



Warszawa, 20-08-2026 r.

RZECZNIK PRAW OBYWATELSKICH

Sylvia Gregorczyk-Abram

II.501.8.2025.DC

**Pan
Waldemar Żurek
Minister Sprawiedliwości – Prokurator
Generalny
/ePUAP/**

**Pani
Katarzyna Kotula
Sekretarz Stanu w Kancelarii Prezesa
Rady Ministrów
Pełnomocniczka Rządu do Spraw
Równości
/ePUAP/**

**Szanowny Panie Ministrze,
Szanowna Pani Minister,**

w dniu 27 czerwca 2027 r. upływa termin implementacji dyrektywy Parlamentu Europejskiego i Rady 2024/1385 w sprawie zwalczania przemocy wobec kobiet i przemocy domowej¹. Dyrektywa ta zakłada z jednej strony odpowiednie kształtowanie polityki społecznej (wsparcie dla osób doświadczających przemocy motywowanej płcią, gromadzenie danych, zmiana praktyki działania poszczególnych organów), a z drugiej – wprowadzenie mechanizmów prawnokarnych pozwalających efektywnie zwalczać

¹ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/1385 z dnia 14 maja 2024 r. w sprawie zwalczania przemocy wobec kobiet i przemocy domowej (Dz. U. UE. L. z 2024 r. poz. 1385); dalej: dyrektywa 2024/1385.

przemoc domową i przemoc wobec kobiet. Analizując całość przepisów, można wskazać na pięć celów, jakie prawodawca unijny chciałby osiągnąć przyjmując ww. dyrektywę:

1. wprowadzenie minimalnych standardów kryminalizacji wybranych zachowań (w tym przemocy w cyberprzestrzeni) i określenie minimalnych wymogów co do sankcji oraz okoliczności obciążających;
2. wzmocnienie ochrony osób pokrzywdzonych i dostępu do wymiaru sprawiedliwości, w tym wypracowanie standardów postępowania w sprawach o przestępstwa motywowane płcią, środków ochrony pokrzywdzonych oraz ograniczenia wtórnej wiktymizacji;
3. zapewnienie wsparcia osobom pokrzywdzonym także poza postępowaniem karnym;
4. rozwój prewencji, koordynacji i współpracy instytucjonalnej, współpracy z organizacjami pozarządowymi, w tym obowiązków szkoleniowych dla organów wymiaru sprawiedliwości;
5. sprawozdawczość w zakresie monitorowania zjawiska przemocy motywowanej płcią.

Zadań i wyzwań, jakie stoją przed krajowym ustawodawcą, a zwłaszcza Ministerstwem Sprawiedliwości, jest wiele. Wydaje się, że podstawowym problemem, jaki wiąże się z implementacją dyrektywy 2024/1385, jest stworzenie adekwatnych ram prawnokarnych – zarówno w sferze prawa materialnego, jak i procesowego – tak, aby możliwe było zapewnienie osobom pokrzywdzonym odpowiedniego wsparcia, rozwijanie prewencji i koordynacji działań zwalczających przemoc motywowaną płcią, a także zrealizowanie obowiązków związanych ze sprawozdawczością. Bez zmian ustawodawczych, zwłaszcza w k.k.² i k.p.k.³ nie będzie możliwe całościowe, kompletne i prawidłowe wdrożenie przepisów unijnych.

1. Dyrektywa 2024/1385 i jej zakres materialnoprawny

Przepisy art. 3-8 dyrektywy 2024/1385 wprowadzają minimalny standard kryminalizacji zachowań (przestępstw). Państwa członkowskie UE powinny zapewnić, by wskazane w dyrektywie zachowania podlegały efektywnym, proporcjonalnym i odstraszającym sankcjom karnym (art. 10 dyrektywy 2024/1385). Minimalne wymogi w sferze prawa karnego materialnego, tj. kryminalizacji określonych zachowań, dotyczą:

² Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2025 r. poz. 383 z późn. zm.).

³ Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2025 r. poz. 383 z późn. zm.).

- **penalizacji okaleczania żeńskich narządów płciowych** (art. 3, female genital mutilation)⁴ – wycięcie, infibulacja lub każde inne okaleczenie całości lub którejkolwiek części warg sromowych większych, warg sromowych mniejszych lub łechtaczki oraz zmuszanie lub doprowadzenie kobiety lub dziewczynki do poddania się któremukolwiek z wcześniej wymienionych działań. Maksymalny wymiar kary powinien wynosić co najmniej 5 lat pozbawienia wolności (art. 10 ust. 2);
- **przymusowe małżeństwa**⁵ (art. 4) - zmuszanie osoby dorosłej lub dziecka do zawarcia małżeństwa, a także zwabienie osoby dorosłej lub dziecka na terytorium państwa innego niż to, w którym zamieszkuje, w celu zmuszenia tej osoby dorosłej lub tego dziecka do zawarcia małżeństwa. Maksymalny wymiar kary powinien wynosić co najmniej 3 lata pozbawienia wolności (art. 10 ust. 3);
- **udostępnianie bez zgody treści intymnych lub zmanipulowanych**⁶ (art. 5) – publiczne udostępnianie za pomocą technologii informacyjno-komunikacyjnych obrazów, nagrań lub podobnych materiałów przedstawiających czynności o wyraźnie seksualnym charakterze lub intymne części ciała osoby bez zgody tej osoby, gdy takie czyny mogą wyrządzić poważną szkodę tej osobie; wytwarzanie obrazów, nagrań wideo lub podobnych treści, które sprawiają wrażenie, że osoba uczestniczy w czynnościach o wyraźnie seksualnym charakterze, manipulowanie takimi obrazami, nagraniami wideo lub innymi treściami lub zmienianie ich, a następnie publiczne udostępnianie ich za pomocą technologii informacyjno-komunikacyjnych bez zgody tej osoby, gdy takie czyny mogą wyrządzić jej poważną szkodę; grożenie publicznym udostępnieniem treści intymnych lub zmanipulowanych w celu zmuszenia osoby do wykonania określonej czynności, przyzwolenia na nią lub powstrzymania się od niej (sextortion). Maksymalny wymiar kary powinien wynosić co najmniej 1 rok pozbawienia wolności (art. 10 ust. 4);

⁴ W Europie, według oficjalnych danych, jest ok. 600.000 kobiet i dziewczynek, które żyją z konsekwencjami okaleczania żeńskich narządów płciowych, a kolejne 190.000 jest zagrożone dokonaniem tej czynności w przyszłości. Zob. dane: <https://endfgm.eu/female-genital-mutilation/fgm-in-europe/> oraz informacje dostępne na stronach: <https://eige.europa.eu/gender-based-violence/female-genital-mutilation>; <https://euobserver.com/2154/an-invisible-crisis-why-female-genital-mutilation-remains-a-challenge-in-europe/>.

⁵ Europejska Agencja Praw Podstawowych dotyczący przymusowych małżeństw jest dostępny na stronie: https://fra.europa.eu/sites/default/files/fra-2014-forced-marriage-eu_en.pdf.pdf.

⁶ Między 2023 a 2025 r. liczba deepfake'ów w przestrzeni internetowej wzrosła z ok. 500.000 do 8.000.000: <https://deepstrike.io/blog/deepfake-statistics-2025>. Problemem są deepfake przedstawiające seksualne wykorzystanie osób małoletnich i wzrost tego typu treści w internecie: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI\(2025\)775855_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf).

- **cyberstalking** (art. 6) - poddawanie danej osoby powtarzającemu się lub ciągłemu nadzorowi, bez jej zgody lub upoważnienia prawnego do takiego działania, za pomocą technologii informacyjno-komunikacyjnych w celu śledzenia lub monitorowania ruchów i działań tej osoby, gdy może to wyrządzić poważną szkodę tej osobie. Maksymalny wymiar kary powinien wynosić co najmniej 1 rok pozbawienia wolności (art. 10 ust. 4);
- **cybernękanie** (art. 7) – powtarzające się lub ciągłe grożenie osobie, przynajmniej w przypadkach, gdy czyny te obejmują groźby popełnienia przestępstwa, za pomocą technologii informacyjno-komunikacyjnych, gdy takie czyny mogą spowodować, że osoba ta poważnie obawia się o swoje bezpieczeństwo lub o bezpieczeństwo osób będących na jej utrzymaniu; kierowanie, wraz z innymi osobami, za pomocą technologii informacyjno-komunikacyjnych, w publicznie dostępny sposób, gróźb lub zniewag wobec osoby, gdy takie czyny mogą wyrządzić tej osobie poważną szkodę psychiczną; przesyłanie osobie, która sobie tego nie życzy, za pomocą technologii informacyjno-komunikacyjnych obrazu, nagrania wideo lub innych podobnych treści przedstawiających genitalia, gdy takie czyny mogą wyrządzić tej osobie poważną szkodę psychiczną; publiczne udostępnianie za pomocą technologii informacyjno-komunikacyjnych treści zawierających dane osobowe osoby bez jej zgody w celu nakłonienia innych do wyrządzenia tej osobie szkody fizycznej lub poważnej szkody psychicznej. Maksymalny wymiar kary powinien wynosić co najmniej 1 rok pozbawienia wolności (art. 10 ust. 4);
- **cyfrowe nawoływanie do przemocy lub nienawiści** (art. 8) - umyślne nawoływanie do przemocy lub nienawiści skierowanej przeciwko grupie osób, którą definiuje się według płci, lub przeciwko członkowi takiej grupy przez publiczne rozpowszechnianie za pomocą technologii informacyjno-komunikacyjnych treści zawierających takie nawoływanie; państwa mogą natomiast podjąć decyzję o penalizacji takich zachowań, które mogą spowodować zakłócenie porządku publicznego lub które stanowią groźbę, obrazę albo zniewagę. Maksymalny wymiar kary powinien wynosić co najmniej 1 rok pozbawienia wolności (art. 10 ust. 4).

Podżeganie, pomocnictwo i usiłowanie zachowań penalizowanych w dyrektywie powinny także podlegać karom⁷. Termin przedawnienia zachowań wskazanych w dyrektywie powinien być odpowiednio długi, a jeśli pokrzywdzonym czynem z art. 3 dyrektywy 2024/1385 jest osoba poniżej 18 roku życia, bieg terminu przedawnienia nie może się rozpocząć wcześniej niż po osiągnięciu pełnoletności.

Dyrektywa 2024/1385 w art. 11⁸ wskazuje, jakie okoliczności popełnienia czynu powinny zostać w prawie krajowym traktowane jako okoliczności obciążające. Nie chodzi jednak o zmiany w prawie, ale przyjęcie „niezbędnych środków”, by np. ponowne popełnienie przestępstwa, czy popełnienie przestępstwa przeciw byłemu lub obecnemu małżonkowi lub partnerowi było surowiej karane. Przepisy unijne odnoszą się także do kwestii jurysdykcji (art. 12). Państwa członkowskie powinny wprowadzić jurysdykcję terytorialną (gdy czyn popełniono w całości lub części na terytorium państwa) oraz opartą na obywatelstwie sprawcy (zasada obywatelstwa). Dyrektywa przewiduje również możliwość rozszerzenia jurysdykcji na czyny popełnione poza terytorium państwa (m.in., gdy pokrzywdzony jest obywatelem lub rezydentem państwa UE albo gdy sprawca ma zwykłe miejsce pobytu na terytorium państwa), a w odniesieniu do czynów popełnianych z użyciem technologii informacyjno-komunikacyjnych nakazuje objęcie jurysdykcją sytuacji, w których dostęp do tych narzędzi uzyskano z terytorium państwa, niezależnie od siedziby dostawcy usług pośrednich. Ponadto, jeśli sprawcą

⁷ Art. 9. 1. Państwa członkowskie zapewniają, aby podżeganie do popełnienia któregośkolwiek z przestępstw, o których mowa w art. 3-6 i art. 7 akapit pierwszy lit. b), podlegało karze jako przestępstwo. 2. Państwa członkowskie zapewniają, aby pomocnictwo w popełnieniu któregośkolwiek z przestępstw, o których mowa w art. 3 akapit pierwszy lit. a) i art. 4-8, podlegało karze jako przestępstwo. 3. Państwa członkowskie zapewniają, aby usiłowanie popełnienia przestępstw, o których mowa w art. 3 i 4, podlegało karze jako przestępstwo.

⁸ Okoliczności obciążające to: a) przestępstwo - lub inne przestępstwo przemocy wobec kobiet lub przemocy domowej - zostało popełnione ponownie; b) przestępstwo zostało popełnione przeciw osobie podatnej na zagrożenia ze względu na szczególne okoliczności, takie jak sytuacja zależności lub stan niepełnosprawności fizycznej, umysłowej, intelektualnej lub sensorycznej; c) przestępstwo zostało popełnione przeciw dziecku; d) przestępstwo zostało popełnione w obecności dziecka; e) przestępstwo zostało popełnione przez co najmniej dwie osoby działające wspólnie; f) przestępstwo poprzedzały lub towarzyszyły mu ekstremalne poziomy przemocy; g) przestępstwo zostało popełnione z użyciem broni lub z groźbą jej użycia; h) przestępstwo zostało popełnione przy użyciu siły lub groźby użycia siły lub przy użyciu przymusu; i) następstwem czynu jest śmierć ofiary bądź poważną szkodę fizyczną lub psychiczną dla ofiary; j) sprawca został wcześniej skazany za przestępstwa o tym samym charakterze; k) przestępstwo zostało popełnione przeciw byłemu lub obecnemu małżonkowi lub partnerowi; l) przestępstwo zostało popełnione przez członka rodziny lub osobę wspólnie zamieszkującą z ofiarą; m) przestępstwo zostało popełnione przez nadużycie uznanego stosunku zaufania, władzy lub wpływu; n) przestępstwo zostało popełnione przeciw danej osobie, ponieważ była ona przedstawicielem publicznym, dziennikarzem lub obrońcą praw człowieka; o) celem przestępstwa było zachowanie lub przywrócenie tzw. honoru danej osoby, rodziny, wspólnoty lub innej podobnej grupy; p) celem przestępstwa było ukaranie ofiary za jej orientację seksualną, płeć, kolor skóry, religię, pochodzenie społeczne lub przekonania polityczne.

czynu z art. 3-9 dyrektywy 2024/1385 jest obywatel państwa UE, dyrektywa znosi wymóg podwójnej karalności, a także konieczność złożenia wniosku o ściganie przez pokrzywdzonego.

Dla pełnego ustalenia zakresu materialnoprawnego dyrektywy, ważne znaczenie ma także art. 24 dyrektywy 2024/1385. Zgodnie z tym przepisem, państwa członkowskie powinny zapewnić, żeby osoby pokrzywdzone mogły dochodzić odszkodowania od sprawców przemocy wobec kobiet lub przemocy domowej, a decyzja o roszczeniach cywilnych powinna móc zostać podjęta także w toku postępowania karnego.

2. Ocena koniecznych zmian w prawie karnym materialnym

Porównując przepisy dyrektywy 2024/1385 z aktualnymi regulacjami prawa karnego materialnego, znaczna część rozwiązań już istnieje w prawie krajowym.

Okaleczenie żeńskich narządów płciowych zostało wyszczególnione w wyliczeniu w art. 156 § 1 pkt 3 k.p.k.⁹. Na etapie procesu legislacyjnego, pojawiły się głosy¹⁰, że zbędne jest wyszczególnianie tej formy „ciężkiego uszczerbku na zdrowiu” i obecny zakres kryminalizacji jest wystarczający. W uzasadnieniu do projektu nowelizacji wskazano jednak, że „obserwując trudności interpretacyjne, jakie wywołuje zrozumienie przyjęcia wspomnianej kwalifikacji (mimo, iż na etapie ratyfikacji Konwencji¹¹ nie zgłaszano zastrzeżeń), dążąc do uzyskania tzw. operacyjności przepisu (jednoznaczny przekaz co do karalności, ułatwienie zbierania statystyk co do skali zjawiska w Polsce), projektodawca zdecydował się uzupełnić art. 156 § 2 k.k. o pkt 3 (art. 5 pkt 2), wyraźnie wskazując, że karalnym ciężkim uszczerbkiem na zdrowiu jest wycięcie, infibulacja lub

⁹ Ustawa z dnia 13 stycznia 2023 r. o zmianie ustawy - Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz. U. poz. 289 z późn. zm.).

¹⁰ Zob. np. Opinię Pierwszej Prezes Sądu Najwyższego, s. 18-19;

<https://orka.sejm.gov.pl/Druki9ka.nsf/0/A88C237C1AF86014C12588EC00465263/%24File/2615-004.pdf>.

¹¹ Dyrektywa 2024/1385 w sprawie zwalczania przemocy wobec kobiet i przemocy domowej jest swego rodzaju unijną odpowiedzią na Konwencję Rady Europy o zapobieganiu i zwalczaniu przemocy wobec kobiet i przemocy domowej (Konwencja Rady Europy o zapobieganiu i zwalczaniu przemocy wobec kobiet i przemocy domowej, sporządzona w Stambule dnia 11 maja 2011 r. (Dz. U. z 2015 r. poz. 961 z późn. zm.); dalej: Konwencja stambulska). Unia Europejska – jako organizacja – ratyfikowała Konwencję stambulską (Opinia 1/19: Wniosek o opinię przedstawiony przez Parlament Europejski w trybie art. 218 ust. 11 TFUE (Dz. U. UE. C. z 2019 r. Nr 413, str. 19/1). UE ratyfikowała Konwencję 1.06.2023 r., a Konwencja obowiązuje w UE od 1.10.2023 r.), ale – z uwagi na specyfikę prawa międzynarodowego i prawa unijnego – celowe było wprowadzenie częściowo odrębnej regulacji unijnej.

inne trwałe i istotne okaleczenie żeńskiego narządu płciowego”¹². Okaleczanie żeńskich narządów płciowych jest zagrożone karą od 3 do 20 lat pozbawienia wolności. Nakłanianie do czynu z art. 156 § 1 pkt 3 k.k. również jest penalizowane. Przepis art. 156a k.k. wprowadza karalność nakłaniania do okaleczenia żeńskich narządów płciowych (§ 1), zaś czyn ten jest zagrożony karą do 3 lat pozbawienia wolności. Zmuszanie groźbą bezprawną lub przemocą do poddania się czynnościom z art. 156 § 1 pkt 3 k.k. jest także penalizowane (art. 156a § 2 k.k.), a zagrożenie karą wynosi od 3 miesięcy do 5 lat. Przedawnienie karalności czynów z art. 156 § 1 pkt 3 k.k. i art. 156a k.k., jeśli pokrzywdzonym była osoba małoletnia, nie może nastąpić przed ukończeniem przez nią 18 roku życia (art. 101 § 4 k.k.).

Przepis penalizujący przymusowe małżeństwa – art. 191b k.k. – został dodany ustawą z dnia 13 stycznia 2023 r. o zmianie ustawy - Kodeks postępowania cywilnego oraz niektórych innych ustaw¹³, której celem było m.in. implementowanie Konwencji stambulskiej. Zagrożenie karą przewidziane przez krajowego ustawodawcę mieści się w granicach wyznaczonych przez dyrektywę 2024/1385. Czyn jest zagrożony karą od 3 miesięcy do 5 lat pozbawienia wolności.

Problem implementacyjny – a w zasadzie luki implementacyjne – dotyczą przede wszystkim art. 5–8 dyrektywy. Ta część karnomaterialna dyrektywy dotyczy przemocy z użyciem technologii informacyjno-komunikacyjnych oraz problematyki jurysdykcji dla przestępstw transgranicznych i cyberprzemocy¹⁴.

Pierwszy problem implementacyjny dotyczy art. 5 dyrektywy 2024/1385, czyli udostępniania bez zgody treści intymnych.

Przepis art. 191a § 1 k.k. penalizuje rozpowszechnianie bez zgody „wizerunku nagiej osoby” lub „wizerunku osoby w trakcie czynności seksualnej”. W doktrynie wskazuje się, że „musi dojść do utrwalenia lub rozpowszechnienia wizerunku twarzy osoby w powiązaniu z innymi elementami jej nagiego ciała lub twarzy osoby wraz z obrazem wskazującym na jej uczestnictwo w czynności seksualnej, choć niekoniecznie łączącym

¹² Uzasadnienie projektu ustawy o zmianie ustawy Kodeks postępowania cywilnego i niektórych innych ustaw, druk sejmowy Sejmu IX kadencji nr 2615, s. 41;

<https://orka.sejm.gov.pl/Druki9ka.nsf/0/F1043B204059F77DC12588C40032E67A/%24File/2615.pdf>.

¹³ Ustawa z dnia 13 stycznia 2023 r. o zmianie ustawy - Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz. U. poz. 289 z późn. zm.).

¹⁴ O cyfrowej przemocy wobec kobiet zob.: M. Lesińska-Staszczuk, *Cyberviolence against Women*, St. Iur.Lubl. 2025, nr 4, s. 117-130.

się z jej nagością”¹⁵. Jeśli wizerunek twarzy jest niewyraźny albo zdjęcie przedstawia wyłącznie nagie części ciała, to taka sytuacja wprost nie mieści się w zakresie przestępstwa z art. 191a § 1 k.k. W doktrynie wskazuje się, że pod pojęciem „wizerunek” mieszczą się także fotografie, nagrania, filmy, itp., które przedstawiają cechy osoby, pozwalające na jej jednoznaczną identyfikację¹⁶. Chodzi np. o specyficzne tatuaże, pozwalające na zidentyfikowanie osoby, blizny, czy znamiona¹⁷. Na podstawie obecnie obowiązujących przepisów, ważne jest jednak to, by „wizerunek” był rozpoznawalny w sposób pozwalający na identyfikację osoby przez szerszy krąg odbiorców, nie tylko przez pokrzywdzonego (obiektywne kryterium rozpoznawalności)¹⁸.

Przepis art. 5 dyrektywy 2024/1385 wprowadza jednak obowiązek kryminalizacji nie tylko ujawnienia „wizerunku”, ale wystarczające jest ujawnienie/rozpowszechnienie materiałów zawierających intymne części ciała danej osoby lub o wyraźnie seksualnym charakterze bez zgody tej osoby. Dyrektywa wprowadza jednak warunek w postaci możliwości wyrządzenia „poważnej szkody” osobie, której zdjęcia intymne zostały udostępnione. Przykładowo może chodzić o utratę zaufania niezbędnego do sprawowania określonej funkcji, czy ośmieszenie określonej osoby w przestrzeni publicznej.

Druga luka implementacyjna, w kontekście art. 5 dyrektywy 2024/1385, dotyczy treści zmanipulowanych, w tym deepfake o charakterze seksualnym.

W rozporządzeniu UE 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji¹⁹ deepfake jest definiowany jako „wygenerowane przez AI lub zmanipulowane przez AI obrazy, treści dźwiękowe lub treści wideo, które przypominają istniejące osoby, przedmioty, miejsca,

¹⁵ R. Krajewski, *Przestępstwo utrwalania i rozpowszechniania wizerunku nagej osoby lub osoby w trakcie czynności seksualnej*, Prok.i Pr. 2012, nr 5, s. 20-40. Zob. również: M. Kowalewska-Łukuć, *Rozpowszechnianie wizerunku nagej osoby lub osoby w trakcie czynności seksualnej bez jej zgody – rozważania o zakresie kryminalizacji*, Pr. w Dział. 2025, nr 61, s. 35-53.

¹⁶ Odmienne: J. Lachowski [w:] *Kodeks karny. Komentarz*, wyd. IV, red. V. Konarska-Wrzošek, Warszawa 2023, art. 191(a). Zob. jednak: K. Lipiński [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa 2021, art. 191(a); J. Kosonoga-Zygmunt [w:] *Kodeks karny. Komentarz*, red. J. Majewski, Warszawa 2024, art. 191(a).

¹⁷ K. Wala [w:] *Kodeks karny. Komentarz*, red. J. Kulesza, Warszawa 2025, art. 191(a).

¹⁸ R. Krajewski, *Przestępstwo utrwalania i rozpowszechniania wizerunku nagej osoby lub osoby w trakcie czynności seksualnej*, Prok.i Pr. 2012, nr 5, s. 20-40.

¹⁹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji). Tekst mający znaczenie dla EOG (Dz. U. UE. L. z 2024 r. poz. 1689).

podmioty lub zdarzenia, które odbiorca mógłby niesłusznie uznać za autentyczne lub prawdziwe” (art. 3 pkt 60). Obecnie obowiązujące przepisy, w odniesieniu do treści zmanipulowanych, kryminalizują takie zachowania wyłącznie, jeśli przedstawiają one dziecko (osobę poniżej 18 roku życia). Przepis art. 202 § 4b k.k. zabrania „produkowania, rozpowszechniania, prezentowania, przechowywania lub posiadania treści pornograficznych przedstawiających wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej”. Ustawodawca posługuje się pojęciami „wytworzony albo przetworzony” wizerunek małoletniego, co pozwala uwzględnić także treści przerobione za pomocą narzędzi sztucznej inteligencji²⁰.

Krajowe przepisy nie chronią jednak materiałów typu deep fake, które przedstawiają osobę dorosłą, której wizerunek – twarz – została przetworzona i wykorzystana²¹. Problemem są nie tylko tzw. revenge porn – czyli filmy, zdjęcia, nagrania, itp., przedstawiające osoby w trakcie czynności seksualnych, gdzie np. twarz została „doklejona” do ciała/sceny z filmu pornograficznego – ale także wykorzystanie wizerunku danej osoby, jej głosu i wytworzenie filmu/rolki na mediach społecznościowych, w sytuacji, gdy materiał zawiera wyraźny kontekst seksualny. **Obecnie osoba dorosła (powyżej 18 roku życia), której twarz wykorzystano i wklejono do filmu o charakterze pornograficznym, materiałów o wyraźnie seksualnym charakterze, pozostaje poza zakresem prawnokarnej ochrony²².**

Trzeci problem implementacyjny w zakresie art. 5 dyrektywy 2024/1385 dotyczy tzw. sextortion²³, czyli grożenia ujawnieniem treści intymnych w celu zmuszenia

²⁰ Zob. szerzej: P. Zakrzewski [w:] *Kodeks karny. Komentarz*, red. J. Majewski, Warszawa 2024, art. 202. Zob. także: M. Łabuz, M. Małecki, K. Mika-Łabuz, *Dziecięca pornografia w formie deep fakes – problemy wykładni na gruncie polskiego prawa karnego i propozycje legislacyjne*, Pr. w Dział. 2025, nr 61, s. 54-84. Zob. także: P. Dolniak, M. Iwański, T. Kuźma, A. Ludwiński, P. Sotowski, K. Wasik, *Fałszywe obrazy, rzeczywiste krzywdy. Deepfake jako forma wykorzystania seksualnego dzieci – prawo polskie na tle unormowań międzynarodowych i unijnych*, PiP 2025, nr 10, s. 101-120.

²¹ Na ten problem zwracał także uwagę Prezes UODO w wystąpieniu generalnym z dnia 5 sierpnia 2026 r., znak sprawy: DPNT.413.4.2026.WI.ER.

²² Może ona próbować dochodzić obrony swoich praw np. na podstawie przepisów art. 212 i 216 k.k., ale konieczne byłoby wykazanie, że doszło do zniesławienia, tj., że filmik miał obraźliwy charakter i mógł narazić na utratę zaufania niezbędnego do pełnionej funkcji. Zob. szerzej: M. Głuchowski, *Karałość tworzenia i rozpowszechniania fałszywych treści pornograficznych deepfake*, Cz. PKiNP 2023, nr 4, s. 5-38.

²³ Zob. m.in.: K. Staciwa, *Nowe formy przestępczości przeciwko dzieciom. Seksualne zmuszanie i wymuszenie online*, [w:] *Badania kryminologiczne a praktyka. Perspektywa krajowa i międzynarodowa*, red. D. Dajnowicz-Piesiecka, E. Jurgielewicz-Delegacz, E. W. Pływaczewski, Warszawa 2021.

osoby do wykonania określonej czynności, przyzwolenia na nią lub powstrzymania się od niej²⁴.

Obecnie, przepisy chronią częściowo przed tego rodzaju zachowaniem. Można bowiem poszukiwać prawnokarnej ochrony korzystając z konstrukcji groźby karalnej (art. 190 k.k.²⁵) albo zmuszenia do określonego zachowania (art. 191 § 1 k.k.²⁶). Przepisy wymagają jednak by „grożono popełnieniem przestępstwa na szkodę tej osoby” albo stosowaniem przemocy. Groźenie udostępnieniem zdjęć, fotografii przedstawiających nagi wizerunek danej osoby albo wizerunek w trakcie czynności seksualnej będzie mieściło się w znamionach czynu z art. 191a k.k. Podobnie w przypadku groźenia udostępnieniem zdjęć, filmów – rzeczywistych, przerobionych lub wytworzonych – przedstawiających osoby poniżej 18 roku życia (art. 202 § 4b k.k.). **Poza zakresem ochrony znajdują się jednak deepfake przedstawiające osoby dorosłe²⁷.** Udostępnianie materiałów zmanipulowanych o charakterze seksualnym obecnie nie mieści się w zakresie żadnego czynu zabronionego, a zatem groźenie takich zachowaniem nie będzie realizowało znamion czynów z art. 190 § 1 k.k. ani z art. 191 § 1 k.k.

Już poza zakresem dyrektywy, rozważenia wymagałoby wprowadzenie odrębnego typu czynu zabronionego, ściganego z urzędu, który obejmowałby swoim zakresem zachowania polegające na gromadzeniu i rozpowszechnianiu (udostępnianiu) zbiorów big data przedstawiających nagi wizerunek, zdjęcia/nagrania miejsc intymnych, itp., bez zgody osób znajdujących się na tych materiałach. W mediach głośne były sprawy platform internetowych, np. w Polsce – sprawa platformy zbiornik.pl, analogiczna strona działała m.in. we Włoszech²⁸, a Policja tłumaczyła, że nie może rozpocząć formalnie postępowania karnego z uwagi na brak wniosku o ściganie czynu z art. 191a k.k.²⁹. Prezes UODO złożył zawiadomienie o możliwości popełnienia przestępstwa

²⁴ Zob. także kampanię policyjną: <https://cieszyn.policja.gov.pl/ka6/prewencja/akcje-i-kampanie-s/pro/339375,Sextortion-uwazaj-bo-YouMayBeNext-TyMozeszBycNastepny.html>.

²⁵ Przepis brzmi: „Kto grozi innej osobie popełnieniem przestępstwa na jej szkodę lub na szkodę osoby dla niej najbliższej, jeżeli groźba wzbudza w osobie, do której została skierowana lub której dotyczy, uzasadnioną obawę, że będzie spełniona, podlega karze pozbawienia wolności do lat 3.”.

²⁶ Przepis brzmi: „Kto, stosując przemoc wobec osoby lub groźbą bezprawną, zmusza ją lub inną osobę do określonego działania, zaniechania lub znoszenia, podlega karze pozbawienia wolności do lat 3.”.

²⁷ Zob. także: K. Pawluczenia, *Aspekty prawne dotyczące pojęcia deepfake w AI Act – uwagi de lege ferenda wobec wyzwań współczesności*, PPH 2026, nr 2, s. 32-36.

²⁸ Strona phica.eu – strona finalnie została zdjęta, strona zbiornik.pl nadal działa.

²⁹ Zob.: <https://wiadomosci.wp.pl/pokaze-zonke-kto-oceni-tysiace-zdjec-nagich-polek-bez-ich-zgody-w-internecie-7204003184634624a>.

przetwarzania danych osobowych – wizerunku – bez zgody danej osoby³⁰. **Obecne ramy prawne są nieefektywne nie tylko z uwagi na tryb ścigania przestępstwa z art. 191a k.k., ale przede wszystkim dlatego, że brak jest przepisów, które penalizowałyby tworzenie baz danych zawierających znaczną liczbę filmów, czy zdjęć typu deep fake, przedstawiających osoby dorosłe.**

Kwestia cyberstalkingu (art. 6 dyrektywy 2024/1385) w kontekście krajowych regulacji jest problematyczna. Z regulacji unijnych wynika konieczność kryminalizacji powtarzającego się lub ciągłego nadzoru osoby, bez jej zgody, za pomocą technologii informacyjno-komunikacyjnych, w celu śledzenia lub monitorowania ruchów i działań, gdy może to wyrządzić jej poważną szkodę. Chodzi np. o instalowanie nadajników GPS, posługiwanie się lokalizatorami (np. AirTagami), instalowanie programów monitorujących aktywność w internecie, itp. Częściowo takie zachowania mieszczą się w zakresie art. 267 § 3 k.k. W orzecznictwie wskazuje się, że „Bezprawne zainstalowanie w cudzym pojeździe urządzenia służącego do pozyskiwania informacji o trasie jazdy i tym samym o miejscu przebywania danej osoby jest niedozwolone i stanowi czyn zabroniony, o którym mowa w art. 267 § 3 k.k.”³¹. Analogicznie, w przypadku np. podrzucenia AirTag’a do torebki nieznanej osoby, by śledzić jej lokalizację, będzie to wypełniało znamiona czynu z art. 267 § 3 k.k.³². Osoby postronne, nawet znajome, nie są uprawnione do ciągłej i stałej informacji o miejscu przebywania kobiety, czy mężczyzny. Pojawia się pytanie, czy nie byłoby zasadne wyróżnienie odrębnego typu czynu zabronionego, wprost opartego na art. 6 dyrektywy 2024/1385. W przypadku czynu z art. 267 § 3 k.k. chronione są poszczególne informacje: lokalizacja, dane osobowe, treść komunikatów wymienianych pomiędzy poszczególnymi osobami. Dyrektywa w art. 6 kładzie jednak nacisk nie tyle na ochronę informacji, co na bezpieczeństwo jednostki i ochronę przed niechcianą kontrolą. W motywie nr 21 wskazano: „Przestępstwo cyberstalkingu powinno obejmować powtarzający się lub stały nadzór nad ofiarą za pomocą technologii informacyjno-komunikacyjnych bez jej zgody lub upoważnienia prawnego. Do takiego nadzoru może dochodzić w wyniku przetwarzania danych osobowych ofiary, np. przez kradzież

³⁰ Zob. informacje: <https://uodo.gov.pl/pl/138/3906>; <https://legalis.pl/wizerunek-w-sieci-a-odpowiedzialnosc-karna/>. W mediach dotychczas nie było informacji odnośnie do losów tego zawiadomienia.

³¹ Postanowienie SN z 27.11.2019 r., V KK 505/18, LEX nr 2966120.

³² Zob. np. sprawę opisywaną tutaj: <https://krakow.wyborcza.pl/krakow/7,44425,32211533,maria-ktos-wrzucil-mi-do-torebki-apple-airtag-policja-nawet.html>.

tożsamości³³, kradzież haseł³⁴, zhakowanie urządzeń ofiary³⁵, zainstalowanie bez jej wiedzy oprogramowania do przechwytywania naciśnięć klawiszy³⁶, aby uzyskać dostęp do przestrzeni prywatnej ofiary, przez zainstalowanie aplikacji do geolokalizacji, w tym aplikacji typu stalkerware³⁷, lub w wyniku kradzieży urządzeń ofiary³⁸. Ponadto przestępstwo cyberstalkingu powinno obejmować monitorowanie ofiary bez jej zgody lub bez upoważnienia przy użyciu urządzeń technologicznych podłączonych do internetu rzeczy takich jak inteligentne urządzenia gospodarstwa domowego.”. Cybernękane np. przy użyciu inteligentnych urządzeń gospodarstwa domowego (np. Alexy, czy Siri) może także realizować znamiona czynu z art. 207 § 1 k.k., jeśli działanie takie podejmowane jest przez obecnego partnera i to z jego konta (np. Apple) urządzenie jest sterowane. Konieczne byłoby jednak posłużenie się konstrukcją znęcania się psychicznego i szeroka interpretacja tego pojęcia.

Większość zachowań, jakie zostały wskazane w art. 6 dyrektywy 2024/1385 jest obecnie kryminalizowana w polskim prawie karnym – zwłaszcza w art. 267 § 1 i 3 k.k., czy art. 190a § 2 k.k. **Brakuje natomiast przepisu, które charakteryzowałyby szczególny cel działania sprawcy cybernękania, jakim jest wzbudzenie poczucia zagrożenia, kontroli i obserwowania określonej osoby. Dodatkowo, kryminalizacja cybernękania jest dość rozproszona i następuje głównie w wyniku nadawania dotychczas znanym pojęciom nowych – bardziej cyfrowych i uwzględniających rozwój technologii znaczeń.** O ile w przypadku bardziej klasycznych form cybernękania – np. za pomocą technologii spywerek, czy urządzeń lokalizacyjnych – zachowania sprawcy realizują znamiona jednego z czynów zabronionych w k.k., o tyle w przypadku cybernękania za pomocą inteligentnych urządzeń w relacjach partnerskich, krajowe przepisy niekoniecznie pozwalają na ściganie tych zachowań. Jediną możliwością jest wykorzystanie instytucji z art. 207 § 1 k.k., natomiast problematyczna jest kwestia adekwatności tego przepisu do formy przemocy, o której mowa w art. 6 dyrektywy 2024/1385.

³³ Art. 190a § 2 k.k.

³⁴ Art. 267 § 1 k.k.

³⁵ Art. 267 § 1 i 3 k.k.

³⁶ Art. 267 § 3 k.k.

³⁷ Art. 267 § 3 k.k.

³⁸ Art. 278 § 1 w zw. z art. 267 § 3 k.k.

Przepis art. 7 dyrektywy 2024/1385 odnosi się do czterech zachowań³⁹ - stalkingu, stalkingu zbiorowego, cyberflashingu oraz doxingu. Stalking jest przestępstwem penalizowanym w art. 190a § 1 k.k. Przepis ten został wprowadzony ustawą z dnia 25 lutego 2011 r. o zmianie ustawy - Kodeks karny⁴⁰ i stanowi, że podlega odpowiedzialności karnej ten, kto przez „uporczywe nękanie innej osoby lub osoby dla niej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia, poniżenia lub udręczenia lub istotnie narusza jej prywatność”. Przepisy nie precyzują, w jakiej formie ma dochodzić do „uporczywego nękania”, tj. czy w świecie realnym (np. osoba chodzi za kimś, czeka na nią w miejscu pracy, szkole, pod domem itp.), czy z wykorzystaniem technologii informacyjno-komunikacyjnych (np. wysyłając tysiące wiadomości, nawiązując kontakt za pośrednictwem mediów społecznościowych). Krajowy zakres kryminalizacji jest nawet szerszy niż to, czego wymaga prawodawca unijny. Na podstawie art. 190a § 1 k.k. wystarczające jest „istotne naruszenie prywatności”, zaś nękanie nie musi wkroczyć w fazę gróźb karalnych, czy gróźb

³⁹ Warto także przytoczyć motyw nr 24 do dyrektywy 2024/1385, w którym wyjaśniono cele i znaczenie art. 7 tego aktu prawnego. Motyw ten brzmi: „Należy ustanowić normy minimalne odnoszące się do przestępstwa cybernękania, aby uwzględnić jego najpoważniejsze formy. Powinny one obejmować powtarzające się lub ciągłe zagrożenie danej osobie, co najmniej w przypadkach, gdy takie czyny obejmują groźby - za pomocą ICT - popełnienia przestępstwa oraz gdy taki czyn może spowodować, że dana osoba poważnie obawia się o swoje bezpieczeństwo lub o bezpieczeństwo osób będących na jej utrzymaniu. Powinno to także obejmować podejmowanie - wraz z innymi osobami, za pomocą ICT, w publicznie dostępny sposób - działania grożącego lub znieważającego wymierzonego w daną osobę, jeżeli takie czyny mogą wyrządzić tej osobie poważną szkodę psychiczną. Takie szeroko zakrojone ataki, w tym skoordynowane ataki masowe w internecie, mogą przekształcić się w napaść poza internetem lub spowodować poważne szkody psychiczne, a w skrajnych przypadkach mogą prowadzić do samobójstwa ofiary. Ataki te są często wymierzone w czołowe polityczki, dziennikarki i obrończynie praw człowieka lub inne znane kobiety; do ataków może również dochodzić w różnych kontekstach, na przykład na kampusach uczelni, w szkołach czy w miejscu pracy. Tego rodzaju przemocą w internecie należy zająć się zwłaszcza w przypadku ataków na szeroką skalę, na przykład w formie zmasowanego nękania przez znaczną liczbę osób. Normy minimalne dotyczące przestępstwa cybernękania powinny również obejmować niezamówione przesyłanie danej osobie obrazu, nagrania wideo lub innych podobnych treści przedstawiających genitalia ("cyberflashing"), w przypadku, gdy taki czyn może wyrządzić tej osobie poważną szkodę psychiczną. Cyberflashing jest powszechną formą zastraszania i uciszania kobiet. Normy minimalne dotyczące przestępstwa cybernękania powinny również obejmować przepisy dotyczące sytuacji, w których dane osobowe ofiary są udostępnione publicznie za pomocą ICT bez zgody ofiary, aby zachęcić inne osoby do wyrządzenia ofierze szkody fizycznej lub poważnej szkody psychicznej ("doxing").”.

⁴⁰ Dz. U. Nr 72, poz. 381.

zastosowania przemocy⁴¹. W teorii wystarczające jest to, że osoba nie życzy sobie określonych wiadomości, intensywność komunikacji jest znaczna i nie ma znaczenia, treść tych wiadomości (tzn. nie muszą one być obraźliwe, czy zawierać gróźb).

Przepisy krajowe nie chronią jednak w wystarczającym stopniu przed stalkingiem zbiorowym (art. 7 lit. b dyrektywy 2024/1385).

Problematyka ta została szczegółowo omówiona w wystąpieniu generalnym z dnia 11 września 2025 r., ale mimo poparcia m.in. Rzeczniczki Praw Dziecka, Ministerstwo Sprawiedliwości odpowiedziało, że aktualnie nie ma planów prowadzenia prac legislacyjnych⁴². Komisja Kodyfikacyjna Prawa Karnego dostrzegła problem odnoszący się do nękania zbiorowego, ale skonkretyzowane prace legislacyjne jeszcze się nie rozpoczęły⁴³.

Poza zakresem kryminalizacji znajduje się jednak cyberflashing i doxing.

Cyberflashing jest formą ekshibicjonizmu, tyle że dokonywanego z wykorzystaniem technologii informacyjno-komunikacyjnych. Zjawisko to definiuje się jako wysyłanie niechcianych fotografii lub filmów przedstawiających miejsca intymne bez zgody odbiorcy. W piśmiennictwie wskazuje się, że chodzi przede wszystkim o wysyłanie niechcianych zdjęć genitaliów przez mężczyzn innym mężczyznom lub kobietom⁴⁴ (tzw. dickpick). Zjawisko to można uznać także za formę molestowania seksualnego⁴⁵. Konsekwencje cyberflashingu mogą być różne w zależności od tego, kto jest odbiorcą fotografii – inaczej na zdjęcia genitaliów (męskich lub żeńskich) będą reagowały dzieci,

⁴¹ Wyróżnia się sześć etapów stalkingu: 1. zaloty (oznaki troski i sympatii, „pełną uczuć” korespondencja); 2. obserwacja (śledzenie zachowań ofiary, w tym możliwe jest wykorzystanie np. lokalizacji GPS); 3. komunikacja (jeśli nie nastąpiła w pierwszym etapie); 4. przemoc symboliczna (wysyłanie niepokojących prezentów np. zwiędłych kwiatów, czy martwych zwierząt, niszczenie mienia, grożenie ofierze lub jej rodzinie); 5. przemoc fizyczna skierowana na ofiarę; 6. przemoc przeniesiona (gdy sprawca nie może nawiązać kontaktu bezpośrednio z ofiarą, może znaleźć cel zastępczy – rodzinę lub bliskich ofiary albo osoby, które przypominają „pierwotną” ofiarę stalkingu).

Zob. szerzej: <https://juststalkingmdresources.org/just-six-stages>.

⁴² Wystąpienie generalne oraz pozostała korespondencja dostępna jest na stronie: <https://bip.brpo.gov.pl/pl/content/rpo-stalking-propozycja-zmiany-prawa-ms-rpd-odpowiedz>.

⁴³ Zob. opinię Komisji Kodyfikacyjnej Prawa Karnego dostępną na stronie: <https://www.gov.pl/web/sprawiedliwosc/opinie-komisji-kodyfikacyjnej-prawa-karnego2>.

⁴⁴ C. McGlynn, K. Johnson, *Criminalising Cyberflashing: Options for Law Reform*, The Journal of Criminal Law 2021, nr 3, v. 85, Issue 3, s. 171-188.

⁴⁵ Zgodnie z polityką równości przyjętą na Uniwersytecie Warszawskim, molestowanie seksualne definiuje się jako „każde niepożądane zachowanie o charakterze seksualnym odnoszące się do płci, którego celem lub skutkiem jest naruszenie godności osoby, a w szczególności stworzenie wobec niej zastraszającej, wrogiej, poniżającej, upokarzającej lub uwłaczającej atmosfery; na zachowanie to mogą się składać elementy fizyczne, werbalne lub pozawerbalne.”. Zob.: <https://rownowazni.uw.edu.pl/molestowanie-seksualne/>.

inaczej nastolatkom, a inaczej osoby dorosłe⁴⁶. W odniesieniu do osób dorosłych, zwłaszcza kobiet, otrzymywanie nagich, niechcianych zdjęć, jest często traktowane jako „pewna niezręczność” i element „normalnego” funkcjonowania w mediach społecznościowych, czy na portalach randkowych⁴⁷.

Sytuacje, w których kobiety czy mężczyźni otrzymują niechciane nagie zdjęcia miejsc intymnych, stopniowo przestaje być „ryzykiem” wpisanym w aktywność sieci, a osoby pokrzywdzone zaczynają poszukiwać ochrony także na gruncie prawa karnego. Niedawno głośna była sprawa mężczyzny z Białegostoku, który dziesiątkom kobiet wysyłał zdjęcia genitaliów⁴⁸. Postępowanie karne – prowadzone w związku z podejrzeniem popełnienia przestępstwa z art. 190a § 1 k.k. – zostało początkowo umorzone⁴⁹. Po nagłośnieniu sytuacji i sprawy przez media, prokurator podjął postępowanie, ale nie ma jeszcze informacji odnośnie do kroków i czynności, jakie zostały podjęte przez organy ścigania.

Przestępstwo stalkingu nie zostało zaprojektowane do ścigania zjawiska cyberflashing. **Pojawia się pytanie o granice interpretacji znamion czynu z art. 190a § 1 k.k., a także jak wyznaczyć granice kryminalizacji cyberflashingu. Jednorazowe wysłanie zdjęć – nawet jeśli dolegliwe dla jednostki – niekoniecznie powinno spotykać się z reakcją prawa karnego.** Dyrektywa 2024/1385 w odniesieniu do zjawiska cyberflashingu – art. 7 lit. c – wymaga kryminalizacji jako przestępstwa tylko, gdy ekspozycja na niechciane materiały przedstawiające genitalia, mogła wyrządzić „poważną szkodę psychiczną”. W przeciwieństwie do innych czynów zabronionych, prawodawca unijny nie proponuje żadnych kar minimalnych (zob. art. 10 dyrektywy

⁴⁶ Inaczej też poszczególne grupy będą odczuwały dolegliwości wynikające z otrzymywania nagich zdjęć czy zdjęć miejsc intymnych. Zob. szerzej: P. Bleakley, D. Kelly, E. Short, *What's the harm? Gender and age differences in acceptance of cyberflashing, reporting intentions, and perceived prevalence*, Current Issues in Criminal Justice 2025, 1–19. <https://doi.org/10.1080/10345329.2025.2513737>

⁴⁷ C. McGlynn, K. Johnson, *Criminalising Cyberflashing: Options for Law Reform*, The Journal of Criminal Law 2021, nr 3, v. 85, Issue 3, s. 171-188.

⁴⁸ Zob.: <https://dziendobry.tvn.pl/styl-zycia/wysyla-kobietom-swoje-nagie-zdjecia-prokuratura-umorzyla-sprawe-st8870307>; <https://bialystok.wyborcza.pl/bialystok/7,35241,32531521,chwali-sie-przed-kobietami-umiesnionym-cialem-i-genitaliami.html>; <https://www.tvp.info/91186644/bialystok-wysylal-kobietom-setki-zdjec-i-filmow-pornograficznych-jakub-b-nekal-kobiety-co-na-to-policja-reporterzy>.

⁴⁹ W uzasadnieniu decyzji o umorzeniu prokurator wskazał, że „Wysyłanie wiadomości z wizerunkiem nagich zdjęć w niniejszej sprawie nie odznaczało się uporczywością. Nie sposób również stwierdzić, by zachowanie sprawcy wyrażało jego szczególne nastawienie - nieustępliwości, przekorności lub nieustępliwości podejmowanych w złej woli. Nadawca tych wizerunków bowiem wysyłał wiadomości zarówno do osób mu znanych, jak również do obcych osób. Pokrzywdzone po otrzymaniu wskazanych wiadomości blokowały numer nadawcy. Miały za tym możliwość skutecznego zablokowania otrzymywania kolejnych wiadomości z danego numeru”.

2024/1385). **O ile jednorazowe wysłanie zdjęcia, czy filmiku przedstawiającego genitalia osobie dorosłej nie powinno być kryminalizowane – nie każde nieprzyjemne doświadczenie powinno spotykać się z reakcją prawnokarną – to jeśli działanie sprawcy ma charakter powtarzający się, może osiągnąć poziom dolegliwości wykroczenia z art. 107 k.w.⁵⁰ albo przestępstwa stalkingu – realizując znamię istotnej ingerencji w prywatność jednostki.** Obecnie zatem – w odniesieniu do osób dorosłych – krajowe przepisy wydają się być zgodne z dyrektywą.

Problemem jest jednak brak adekwatnej reakcji prawnokarnej na sytuacje, kiedy niechciane, nagie zdjęcia obcych (albo znajomych) osób dostają dzieci – zwłaszcza dzieci poniżej 15 roku życia. Aktualne brzmienie art. 200 § 3 k.k. penalizuje prezentowanie treści pornograficznych, zaś § 4 tego przepisu – prezentowanie wykonania czynności seksualnej. Przesyłanie zdjęć genitaliów niekoniecznie wypełnia znamię „treści pornograficznych”. W doktrynie, w ślad za orzecnictwem, za treści pornograficzne mogą zostać uznane materiały 1) przedstawiające płciowość i życie płciowe człowieka; 2) koncentrujące się wyłącznie na technicznych aspektach płciowości i życia płciowego z pominięciem wszelkiej warstwy intelektualno-personalistycznej; 3) ukazujące ludzkie narządy płciowe w ich funkcjach seksualnych; 4) z przebijającą treścią przekazu jaką jest wywołanie podniecenia seksualnego u odbiorcy⁵¹. Wskazuje się także na kryteria pomocnicze pozwalające ustalić, czy dana treść miała charakter treści pornograficznej, czy nie. Takim kryterium pomocniczym może być np. walor estetyczny: „im jest on niższy, tym bardziej sugerować może ocenę danej prezentacji jako pornograficznej”⁵². Jak podkreśla K. Lipiński „pojęcie „treści pornograficznych” obejmuje zatem przedstawienia czynności seksualnych (obcowania płciowego i innej czynności seksualnej), wszelako nie wszystkich – a to z uwagi na konieczność zastosowania wyżej wymienionych kryteriów, pozwalających na wprowadzenie „pośredniej” kategorii treści erotycznych.”⁵³. **Tymczasem art. 7 lit. c dyrektywy 2024/1385 niejako „zwalnia” z konieczności oceny charakteru materiałów – czy były to treści pornograficzne czy erotyczne – a wystarczająca jest zbiektywizowana ocena nagrania, czy zdjęcia pod kątem tego, co się tam znajduje, tj. czy są tam męskie albo żeńskie narządy płciowe.**

⁵⁰ Przepis brzmi: „Kto w celu dokuczenia innej osobie złośliwie wprowadza ją w błąd lub w inny sposób złośliwie niepokoi, podlega karze ograniczenia wolności, grzywny albo karze nagany.”.

⁵¹ Por.: P. Zakrzewski [w:] *Kodeks karny. Komentarz*, red. J. Majewski, Warszawa 2024, art. 202.

⁵² Tak: K. Lipiński [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa 2021, art. 202 i cytowana tam literatura.

⁵³ Tak: K. Lipiński [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa 2021, art. 202 i cytowana tam literatura.

Przepis art. 7 lit. d dyrektywy 2024/1385 wymaga wprowadzenia w prawie krajowym nowego rodzaju przestępstwa, tj. doxingu. Ministerstwo Cyfryzacji definiując pojęcie doxingu wskazało, że zjawisko to polega na „gromadzeniu i wykorzystywaniu danych zebranych w Internecie na temat innych osób w celu zawstydzenia, zastraszenia, zniesławienia, bądź wywołania u ofiary poczucia zagrożenia. Termin jest neologizmem powstałym na bazie anglojęzycznych wyrażen *docs* (dokumenty) i *compiling/releasing* (przetwarzać, upubliczniać).”⁵⁴. Doxing opiera się na wyszukiwaniu już wcześniej udostępnionych informacji (np. w mediach społecznościowych, w tym na zamkniętych/prywatnych profilach) i rozpowszechnieniu ich nieograniczonemu kręgowi odbiorców. **Dyrektywa wymaga kryminalizacji nie samego rozpowszechniania danych osobowych wcześniej upublicznionych, ale takiego ich rozpowszechnienia, kiedy zamiarem sprawcy jest nakłonienie innych do wyrządzenia tej osobie szkody fizycznej lub poważnej szkody psychicznej.**

Jeśli chodzi o rozumienie pojęcia „dane osobowe”, to definicja tego pojęcia znajduje się w rozporządzeniu 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)⁵⁵. Przepis art. 4 pkt 1 RODO definiuje dane osobowe jako „wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak **imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej**”.

Obecnie art. 107 ust. 1 ustawy o ochronie danych osobowych⁵⁶ penalizuje nieuprawnione przetwarzanie danych osobowych. Czyn ten jest zagrożony karą do 2 lat pozbawienia wolności, karą ograniczenia wolności albo karą grzywny. Przepis art. 107 ust. 2 ustawy o ochronie danych osobowych wprowadza typ kwalifikowany tego przestępstwa, jeśli przetwarzane były dane ujawniające pochodzenie rasowe lub

⁵⁴ <https://www.gov.pl/web/baza-wiedzy/doxing--nowe-zjawisko-i-cyberzagrozenie>.

⁵⁵ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

⁵⁶ Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781).

etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej. Takie zachowanie podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech. Problemem jest jednak wąski zakres penalizacji, odnoszący się do „ujawnienia” określonych informacji. Oznacza to, że jeśli osoba sama ujawniła np. informacje dotyczące orientacji seksualnej czy pochodzenia etnicznego, to dalsze powielenie tej informacji – w celu nakłonienia do wyrządzenia szkody – nie będzie przestępstwem z art. 107 ustawy o ochronie danych osobowych.

Samo rozpowszechnienie danych osobowych, jeśli określona osoba je wcześniej upubliczniła albo jest osobą publiczną, także nie będzie przestępstwem. Rozpowszechnienie danych osobowych, zawierające wezwanie do wyrządzenia szkody osobie fizycznej albo poważnej szkody psychicznej może realizować znamiona czynu z art. 255 § 1 lub 2 k.k., kiedy sprawca wzywa np. do pobicia, kierowania gróźb karalnych, czy do kierowania zniewag. Krajowe przepisy wymagają jednak, by takie działanie było „publiczne”, tj. by nieograniczony krąg osób mógł się zapoznać z danymi osobowymi osoby oraz treścią wiadomości wzywającą do przemocy. **Poza zakresem kryminalizacji pozostają jednak sytuacje, gdy doxing i wzywanie do wyrządzenia szkody psychicznej lub fizycznej odbywa się na zamkniętych grupach w mediach społecznościowych albo na grupach w komunikatorach (jak whatsapp) albo na kanałach nadawczych określonego podmiotu (np. na kanałach na Instagramie, czy Telegramie).** Mimo znacznego kręgu odbiorców, nie można uznać, że było to działanie „publiczne”. Rozważyć także można wykorzystanie konstrukcji przestępstwa stalkingu albo groźby karalnej, ale w przypadku tego pierwszego konieczne jest wykazanie „uporczywości” zachowania, a w przypadku drugiego „obawy spełnienia groźby”. Nie w każdej sytuacji będzie to możliwe. Przykładowo, jeśli rozpowszechniono dane osobowe określonej osoby wraz z informacją o orientacji seksualnej i wzywano w obraźliwy sposób do komentowania wyglądu na zamkniętej grupie na Instagramie, to o ile pokrzywdzony nie poweźmie informacji o takim działaniu i nie będzie próbował skorzystać z ochrony jaką gwarantuje art. 212 lub 216 k.k., to takie zachowanie nie będzie przestępstwem. W przypadku art. 212 § 1 k.k. należy bowiem wykazać, że komentarze, czy zdjęcia mogły poniżyć pokrzywdzonego w opinii publicznej lub narazić na utratę zaufania potrzebnego dla danego stanowiska, zawodu lub rodzaju działalności. W przypadku zniewagi – art. 216 § 1 k.k. – jeśli dokonano jej pod

nieobecność pokrzywdzonego, to takie działanie, by było karalne, musi być publiczne albo zamiarem sprawcy było to, by zniewaga dotarła do pokrzywdzonego.

Pojawia się pytanie, czy nie byłoby celowe dodanie do art. 107 ustawy o ochronie danych osobowych ust. 3, który wprost penalizowałby sytuacje, o których mowa w art. 7 lit. d dyrektywy 2024/1385. Ponadto, zachowanie, o którym mowa w art. 7 lit. d dyrektywy 2024/1385 jest zbliżone do stalkingu zbiorowego (kampanii hejtu). Być może – jeśli ustawodawca zdecyduje się wprowadzić taki typ czynu zabronionego, to znamiona zostaną tak ukształtowane, by objąć również doxing.

Problematyka przestępstw motywowanych uprzedzeniami, w szczególności mowy nienawiści ze względu na płeć, o których mowa w art. 8 dyrektywy 2024/1385, była przedmiotem innej sprawy, w której Rzecznik Praw Obywatelskich w dniu 11 sierpnia 2026 r. skierowała wystąpienie generalne⁵⁷.

Kwestie jurysdykcji oraz odszkodowania nie wymagają implementacji, poza zniesieniem warunku podwójnej karalności w przypadku okaleczania żeńskich narządów płciowych (art. 3 dyrektywy) oraz przymusowych małżeństw (art. 4 dyrektywy). Jeśli sprawcą przestępstwa był cudzoziemiec albo Polak, a czyn był popełniony za granicą, to zgodnie z art. 111 § 1 k.k. „warunkiem odpowiedzialności za czyn popełniony za granicą jest uznanie takiego czynu za przestępstwo również przez ustawę obowiązującą w miejscu jego popełnienia.”. **Konieczna jest zmiana wyłączająca z zakresu art. 111 § 1 k.k. czynów z art. 156 § 1 pkt 3 k.k. i art. 191b k.k.**

Podsumowując, w zakresie koniecznych zmian w prawie karnym materialnym, implementacja dyrektywy 2024/1385 nie wiąże się z zasadniczą przebudową polskich regulacji. Potrzeba zmian dotyczy przede wszystkim nowych form przemocy cyfrowej. W tym zakresie konieczne jest w szczególności:

- **rozszerzenie zakresu kryminalizacji czynu z art. 191a k.k.** – obecne brzmienie tego przepisu odnosi się do rozpowszechniania bez zgody „wizerunku” nagiej osoby albo osoby w trakcie czynności seksualnej. Dla kryminalizacji konieczne jest rozpowszechnienie materiału pozwalającego na identyfikację pokrzywdzonego. Tymczasem, art. 5 dyrektywy 2024/1385 wymaga objęcia penalizacją także **publicznego udostępniania materiałów przedstawiających intymne części ciała lub treści o wyrażnie seksualnym charakterze, jeżeli ich ujawnienie może wyrządzić ofierze poważną szkodę, nawet jeśli materiał nie mieści się w**

⁵⁷ Znak sprawy: II.501.10.2025.

rozumieniu „wizerunku”; penalizacja musi dotyczyć co najmniej tych sytuacji, kiedy działania sprawcy mogłyby wyrządzić pokrzywdzonemu poważną szkodę;

- **wprowadzenie wyraźnej penalizacji seksualnych treści zmanipulowanych (deepfake) dotyczących osób dorosłych** – obecnie przepisy prawa karnego obejmują treści wytworzone albo przetworzone przede wszystkim w odniesieniu do materiałów przedstawiających małoletnich (art. 202 § 4b k.k.), natomiast brak jest podstawy prawnej do objęcia kryminalizacją zachowań, gdy zmanipulowany materiał o charakterze seksualnym dotyczy osoby dorosłej. Zmiana jest konieczna, ponieważ art. 5 dyrektywy 2024/1385 wymaga kryminalizacji także wytwarzania, przerabiania i publicznego udostępniania bez zgody materiałów sprawiających wrażenie, że osoba uczestniczy w czynnościach o wyraźnie seksualnym charakterze, niezależnie od tego, czy pokrzywdzony jest małoletni czy pełnoletni; penalizacja musi dotyczyć co najmniej tych sytuacji, kiedy działania sprawcy mogłyby wyrządzić pokrzywdzonemu poważną szkodę;
- **uzupełnienie kryminalizacji o tzw. sextortion** – obecnie zagrożenie ujawnieniem materiałów intymnych może być tylko częściowo obejmowane przez konstrukcję groźby karalnej (art. 190 k.k.) albo zmuszania (art. 191 § 1 k.k.), jednak rozwiązanie to nie zapewnia pełnej zgodności z dyrektywą, zwłaszcza wtedy, gdy przedmiotem groźby są treści zmanipulowane dotyczące osób dorosłych; penalizacja musi dotyczyć co najmniej tych sytuacji, kiedy działania sprawcy mogłyby wyrządzić pokrzywdzonemu poważną szkodę; penalizacja musi dotyczyć co najmniej tych sytuacji, kiedy działania sprawcy mogłyby wyrządzić pokrzywdzonemu poważną szkodę;
- **rozważenie wprowadzenia odrębnego typu czynu zabronionego odpowiadającego cybernękaniu** – część zachowań wskazanych w art. 6 dyrektywy może być obecnie kwalifikowana na podstawie art. 267 § 1 i 3 k.k. albo art. 190a § 2 k.k., jednak przepisy te chronią przede wszystkim poufność informacji lub określone aspekty prywatności. Nie oddają wprost istoty zachowania polegającego na ciągłej cyfrowej kontroli i monitorowaniu ofiary. Zmiana wydaje się celowa z uwagi na rozproszoność obecnej kryminalizacji i nie zawsze adekwatne uwzględnienie nowych form technologicznej kontroli (np. urządzenia typu SmartHome);
- **uzupełnienie karnoprawnej ochrony w zakresie stalkingu zbiorowego** – klasyczny typ stalkingu z art. 190a § 1 k.k. zasadniczo obejmuje uporczywe nękanie, także z wykorzystaniem środków komunikacji elektronicznej, jednak nie daje

dostatecznie jasnej i skutecznej podstawy do ścigania sytuacji, w których nękanie przybiera postać skoordynowanego działania wielu osób. Kwestia ta jest przedmiotem aktywnych działań RPO, zaś problem ten został omówiony poza zakresem dyrektywy – ma bowiem szerszy zakres niż wyłącznie przemoc wobec kobiet i przemoc domowa;

- **wprowadzenie odrębnej penalizacji doxingu albo wyraźne rozszerzenie istniejących przepisów o ochronie danych osobowych** – obecne przepisy, w szczególności art. 107 ustawy o ochronie danych osobowych, penalizują nieuprawnione przetwarzanie danych osobowych, ale nie obejmują w pełni sytuacji, w których sprawca rozpowszechnia także wcześniej ujawnione dane osobowe w celu nakłonienia innych osób do wyrządzenia ofierze szkody fizycznej albo poważnej szkody psychicznej;
- **doprecyzowanie ochrony dzieci przed cyberflashingiem** – w odniesieniu do osób dorosłych powtarzające się przesyłanie niechcianych materiałów przedstawiających genitalia może być w pewnych sytuacjach ujmowane przez istniejące przepisy o stalkingu albo wykroczeniu z art. 107 k.w., jednak problem pojawia się zwłaszcza wtedy, gdy odbiorcą takich materiałów jest dziecko. Obowiązujące przepisy art. 200 § 3 i 4 k.k. odwołują się do pojęcia „treści pornograficznych” albo prezentowania czynności seksualnej, co może nie obejmować wszystkich przypadków przesyłania samych zdjęć genitaliów. Zmiana jest konieczna, ponieważ art. 7 lit. c dyrektywy 2024/1385 konstruuje ochronę szerzej – przez odwołanie do samego przesyłania niechcianych materiałów przedstawiających genitalia, jeśli mogłoby to wyrządzić szkodę psychiczną – i tym samym uniezależnia penalizację od spornej oceny, czy dany materiał miał charakter pornograficzny w rozumieniu prawa krajowego;
- **rozszerzenie regulacji dotyczących cyfrowej przemocy seksualnej na przypadki masowego gromadzenia i udostępniania materiałów przedstawiających realny i przetworzony wizerunek osoby bez jej zgody**. Choć zagadnienie to częściowo wykracza poza zakres dyrektywy, to obecne przepisy są nieefektywne wobec zjawisk polegających na tworzeniu i rozpowszechnianiu zbiorów materiałów intymnych lub seksualnych bez zgody osób przedstawionych na tych materiałach. Zmiana wydaje się potrzebna także dlatego, że obecne instrumenty – zwłaszcza przy ściganiu wnioskowym i przy wąskim zakresie art. 191a k.k. – nie zapewniają skutecznej reakcji karnej na zjawiska o skali big data, które realnie godzą w dobra osobiste, prywatność i bezpieczeństwo pokrzywdzonych.

3. Dyrektywa 2024/1385 i zakres koniecznych zmian o charakterze proceduralnym

Przepisy art. 14–24 dyrektywy 2024/1385 ustanawiają minimalne wymogi proceduralne dotyczące: sposobu zgłaszania przestępstw objętych dyrektywą, prowadzenia postępowań przygotowawczych, oceny potrzeb osób doświadczających przemocy domowej albo przemocy motywowanej płcią w zakresie ochrony i wsparcia, stosowania środków ochronnych, ochrony prywatności pokrzywdzonych, a także stworzenia ram prawnych pozwalających na reagowanie i usuwanie bezprawnych treści w środowisku cyfrowym. Dyrektywa wymaga, aby postępowania w sprawach przemocy wobec kobiet i przemocy domowej były prowadzone w sposób szybki, skoordynowany i uwzględniający bezpieczeństwo pokrzywdzonych, z poszanowaniem ich praw procesowych oraz z dążeniem do zapobiegania wtórnej i ponownej wiktymizacji.

W zakresie koniecznych zmian w prawie karnym procesowym, kluczowe znaczenie ma poprawna implementacja art. 23 dyrektywy 2024/1385.

Problematyka indywidualnej oceny potrzeb osoby doświadczającej przemocy (art. 16 i 17 dyrektywy 2024/1385) była przedmiotem analizy i implementacji w 2023 r. Przepis art. 52a k.p.k. został dodany ustawą z dnia 13 stycznia 2023 r. o zmianie ustawy - Kodeks postępowania cywilnego oraz niektórych innych ustaw⁵⁸. Formularz indywidualnej oceny potrzeb pokrzywdzonego i świadka z rozporządzenia Ministra Sprawiedliwości z dnia 2 lutego 2025 r. w sprawie określenia wzoru kwestionariusza indywidualnej oceny pokrzywdzonego i świadka⁵⁹ nie zawiera luk i co najwyżej wymaga przeglądu pod kątem przestępstw cyfrowych – pod warunkiem wprowadzenia odpowiednich zmian w prawie karnym materialnym. Środki ochrony pokrzywdzonego związane ze stosowaniem wobec podejrzanego środków zapobiegawczych (art. 19 dyrektywy 2024/1385), np. nakazu opuszczenia lokalu zajmowanego wspólnie z pokrzywdzonym (art. 275a k.p.k.), zakazu kontaktowania się, czy zakazu zbliżania się (art. 275 k.p.k.), są już uregulowane w przepisach k.p.k. Odrębną kwestią jest ocena stosowania tych środków w praktyce i np. efektywność prowadzonych postępowań, dostępność szkoleń z zakresu przestępstw motywowanych płcią itp. (art. 15 dyrektywy 2024/1385). Ochrona życia prywatnego (art. 20 dyrektywy 2024/1385) w zakresie ograniczenia możliwości zadawania pytań odnoszących się do sfery życia seksualnego pokrzywdzonego, także została implementowana. Przepis art. 171 § 4a k.p.k. został dodany ustawą z dnia 13 stycznia 2023 r. o zmianie ustawy - Kodeks postępowania cywilnego oraz niektórych

⁵⁸ Dz. U. poz. 289 z późn. zm.

⁵⁹ Dz. U. poz. 161.

innych ustaw⁶⁰ i wprowadza quasi zakaz dowodowy polegający na niedopuszczalności zadawania pytań świadkowi, które dotyczą jego życia seksualnego, chyba że jest to niezbędne dla rozstrzygnięcia sprawy.

W części proceduralnej dyrektywa 2024/1385 w większości opiera się na rozwiązaniach wynikających z Konwencji stambulskiej. Krajowy ustawodawca już wcześniej wdrożył odpowiednie rozwiązania.

Najistotniejszą luką implementacyjną w zakresie przepisów proceduralnych jest mechanizm przewidziany w art. 23 dyrektywy 2024/1385.

Przepis ten wymaga wprowadzenia - bez uszczerbku dla rozporządzenia 2022/2065 DSA⁶¹ (akt o usługach cyfrowych) i mechanizmu przewidzianego w art. 9 tego rozporządzenia – niezbędnych środków, które zapewnią szybkie usuwanie określonych, publicznie dostępnych treści online albo uniemożliwią dostęp do takich treści. Chodzi przede wszystkim o treści objęte art. 5 ust. 1 lit. a i b (rozpowszechnianie treści intymnych, w tym treści przetworzonych lub wytworzonych) oraz art. 7 (cybernękąnie) i 8 (cyfrowa mowa nienawiści) dyrektywy 2024/1385. Środki te powinny obejmować możliwość wydawania przez właściwe organy wiążących nakazów prawnych usunięcia określonych materiałów (zdjęć, komentarzy, postów) lub zablokowania dostępu do nich. Nakazy te powinny być kierowane do dostawców usług hostingowych, a jeżeli usunięcie nie jest wykonalne – także do innych dostawców usług pośrednich dysponujących techniczną i operacyjną zdolnością do podjęcia działania. Jeżeli postępowanie karne zakończy się niestwierdzeniem popełnienia przestępstwa, nakazy te powinny zostać cofnięte, a ich adresaci – poinformowani o tym fakcie. Dyrektywa wymaga ponadto, aby środki te były stosowane zgodnie z przejrzystymi procedurami i podlegały odpowiednim gwarancjom, w szczególności w zakresie konieczności, proporcjonalności i poszanowania praw podstawowych wszystkich zainteresowanych podmiotów. Dostawcy usług hostingowych, inni dostawcy usług pośrednich oraz dostawcy treści, których dotyczy nakaz, powinni mieć zapewnione prawo do skutecznego środka zaskarżenia, w tym do zaskarżenia nakazu przed sądem państwa członkowskiego właściwego organu, który go wydał. Dostawcy usług hostingowych powinni być też informowani o przyczynach usunięcia określonych treści lub uniemożliwienia dostępu do nich oraz o dostępnych środkach odwoławczych. Jednocześnie usunięcie treści albo zablokowanie dostępu nie może uniemożliwiać

⁶⁰ Dz. U. poz. 289 z późn. zm.

⁶¹ Rozporządzenie Parlamentu Europejskiego i Rady 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz. U. UE. L. z 2022 r. Nr 277, str. 1 z późn. zm.).

właściwym organom bezzwłocznego uzyskania lub zabezpieczenia materiału dowodowego potrzebnego do prowadzenia postępowania przygotowawczego lub ścigania.

Pod kątem konstrukcyjnym przepis art. 23 dyrektywy 2024/1385 wymaga, by w prawie krajowym istniały przepisy pozwalające:

- uniemożliwiać dostęp do treści, które mogą realizować znamiona czynów zabronionych zdefiniowanych w art. 5 ust. 1 lit. a i b (rozpowszechnianie treści intymnych, w tym treści przetworzonych lub wytworzonych) oraz art. 7 (cybernękąnie) i 8 (cyfrowa mowa nienawiści) dyrektywy 2024/1385;
- zabezpieczać materiał dowody na potrzeby postępowania karnego;
- usuwać materiały/treści, które mogą realizować znamiona czynów zabronionych zdefiniowanych w art. 5 ust. 1 lit. a i b (rozpowszechnianie treści intymnych, w tym treści przetworzonych lub wytworzonych) oraz art. 7 (cybernękąnie) i 8 (cyfrowa mowa nienawiści) dyrektywy 2024/1385.

Prawo krajowe powinno przewidywać kontrolę sądową decyzji o usunięciu, uniemożliwieniu dostępu czy zabezpieczeniu danych (art. 24 ust. 4 in fine dyrektywy 2024/1385).

Mechanizm blokowania dostępu do treści, jaki wynika z art. 23 dyrektywy 2024/1385, jest zbliżony do rozwiązania wynikającego z art. 218a k.p.k. Przepis art. 218a § 1 k.p.k. zobowiązuje urzędy, instytucje i podmioty prowadzące działalność telekomunikacyjną lub świadczące usługi drogą elektroniczną oraz dostawców usług cyfrowych do niezwłocznego zabezpieczenia - na mocy postanowienia sądu lub prokuratora w postępowaniu przygotowawczym - na czas określony, nieprzekraczający 90 dni, danych informatycznych przechowywanych w urządzeniach zawierających te dane na nośniku lub w systemie informatycznym. W sprawach o przestępstwa w art. 200b k.k. (propagowanie pedofilii⁶²), art. 202 § 3 k.k. (posiadanie, rozpowszechnianie, przechowywanie itp. treści pornograficznych z udziałem małoletniego⁶³), art. 202 § 4 k.k. (utrwalanie treści pornograficznych z udziałem małoletniego⁶⁴), art. 202 § 4a k.k.

⁶² Przestępstwo jest zagrożone karą do 3 lat pozbawienia wolności.

⁶³ Przepis brzmi „Kto w celu rozpowszechniania produkuje, utrzuła lub sprowadza, przechowuje lub posiada albo rozpowszechnia lub prezentuje treści pornograficzne z udziałem małoletniego albo treści pornograficzne związane z prezentowaniem przemocy lub posługiwaniem się zwierzęciem, podlega karze od 2 do 15 lat pozbawienia wolności.”.

⁶⁴ Przestępstwo jest zagrożone karą od roku do 10 lat pozbawienia wolności.

(przechowywanie, posiadanie i uzyskiwanie dostępu do treści pornograficznych z udziałem małoletniego⁶⁵), art. 202 § 4b k.k. (produkowanie, rozpowszechnianie, prezentowanie, przechowywanie lub posiadanie treści pornograficznych przedstawiających wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej⁶⁶) lub art. 255a k.k. (rozpowszechnianie lub publiczne prezentowanie treści mogące ułatwić popełnienie przestępstwa o charakterze terrorystycznym w zamiarze, aby przestępstwo takie zostało popełnione⁶⁷) oraz przestępstw z rozdziału 7⁶⁸ ustawy o przeciwdziałaniu narkomanii⁶⁹, zabezpieczenie danych informatycznych może polegać na uniemożliwieniu uzyskaniu dostępu do nich. Zobowiązany do wykonania postanowienia o zabezpieczeniu danych może być także administrator treści (art. 218a § 3 k.p.k.), jeśli treści zostały upublicznione lub udostępnione drogą elektroniczną.

Postanowienie, o którym mowa w art. 218a § 1 k.p.k. doręcza się dostawcom usług łączności i usług świadczonych drogą elektroniczną, ale doręczenie może być odroczone na czas oznaczony, niezbędny ze względu na dobro sprawy, ale nie później niż do czasu prawomocnego zakończenia postępowania (art. 218a § 1 in fine w zw. z art. 218 § 2 zd. 2 k.p.k.). Podmiotom, których postanowienie dotyczy, przysługuje zażalenie na zasadach określonych w art. 236 k.p.k. W postępowaniu przygotowawczym, zażalenie wnosi się do właściwego miejscowo sądu rejonowego, tj. do sądu rejonowego, w okręgu którego prowadzi się postępowanie przygotowawcze. Warto zwrócić uwagę na różnicę w zaskarżalności postanowień. Dostawca usług hostingowych, usług łączności i inne podmioty, o których mowa w art. 218a § 1 k.p.k. mogą zaskarżyć decyzję o zabezpieczeniu danych w terminie 7 dni od daty doręczenia postanowienia. Wniesienie zażalenia nie wstrzymuje jednak wykonania decyzji o zabezpieczeniu (w tym decyzji o uniemożliwieniu dostępu), zgodnie z art. 462 § 1 k.p.k. Warto także podkreślić, że w odniesieniu do podmiotów zobowiązanych do wykonania postanowienia z art. 218a § 1

⁶⁵ Przestępstwo jest zagrożone karą od 3 miesięcy do 5 lat pozbawienia wolności.

⁶⁶ Przestępstwo jest zagrożone karą do 3 lat pozbawienia wolności.

⁶⁷ Przestępstwo jest zagrożone karą od 3 miesięcy do 5 lat pozbawienia wolności. Tej samej karze podlega, kto w celu popełnienia przestępstwa o charakterze terrorystycznym uczestniczy w szkoleniu mogącym umożliwić popełnienie takiego przestępstwa lub samodzielnie zapoznaje się z treściami umożliwiającymi popełnienie przestępstwa o charakterze terrorystycznym.

⁶⁸ M.in. wytwarzanie środków odurzających (art. 53), przywóz, wywóz, przewóz, wewnątrzwspólnotowe nabycie, wewnątrzwspólnotowa dostawa środków odurzających, substancji psychotropowych, nowych substancji psychoaktywnych lub słomy makowej (art. 55), wprowadzanie do obrotu środków odurzających (art. 56), udzielanie innej osobie środka odurzającego (art. 58), czy posiadanie środków odurzających (art. 62).

⁶⁹ Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (t.j. Dz. U. z 2023 r. poz. 1939 z późn. zm.).

k.p.k. nie znajduje zastosowania art. 218 § 2 zd. 2 k.p.k., tj. możliwość odroczenia doręczenia postanowienia o zabezpieczeniu danych.

Jeśli zostanie stwierdzone, że publikacja lub udostępnienie treści stanowiło czyn zabroniony, o którym mowa w art. 218a § 1 k.p.k., sąd lub prokurator może zarządzić usunięcie tych treści. Usunięcie tych treści powinno nastąpić w sposób zabezpieczający przed ich nieuprawnionym odzyskaniem (§ 9 ust. 1 rozporządzenia Ministra Sprawiedliwości z dnia 18 czerwca 2021 r. w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji do gromadzenia danych informatycznych oraz danych niestanowiących treści rozmowy telefonicznej lub innego przekazu informacji, a także sposobów ich zabezpieczania w urządzeniach zawierających te dane oraz w systemach i na informatycznych nośnikach danych)⁷⁰.

Patrząc pod kątem konstrukcyjnym na art. 218a k.p.k., to mechanizm wynikający z tego przepisu umożliwia:

- zabezpieczenie danych w celach dowodowych (cel zasadniczy art. 218a k.p.k.);
- uniemożliwienie dostępu do danych w przypadku podejrzenia, że dane/treści te stanowią jeden z czynów zabronionych z art. 218a § 1 k.p.k.
- trwałe usunięcie danych informatycznych w przypadku stwierdzenia, że treści stanowią jeden z czynów zabronionych z art. 218a § 1 k.p.k. Jeśli w toku postępowania karnego nie stwierdzono, że treści przesyłane drogą elektroniczną nie realizują znamion jednego z czynów zabronionych wymienionych w art. 218a § 1 k.p.k., należy niezwłocznie dane zwolnić spod zabezpieczenia.

Porównując obie instytucje – art. 23 dyrektywy 2024/1385 i art. 218a k.p.k. – to z perspektywy ich konstrukcji, są one zbliżone. Obie dotyczą uniemożliwienia dostępu do treści, które mogą realizować znamiona określonych czynów zabronionych, zabezpieczenia treści w celach dowodowych, a także – po stwierdzeniu, że doszło do popełnienia przestępstwa – trwałego usunięcia treści i danych. Inaczej rozłożone są jednak akcenty. Przepisy k.p.k. koncentrują się na kwestiach dowodowych (zabezpieczenie w celach dowodowych), zaś dyrektywa – na ochronie pokrzywdzonych przed wtórną wiktymizacją, i szybkim „zdjęciu” z internetu/przestrzeni cyfrowej danych mogących stanowić jedno z przestępstw wskazanych w art. 23 ust. 1 dyrektywy 2024/1385, a cel dowodowy jest niejako na

⁷⁰ Dz. U. poz. 1101.

drugim planie. Oznacza to, że ustawodawca chcąc implementować art. 23 dyrektywy 2024/1385 nie musi tworzyć zupełnie nowego mechanizmu. Już istnieje on w prawie krajowym i wymaga jedynie dostosowania do wymagań wynikających z prawa unijnego.

Po pierwsze, konieczne jest rozszerzenie katalogu czynów zabronionych, w sprawach o które sąd lub prokurator będą mogli żądać uniemożliwienia dostępu do treści/danych przesyłanych drogą elektroniczną.

Obecnie, jak to zostało już wcześniej wskazane, przepis art. 218a § 1 k.p.k. pozwala na czasowe „zdjęcie” danych w sprawach o przestępstwa określone w art. 200b k.k., art. 202 § 3, 4, 4a, 4b k.k. lub art. 255a k.k. oraz w rozdziale 7 ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii. Katalog ten musi zostać rozszerzony o art. 190a i 191a k.k., a także o przepisy kryminalizujące rozpowszechnianie deepfake’ów przedstawiających osoby dorosłe w kontekstach seksualnych (art. 5 lit. a i b dyrektywy 2024/1385), cyberflashing (art. 7 lit. c dyrektywy 2024/1385), doxing (art. 7 lit. d dyrektyw 2024/1385) oraz treści, które stanowią mowę nienawiści motywowaną płcią (art. 8 dyrektyw 2024/1385). Pełna implementacja art. 23 dyrektywy 2024/1385 jest możliwa tylko wtedy, gdy ustawodawca dostosuje przepisy prawa karnego materialnego do wymagań, jakie wynikają z prawa unijnego.

Po drugie, wydaje się, że art. 218a k.p.k. wprowadza z jednej strony bardzo szeroki katalog podmiotów, a jednocześnie – nie obejmuje wszystkich dostawców usług, o których mowa w art. 23 dyrektywy 2024/1385.

Przepis art. 218a § 1 k.p.k. mówi o „urzędach, instytucjach i podmiotach prowadzących działalność telekomunikacyjną lub świadczących usługi drogą elektroniczną oraz dostawcach usług cyfrowych”, zaś art. 23 ust. 2 dyrektywy 2024/1385 o „dostawcach usług hostingowych” oraz „dostawcach usług pośrednich, innych niż dostawcy usług hostingowych, którzy mają techniczną i operacyjną zdolność podjęcia działań w odniesieniu do danych treści”. Pojawia się pytanie, czy pojęcia „dostawca usług cyfrowych” i „dostawca usług hostingowych” mają taki sam zakres pojęciowy.

Ministerstwo Cyfryzacji nie udziela precyzyjnej odpowiedzi na takie pytanie⁷¹. Nie ma także definicji legalnych obu pojęć. Opierając się na definicjach z rozporządzenia DSA (akt o usługach cyfrowych), usługa hostingu jest usługą pośrednią polegającą na przechowywaniu informacji przekazanych przez odbiorcę usługi oraz na jego żądanie (art. 3 lit. g pkt iii). Przechowywanie informacji może odbywać się na serwerach, w chmurze itp. Usługi cyfrowe nie zostały zdefiniowane w rozporządzeniu DSA. Wydaje się jednak, że pojęcie „dostawca usług cyfrowych” niekoniecznie obejmuje „dostawcę usług hostingowych”. Przykładowo, wyszukiwarki internetowe i ich funkcjonowanie są świadczeniem usługi cyfrowej, ale nie jest to świadczenie usługi hostingowej – żadne informacje nie są bowiem przechowywane. Dostawcy usług hostingowych zapewniają infrastrukturę np. serwery, a dostawca usług cyfrowych zarządza interakcjami użytkowników. Na gruncie instytucji z art. 218a k.p.k. objęcie zakresem tego przepisu także dostawców usług hostingowych jest o tyle istotne, że trwałe usunięcie treści stanowiących czyn zabroniony, nie będzie możliwe bez zaangażowania tych podmiotów. Dostawca usług cyfrowych nie będzie w stanie trwale usunąć określonych materiałów z przestrzeni cyfrowej – może jedynie uniemożliwiać do nich dostęp.

Celowe jest albo wprowadzenie definicji legalnej „dostawcy usług cyfrowych” obejmującej także „dostawcę usług hostingowych” albo rozszerzenie katalogu podmiotów zobowiązanych do wykonania postanowienia z art. 218a § 1 k.p.k. o kategorię „dostawców usług hostingowych”.

Po trzecie, konieczne jest uzupełnienie art. 218a k.p.k. o notyfikację decyzji o uchyleniu zabezpieczenia danych informatycznych.

Obecnie, przepisy nie precyzują trybu, w jaki sposób podejrzany i pokrzywdzony – jeśli uczestniczą w postępowaniu w charakterze stron – są informowani o zwolnieniu danych

⁷¹ Na stronie internetowej Ministerstwa Cyfryzacji można znaleźć takie pytanie: „Czy w rozumieniu Art. 17. ust. 1. oraz Załącznika nr 2 do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, usługodawca hostingowy jest dostawcą usługi cyfrowej?”, na które Ministerstwo udziela takiej odpowiedzi: „Zgodnie Dyrektywą NIS dostawcą usługi cyfrowej jest każda osoba prawna, która świadczy usługę cyfrową, czyli taką usługę, która jest świadczona za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usługi. Do usług cyfrowych w rozumieniu ustawy o ksc zaliczamy: internetową platformą handlową, wyszukiwarką internetową lub usługą przetwarzania w chmurze.”; <https://www.gov.pl/web/cyfryzacja/dostawcy-uslug-cyfrowych3>. Dyrektywa NIS już nie obowiązuje (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii; Dz. U. UE. L. z 2016 r. Nr 194, str. 1) – została zastąpiona dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE. L. z 2022 r. Nr 333, str. 80 z późn. zm.).

spod zabezpieczenia, a także, czy do decyzji z art. 218a § 2 k.p.k. może znaleźć zastosowanie odroczenie doręczenia postanowienia, o którym mowa w art. 218 § 2 zd. 2 k.p.k. Wydaje się – że wobec braku odesłania – nie można odroczyć doręczenia postanowienia o zwolnieniu danych informatycznych spod zabezpieczenia. Prowadzi to jednak do sytuacji, w której – przynajmniej teoretycznie – podejrzanemu może nie zostać doręczone postanowienie z art. 218a § 1 k.p.k., ponieważ prokurator podjął decyzję o odroczeniu doręczenia tej decyzji procesowej, a jednocześnie – zostanie mu doręczona niezwłocznie decyzja (postanowienie) o zwolnieniu danych spod zabezpieczenia). I postanowienie o zabezpieczeniu i uniemożliwianiu dostępu do danych oraz postanowienie o zwolnieniu danych spod zabezpieczenia są zaskarżalne na zasadach określonych w art. 236 k.p.k. Nie może jednak dojść do sytuacji, w której podmiot uprawniony będzie mógł zaskarżyć postanowienie z art. 218a § 2 k.p.k. (np. pokrzywdzony będzie mógł wnieść zażalenie na postanowienie o zwolnieniu danych spod zabezpieczenia), a podejrzany nie będzie mógł zaskarżyć – z uwagi na brak doręczenia postanowienia – postanowienia z art. 218a § 1 k.p.k. Przepis art. 218a k.p.k. powinien w sposób autonomiczny regulować problematykę odroczenia doręczenia postanowienia o zabezpieczeniu danych, uniemożliwianiu dostępu do danych oraz zwolnieniu spod zabezpieczenia. O ile w przypadku zabezpieczenia danych – bez podejmowania dalszych kroków w postaci uniemożliwienia dostępu do danych – odroczenie doręczenia postanowienia prokuratora lub sądu może być celowe w określonych sytuacjach, to w przypadku decyzji o zabezpieczeniu danych i uniemożliwianiu dostępu do danych takie odroczenie doręczenia postanowienia nie wydaje się sensowne. Podejrzany (albo osoba podejrzana, jeśli w sprawie nie zostały jeszcze przedstawione zarzuty) zorientuje się bowiem, że nie może np. zalogować się na swoje konto w chmurze albo że treści, które publikował/publikowała „zniknęły” z jego social mediów. Dodatkowo, art. 218a k.p.k. powinien wprost wskazywać, jakim podmiotom doręcza się decyzje procesowe wskazane w tym przepisie, analogicznie jak to reguluje art. 218 § 2 zd. 1 k.p.k.

Podsumowując, dla dostosowania przepisów krajowych do treści art. 23 dyrektywy 2024/1385 wystarczające jest doprecyzowanie obecnie istniejącego mechanizmu z art. 218a k.p.k. przez:

- rozszerzenie katalogu czynów wskazanych w art. 218a § 1 k.k. o art. 190a § 1 k.k. i art. 191a § 1 k.k. oraz nowych typów czynów zabronionych, które powinny zostać wprowadzone do krajowego porządku prawnego w związku z wdrożeniem art. 5 lit. a i b, art. 7 i 8 dyrektywy 2024/1385;

- doprecyzowanie kręgu adresatów nakazu zabezpieczenia, uniemożliwienia dostępu i usunięcia danych/treści tak, by nie było wątpliwości, że adresatem postanowienia z art. 218a § 1 k.p.k. może być także dostawca usług hostingowych;
- doprecyzowanie przepisów odnoszących się do poinformowania o uchyleniu nakazu zabezpieczenia danych i uniemożliwienia dostępu do danych.

Mając na uwadze przedłożone racje, stosownie do art. 16 ust. 2 pkt 1 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich⁷², zwracam się do Pani Minister i Pana Ministra z uprzejmą prośbą o udzielenie następujących informacji:

- czy w Ministerstwie Sprawiedliwości prowadzone są prace legislacyjne, we współpracy z Pełnomocnik ds. Równości, w celu wdrożenia dyrektywy 2024/1385 i dokonania niezbędnych zmian w przepisach prawa karnego materialnego i procesowego dostosowujących polskie przepisy do wymagań, jakie wynikają z członkostwa w Unii Europejskiej;
- czy w Ministerstwie Sprawiedliwości prowadzone są prace legislacyjne także w szerszym zakresie niż wynika to z dyrektywy 2024/1385, tj. w celu dokonania niezbędnych zmian w przepisach prawa karnego materialnego i procesowego, które będą wprowadzały skuteczne mechanizmy umożliwiające m.in. usuwanie treści, w których gromadzone są zbiory materiałów/danych, przedstawiających wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej bez zgody tej osoby.

Proszę także uprzejmie o poinformowanie mnie o stanowisku zajęтым wobec przedstawionych problemów i postulatów natury legislacyjnej.

Z wyrazami szacunku

Sylwia Gregorczyk-Abram

Rzecznik Praw Obywatelskich

/-wydano i podpisano elektronicznie/

⁷² Ustawa z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2024 r., poz. 1264 ze zm.).

