Stanowisko Rady do Spraw Cyfryzacji w sprawie optymalizacji zwalczania cyberprzestępczości ukierunkowanej na osiągnięcie korzyści finansowych przez sprawców.

Cyberprzestępczość ukierunkowana na osiągnięcie korzyści finansowych przez sprawców stała się jednym z najpoważniejszych zagrożeń dla bezpieczeństwa obywateli, zaufania do usług cyfrowych oraz stabilności rynku finansowego.

Z opublikowanego w kwietniu 2026 r. raportu CERT Polska podsumowującego rok 2025 wynika, że zespół otrzymał 658 320 zgłoszeń. Na ich podstawie zarejestrowano 260 783 unikalne incydenty bezpieczeństwa, przy czym aż 97% sklasyfikowano jako oszustwa komputerowe. W tej kategorii incydentów sklasyfikowano zarówno wyłudzenia poufnych danych, takich jak loginy i hasła do poczty elektronicznej, serwisów bankowych, portali społecznościowych czy innych usług online, fałszywe sklepy internetowe oraz oszustwa inwestycyjne, w których przestępcy podszywali się pod koncerny paliwowo-energetyczne, firmy, instytucje, wykorzystywali też wizerunki znanych osób. CERT Polska wskazuje jednocześnie na gwałtowny wzrost skali zagrożeń, gdyż liczba zarejestrowanych incydentów wzrosła rok do roku o ponad 152%. Szczególnie niepokojąca pozostaje skala phishingu i smishingu. W 2025 r. do CERT Polska zgłoszono blisko 295 tys. podejrzanych wiadomości SMS, a dzięki systemowi wzorców fałszywych wiadomości zablokowano ponad 1,88 mln złośliwych SMS-ów. Na listę ostrzeżeń CERT Polska wpisano niemal 245 tys. niebezpiecznych domen, co pozwoliło zablokować ponad 141 mln prób wejścia użytkowników na strony służące wyłudzeniom.

Zdecydowana większość obserwowanych cyberataków nakierowana jest finalnie na osiągnięcie korzyści finansowych przez sprawców. Ukierunkowane na monetyzację są nie tylko grupy odpowiedzialne za oszustwa w serwisach aukcyjnych i społecznościowych, fałszywe sklepy internetowe, oszustwa inwestycyjne, BEC, CEO fraud, oszustwa na legendę, love scam czy ransomware, ale również grupy tworzące strony podszywające się pod panele logowania do poczty elektronicznej, mediów społecznościowych, bankowości elektronicznej czy zajmujące się infekowaniem użytkowników internetu złośliwym oprogramowaniem. Tam również finalnie celem sprawców najczęściej jest korzyść finansowa (wyłudzanie kodów BLIK po przejęciu dostępu do mediów społecznościowych, kradzież środków z rachunku bankowego po wyłudzeniu danych do logowania do bankowości elektronicznej na stronie podszywającej się pod bank lub pozyskaniu ich w wyniku działania złośliwego oprogramowania). Incydenty te stanowią jedocześnie czyny zabronione, podlegające ściganiu karnemu. Analiza struktury przestępstw finansowych oraz cyberprzestępstw wskazuje, że dominującą kwalifikacją prawną dla rejestracji postępowań z tego zakresu jest art. 286 § 1 k.k. określający znamiona przestępstwa oszustwa. Jednocześnie artykuł ten jest najczęstszą podstawą rejestracji postępowań karnych w prokuraturze. Dodatkowo należy podkreślić, że ponad połowa oszustw w policyjnych bazach danych oznaczana jest jako popełniona online.

Szczególnie alarmująca pozostaje skala oszustw inwestycyjnych wymierzonych w klientów rynku finansowego. Z Raportu Rocznego CSIRT KNF za 2025 r. wynika, że zespół zidentyfikował i zgłosił do blokady 41 751 niebezpiecznych domen (ponad 50 tys. w roku 2024), z czego aż 40 225 domen (ponad 96,3%) było związanych z fałszywymi inwestycjami. CSIRT KNF podkreśla, że oszuści coraz częściej wykorzystują zaawansowaną socjotechnikę, reklamy typu „lead ads", a także wizerunki polityków, celebrytów, przedsiębiorców i instytucji finansowych w celu uwiarygodnienia przestępstwa. Dominującym kanałem dystrybucji pozostają reklamy publikowane w mediach społecznościowych, wyszukiwarkach oraz popularnych serwisach internetowych. W odpowiedzi na skalę zjawiska CSIRT KNF doprowadził w 2025 r. do zablokowania 9 751 oszukańczych reklam oraz 4 358 profili publikujących fałszywe treści inwestycyjne.

Rada ds. Cyfryzacji wskazuje, że cyberbezpieczeństwo sektora finansowego nie może być rozumiane wyłącznie jako bezpieczeństwo instytucji finansowych. Głównym celem ataku jest obywatel - konsument, klient bankowości elektronicznej, senior, a państwo powinno zapewnić mu realną ochronę, a więc szybkie zgłaszanie incydentów oraz cyberprzestępstw, realną ochronę środków finansowych, szybką reakcję, skuteczną odpowiedzialność platform, efektywne procedury zabezpieczenia dowodów oraz skuteczną karnoprawną reakcję organów ścigania i wymiaru sprawiedliwości.

Wysoka skala naruszeń oraz niska skuteczność zwalczania cyberprzestępczości powinna skłonić do podjęcia realnych działań mających na celu zapewnienie bardziej skutecznych proaktywnych i reaktywnych narzędzi prowadzących do lepszej ochrony osób korzystających z usług online.

Skala zjawiska oraz jego dynamika wskazują, że obecny model przeciwdziałania cyberprzestępczości finansowej nie jest wystarczająco skuteczny. Konieczne jest przejście od modelu reaktywnego do modelu proaktywnego, opartego na odpowiedzialności systemowej platform, szybkiej wymianie danych oraz mechanizmie „follow the money". Rada identyfikuje trzy kluczowe obszary wymagające pilnej interwencji:

a) odpowiedzialność platform i reklamy,

b) dostęp do danych i środków finansowych,

c) skuteczność narzędzi karnoprawnych.

Rekomendacje Rady

1. Pilne wdrożenie DSA oraz wzmocnienie egzekucji prawa wobec platform.

Rada rekomenduje jak najszybsze zakończenie prac nad nowelizacją ustawy o świadczeniu usług drogą elektroniczną oraz stworzenie realnych narzędzi egzekwowania obowiązków platform. DSA ma wzmacniać ochronę przed oszustwami, manipulacją, nieuczciwym profilowaniem, zwiększać przejrzystość reklam i algorytmów oraz umożliwiać wydawanie nakazów wobec treści nielegalnych.

Rada rekomenduje, aby przepisy krajowe wyraźnie przewidywały:

- obowiązek priorytetowego rozpoznawania zgłoszeń dotyczących oszustw finansowych, fałszywych inwestycji i deepfake w reklamach;
- możliwość nakazania platformie natychmiastowego ograniczenia widoczności reklamy lub treści, gdy zachodzi wysokie prawdopodobieństwo oszustwa;
- wysokie administracyjne kary finansowe za brak reakcji na powtarzalne kampanie promujące strony internetowe wyłudzające dane oraz doprowadzające użytkowników internetu do niekorzystnego rozporządzenia ich mieniem, w tym w szczególności za brak reakcji na zgłoszenia krajowych zespołów CSIRT;
- obowiązek stosowania listy ostrzeżeń i wysokie administracyjne kary finansowe za nieblokowanie przekierowania na domeny internetowe objęte listą ostrzeżeń prowadzoną przez CSIRT NASK na podstawie ustawy o zwalczaniu nadużyć w komunikacji elektronicznej[1];
- obowiązek analizowana i zgłaszania nieprawidłowości w zakresie publikowanych na platformie reklam finansowych, obejmujący również przekazywania danych organom ścigania (kto zapłacił, jaki podmiot był reklamodawcą, jaki był zasięg, komu reklama była targetowana i jakie domeny promowała);

W szczególności należy traktować masowe kampanie oszustw inwestycyjnych jako systemowe ryzyko w rozumieniu art. 34 DSA, co uzasadnia stosowanie środków nadzorczych wobec bardzo dużych platform internetowych (VLOPs).

2. Zakaz anonimowej i niemożliwej do zweryfikowania reklamy usług finansowych.

Rada rekomenduje wprowadzenie zasady „poznaj swojego reklamodawcę" dla reklam finansowych i inwestycyjnych. Platforma, wyszukiwarka lub sieć reklamowa nie powinna emitować reklamy inwestycji, kryptoaktywów, pośrednictwa finansowego, kredytów, obligacji, akcji lub „łatwego zarobku" bez uprzedniej weryfikacji reklamodawcy.

Wymóg powinien obejmować weryfikację tożsamości i beneficjenta rzeczywistego reklamodawcy, sprawdzenie, czy podmiot ma wymagane zezwolenia lub nie figuruje na liście ostrzeżeń publicznych, obowiązek przechowywania danych reklamodawcy i kampanii przez co najmniej 24 miesiące, odpowiedzialność administracyjną platformy za powtarzające się dopuszczanie publikacji reklam, które w sposób oczywisty są reklamami promujące strony internetowe wyłudzające dane, w tym dane osobowe, oraz doprowadzające użytkowników internetu do niekorzystnego rozporządzenia ich mieniem oraz reklamami, w którym bez uprawnienia wykorzystano wizerunek innej osoby.

Rada wskazuje ponadto, że największe platformy społecznościowe nie pełnią już wyłącznie funkcji prywatnych serwisów wymiany treści. Ich wpływ na debatę publiczną, decyzje

[1] Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1803 z późn. zm.)

konsumenckie i bezpieczeństwo finansowe obywateli uzasadnia nałożenie podwyższonych obowiązków przejrzystości, rzetelności reklam, reagowania na oszustwa i współpracy z państwem. Nie oznacza to zrównania każdego użytkownika z nadawcą medialnym, lecz oznacza, że platformy zarabiające na dystrybucji treści i reklam powinny ponosić odpowiedzialność za systemowe tolerowanie scamów.

W przypadku uzyskiwania przez platformę przychodów z kampanii reklamowych, które okażą się kampaniami oszukańczymi, należy rozważyć wprowadzenie mechanizmu:

- obowiązku zwrotu uzyskanych przychodów,
- partycypacji w naprawieniu szkody użytkownikom, w przypadku braku dochowania należytej staranności w weryfikacji reklamodawcy.

3. Utrzymanie aktualnej długości retencjonowania danych telekomunikacyjnych oraz zwiększenie wiarygodności rejestracji przedpłaconych kart SIM i eSIM.

Rada sprzeciwia się skracaniu okresu retencji danych telekomunikacyjnych w sposób, który uniemożliwi lub utrudni skuteczne prowadzenie postępowań karnych. Obecne ustawa - Prawo komunikacji elektronicznej[2] przewiduje zatrzymywanie i przechowywanie określonych danych przez okres 12 miesięcy. Dane objęte obowiązkiem obejmują m.in. informacje konieczne do identyfikacji użytkownika, urządzenia, daty i godziny połączenia, czasu trwania, rodzaju połączenia oraz lokalizacji urządzenia końcowego. Rada rekomenduje utrzymanie 12-miesięcznej ogólnej retencji jako niezbędnej dla przeprowadzania ustaleń faktycznych w postępowaniach karnych. Skrócenie tego okresu spowoduje, że w praktyce organy ścigania nie będą miały faktycznej możliwości przeprowadzenia ustaleń w oparciu o dane telekomunikacyjne, albowiem ustalenia te zazwyczaj muszą być poprzedzone realizacją innych czynności – przesłuchaniem świadków, pozyskaniem danych (w tym w szczególności logów) od dostawców usług świadczonych elektronicznie czy banków. Jednocześnie postulowane rozwiązania powinny być wdrażane z zachowaniem standardów wynikających z orzecznictwa TSUE i ETPC, w szczególności zasady proporcjonalności i celowości przetwarzania danych.

Dodatkowo należy wskazać, że obowiązujące regulacje dotyczące rejestracji kart SIM typu pre-paid nie zapewniają wystarczającej kontroli nad skalą i strukturą ich nabywania oraz aktywacji, co ogranicza możliwość wczesnego identyfikowania zjawisk o charakterze nadużyć w komunikacji elektronicznej. Dopuszczenie pośredniej identyfikacji abonenta przez osoby trzecie działające w imieniu dostawcy usług telekomunikacyjnych obniża dodatkowo jednolitość i jakość stosowanych procedur weryfikacyjnych oraz osłabia zaufanie do danych rejestrowych oraz skuteczność systemu przeciwdziałania nadużyciom w komunikacji elektronicznej. Co więcej na wielu stronach internetowych oferowane są usługi rejestracji kart na dane osób trzecich. Wykorzystywanie zarejestrowanych kart SIM przez osoby inne niż

[2] Ustawa z dnia 12 lipca 2024 r. - Prawo komunikacji elektronicznej (Dz. U. poz. 1221 z późn. zm.)

formalny abonent umożliwia sprawcom ukrycie tożsamości, rozproszenie odpowiedzialności karnej oraz utrudnia identyfikację i ściganie sprawców przestępstw.

Aktualna regulacja sprzyja anonimowej komunikacji wykorzystywanej w działalności przestępczej i nie realizuje celów dla jakich rejestracja kart typu pre-paid została wprowadzona.

Rada rekomenduje w tym zakresie:

- wzmocnienie systemowej kontroli nad rynkiem kart SIM i eSIM typu pre-paid poprzez wprowadzenie jednolitych, bezpośrednich i weryfikowalnych standardów identyfikacji abonenta oraz mechanizmów raportowania przypadków ponadnormatywnego rejestrowania kart;
- wprowadzenie obowiązku zgłaszania przypadków masowej rejestracji kart SIM oraz eSIM;
- Wprowadzenie zakazu obrotu zarejestrowanymi kartami SIM lub obowiązku niezwłocznego nierejestrowania zakupionej karty SIM;
- Prowadzenie sankcji za rejestrowanie kart SIM lub eSIM na dane osoby nieistniejącej oraz na dane innej osoby bez jej wiedzy lub zgody, w szczególności w celu ich dalszego odpłatnego zbywania lub udostępniania osobom trzecim;
- obowiązek korzystania z mechanizmów listy ostrzeżeń prowadzonej na podstawie ustawy o zwalczaniu nadużyć w komunikacji elektronicznej przez wszystkich dostawców usług dostępu do Internetu.

Zjawisko masowej rejestracji kart SIM powinno być traktowane jako potencjalny wskaźnik ryzyka w systemach przeciwdziałania praniu pieniędzy (AML) oraz podlegać raportowaniu do właściwych organów.

4. Standard przekazywania danych przez podmioty świadczące usługi drogą elektroniczną.

Rada rekomenduje ustawowe określenie minimalnego standardu logów oraz okresu ich przechowywania dla podmiotów świadczących usługi hostingu, poczty elektronicznej oraz innych usług pośrednich, w zakresie, w jakim przechowują lub transmitują dane niezbędne do identyfikacji incydentu, w szczególności obejmującego datę i godzinę zdarzenia wraz ze strefą czasową, adres IP oraz port, identyfikator użytkownika lub konta, identyfikator sesji lub urządzenia, informacje o logowaniu, zmianie danych uwierzytelniających oraz dane pozwalające na odtworzenie przebiegu incydentu. Postulowane rozwiązania powinny uwzględniać zasadę proporcjonalności i minimalizacji danych oraz pozostawać adekwatne do charakteru świadczonej usługi.

5. Szybki proces zgłaszania incydentów i cyberprzestępstw.

Rada rekomenduje stworzenie jednego publicznego punktu zgłaszania incydentów zarówno do krajowych zespołów CSIRT, PUODO, policji i prokuratury. System powinien umożliwiać automatyczną kwalifikację zgłoszenia według rodzaju incydentu oraz automatyczne

przekazywanie go do właściwego organu, bez konieczności ponownego składania zawiadomienia przez pokrzywdzonego.

Jednocześnie pokrzywdzony powinien mieć automatycznie przekazywane instrukcje, co zrobić w pierwszych minutach po ataku. Instrukcje te powinny obejmować także sposób zabezpieczenia materiału dowodowego, w szczególności linków, zrzutów ekranu, numerów rachunków, numerów telefonów, identyfikatorów reklam, wiadomości SMS i e-mail oraz danych o czasie zdarzenia. Celowe jest również rozbudowanie funkcjonalności w aplikacji mObywatel o możliwość przesłania zawiadomienia o podejrzeniu popełnienia cyberprzestępstwa.

Rada wskazuje na konieczność stałego podnoszenia cyberhigieny oraz budowania wiedzy i umiejętności zgłaszania incydentów (np. poprzez kampanie edukacyjne państwa „Zgłoś w 15 minut"). Obywatel powinien wiedzieć, że w przypadku cyberprzestępstw szczególne znaczenie odgrywa czas, zatem niezbędna jest wiedza o sposobach reakcji, w zależności od rodzaju przestępstwa (zgłaszanie reklamacji w banku, nr 8080, zgłaszanie incydentów, składanie zawiadomienia o podejrzeniu popełnienia przestępstwa) oraz o tym w jakie dane są niezbędne do podjęcia działań przez podmioty zobowiązane.

6. Zapewnienie skutecznych mechanizmów „follow the money".

Znajomość sposobów działania sprawców prowadzi do wniosku, że to dostęp do informacji stanowiących tajemnicę bankową w aktualnym kształcie prawnym jest krytycznym mechanizmem wpływającym negatywnie na skuteczność organów ścigania w walce z przestępczością ekonomiczną i cyberprzestępczością nakierowaną na monetyzację.

Sprawcy oszustw działają w celu doprowadzenia innych osób do niekorzystnego rozporządzenia mieniem, zatem podążanie za przepływami finansowymi jest najskuteczniejszą metodą wykrywczą. Kluczowym elementem skuteczności mechanizmów „follow the money" jest czas reakcji – dostęp do danych oraz możliwość zabezpieczenia środków powinny być realizowane w ramach godzin, a nie dni czy tygodni. Opóźnienia w tym zakresie powodują, że środki finansowe są nieodwracalnie wyprowadzane i poddawane dalszemu praniu, co istotnie ogranicza możliwość ich odzyskania przez pokrzywdzonych.

Pamiętać należy jednak, że sprawcy cyberprzestępstw dbając o zachowanie własnej anonimowości, ukrywają własną tożsamość. Do przyjmowania korzyści finansowych z przestępstw posługują się wieloma rachunkami założonymi na dane innych osób (tzw. słupów), kontami na giełdach kryptowalut założonymi na dane innych osób (w tym również pokrzywdzonych) oraz stosują różne mechanizmy utrudniające analizę przepływów finansowych.

Tryb dostępu prokuratora do informacji objętych tajemnicą bankową jest zróżnicowany i zależny od fazy postępowania (tzn. czy jest ono prowadzone w sprawie czy przeciwko osobie fizycznej będącej dysponentem rachunku bankowego), dysponenta rachunku bankowego (osoba fizyczna, osoba prawna lub jednostka organizacyjna niemająca osobowości prawnej),

o jakie czyny prowadzone jest postępowanie (szczególna regulacja odnosi się do przestępstwa prania pieniędzy i finansowania przestępstwa o charakterze terrorystycznym).

Aktualnie, poza przypadkami określonymi w art. 105 i art. 106a ustawy Prawo bankowe[3] prokurator może żądać od banku, osób zatrudnionych w banku oraz osób, za pośrednictwem których bank wykonuje czynności bankowe, udzielenia informacji stanowiących tajemnicę bankową jedynie na podstawie postanowienia wydanego na jego wniosek przez właściwy miejscowo sąd okręgowy. Jeśli zatem postępowanie prowadzone jest w sprawie (faza in rem) i obejmuje kwalifikacje bazowe takie jak oszustwo (art. 286 k.k.), oszustwo komputerowe (art. 287 k.k.) czy hacking (art. 267 k.k.), poza przypadkami określonymi w art. 105 i art. 106a, prokurator prowadzący postępowanie może żądać od banku oraz osób, za pośrednictwem których bank wykonuje czynności bankowe, udzielenia informacji stanowiących tajemnicę bankową, jedynie na podstawie postanowienia wydanego na jego wniosek przez właściwy miejscowo sąd okręgowy. Po rozpatrzeniu wniosku sąd, w drodze postanowienia, wyraża zgodę na udostępnienie informacji, określając ich rodzaj i zakres, osobę lub jednostkę organizacyjną, których dotyczą oraz podmiot zobowiązany do ich udostępnienia, albo odmawia udzielenia zgody na udostępnienie informacji.

Podczas gdy sprawcy operują na wielu rachunkach bankowych używanych do przestępstw (najczęściej założonych na dane tzw. słupów), a przelewy i operacje bankowe realizowane są niemal natychmiastowo, uzyskanie po tygodniach lub miesiącach informacji objętych tajemnicą bankową sprowadza się najczęściej do biernego odtwarzania kolejnych przelewów i kierowania kolejnych wniosków, podczas gdy pieniądze pokrzywdzonych są bezpowrotnie tracone i poddawane praniu.

Mając na względzie powyższe należy albo jednolicie przyjąć, że prokurator może zawsze samodzielnie zwolnić bank z zachowania tajemnicy bankowej, albo co najmniej, że może samodzielnie zwolnić bank z tajemnicy bankowej w zakresie przestępstw katalogowych wskazanych w art. 3 pkt 6 ustawy o Systemie Informacji Finansowej[4].

Dodatkowo konieczne jest doprecyzowanie obowiązków banków i innych instytucji finansowych w zakresie gromadzenia i przekazywania informacji i danych informatycznych dotyczących prowadzonych rachunków bankowych i innych usług oraz produktów za pośrednictwem zdalnych kanałów dostępowych (sieci Internet). W informacjach przekazywanych przez banki, niejednokrotnie brakuje informacji o porcie przypisanym do ustalonego adresu IP. Tak przekazana informacja często uniemożliwia organom ścigania ustalenie sprawcy czynu zabronionego, gdyż informacja o adresie IP bez portu, wskazuje nam na dane wielu osób, które korzystały z danego publicznego adresu IP w ustalonej dacie i godzinie.

Należy mieć również na uwadze, że cyberprzestępcy, aby utrudnić analizę przepływów pieniężnych na wstępnym etapie prania pieniędzy bardzo często dokonują ich wypłat w

[3] Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2024 r. poz. 1646 z późn. zm.)
[4] Ustawa z dnia 1 grudnia 2022 r. o Systemie Informacji Finansowej (Dz. U. z 2023 r. poz. 180)

bankomatach w Polsce, a następnie wpłat we wpłatomatach lub bitomatach. Aktualna procedura zwolnienia z tajemnicy bankowej sprawia, że nawet jeśli bankomat wyposażony był w monitoring, nie ma możliwości zabezpieczenia nagrań z monitoringu, z uwagi na krótki czas ich przechowywania. Dotyczy to również monitoringu z miejsca dojścia i odejścia od bankomatu. Powoduje to oprócz wymiernych strat finansowych, dodatkowe przeświadczenie u cyberprzestępców o opłacalności popełniania tego typu przestępstw, a w konsekwencji eskalację zjawiska. Co więcej brak jest nałożonych na banki, właścicieli lub posiadaczy bankomatu lub wpłatomatu obowiązków związanych z rejestrowaniem wizerunku osób korzystających z usług bankomatu oraz przechowywanie zarejestrowanych nagrań w ustalonym minimalnym czasie.

Dostrzegając rosnącą ilość oszustw i oszustw komputerowych, rosnącą ilość pokrzywdzonych oszustwami finansowymi oraz niską skuteczność ścigania **Rada rekomenduje:**

- zainicjowanie prac nad zmianami ustawy Prawo bankowe i ujednolicenie trybu zwalniania banku z obowiązku zachowania tajemnicy, wprowadzenie możliwości pozyskiwania przez prokuratora informacji stanowiących tajemnicę bankową w toku postępowania karnego, zarówno w fazie in rem jak i w fazie ad personam, jedynie na podstawie postanowienia prokuratora, bez udziału właściwego miejscowo sądu okręgowego, co najmniej dla przestępstw katalogowych;
- doprecyzowanie obowiązków banków w zakresie gromadzenia i przekazywania danych dotyczących prowadzonych rachunków, niezbędnych w postępowaniach karnych z zakresu cyberprzestępczości;
- nałożenie na banki, właścicieli lub posiadaczy bankomatów lub wpłatomatów obowiązku rejestrowania wizerunku osób korzystających z usług bankomatu oraz przechowywanie zarejestrowanych nagrań przez okres co najmniej 90 dni od dnia wykonania usługi;
- wprowadzenie odpowiedzialności wykroczeniowej za zakrywanie twarzy lub część twarzy w sposób uniemożliwiający identyfikację osoby korzystającej z usług płatniczych przy użyciu bankomatu lub wpłatomatu;
- wprowadzenie rejestru lokalizacji kamer istotnych dla bezpieczeństwa publicznego (obejmujących nagrania przestrzeni publicznej). Rejestr powinien umożliwić ustalenie administratora danych, obszaru objętego przez monitoring, czasu przechowywania nagrań;
- wprowadzenie szybkiego mechanizmu czasowego zabezpieczania lub blokowania środków pieniężnych po zgłoszeniu oszustwa, z następczą kontrolą właściwego organu;
- określenie maksymalnych terminów przekazywania danych oraz reakcji po stronie banków i innych instytucji finansowych w sprawach dotyczących podejrzenia oszustwa lub prania pieniędzy;

- wprowadzenie uproszczonych zasad współpracy między bankami oraz innymi instytucjami finansowymi w celu zatrzymania dalszego transferu środków po wykryciu oszustwa.

7. Szczególna ochrona wizerunku, dóbr osobistych i reputacji przed bezprawnym wykorzystaniem w środowisku cyfrowym.

Rada wskazuje, że cyberprzestępczość ukierunkowana na osiągnięcie korzyści finansowych przez sprawców obejmuje nie tylko bezpośrednie wyłudzenia środków finansowych, lecz również działania polegające na bezprawnym wykorzystaniu wizerunku, głosu, nazwiska, firmy, oznaczeń identyfikujących oraz rozpowszechnianiu nieprawdziwych informacji naruszających dobra osobiste w celu uwiarygodnienia oszustwa, wywarcia presji na odbiorców albo spowodowania szkody reputacyjnej. Zjawiska te obejmują w szczególności podszywanie się pod osoby publiczne, dziennikarzy, przedsiębiorców, instytucje finansowe i media, wykorzystywanie ich wizerunku lub renomy w fałszywych reklamach, materiałach audio-wideo, treściach syntetycznych oraz w kampaniach prowadzących do wyłudzeń danych lub środków pieniężnych.

Rada rekomenduje w tym zakresie:

- wprowadzenie priorytetowego trybu zgłaszania i rozpoznawania przez platformy oraz sieci reklamowe treści polegających na podszywaniu się, bezprawnym wykorzystaniu wizerunku, głosu lub innych oznaczeń identyfikujących oraz treści naruszających dobra osobiste;
- nałożenie na platformy i pośredników reklamowych obowiązku niezwłocznego zabezpieczenia danych dotyczących kampanii, konta reklamowego, płatności, zasięgów oraz powiązanych domen po otrzymaniu wiarygodnego zgłoszenia;
- wprowadzenie obowiązku stosowania skutecznych mechanizmów zapobiegania ponownemu publikowaniu treści już uprzednio uznanych za bezprawne z uwagi na podszywanie się, bezprawne wykorzystanie wizerunku lub naruszenie dóbr osobistych;
- zapewnienie osobom pokrzywdzonym szybkiej i przejrzystej ścieżki dochodzenia usunięcia treści, zabezpieczenia dowodów oraz uzyskania informacji o reklamodawcy lub podmiocie publikującym treść, w granicach przewidzianych prawem;
- rozważenie wprowadzenia odpowiedzialności administracyjnej platform i pośredników reklamowych za powtarzające się tolerowanie kampanii opartych na podszywaniu się, bezprawnym wykorzystaniu wizerunku lub oczywistym naruszeniu dóbr osobistych – w przypadku braku dochowania należytej staranności.

Postulowane rozwiązania powinny dotyczyć wyłącznie treści bezprawnych, w szczególności treści polegających na podszywaniu się, bezprawnym wykorzystaniu wizerunku lub innych oznaczeń identyfikujących, treści oszukańczych oraz treści naruszających dobra osobiste, i powinny być projektowane w sposób zapewniający poszanowanie wolności mediów i

niezależności redakcyjnej; nie mogą one prowadzić do wprowadzenia ogólnego obowiązku monitorowania treści ani ingerencji w legalną działalność redakcyjną mediów, w tym do ingerencji w spory dotyczące prawdziwości informacji, ocen lub dopuszczalnej krytyki w debacie publicznej.

Przez pojęcie „platform" rozumie się platformy internetowe, dostawców usług hostingu, pośredników reklamowych oraz bardzo duże platformy internetowe – w zakresie, w jakim umożliwiają rozpowszechnianie treści lub reklam przez podmioty trzecie.

Regulacja nie powinna obejmować legalnego wykorzystania narzędzi AI w działalności redakcyjnej, jeżeli materiał podlegał weryfikacji, ludzkiej kontroli i odpowiedzialności redakcyjnej.

8. Przegląd karnoprawnej regulacji dotyczącej cyberprzestępczości i wprowadzenie nowych typów czynów zabronionych.

Obecny poziom zagrożenia ustawowego nie odpowiada społecznej szkodliwości przestępczości teleinformatycznej, powszechności zagrożenia przez taką przestępczość oraz gwałtownie rosnącej liczby czynów oraz osób pokrzywdzonych. **Celowe jest zatem dostosowanie kar za określone cyberprzestępstwa – w szczególności z art. 267 k.k.,** z jednoczesnym wprowadzeniem postaci uprzywilejowanych („wypadki mniejszej wagi") oraz względnej skargowości ścigania („jeżeli czyn został popełniony na szkodę osoby najbliższej").

W zakresie przestępstwa kradzieży tożsamości, wskazać należy, że aktualna redakcja art. 190 a § 2 k.k. nie odpowiada celom i zakresowi działania sprawców cyberprzestępstw. Wykorzystanie tożsamości może być zarówno głównym celem sprawców, jak również środkiem do osiągnięcia innego celu (ukrycia własnej tożsamości lub zwiększenie skuteczności ataku opartego na socjotechnice). Mając na względzie powyższe niezbędne jest wskazanie, że celem działania sprawców jest wyrządzenie szkody osobie, pod którą się podszywają lub innej osobie. Co więcej, aktualnie kradzież tożsamości obejmuje podszycie jedynie pod osoby fizyczne. Penalizacją nie są objęte podszycia pod inne niż osoby fizyczne podmioty, a jest to również typowe zachowanie sprawców cyberprzestępstw.

Celowe jest również wprowadzenie kryminalizacji czynu określanego mianem tzw. deepfake. Istota tego zachowania polega na wprowadzającej w błąd manipulacji wizerunkiem osoby, jej danymi osobowymi lub innymi danymi, za pomocą których jest ona publicznie identyfikowana. Takie działanie jest najczęściej osadzone w określonym kontekście, co pozwala na manipulacją emocjami i zaufaniem innych osób. Polega ono zwykle na prezentowaniu fałszywych filmów lub nagrań, w których znane osoby rzekomo reklamują produkty lub usługi, a ich masowe rozpowszechnienie w sieci może wprowadzić odbiorców w błąd. Penalizacji powinno podlegać co najmniej produkowanie, rozpowszechnianie lub publiczne prezentowanie obrazów, treści dźwiękowych lub treści wideo zawierających wizerunek innej osoby, inne jej dane osobowe lub inne dane, za pomocą których jest ona publicznie identyfikowana i mogących wprowadzić w błąd co do ich prawdziwości.

Należy również rozważyć **zmianę brzmienia definicji rzeczy ruchomej z art. 115 § 9 k.k. poprzez uzupełnienie o kryptoaktywa katalogu przedmiotów, którym dotychczas ustawodawca przyznał walor rzeczy ruchomej lub przedmiotu w rozumieniu karnym.** Aktualnie na gruncie prawa karnego materialnego, jako przedmiot przestępstwa, kryptowaluty traktowane są najczęściej jako prawo majątkowe/mienie, a jednocześnie dane informatyczne. Tym samym zachowanie polegające na kradzieży przedmiotowych środków z portfela pokrzywdzonego, kwalifikowane jest co do zasady z art. 287 § 1 k.k., zagrożonego karą do 5 lat pozbawienia wolności. Tymczasem pod względem naganności i stopnia społecznej szkodliwości, jak i strat materialnych po stronie pokrzywdzonych, zachowanie to nie różni się niczym od kradzieży z włamaniem środków pieniężnych zapisanych na rachunku bankowym, które to przestępstwo, stypizowane w art. 279 § 1 k.k., zagrożone jest karą do 10 lat pozbawienia wolności. Powyższa sytuacja jest trudna do zaakceptowania, tak z punktu widzenia równości wobec prawa, jak i braku możliwości wymierzenia podejrzanemu adekwatnej kary. Jednocześnie na uwadze mieć należy, że środek pieniężny zapisany na rachunku, uznany został przez ustawodawcę za rzecz ruchomą/przedmiot.

Niezależnie od powyższego na uwagę zasługuje również fakt, że zgodnie z brzmieniem art. 236b k.p.k. rzeczą lub przedmiotem, także w rozumieniu przepisów kodeksu postępowania karnego, są środki na rachunku. Nadto postanowienie w przedmiocie dowodów rzeczowych może dotyczyć środków na rachunku, jeżeli zostały zatrzymane jako dowód w sprawie. Tym samym na gruncie prawa karnego procesowego również środki na rachunku traktowane są jak rzeczy, a także mogą zostać uznane w toku postępowania za dowód rzeczowy. **Analogicznej podstawy prawnej brak jest obecnie w stosunku do kryptoaktywów.** Mając na względzie powyższym celowa jest również zmiana brzmienia art. 236b k.p.k.

Rada rekomenduje w tym zakresie zmiany polegające na:

- zmianie definicji rzeczy w k.k. i k.p.k. i objęcie nią również kryptoaktywów;
- zmianie regulacji kradzieży tożsamości;
- kryminalizację tzw. deepfake;
- zmianie granic zagrożenia karnego dla wybranych cyberprzestępstw, z jednoczesnym wprowadzeniem wypadków mniejszej wagi oraz względnej wnioskowości.

9. Udostępnienie publicznych narzędzi do weryfikacji deepfake i fałszywych reklam.

Niezależnie od wprowadzenia kryminalizacji deepfake Rada rekomenduje powierzenie np. NASK przygotowania publicznego narzędzia wspierającego obywateli w ocenie, czy nagranie, reklama lub wizerunek znanej osoby został wygenerowany przez AI oraz prowadzenia powszechnych szkoleń z zakresu rozpoznawania zmanipulowanych zobrazowań i treści.

Agnieszka Jankowska
Przewodnicząca Rady do Spraw Cyfryzacji
/podpisano elektronicznie/

PODPIS ZAUFANY
AGNIESZKA
JANKOWSKA
22.06.2026 15:00:08 GMT+0200
Dokument podpisany elektronicznie
podpisem zaufanym