnológicas se encontram disponíveis quer para a previsão, quer para a deteção das principais formas de OCSEA. A sua escolha deve basear-se numa avaliação cuidadosa sobre qual de entre as tecnologias disponíveis é a mais eficiente para a finalidade considerada. A título de exemplo, no caso de se procurar a disponibilidade em linha do CSAM, verificamos que todas as três famílias de ferramentas de deteção automatizadas são aplicáveis: FH, CV e IA. No entanto, o seu modo de aplicação pode diferir significativamente, tendo em consideração os diferentes objetivos que se pretendem atingir.

	Prevenção	Deteção
Disponibilidade CSAM em linha	*File Hashing* Visão Computacional, como PhotoDNA Inteligência Artificial	*File Hashing* Visão Computacional, como PhotoDNA Inteligência Artificial
Aliciamento de crianças para fins sexuais	*File Hashing,* Visão Computacional, como PhotoDNA Inteligência Artificial, como a ferramenta anti aliciamento (texto, meta-dados, conteúdo visual)	*File Hashing,* Visão Computacional, como PhotoDNA Inteligência Artificial, como a ferramenta anti aliciamento (texto, meta-dados, conteúdo visual)
Imagens sugestivas ou explícitas de crianças e/ou vídeos produzidos, partilhados e recebidos pelas crianças	*File Hashing,* Visão Computacional, como PhotoDNA Inteligência Artificial, como a ferramenta anti aliciamento (texto, meta-dados, conteúdo visual)	*File Hashing,* Visão Computacional, como PhotoDNA Inteligência Artificial, como a ferramenta anti aliciamento (texto, meta-dados, conteúdo visual)
Coerção e extorção sexual	*File Hashing,* Visão Computacional, como PhotoDNA Inteligência Artificial, como a ferramenta anti aliciamento (texto, meta-dados, conteúdo visual)	*File Hashing,* Visão Computacional, como PhotoDNA Inteligência Artificial, como a ferramenta anti aliciamento (texto, meta-dados, conteúdo visual)
Abuso de crianças à distância e ao vivo	Visão Computacional (baseada em descritores locais) pode ajudar a identificar uma cena de crime (quarto ou edifício conhecido) Inteligência Artificial (texto, metadados, conteúdo visual)	*File Hashing* Visão Computacional (baseada em descritores locais) pode ajudar a identificar uma cena de crime (quarto ou edifício conhecido) Inteligência Artificial (texto, metadados, conteúdo visual)

2.2.1. Atividades orientadas para o conteúdo

Associação Internacional de Linha Diretas da Internet (INHOPE)

Um bom exemplo do uso das tecnologias FH e CV é a atividade da Associação Internacional de Linhas Diretas de Denúncia da Internet (INHOPE), criada em 1999. A INHOPE é atualmente composta por 47 linhas diretas de denúncia, que operam em 43 países. Cada linha direta permite que o público comunique anonimamente material online que suspeite ser ilegal, com foco no CSAM[39].

39 A descrição deste processo baseia-se no relatório INHOPE 2020, (disponível em: https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf).

A fim de recolher, trocar e classificar as comunicações do CSAM, as linhas diretas de denúncia utilizam uma plataforma segura chamada "I see Child abuse material" (ICCAM)[40] que também disponibiliza tecnologias de *hashing* de imagem/vídeo/impressão digital e de rastreio. Quando uma linha direta recebe uma denúncia do público, o analista da linha direta avalia o material reportado e, se ficar estabelecido que há material ilegal nessa página, o *Uniform Resource Locator* (URL)[41] é inserido no ICCAM, cuja principal característica é a automação. O sistema então rastreia todas as informações encontradas nesse URL, atribui um valor *hash* a cada imagem/vídeo e rastreia a localização da sua hospedagem. O valor de *hash* é comparado com as listas de *hash* existentes na base CSAM (ilegal, a nível internacional, de acordo com os critérios da INTERPOL),[42] e com o CSAM nacional (de acordo com a legislação nacional do país que recebe e do país de armazenamento) e identifica material único/já classificado. Se o conteúdo for único (não encontrado numa lista de *hash*), o analista pode então classificar cada imagem rastreada/vídeo separadamente como: base de referência (baseline), ilegal ou não ilegal a nível nacional.

40 A plataforma ICCAM foi desenvolvida pela INHOPE e pela Ziuz Forensics com financiamento da Comissão Europeia no âmbito dos programas do Mecanismo Internet Mais Segura e Interligar a Europa. Permite a colaboração de várias partes interessadas entre as linhas diretas, as agências de aplicação da lei (particularmente a INTERPOL) e a indústria.

41 URL é uma referência a um recurso web que especifica sua localização numa rede de computadores e um mecanismo para recuperá-lo. Um URL típico pode ter a forma: http://www.example.com/index.html.

42 O sistema de bases de referência permite que os agentes dos setores público e privado reconheçam, comuniquem e removam material conhecido de abuso sexual de crianças das suas redes. Podem fazê-lo verificando imagens e vídeos na lista da INTERPOL, que contém as «*assinaturas digitais*» de algumas das piores imagens e vídeos de abuso de crianças. Para serem incluídas na lista de base de referência, as imagens e vídeos de abuso infantil devem ser reconhecidos como tal por uma rede especializada de investigadores e satisfazer critérios específicos em termos de gravidade do conteúdo da imagem, por exemplo, aqueles que se acredita apresentarem crianças com idade igual ou inferior a 13 anos. Os critérios rigorosos garantem que a lista de bases de referência se refere apenas a imagens e vídeos que seriam considerados ilegais em qualquer país. Mais informações estão disponíveis em : https://www.interpol.int/Crimes/Crimes-against-children/Blocking-and-categorizing-content.

O fluxograma apresentado a seguir mostra os cenários mais comuns do processo de remoção de CSAM.

Este processo automatizado reduz tanto a quantidade de CSAM a que os analistas estão expostos, como a duplicação de trabalho. Por exemplo, em 2020, as comunicações feitas para a linha direta dos EUA, CyberTipline, incluíram 33,6 milhões de imagens, das quais 10,4 milhões eram únicas (utilizando CV com base em descritores globais), e 31,6 milhões de vídeos, dos quais 3,7 milhões eram únicos (usando CV com base em descritores locais).[43] Como relatado pela INHOPE, 60% de todos os URLs avaliados pelas linhas diretas de denúncia INHOPE, em 2020, provinham de material previamente avaliado, o que significa que o mesmo conteúdo está a difundir-se e a ser repetidamente reportado .[44]

Na maioria dos casos, a linha direta de receção informa as autoridades policiais e/ou judiciárias e emite uma Ordem de Aviso e Remoção[45] ao prestador responsável pelo armazenamento em causa, no caso de se concluir pela ilicitude do material que se encontra conservado em determinado servidor. Todas as imagens e vídeos assinalados como bases de referência, classificadas ilegais a nível nacional são disponibilizados à INTERPOL através de um portal ICCAM especificamente concebido para esse efeito. Consequentemente, a INTERPOL descarrega este material e transfere-o para inclusão na base de dados internacional de imagens de exploração sexual infantil (ICSE Database).[46]

Uma das principais características dos processos acima descritos é o nível de conhecimento dos analistas da linha de denúncia, que avaliam a ilegalidade do conteúdo reportado e decidem pela inserção da denúncia no ICCAM – concluindo-se que o conteúdo em causa é único e original (ou seja, não se encontra incluído numa lista de *hash*) - classifica cada imagem rastreada/vídeo como base de referência, nacional, ou não ilegal. Esta tarefa acarreta uma grande responsabilidade, pois se o conteúdo for incorretamente classificado vai servir de referência para futuros controlos cruzados, podendo potencialmente resultar numa série de falsos positivos. Algumas das linhas diretas de denúncia da INHOPE, como por exemplo, o IWF utiliza o método de verificação dos "três pares de olhos", através do

43 https://www.missingkids.org/gethelpnow/cybertipline

44 Relatório da INHOPE de 2020, p. 28.

45 Uma ordem de aviso e de remoção (como explicado no relatório de 2020 da INHOPE) é um procedimento que solicita a um prestador de armazenamento no servidor (HP) ou motor de busca que remova ou desative imediatamente o acesso a informações ilegais, irrelevantes ou desatualizadas alojadas nos seus serviços. As linhas diretas de denúncia da INHOPE enviam ordens de aviso e de remoção para as HP quando um membro do público lhes envia um URL contendo imagens e vídeos ilegais retratando o abuso e a exploração sexual de crianças.

46 A base de dados de imagens e vídeos da *International Child Sexual Exploitation* (ICSE) é uma ferramenta de informação e investigação, que permite que investigadores especializados de mais de 60 países partilhem dados, sobre casos de abuso sexual de crianças. A base de dados evita a duplicação de esforços e poupa tempo permitindo aos investigadores saber se uma série de imagens já foi descoberta ou identificada noutro país, ou se tem características semelhantes às de outras imagens. Possui mais de 2,7 milhões de imagens e vídeos e ajudou a identificar 23.500 vítimas em todo o mundo. Mais informações estão disponíveis em: https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database.

qual três analistas treinados analisam cada imagem e avaliam-na antes de uma imagem de *hash* ser incluída na lista.[47]

O papel específico do Centro Nacional para Crianças Desaparecidas e Exploradas (NCMEC, EUA)

A lei federal dos EUA exige que os PS baseados nos EUA reportem situações de aparente CSAM de que tenham conhecimento nos seus sistemas à CyberTipline do NCMEC.[48] Até ao momento, mais de 1.400 empresas estão registadas para reportar à CyberTipline do NCMEC.[49] Estas comunicações são vitais para ajudar a remover imagens de crianças em situações adversas e para impedir mais vitimização.

Em 2020, a CyberTipline recebeu mais de 21,7 milhões de denúncias, o que representa um aumento de 28% em relação a 2019 (16,9 milhões em 2019). Enquanto a maioria destas comunicações (21,4 milhões) foi obtida a partir de PSE (prestadores de serviços externos), 303 299 provieram do público, mais do que duplicando os números de 2019 (150 667 comunicações).[50] Tal como sugerido pelo NCMEC, um maior número de comunicações pode ser indicativo de múltiplos fatores, incluindo um número maior de utilizadores numa plataforma ou de quão robustos são os esforços de um PSE para identificar e remover conteúdo abusivo.[51]

Há mais de 30 empresas com acesso à plataforma do NCMEC, que contém mais de 7,1 milhões de *hashes* CSAM neste momento. A IWF[52] e o Canadian Centre for Child Protection também facultam uma lista de *hashes* (via plataforma *hash* do NCMEC) para empresas sediadas nos EUA. Como exemplo, indica-se que só a lista de *hash* do NCMEC contém 3,5 milhões de imagens e 385.000 vídeos. As próprias empresas também criam listas de *hash* CSAM, que partilham entre si (através de uma plataforma que o NCMEC disponibiliza). Este processo significa que o CSAM é frequentemente identificado e removido antes de o público ou de as linhas diretas de denúncia terem conhecimento disso. O NCMEC não utiliza o ICCAM nestes casos porque o conteúdo já foi removido da internet.

47 https://annualreport2020.iwf.org.uk/tech/keyservices/hash

48 18 U.S.C. § 2258A

49 https://www.missingkids.org/theissues/csam#bythenumbers

50 https://www.missingkids.org/gethelpnow/cybertipline

51 https://www.missingkids.org/content/dam/missingkids/gethelp/2020-reports-by-esp.pdf

52 https://www.iwf.org.uk/our-services/hash-list

O fluxograma apresentado em baixo mostra os cenários mais comuns do processo de comunicação e de partilha de ficheiros *hash* da *CyberTipline*

Serviço de Verificação de *Hash* - Expertise Bureau Online Kindermisbruik (EOKM, Países Baixos)

Um outro exemplo da utilização da tecnologia descrita é retirado da experiência da linha de denúncia dos Países Baixos, gerida pelo Escritório de Especialização sobre Abuso de Menores Online, o EOKM. Desde 2019, o EOKM oferece um serviço de verificação de *Hash* (HCS), que inclui uma base de dados de milhões de *hashes* de imagens que envolvem a exploração sexual de crianças. Através da utilização de uma plataforma eletrónica os utilizadores podem verificar imagens na base de dados e ver se existe algum registo deles próprios. Em 2020, o HCS verificou 18,2 bilhões de imagens, o que gerou cerca de 7,4 milhões de resultados (hits).[53] Graças a esta verificação, as empresas de armazenamento de dados conseguiram excluí-las dos seus servidores.

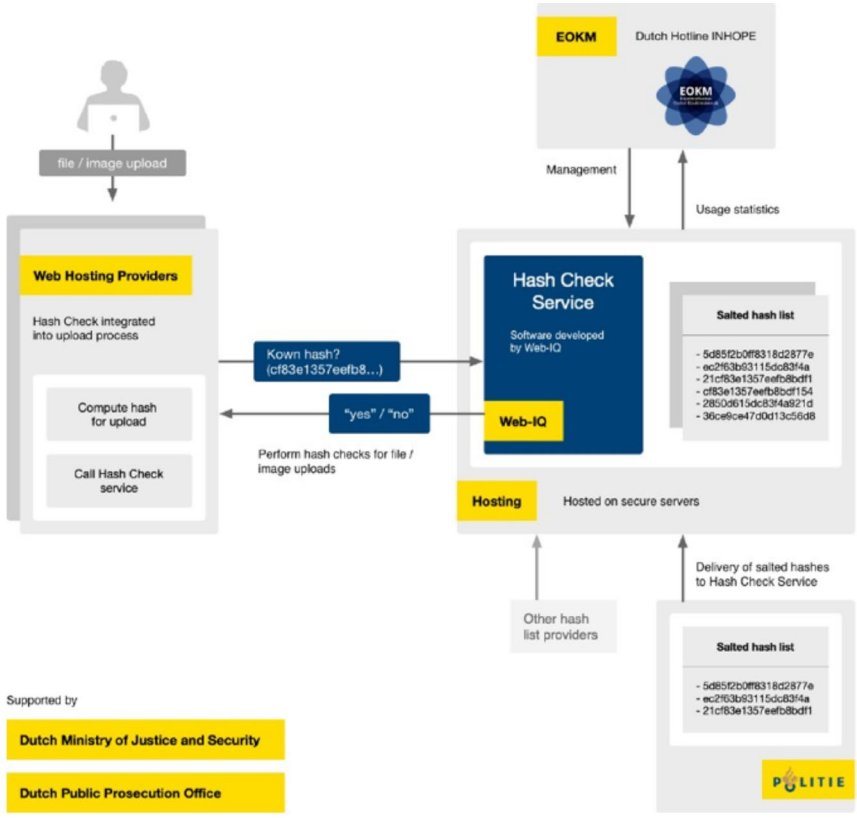
Tal como sugerido pelo EOKM, os números são elevados porque muitos utilizadores começaram por querer verificar todas as suas imagens de uma só vez. As expectativas vão no sentido de que o número de imagens verificadas diminuirá no futuro. No entanto, porque novos utilizadores se continuam a ligar ao HCS, é difícil fazer previsões definitivas nesta fase.[54]

53 Relatório do EOKM 2020, p. 10, (disponível em: https://www.eokm.nl/wp-content/uploads/2021/04/EOKM-Jaarveslag-2020-DEF-ENG.pdf).

54 Ibid.

No decurso de 2021, o EOKM lançará dois novos projetos: o primeiro projeto visa adquirir mais informações sobre o número de resultados (hits) que obtêm. Como estes são *hashes* em vez de imagens reais, são atualmente incapazes de analisar suficientemente o tipo de imagens que encontram, e assim dados mais precisos irão ajudar a obter respostas melhores. O segundo é um projeto piloto com *Web-IQ*[55], destinado a analisar como o efeito do servidor de verificação *hash* difere entre as partes que estão ligadas e as partes que não estão.

O seguinte fluxograma explica a funcionalidade do HCS:



Internet Watch Foundation (IWF, UK)

A IWF adotou uma outra abordagem para a utilização da tecnologia em causa, partilhando, em vez de oferecer um serviço de verificação de *hashes*, a Lista *Hash* da IWF, sob licença, com

55 https://web-iq.com/

os membros da IWF. Para tornar a sua utilização mais fácil para as empresas de tecnologia, cada imagem em *hash* é classificada de acordo com os padrões internacionais, para que as empresas tenham confiança nos dados que lhes são fornecidos. A IWF desenvolveu uma maneira eficiente de classificar os *hash* de milhões de imagens de abuso sexual de crianças: uma ferramenta de classificação de imagens, que também elimina a duplicação de *hashes* e imagens. Isso significa que também pode incorporar *hashes* ou imagens de outras organizações e automaticamente eliminar a duplicação de *hashes* existentes no sistema. Esta solução poupa ainda tempo e dinheiro, salvaguardando o bem-estar dos analistas que, de outra forma, teriam de ver imagens de abuso sexual de crianças, caracterizadas por serem de extrema violência para a saúde psicológica e emocional dos analistas.[56]

Exemplos de inovação

Nos últimos anos, registou-se um aumento dos esforços de pesquisa nesta área, desenvolvidos de forma proativa pelas linhas diretas de denúncia, sempre que a jurisdição nacional o permite. No entanto, é preciso notar que, embora as comunicações públicas levem predominantemente à descoberta de material anteriormente desconhecido, a pesquisa proativa apoia predominantemente a remoção de material já conhecido, que continua a reaparecer na internet.[57]

Na rede INHOPE, apenas a IWF pesquisou proativamente CSAM online, em 2020.[58] Tal foi possibilitado pela criação de um *web crawler* inteligente[59], carregado com mais de 566.000 *hashes* de imagens conhecidas de abuso sexual de crianças, que foi desenhado para navegar metodicamente em áreas-alvo da internet. De entre um conjunto de ferramentas projetadas para encontrar, remover e interromper a disponibilidade de material de abuso sexual de crianças o *crawler* é usado como tática operacional, de forma a produzir comunicações proativas para os analistas da IWF e verificar os domínios de um número crescente de membros proprietários de registo de domínio, que estão empenhados em tomar medidas preventivas para impedir que haja abuso nos seus serviços. As estatísticas mostram que a pesquisa proativa conduz à identificação de um número substancialmente maior de CSAM. Em 2020, rastrearam-se quase 42 milhões de páginas web e mais de meio bilhão de imagens. A busca

56 Relatório da IWF de 2020, (disponível em: https://annualreport2020.iwf.org.uk/tech/key-services/hash).

57 '*Study on framework of best practices to tackle child sexual abuse material online*', ("Estudo sobre o quadro das melhores práticas para combater o abuso sexual de crianças em linha"), realizado para a Comissão Europeia pelo ICF S.A, Wavestone and Grimaldi Studio Legale, p. 5, (disponível em: https://www.researchgate.net/publication/343813142_Study_on_Framework_of_best_practices_to_tackle_ch___ild_sexual_abuse_material_online_EXECUTIVE_SUMMARY_English).

58 Relatório da INHOPE 2020, p.33.

59 https://annualreport2020.iwf.org.uk/tech/new/crawlers

proativa resultou em 154.311 comunicações avaliadas, igual a 52% do número total de comunicações da IWF.[60]

Um outro exemplo de inovação nesta área encontra-se no Projeto *Arachnid*,[61] a funcionar desde 2016, no Canadá. A plataforma determina que um URL específico contém CSAM ao comparar a média exibida no URL com uma base de dados de assinaturas digitais conhecidas, que foram primeiro avaliadas por analistas como sendo CSAM. Se o CSAM for detetado, um aviso é enviado ao prestador do serviço de armazenamento a solicitar a sua remoção. Com capacidade para processar dezenas de milhares de imagens por segundo, o Projeto *Arachnid* deteta conteúdos a um ritmo que excede largamente o dos métodos tradicionais de identificação e tratamento deste material prejudicial para os mais novos.

O Projeto *Arachnid* consegue, nos dias de hoje, detetar mais de 100.000 imagens únicas por mês, que exigem uma avaliação dos analistas, e este número tem vindo a aumentar todos os meses. Os resultados do Projeto *Arachnid* são óbvios. A 1 de junho de 2021, mais de 127 bilhões de imagens foram verificadas, 39 milhões de imagens sinalizadas para revisão de analistas, mais de 7,5 milhões de avisos enviados aos prestadores, sendo que 85% dos avisos emitidos dizem respeito a vítimas que não foram identificadas antes pela polícia.[62] Este grande número de imagens sinalizadas para revisão por parte dos analistas precisou da colaboração das linhas diretas de denúncia de proteção infantil em todo o mundo. Em 2017, o Centro Canadiano criou o *Arachnid Orb* - um dispositivo que permite que outras linhas diretas internacionais trabalhem de forma colaborativa dentro do Projeto *Arachnid*.

O *Arachnid Orb* permite que analistas de todo o mundo agrupem os seus conhecimentos, reduzindo assim a duplicação de avaliações e, em última análise, aumentando o número de avisos que podem ser enviados através do Projeto *Arachnid*. Quanto maior o volume de *hashes* fiáveis e de qualidade garantida, mais eficaz o Projeto *Arachnid* se tornará na deteção de CSAM e na aceleração dos pedidos feitos aos prestadores para remover essas imagens e/ou vídeos.

A plataforma foi inicialmente projetada para rastrear *links* em sites, previamente comunicados à Cybertip.ca, que continham CSAM e detetar onde é que essas imagens e/ou vídeos estão a ser disponibilizados ao público. Atualmente o Projeto *Arachnid* continua a realizar as atividades de rastreamento descritas, mas está continuamente a evoluir e a adaptar-se para melhorar as suas capacidades no combate ao CSAM. Por exemplo, o *Shield by Project Arachnid* foi desenvolvido para ser utilizado pelos PS para melhorar e acelerar a deteção deste material prejudicial, facilitando assim a sua rápida remoção.

60 Ibid.

61 https://projectarachnid.ca/en/#what-is-it and https://www.protectchildren.ca/en/press-and-media/news- releases/2021/project-arachnid-csam-online-availability

62 Ibid.

Como nota final sobre as iniciativas orientadas para a partilha de *hashes*, há que mencionar um projeto recentemente atribuído pela DG CONNECT (CNET/LUX/2020/OP/0059)[63], com o objetivo de facilitar a rápida remoção de CSAM em linha. A solução conceptual será desenvolvida pela PwC EU Services[64] conjuntamente com o EOKM, a Rede Europeia de Serviços (ESN) e a Web-IQ, deverá facilitar a rápida e voluntária remoção de CSAM e melhorar a interoperabilidade, a interligação e a qualidade dos conjuntos de dados. Especificamente, contribuirá para a identificação proativa por parte de prestadores de serviço de armazenamento relativamente a CSAM já conhecido. A ferramenta também oferece uma opção menos invasiva para a indústria através da análise preventiva no momento do carregamento (*upload*) para filtrar material censurável na fonte. Com efeito, isto cria uma base harmonizada e holística para todas as partes interessadas recolherem, partilharem e utilizarem as bases de dados de *hash* inestimáveis, que catalogam todos os conteúdos conhecidos de CSAM. Esta iniciativa implica igualmente o reforço da transparência das medidas destinadas a combater a disponibilidade em linha de CSAM.

Um último exemplo de inovação, desta vez pela IWF, é o uso da IA para melhorar a capacidade de monitorização dos analistas, criando um classificador para ajudar na triagem de imagens[65]. Esta tecnologia utiliza a aprendizagem automática (machine learning) para sinalizar as comunicações mais suscetíveis de conter material de abuso sexual de crianças e aquelas que podem não conter esse tipo de material. Isso permitirá que os analistas priorizem o seu trabalho e se centrem nas comunicações que incluem imagens de crianças mais pequenas que são abusadas sexualmente. No entanto, há que salientar que, em termos de identificação das vítimas, é de vital importância que sejam pessoas a avaliar e a analisar o conteúdo. A IA ainda não chegou à fase em que consegue fazer distinções granulares[66]. Atualmente, estão a ser realizados projetos semelhantes por outras partes interessadas na segurança das crianças no Ciberespaço, como seja o projeto APAKT, liderado pela linha de denúncia direta polaca, Dyżurnet.pl.[67]

63 https://etendering.ted.europa.eu/cft/cft-display.html?cftId=6634

64 https://www.pwc.com/gx/en/services/european-union.html

65 https://annualreport2020.iwf.org.uk/tech/new/classifiers_e ainda_https://www.blog.google/around-the- globe/google-europe/using-ai-help-organizations-detect-and-report-child-sexual-abuse-material-online/

66 Ibid.

67 https://www.nask.pl/pl/dzialalnosc/nauka-i-biznes/projekty-badawcze/4100,System-reagujacy-na- zagrozenia-bezpieczenstwa-dzieci-w-cyberprzestrzeni-ze-szcze.html?-search=382648399

2.2.2. Atividades orientadas para o comportamento

Ferramenta anti aliciamento

O combate bem-sucedido de alguns dos tipos atualmente existentes de OCSEA exige a utilização de outras soluções tecnológicas para além das que se encontram orientadas para os conteúdos acima descritos. A técnica de deteção de aliciamento, recentemente anunciada, baseia-se na IA e visa comportamentos típicos dos predadores em linha que tentam aliciar crianças para fins sexuais. A partir da descrição publicamente disponível sobre a forma como a técnica funciona, pode-se inferir que a mesma não necessita de uma aprendizagem profunda (deep learning). O conjunto de dados parece ser, de facto, demasiado limitado para uma aprendizagem profunda, que requer milhares de milhões de dados.

O desenvolvimento desta nova técnica/ferramenta iniciou-se em novembro de 2018 e, a partir de janeiro de 2020, a sua licença e implementação ficou a cargo da *Thorn*.[68] A técnica pode ser usada, sem custos, por empresas tecnológicas com uma função de chat que procuram proteger as crianças de aliciamento em linha nas suas plataformas. As autoridades policiais e judiciárias e as organizações não-governamentais (ONG), também a podem utilizar.[69] Construída a partir da tecnologia patenteada da Microsoft "Identificação e quantificação do comportamento predatório entre sistemas de comunicação", a técnica é aplicada ao histórico de conversas baseadas em texto. Avalia e "calcula" as características da conversação e atribui uma classificação de probabilidade global. Esta classificação pode então ser usada como um determinante, definido pelas empresas individuais que implementam a técnica, sempre que uma conversa sinalizada deva ser enviada a moderadores humanos para revisão. Os moderadores humanos conseguem assim identificar ameaças iminentes que encaminham para as autoridades de investigação criminal, incluindo o envio de incidentes de suspeita de exploração sexual de crianças para o NCMEC.[70]

No momento em que se escreve este texto, a disponibilidade de informações públicas sobre o estado da implementação desta tecnologia pela indústria e pelas autoridades de aplicação da lei é muito limitada. Sabe-se que a *Microsoft* tem vindo a aproveitar a técnica em programas incluídos na sua plataforma *Xbox* há vários anos e que está a explorar o seu uso em serviços de chat, incluindo o *Skype*.[71]

---

68 *Thorn*: Digital Defenders of Children, anteriormente conhecida como DNA Foundation, é uma organização internacional anti tráfico que aborda a exploração sexual de crianças. Os principais esforços de programação da organização concentram-se na tecnologia da Internet e no papel que esta desempenha na facilitação da pornografia infantil e da escravidão sexual de crianças numa escala global. A organização foi fundada pelos atores americanos Demi Moore e Ashton Kutcher.

69 https://www.thorn.org/blog/what-is-project-artemis-thorn-microsoft-grooming/

70 https://blogs.microsoft.com/on-the-issues/2020/01/09/artemis-online-grooming-detection/

71 Ibid.

IWF reThink Chatbot

O último exemplo de soluções tecnológicas que visam comportamentos em linha é um chatbot interativo que está a ser desenvolvido pela IWF, como parte de um projeto, com a duração de dois anos, financiado pelo "End of Violence Fund".[72] O chatbot visa reduzir a procura de material de abuso sexual de crianças em linha e restringir as pessoas que tentam aceder a estas imagens, impedindo-as de cometer um crime. O IWF reThink Chatbot interagirá com os utilizadores da internet que mostrem sinais de estar à procura de imagens de abuso sexual infantil. Tentará envolvê-los numa conversa amigável e solidária e, no momento certo, irá sinalizá-los para a ajuda e intervenção de que precisam. Este projeto visa lançar um piloto até ao final de 2021, com uma plena implementação operacional em 2022. Acredita-se que este projeto tem um enorme potencial e que vai ajudar na luta proativa contra o abuso e a exploração sexual de crianças em linha.

2.2.3. Implicações para o presente relatório

É importante salientar que os exemplos práticos da utilização da tecnologia automatizada para detetar a OCSEA acima referidos dependem da existência de uma decisão humana que se responsabilize pelo emprego das soluções tecnológicas utilizadas. A intervenção humana continua a ser vital em todos os aspetos da área em discussão: desde a escolha dos conjuntos de dados para treinar a tecnologia até à definição sobre o conteúdo ilegal reportado.

Em circunstâncias específicas, como o caso do aliciamento e do seu potencial risco de proliferação em todas as plataformas que oferecem funções de *chat*, a utilização de tecnologias automatizadas é essencial, uma vez que faculta atualmente o único meio possível para analisar grandes volumes de dados e salvar a criança antes de a exploração ocorrer.

Embora existam preocupações globais relacionadas com as operações comerciais de certas empresas do setor privado, entende-se que seguindo a opinião de profissionais experientes no combate à OCSEA, estas preocupações devem ser consideradas irrelevantes para a utilização de medidas de *hashing* e de aliciamento para combater a OCSEA. Tal como referido pelos representantes do NCMEC quando se dirigiram aos deputados do PE sobre a apreciação da proposta de Regulamento relativo a uma derrogação temporária de determinadas disposições da Diretiva *e-Privacy*: "A tecnologia de *hashing* para combater a OCSEA tem sido utilizada há quase 20 anos e, com base nesta experiência, pode afirmar-se que o *hashing* e os indicadores de aliciamento mais recentes, quando utilizados em relação à OCSEA, não monitorizam ou identificam atividades em linha não relacionadas e envolvem sempre algum nível de revisão humana ou secundária. Quando um serviço em linha utiliza tecnologia de *hashing* para detetar abusos sexuais de crianças em linha, não cataloga nem compreende

72 https://annualreport2020.iwf.org.uk/tech/new/chatbots

o conteúdo que analisa, apenas procura imagens específicas de abuso sexual de crianças, que é treinado para reconhecer. Todos os outros conteúdos passam sem qualquer reconhecimento, conhecimento ou catalogação. Os indicadores de aliciamento funcionam de forma semelhante; só uma combinação de fatores específicos é que produz um alerta".

Embora as vozes profissionais de pessoas experientes no combate à OCSEA sejam muito importantes no discurso público, uma maior transparência na utilização de tecnologias de deteção automatizada reforçaria o desenvolvimento de mecanismos de responsabilização. O levantamento dos tipos de aplicações existentes, incluindo uma descrição das funções e responsabilidades de todos os intervenientes, deverá constituir o primeiro passo para reforçar este nível de transparência e de responsabilização.

3. ENQUADRAMENTO JURÍDICO

3.1. Diretiva relativa à privacidade e às comunicações eletrónicas (EPrivacy) e o Código Europeu das Comunicações Eletrónicas

O contexto do debate no PE sobre uma derrogação temporária a certas disposições da Diretiva *e-Privacy*, mencionada na introdução do presente documento, servirá de ponto de partida para a análise do enquadramento jurídico aplicável.

A 10 de setembro de 2020, a CE publicou uma "Proposta de Regulamento relativa a uma derrogação temporária a determinadas disposições da Diretiva e-Privacy no que respeita à utilização de tecnologias por parte de prestadores de serviços de comunicações interpessoais independentes do número para o tratamento de dados pessoais ou de outro tipo para efeitos de luta contra o abuso sexual de crianças em linha"[73]. A CE considerou que tal derrogação era necessária, uma vez que com a aplicação integral do Código Europeu das Comunicações Eletrónicas (EECC)[74] a partir de 21 de dezembro de 2020, os prestadores de determinados serviços de comunicações em linha, incluindo NI-ICS (como por exemplo serviços de voz sobre Protocolo Internet, serviços de mensagens eletrónicas baseados na WEB) seriam abrangidos pelo âmbito de aplicação da Diretiva *e-Privacy*.

Uma das principais consequências do EECC foi alterar a situação jurídica de certos serviços de comunicação em linha, sujeitos até então, à Diretiva sobre o Comércio Eletrónico, que opera com base num país de origem, ou seja, os PS estabelecidos num Estado Membro são livres de prestar serviços nos outros Estados Membros sem restrições adicionais.[75] Embora

73 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0568

74 Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2018, que estabelece o Código Europeu das Comunicações Eletrónicas. Jornal Oficial da União Europeia, L 321, 17.12.2018, (disponível em: https://eur-lex.europa.eu/eli/dir/2018/1972/oj).

75 Diretiva 2000/31/CE relativa a certos aspetos legais dos serviços da sociedade de informa-

os Estados Membros possam tomar medidas derrogatórias deste princípio , em relação a determinados serviços da sociedade de informação , caso sejam preenchidas certas condições como "a prevenção, investigação, deteção e incriminação de delitos penais, incluindo a proteção de menores",[76] na maioria dos Estados Membros a legislação que permitia às autoridades responsáveis pela aplicação da lei solicitar dados aos PS estava ligada ao seu estatuto de "prestadores de serviços de comunicações eletrónicas" e, por conseguinte, os poderes não eram geralmente exercidos contra os prestadores de comunicações em linha.[77]

Com a entrada em vigor do EECC, estes PS são agora abrangidos por um regime regulamentar que funciona segundo o princípio do país de destino, ou seja, os PS estão sujeitos à legislação de cada Estado Membro em que prestam serviços. Esta mudança regulamentar significa agora que os PS das comunicações em linha estão, de um modo geral, abrangidos pelo âmbito de aplicação das regras de processo penal nacionais relativas à interceção e dados de comunicações conexos, bem como pelas disposições da Diretiva e-Privacy aplicáveis aos prestadores de "serviços de comunicações eletrónicas".

A proposta de derrogação temporária foi vital para permitir que as atividades voluntárias que envolvem a utilização de tecnologias automatizadas destinadas à deteção, comunicação e remoção de CSAM prosseguissem após 21 de dezembro de 2020. Além disso, a proposta era igualmente necessária para dar tempo para a adoção de legislação setorial específica para combater mais eficazmente a OCSEA, respeitando ao mesmo tempo os direitos fundamentais, incluindo o direito à privacidade e a liberdade de expressão.

Os desafios inerentes ao equilíbrio entre a privacidade e a proteção das crianças, abordados na proposta da CE, deram origem a um debate importante entre várias partes interessadas, incluindo as que estão ativamente envolvidas no combate à OCSEA. Vale a pena referir que empresas do setor privado como a *Google*, *LinkedIn*, *Microsoft*, *Roblox* e *Yubo* se comprometeram publicamente a continuar a fazer esforços proativos na deteção e comunicação de OCSEA, enquanto a UE deliberou sobre os próximos passos a dar.[78]

Analisam-se a seguir três pareceres relevantes para a problemática em questão: a Autoridade Europeia para a Proteção de Dados, a Comissão das Liberdades Cívicas e o Comité Económico e Social Europeu.

ção, em especial do comércio eletrónico, no mercado interno, Jornal Oficial L 178/1, 17 julho 2000.

76 Ibid., Art. 3(4)(a)(i).

77 Cf. *Google LLC v Bundesrepublik Deutschland (C-193/18)* [2019] 1 W.L.R. 6044.

78 https://www.missingkids.org/blog/2020/we-are-in-danger-of-losing-the-global-battle-for-child-safety

3.1.1. Parecer da Autoridade Europeia para a Proteção de Dados

A Autoridade Europeia para a Proteção de Dados (AEPD) publicou, a 10 de novembro de 2020, o Parecer 7/2020 sobre a proposta da CE.[79] A AEPD observou que "a confidencialidade das comunicações é uma pedra angular dos direitos fundamentais relativos ao respeito pela vida privada e familiar e à proteção dos dados pessoais" e que as medidas previstas na proposta interferirão com os "direitos ao respeito pela vida privada e à proteção de dados das pessoas em causa (utilizadores, infratores e vítimas)". Além disso, a AEPD considerou que a "análise geral, indiscriminada e automatizada de todas as comunicações em texto transmitidas através de NI-ICS com vista à identificação de potenciais novas infrações não respeita o princípio da necessidade e da proporcionalidade. Mesmo que a tecnologia utilizada se limite à utilização de "indicadores-chave relevantes", a AEPD considerou que a implementação dessa análise geral e indiscriminada é excessiva". A AEPD observou igualmente que "a análise automatizada da fala ou do texto com vista a identificar potenciais casos de aliciamento de crianças é suscetível de constituir uma interferência mais significativa do que a correspondência de imagens ou vídeos com base em casos previamente confirmados de "pornografia infantil".

Em termos de necessidade e proporcionalidade, a AEPD salientou que "devido à ausência de uma avaliação de impacto que acompanhe a proposta, a CE ainda não demonstrou que as medidas previstas na proposta são estritamente necessárias, eficazes e proporcionadas para alcançar o objetivo pretendido". A AEPD, em primeiro lugar, solicitou à CE que facultasse informações adicionais que permitissem aos co-legisladores analisar se as medidas previstas satisfazem os requisitos de necessidade, eficácia e de proporcionalidade. De acordo com o parecer da AEPD, a fim de avaliar o impacto de uma medida nos direitos fundamentais à privacidade e à proteção dos dados pessoais, era imperativo identificar com precisão[80]:

- O âmbito de aplicação da medida, incluindo o número de pessoas afetadas e possibilidade de gerar "intrusões colaterais" (ou seja, interferência com a privacidade de outras pessoas que não os sujeitos da medida);
- A extensão da medida, incluindo a quantidade de informações recolhidas; por quanto tempo; se a ação em apreço exige a recolha e o processamento de categorias especiais de dados;
- O nível de intrusão, tendo em conta: a natureza da atividade sujeita à medida - se afeta ações abrangidas pelo dever de confidencialidade ou não, a relação advoga-

79 Autoridade Europeia para a Proteção de Dados, «Parecer 7/2020 sobre a proposta de derrogações temporárias à Diretiva 2002/58/CE para efeitos de luta contra o abuso sexual de crianças em linha», (disponível em:https://edps.europa.eu/sites/default/files/publication/20-11-10_opinion_combatting_child_abuse_en.pdf

80 Ibid.

do-cliente, atividade médica; o contexto - quer se trate ou não da caracterização dos indivíduos em causa, ou o processamento implique a utilização de um sistema de tomada de decisão (parcial ou totalmente) automatizado com uma "margem de erro".

- Se diz respeito ou não a pessoas vulneráveis;
- Se afeta também outros direitos fundamentais.

A AEPD mostrou-se também particularmente preocupada com o facto de a proposta não ter explicado o modelo de regulamentação aplicável aos prestadores de serviços externos (PSE) que utilizam a derrogação, incluindo a forma de comunicação ou a entidade de reporte, ou ainda a entidade responsável pela manutenção e atualização das bases de dados pertinentes para identificar futuras instâncias de OCSEA. Além disso, a AEPD recomendou que a validade de qualquer medida transitória não deveria exceder dois anos.

3.1.2. Relatório da Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos

A Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos (LIBE) do PE publicou, a 11 de dezembro de 2020, um relatório sobre a proposta da CE.[81] A apreciação geral da Comissão LIBE foi a de que "a proposta de regulamento não previa, por si só, uma base jurídica para a análise da comunicação pelos respetivos prestadores de serviços externos (PSE). Em vez disso, previa a restrição de certos direitos e obrigações estabelecidos na Diretiva *e-Privacy* e criou salvaguardas adicionais a serem respeitadas pelos prestadores de serviços, caso estes pretendam recorrer a este regulamento".[82]

Além disso, a Comissão LIBE clarificou o âmbito de aplicação da medida e declarou que a proposta da CE "deve aplicar-se apenas a vídeos, ou imagens, partilhados através de serviços de mensagens ou de correio eletrónico. Não deve aplicar-se à análise de texto ou comunicação áudio, que continua inteiramente sujeita às disposições da Diretiva *e-Privacy*". Tendo em conta o seu caráter temporário, o âmbito de aplicação material do regulamento deve

81 Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos do Parlamento Europeu. «Relatório sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo a uma derrogação temporária a certas disposições da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho no que diz respeito à utilização de tecnologias por fornecedores de serviços de comunicações interpessoais independentes do número para o tratamento de dados pessoais e outros para efeitos de luta contra o abuso sexual de crianças em linha» (COM(2020)0568 - C9-0288/2020 - 2020/0259(COD)), (disponível em: https://www.europarl.europa.eu/doceo/document/A-9-2020-0258_EN.html).

82 Conforme expresso na Exposição de Motivos, para. a.

limitar-se à definição estabelecida de "pornografia infantil" e de "espetáculo pornográfico", tal como definido na Diretiva 2011/93/UE (Diretiva CSEA). [83]

De acordo com a LIBE,[84] a fim de assegurar a proporcionalidade da restrição aos direitos fundamentais, os prestadores de NI-ICS que desejem recorrer a este regulamento, deverão preencher determinadas condições, nomeadamente:

- Premente à utilização de tecnologia, proceder a uma avaliação de impacto, obrigatória, sobre a proteção de dados, e lançar um procedimento de consulta obrigatória, conforme exigido pelos artigos 35.º e 36.º do RGPD);
- Utilizar como base jurídica o artigo 6.º, n.º 1, alíneas d) ou e), do RGPD;
- Garantir uma visão geral e a obrigatoriedade de intervenção humana em qualquer tratamento de dados pessoais e que nenhum resultado positivo seja enviado às autoridades responsáveis pela aplicação da lei ou organizações que atuem no interesse público sem prévia revisão humana;
- Implementar procedimentos e mecanismos de reparação adequados, que não admitam nenhuma interferência com qualquer comunicação protegida pelo sigilo profissional; e a utilização de uma base jurídica adequada no caso de transferência de dados pessoais para fora da UE, em conformidade com o capítulo V do RGPD;
- Vias de recurso eficazes proporcionadas pelos Estados Membros a nível nacional.

Quanto ao limite temporal do regulamento proposto, a Comissão LIBE observou que o período de aplicação do regulamento da CE deve ser limitado até 31 de dezembro de 2022. No caso de futura legislação, de longo prazo, vir a ser adotada e entrar em vigor antes dessa data, essa legislação deve revogar o regulamento.

3.1.3. Parecer do Comité Económico e Social Europeu

No parecer publicado a 11 de janeiro de 2021, o Comité Económico e Social Europeu (EESC)[85]

83 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, (disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093).

84 Conforme expresso na Exposição de Motivos, para. c.

85 Parecer do Comité Económico e Social Europeu sobre a "Proposta de regulamento do Parlamento Europeu e do Conselho relativo a uma derrogação temporária a certas disposições da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho no que diz respeito à utilização de

salientou o seu acordo geral com a proposta de regulamento relativamente a uma derrogação temporária e estritamente limitada ao artigo 5.º, n.º 1 e ao artigo 6.º da Diretiva *e-Privacy*. O EESC entende que, para salvaguardar a privacidade e a proteção dos dados pessoais:[86]

- O processamento de dados deve ser proporcionado e limitar-se a tecnologias consolidadas, utilizadas normalmente pela NI-ICS para a referida finalidade;
- A tecnologia utilizada deve estar em conformidade com a tecnologia mais moderna utilizada pela indústria e invadir a privacidade com a menor intensidade possível;
- A tecnologia utilizada deve, por si só, ser suficientemente fiável para limitar ao máximo possível a taxa de erro e, caso ocorram, as suas consequências devem ser rapidamente retificadas;
- A tecnologia utilizada para detetar o aliciamento de crianças deve limitar-se à utilização de indicadores-chave;
- O processamento deve ser limitado ao estritamente necessário para esse fim, mas a remoção deve ocorrer de imediato quando exista deteção de OCSEA em linha;
- O prestador deverá estar obrigado a publicar um relatório anual sobre o tratamento de dados por si efetuado neste contexto.

O EESC não se pronunciou a favor do prazo de derrogação proposto (até 31 de dezembro de 2025) e defende que a CE deveria assegurar o desenvolvimento e implementação das salvaguardas adequadas em matéria de privacidade das crianças antes do decurso de cinco anos.

3.1.4. Implicações para o presente relatório

De acordo com os valores recentemente comunicados pelo NCMEC, a situação supra debatida impactou o nível de comunicação de OCSEA. O centro registou uma diminuição de 58% na comunicação de casos relacionados com a OCSEA da UE, desde 21 de dezembro de 2020, altura em que os novos regulamentos entraram em vigor.[87]

---

tecnologias por fornecedores de serviços de comunicações interpessoais independentes do número para o tratamento de dados pessoais e outros para efeitos de luta contra o abuso sexual de crianças em linha», (disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020AE4192&rid=2).

86 Ibid, para. 2.5.

87 https://www.missingkids.org/blog/2020/we-are-in-danger-of-losing-the-global-battle-for-child-safety

Por conseguinte, é muito importante notar que, a 29 de abril de 2021, a UE chegou a um acordo provisório sobre a legislação temporária acima discutida. Foram acordadas várias salvaguardas e o processo de elaboração da legislação, de longo prazo, teve início com propostas a elaborar pela CE até ao verão de 2021. De acordo com o comunicado de imprensa do PE[88] "as alterações acordadas preveem uma derrogação de normas sobre o sigilo dos dados de tráfego que regem a privacidade das comunicações eletrónicas e que permitem aos prestadores de serviços de correio eletrónico, de texto e de mensagens na Internet detetar, remover e comunicar voluntariamente o abuso sexual de crianças em linha, bem como utilizar tecnologias de análise para detetar o aliciamento cibernético. (...). Os negociadores do Parlamento garantiram que as autoridades nacionais de proteção de dados terão uma maior supervisão sobre as tecnologias utilizadas, existirá um mecanismo de reclamação e de recurso mais eficiente e que os dados processados terão de ser analisados por uma pessoa antes de serem comunicados. Os prestadores de serviços terão também de melhorar a sua comunicação sobre estatísticas relativas a este fenómeno. Esta legislação temporária deve aplicar-se por um período máximo de três anos, ou menos, caso, entretanto, sejam acordadas novas regras permanentes em matéria de luta contra o abuso sexual de crianças em linha".

No momento da redação do presente documento, o texto final e aprovado da proposta da CE não foi tornado público.

3.2. Conduta dos prestadores de serviços

A presente secção analisa a natureza jurídica do PS, as complexidades jurisdicionais decorrentes da prestação de serviços transfronteiriços e a base legal para monitorizar e comunicar a disponibilidade em linha de CSAM.

3.2.1. O conceito de "prestador de serviço"

A Convenção de Budapeste define o conceito de "prestador de serviços" nos seguintes termos:

- Qualquer entidade pública ou privada que faculte aos utilizadores dos seus serviços a possibilidade de comunicarem por meio de um sistema informático, e

88 Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos. Comunicado de imprensa. "Acordo provisório sobre regras temporárias para detetar e remover o abuso de crianças em linha", 30 Abril 2021, (disponível em: https://www.europarl.europa.eu/news/en/press-room/20210430IPR03213/provisional-agreement-on- temporary-rules-to-detect-and-remove-online-child-abuse).

- Qualquer outra entidade que processe ou armazene dados informáticos em nome desse serviço de comunicações ou dos seus utilizadores [89].

Trata-se de uma abordagem deliberadamente muito ampla, que inclui tanto o prestador tradicional de serviços de telecomunicações como uma vasta gama de PS em linha que armazenam conteúdos em nome dos utilizadores, tais como os prestadores que suportam a utilização das redes sociais.[90] A CB vai além do EECC e pode incluir entidades que prestam o que é denominado no direito da UE como "serviços da sociedade da informação"[91] e "serviços de comunicação social audiovisual"[92], desde que o serviço inclua "serviços de comunicação ou de tratamento de dados conexos".[93]

Importa igualmente salientar que a definição de PS nos termos das regras nacionais que regem a prestação de serviços para fins regulatórios não está necessariamente em consonância com a definição de PS para efeitos de processo penal. A segunda pode ser mais ampla do que a primeira, como é o caso do Reino Unido[94] e da Bélgica.[95]

3.2.2. Enquadramento jurídico

A implementação de sistemas para combater a OCSEA implica que os PS adotem duas formas principais de conduta, a deteção (incluindo a remoção) e a comunicação. A deteção envolve a monitorização e a análise dos dados dos utilizadores, geralmente identificados em três categorias principais:

- Conteúdo, quer em transmissão quer em pausa;

89 Artigo 1c.

90 Exposição de Motivos, para. 27.

91 Diretiva (UE) 2015/1535, de 9 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação, Jornal Oficial da União Europeia, J L 241/1, 17 setembro 2015, (disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2015:241:FULL&from=RO).

92 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 95/1, 15 abril 2010, alterada pela Diretiva (UE) 2018/1808, (disponível em: https://eur-lex.europa.eu/eli/dir/2010/13/oj).

93 Exposição de Motivos, para. 27.

94 Lei dos poderes de investigação 2016, s. 261(11) e (12). (disponível em: https://www.legislation.gov.uk/ukpga/2016/25/section/261).

95 Procurador Geral Bij Het Hof van Beroep te Gent v Yahoo! Inc., Court of Cassation of Belgium, No. P.10.1347.N, 18 January 2011.

• Dados de tráfego, detalhando as características das atividades de comunicação de um utilizador;[96]

• Informações do assinante, dadas ao PS quando este entra numa relação com o cliente.[97]

A base "legal" para qualquer processamento tem conotações quer negativas quer positivas. Negativas, no sentido de que o processamento não deve violar nenhuma obrigação legal, como as obrigações de confidencialidade e a interceção ilegal. Positivas no sentido de ter uma justificação legal, como exigido pela lei de proteção de dados.[98] A base jurídica para o processamento também pode variar dependendo do tipo de dados que estão a ser processados.[99]

Em termos de comunicação de OCSEA, seja a uma autoridade pública de aplicação da lei (polícias, Ministério Público ou Tribunais) ou a uma linha de denúncia direta reconhecida, a natureza potencial de qualquer divulgação pode ser amplamente reconhecida em quatro cenários:

1. Voluntária - um PS pode fazer uma comunicação numa base puramente voluntária. Normalmente, tal exigirá uma previsão legal, a acrescer a uma cláusula contratual vigente entre o PS e o utilizador. De notar, que a validade de tal singela autorização por parte do utilizador ao PS pode ser contestada, na medida em que o consentimento de um utilizador em ficar vinculado nesses termos pode ser considerado inválido devido ao estatuto deste (quando criança), à forma como o consentimento foi obtido ou ao facto de o próprio termo de autorização poder estar em violação de regras obrigatórias;

2. Voluntária qualificada - a comunicação voluntária pode ocorrer de acordo com um quadro legal que permita expressamente essa divulgação, especificando frequentemente as circunstâncias e condições particulares em que a divulgação pode ser efetuada e concedendo ao PS imunidade em relação a qualquer responsabilidade que possa surgir;[100]

96 BC, Art. 1d.

97 BC, Art. 18(3).

98 RGPD, Art. 6.

99 Cf Diretiva e-Privacy, Art. 6 em relação aos dados de tráfego.

100 Cf. Lei de Proteção de Dados do Reino Unido 2018, Sch. 2, Pt. 1, para. 2.

3. Obrigatória mediante o estabelecimento de responsabilidade - um PS pode comunicar proativamente a OCSEA identificada porque tem o dever legal de comunicar tal material. A falta de reporte pode resultar em responsabilidade por não conformidade, sendo aplicável uma coima, de natureza administrativa ou prevendo-se, também, responsabilidade conjunta (quer como um infrator primário ou secundário);[101]

4. Obrigatória mediante pedido - um PS pode receber um pedido oficial, de "um tribunal ou de uma autoridade administrativa independente",[102] para divulgar dados relacionados com a investigação da conduta criminosa de um utilizador.

Nenhum dos cenários, 1 ou 4 parece poder constituir uma sustentação jurídica adequada para facilitar a implementação de sistemas automatizados de deteção de OCSEA pelos prestadores de serviços externos. No cenário 1, a base jurídica situa-se principalmente no direito privado, o que apresenta riscos significativos tanto para os interesses dos PS como para os direitos dos utilizadores. Embora o cenário 4 possa representar o quadro jurídico mais robusto, é de natureza reativa, ao retirar a responsabilidade pela monitorização de tais tipos de dados dos PS, e seria desajustado tendo em conta os volumes envolvidos. O cenário 3, pode gerar preocupações quanto às potenciais implicações da divulgação de informações baseadas na responsabilidade da conduta dos PS, incluindo a possibilidade de comunicar em excesso, e consequentes impactos adversos nos utilizadores, nas linhas diretas de denúncia e nas autoridades responsáveis pela aplicação da lei.

Embora estes cenários sejam apresentados como alternativas, a concorrência jurisdicional num ambiente transfronteiriço pode fazer surgir um quadro mais complexo. Do ponto de vista de um PS, que esteja estabelecido num território, o cumprimento de uma obrigação noutro território em que presta serviços pode ser entendido como "voluntário" ou, pelo menos, "inexequível".[103] A questão de saber se a atuação do PS é legal pode exigir uma decisão judicial, que qualquer uma das partes pode não estar disposta a perseguir.

101 Cf. US (18 U.S.C. § 2258A) a lei Italiana.

102 Tele2 Sverige AB v Post-och Telestyrelsen [2017] 2 C.M.L.R 30. Ver também Szabó and Vissy v Hungary (2016) 63 E.H.R.R. 3, para. 77.

103 A Cloud Act dos EUA, por exemplo, suprime a disposição de "bloqueio" ao abrigo da Lei relativa às Comunicações Armazenadas no que diz respeito a pedidos das autoridades de aplicação da lei dos países com os quais os EUA celebraram um acordo bilateral (18 U.S.C. 2511(2)(j)). No entanto, não impõe a divulgação de informações.

3.2.3. Proposta de regulamento da UE relativo à deteção, remoção e denúncia de abuso sexual de crianças em linha

No contexto da conduta dos PS, é também muito útil apresentar cenários propostos pela CE no âmbito da iniciativa destinada a definir as responsabilidades dos PS em linha relevantes, exigindo-lhes que detetem e denunciem o abuso sexual de crianças em linha e comuniquem esse material às autoridades públicas.

Em dezembro de 2020, a CE lançou um convite público à apresentação de comentários sobre uma Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à deteção, remoção e denúncia de abusos sexuais de crianças em linha. De acordo com a Avaliação de Impacto Inicial[104] em relação a esta iniciativa a CE sustenta-se que, "os esforços para combater o abuso sexual de crianças na UE são fragmentados, duplicados e/ou insuficientes em alguns domínios, como demonstrado, em particular, pela monitorização da aplicação da Diretiva CSEA. Em especial, os esforços para prevenir o abuso sexual de crianças em linha e fora de linha na UE são insuficientes, descoordenados e têm uma eficácia pouco clara, ao passo que a eficiência e a eficácia dos esforços dos Estados Membros para ajudar as vítimas de abuso sexual de crianças são limitadas, uma vez que não utilizam sistematicamente as melhores práticas existentes e as lições aprendidas noutros Estados Membros ou a nível mundial (...)".

No que diz respeito às opções legislativas, a CE irá desenvolver várias opções políticas com base numa análise mais profunda, centrando-se, em particular, nas seguintes medidas possíveis a nível da UE:

- Um quadro jurídico que estabeleça uma base jurídica clara ao abrigo da qual os PS relevantes poderiam optar por implementar medidas voluntárias de deteção, denúncia e remoção de abusos sexuais de crianças dos seus serviços, incluindo tanto material previamente conhecido como novo material e incluindo as ameaças baseadas em texto. Este quadro poderá igualmente definir as autoridades públicas competentes, ao nível da União ou a nível nacional, às quais as comunicações devem ser enviadas.

- Um quadro jurídico que, para além de estabelecer uma base jurídica clara como na Opção 1, criasse também uma obrigação, vinculativa para os PS relevantes, de detetarem, denunciarem e removerem dos seus serviços materiais conhecidos de abuso sexual de crianças. Ao abrigo desta Opção, os PS adequados poderiam também op-

104 Avaliação de Impacto Inicial. Regulamento do Parlamento Europeu e do Conselho relativo à deteção, remoção e denúncia de abuso sexual de crianças em linha, criando o centro da UE para prevenir e combater o abuso sexual de crianças, (disponível em: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726- Fighting-child-sexual-abuse-detection-removal-and-reporting-of-illegal-content-online_en).

tar por implementar medidas para detetar, comunicar e remover novos materiais e/ou ameaças baseadas em texto, mas tal não seria obrigatório.

• Um quadro jurídico que crie uma obrigação, vinculativa para os PS relevantes para detetar, denunciar e remover o abuso sexual de crianças dos seus serviços, abrangendo material conhecido, material novo e ameaças em texto, tais como o aliciamento. Tal como na Opção 1, este quadro definiria igualmente as autoridades públicas competentes, a nível da União ou a nível nacional, às quais as comunicações devem ser enviadas[105].

Do convite público para a apresentação de comentários resultaram 41 opiniões[106] emitidas por representantes de várias esferas, incluindo o setor privado e as ONG. Embora o quadro legal existente na UE e as principais opiniões expressas não fossem homogéneas nem unívocas, indicaram que a abordagem na prevenção e no combate à CSEA, não responde adequadamente aos desafios existentes, pelo que é urgente dispor de um novo enquadramento jurídico, que seja coerente e consistente ao nível da UE.

3.2.4. Implicações para o presente relatório

Com a liberalização do setor de comunicações nos últimos 40 anos, combinada com rápidos desenvolvimentos tecnológicos, como a computação em nuvem, associada à complexidade das atividades de negócio, emergiram dificuldades de compreensão quanto à governança e conduta dos PS. Na verdade, o mercado das comunicações está simultaneamente interligado e fortemente estratificado, com extensas cadeias de fornecimento a nível físico, lógico e operacional.

A complexidade da cadeia de fornecimento de serviços pode ter implicações em termos de transparência, legalidade e responsabilidade. Embora haja disposições legais ou regulamentares que identificam um PS como legalmente responsável, o cumprimento de qualquer dever ou obrigação pode ser transferido para outro PS mediante a celebração de um contrato. O resultado da divisão de responsabilidades através de uma combinação de mecanismos de direito público e privado pode servir para tornar opacas as questões de atribuição efetiva de responsabilidade pelo funcionamento dos sistemas de deteção automática. O ponto-chave reside em perceber que a noção de entidade singular, quando está em causa a conduta de

105 Ibid.

106 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Fighting-child-sexual-abuse-detection-removal-and-reporting-of-illegal-content-online/feedback_en?p_id=16375286

um "prestador de serviços", não representa com rigor, frequentemente a complexidade da cadeia de fornecimento da qual o "serviço", em concreto, realmente depende.

Outra consequência é a de que os PS podem aceder aos mercados numa base transfronteiriça operando a partir de um único território. A implicação jurisdicional de tal flexibilidade é a possibilidade de sujeitar o fornecedor de serviços a reclamações jurisdicionais concorrentes, tanto a partir do território em que se encontram sedeados, como nos territórios em que "oferecem serviços".[107] Essa concorrência jurisdicional tem um "custo" para os PS, tanto em termos de conformidade, ou seja, ter de cumprir múltiplos e diferentes regimes legais e regulamentares, nomeadamente em caso de necessidade de resolução de conflitos de normas, nos casos em que a conformidade numa jurisdição resulta numa potencial violação da lei noutra jurisdição. Enquanto o primeiro caso parece ser um "custo" normal de concretização de negócios, o segundo pode ter implicações mais profundas em termos de exposição do PS à responsabilidade, tanto empresarial como individual, bem como dificuldades em assegurar que uma conduta que interfira com os direitos individuais ocorra "de acordo com a lei".[108]

3.3. Obrigações positivas ao abrigo do Direito Internacional e Europeu dos Direitos Humanos relativamente à proteção das crianças contra a exploração sexual e o abuso sexual em linha

O direito internacional e europeu relativo aos direitos humanos concebe os direitos humanos tanto num sentido negativo como positivo. Existe neste momento um consenso internacional sobreposto de que "os direitos vão além dos direitos individuais subjetivos que impõem limitações ao Estado ou a outro portador de deveres, e que os direitos incorporam a noção de que os Estados ou outros atores têm deveres de respeitar e proteger os direitos e não apenas o dever de os não violar".[109] Este ponto de partida conceptual é central para a ideia de que os Estados têm deveres de proteção em relação a pessoas que se encontram em risco de serem prejudicadas pela atividade de atores privados.[110] Pelo que, os tribunais nacionais internacionais e regionais de direitos humanos têm, pois, mantido e desenvolvido deveres de proteção no campo da justiça criminal, incluindo a proteção contra a OCSEA. Em-

107 Proposta da Comissão Europeia de Regulamento do Parlamento Europeu e do Conselho relativo às decisões europeias de produção e conservação de provas eletrónicas em matéria penal, COM(2018) 225 final (17.4.2018), n.º 1 do artigo 1.º (disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN).

108 i.e. ECHR, n.º 2 do artigo 8.º.

109 L Lazarus et al, 'The Evolution of Fundamental Rights Charters and Case Law', Direcção-Geral de Políticas Internas do Parlamento Europeu, Direitos do Cidadão e Assuntos Constitucionais, 2011, 34.

110 Ver L Lazarus, 'The Right to Security' in (ed), Max Planck Encyclopedia of Comparative Constitutional Law (Oxford University Press 2017).

bora o potencial da "intervenção coerciva" desta tendência exija um escrutínio contínuo,[111] está agora bem estabelecido que os Estados têm deveres de proteção para com vítimas, em relação a danos reais ou potenciais, à luz de normas de direito internacional e europeu dos direitos humanos.

3.3.1. Direitos das crianças e obrigações positivas no âmbito do direito dos tratados de direitos humanos internacionais e europeus

Nações Unidas

O ponto de partida no sistema das Nações Unidas relativamente à proteção contra a OCSEA é a Convenção das Nações Unidas sobre os Direitos da Criança (UNCRC). No artigo 3.º da UNCRC determina-se que "Todas as decisões relativas a crianças, adotadas por instituições públicas ou privadas de proteção social, por tribunais, autoridades administrativas ou órgãos legislativos, terão primacialmente em conta o interesse superior da criança". Além disso, o artigo 3.º afirma que "Os Estados Partes se comprometem a garantir à criança a proteção e os cuidados necessários ao seu bem-estar" e a tomar "todas as medidas legislativas e administrativas adequadas" para o efeito. O n.º 1 do artigo 19.º da UNCRC exige que os "Estados Partes tomem todas as medidas legislativas, administrativas, sociais e educativas adequadas à proteção da criança contra todas as formas de violência física ou mental, dano ou sevícia, abandono ou tratamento negligente, maus-tratos ou exploração, incluindo a violência sexual." O n.º 2 do artigo 19.º exige que os Estados implementem "outras formas de prevenção, e para identificação, elaboração de relatório, transmissão, investigação, tratamento e acompanhamento dos casos de maus-tratos infligidos à criança, acima descritos, compreendendo igualmente, se necessário, processos de intervenção judicial". O artigo 34.º da UNCRC exige que os Estados Partes "protejam a criança de todas as formas de exploração e de violência sexuais". Exige ainda que os Estados Partes tomem todas as medidas adequadas, nos planos nacional, bilateral e multilateral para impedir (a) que a criança seja incitada ou coagida a dedicar-se a uma atividade sexual ilícita; (b) que a criança seja explorada para fins de prostituição ou de outras práticas sexuais ilícitas; (c) que a criança seja explorada na produção de espetáculos ou de material de natureza pornográfica". Finalmente, o Artigo 36.º da UNCRC declara que "Os Estados Partes protegem a criança contra todas as formas de exploração prejudiciais a qualquer aspeto do seu bem-estar".

A UNCRC é complementada pelo Protocolo Facultativo à UNCRC relativo à Venda de Crianças, Prostituição Infantil e Pornografia Infantil (OPSC).[112] Um instrumento que chama a aten-

111 L Lavrysen and N Mavronicola (eds), 'CoErcive Human Rights', Hart 2020.

112 Assembleia Geral das Nações Unidas, Volume 2171, A-27531 adotado a 25 de maio de 2000 (em julho de 2019 176 os Estados tinham ratificado ou aderido ao Protocolo Facultativo) http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx

ção em especial para as obrigações do Estado de criminalizar, prevenir, investigar, processar, punir e cooperar internacionalmente, a fim de impedir a venda de crianças, a prostituição infantil e a pornografia infantil, tanto dentro como fora das fronteiras dos Estados.[113]

A violência sexual, a exploração e o abuso de crianças são também abordados em instrumentos complementares da ONU, tais como o "Protocolo Adicional Relativo à Prevenção, à Repressão e à Punição do Tráfico de Pessoas, em especial de Mulheres e Crianças", que complementa a Convenção das Nações Unidas contra o Crime Organizado Transnacional[114], bem como em materiais de direito internacional não vinculativos, incluindo: A Agenda das Nações Unidas para o Desenvolvimento Sustentável[115], (Objetivos 5, 8 e 16), a Declaração do Rio de Janeiro e o Apelo à Ação para Prevenir e Parar a Exploração Sexual de Crianças e Adolescentes,[116] a recente publicação "Orientações Terminológicas do Grupo de Trabalho Interagências sobre Exploração Sexual de Crianças",[117] e a Resolução da Comissão das Nações Unidas sobre Prevenção do Crime e Justiça Criminal "Combater a exploração sexual e o abuso sexual de crianças em linha".[118] Além disso, foram emitidas orientações através dos relatórios do Relator Especial da ONU sobre a venda e exploração sexual de crianças, incluindo a prostituição infantil, a pornografia infantil e outros materiais sobre abuso sexual de crianças.[119]

113 Na sua octogésima primeira sessão (13-31 de maio de 2019), o Comité dos Direitos da Criança das Nações Unidas (UNCRC) adotou Diretrizes relativas à implementação do OPSC. O Relatório Explicativo das Diretrizes do OPSC inclui referências a normas internacionais e regionais ligadas às questões abrangidas pelo OPSC, os Comentários Gerais relevantes da UNCRC e recomendações de outros organismos semelhantes, tais como o Comité das Partes da Convenção do Conselho da Europa para a Proteção das Crianças contra a Exploração Sexual e os Abusos Sexuais, também conhecido como "Comité Lanzarote".

114 https://www.ohchr.org/en/professionalinterest/pages/protocoltraffickinginpersons.aspx

115 https://www.un.org/sustainabledevelopment/sustainable-development-goals/

116 https://www.ecpat.org/wp-content/uploads/2016/04/WCIII_Outcome_Document_Final.pdf

117 Diretrizes Terminológicas para a Proteção das Crianças da Exploração Sexual e do Abuso Sexual, adotadas pelo Grupo de Trabalho Interagências no Luxemburgo, 28 de Janeiro de 2016 (disponível em: http://luxembourgguidelines.org/).

118 https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_28/ECN152019_L3REv1_e_V1903716.pdf

119 Ver o último relatório do Relator Especial da ONU sobre a venda de crianças, prostituição infantil e pornografia infantil, "Sale and sexual exploitation of children", A/HRC/43/40, 21 de janeiro de 2020. Ver também: UN Special Rapporteur on the sale of children, child prostitution and child pornography, '25 years of Fighting the Sale and sexual Exploitation of Children: Addressing New Challenges' 2016, (disponível em: https://www.ohchr.org/Documents/Issues/Children/SR/25YearsMandate.pdf).

Convenção de Lanzarote

Segundo o sistema do CoE, a Convenção de Lanzarote (CL) exige a criminalização de todos os tipos de ofensas sexuais contra crianças. Também "proporciona um quadro abrangente e coerente que abrange a prevenção, coordenação de diferentes atores, proteção e assistência às vítimas, criminalização abrangente de várias formas de abuso e exploração, [e] regras e instrumentos para facilitar a investigação, a ação penal e o direito processual".

De relevância específica para a área em questão são em particular os artigos 18.º ("abusos sexuais"), 20.º ("pornografia infantil"), 21.º ("espetáculos de pornografia infantil"), 22.º ("corrupção de menores") e 23.º ("abordagem de crianças para fins sexuais") da CL. Todas estas disposições exigem que os Estados Partes "tomem as medidas legislativas ou outras necessárias para assegurar que a conduta proscrita seja criminalizada". O parecer interpretativo, referido na introdução ao presente documento, esclareceu que "os delitos existentes na Convenção de Lanzarote continuam a ser criminalizados pela legislação nacional da mesma forma, quaisquer que sejam os meios utilizados pelos infratores sexuais para os cometer, seja através da utilização das TIC ou não, mesmo quando o texto da Convenção de Lanzarote não menciona especificamente as TIC.[120]

Além disso, o parecer interpretativo apela aos Estados Partes para "assegurarem respostas adequadas à evolução tecnológica e utilizarem todos os instrumentos, medidas e estratégias relevantes para prevenir e combater eficazmente os crimes sexuais contra crianças facilitados pela utilização das TIC"; atribuírem recursos às autoridades responsáveis pela investigação e pela ação penal "a fim de assegurar uma investigação e uma ação penal eficazes dos crimes sexuais contra crianças facilitados pela utilização das TIC";[121] e "encorajar o sector privado que trabalha no domínio das TIC a contribuir para a prevenção e combate à exploração e abusos sexuais de crianças facilitados pela utilização das TIC".[122]

De relevância específica para a área discutida é o artigo 10.º da CL que, nos termos da sua alínea b) exige "sistemas de recolha de dados e de pontos focais, a nível nacional ou local e em cooperação com a sociedade civil, permitindo, no respeito pelas exigências relacionadas com a proteção de dados de caráter pessoal, a observação e a avaliação dos fenómenos de exploração sexual e abusos sexuais de crianças". O Parecer Interpretativo encoraja, consequentemente, "a cooperação entre as autoridades estatais competentes, a sociedade civil

120 Parecer Interpretativo, par. 12.

121 Ibid, par. 14.

122 Ibid, par. 17.

e o setor privado, a fim de melhor prevenir e combater a exploração e o abuso sexual de crianças que é facilitado através da utilização das TIC".

Outras consequências para esta análise são os requisitos da CL relacionados com "Investigações, procedimentos penais e direito processual". O n.º 5 do artigo 30.º exige que os Estados Partes "tomem as medidas legislativas ou outras necessárias para garantir o exercício eficaz da ação penal relativamente a infrações penais estabelecidas em conformidade com a presente Convenção, prevendo, se apropriado, a possibilidade de operações encobertas" e "permitir que as unidades ou serviços de investigação identifiquem vítimas de infrações penais estabelecidas em conformidade com o artigo 20.º, em particular através da análise de material relacionado com pornografia infantil tal como fotografias e registos audiovisuais transmitidos ou disponibilizados através de tecnologias de informação ou comunicação".

Finalmente, de importância para o presente relatório é o disposto no artigo 38.º da CL que estabelece os princípios gerais e as medidas para a cooperação internacional. De facto, o n.º 3 do artigo 38.º estabelece uma base jurídica para o auxílio mútuo em matéria penal ou extradição. O Parecer Interpretativo apela ainda aos Estados a "cooperarem no sentido de enfrentarem o caráter transnacional frequentemente presente nos delitos sexuais contra crianças facilitados através da utilização das TIC".[123]

Outros instrumentos do CoE complementam a CL na abordagem de certos aspetos de proteção, incluindo o artigo 7.º da Carta Social Europeia (proteção especial das crianças e dos jovens contra o perigo físico e moral),[124] a Carta Social revista, artigo 17.º (direito das crianças a proteção social, jurídica e económica adequada) e artigo 17.º, n.º 1, alínea b) (exigência de medidas adequadas e necessárias para proteger as crianças e jovens contra negligência, violência ou exploração), as "Diretrizes do CoE sobre Justiça Amiga das Crianças" adotadas pelo Comité de Ministros do CoE em Novembro de 2010;[125] e a Convenção de Istambul.[126]

Mais recentemente, o Comité de Ministros do Conselho da Europa emitiu a "Recomendação com orientações para respeitar, proteger e cumprir os direitos das crianças no ambiente digital" que sublinha as obrigações dos atores estatais e não estatais (incluindo as empresas) e

123 Ibid, para. 19.

124 Conselho da Europa, Série de Tratados Europeus - No. 35, Turim 18.X.1961. Isto é interpretado pelo Comité Europeu dos Direitos Sociais para proteger contra "todas as formas de exploração sexual comercial de crianças", incluindo "prostituição infantil, pornografia infantil e tráfico de crianças" (Comité Europeu dos Direitos Sociais, Direitos da Criança ao abrigo da Carta Social Europeia, Documento de Informação).

125 Ver também: Convenção do Conselho da Europa sobre "Prevenção e o Combate à Violência contra as Mulheres e a Violência Doméstica" (Convenção de Istambul); a Convenção do Conselho da Europa sobre Ações contra o Tráfico de Seres Humanos, e a Convenção.

126 Convenção do Conselho da Europa para a Prevenção e o Combate à Violência contra as Mulheres e a Violência Doméstica (Convenção de Istambul), disponível em: https://www.CoE.int/en/web/conventions/full-list/-/conventions/treaty/210).

afirma o direito das crianças "a serem protegidas de todas as formas de violência, exploração e abuso no ambiente digital".[127] As orientações reconhecem nomeadamente que "quaisquer medidas de proteção devem ter em consideração o superior interesse e a evolução das capacidades da criança e não restringir indevidamente o exercício de outros direitos".[128]

Convenção de Budapeste

De particular significado para este relatório é a Convenção do CoE sobre o Cibercrime (Convenção de Budapeste - CB).[129] O artigo 9.º, alíneas b) e c), exige que as Partes criminalizem "infrações relacionadas com a pornografia infantil", desde a produção e oferta até à distribuição, aquisição e posse de tais materiais. Muito importante, é o facto de a CB prever prerrogativas processuais para investigar e obter provas não só relacionadas com o cibercrime, mas também qualquer infração que envolva provas num sistema informático. O mesmo âmbito aplica-se às disposições da Colômbia Britânica sobre cooperação internacional.

As Partes na CB - através do Comité da Convenção sobre o Cibercrime (T-CY) - estão atualmente a negociar um 2.º Protocolo Adicional à CB sobre cooperação reforçada e divulgação de provas eletrónicas. O projeto completo deste Protocolo[130] foi aprovado pela T-CY a 28 de maio de 2021. Este Protocolo prevê novos tipos de medidas que anteriormente não estavam disponíveis em acordos internacionais de direito penal, incluindo: cooperação direta com PS sedeados em outros Estados Partes para obter a divulgação de informações dos subscritores (artigo 7.º), com entidades que prestam serviços de registo de nomes de domínio para obter a divulgação de informações das pessoas registadas (artigo 6.º); divulgação rápida de dados informáticos armazenados em caso de emergência (artigo 9.º), e assistência mútua em caso de emergência (artigo 10.º); e salvaguardas de proteção de dados em relação aos dados transferidos ao abrigo do protocolo (artigo 14.º).

O 2.º Protocolo Adicional será muito relevante por vários motivos. Em primeiro lugar, a CB abrange 66 Estados Partes, incluindo os EUA, onde muitos dos PS estão sediados. Em segundo lugar, os poderes processuais e as disposições de cooperação internacional desta Convenção permitem investigar infrações e obter provas eletrónicas não só para infrações relacionadas com pornografia infantil ao abrigo do artigo 9.º, alíneas b) e c), mas também para outras infrações abrangidas pela Convenção de Lanzarote.

127 CM/Rec(2018)7.

128 Ibid, par. 50, p. 7. Mais informação disponível no Anexo.

129 https://www.CoE.int/en/web/cybercrime/the-budapest-convention

130 https://rm.CoE.int/0900001680a2aa1c

Em terceiro lugar, prevê-se a possibilidade de cooperação direta com os PS para obter informações dos subscritores ao abrigo do artigo 18.º, alíneas b) e c) e dos artigos 6.º e 7.º do futuro Protocolo que permitem identificar os utilizadores de um determinado endereço IP, conta de correio eletrónico, conta de redes sociais ou pessoa que registou um domínio. Em quarto lugar, as medidas de emergência do novo Protocolo estarão disponíveis para salvar as crianças vítimas. Assim, em suma, as medidas das alíneas b) e c) e do seu novo Protocolo também permitirão o acompanhamento de relatórios sobre o CSAM recebidos de PS.

As negociações deste 2.º Protocolo Adicional, contudo, sublinharam a necessidade de salvaguardas, em particular num contexto transfronteiriço. Por exemplo, as medidas do Protocolo aplicam-se apenas a investigações e processos penais específicos e não implicam uma vigilância geral das comunicações. Além disso, os Estados Partes terão de estabelecer uma base jurídica ao abrigo do direito interno para a execução das medidas ao abrigo do Protocolo.

O Protocolo permite uma série de reservas e declarações, a fim de satisfazer os requisitos específicos da legislação interna dos Estados Partes. Por exemplo, os Estados Partes podem exigir ser notificados quando outro Estado Parte envia um pedido diretamente a um PS estabelecido no seu território. Outras salvaguardas incluem: limitações de utilização, requisitos de confidencialidade ou motivos de recusa que podem ser aplicáveis; foi incluída uma disposição detalhada sobre a proteção de dados pessoais (artigo 14.º) para assegurar que a transferência transfronteiriça de dados pessoais beneficia de um padrão de proteção considerado adequado por todos os Estados Partes, incluindo os Estados Membros da União Europeia. Finalmente, os PS e as entidades que prestam serviços de registo de domínio reagirão a ordens ou pedidos ao abrigo do 2.º Protocolo adicional, que também enumera o que tais ordens ou pedidos, podem especificar e quando e em que termos devem ser fornecidas informações suplementares.

União Europeia

Na União Europeia, o ponto de partida em relação à proteção da OCSEA, é o artigo 24.º da Carta dos Direitos Fundamentais da União Europeia (Carta da UE). O n.º 1 do artigo 24.º da Carta da UE estabelece que "as crianças têm direito à proteção e aos cuidados necessários para o seu bem-estar". Além disso, o n.º 2 do artigo 24.º da Carta da UE declara que "Todos os atos relativos às crianças, quer praticados por entidades públicas, quer por instituições privadas, terão primacialmente em conta o interesse superior da criança". Os "direitos da criança" são também explicitamente promovidos ao abrigo do n.º 3 do artigo 3.º do Tratado da União Europeia. Além disso, ao abrigo do n.º 1 do artigo 83.º do Tratado sobre o Funciona-

mento da União Europeia, "a exploração sexual de mulheres e crianças" é enumerada como uma forma de criminalidade "particularmente grave com dimensão transfronteiriça que resulte da natureza ou das incidências dessas infrações, ou ainda da necessidade especial de as combater, assente em bases comuns".

Diretiva sobre a Exploração e Abuso Sexual de Crianças (Diretiva CSEA)

Atualmente, o principal instrumento legislativo da UE sobre a OCSEA é a Diretiva CSEA, que foi adotada pelo PE e pelo Conselho a 13 de dezembro de 2011.[131] O objetivo declarado da Diretiva CSEA é a proteção dos "direitos da criança" assegurando que o "interesse superior da criança" constitui a "preocupação primordial" das "entidades públicas e instituições privadas".[132] O seu objeto é o de "estabelecer regras mínimas relativas à definição dos crimes e sanções no domínio do abuso sexual e da exploração sexual de crianças, da pornografia infantil e do aliciamento de crianças para fins sexuais", bem como introduzir "disposições para reforçar a prevenção desses crimes e a proteção das suas vítimas".[133] A Diretiva CSEA foi o "primeiro instrumento jurídico abrangente da EU" que inclui a "prevenção, investigação e repressão de crimes, bem como a assistência e proteção das vítimas".[134] A Diretiva baseia-se no reconhecimento de que o abuso e exploração sexual de crianças, dentro e fora de linha, constituem "violações graves dos direitos das crianças à proteção e cuidados necessários ao

131 A Diretiva CSEA foi em parte motivada pelo Programa de Estocolmo para combater as "ameaças transnacionais" à segurança interna da UE e para promover o projeto de reconhecimento mútuo em conformidade com o n.º 1 do artigo 83.º do TFUE (O Programa de Estocolmo - Uma Europa aberta e segura ao serviço e proteção dos cidadãos, 2010 /C 115/01, 4.5.2010). A Diretiva CSEA também coincidiu com a realização da Agenda da UE para os Direitos da Criança (An EU Agenda for the Rights of the Child, Brussels, 15.2.2011 COM(2011) 60 final). A Agenda reafirmou o compromisso da UE de eliminar todas as formas de violência contra crianças, incluindo a violência sexual" (p.7). Durante o mesmo período de tempo, foram estabelecidos objetivos complementares no âmbito do Programa da UE para uma Internet mais segura, que incluíam o objetivo de: reduzir a quantidade de conteúdos ilegais que circulam em linha e lidar adequadamente com comportamentos prejudiciais em linha, principalmente a distribuição em linha de material pedo-pornográfico" (Proposta de Decisão do Parlamento Europeu e do Conselho que estabelece um programa comunitário plurianual para a proteção das crianças que utilizam a Internet e outras tecnologias da comunicação, 27.2.2008, COM(2008)106 final). Em conjunto, estas iniciativas na UE levaram a uma reforma decisiva da Decisão-Quadro 2004/68/JAI existente e à adoção da Diretiva CSEA (ver considerandos 6 e 48 da Diretiva CSEA).

132 Diretiva CSEA, Considerandos 1, 2 e 6.

133 Diretiva CSEA, artigo 1.º.

134 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'EU strategy for a more effective fight against child sexual abuse' (Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, "Estratégia da UE para uma luta mais eficaz contra o abuso sexual de crianças") de 24.7.2020 COM(2020) 607 final (Estratégia CSA).

seu bem-estar".[135] A Diretiva é explícita na busca "primacial " do "interesse superior da criança", de acordo com o n.º 2 do artigo 24.º da Carta da UE e do artigo 3.º da Convenção sobre os Direitos da Criança.[136]

Uma disposição importante e altamente relevante para este relatório é o artigo 25.º da Diretiva CSEA, o qual impõe duas obrigações principais aos Estados Membros. O n.º 1 do artigo 25.º exige que os Estados-Membros "assegurem a supressão imediata das páginas eletrónicas que contenham ou difundam pornografia infantil", no seu território e "procurem obter a supressão dessas mesmas páginas sediadas fora do seu território". O n.º 2 do artigo 25.º constituiu uma cláusula facultativa e permissiva que permite aos Estados-Membros "bloquear o acesso a páginas eletrónicas". Exige que as medidas sejam "adotadas através de processos transparentes e devem incluir garantias adequadas, nomeadamente para assegurar que a restrição se limite ao que é necessário e proporcional , e que os utilizadores sejam informados do motivo das restrições". Além disso, preceitua que estas "garantias devem incluir também a possibilidade de recurso judicial". O considerando 47 da Diretiva CSEA observa também, além disso, que o cumprimento do artigo 25.º da Diretiva CSEA não envolve necessariamente medidas legislativas: "... As medidas tomadas pelos Estados-Membros em conformidade com a presente diretiva para eliminar ou, se for caso disso, bloquear sítios da Internet que contêm pornografia infantil podem consistir em vários tipos de ação pública, nomeadamente de cariz legislativo, não legislativo, judicial ou outro. Nesse contexto, a presente diretiva não prejudica as medidas voluntárias tomadas pelo setor da Internet para evitar o uso indevido dos seus serviços, nem qualquer tipo de apoio dos Estados-Membros a tais medidas."

Em 2016, a Comissão Europeia e o Conselho publicaram um relatório de avaliação sobre a implementação do artigo 25.º da Diretiva CSEA (o relatório do artigo 25.º).[137] O relatório assinalou a necessidade crucial de "cooperação entre o setor privado, incluindo a indústria e a sociedade civil, e as autoridades públicas, incluindo as autoridades policiais e judiciais", a fim de cumprir os objetivos do artigo 25.º.[138] Além disso, assinalou que "as medidas não legislativas precisavam de ser avaliadas em relação aos resultados do artigo 25.º na prática".[139]. Após o levantamento das medidas em vigor, o Relatório sobre o artigo 25.º concluiu que os Estados-Membros deveriam a assegurar um nível satisfatório de transposição e aplicação.

135 Diretiva CSEA, considerando 1.

136 Resolução 44/25 da Assembleia Geral das Nações Unidas de 20 de novembro de 1989.

137 Relatório da Comissão ao Parlamento Europeu e ao Conselho avaliando a aplicação das medidas referidas no artigo 25.º da Diretiva 2011/93/UE, de 13 de Dezembro de 2011, relativa à luta contra o abuso e a exploração sexual de crianças e a pornografia infantil, COM(2016) 872 final, Bruxelas 16.12.2016 (doravante Relatório do artigo 25.º).

138 Relatório do artigo 25.º, p. 4.

139 Ibid.

Os "principais desafios" identificados relacionavam-se tanto com a remoção de material de abuso sexual de crianças como com as garantias necessárias nos casos em que o acesso dos utilizadores da Internet fosse bloqueado. O relatório apelava, por conseguinte, a uma maior colaboração de múltiplos intervenientes a nível da UE.[140]

A Resolução CSEA do PE expressou subsequentemente o seu pesar pelo facto de "apenas metade dos Estados-Membros ter incorporado na sua legislação disposições que permitem bloquear o acesso" e exortou ainda a uma maior utilização de medidas de supressão "mais eficazes".[141] Além disso, apelou aos Estados-Membros e às instituições da UE para intensificarem a cooperação com a indústria da Internet, Europol/Centro Europeu de Cibercriminalidade, Eurojust, Interpol, Estados de países terceiros, bem como várias iniciativas, tais como INHOPE e Connecting Europe Facility, na realização dos objetivos do artigo 25.º.[142]

Estes apelos foram seguidos na mais recente Estratégia da UE para uma luta mais eficaz contra o abuso sexual de crianças,[143] e foram reiterados na iniciativa da CE, *Delivering for children: an EU Strategy on the Rights of the Child.*[144] Ambos os documentos sugerem que a Diretiva CSEA exigirá uma modificação ou substituição para continuar a ser adequada ao objetivo da luta contra a OCSEA, em especial porque "os autores dos crimes utilizam de forma cada vez mais sofisticada tecnologias e capacidades técnicas que incluem a cifragem e o anonimato".[145]

3.3.2. Jurisprudência sobre a proteção das crianças relativamente à exploração sexual e ao abuso sexual em linha

Esta secção centrar-se-á especificamente na evolução do tratamento jurisprudencial das obrigações positivas dos Estados em matéria de proteção das crianças contra a exploração e o abuso sexual em linha.

140 Ibid.

141 Resolução do Parlamento Europeu, de 14 de dezembro de 2017, sobre a aplicação da Diretiva 2011/93/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso e a exploração sexual de crianças e a pornografia infantil (2015/2129(INI)) (doravante Resolução EP CSA), parágrafos 40 e 44.

142 Resolução CSA do Parlamento Europeu, parágrafos 45, 46, 47, 48, 49.

143 Estratégia da UE para uma luta mais eficaz contra o abuso sexual de crianças, Bruxelas, 24.7.2020 COM(2020) 607 final, (disponível em: https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda- security/20200724_com-2020-607-commission-communication_en.pdf).

144 EC, Delivering for children: an EU strategy on the rights of the child, Ref. Ares(2020)3149750 - 17/06/2020, (disponível em: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12454-EU-strategy-on- the-rights-of-the-child-2021-24-_en).

145 Estratégia CSEA, p. 6, ênfase no original.

Tribunal Europeu dos Direitos do Homem (TEDH)

O TEDH tem afirmado e desenvolvido obrigações positivas em relação ao abuso sexual de crianças desde meados da década de 1980.[146] Inicialmente, estas obrigações foram enquadradas no artigo 8.º[147] da CEDH. Em MC v Bulgária,[148] contudo, a violação, o abuso sexual e a exploração sexual foram considerados como violações da proibição absoluta de tratamento desumano e degradante nos termos do artigo 3.º da CEDH. A jurisprudência subsequente relativa à exploração e abuso sexual de crianças tem, desde então, considerado os casos graves de abuso como uma violação do artigo 3.º da CEDH, embora crimes menos graves possam também ser considerados pelo TEDH como uma violação do artigo 8.º.

Como a sensibilidade relativamente à gravidade do abuso sexual de crianças se alterou com o decurso do tempo, o entendimento do Tribunal relativo à margem de apreciação do Estado no que diz respeito à realização de obrigações positivas reduziu-se. Isto já era evidente no caso KU contra a Finlândia, que descreveu a OCSEA como "um tipo abominável de delito, com efeitos debilitantes para as suas vítimas".[149] Cada vez mais, o TEDH tem referido a CL e a UNCRC, em particular "a proteção do interesse superior da criança", para esclarecer o conteúdo das obrigações de proteção e investigação eficaz do abuso sexual de crianças.[150]

Nos últimos três anos, a Grande Câmara (GC) do TEDH abordou as obrigações positivas dos Estados em relação ao abuso sexual de crianças nas duas principais decisões de A e B contra a Croácia (2019) e de X e outros contra a Bulgária (2021).[151] Estes casos representam o culminar de mais de 25 anos de jurisprudência do TEDH nesta área, e fornecem uma orientação autorizada sobre a forma das obrigações dos Estados Membros neste domínio.

146 X e Y v Países Baixos, An. n.º 8978/80, 26 de março de 1985; Stubbings v Reino Unido, An. n.º 22083/93, 22 de outubro de 1996; MC v Bulgária, An. n.º 39272/98, 4 de dezembro de 2003; K.U. v Finlândia, An. n.º 2872/02, 02 de março de 2009; O'Keeffe v. Irlanda [GC], n.º 35810/09, ECHR 2014; Y. v. Eslovénia, n.º 41107/10, § 101, ECHR 2015; M.G.C v Roménia, n.º 61495/11, 15 de março de 2016; Trabajo Rueda v Espanha, An. n.º 32600/12, 30 de maio de 2017; A e B v Croácia, GC, An. n.º 7144/15, final 4/11/2019; X e outros v Bulgária, GC, An. n.º 22457/16, 2 de fevereiro de 2021.

147 X e Y v Países Baixos, An. n.º 8978/80, 26 de março de 1985, ver par. 23; Stubbings v United Kingdom, An. n.º 22083/93, 22 de outubro de 1996, parágrafos 62 - 64.

148 MC v Bulgaria, An. n.º 39272/98, 4 de dezembro de 2003.

149 K.U. v Finland, An. n.º 2872/02, 02 de março de 2009, par. 46.

150 Söderman v Sweden, An. n.º 5786/08, 12 de novembro de 2013, par. 80 - 82.

151 A e B v Croácia, GC, An n.º 7144/15, final 4/11/2019; X e outros v Bulgária, GC, An. n.º 22457/16, 2 de fevereiro de 2021.

Em A e B v Croácia,[152] o TEDH foi chamado a examinar o tratamento de uma alegada agressão sexual de uma vítima de quatro anos e meio de idade pelo seu pai. Em primeiro lugar, o Tribunal procedeu ao exame da adequação do quadro jurídico que rege a conduta das autoridades na investigação e tratamento de casos de abuso sexual de crianças. Em segundo lugar, analisou "se as autoridades competentes tinham realizado uma investigação exaustiva, eficaz e rápida". Em terceiro lugar, examinou "se as autoridades tinham proporcionado proteção suficiente ao direito do requerente pelo respeito pela vida privada, e especialmente pela sua integridade pessoal, à luz da sua vulnerabilidade devido à sua tenra idade e alegado abuso sexual e tendo como principal consideração o interesse superior da criança". Assim, a questão era "não só a eficácia da investigação, mas a alegada falta ou insuficiência de medidas destinadas a proteger em processos penais os direitos de uma criança, alegadamente vítima de abuso sexual".[153]

O TEDH observou que o artigo 3.º (juntamente com o artigo 8.º) da CEDH, "implica uma obrigação para o Estado de salvaguardar a integridade física e psicológica de uma pessoa" e que "as crianças e outros indivíduos vulneráveis, em particular, têm direito a uma proteção efetiva".[154] O tribunal observou que, nos termos do artigo 3.º, "as autoridades têm uma obrigação positiva" que inclui "o dever de manter e aplicar na prática um quadro jurídico adequado que proporcione proteção contra atos de violência por particulares"[155], bem como "requisitos relacionados com a eficácia da investigação".[156] Consequentemente, os Estados-Membros devem "assegurar que as disposições de direito penal para a punição efetiva do abuso sexual de crianças estejam em vigor e que sejam aplicadas na prática através de uma investigação e ação penal eficazes".[157]Quanto à margem de apreciação do Estado no cumprimento destas obrigações, a GC observou que "quando está em jogo uma faceta particularmente importante da existência ou identidade de um indivíduo, ou quando as atividades em questão envolvem um aspeto mais íntimo da vida privada, a margem permitida ao Estado é correspondentemente reduzida".[158]

152 MC v Bulgária, An. n.º 39272/98, 4 de dezembro de 2003. Ver também: O'Keeffe v. Irlanda [GC], n.º 35810/09, ECHR 2014; Y. v. Eslovénia, n.º 41107/10, § 101, ECHR 2015; M.G.C v Roménia, n.º 61495/11, 15 de março de 2016.

153 A e B v Croácia, par. 105.

154 Par. 106, citando O'Keeffe v. Irlanda para 144; X e Y v. Países Baixos, par. 23-24 e 27, e M.C. v. Bulgária, par. 150

155 Par. 107, citando Söderman v. Sweden [GC], n.º 5786/08, par. 80, ECHR 2013 com outras referências.

156 Par. 108.

157 Par. 110, citando MC v. Bulgária par. 153.

158 A e B v. Croácia, par. 113.

A GC concluiu a avaliação geral com os seguintes parágrafos importantes que delimitam a atual posição do TEDH sobre o peso atribuído às obrigações positivas no que diz respeito ao abuso sexual de crianças, recorrendo também à LC:[159]

"O Tribunal reitera que nos casos de abuso sexual as crianças são particularmente vulneráveis. O Tribunal também recorda que o direito à dignidade humana e integridade psicológica requer uma atenção especial quando uma criança é vítima de violência. O Tribunal recorda que as obrigações incorridas pelo Estado ao abrigo dos artigos 3.º e 8.º da Convenção em casos como este, envolvendo e afetando uma criança, alegadamente vítima de abuso sexual, exigem a implementação efetiva do direito das crianças a terem os seus melhores interesses como consideração primária e a terem a vulnerabilidade particular da criança e as necessidades correspondentes adequadamente abordadas pelas autoridades domésticas.

Tendo em conta o acima exposto, o Tribunal considera que os Estados são obrigados, nos termos dos artigos 3.º e 8.º, a promulgar disposições que criminalizem o abuso sexual de crianças e a aplicá-las na prática através de uma investigação e ação penal eficazes tendo assim em conta a vulnerabilidade particular das crianças, a sua dignidade e os seus direitos enquanto crianças e enquanto vítimas. Estas obrigações resultam também de outros instrumentos internacionais, tais como, entre outros, a Convenção do Conselho da Europa para a Proteção das Crianças contra a Exploração Sexual e o Abuso Sexual e a Convenção do Conselho da Europa para a Prevenção e Combate à Violência contra as Mulheres e à Violência Doméstica…".

Em X e outros v. Bulgária,[160] a GC lidou com o insucesso do Estado na proteção e investigação do abuso sexual de crianças num orfanato na Bulgária, previamente à sua adoção em Itália. Os factos do caso exigiam a cooperação internacional entre as autoridades italianas e búlgaras na investigação do alegado abuso. A GC resumiu a jurisprudência do TEDH e expôs os princípios gerais que se aplicavam, fazendo eco dos estabelecidos em A e B v. Croácia. Nesta base, a GC afirmou que[161]:

"resulta do caso do Tribunal... que as obrigações positivas das autoridades nos termos do artigo 3.º da Convenção incluem, em primeiro lugar, a obrigação de criar um quadro legislativo e regulamentar de proteção; em segundo lugar, em determinadas circunstâncias bem definidas, a obrigação de tomar medidas operacionais para proteger indivíduos específicos contra um risco de tratamento contrário a essa disposição; e, em terceiro lugar, a obrigação de realizar uma investigação eficaz perante queixas relativas a alegado tratamento deste tipo. Em termos gerais, os dois primeiros aspetos destas obrigações positivas são classifica-

159 A e B v. Croácia, par. 111 e 112.

160 X e outros v. Bulgária, GC, An. n.º 22457/16, 2 de fevereiro de 2021.

161 Ibid, par. 178.

dos como «substantivos», enquanto o terceiro aspeto corresponde à obrigação «processual» positiva do Estado".

No que diz respeito à exigência de uma investigação criminal eficaz, a GC observou que esta pode "incluir a obrigação de as autoridades de investigação cooperarem com as autoridades de outro Estado, implicando uma obrigação de procurar ou de prestar assistência". Embora observando que a natureza e âmbito desta obrigação de cooperação depende inevitavelmente dos factos, a GC observou que "os Estados em causa devem tomar todas as medidas razoáveis para cooperarem entre si, esgotando de boa-fé as possibilidades que lhes são oferecidas pelos instrumentos internacionais aplicáveis em matéria de assistência jurídica mútua e cooperação em matéria penal". Além disso, observou que o Tribunal "normalmente verifica neste contexto se o Estado requerido utilizou as possibilidades disponíveis ao abrigo destes instrumentos".[162]

Note-se que, de forma muito relevante, o Tribunal acentuou que a obrigação positiva nos termos do artigo 3.º da CEDH de estabelecer um "quadro legislativo e regulamentar eficiente" e praticamente "eficaz" para proteger os indivíduos contra abusos sexuais, foi reforçada pelos "artigos 18.º a 24.º da Convenção de Lanzarote".[163] Além disso, "a este respeito, o Tribunal reitera que a Convenção deve ser aplicada de acordo com os princípios do direito internacional, em particular os relativos à proteção internacional dos direitos humanos" (179).[164] Por fim, a influência interpretativa geral dos princípios fundadores da Convenção de Lanzarote foi reafirmada pela GC na conclusão da sua análise das normas jurídicas aplicáveis.

Por último, resulta claro da jurisprudência do Tribunal que, nos casos em que as crianças possam ter sido vítimas de abuso sexual, o cumprimento das obrigações positivas decorrentes do artigo 3.º exige, no contexto dos procedimentos internos, a aplicação efetiva do direito das crianças a terem os seus melhores interesses como consideração primordial e a terem adequadamente abordadas a vulnerabilidade particular da criança e as necessidades correspondentes (ver A e B v. Croácia, acima citado, § 111, e M.M.B. v. Eslováquia, no. 6318/17, § 61, 26 de novembro de 2019; ver também M.G.C. v. Roménia, acima citado, §§ 70 e 73). Estes requisitos são também estabelecidos noutros instrumentos internacionais relevantes para o presente caso, tais como a Convenção sobre os Direitos da Criança, a Convenção de Lanzarote e os instrumentos adotados no quadro da União Europeia (ver parágrafos 124-27 e 135-37 acima).

Em termos mais gerais, o Tribunal considera que em casos que potencialmente envolvam abuso sexual de crianças, a obrigação processual prevista no artigo 3.º da Convenção de conduzir uma investigação eficaz deve ser interpretada à luz das obrigações decorrentes

162 Ibid, par. 191.
163 Ibid, par. 179.
164 Ibid.

dos outros instrumentos internacionais aplicáveis, e mais especificamente da Convenção de Lanzarote.[165]

Tribunal de Justiça da União Europeia (TJUE)

O TJUE tem tido poucas oportunidades para se pronunciar sobre OCSEA. No entanto, duas decisões relacionadas com os crimes previstos na Diretiva CSEA indicam o peso atribuído aos direitos das crianças vítimas de abuso sexual, exploração e pornografia.

A primeira decisão, P.I. v. Oberbürgermeisterin der Stadt Remscheid,[166] foi tomada pouco depois da adoção da Diretiva CSEA. Tratava-se da questão de saber se cometer o crime de exploração sexual de crianças por uma pessoa do círculo de confiança, tal como definido nos artigos 3.º e 9.º da Diretiva CSEA, constitui um crime suficientemente grave para ser abrangido pelo conceito de "razões imperativas de segurança pública" capazes de justificar uma medida de expulsão ao abrigo do n.º 3 do artigo 28.º da Diretiva 2004/38/CE. No decurso desta decisão, o TJUE sublinhou a gravidade das infrações ao abrigo da Diretiva CSEA como constituindo "uma violação especialmente grave de um interesse fundamental da sociedade, suscetível de representar uma ameaça direta para a tranquilidade e a segurança física da população" apresentando características especialmente graves".[167] Para chegar a esta conclusão, o TJUE citou a inclusão da exploração sexual de crianças nos seguintes termos: "a exploração sexual de crianças faz parte dos domínios de criminalidade particularmente grave, com dimensão transfronteiriça, nos quais está prevista a intervenção do legislador da União" ao abrigo do n.º 1 do artigo 83.º do TFEU.[168] O TJUE também sublinhou o Considerando 1 da Diretiva CSEA ao reconhecer o abuso e exploração sexual de crianças como constituindo uma grave violação dos direitos das crianças à proteção e cuidados necessários ao seu bem-estar, tal como previsto na UNCRC e na Carta dos Direitos Fundamentais da União Europeia.[169] Finalmente, retirou orientações das penas mínimas previstas na própria Diretiva CSEA:[170]

165 Ibid, par. 192.

166 P.I. v. Oberbürgermeisterin der Stadt Remscheid, Caso C-348/09, 22 de maio de 2012.

167 Ibid, par. 28

168 Ibid, par. 25.

169 Ibid, par. 26: "Ao expressar o referido objetivo, o primeiro considerando da Diretiva 2011/93 sublinha que o abuso sexual e a exploração sexual de crianças constituem violações graves dos direitos fundamentais, em especial do direito das crianças à proteção e aos cuidados necessários ao seu bemestar, tal como estabelecido na Convenção das Nações Unidas sobre os Direitos da Criança, de 20 de novembro de 1989, e na Carta dos Direitos Fundamentais da União Europeia.

170 Ibid, par. 27.

"A gravidade deste tipo de infração resulta igualmente do artigo 3.° da Diretiva 2011/93, que dispõe, no seu n.º 4, que praticar atos sexuais com uma criança que não tenha atingido a maioridade sexual é punível com uma pena máxima de prisão não inferior a cinco anos, ao passo que, por força do n.º 5, alínea i), do mesmo artigo, praticar atos sexuais com uma criança, abusando de uma posição de manifesta confiança, de autoridade ou de influência sobre a criança, é punível com uma pena máxima de prisão não inferior a oito anos. Segundo o mesmo n.º 5, alínea iii), esta pena deve ser de pelo menos dez anos, em caso de uso de coação, de força ou de ameaça. Em conformidade com o artigo 9. °, alíneas b) e g), da mesma diretiva, devem ser consideradas agravantes a circunstância de a infração ter sido cometida por um membro da família da criança, uma pessoa que coabita com a criança ou uma pessoa que abusou de posição de manifesta confiança ou de autoridade e a circunstância de a infração ter sido cometida com especial violência ou ter causado danos particularmente graves à criança.

Em suma, o Acórdão P.I. v. Oberbürgermeisterin der Stadt Remscheid reafirma a gravidade dos crimes previstos na Diretiva CSA na ordem da UE, e o reconhecimento dos mesmos como graves violações dos direitos fundamentais das crianças.

A segunda decisão de relevância para a OCSEA é a de La Quadrature du Net e outros v. Premier Ministre e outros, que foi decidida pela GC em 6 de outubro de 2020.[171] Neste caso, a referência à Diretiva CSEA surgiu na análise da matéria relativa à "Conservação preventiva dos endereços IP e dos dados relativos à identidade civil para efeitos da luta contra a criminalidade e da salvaguarda da segurança pública".[172] No que respeita à retenção de dados de endereços IP, o TJUE observou que a gravidade da interferência no que respeita aos artigos 7.º e 8.º da Carta da UE só poderia ser justificada por "ações de combate à criminalidade grave, prevenção de ameaças graves à segurança pública e salvaguarda da segurança nacional". As ações tomadas em conformidade com a Diretiva CSEA foram determinadas pelo TJUE para se enquadrarem diretamente nesta categoria, e foram abrangidas pelo n.º 1 do artigo 15.º da Diretiva sobre privacidade e comunicações eletrónicas, "desde que essa possibilidade esteja sujeita ao estrito cumprimento das condições materiais e processuais que devem reger a utilização desses dados".[173]

O raciocínio do TJUE neste caso dá indicações valiosas quanto ao peso a dar aos imperativos concorrentes de proteção contra a OCSEA e os direitos de proteção de dados:

"**154.** Ora, para efeitos da necessária ponderação dos direitos e dos interesses em causa exigida pela jurisprudência referida no n.º 130 do presente acórdão, há que ter em conta o

171 La Quadrature du Net e outros v. Premier Ministre e outros, Processos apensos C-511/18, C-512/18 e C-520/18, 6 de outubro de 2020.

172 Ibid, par. 152.

173 Ibid, par. 155.

facto de, no caso de uma infração cometida em linha, o endereço IP poder constituir o único meio de investigação que permite a identificação da pessoa no momento da prática dessa infração. A isto acresce o facto de a conservação dos endereços IP pelos prestadores de serviços de comunicações eletrónicas para lá do período de atribuição destes dados não se afigurar, em princípio, necessária para efeitos da faturação dos serviços em causa, pelo que a deteção das infrações cometidas em linha pode, por esse motivo, como referiram vários Governos nas suas observações apresentadas ao Tribunal de Justiça, revelar-se impossível sem recurso a uma medida legislativa nos termos do artigo 15.º, n.º 1, da Diretiva 2002/58. Isto pode ocorrer, como alegaram esses Governos, com infrações particularmente graves em matéria de pornografia infantil, como a aquisição, a difusão, a transmissão ou a colocação à disposição em linha de pornografia infantil, na aceção do artigo 2.º, alínea c), da 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 2011, L 335, p. 1).

155. Nestas condições, embora seja verdade que uma medida legislativa que prevê a conservação dos endereços IP de todas as pessoas singulares proprietárias de um equipamento terminal a partir do qual pode ser efetuado um acesso à Internet visa pessoas que, à primeira vista, não têm uma relação, na aceção da jurisprudência referida no n.º 133 do presente acórdão, com os objetivos prosseguidos e que os internautas são titulares, conforme referido no n.º 109 do presente acórdão, do direito de esperar, por força dos artigos 7.º e 8.º da Carta, que a sua identidade não seja, em princípio, revelada, uma medida legislativa que prevê a conservação generalizada e indiferenciada apenas dos endereços IP atribuídos à fonte de uma ligação não se afigura, em princípio, contrária ao artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, desde que essa possibilidade esteja sujeita ao estrito respeito das condições materiais e processuais que devem reger a utilização desses dados.

156. Tendo em conta o caráter grave da ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta que esta conservação comporta, só a luta contra a criminalidade grave e a prevenção das ameaças graves contra a segurança pública são suscetíveis, à semelhança da salvaguarda da segurança nacional, de justificar essa ingerência. Além disso, o período de conservação não pode exceder o estritamente necessário à luz do objetivo prosseguido. Por último, uma medida desta natureza deve prever requisitos e garantias estritas quanto à exploração desses dados, nomeadamente através de um rastreio das comunicações e atividades efetuadas em linha pelas pessoas em causa. "

3.3.3. Implicações para o presente relatório

A evolução da jurisprudência internacional sobre obrigações positivas nas últimas décadas tem sido acompanhada por um aumento das normas e instrumentos dos tratados internacionais e regionais. O resultado é um corpo consolidado de obrigações internacionais e europeias em matéria de direitos humanos impostas aos Estados para criminalizar, prevenir, investigar, processar e punir as violações dos direitos fundamentais por parte de atores privados. A par da proteção da vida, segurança e violência de género, a proteção das crianças contra o abuso sexual é um objetivo-chave deste campo do direito.

O interesse superior da criança como consideração primordial de todas as autoridades públicas, e a proteção contra a violência sexual, abuso e exploração, está incorporado na UNCRC e no respetivo Protocolo Opcional sobre a Venda de Crianças, Prostituição Infantil e Pornografia Infantil. Estes instrumentos sustentam uma série de instrumentos de direito internacional mais recentes na salvaguarda destes direitos fundamentais da criança.[174] No Conselho da Europa, a CL é o principal tratado especializado que "prevê, sem dúvida, os mais elevados padrões internacionais de proteção das crianças contra o abuso e exploração sexual".[175] Este instrumento complementa uma série de normas do CoE, em particular a Convenção de Budapeste, destinada à proteção das crianças contra a violência e exploração sexual em linha e fora de linha.[176] Na UE, o artigo 24.º da Carta da UE, e o n.º 3 do artigo 3.º do Tratado da UE, salvaguardam os direitos da criança e o princípio de que "as crianças têm direito à proteção e aos cuidados necessários ao seu bem-estar".[177] Além disso, o n.º 1 do artigo 83.º do Tratado sobre o Funcionamento da União Europeia enumera "a exploração sexual de mulheres e crianças" como um dos " domínios de criminalidade particularmente grave com dimensão transfronteiriça ". Finalmente, a Diretiva CSEA é um instrumento legislativo especializado concebido para incorporar a proteção oferecida

174 Protocolo para Prevenir, Reprimir e Punir o Tráfico de Pessoas, Especialmente Mulheres e Crianças, em complemento à Convenção das Nações Unidas contra o Crime Organizado Transnacional (15 de novembro de 2000); Agenda da ONU para o Desenvolvimento Sustentável, Objetivos 5, 8 e 16; Declaração do Rio de Janeiro e Apelo à Ação para Prevenir e Parar a Exploração Sexual de Crianças e Adolescentes (2008); "Diretrizes Terminológicas do Grupo de Trabalho Interagências sobre Exploração Sexual de Crianças"; e o Conselho Económico e Social da ONU, Comissão de Prevenção do Crime e Justiça Criminal, "Combater a exploração sexual e o abuso sexual de crianças em linha" (24 de maio de 2019).

175 Proposta de Decisão-Quadro da UE relativa à luta contra o abuso sexual, a exploração sexual de crianças e a pornografia infantil (COM (2010) 94 final, p. 2), que revoga a Decisão-Quadro 2004/68/JAI.

176 Artigo 7.º da Carta Social Europeia; artigo 17.º da Carta Social Europeia revista; Orientações do Conselho da Europa sobre Justiça Amiga da Criança (2010); Recomendação sobre orientações para respeitar, proteger e cumprir os direitos da criança no ambiente digital (CM/Rec(2018)). Ver ainda o Anexo.

177 N.º 1 do artigo 24.º da Carta dos Direitos Fundamentais da União Europeia.

pela CL no direito da UE. Tal como a CL, a Diretiva CSEA inclui obrigações específicas do Estado para proteger as crianças da OCSEA.

No TEDH, a proteção das crianças contra o abuso e exploração sexual é afirmada como uma obrigação positiva decorrente dos artigos 3.º e 8.º da CEDH. O âmbito e a estrutura desta obrigação geral foram desenvolvidos ao longo de vinte e cinco anos de jurisprudência do TEDH, e evoluíram à luz do desenvolvimento de normas internacionais e europeias. O TEDH sublinha que a concretização desta obrigação positiva deve ser "prática e eficaz". Os Estados devem consequentemente alcançar o seu objetivo declarado, na prática e não num sentido teórico ou ilusório. Tal como recentemente densificado em dois casos principais,[178] a obrigação consiste no dever de "manter e aplicar na prática um quadro jurídico adequado que proporcione proteção contra atos de violência por particulares". Isto implica que os Estados adotem disposições de direito penal para a punição efetiva do abuso sexual de crianças e apliquem estas disposições, na prática, através de uma investigação e ação penal eficazes. A obrigação também exige que os Estados cooperem com as autoridades de outros Estados para procurarem ou prestarem assistência mútua e esgotarem "de boa-fé" todos os "instrumentos internacionais aplicáveis em matéria de assistência jurídica mútua e cooperação em matéria penal".[179]

O TJUE reconhece o peso da proibição do abuso sexual de crianças na ordem jurídica da UE, observando a gravidade do crime como uma "ameaça particularmente grave a um dos interesses fundamentais da sociedade",[180] constituindo uma "ameaça grave à segurança pública",[181] e apresentando "características particularmente graves".[182] O TJUE vê o abuso sexual de crianças como uma grave violação dos direitos fundamentais das crianças, e incorporou a proteção contra a OCSEA no princípio do interesse superior da criança, tal como expresso no artigo 24.º da Carta da UE, na UNCRC e na Diretiva da CSEA.[183]

A jurisprudência sobre obrigações positivas também tem sido clara relativamente à margem de apreciação dos Estados quanto aos meios de cumprimento das obrigações de proteção. Quando a margem de apreciação do Estado é correspondentemente estreita porque é definida por um direito absoluto, há uma forte presunção de que a obrigação positiva deve ser cumprida através de meios práticos, eficazes e adequados. Este é claramente o caso no que respeita à proteção contra a OCSEA, que tem sido repetidamente considerada como uma violação das garantias dos direitos mais fundamentais das ordens internacionais e eu-

178 A e B v. Croácia, GC, Na. N.º 7144/15, final 4/11/2019; X e outros v. Bulgária, GC, An. n.º 22457/16, 2 de fevereiro de 2021.

179 X e outros v. Bulgária, par. 191.

180 P.I. v. Oberbürgermeisterin der Stadt Remscheid, par. 28

181 La Quadrature du Net e outros v. Premier Ministre e outros, par. 152.

182 P.I. v. Oberbürgermeisterin der Stadt Remscheid, par. 28.

183 P.I. v. Oberbürgermeisterin der Stadt Remscheid, par. 32.

ropeias, em matéria de direitos humanos. Embora o âmbito da margem de apreciação do Estado neste contexto seja reduzido,[184] o TEDH ainda não exigiu aos Estados a adoção de um sistema obrigatório de apresentação de relatórios por entidades privadas. Além disso, resulta da jurisprudência do TEDH e do TJUE que os Estados não podem negar direitos compensatórios/ indemnizações em caso de violação da privacidade e do direito à proteção de dados pessoais.[185] Por conseguinte, os Estados-Membros devem encontrar um bom equilíbrio entre o respeito pela proteção da privacidade e a proteção de dados, respeitando simultaneamente as normas mínimas exigidas pelas obrigações positivas que lhes são impostas.

3.4. Condições e salvaguardas de proteção de dados

A deteção e comunicação voluntária da OCSEA por PS são frequentemente caracterizadas como uma restrição ilegal da privacidade individual e, consequentemente, não admissíveis ao abrigo da legislação de proteção de dados aplicável. Embora esse tratamento de dados constitua efetivamente uma interferência considerável aos direitos à privacidade e à proteção de dados pessoais, esta secção fornece orientações em relação às condições e garantias de proteção de dados que podem sustentar a realização de deteção e comunicação voluntária de dados de OCSEA.

Mais especificamente, providencia orientações sobre quais os conteúdos (tais como imagens, vídeo e texto) ou dados de tráfego que podem ser tratados para detetar automaticamente a OCSEA e denunciar voluntariamente esses casos às autoridades competentes em matéria penal e/ou às linhas diretas reconhecidas ou outras organizações que atuam no interesse público contra a OCSEA. A proteção de dados e as garantias a seguir descritas são dirigidas aos PS, tal como definidas na introdução do presente relatório. Inclui-se a comunicação e PS, relativamente a prestadores dos já mencionados NI-ICS e aos intermediários que fornecem serviços publicamente disponíveis relacionados com o armazenamento, transmissão ou fornecimento de informações através da Internet (tais como alojamento, simples transporte, (nuvem) espaço para carregamento de conteúdos). Além disso, e em conformidade com a abordagem geral deste relatório, esta secção centra-se na prática da deteção e comunicação voluntária da OCSEA por PS principalmente fundamentada em motivos de interesse público, tal como descrito pelos quadros legais aplicáveis existentes.

184 K.U. v. Finlândia, An. n.º 2872/02, 02 de março de 2009; Söderman v. Suécia, An. n.º 5786/08, 12 de novembro de 2013; A e B v. Croácia, An. n.º 7144/15, final 4/11/2019; X e outros v. Bulgária, GC, An. n.º 7144/15, final 4/11/2019; X e outros v Bulgária, GC, App. No. 22457/16, 2 de fevereiro de 2021.

185 CJEU: La Quadrature du Net e outros v. Premier Ministre e outros; ECtHR: Trabajo Rueda v. Espanha, An. n.º 32600/12, 30 de maio de 2017.

3.4.1. Jurisprudência relevante do TEDH sobre o artigo 8.º da CEDH

As condições para a utilização legítima de exceções foram inicialmente desenvolvidas pelo TEDH em casos relacionados com a vigilância estatal das comunicações, tais como no caso Malone v. Reino Unido quanto à "previsibilidade das medidas",[186] Huvig v. França, Kruslin v. França quanto à "natureza suficientemente clara da legislação subjacente",[187] Weber & Saravia v. Alemanha quanto às "salvaguardas mínimas" [188] e Zakharov v. Rússia e Szabó v. Hungria quanto à "suspeita razoável", "necessidade estrita" e "autorização judicial".[189] Em casos como o K.U. v. Finlândia , na procura do equilíbrio entre as "obrigações positivas dos Estados" de fornecer meios eficazes para a proteção dos indivíduos contra a OCSEA e as condições de proteção da confidencialidade das comunicações, foi dada uma importância significativa às primeiras.[190] Em Trabajo Rueda v. Espanha, no entanto, a "busca e apreensão desproporcionada" de material da OCSEA foi vista como uma violação do artigo 8.º e em Benedik v. Eslovénia foi dada prioridade ao "respeito pelas garantias processuais", bem como à "admissibilidade da prova perante um tribunal" em relação à acusação da OCSEA.[191]

3.4.2. Proteção global de dados do Conselho da Europa

As seguintes regras e garantias de proteção de dados nos quais os prestadores de serviços podem confiar quando detetam e comunicam voluntariamente OCSEA, baseiam-se nas obrigações decorrentes da Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (ETS n.º 108, a seguir denominada: Convenção 108), e, quando vier a entrar em vigor, na Convenção 108 alterada pelo Protocolo CETS 223 (a seguir denominada: Convenção 108+), que constitui o quadro geral de proteção de dados do Conselho da Europa. Estes estão também em consonância com outros enquadramentos de proteção de dados potencialmente aplicáveis, incluindo os da União Europeia. As diretrizes só são relevantes se os dados pessoais forem efetivamente tratados quando a OCSEA for detetada, comunicada e apagada ou para qualquer outro tratamento subsequente compatível. É importante notar que, embora a utilização de tecnologia de *hashing* para a pseudonimização não reconvertível de imagens e vídeos seja considerada

186 Malone v. Reino Unido, An. n.º 8691/79, 2 de agosto de 1984.

187 Kruslin v. França, An. n.º 11801/85, 24 de abril de 1990; Huvig v. França, An. n.º 11105/84, 24 de abril de 1990.

188 Weber e Saravia v. Alemanha, An. n.º 54934/00, 29 de junho de 2006.

189 Zakharov v. Rússia, An. n.º 47134/06, 4 de dezembro de 2015; Szabó e Vissy v. Hungria, An. n.º 37138/14, 06 de junho de 2016.

190 K.U. v. Finlândia, An. n.º 2872/02, 02 de março de 2009. Ver também secção 3.3. acima sobre obrigações positivas de proteção contra a OCSEA.

191 Trabajo Rueda v. Espanha, An. n.º 32600/12, 30 de maio de 2017; Benedik v. Eslovénia, An. n.º 62357/14, 8 de abril de 2015.

uma salvaguarda importante - tendo em vista a sua comparação anónima com material de abuso e exploração sexual de crianças em repositórios ou bases de dados de confiança e com dados de qualidade - isto não isenta tais processos de deteção do cumprimento dos requisitos da lei de proteção de dados. O *hashing* é apenas uma técnica de preservação da privacidade e o próprio processo de anonimização de dados pessoais, tais como imagem e conteúdo vídeo, envolve o tratamento de dados pessoais, que permanece sujeito à lei de proteção de dados. Além disso, qualquer comunicação baseada num "resultado/*hit*" positivo após comparação, ou baseada em suspeita razoável após deteção de padrão (baseado em IA) em dados de texto ou de tráfego, utilizando, em alguns casos, dados históricos, envolverá a transferência de dados pessoais (informação de utilizador ou de IP) e, por conseguinte, estará sujeita à lei de proteção de dados.

Base legal

Para que os PS nos Estados Membros do CoE possam detetar automaticamente e denunciar voluntariamente a OCSEA quando esta envolve o tratamento de dados pessoais, esse tratamento deve cumprir as condições estabelecidas no artigo 8.º da CEDH, bem como as regras internas aplicáveis em matéria de proteção de dados, incluindo nos termos das obrigações decorrentes da Convenção 108+.

Embora o artigo 11.º da Convenção 108+ permita exceções a um número limitado de princípios de proteção de dados sujeitos a condições estritas, não é permitida qualquer derrogação aos artigos 5.º, n.º 2 e 5.º, n.º 3 da Convenção 108+, os quais exigem uma base legal para qualquer tratamento pretendido.

Embora o artigo 5.3 da Convenção 108+ exija que qualquer tratamento de dados pessoais ocorra de forma lícita, o artigo 5.2 limita a possibilidade de os PS detetarem automaticamente e comunicarem voluntariamente à OCSEA desde que haja (a) consentimento livre, específico, informado e inequívoco dos utilizadores em causa ou outro fundamento legítimo previsto por lei, que, de acordo com o parágrafo 46 do Relatório Explicativo da Convenção 108+, abrange, entre outros, o tratamento de dados (b) de acordo com interesses legítimos predominantes do responsável pelo tratamento ou de terceiros ou (c) realizado com fundamento em interesse público.[192]

Os três fundamentos potenciais supra referidos para a deteção automática da OCSEA e a apresentação voluntária de relatórios são seguidamente avaliados de forma substantiva.

192 Relatório Explicativo do Protocolo que altera a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automático de Dados Pessoais (CETS 223) (doravante: Relatório Explicativo da Convenção 108+), Estrasburgo 10.X.2018, par. 46.

Consentimento

A questão de saber se os PS podem fundamentar o tratamento de dados para a deteção automática e comunicação voluntária da OCSEA, apenas com base no mero consentimento do utilizador, ou seja, estabelecendo nos seus termos e condições que a aceitação da prestação de serviços por parte do utilizador abrange a digitalização automática do conteúdo das comunicações ou dos dados de tráfego a fim de detetar possíveis OCSEA e comunicá-los às autoridades ou a linhas diretas reconhecidas ou a outras organizações que atuem no interesse público, deve ser respondida negativamente. O consentimento do utilizador, a fim de ser qualificado como fundamento válido para o tratamento de dados pessoais, não só deve ser específico e informado (eventualmente poderá ser o caso se estipulado nos termos e condições), como também deve ser dado livremente. De acordo com o parágrafo 42 do Relatório Explicativo da Convenção 108+, "o consentimento deve representar a livre expressão de uma escolha intencional, [...] que indica claramente neste contexto específico a aceitação do tratamento de dados pessoais proposto", de modo que "o consentimento não deve ser considerado como dado livremente quando a pessoa em causa não tem escolha genuína ou livre". No caso de aceitação obrigatória dos termos e condições, não existe consequentemente uma escolha genuína ou livre. Além disso, uma vez que a OCSEA detetada seria também comunicada, através das linhas diretas reconhecidas ou de outras organizações que atuam no interesse público, às autoridades competentes em matéria penal, a fim de permitir a essas autoridades investigar e processar a OCSEA, o consentimento obrigatório do utilizador é ainda menos aceitável como fundamento legal para o processamento.

Interesse legítimo

A resposta à questão de saber se os PS podem fundamentar validamente o processamento para a deteção automática e comunicação voluntária de OCSEA em "interesses legítimos predominantes " (como definido no parágrafo 46 do Relatório Explicativo da Convenção 108+), de si próprios (enquanto controladores de dados), ou de terceiros, é mais complexa.

Embora as autoridades competentes em matéria penal, às quais a OCSEA seja voluntariamente notificada ou revelada, tenham interesse em receber tal informação, o "interesse de terceiro" (em investigar e acusar) não seria facilmente qualificado como fundamento legítimo nos termos do n.º 2 do artigo 5.º da Convenção 108+. Neste último caso, os Estados-Membros estariam melhor colocados para tratar dados pessoais com base no interesse público, tal como se refere a seguir.

Quando se trata do interesse legítimo do próprio PS, a resposta à questão pode variar, dependendo das regras internas que se lhes aplicam e/ou se se qualificam legalmente como sendo PS de comunicação eletrónica. Na UE, por exemplo, os PS de comunicações eletrónicas têm a obrigação de assegurar estritamente a confidencialidade do conteúdo das comu-

nicações e dos dados de tráfego relacionados, nos termos dos artigos 5.º e 6.º da Diretiva de Privacidade e Comunicações Eletrónicas, não sendo permitida qualquer derrogação com base no seu próprio interesse legítimo. Em conformidade com o artigo 15.º da Diretiva relativa à Privacidade, as restrições das suas obrigações nos termos dos artigos 5.º e 6.º só são possíveis tendo por base medidas legislativas adotadas pelos Estados-Membros. Assim, os prestadores que se encontrem abrangidos pelo âmbito geográfico e material da Diretiva relativa à Privacidade e às Comunicações Eletrónicas, que desde 21 de dezembro de 2021 inclui os prestadores de NI-ICS, só estão autorizados a procurar automaticamente OCSEA e a proceder à comunicação respetiva se puderem assentar numa base legal, sustentada no interesse público. Tal base jurídica deve prosseguir os objetivos, e estar de acordo com as disposições específicas, dos instrumentos internacionais aplicáveis, tais como a Convenção de Lanzarote (cfr infra). Nos casos em que PS têm a obrigação de pesquisar OCSEA, as disposições de tais regimes obrigatórios constituiriam elas próprias a base jurídica.

Como resultado, apenas os PS que não estejam sob uma obrigação tão estrita, podem legalmente fundamentar a deteção automática e consequente comunicação de OCSEA, no seu próprio interesse legítimo, mesmo que com condições e limitações. Embora seja uma perspetiva empresarial legítima para os PS querer que os seus serviços estejam livres de conteúdos e material que considerem indesejáveis, ou simplesmente porque não desejam facilitar a disponibilidade em linha de tal material (que pode mesmo ir além do conteúdo impróprio, como a OCSEA), isto não proporciona aos PS uma capacidade incondicional ou ilimitada de reservar o direito (por exemplo , nos seus termos e condições) de tratar automaticamente o conteúdo ou dados de tráfego de comunicações para detetar tal conteúdo ou material e removê-lo ou, no caso da OCSEA, denunciá-lo.

Tanto a digitalização automática como as comunicações são operações de tratamento que, mesmo quando realizadas no legítimo interesse empresarial do PS, justificam um teste de equilíbrio. De acordo com o parágrafo 48 do Relatório Explicativo da Convenção 108+, "a legitimidade de uma finalidade dependerá das circunstâncias, sendo o objetivo assegurar, em cada caso, um justo equilíbrio entre os direitos liberdades e interesses em jogo: o direito à proteção de dados pessoais, por um lado, e a proteção de outros direitos, por outro. Deve ser encontrado um justo equilíbrio entre os interesses do entre os interesses da pessoa em causa e os do responsável pelo tratamento ou da sociedade" parágrafo 46 do Relatório Explicativo da Convenção 108+, como já referido anteriormente , implica ainda maior rigor, ao exigir que o interesse legítimo do responsável pelo tratamento de dados seja "predominante", o que significa que não pode ser anulado pelos interesses ou direitos e liberdades fundamentais da(s) pessoa(s) implicada(s), incluindo o seu direito à proteção de dados, à privacidade e à confidencialidade da sua correspondência. A verificação e a comunicação da OCSEA afetam populações inteiras de utilizadores, pelo que o controlo indiscriminado e generalizado do conteúdo e dos dados de tráfego apenas resistirá ao teste do equilíbrio quando sujeito a condições e salvaguardas rigorosas de preservação da privacidade.

Interesse público

De acordo com o parágrafo 47 do Relatório Explicativo da Convenção 108+, o tratamento de dados efetuado por motivos de interesse público deve ser previsto por lei, e pode, entre outros, ser efetuado para a prevenção, investigação, deteção e repressão de infrações penais, como a OCSEA. Como já anteriormente mencionado, um enquadramento jurídico sustentado no interesse público irá, para muitos prestadores, dependendo das regras internas a que estão sujeitos, proporcionar o caminho legal mais sólido para tratamento automático da OCSEA e a respetiva comunicação voluntária.

Assim, recomenda-se vivamente que os Estados-Membros do CoE, de acordo com as suas obrigações positivas, estabelecidas na jurisprudência do TEDH,[193] em relação aos artigos 3.º e 8.º da CEDH e à proteção das crianças contra a OCSEA, estabeleçam um enquadramento legal específico baseado no interesse público, permitindo aos PS detetar automaticamente e comunicar voluntariamente OCSEA sob uma série de condições e garantias. Neste contexto, a Convenção de Lanzarote poderia representar normas partilhadas sobre a definição de tal interesse público.

Dados sensíveis

Quando o tratamento de imagens e vídeos para efeitos de deteção de OCSEA for revelador da vida sexual/preferência de indivíduos, incluindo crianças, tais dados devem ser considerados como dados sensíveis. Isto implica, em conformidade com o artigo 6.º da Convenção 108+, que tal tratamento só será permitido quando, para além das salvaguardas incluídas na Convenção 108+, tenham sido consagradas na lei salvaguardas adequadas. Estas salvaguardas devem oferecer proteção contra os riscos que o tratamento em causa possa apresentar para os interesses, direitos e liberdades fundamentais dos titulares dos dados

A proteção dos interesses, direitos e liberdades fundamentais das crianças implica que os PS, ao longo das suas atividades relacionadas com a deteção automática, remoção e denúncia voluntária da OCSEA, impeçam interferências indevidas nos direitos dos adolescentes que apareçam em comportamentos sexualmente explícitos, incluindo o seu direito à privacidade e à exploração da sua sexualidade, enquanto dimensões do seu direito à vida privada. Não obstante os desafios tecnológicos e legais que significa fazer distinções qualitativas entre imagens, a proteção do direito das crianças à privacidade deve incluir o direito à descoberta da sua identidade sexual num ambiente seguro e privado. Além disso, os PS devem proteger o desenvolvimento da identidade e experiências sexuais das crianças, e a priva-

193 Ver secção 3.3 acima.

cidade de imagens ou vídeos explícitos nos quais as crianças aparecem e enviam aos seus pares, ou, quando tenham atingido a idade do consentimento sexual ao abrigo da legislação nacional, partilhem mais amplamente esse material.

Os PS devem também evitar a denúncia de aliciamento de crianças às autoridades competentes em matéria penal, quando os utilizadores e os retratados tenham atingido a idade do consentimento sexual nos termos da legislação nacional.

Além disso, a comparação de imagens e vídeos deve evitar a utilização de dados biométricos que são processados através de meios técnicos e legais que permitam a identificação ou autenticação única de uma pessoa singular. Isto exige que se avalie se os dados processados constituem dados biométricos.

3.4.3. Condições e salvaguardas[194]

Não obstante a necessidade de serem estabelecidas outras salvaguardas importantes, associadas ao Estado de direito ao direito penal e às garantias processuais penais, as condições e garantias abaixo indicadas constituem padrões mínimos em matéria de proteção de dados, sem prejuízo da plena aplicação do artigo 8.º da CEDH e das regras nacionais aplicáveis em matéria de proteção de dados, nomeadamente nos termos das obrigações decorrentes da Convenção 108, e, aquando da sua entrada em vigor, da Convenção 108+.

Deve também notar-se que, na medida em que a deteção automática e a comunicação voluntária da OCSEA podem fundamentar-se em interesses legítimos (ver supra), não são permitidas exceções à Convenção 108+. Especificamente para o tratamento de dados, o "teste de equilíbrio" (ou seja, equilíbrio entre o interesse legítimo superior do responsável pelo tratamento e os direitos e interesses dos titulares dos dados, desde que tenham sido estabelecidas garantias adequadas) deve ser a regra. As exceções ao abrigo do artigo 11.º da

194 Inspirado tanto pela Convenção 108+ como pelo projeto de Regulamento do Parlamento Europeu e do Conselho relativo a uma derrogação temporária de certas disposições da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho no que respeita à utilização de tecnologias por prestadores de serviços de comunicações interpessoais independentes do número para o tratamento de dados pessoais e outros para efeitos de combate ao abuso sexual de crianças em linha. As condições e salvaguardas sugeridas incorporam fragmentos de texto do projeto de regulamento, especialmente as alterações propostas pela Comissão LIBE, na sua última versão acessível ao público no momento da redação: Conselho da União Europeia, Proposta de Regulamento do Parlamento Europeu e do Conselho relativo a uma derrogação temporária de certas disposições da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho no que respeita à utilização de tecnologias por prestadores de serviços de comunicações interpessoais independentes do número para o tratamento de dados pessoais e outros para efeitos de combate ao abuso sexual de crianças em linha. Ponto de situação das reuniões técnicas com o PE e discussão das alterações propostas, Bruxelas, 26 de janeiro de 2021, 5616/21.

Convenção 108+ só serão permitidas se forem estabelecidas por lei e apenas a um número limitado de princípios de proteção de dados. Em qualquer caso, tais restrições devem basear-se num interesse público enquadrado na legislação, ter um objetivo legítimo e constituir "uma medida necessária e proporcional numa sociedade democrática", tal como resulta da jurisprudência relevante do TEDH sobre proteção de dados.

Limitação estrita da finalidade

Nos termos do n.º 4, alínea b), do artigo 5.º da Convenção 108+, qualquer tratamento de dados pessoais por PS ao tratar comunicações e dados de tráfego relacionados, deve ser limitado à única finalidade de detetar a OCSEA com o objetivo de a remover, denunciar ou divulgar voluntariamente às autoridades competentes em matéria penal, a linhas diretas reconhecidas ou outras organizações que atuem no interesse público contra a OCSEA.

Minimização dos dados e proporcionalidade

Os dados pessoais tratados na deteção e comunicação voluntária ou divulgação utilizados devem ser minimizados ao estritamente necessário, em conformidade com a alínea b), do n.º 4, do artigo 5.º da Convenção 108+, de modo a assegurar que a proporcionalidade seja o princípio-chave da proteção de dados a ser respeitado.

Proteção de dados desde a conceção e por defeito

Os PS, tal como estabelecido no n.º 2 do artigo 10.º da Convenção 108+, devem conceber o tratamento de dados de forma a evitar ou minimizar o risco de interferência com os direitos e liberdades fundamentais das pessoas em causa. Por conseguinte, as tecnologias que utilizam para a deteção automática:

- devem ser o menos intrusivas possível da privacidade, de acordo com o estado da arte na indústria;

- devem, sempre que sejam utilizadas para tratar imagens ou conteúdos de vídeo, utilizar de preferência o *hashing* para a pseudonimização não reconvertível de imagens e vídeos, tendo em vista a sua comparação anónima com material verificado sobre abuso e exploração sexual de crianças, constante de repositórios ou bases de dados reconhecidamente de confiança e com dados de qualidade;

- devem poder quando são utilizadas para tratar comunicações contendo texto, não ser capazes de compreender a substância do conteúdo, mas apenas detetar padrões

que apontam para possíveis OCSEA, utilizando indicadores-chave relevantes e fatores de risco objetivamente identificados;

• devem ser suficientemente fiáveis na medida em que limitam a taxa de erro de (resultado/*hit*) que sejam falsos positivos ou de deteção de padrões falsos positivos (ou seja, quando o conteúdo é erroneamente identificado ou suspeito de representar OCSEA) na medida do possível, de acordo com o estado da arte no setor. Quando tais erros ocasionais ocorrem, as suas consequências devem ser retificadas sem demora;

• sempre que tecnicamente possível, não devem interferir com qualquer comunicação protegida pelo segredo profissional, tal como o segredo entre médicos e os seus pacientes, os jornalistas e as suas fontes ou os advogados e os seus clientes.

Avaliação do impacto

Os PS devem avaliar o impacto provável do tratamento de dados, nos direitos e liberdades fundamentais dos titulares dos dados, antes do início desse tratamento, tal como devem indicar que o tratamento previsto não implicará um risco elevado para os direitos e liberdades fundamentais das pessoas em causa ou que foram tomadas medidas para atenuar esse risco.

Transparência

Os PS devem informar os titulares dos dados, dos termos e condições relativos à restrição da confidencialidade das suas comunicações e às informações de tráfego relacionadas, com o único objetivo de detetar OCSEA tendo em vista a sua remoção e/ou a sua denúncia ou divulgação voluntária às autoridades competentes em matéria penal e/ou a linhas diretas reconhecidas ou a outras organizações que atuem no interesse público contra a OCSEA.

Além disso, no caso de um "resultado/hit" positivo após comparação com material verificado sobre abuso e exploração sexual de crianças constante de repositórios ou bases de dados reconhecidamente de confiança e com dados de qualidade, ou no caso de uma suspeita razoável após a deteção de padrões (baseados em IA) em dados de texto ou de tráfego, utilizando, em alguns casos, dados históricos, os titulares dos dados devem receber as seguintes informações:

• a identificação das autoridades competentes em matéria penal e as linhas diretas reconhecidas ou outras organizações que atuam no interesse público contra a OCSEA, com as quais os seus dados pessoais tenham sido partilhados;

• as vias de reclamação perante os PS; e

- a possibilidade de apresentar uma queixa junto da autoridade de controlo competente e de um recurso judicial, bem como a identificação dessas autoridades.

O fornecimento destas informações só pode ser adiado na medida estritamente necessária de forma a não prejudicar uma investigação em curso, devendo os titulares dos dados ser informados sem demora após o encerramento da investigação.

Comunicação de OCSEA após deteção automática

Uma vez que a comunicação de OCSEA após a sua deteção automática pode afetar significativamente o titular dos dados, nenhuma comunicação deve basear-se unicamente no resultado do processo de deteção automática. Assim, os PS devem assegurar a supervisão e intervenção humana para o tratamento automatizado de dados pessoais. Aliás, nenhum (resultado/*hit*) positivo ou suspeita razoável deve ser comunicado ou revelado às autoridades competentes em matéria penal e/ou a linhas diretas reconhecidas ou outras organizações que atuem no interesse público contra a OCSEA, sem reavaliação e confirmação humana prévia.

Segurança dos dados

Os PS devem estabelecer procedimentos internos para prevenir abusos, acesso não autorizado, utilização, apagamento ou transferências.

Retenção limitada

Se não tiver sido detetada e confirmada nenhuma OCSEA, todos os dados de conteúdo, dados de tráfego relacionados e qualquer resultado do processamento destes dados serão apagados imediatamente após o seu processamento.

Se a OCSEA tiver sido detetada e confirmada, os dados de conteúdo estritamente relevantes, os dados de tráfego relacionados e os dados pessoais gerados através de tal processamento, serão retidos unicamente para os seguintes fins e apenas durante o período de tempo estritamente necessário, após o qual serão apagados imediata e permanentemente:

- a fim de comunicar e transferir dados sem atrasos indevidos às autoridades competentes em matéria penal e/ou a linhas diretas reconhecidas ou outras organizações que atuem no interesse público contra a OCSEA;

• a fim de bloquear a conta do utilizador em causa ou de suspender um serviço que lhe seja oferecido;

• relativamente a dados pessoais indubitavelmente identificados como OCSEA, a fim de criar um *hash* para comparação futura;

• com o objetivo de permitir a apresentação de queixas e a prossecução de sanções e/ou vias de recurso judiciais e extrajudiciais.

Mecanismo de reclamação e medidas jurídicas corretivas eficazes

Sem prejuízo das reparações a que tenham direito por qualquer violação das regras de proteção de dados, os utilizadores que tenham sido prejudicados pela utilização de tecnologias específicas para o tratamento de dados pessoais para detetar e remover ou denunciar a OCSEA, devem poder apresentar uma queixa contra a ação do PS e ter o direito a medidas jurídicas corretivas eficazes, quando o material removido ou denunciado não constituir OCSEA. Assim, os PS devem estabelecer mecanismos de queixa eficazes e acessíveis e o membro do Conselho da Europa deve estabelecer procedimentos eficazes de recurso, incluindo os casos em que:

• o conteúdo dos utilizadores tenha sido removido ou a sua conta tenha sido bloqueada ou um serviço que lhes tenha sido oferecido tenha sido suspenso;

• o conteúdo ou identidade dos utilizadores tenham sido comunicados às autoridades competentes em matéria penal ou a uma linha direta reconhecida ou outra organização que atue no interesse público contra a OCSEA.

Fluxos transfronteiriços de informação

Durante todo o processo de comparação automática do conteúdo de imagens ou vídeos tratados com repositórios ou bases de dados externas, comunicação ou divulgação da OCSEA às autoridades competentes em matéria penal e/ou a linhas diretas reconhecidas ou outras organizações que atuem no interesse público, os PS devem respeitar integralmente as condições aplicáveis aos fluxos transfronteiriços de dados pessoais, tais como as que se encontram estabelecidas no Capítulo III da Convenção 108+.

Isto implica que os PS poderiam recorrer ao artigo 14.º da Convenção 108+ quando o Protocolo de Alteração CETS n.º 223 entrar em vigor e enviar dados pessoais sem quaisquer condições adicionais, a outras Partes nesse Protocolo, se nenhuma das exceções previstas no n.º 1 do artigo 14.º se aplicar a essa transferência de dados em particular. Como é pou-

co provável que tal aconteça no futuro imediato e certamente não antes de 2023, e ainda assim provavelmente não para todas as principais jurisdições envolvidas na transferência de dados para fins da OCSEA, o n.º 3 do artigo 14.º da Convenção 108+ poderia também desempenhar um papel legitimador em relação a um PS que deseje enviar dados pessoais para outro Estado ou jurisdição.

Nestes termos, "é assegurado um nível adequado de proteção com base nas disposições da presente Convenção" durante a transferência e no Estado recetor, o que deverá dar garantias suficientes a qualquer entidade privada para cooperar e enviar dados através de um dos métodos que a seguir descreveremos. Nos termos do n.º 3 do artigo 14.º da Convenção 108+, "um nível adequado de proteção pode ser assegurado pela: a) lei desse Estado ou organização internacional, incluindo os tratados ou acordos internacionais aplicáveis; ou por b) garantias *ad hoc* ou normalizadas e aprovadas, estabelecidas por instrumentos juridicamente vinculativos e executórios, adotados e implementados pelas pessoas envolvidas na transferência e no tratamento posterior dos dados". Consequentemente, seriam necessários mais esforços na avaliação e, quando aplicável, no desenvolvimento de tais salvaguardas provisórias.

Os termos e condições do artigo 14.º do segundo Protocolo adicional à Convenção de Budapeste (tal como descrito na secção 3.3.1) poderiam também desempenhar um papel central ao decidir sobre a condição a) (isto é, se a lei de um país proporciona um nível adequado de proteção de dados pessoais durante as transferências de dados de natureza transfronteiriça). De acordo com a Convenção 108+ - e especialmente o seu primeiro regime de exceção descrito no n.º 1 do artigo 11.º - bem como o regime de proteção de dados da União Europeia e dos Estados Partes na Convenção de Budapeste (incluindo os EUA, Canadá, Austrália e Japão, etc.), esses termos e condições poderiam ser analisados quando os Estados estão envolvidos na cooperação em matéria de auxílio judiciário mútuo em matéria penal, que também envolve o tratamento de provas eletrónicas, ao mesmo tempo que se procura assegurar um nível adequado de proteção durante a transferência de dados entre autoridades relativamente a investigações específicas em curso que dizem respeito a dados já disponíveis e frequentemente detidos por PS. O segundo protocolo adicional à Convenção de Budapeste deverá ser aberto a assinatura na Primavera de 2022. O regime de transferência que estabeleceria aquando da sua entrada em vigor significaria para os PS, que o país em que estão estabelecidos tomasse uma série de medidas, incluindo medidas legislativas, aquando da sua ratificação e que continuasse a cumprir os regulamentos de proteção de dados desse país. Por conseguinte, é provável que a condição b) (isto é, quando o nível adequado de proteção se concretizar através de garantias ad hoc ou normalizadas e aprovadas, juridicamente vinculativas) venha a ser utilizada por entidades privadas durante algum tempo.

A fim de os auxiliar na avaliação do nível de proteção que um Estado ou uma organização internacional poderia garantir através da sua legislação, os interessados poderiam ser encorajados e apoiados a desenvolver "registos" de importadores de dados" e "centros de

relatórios de países" que já estão a ser utilizados ou a ser desenvolvidos por entidades públicas e privadas globais. Tais instrumentos incluem listas de países, baseadas numa avaliação jurídica completa, para onde os dados pessoais poderiam ser enviados sem descer o nível de proteção de dados pessoais existente no país onde o PS está estabelecido ou fornece serviços. Avaliações de entidades públicas, tais como as decisões de adequação da Comissão Europeia ou as avaliações realizadas pelo Comité da Convenção 108 em relação a países que solicitem a adesão à Convenção 108 ou que no futuro solicitem uma avaliação do seu nível de proteção nos termos das alíneas e) e f) do artigo 23.º, poderiam também ser utilizadas como guias de avaliação.

Em termos de cumprimento da condição da alínea b) do n.º 3 do artigo 14.º da Convenção 108+, várias opções estão já disponíveis e poderiam orientar o processo de transferência de dados pessoais de uma jurisdição para outra, no que diz respeito ao nível de proteção já existente, sendo de relevar entre outros, o seguinte : as cláusulas contratuais-tipo (SCC) para transferências de dados entre países da UE e países terceiros que podem ser utilizadas com segurança num contexto não comunitário ou não exclusivamente comunitário; ou as normas ao abrigo das Recomendações 01/2020 sobre medidas que complementam os instrumentos de transferência para assegurar o cumprimento do nível de proteção de dados pessoais da UE e as Recomendações 02/2020 sobre as Garantias Essenciais Europeias para medidas de vigilância, ambas adotadas pelo Conselho Europeu para a Proteção de Dados (CEPD).

No que concerne à transferência de dados e à sua devolução, esta situação respeita às obrigações que incumbem aos destinatários dos dados no estrangeiro, após terminado o tratamento de dados. As partes podem nomeadamente acordar que, uma vez terminados estes serviços, o importador de dados e o subcontratante ulterior devem devolver (ou destruir, caso seja solicitado) todos os dados pessoais transferidos, exceto se a legislação imposta ao importador de dados o impedir.

Contudo, tanto as SCC como as Recomendações, precisam de ser avaliadas à luz das decisões da decisão do TJUE no âmbito do Comissário de Proteção de Dados v. Facebook Ireland Limited e Maximillian Schrems ("Schrems II")[195]. A decisão Schrems II, considera inválido o instrumento de transferência bilateral entre a União Europeia e os EUA pela segunda vez e debruça-se sobre dois requisitos específicos. O primeiro é a necessidade de previsão de medidas jurídicas corretivas eficazes, ou seja, direitos efetivos de recurso individual, perante um tribunal independente e imparcial. O segundo, relativo ao nível de determinados programas de vigilância, é a ausência de limitações ao acesso por parte das autoridades estatais aos dados pessoais, violando assim o princípio da necessidade estrita. À luz do acórdão, está a ser negociado um novo acordo mais duradouro e sustentável entre a União Europeia e os

195 Comissário de Proteção de Dados v. Facebook Ireland Limited e Maximillian Schrems, Processo C-311/18, 16 de julho de 2020.

EUA que poderá também ter um impacto nas transferências de dados para efeitos da OCSEA e já teve consequências diretas na versão SCC atualizada, recentemente publicada pela Comissão Europeia, a 4 de junho de 2021[196]. Além disso, esta decisão também levou o CEPD a resumir os requisitos essenciais que um responsável pelo tratamento de dados tem de observar ao transferir dados pessoais da União Europeia para um Estado não membro da UE. Isto contém condições muito semelhantes às estabelecidas pelo artigo 11.º da Convenção 108+ que se baseia na jurisprudência precedente do TEDH acima explicada.

Alguns dos modelos que foram desenvolvidos (e publicados) pela indústria, tais como a prática de "Avaliação do impacto da transferência de dados" também necessitariam de maior análise. A metodologia completa de tais avaliações não pode ser descrita neste relatório, mas alguns dos seus elementos-chave poderiam servir de base para futuras reflexões. Estes geralmente recomendam, após o levantamento de todas as operações de transferência, soluções técnicas como salvaguardas adicionais às que já são aplicadas às transferências (em relação à segurança dos dados, qualidade dos dados, transparência, base jurídica apropriada, cuidados devidos aos dados sensíveis, requisitos de responsabilização, etc.). Exemplos de tais soluções incluem a encriptação com a chave na posse do pessoal do país remetente, e a colocação de transferências estratégicas Onshore. Além disso, as avaliações recomendam geralmente a elaboração de Regras Corporativas Vinculativas próprias por parte das empresas, a fim de serem validadas pela Autoridade Local de Proteção de Dados e, em última instância, pelo CEPD. Finalmente, como solução a longo prazo, as avaliações recomendam a organização de armazenamento de dados local para utilização de soluções técnicas mais subtis, tais como serviços de nuvem facilitados por prestadores na mesma jurisdição, blockchain, fiéis depositários de dados, "Data trusts", etc.

3.4.4. Implicações para este relatório

A deteção automática e a comunicação voluntária de casos de OCSEA tem impacto quanto à confidencialidade do conteúdo das comunicações e dos dados de tráfego relacionados, que os PS devem assegurar. Constitui uma interferência no direito à vida privada e familiar e à proteção dos dados pessoais das pessoas envolvidas, ou seja, dos utilizadores, incluindo potenciais infratores, bem como das crianças que figuram em OCSEA, que também devem poder comunicar confidencialmente com um adulto de confiança, organizações ativas na luta contra o abuso ou exploração sexual de crianças, e com os seus advogados.

Embora a utilização de tecnologia de *hashing* para a pseudonimização não reconvertível de imagens e vídeos - tendo em vista a sua comparação anónima com material verificado sobre

196 Standard contractual clauses for international transfers | European Commission (europa.eu).

abuso e exploração sexual de crianças, constante de repositórios ou bases de dados reconhecidamente de confiança e com dados de qualidade - seja considerada uma salvaguarda importante, não isenta esse processo de deteção dos requisitos da lei de proteção de dados. O *hashing* é apenas uma técnica de preservação da privacidade, e o próprio processo de anonimização de dados pessoais, tais como conteúdos de imagem e vídeo, envolve um tratamento de dados pessoais, que permanece sujeito à lei de proteção de dados. Além disso, qualquer comunicação baseada num (resultado/*hit*) positivo após comparação ou baseada em suspeita razoável após deteção de padrão (baseado em IA), em dados de texto ou de tráfego, utilizando, em alguns casos, dados históricos, envolverá a transferência de dados pessoais (informação de utilizador ou de IP) e, por conseguinte, estará sujeita à lei de proteção de dados.

4. PRINCIPAIS CONCLUSÕES E RECOMENDAÇÕES

Atualmente os tipos de exploração sexual e abuso sexual de crianças, mais do que duplicaram, em comparação com o final da década de 90. O uso prevalecente das tecnologias da informação e comunicação (TIC) dá origem a uma situação em que as crianças podem estar expostas em linha a muitos dos mesmos riscos a que estão sujeitas no mundo real. O apelo a uma ação concertada para as proteger da OCSEA adquire ainda mais força, face à influência que a pandemia do COVID-19 exerceu sobre as principais ameaças por detrás da OCSEA.

> **Recomendação 1:** O sucesso da prevenção e combate das atuais formas de OCSEA exige que os atores do Estado se mantenham atualizados e reajam aos constantes desenvolvimentos tecnológicos nesta área, facilitados especialmente pela utilização prevalecente das TIC em constante evolução. A utilização de tecnologia automatizada na luta contra a OCSEA é, a este respeito, essencial.

Existe uma discrepância entre a utilização de tecnologias de deteção automática e o nível de informação pública disponível sobre a sua adoção. Este nível insuficiente de informação dificulta que decisores políticos e os reguladores estejam habilitados a desenvolver uma opinião adequada sobre a forma de regular estas tecnologias e sugerir garantias adequadas.

> **Recomendação 2:** Garantir um equilíbrio adequado entre a privacidade e a proteção das crianças contra a exploração e o abuso sexual, promovendo um diálogo entre empresas do setor privado e decisores/reguladores políticos, é da maior importância. Tal diálogo deve ter como principal objetivo assegurar uma transparência adequada na escolha da tecnologia utilizada e dos processos em torno da sua utilização.

O atual nível de transparência, sobre a qualidade e dimensão das *hashlists* de CSAM conhecidas, é insuficiente e limita, em certa medida, o potencial de uma solução tecnológica em relação à rápida remoção de tal material.

> **Recomendação 3:** As iniciativas destinadas a melhorar a coordenação nesta área devem ser indicadas e apoiadas, uma vez que são vitais para a fiabilidade das bases de dados de referência. A este respeito, é também necessário assegurar maior clareza sobre a forma como os mecanismos de responsabilização são geridos, incluindo o recrutamento e formação de indivíduos cuja função em empresas do setor privado implica a avaliação de conteúdos ilegais, tais como o CSAM.

Quando se trata de definir garantias, uma tecnologia bem testada, bem documentada e estável é uma escolha mais segura para os decisores políticos e reguladores. Contudo, para enfrentar os atuais desafios em relação à OCSEA, pode ser aconselhável ou necessário utilizar tecnologias mais poderosas numa fase inicial do seu desenvolvimento.

> **Recomendação 4:** Para melhor manter um equilíbrio entre a privacidade e a proteção das crianças contra a exploração e o abuso sexual, a definição do nível adequado de garantias deve ter lugar o mais cedo possível no processo de desenvolvimento da tecnologia. Os decisores políticos e os reguladores devem dar especial atenção ao conjunto de dados utilizado por essa tecnologia para formar combinações complexas de algoritmos.

Cada ferramenta de deteção de OCSEA é diferente e tem os seus próprios objetivos. A identificação dos meios menos restritivos de deteção de OCSEA requer uma compreensão muito precisa do objetivo e do ambiente para o qual a tecnologia virá a ser selecionada.

> **Recomendação 5:** A fim de reforçar a privacidade, dando prioridade à proteção das crianças contra a exploração e o abuso sexual, é necessário promover soluções tecnológicas que sejam as mais eficientes para o fim considerado.

O número limitado de peritos em diferentes áreas temáticas leva a discussões em nichos, enquanto que o debate em torno da controvérsia relativa à proposta da CE, salientou a necessidade de adoção de soluções sistémicas poderosas destinadas a prevenir e combater a OCSEA.

> **Recomendação 6:** As iniciativas orientadas para o diálogo transversal devem ser identificadas e apoiadas.

É de notar o peso considerável dado pelos organismos internacionais relevantes, o Tribunal Europeu dos Direitos do Homem e o Tribunal de Justiça da UE à necessidade de proteção contra crimes sexuais contra crianças, bem como à Convenção de Lanzarote e à Diretiva CSEA, ao conciliar a proteção das crianças com os direitos de proteção de dados.

Recomendação 7: A relevância que é atribuída às obrigações positivas contra a OCSEA ao abrigo do direito internacional e europeu dos direitos humanos, tendo em conta o melhor interesse da criança, necessita de uma apreciação adequada no debate legislativo que se perspetiva.

As leis ainda em evolução que regem atualmente a tecnologia de deteção automática não respondem adequadamente ao desafio de prevenir e proteger as crianças da OCSEA, assegurando ao mesmo tempo a máxima privacidade nas comunicações em linha.

Recomendação 8: Reconhecendo as atuais lacunas jurídicas, os Estados Membros do Conselho da Europa devem considerar a necessidade de adotar um quadro jurídico harmonizado e sustentável que possa proporcionar segurança jurídica aos PS e abordar futuros desenvolvimentos tecnológicos.

A análise das normas dos tratados de proteção de dados do CoE, à luz da jurisprudência do TEDH aplicável, conclui que um enquadramento jurídico específico baseado no interesse público, proporcionará a via mais sustentada para a utilização de tecnologias de tratamento automático de OCSEA, reporte voluntário relacionado e fluxos transfronteiriços de dados pessoais, e que a Convenção de Lanzarote poderia sustentar normas sobre a definição de tal interesse público comum.

Recomendação 9: Os Estados-Membros do CoE são fortemente encorajados, em conformidade com as suas obrigações positivas de proteção das crianças contra a OCSEA, a estabelecer um enquadramento baseado no interesse público fundamentado na Convenção de Lanzarote, permitindo aos PS detetar, remover, comunicar e transferir automaticamente informações relacionadas com a OCSEA sob as condições de proteção de dados e privacidade e as salvaguardas enumeradas na secção 3.4.

5. GLOSSÁRIO

IA – Inteligência Artificial.

CoE – Council of Europe / Conselho da Europa.

DL – Deep Learning / Aprendizagem profunda.

EC – Comissão Europeia.

EDPS – European Data Protection Supervisor / Autoridade Europeia para a Proteção de Dados.

EECC – European Electronic Comunication Code / Código Europeu das Comunicações Eletrónicas.

EESC – European Economic and Social Committee / Comité Económico e Social Europeu.

EOKM – Escritório de Especialização Online indermisbruik.

PE – Parlamento Europeu.

EDPB – European Data Protection Board / Conselho Europeu para a proteção de dados.

PS – Prestadores de Serviços.

EUROPOL – European Agency for Law Enforcement Cooperation / Agência da União Europeia para a Cooperação Policial.

FH – File Hashing.

HCS – Hash Check Service.

IP – Internet Protocol / Protocolo da Internet.

ICCAM – Plataforma segura chamada "I see child abuse material" que também disponibiliza tecnologias de *hashing* de imagem/vídeo/impressão digital e de rastreio.

ICSE – International Child Sexual Exploitation Data Base / Base de Dados Internacional de Imagens e Vídeos de Exploração Sexual de Crianças.

TIC – Tecnologias da Informação e da Comunicação.

CSAM – Child Sexual Abuse Material / Material de Abuso Sexual de Crianças.

CSEA – Child Sexual Exploitation and Abuse / Exploração e Abuso Sexual de Crianças.

CV – Computacional Vision / Visão Computacional.

INHOPE – International Online Operator of Europe / Associação Internacional de Linhas Diretas da Internet.

INTERPOL – International Criminal Police Organization / Organização Internacional de Polícia Criminal.

IOCTA – International Organized Crime Threath Assessment / Avaliação de Ameaças ao Crime Organizado na Internet.

IWF – Internet Watch Foundation.

CTL – Comité de Lanzarote.

CL – Convenção de Lanzarote.

LIBE – Comittee on civil liberties, Justice and Home affairs / Comissão das Liberdades Cívicas, Justiça e Assuntos Internos.

ML – Machine Learning / Aprendizagem Automática.

MVNO – Mobile Virtual Network Operator / Operador de Rede Móvel Virtual.

NCMEC – National Center for Missing and Exploited Children / Centro Nacional para Crianças Desaparecidas e Exploradas.

ONG – Organizações não governamentais.

NI-IC – Number-independent interpersonal communication / Comunicações interpessoais independentes do número.

OCSEA – Online Child Sexual Explotation and Abuse / Exploração e Abuso Sexual de Crianças Online.

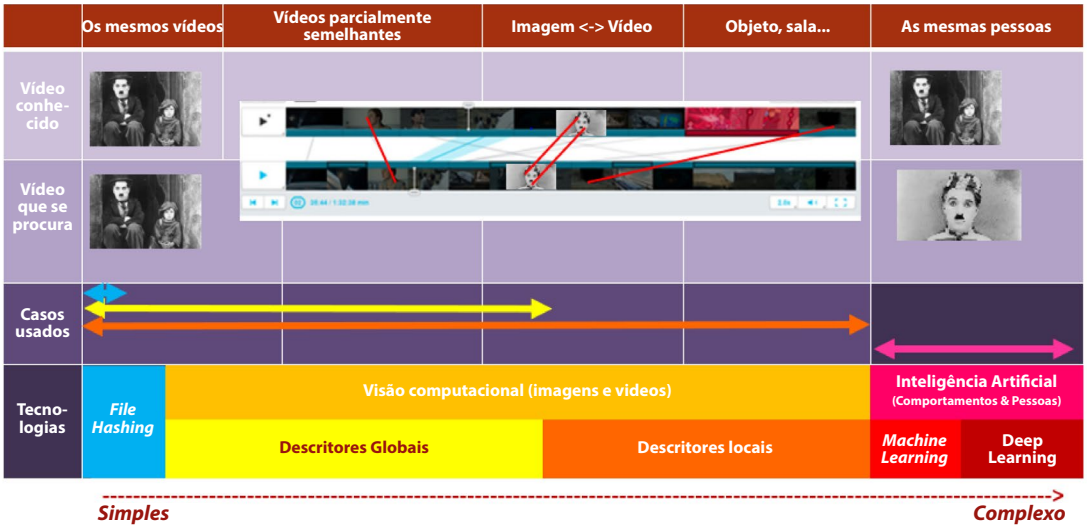
OPSC – Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography / Protocolo facultativo à CRC sobre a Venda de Crianças, Prostituição Infantil e Pornografia Infantil.

ANEXO

6. ANEXO

1. Visão geral simplificada sobre tecnologias para detetar conteúdos visuais em imagens e vídeos:

Como ler este diagrama: *File Hashing* esta tecnologia apenas se aplica para detetar o mesmo ficheiro, razão pela qual a seta azul apenas se aplica a detetar "o mesmo ou quase". Uma vez que a tecnologia de *File Hashing* não consegue detetar imagens com diferenças pequenas (mudança de 1 pixel), a seta é pequena. Os "descritores globais" aplicam-se para detetar as mesmas imagens e podem também detetar imagens com parcialmente o mesmo conteúdo. Os "descritores locais" são eficientes para detetar todos os cenários (mesmos, semelhantes, modificados, etc.). A "inteligência artificial" pode abranger muitos casos usados, mais do que o que é mostrado neste diagrama, mas é também mais complexa do que a tecnologia de visão computacional.



Como ler este diagrama: O mesmo que na secção 3. A gama de aplicação de cada uma destas tecnologias é indicativa. Além disso, a gama não é indicativa do nível de adoção. Por exemplo, o file hashing é mostrado com a gama mais pequena nesta tabela, mas na prática é muito mais amplamente utilizada do que as outras tecnologias.

1. Fontes adicionais:

• https://www.culture.gouv.fr/ ou https://bit.ly/3vWJRip - um relatório publicado em 2020 pelo Ministério da Cultura francês no contexto da Diretiva dos Direitos de Autor, estabelecendo que a visão informática é uma tecnologia madura e acessível para organizações de todas as dimensões;

• Diretrizes relativas à implementação do Protocolo Facultativo à Convenção sobre os Direitos da Criança relativo à venda de crianças, prostituição infantil e pornografia infantil, disposições específicas sobre "recolha de dados" e "prevenção":

B. Recolha de dados

20. O Comité insta os Estados Partes a desenvolverem e implementarem um mecanismo abrangente e sistemático para a recolha, análise, controlo e avaliação do impacto dos dados, bem como para a sua divulgação, sobre todas as questões abrangidas pelo Protocolo Facultativo.

É importante que a recolha de dados seja coordenada entre todos os intervenientes relevantes, incluindo o gabinete nacional de estatística e as entidades de proteção de menores, e que os dados sejam centralizados para evitar dados incoerentes ou contraditórios entre as diferentes agências estatais. O Comité recomenda, em particular, que os Estados Partes:

a) implementem uma abordagem desagregada dos dados, abordando a forma como estes delitos afetam diferentes grupos de crianças. No mínimo, os dados devem ser desagregados por sexo, idade e forma de exploração;

b) recolham dados sobre a forma como as crianças acedem e utilizam as redes digitais e sociais e o seu impacto na vida e segurança das crianças, e sobre fatores que afetam a resiliência das crianças à medida que acedem e utilizam as TIC;

c) recolher dados sobre o número de casos comunicados, acusações, condenações e sanções, de preferência incluindo a reparação fornecida às vítimas, desagregados pela natureza do crime, incluindo no que diz respeito à atividade online e offline, a categoria do perpetrador e a relação entre o perpetrador e a vítima, e o sexo e idade da criança vítima;

d) desenvolver indicadores comuns e um sistema normalizado de recolha de dados se os dados forem recolhidos a nível regional ou local (por exemplo, municípios).

21. Todos os dados devem ser recolhidos com o devido respeito pelo direito das crianças à privacidade.

C. Prevenção da venda online e da exploração sexual de crianças

37. Os Estados Partes devem prevenir e abordar a venda online, a exploração sexual e o abuso sexual de crianças através das suas medidas de implementação. Os quadros jurídicos e políticos nacionais devem ser avaliados para assegurar que cobrem adequadamente todas as manifestações da venda, exploração sexual e abuso sexual de crianças, incluindo quando estes crimes são cometidos ou facilitados através das TIC.

38. Deverão ser realizadas análises, investigações e monitorizações específicas online para melhor compreender estes crimes, e as respostas aos crimes online deverão ser desenvolvidas em estreita colaboração com as indústrias e organizações relevantes.

...

41. Considerando que o material pedo-pornográfico, como imagens e vídeos, pode circular online indefinidamente, o Comité alerta os Estados partes para o facto de a circulação contínua desse material, para além de perpetuar os danos causados às crianças vítimas, contribuir para uma perceção da criança como um objeto sexual e correr o risco de reforçar a crença entre pessoas com um interesse sexual por crianças de que é "normal", uma vez que muitos outros partilham o mesmo interesse. O Comité insta, portanto, os Estados Partes a assegurarem que os prestadores de serviços da Internet controlem, bloqueiem e removam esse conteúdo o mais rapidamente possível, como parte das suas medidas de prevenção.

42. O Comité chama a atenção dos Estados Partes para a necessidade de abordar o "sexting" por crianças, através do qual o conteúdo sexual auto-gerado é enviado através do telemóvel para outros. O sexting parece frequentemente ser um produto da pressão dos pares jovens e, em certa medida, os adolescentes consideram cada vez mais que o sexting é "normal". Embora esta conduta em si mesma não seja necessariamente ilegal ou injusta, envolve uma série de riscos. As imagens sexualizadas de crianças podem facilmente propagar-se online ou offline para além ou contra a vontade da criança, podem ser muito difíceis de remover e podem ser utilizadas no contexto de bullying e para extorsão sexual, o que pode ter consequências graves e traumatizantes para as crianças, incluindo o suicídio. Esta questão complexa requer uma atenção cuidadosa, e o Comité encoraja os Estados Partes a estabelecerem quadros legais claros que protejam as crianças e, através de esforços de prevenção, assegurem que elas sejam educadas e sensibilizadas para a gravidade da divulgação de imagens dos outros e de si próprias.

• A Recomendação sobre Ambiente Digital (CM/Rec(2018)7, Par. 51 - 66) inclui as seguintes "medidas relativas ao material sobre abuso sexual de crianças":

Medidas relativas ao material sobre abuso sexual de crianças

61. O policiamento relativo ao material sobre abuso sexual de crianças deve ser focado nas vítimas, sendo dada a máxima prioridade à identificação, localização, proteção e prestação de serviços de reabilitação à criança retratada em tais materiais.

62. Os Estados deveriam controlar continuamente se e como os materiais sobre abuso sexual de crianças são alojados dentro da sua jurisdição e exigir que as autoridades responsáveis pela aplicação da lei estabeleçam bases de dados de "hashes", com vista a acelerar as ações de identificação e localização de crianças sujeitas a exploração ou abuso sexual e de detenção dos perpetradores.

63. Os Estados devem colaborar com as empresas para prestar assistência, incluindo, se necessário, apoio técnico e equipamento, às autoridades responsáveis pela aplicação da lei para apoiar a identificação dos perpetradores de crimes contra crianças e recolher as provas necessárias para os processos penais.

64. Conscientes das tecnologias disponíveis e sem prejuízo dos princípios de responsabilidade dos intermediários da Internet e da sua isenção das obrigações gerais de controlo, os Estados deverão exigir às empresas que tomem medidas razoáveis, proporcionais e eficazes para assegurar que as suas redes ou serviços em linha não sejam indevidamente utilizados para fins criminosos ou outros fins ilícitos, de modo a não prejudicar as crianças, por exemplo, em relação à produção, distribuição, fornecimento de acesso, publicidade ou armazenamento de material pedo-pornográfico ou outras formas de abuso sexual de crianças online.

65. Os Estados devem exigir que as empresas comerciais relevantes apliquem listas de *hash* com vista a garantir que as suas redes não estão a ser utilizadas abusivamente para armazenar ou distribuir imagens de abuso sexual de crianças.

66. Os Estados devem exigir que as empresas e outras partes interessadas relevantes tomem prontamente todas as medidas necessárias para assegurar a disponibilidade de metadados relativos a qualquer material sobre exploração e abuso sexual de crianças encontrado em servidores locais, os disponibilizem às autoridades responsáveis pela aplicação da lei, removam esses materiais e, enquanto se aguarda a sua remoção, restrinjam o acesso a tais materiais encontrados em servidores fora da sua jurisdição.

I **Nota explicativa:** foi, entretanto, publicado o Regulamento (UE) 2021/1232 do Parlamento Europeu e do Conselho de 14 de julho de 2021, relativo a uma derrogação temporária de determinadas disposições da Diretiva 2002/58/CE no que respeita à utilização de tecnologias por prestadores de serviços de comunicações interpessoais independentes do número para o tratamento de dados pessoais e outros para efeitos de combate ao abuso sexual de crianças em linha, disponível em
https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32021R1232
qid=1627664571631

II **Nota explicativa:** refere-se à possibilidade que consta do RGDP no âmbito da transferência de dados que passa pela adesão por parte do destinatário além fronteiras de adesão a um código de conduta ou a um procedimento de certificação, acompanhado de compromissos vinculativos assumidos pelos destinatários dos dados, no sentido de aplicarem as garantias adequadas para proteger os dados transferidos. Como exemplo os "certificados de idoneidade" - conceito largamente utilizado no sistema bancário.

III **Nota explicativa:** No que concerne à transferência de dados e à sua devolução, esta situação respeita às obrigações que incumbem aos destinatários dos dados no estrangeiro, após terminado o tratamento de dados. As partes podem, nomeadamente acordar que, uma vez terminados estes serviços, o importador de dados e o subcontratante ulterior devem devolver (ou destruir, caso seja solicitado) todos os dados pessoais transferidos, exceto se a legislação imposta ao importador de dados o impedir.

Imagem da capa: https://br.freepik.com/fotos/fundo'>Fundo foto criado por kjpargeter / Edição CIC / DGPJ: https://dgpj.justica.gov.pt/

DGPJ DIREÇÃO-GERAL DA POLÍTICA DE JUSTIÇA

REPÚBLICA PORTUGUESA
JUSTIÇA