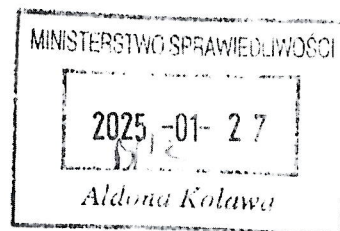




KOMENDA GŁÓWNA POLICJI

BIURO KONTROLI
Wydział Skarg i Wniosków

ul. Puławska 148/150; 02-624 Warszawa; tel.: 47-72-12461, fax: 47-72-13571



L.dz.: Is-836/821/25/PN

Warszawa, dnia 22.01.2025 r.

Egz. nr 1

Ministerstwo Sprawiedliwości
Al. Ujazdowskie 11
00-950 Warszawa

W załączeniu, przekazuję uprzejmie petycję p. *(dotyczącą wprowadzenia obligatoryjnego zakazu korzystania z usług teleinformatycznych dla osób skazanych za cyberprzestępstwa)*, która wpłynęła do Komendy Głównej Policji drogą elektroniczną - z prośbą o rozpoznanie przedmiotowej sprawy we własnym zakresie.

Załączniki:

Wyżej wymienione pismo p.

(wydruk e-maila z dnia 17.01.2025 r.) - 5 kart.

Wyk. PN w 2 egz.:

Egz. nr 1 - Adresat

Egz. nr 2 - p.

- a a

WYDZIAŁ SKARG I WNIOSKÓW
POLICJI
KOMENDA GŁÓWNA POLICJI
AL. UJAZDOWSKIE 11
00-950 WARSZAWA

Administratorem danych osobowych jest Komendant Główny Policji (KGP). KGP wyznaczył Inspektora Ochrony Danych Osobowych. Adres mailowy: iod.kgp@policja.gov.pl. Pani/Pana dane osobowe będą wykorzystywane w celu rozpatrzenia wniesionej go przez Panią/Pana skargi/wniosku/petycji. Pani/Pana dane osobowe będą przetwarzane na podstawie przepisów Kodeksu postępowania administracyjnego/ustawy o petycjach. Pani/Pana dane osobowe będą udostępnione wyłącznie podmiotom upoważnionym na podstawie przepisów prawa oraz nie będą wykorzystywane w celu profilowania. KGP nie zamierza przekazywać Pani/Pana danych osobowych do państwa trzeciego organizacji międzynarodowej. Pani/Pana dane osobowe będą przechowywane przez czas realizacji sprawy, a następnie archiwizowane zgodnie z obowiązującymi przepisami prawa. Przysługuje Pani/Panu prawo dostępu do treści danych oraz ich sprostowania. Przysługuje także Pani/Panu prawo do wniesienia skargi do organu nadzorczego tj.: Prezesa Urzędu Ochrony Danych Osobowych. Podanie Pani/Pana danych osobowych jest obowiązkowe, gdyż wynika z przepisów Kodeksu postępowania administracyjnego/ustawy o petycjach i jest niezbędne do rozpatrzenia wniesionej go przez Panią/Pana skargi/wniosku/petycji.





Prośba o opinie

: kancelaria.gabinetkgp@policja.gov.pl 17.01.2025 16:04

Od: "

Do: "kancelaria.gabinetkgp@policja.gov.pl" <kancelaria.gabinetkgp@policja.gov.pl>

UWAGA: Ten e-mail pochodzi spoza organizacji. Nie klikaj żadnych linków ani nie otwieraj załączników jeśli nie ufasz nadawcy i nie wiesz, czy zawartość jest bezpieczna

Szanowni Państwo,

Zwracam się z uprzejmą prośbą o zapoznanie się z załączoną petycją dotyczącą wprowadzenia obligatoryjnego zakazu korzystania z usług teleinformatycznych dla osób skazanych za cyberprzestępstwa. Petycja ta ma na celu zwiększenie bezpieczeństwa w sieci oraz ochronę użytkowników przed potencjalnymi zagrożeniami.

W załączonej petycji przedstawiamy propozycje zmian w polskim prawie karnym, które obejmują m.in. wprowadzenie zakazu korzystania z usług teleinformatycznych dla osób skazanych za cyberprzestępstwa. Proponowane zmiany mają na celu ograniczenie możliwości ponownego popełnienia przestępstwa przez skazanych oraz zwiększenie bezpieczeństwa w sieci dla wszystkich użytkowników.

Będziemy wdzięczni za Państwa opinię na temat przedstawionych propozycji oraz ewentualne wsparcie w dążeniu do wprowadzenia tych ważnych zmian.

Z poważaniem,

Zaakaz korzystania z usług teleinformatycznych dla skazanych za cyberprzestępstwa i posiadanie nielegalnych treści - Petycjeonline.com

Wysłano z bezpiecznej poczty e-mail Proton Mail.

Email secured by CSI (TX1)

WYDZIAŁ KARET W MIONKOW
BANKI KONTROLING

Wpłynęło on. 2.01.2025

L.dz. Is. 331/25/PN

2-10-5202
2025-01-2
01/25/24

2.01.2025
850

ZAKAZ KORZYSTANIA Z USŁUG TELEINFORMATYCZNYCH DLA SKAZANYCH ZA CYBERPRZESTĘPSTWA I POSIADANIE NIELEGALNYCH TREŚCI

 Petycja

Szanowni Państwo

My, niżej podpisani, zwracamy się z prośbą o wprowadzenie zmian w polskim prawie karnym, które nakładałyby obowiązkowy zakaz korzystania z usług teleinformatycznych na osoby skazane za popełnienie cyberprzestępstw takich jak;

1. **Phishing:-** Ataki mające na celu wyłudzenie danych osobowych poprzez podszywanie się pod zaufane osoby lub instytucje.
2. **Hacking:-** Nieautoryzowane włamania do systemów komputerowych w celu kradzieży danych lub zakłócenia pracy.
3. **Malware:** - Używanie złośliwego oprogramowania, takiego jak wirusy, robaki lub ransomware, aby uszkodzić systemy komputerowe lub uzyskać nieautoryzowany dostęp do danych.
4. **Cyberstalking:** - Prześladowanie i nękanie osób za pomocą technologii, np. przez e-maile, media społecznościowe.
5. **Identity Theft: Kradzież tożsamości** - w celu uzyskania dostępu do kont bankowych, kart kredytowych lub innych zasobów.
6. **Financial Fraud: Oszustwa finansowe,** - takie jak kradzież kart kredytowych, wyłudzenie danych bankowych.

7. **Cyberbullying: Przemoc w sieci,-** polegająca na upokarzaniu, grożeniu lub nękanii innych osób.
8. **Posiadanie treści prawnie zabronionych -** takich jak pornografia dziecięca i inne opisane w prawie.
9. **Popagowanie nienawiści -** działania polegające na szerzeniu wrogości, dyskryminacji lub przemocy wobec osób lub grup na podstawie ich rasy, religii, narodowości, orientacji seksualnej, płci, niepełnosprawności lub innych cech.
10. **Oszustwa socjotechniczne -** przestępstwa, w których sprawcy wykorzystują techniki manipulacji psychologicznej, aby oszukać ofiary i wyłudzić od nich pieniądze lub inne korzyści. popularnie nazywane **oszustwami na wnuczka**.
11. **INNE -** inne przestępstwa wskazane przez **CENTRALNE BIURO ZWALCZANIA CYBERPRZESTĘPCZOŚCI**

Uzasadnienie:

W dobie rosnącej liczby cyberprzestępstw, takich jak phishing, hacking, cyberstalking, kradzież tożsamości, oszustwa finansowe, propagowanie terroryzmu oraz posiadanie treści prawnie zabronionych, konieczne jest wprowadzenie dodatkowych środków prewencyjnych, które skutecznie przeciwdziałałyby takim działaniom i znacząco przyczyniły się do ochrony społeczeństwa.

Proponowane zmiany:

1. Wprowadzenie obligatoryjnego zakazu korzystania z usług teleinformatycznych przez okres 5 lat dla osób skazanych za cyberprzestępstwa
2. Wprowadzenie obligatoryjnego dożywotniego zakazu korzystania z usług teleinformatycznych dla osób, które ponownie popełniły cyberprzestępstwa (recydywa).
3. Zakaz obejmowałby korzystanie z internetu oraz usług telekomunikacyjnych

5. **Lepsza kontrola i nadzór** - Powiązanie zakazu z bazą zastrzeżonych numerów PESEL oraz obowiązek informowania operatorów sieci komórkowych i dostawców usług internetowych pozwoli na lepszą kontrolę i nadzór nad przestrzeganiem zakazów.
6. **Podniesienie świadomości społecznej** - Zmiany w prawie mogą zwiększyć świadomość społeczną na temat cyberprzestępczości i konsekwencji związanych z jej popełnianiem, co może wpłynąć na zmniejszenie liczby takich przestępstw zwłaszcza z połączeniem z kampaniami edukacyjnymi
7. **Wzmocnienie systemu prawnego** - Wprowadzenie surowych kar za niewyłączenie dostępu do usług teleinformatycznych przez operatorów po otrzymaniu informacji od sądu wzmocni system prawny i egzekwowanie przepisów.

4. Powiązanie zakazu z bazą zastrzeżonych numerów **PESEL**, aby skutecznie monitorować i egzekwować przestrzeganie zakazu.
5. Zobowiązanie sądów do informowania operatorów sieci komórkowych i dostawców usług internetowych o nałożonym zakazie korzystania z usług teleinformatycznych.
6. Zobowiązanie operatorów sieci komórkowych i dostawców usług internetowych do wyłączenia dostępu do usług teleinformatycznych dla osób, które otrzymały zakaz, po otrzymaniu informacji od sądu.
7. Ustanowienie mechanizmów nadzoru i egzekwowania przestrzegania zakazu.
8. Ustanowienie kar dla operatorów sieci komórkowych i dostawców usług internetowych za niewyłączenie dostępu do usług pomimo otrzymania informacji od sądu.

Korzyści z wprowadzonych zmian

1. **Ochrona dziedzici** - Wprowadzenie zmian pozwoli chronić dzieci przed wykorzystaniem przez pedofili co jak wiemy jest traumą na całe życie
2. **Ograniczenie recydywy** - Proponowane zmiany będą skutecznie przeciwdziałać ponownemu popełnianiu cyberprzestępstw przez osoby skazane, co przyczyni się do zmniejszenia liczby takich przestępstw.
3. **Zwiększenie bezpieczeństwa w sieci** - Wprowadzenie zakazu korzystania z usług teleinformatycznych dla cyberprzestępców zwiększy ogólne bezpieczeństwo w sieci, chroniąc użytkowników przed potencjalnymi zagrożeniami.
4. **Zmniejszenie liczby ofiar** - Proponowane zmiany pomogą w zmniejszeniu liczby ofiar cyberprzestępstw, takich jak phishing, oszustwa socjotechniczne czy kradzież tożsamości jak i zmniejszenie liczby samobójstw spowodowanych przez takich cyberprzestępców