TELLES

Nota Informativa

9 MAIO 2024

Digital, Privacidade e Cibersegurança

UE adota primeiro ato legislativo para combater a violência online contra as mulheres

No dia 07 de maio de 2024, o Conselho da União Europeia (UE) aprovou a primeira diretiva para a prevenção e combate eficaz da violência contra as mulheres e da violência doméstica em toda a União. Esta diretiva prevê, nomeadamente

a. a criminalização de práticas relativas à exploração sexual de mulheres e crianças e comportamentos que constituam crimes informáticos – como, a mutilação genital feminina, o casamento forçado, a partilha não consensual de imagens ou vídeos íntimos ou a sua manipulação, a ciberperseguição, o ciberassédio, o incitamento à violência e ao ódio em linha;
b. a aplicação de penas de prisão de, pelo menos, um a cinco anos para essas infrações;
c. a definição de circunstâncias agravantes, nomeadamente a infração ter sido cometida contra uma criança ou na sua presença, contra o atual ou ex-cônjuge/parceiro, para punir a vítima pela sua orientação sexual, género, cor, religião, origem social ou convicções políticas, entre outras;
d. regras sobre as medidas de assistência e proteção a ser prestadas às vítimas;
e. mecanismos de denúncia através de canais acessíveis, fáceis de utilizar, seguros e prontamente disponíveis;
f. a possibilidade de fazer denúncias online ou através de outras Tecnologias da Informação e da Comunicação (“TIC”) acessíveis e seguras;
g. a garantia de que os elementos de prova relativos ao comportamento sexual passado da vítima só sejam permitidos em processo penal quando forem pertinentes e necessários, de modo a proteger a privacidade da vítima e evitar a vitimização repetida.

A partilha não consensual de imagens ou vídeos íntimos e a sua manipulação, bem como a ciberperseguição, o ciberassédio e o incitamento à violência e ao ódio online, vão passar a ser crimes. Os Estados-Membros têm três anos para transpor a diretiva.

A presente diretiva prevê regras mínimas apenas para as formas mais graves de ciberviolência, pelo que os crimes aí definidos limitam-se a comportamentos suscetíveis de causar danos graves ou danos psicológicos graves à vítima, ou a comportamentos suscetíveis de a fazer recear seriamente pela sua própria segurança ou pela segurança das pessoas a cargo. Destacamos as seguintes notas:

a. **Partilha não consensual de material íntimo ou manipulado**: o crime em causa deverá abranger todo o tipo de materiais desse género, tais como imagens, fotografias e vídeos, incluindo imagens sexualizadas, clipes de áudio e clipes de vídeo;

b. **Ciberperseguição:** deverá abranger a vigilância repetida ou contínua da vítima, através das TIC, sem o seu consentimento ou autorização legal. Essa vigilância pode ocorrer através do tratamento ilícito dos dados pessoais da vítima, por exemplo através da usurpação de identidade, do roubo de palavras-passe, do pirateio dos dispositivos da vítima, da ativação secreta de software de registo das teclas pressionadas para aceder aos espaços privados da vítima, da instalação de aplicações de geolocalização (incluindo o *stalkerware*), do roubo dos dispositivos da vítima ou através de dispositivos tecnológicos ligados através da Internet, como os eletrodomésticos inteligentes. Excecionam-se as situações em que a vigilância seja efetuada por razões legítimas, por exemplo, no contexto da monitorização, pelos pais, do paradeiro dos filhos e da sua atividade *online*;

c. **Ciberassédio**: deverá ser abrangida a prática repetida ou continuada de comportamentos ameaçadores contra uma pessoa, pelo menos quando tais comportamentos envolvam ameaças, através das TIC, da prática de crimes e quando tais comportamentos sejam suscetíveis de fazer com que a pessoa em causa receie seriamente pela sua própria segurança ou pela segurança de pessoas a cargo;

d. **Incitamento à violência ou ao ódio em linha**: pressupõe que o incitamento não seja expresso num contexto puramente privado, mas sim publicamente através da utilização das TIC. Por conseguinte, deve exigir a disseminação ao público, o que deverá ser entendido como implicando a disponibilização a um número potencialmente ilimitado de pessoas, ou seja, tornando o material facilmente acessível aos utilizadores em geral, sem exigir nova intervenção da pessoa que disponibilizou o material, independentemente de essas pessoas acederem efetivamente à informação em causa. Ao avaliar se o material pode ser considerado um incitamento ao ódio ou à violência, as autoridades competentes deverão ter em conta o direito fundamental à liberdade de expressão.

Os Estados-Membros têm três anos, após a entrada em vigor da diretiva, para a transpor para o direito nacional.
Este diploma revela a especial preocupação da UE em combater o crescimento da ciberviolência, em que a violência está intrinsecamente ligada à utilização das TIC, permitindo essas tecnologias amplificar consideravelmente a gravidade do impacto nocivo do crime, atendendo à facilidade da sua difusão,

rapidez e alcance, com o risco manifesto de criação ou intensificação de danos profundos e duradouros para a vítima.
A presente diretiva cria um regime jurídico mínimo, relativamente a estas matérias, permitindo aos Estados-Membros adotar ou manter regras penais mais rigorosas.

Contactos

Pedro Vidigal Monteiro
Sócio
p.vidigalmonteiro@telles.pt

Ana Ferreira Neves
Of Counsel
a.neves@telles.pt