



Warszawa, 07-04-2026 r.

RZECZNIK PRAW OBYWATELSKICH

Marcin Wiącek

II.510.21.2026.DC

Pan

Waldemar Żurek

**Minister Sprawiedliwości – Prokurator
Generalny**

/ePUAP/

Szanowny Panie Ministrze,

zwracam się z uprzejmą prośbą o analizę problemu przypadku elektronicznych nośników danych, przypadku danych informatycznych oraz innych niematerialnych składników mienia wykorzystywanych do popełnienia przestępstwa.

W praktyce ujawnia się bowiem problem dotyczący relacji pomiędzy przypadkiem elektronicznego nośnika danych (np. telefonu, smartfona, laptopa, dysku SSD, czy innego dysku zewnętrznego) a przypadkiem danych informatycznych zapisanych na takim urządzeniu. Z napływających do Biura RPO sygnałów wynika, że odrębne traktowanie tych dwóch kategorii nie stanowi utrwalonej praktyki orzeczniczej. W orzecznictwie incydentalnie wskazuje się bowiem, że „Orzeczone na podstawie art. 44 § 2 k.k. przypadek samego nośnika informatycznego (dysku, notebooka) nie obejmuje zapisanych na nim danych. Przypadek danych informatycznych i przypadek ich nośnika muszą być traktowane jako dwa odrębne rozstrzygnięcia; przypadek danych można orzec bez orzekania przypadku nośnika i odwrotnie”¹. **Z danych, jakie wpływają do mojego Biura wynika, że sądy orzekając przypadek np. smartfona, nie analizują**

¹ Postanowienie SA we Wrocławiu z 22.05.2013 r., II AKz 233/13, OSAW 2013, nr 3, poz. 293.

potrzeby orzeczenia także danych znajdujących się na urządzeniu i nie pozwalają np. na zgranie treści o znaczeniu emocjonalnym na inny nośnik danych. Tymczasem obecnie, telefon/smartfon to urządzenie, na którym znajdują się dane - zdjęcia, nagrania, wiadomości, dotyczące np. uroczystości rodzinnych, zdjęcia najbliższych. Orzeczenie przypadku tych danych niejako „automatycznie”, wraz z przypadkiem nośnika danych jest dodatkową, niewspółmierną dolegliwością. Tymczasem przypadek nośnika danych oraz przypadek danych informatycznych powinny być traktowane jako dwa odrębne rozstrzygnięcia.

Dalsze wątpliwości dotyczą danych przechowywanych poza urządzeniem, ale z nim funkcjonalnie powiązanych, w szczególności danych zapisanych równoległe na dyskach wirtualnych lub w chmurze, takich jak iCloud, Google Drive, OneDrive czy Dropbox. W praktyce rodzi to pytanie, czy ewentualny przypadek danych informatycznych obejmuje również takie zasoby, a jeżeli tak, to w jaki sposób miałyby być skutecznie wykonywane. Jeśli bowiem intencją sądu orzekającego o przypadku nośnika danych (np. telefonu) jest objęcie przypadkiem danych na nim zapisanych, to jeśli użytkownik urządzenia równoległe korzysta z możliwości zapisania danych w chmurze (np. iCloud), przypadek urządzenia nie oznacza przypadku danych. Użytkownik może w łatwy sposób odzyskać dostęp do danych logując się na swoje konto iCloud na nowym urządzeniu. **Wydaje się, że aktualnie brak jest rozwiązań normatywnych, które odnosiłyby się do przypadku danych informatycznych zapisanych w chmurze lub dyskach wirtualnych.**

Wątpliwości odnoszące się do problemów związanych z orzekaniem przypadku mienia należy oceniać również w świetle prawa Unii Europejskiej. Przepis art. 2 pkt 3 rozporządzenia 2018/1805² termin „mienie” definiuje jako mienie każdego rodzaju, materialne lub niematerialne, ruchome lub nieruchome, oraz dokumenty lub instrumenty prawne potwierdzające prawo do takiego mienia lub prawo z nim związane, które organ wydający uznaje za:

- a) korzyści pochodzące z przestępstwa albo ich pełną lub częściową równowartość;
- b) narzędzia służące do popełnienia przestępstwa albo wartość takich narzędzi;

² Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1805 z dnia 14 listopada 2018 r. w sprawie wzajemnego uznawania nakazów zabezpieczenia i nakazów konfiskaty (Dz. U. UE. L. z 2018 r. Nr 303, str. 1 z późn. zm.).

- c) podlegające konfiskacie poprzez zastosowanie w państwie wydającym uprawnień do konfiskaty określonych w dyrektywie 2014/42/UE³; lub
- d) podlegające konfiskacie na podstawie innych przepisów dotyczących uprawnień do konfiskaty, w tym konfiskaty bez prawomocnego wyroku skazującego, na mocy prawa państwa wydającego, po przeprowadzeniu postępowania w związku z popełnieniem przestępstwa.

W najnowszej dyrektywie 2024/1260⁴ wprost terminem mienie obejmuje się kryptoaktywa.

Mieniem niematerialnym – narzędziem służącym do popełnienia przestępstwa, jest zgodnie z przepisami rozporządzenia 2018/1805 oraz dyrektywy 2014/42 i dyrektywy 2024/1260 także np. konto na giełdzie kryptowalut (np. Binance) w przypadku tzw. karuzeli VAT, czy konto na YouTube, które rozpowszechnia treści propagujące ustrój totalitarny albo rozpowszechniające treści antysemickie, antyislamskie, czy antyukraińskie. Przepadek mienia – np. komputera – nie oznacza, że przypadkowi ulegną dane informatyczne np. filmy, nagrania, posty, zamieszczane na kontach w mediach społecznościowych. Tymczasem, zgodnie z prawem unijnym – rozporządzeniem, które jest bezpośrednio skuteczne w prawie krajowym i może stanowić samodzielną podstawę orzekania, bez potrzeby implementacji tego aktu prawnego – mienie niematerialne, będące narzędziem służącym do popełnienia przestępstwa, także powinno być objęte przypadkiem. W prawie krajowym powinny istnieć procedury, które pozwolą na skuteczne wykonanie przypadku niematerialnych narzędzi służących do popełnienia przestępstwa, tj. w odniesieniu do danych przechowywanych „wirtualnie” (na dyskach wirtualnych, czy umieszczone na kontach w mediach społecznościowych). Chodzi o zapewnienie, że przepadek mienia, tj. przepadek nośnika danych wraz z zapisanymi na nim danymi, nie będzie środkiem pozornym, ponieważ użytkownik w łatwy sposób odzyska dostęp do danych – pobierając je z dysku wirtualnego.

³ Dyrektywa Parlamentu Europejskiego i Rady 2014/42/UE z dnia 3 kwietnia 2014 r. w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej (Dz. U. UE. L. z 2014 r. Nr 127, str. 39 z późn. zm.). W dyrektywie 2014/42 mienie definiuje się jako „oznacza mienie każdego rodzaju, materialne lub niematerialne, ruchome lub nieruchome, oraz dokumenty lub instrumenty prawne potwierdzające prawo do takiego mienia lub prawo z nim związane”, zaś „narzędzia” jako „każde mienie użyte lub które ma zostać użyte w jakikolwiek sposób, w całości lub w części, do popełnienia przestępstwa lub przestępstw”.

⁴ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/1260 z dnia 24 kwietnia 2024 r. w sprawie odzyskiwania i konfiskaty mienia (Dz. U. UE. L. z 2024 r. poz. 1260).

Trudności w znalezieniu odpowiedniej podstawy prawnej do orzeczenia przypadku „rzeczy” niematerialnych dotyczą kont na giełdach kryptowalut, kont lub profili w mediach społecznościowych, kanałów na komunikatorach (jak Whatsapp czy Telegram). W realiach obrotu cyfrowego „konto” nie ma charakteru rzeczy, lecz stanowi zespół uprawnień majątkowych i faktycznych możliwości dysponowania określonym narzędziem. To „mienie niematerialne” – profil w mediach społecznościowych, kanał nadawczy na Telegramie, czy konto na giełdzie kryptowalut – w postaci praw majątkowych związanych z kontem (uprawnień wynikających z umowy o prowadzenie konta związanych z dostępem do konta, jego promowaniem, umieszczaniem postów, odpowiadaniem na wiadomości) może być narzędziem służącym do popełnienia przestępstwa (np. prania pieniędzy, promowania terroryzmu, przestępstw seksualnych).

Powstaje zatem pytanie, czy i w jaki sposób obecne przepisy prawa karnego materialnego, procesowego i wykonawczego pozwalają na skuteczne objęcie takich składników mienia (mienia niematerialnego) rozstrzygnięciem o przypadku albo zabezpieczeniem oraz na wykonanie takiego rozstrzygnięcia, zwłaszcza gdy usługodawca ma siedzibę poza Polską albo poza Unią Europejską.

Konieczne jest także ustalenie, w jaki sposób kształtuje się praktyka orzecznicza sądów. W mojej ocenie problem wymaga co najmniej rozważenia, czy obecny stan prawny jest wystarczający, czy też konieczne jest rozpoczęcie prac legislacyjnych, dostosowujących przepisy krajowe do prawa unijnego oraz do realiów obecnego, coraz bardziej cyfrowego świata. Dotyczy to w szczególności:

- wyraźnego rozróżnienia przypadku nośnika danych i przypadku danych informatycznych;
- określenia zasad postępowania z danymi niemającymi związku z przestępstwem, w tym danymi o charakterze osobistym,
- ustalenia, czy i na jakich zasadach przypadek może obejmować dane przechowywane w chmurze, dyskach wirtualnych itp.,
- doprecyzowania podstaw prawnych dotyczących przypadku niematerialnych narzędzi służących do popełnienia przestępstwa, w tym praw związanych z kontami na giełdach kryptowalut i kontami w mediach społecznościowych,
- stworzenia skutecznych mechanizmów wykonawczych pozwalających na realne pozbawienie sprawcy władztwa nad mieniem niematerialnym poprzez uniemożliwienie odzyskania dostępu do konta, w tym także w relacjach z podmiotami zagranicznymi.

Jednocześnie, gdyby Pan Minister uznał, że przed podjęciem decyzji legislacyjnych celowe jest uprzednie pogłębione rozpoznanie skali i charakteru problemu w praktyce orzeczniczej oraz wykonawczej, zasadnym wydaje się rozważenie zwrócenia się o przeprowadzenie stosownych badań do Instytutu Wymiaru Sprawiedliwości, na co pozwala § 5 ust. 2 statutu Instytutu Wymiaru Sprawiedliwości⁵. Badania takie mogłyby objąć w szczególności:

- sposób ujmowania w orzecznictwie relacji pomiędzy przypadkiem nośnika a przypadkiem danych,
- praktykę dotyczącą danych przechowywanych poza urządzeniem, w tym w chmurze,
- praktykę dotyczącą kont na giełdach kryptowalut oraz kont, kanałów i profili w mediach społecznościowych jako potencjalnych niematerialnych narzędzi służących do popełnienia przestępstwa.

Mając na uwadze przedłożone racje, stosownie do art. 16 ust. 2 pkt 1 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich⁶, zwracam się do Pana Ministra z uprzejmą prośbą o dokonanie analizy wskazanych w niniejszym stanowisku problemów i poinformowanie mnie o stanowisku zajęтым w przedstawionej materii.

Z wyrazami szacunku

Marcin Wiącek

Rzecznik Praw Obywatelskich

/-wydano i podpisano elektronicznie/

Do wiadomości:

- Pan Poseł Marek Ast Przewodniczący Komisji Ustawodawczej Sejmu RP (kust@sejm.gov.pl);
- Pani Poseł Barbara Dolniak Przewodnicząca Komisji Nadzwyczajnej do spraw zmian w kodyfikacjach (knkk@sejm.gov.pl);
- Pan Senator Krzysztof Kwiatkowski Przewodniczący Komisji Ustawodawczej Senatu RP (ku@senat.gov.pl)

⁵ Zarządzenie Ministra Sprawiedliwości z dnia 12 lipca 2010 r. w sprawie nadania statutu Instytutowi Wymiaru Sprawiedliwości (Dz. Urz. MS z 2010 r. Nr 7, poz. 88).

⁶ Ustawa z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2024 r., poz. 1264).