Od monetizovaného nátlaku k odpovědnosti:

Nástroje práva EU proti cyberstalkingu a komercionalizovanému obtěžování

Zdroj: Evropský parlament, kancelář JUDr. Ondřeje Dostála, Ph.D., LL.M., poslance Evropského parlamentu (11/2025)

Úvod

Rozvoj sociálních sítí a jejich hluboké proniknutí do každodenního života zásadně mění způsob, jakým lidé komunikují, sdílejí informace a utvářejí veřejnou debatu. S tímto vývojem se však paralelně objevují nové formy zneužití těchto platforem, jako jsou systematické online útoky zaměřené na konkrétní osoby, spojené s ekonomickým ziskem pachatelů. Jednou z těchto forem je i fenomén, který v této analýze označujeme jako **monetizovaný cyberstalking**.

Debata o tom, jak na tyto jevy reagovat, se v Evropské unii i členských státech často odehrává mezi dvěma póly: na jedné straně je legitimní snaha chránit důstojnost, soukromí a bezpečí jednotlivců, na straně druhé je zásadní potřeba zachovat svobodu projevu a zabránit tomu, aby regulace digitálního prostředí vedla k faktické cenzuře nebo k „privatizaci" výkonu veřejné moci v rukou velkých platforem. Tato analýza vychází z přesvědčení, že **i v oblasti digitálního prostoru musí platit zásada *in dubio pro libertate*** – v pochybnostech ve prospěch svobody – a že každý zásah do svobody projevu musí být odůvodněný, nezbytný a přiměřený, pravidelně podrobován revizi.

Cílem textu je ukázat, že **stávající právní rámec** – zejména nařízení Evropského parlamentu a Rady EU 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále též jen „**Nařízení GDPR**", nařízení Evropského parlamentu a Rady EU o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (dále též jen „**Nařízení DSA**" a relevantní ustanovení trestního práva a soukromého práva členských států – již dnes obsahuje řadu nástrojů, které lze k ochraně obětí monetizovaného cyberstalkingu využít. Namísto přijímání další, stále detailnější, regulace by se Evropská unie i členské státy měly v první řadě soustředit na **důslednou a předvídatelnou aplikaci existujících pravidel**.

Analýza vychází z konkrétních případů monetizovaného cyberstalkingu, které se objevily v českém prostředí, a ukazuje, jak lze na tyto situace aplikovat současné nástroje vnitrostátního práva i práva EU. Případy pocházejí z jednoho členského státu, nicméně vykazují rysy, jež jsou typové a přenositelné i do dalších jurisdikcí: kombinaci dlouhodobého obtěžování, cíleného poškozování konkrétních osob a ekonomické motivace pachatelů.

Záměrem této analýzy **není** navrhovat další vrstvy regulace digitálního prostoru, ale naopak poukázat na to, že :

- existující právní nástroje – pokud jsou skutečně využívány – mohou poskytnout obětem efektivní ochranu,
- plošné přenášení odpovědnosti za posuzování a odstraňování obsahu na platformy s sebou nese vážná rizika pro svobodu projevu a právní jistotu,
- a že případné další legislativní zásahy by měly být až **druhým krokem**, který přichází teprve poté, co je ověřeno, že stávající právní rámec nefunguje, a že namísto přijímání nové regulace by měla být dána přednost revizi předpisového rámce stávajícího .

K pojmu monetizovaného cyberstalkingu

Konkrétní příklady monetizovaného cyberstalkingu a znaky tohoto jednání

V rámci zpracování této analýzy jsme hovořili s několika osobami, které se staly obětí cyberstalkingu, a zkoumali jsme rovněž několik dalších případů. Cílem bylo identifikovat způsob této formy nátlaku i reálné zkušenosti z obrany proti podobným útokům.

Případ 1

Novinář se stal terčem opakovaných útoků ze strany organizované skupiny osob. Tyto osoby koordinovaly své útoky otevřeně na sociálních sítích, svá jednání zaznamenávali na video a následně sdíleli zejména na platformách HeroHero.co (platforma založená v České republice) a na síti X. Obě tyto platformy přitom nabízejí model monetizace obsahu. Platforma HeroHero.co prostřednictvím standardního předplatného (z něhož si provozovatel účtuje procentuální podíl coby cenu za své služby). Platforma X (dříve Twitter) také nabízí řadu monetizačních nástrojů (předplatné, sdílení výnosů, sponzoring apod.), navíc tvůrcům obsahu zvyšuje popularitu (síť X je sledována i mnoha novináři apod.), která pak zvyšuje dosah obsahu zveřejňovaného prostřednictvím platformy HeroHero.

Útoky na novináře zahrnovaly:

- fyzické napadení
- hrubé slovní urážky a výhrůžky
- pronásledování
- narušování soukromí

Dle vyjádření oběti v několika případech útokům přihlíželi příslušníci policie, ale nijak proti nim nezakročili. Naopak, členové skupiny sledovali novináře tak dlouho, až se při pokusu o únik dopustil dopravního přestupku. Na to útočící skupina upozornila strážníky obecní policie, kteří pak novináře zastavili. Členové skupiny opakovaně novináře uráželi a, jak je uvedeno výše, celý průběh si nahrávali a následně zveřejnili. Uvedený novinář eviduje až sto podobných útoků v reálném i online prostoru. Ačkoliv k útokům došlo již v první polovině roku 2025 (i dříve), policie ani jiné orgány dosud nebyly schopny věc vyřešit.

Případ 2

Několik osob podniklo útoky vůči provozovateli internetového televizního kanálu. V blízkosti jeho domu aktivovali pyrotechniku (rachejtle apod.), cíleně směřované přímo nad nemovitost tohoto provozovatele. Tento útok si pak skupina nahrávala prostřednictvím dronu, který se pohyboval i nad nemovitostí oběti. Oběť byla již předtím řadu měsíců pronásledována, veřejně difamována,

přičemž veškeré tyto útoky byly následně zveřejněny na online platformách přístupných prostřednictvím placených účtů. Ani v tomto případě dosud orgány veřejné moci věc definitivně nevyřešily.

Případ 3

Dalším zdokumentovaným případem kyberšikany byl koordinovaný útok na petiční stánek umístěný před budovou Úřadu vlády, který se odehrál v roce 2024. Petiční stánek organizoval známý aktivista jako protest proti tehdejší vládní politice. Skupina osob zahájila své aktivity výhrůžkami směřovanými k organizátorovi petičního stánku, včetně výhrůžek fyzickým útokem. Následoval i reálný fyzický útok na petiční stánek. Ze všech těchto aktivit vznikly video-záznamy, které byly následně umístěny na sociální sítě. Policejní orgány ani soudy přitom nebyly schopny účinně proti této skupině zasáhnout.

Případ 4

Další obětí se stala aktivistka, kterou organizovaná skupina sledovala, zjišťovala si o ní informace (například registrační značku a typ auta, bydliště apod.), které následně zveřejňovala na svých účtech na sociálních sítích. Šlo většinou o platformy HeroHero.co či YouTube (i YouTube nabízí programy monetizace obsahu, například YouTube Partner Program, Shorts Monetization apod.)

Součástí útoků bylo i šíření hanlivých vyjádření ve vztahu k oběti. Ani v těchto případech se obrana ze strany policejních orgánů či soudů neukázala jako účinná, provozovatelé online platforem rovněž odmítli jakkoliv zasáhnout.

Případ 5

Řada evidovaných případů dokazuje, že útoky ve formě monetizovaného cyberstalkingu se dotýkají i oblasti politiky. V České republice bylo podobných případů zaznamenáno několik. Často se jejich původci skrývají pod instituty práva na svobodu projevu či veřejného zájmu. V nedávné době tak například zkombinovali starší záznamy ze soukromí nově zvoleného poslance se záběry jeho rodinných příslušníků (vč. nezletilého dítěte) s tím, že veřejnost má právo vědět o soukromém životě zvoleného poslance, pokud souvisí s jeho politickými názory. Jakkoliv v obecné rovině jistě nelze vyloučit situace, kdy i jinak nedotknutelné informace o soukromém životě veřejně činné osoby mohou být předmětem veřejného zájmu, v předmětném případě forma i rozsah zveřejnění naznačují, že původcům zřejmě nešlo o společenskou diskusi, ale o skandalizaci

dané osoby za účelem osobního obohacení prostřednictvím monetizace na online platformách. Tento případ ilustruje citlivost analyzovaného tématu, neboť jakkoliv je nutné poskytnout občanům ochranu před zneužíváním nových online nástrojů k narušování soukromí a útokům pro lidské důstojnosti, nelze rovněž připustit, aby taková ochrana omezovala základní právo na informace či na kontrolu výkonu politické moci. Jakákoliv regulace proto musí být volena uvážlivě s respektem ke všem chráněným právům a svobodám, za důsledné aplikace principu proporcionality (vyváženosti).

Nástroje zpeněžení obsahu

Ke zpeněžení obsahu zveřejňovaného na sociálních sítích a dalších online platformách lze v současné době využít řadu nástrojů. Za základní modely takové monetizace obsahu lze považovat:

- **Reklamy a sdílení výnosů z platforem**

  Asi nejklasičtější formou je sdílení příjmů provozovatele platformy s digitálním tvůrcem. V tomto modelu provozovatel platformy část svých zisků z reklamy či předplatného sdílí s držiteli účtu s vysokou návštěvností, resp. sledovaností.

  Finanční prostředky jsou tedy v tomto případě distribuovány přímo **prostřednictvím provozovatele online platformy** (není zde tedy přímý vztah zadavatel reklamy – tvůrce obsahu/držitel konkrétního účtu či kanálu).

- **Affiliate marketing**

  V tomto případě obvykle tvůrce obsahu spolupracuje s profesionální společností, která rozvíjí tzv. affiliate sítě. Jejich prostřednictvím šíří reklamní (obchodní) sdělení třetích stran svým affiliate partnerům, přičemž tito partneři (většinou držitelé konkrétního účtu na sociální síti) pak taková obchodní či reklamní sdělení sdílejí.

  Finanční prostředky v tomto případě **provozovatele online platformy míjejí**, většinou jsou distribuovány provozovatelem affiliate sítě.

- **Reklama / Sponzoring**

  Jde zřejmě o nejklasičtější model obchodního využití účtu na sociální síti, kdy jeho držitel účtu (a tvůrce obsahu) šíří (případně i vytváří) reklamní sdělení ve prospěch určitého zboží či služby, přičemž za takovou reklamu je odměněn prodejcem.

  Variantou této formy spolupráce je tzv. „*product placement*“, kdy tvůrce obsahu použije či zmíní ve svém obsahu zboží či službu třetí strany.

V tomto případě finanční tok směřuje nejčastěji od prodejce zboží či služby přímo tvůrci obsahu (případně prostřednictvím reklamní či marketingové agentury), tedy **mimo provozovatele online platformy**.

- **Předplatné**

  Některé platformy umožňují poskytovat tzv. placený obsah, tedy omezit přístup k obsahu pro určitou komunitu, která za takový přístup platí předplatné.

  V takovém případě jsou **finanční toky zprostředkovávané provozovatelem online platformy**, který většinou zajišťuje platební brány (nástroje) k placení předplatného.

- **Přímý prodej zboží či služeb**
  V tomto případě nejde o klasickou monetizaci obsahu na sociálních sítích, ale o prodej vlastního zboží či služeb prostřednictvím sociálních sítí. Určitou obdobou přímého prodeje může být financování obsahu prostřednictvím dobrovolných příspěvků a darů.

  Finanční prostředky v tomto případě obvykle směřují přímo od zákazníka k držiteli účtu, tedy **bez účasti provozovatele online platformy**.

Společné znaky monetizovaného cyberstalkingu

Vedle shora uvedených případů jsme zkoumali desítky podobných útoků, organizovaných různými skupinami. Pro účely této analýzy je přitom podstatné zhodnotit jejich společné znaky, tedy identifikovat jakési základní znaky monetizovaného cyberstalkingu.

Jde o jednání, kdy konkrétní osoba či skupina osob vytvářejí systematický a dlouhodobý nátlak na svou oběť, obtěžují ji doma či kdekoliv na veřejnosti, své činy si nahrávají a následně je sdílejí na sociálních sítích. Tento obsah se pak stává zdrojem finančních příjmů pro tvůrce tohoto obsahu, obvykle formou předplatného, s rostoucím počtem návštěvníků (sledujících) i formou sdílení výnosů apod.

Aby byl zajištěn dostatečný příjem, je nezbytné, aby se obětí podobného nátlaku stávaly osoby veřejně známé. Proto se terčem podobných aktivit stávají zejména osoby politicky aktivní, v poslední době ale tento způsob nátlaku směřuje i vůči novinářům či různým občanským aktivistům, kteří jsou aktivní na sociálních sítích. Právě podobně politicky motivovaný cyberstalking lze přitom považovat za společensky vysoce rizikové chování, protože může vést (a často vede) k zastrašení politických oponentů či kriticky informujících novinářů, což je jev, který destruuje demokratickou diskusi a volnou politickou soutěž. Jev, jehož důsledkem je i omezování svobody projevu (protože oběti se často raději z veřejného prostoru stáhnou).

Ze zkušeností obětí podobných útoků je zjevné, že proti nim neexistuje žádná rychlá účinná ochrana. Policejní orgány útoky vyšetřují, většinou je však odloží nebo vyhodnotí pouze jako přestupek. Pachatelům je pak uložena pokuta, a to i přesto, že v útocích pokračují.

Provozovatelé online platforem pak při přezkumu nahraného obsahu vyhodnocují věc často tak, že nejde o porušení zásad a pravidel platformy. Bez soudního rozhodnutí tak obsah na platformě existuje i nadále a generuje jeho tvůrcům příjmy z monetizačních nástrojů.

Na základě analýz oznámení ze strany obětí a policejních záznamů lze cyberstalking popsat takto:

- opakované útoky organizovaných skupin a jejich členů
- útoky spočívají v lehčích fyzických útocích (bez viditelného zranění), v urážkách, pronásledování, poškozování cizí věci
- součástí útoků je i zapojení policejních orgánů v rámci vyprovokovaných situací
- narušování soukromí a domovní svobody (opakované zvonění na zvonky u dveří, sledování prostor pomocí dronů apod.
- veškeré útoky jsou nahrávány, doprovázeny vulgárními a posměšnými komentáři
- nahrávky jsou pak šířeny zejména prostřednictvím online platforem, nabízejících monetizaci obsahu

Pro účely této analýzy rozumíme **monetizovaným cyberstalkingem** takové jednání, při kterém:

1. jedna nebo více osob **dlouhodobě** a **systematicky sleduje**, **kontaktuje** nebo **jinak obtěžuje** konkrétního člověka či úzký okruh osob,

2. součástí tohoto jednání je **zaznamenávání** (např. formou videí, livestreamů či fotografií) a následné **zveřejňování** těchto záznamů na online platformách,

3. zveřejněný obsah je **monetizován**, tedy přímo nebo nepřímo zpeněžován (například prostřednictvím platforem umožňujících sdílení příjmů z reklamy, placených odběrů, darů, předplatného či affiliate programů),

4. primárním nebo podstatným motivem pachatele je **ekonomický zisk**, v některých případech i zastrašení, diskreditace nebo umlčení oběti, nikoli účast na věcné veřejné diskusi či výkon legitimní kritiky.

Monetizovaný cyberstalking tak navazuje na „klasické“ formy stalkingu a kyberšikany, avšak doplňuje je o specifický prvek **obchodního modelu**: úspěch a dosah pachatelova obsahu – měřený počtem sledovatelů, zhlédnutí či interakcí – je přímo spojen s jeho finančním profitem. čím intenzivnější, více šokující nebo ponižující jsou útoky na oběť, tím větší může být finanční odměna. Tento ekonomický stimul vede k eskalaci jednání a vytváří tlak na jeho opakování, často navzdory výslovným nesouhlasům či právním krokům oběti.

V praxi se monetizovaný cyberstalking projevuje například:

- opakovaným „doprovázením“ oběti na veřejných místech, jejím natáčením bez souhlasu a následným zveřejňováním záznamů,
- pořádáním „návštěv“ u bydliště oběti či jejích blízkých, spojených s nahráváním a streamováním,
- vytvářením sérií videí nebo přenosů, v nichž je oběť dlouhodobě zesměšňována, obviňována či líčena jako nebezpečná osoba.

V této analýze používáme pojmy **„cyberstalking“** a **„kyberšikana“** částečně zaměnitelně, přičemž **monetizovaný cyberstalking** představuje jejich zvláštní, užší podkategorii, vyznačující se výše uvedenými znaky a ekonomickou motivací.

Rizika regulace cyberstalkingu v demokratické společnosti

Pro zkoumání efektivity právní obrany před cyberstalkingem je naprosto nezbytné identifikovat jeho typické znaky. Důvodem je zejména snaha chránit základní práva a svobody jednotlivce, zejména svobodu projevu, právo na informace a právo na kritiku. Ne každý zveřejněný obsah, v němž je člověk vyobrazován v negativním světle, je cyberstalkingem. Je nezbytné umožnit člověku projevovat svůj nesouhlas s politicky činnými osobami, a to i formou nadsázky, humoru a ironie. Samotný fakt, že se někdo cítí dotčen obsahem, který je zveřejněn na sociálních sítích, neznamená, že jde o jev nechtěný či dokonce nezákonný.

Nástroje ochrany člověka před cyberstalkingem je nezbytné volit právě s přihlédnutím k potřebě minimalizace regulace. Nelze připustit, aby se jakékoliv právní instrumenty staly nástrojem k potlačování kritiky ze strany médií, odhalování nežádoucí a nezákonných jevů ve společnosti apod.

Je dále naprosto nezbytné přihlédnout k tomu, že jakákoliv forma kontroly obsahu musí umožnit tvůrci obsahu (držiteli účtu na sociálních sítích) účinnou obranu, je třeba také jakékoliv zásahy podmínit nezákonným jednáním (tedy nikoliv jen jednáním nepříjemným). Snahu některých evropských států kriminalizovat projevy, které snad mohou být pro někoho zraňující, které však nejsou nezákonné, je třeba absolutně odmítnout.

Právě proto je nutné identifikovat základní typické znaky cyberstalkingu, aby se existující (či budoucí) nástroje ochrany člověka neobrátily proti člověku samotnému, aby se nestaly nástrojem totalitní moci. A současně volit nástroje, které co nejméně zasahují do zaručených práv, zejména práva na svobodu projevu a práva na informace. Jsme přesvědčeni, že bez zásahu veřejné moci (policejních orgánů, soudu či správního úřadu) je možné přistoupit k tak zásadním krokům, jakým je odstranění obsahu, pouze výjimečně, je třeba upřednostnit nástroje s mírnějšími dopady do sféry tvůrce či šiřitele obsahu. Asi hlavním takovým nástrojem je dočasné omezení peněžních toků za problematický obsah k jeho tvůrci (držiteli příslušného účtu, na němž je obsah šířen), tzv.

„demonetizace“. Jak naznačuje shora uvedený popis modelů, které jsou dnes s šířením online obsahu využívány, v mnoha případech jde o modely, do nichž aktivně zasahuje i provozovatel online platformy. Lze tedy předpokládat, že právě demonetizace by mohla být vhodným nástrojem pro omezení monetizovaného cyberstalkingu do doby, než o konkrétním případu rozhodnou orgány veřejné moci.

V demokratické společnosti je nutné přijmout fakt, že podnikatelé (jimiž provozovatelé online platforem nesporně jsou) nemohou nahrazovat činnost státní moci, ať již jde o kontrolu jednání třetích osob, nebo zavádění represe za nezákonné jednání. Je třeba najít rovnováhu mezi svobodou podnikání a osobní odpovědností na jedné straně, a nápomocí k nezákonnému jednání. Za určitý příklad takové rovnováhy lze uvést český zákon č. 480/2004 Sb., o některých službách informační společnosti, který ve svém § 5 upravuje situace, kdy jedině odpovídá provozovatel online platformy za obsah v ní uložených informací. Takovou odpovědnost provozovatel (slovy zákona: poskytovatel služby, jež spočívá v ukládání informací poskytnutých uživatelem) nese v těchto případech:

- mohl-li vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní, nebo
- dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací.[1]

Jakkoliv první podmínka již zavedla jakousi preventivní povinnost provozovatelů platforem, interpretace této povinnosti byla dosud velice korektní v tom smyslu, že byl požadován skutečně kvalifikovaný důvod vědět o protiprávním jednání či obsahu. Jsme přesvědčeni, že tento limit by neměl být překročen bez zcela zásadního konkrétního důvodu a pro velice konkrétní specifické situace. Právě porušení této rovnováhy je v dnešní době vyčítáno Nařízení DSA, které zejména provozovatele velmi velkých online platforem zatížilo řadou povinností, jež mohou mít za následek omezování svobody projevu a práva na informace, jež navíc mohou prolamovat právo na soukromí apod.

Právní nástroje obrany

[1] Odpovědnost poskytovatele služby za ukládání obsahu informací poskytovaných uživatelem
(1) Poskytovatel služby, jež spočívá v ukládání informací poskytnutých uživatelem, odpovídá za obsah informací uložených na žádost uživatele, jen
a) mohl-li vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní, nebo
b) dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací.
(2) Poskytovatel služby uvedený v odstavci 1 odpovídá vždy za obsah uložených informací v případě, že vykonává přímo nebo nepřímo rozhodující vliv na činnost uživatele.

Způsob právní ochrany proti útokům v podobě monetizovaného cyberstalkingu lze obecně rozdělit do dvou částí:

- právní nástroje vnitrostátního práva
- právní nástroje práva EU

Vnitrostátní právo

Ačkoliv se právní nástroje v jednotlivých členských státech Evropské unie liší (v závislosti na vlastní právní úpravě), v obecné rovině právo České republiky nabízí do jisté míry obdobnou formu ochrany, jako právo většiny ostatních členských států. I proto považujeme za vhodné upozornit na úrovně této (domácí) ochrany z teoretického i praktického hlediska. Ze závěrů lze jistě dovodit požadavky na přiměřenou vnitrostátní regulaci i pro ostatní členské státy Evropské unie, s přihlédnutím k jejich právním, ekonomickým, společenským i kulturním specifikům.

Ochranu proti cyberstalkingu lze z hlediska vnitrostátního práva rozdělit do oblasti veřejnoprávní (zejm. trestněprávní) a soukromoprávní (žaloby o ochranu osobnosti, příp. i předběžné opatření).

V oblasti **trestněprávní** mohou uvedené útoky (zejména jde-li o útoky opakované) naplnit skutkovou podstatu řady trestných činů, jako je nebezpečné vyhrožování (§ 353 trestního zákoníku)[2], nebezpečné pronásledování (§ 354 trestního zákoníku)[3], vydírání (§ 175 trestního

[2] Kdo jinému vyhrožuje usmrcením, těžkou újmou na zdraví nebo jinou těžkou újmou takovým způsobem, že to může vzbudit důvodnou obavu, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.

[3] Kdo jiného dlouhodobě pronásleduje tím, že
a) vyhrožuje ublížením na zdraví nebo jinou újmou jemu nebo jeho osobám blízkým,
b) vyhledává jeho osobní blízkost nebo jej sleduje,
c) vytrvale jej prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje,
d) omezuje jej v jeho obvyklém způsobu života, nebo
e) zneužije jeho osobních údajů za účelem získání osobního nebo jiného kontaktu,
a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.

zákoníku)[4], útisk (§ 177 trestního zákoníku)[5], pomluva (§ 184 trestního zákoníku)[6], ublížení na zdraví (§ 146 trestního zákoníku)[7], o výtržnictví (§ 358 trestního zákoníku)[8] apod.

Výhodou postupu, kdy oběť oznámí podezření ze spáchání trestného činu policejnímu orgánu, je zejména to, že další kroky již realizuje policie, která je povinna prověřit, zda v konkrétních případech skutečně nedošlo ke spáchání trestného činu. K tomuto kroku tedy postačí doručit bez zbytečného odkladu po útoku oznámení, obsahující podrobný popis průběhu, uvedení možných podezřelých osob a doplnění důkazů či návrhů důkazů. Policejní orgán by měl (vyžádá-li si to oznamovatel) oznamovatele následně informovat o tom, jak s podnětem naložil. Lze jen doporučit (byť by tak policejní orgán měl činit i bez návrhu), aby v případě, že policie neshledá v jednání naplnění znaků trestného činu, zvážila, zda nemohl být spáchán alespoň přestupek (v takovém případě by policie měla předat věc příslušnému přestupkovému orgánu k došetření).

Podání trestního oznámení je vždy třeba zvážit, zejména obsahuje-li identifikaci osob, které oznamovatel považuje za viníky. Pokud totiž osoba někoho obviní z trestného činu, přičemž si je vědoma toho, že takové obvinění je lživé (případně je jí pravdivost takového oznámení lhostejná), může se sama dopustit například trestného činu křivého obvinění (§ 345 trestního zákoníku)[9].

Jak ukazuje praxe námi zkoumaných případů, nevýhodou tohoto postupu je jeho pomalost a neúčinnost v praxi. Bohužel, šetření trestných činů v oblasti cyberstalkingu často nevede k účinné ochraně obětí. Je tomu tak často z důvodu nedostatku důkazů (kdy je uplatňována zásada, že v případě pochybností je třeba rozhodnout ve prospěch podezřelého), ale i proto, že povaha jednotlivých útoků (nejde-li o zcela zásadní exces) nemusí být policejními orgány vyhodnocena jako trestný čin, přičemž orgány jen složitě spojují jednotlivé útoky do celkového řetězce

---

[4] Kdo jiného násilím, pohrůžkou násilí nebo pohrůžkou jiné těžké újmy nutí, aby něco konal, opominul nebo trpěl, bude potrestán odnětím svobody na šest měsíců až čtyři léta nebo peněžitým trestem.

[5] Kdo jiného nutí, zneužívaje jeho tísně nebo závislosti, aby něco konal, opominul nebo trpěl, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.

[6] Kdo o jiném sdělí nepravdivý údaj, který je způsobilý značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu, bude potrestán odnětím svobody až na jeden rok.

[7] Kdo jinému úmyslně ublíží na zdraví, bude potrestán odnětím svobody na šest měsíců až tři léta.

[8] Kdo se dopustí veřejně nebo na místě veřejnosti přístupném hrubé neslušnosti nebo výtržnosti zejména tím, že napadne jiného, hanobí hrob, historickou nebo kulturní památku, anebo hrubým způsobem ruší přípravu, průběh nebo zakončení organizovaného sportovního utkání, shromáždění nebo obřadu lidí, bude potrestán odnětím svobody až na dvě léta.

[9]
(1) Kdo jiného lživě obviní z trestného činu, bude potrestán odnětím svobody až na dvě léta.
(2) Kdo jiného lživě obviní z trestného činu v úmyslu přivodit jeho trestní stíhání, bude potrestán odnětím svobody až na tři léta.

uceleného trvajícího útoku. S ohledem na to, že ve zkoumaných případech byla převážná většina útoků směřována proti osobám, které otevřeně vystupovaly proti aktuální vládní politice, nelze v některých případech vyloučit i politické ovlivňování trestních řízení.

I přesto, že v těchto případech je ochrana neúčinná a pomalá (dopady útoků na oběti rostou každý den, kdy jsou zvukově-obrazové záznamy z útoku veřejně dostupné a jsou dále šířeny, kdy jim hrozí opakování útoku apod.), lze předpokládat, že i když orgány nevyhodnotí konkrétní podnět jako relevantní, obdrží-li v tomto směru podnětů více od více osob, problematice cyberstalkingu mohou dát vyšší prioritu.

V oblasti **soukromoprávní** se lze bránit zejména žalobou o ochranu osobnosti. V tomto případě je žalobou zahájeno občanskoprávní řízení, v němž se oběť může domáhat zejména toho, aby se pachatel zdržel svého jednání (např. odstranil zveřejněná videa) a poskytl oběti zadostiučinění ve formě omluvy, případně i ve formě peněžité náhrady nemajetkové újmy.

Výhodou tohoto postupu je, že soud se žalobou musí zabývat, tj. v tomto případě je řízení zahájeno bez ohledu na vyhodnocení věci ze strany orgánů veřejné moci.

Značnou nevýhodou je časová i finanční náročnost tohoto postupu. Řízení v této oblasti trvá obvykle 6-12 měsíců v prvním stupni. Pravomocného rozsudku se lze domoci standardně do 2 let od podání žaloby. Pokud však žalovaná strana použije dostupné nástroje obstrukcí a soud proti nim nezakročí, může podobné řízení trvat i déle. V takovém případě je pak již náprava v podstatě zcela neúčinnou. Podobná řízení si často vyžadují právní podporu, za podání žaloby je nutné zaplatit soudní poplatek, v případě neúspěchu navíc hradí neúspěšná strana náklady soudního řízení straně druhé (ty přitom jen málokdy kompenzují skutečně náklady za advokáta v plné výši).

Domáhá-li se žalobce i peněžité náhrady, je pak (poměrně překvapivě) často problémem i prokázání tak intenzivní újmy, která by odůvodňovala kompenzaci v penězích.

Velmi zásadním problémem navíc často bývá neschopnost oběti identifikovat pachatele. V žalobě musí být jasně uvedeno, proti komu směřuje. Takové informace ale často oběť nemá.

Žaloba musí v těchto případech obsahovat vedle určení žalobce a žalovaného i vylíčení rozhodujících skutečností, označení důkazů i uvedení, čeho se žalobce po soudu domáhá. Žalobce musí k žalobě rovněž připojit písemné důkazy, které navrhuje, a to v listinné či elektronické podobě. Řízení o ochranu osobnosti jsou specifická tím, že žalobce nemusí prokazovat lživost výroků, které o něm žalovaný šíří. Je to naopak žalovaný, kdo je povinen prokázat jejich pravdivost. Žalobce tak v podstatě pouze prokazuje, jakým jednáním došlo k zásahu do jeho práv a jaká újma mu vznikla. Zejména tam, kde žádá i zaplacení peněžité náhrady, je přitom schopnost podrobně tvrdit (popsat) újmu a prokázat ji často velice složité. Lze proto doporučit v případě dlouhodobých útoků zajistit si vyjádření lékaře, psychologa, svědectví kolegů či blízkých o tom, jak se útoky na oběti projevily, jaký vliv měly na její profesní i soukromí život.

Časovou náročnost lze do jisté míry kompenzovat využitím institutu tzv. předběžného opatření. Jím soud může upravit poměry mezi účastníky do doby, než bude pravomocně rozhodnuto, je-li to s ohledem na situaci nezbytné. V případech cyberstalkingu si lze důvodnost předběžného opatření jistě představit, a to zejména pokud jde o požadavek na dočasného odstranění (zablokování) nahrávky útoků z veřejného online prostoru. Předběžné opatření lze přitom směřovat nejen na pachatele, ale i na třetí osobu, tedy například na provozovatele příslušné online platformy.

Výhodou tohoto postupu je jeho rychlost – soud je povinen o předběžném opatření rozhodnout do sedmi dnů od podání návrhu. Pro zahájení řízení je však nezbytné, aby žalobce nejpozději v den, kdy návrh na vydání (nařízení) předběžného opatření podává, uhradil soudu tzv. jistotu, která v těchto případech činí částku 10.000 Kč.

Řízení o předběžném opatření probíhá pouze na základě návrhu, soud tedy nekomunikuje se žalovaným ani s jinou třetí osobou. Je proto nezbytné podrobně popsat soudu nejen skutky, z nichž žalobce dovozuje svůj nárok, ale i důvody, proč je nutné dočasně upravit poměry účastníků, a vše doložit písemnými důkazy (aby měl soud k dispozici dostatek podkladů pro rozhodnutí). Z praktického hlediska je výhodou i to, že pokud soud předběžné opatření nevydá (nenařídí), informuje o tom pouze žalobce, který tak často získá alespoň základní obraz o tom, jak na jeho věc soud nahlíží, případně jak je třeba případnou žalobu doplnit apod. Návrh na nařízení předběžného opatření lze přitom podávat opakovaně, před i po podání žaloby samotné.

V námi evidovaných případech je třeba upozornit na zásadní praktický aspekt ochrany prostřednictvím žalob, a tím je jejich často složitá vynutitelnost. Ani pravomocný rozsudek ve prospěch žalobce totiž automaticky nemusí znamenat, že žalovaný od útoků upustí, že se rozsudku podrobí nebo že zaplatí náhradu nákladů řízení, případně i peněžitou náhradu nemajetkové újmy (nebo se alespoň řádně omluví). Pak je možné postupovat formou vykonávacího (exekučního) řízení, které ovšem také není vždy zcela efektivní.

Přes shora uvedené jsme přesvědčeni o tom, že i postup formou občanskoprávního řízení má praktické dopady. Jednání osob, které porušují své pravomocně stanovené povinnosti, jim může značně přitížit při trestněprávním přezkumu. Navíc, pravomocný rozsudek je velmi silným podkladem pro to, aby příslušný provozovatel online platformy, na které se nahrávka vyskytuje, takový obsah odstranil, a to nikoliv na základě vlastního přezkumu (k tomu viz dále), ale právě na základě rozhodnutí soudu.

Ochrana nástroji práva EU

Ochrana podle Nařízení GDPR

Obecným cílem Nařízení GDPR je posílit základní právo jednotlivce na ochranu jeho soukromí. Každý má právo na ochranu osobních údajů, které se ho týkají, avšak toto právo **není absolutní** –

musí být vyvažováno s dalšími základními právy a svobodami podle principu proporcionality. Nařízení GDPR tedy reflektuje i svobodu projevu a právo na informace a snaží se nalézt rovnováhu mezi právem na soukromí a jinými veřejnými zájmy. Tyto obecné zásady jsou klíčové při posuzování případů cyberstalkingu a obtěžování veřejně činných osob, kde dochází ke střetu mezi právem oběti na ochranu osobních údajů a snahou útočníků obhajovat své jednání svobodou projevu, právem na informace či výkonem práva novináře.

Kyberšikana a komercionalizované obtěžování veřejně činných osob (např. novinářů či politiků) zpravidla spočívá v systematickém obtěžování, narušování soukromí nebo verbálních útocích, které jsou nahrávány a veřejně šířeny online za účelem zisku (monetizace obsahu). Tyto nahrávky často obsahují osobní údaje obětí – zejména obrazové či zvukové záznamy jejich osoby, jméno, případně další informace – a jsou zveřejňovány bez souhlasu obětí. Z pohledu GDPR tak ve většině případů dochází ke zpracování osobních údajů obětí útočníky (či platformami) jako správci, a to potenciálně protiprávním způsobem. Nařízení GDPR přitom takovým obětem poskytuje k obraně některé nástroje, zejména právo na výmaz a námitku (viz dále).

Zákonnost zpracování osobních údajů (čl. 6 GDPR)

Nařízení GDPR vyžaduje, aby každé zpracování osobních údajů mělo tzv. právní základ ve smyslu čl. 6 odst. 1.

Článek 6

Zákonnost zpracování

1. Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;

b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;

c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;

d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;

e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;

f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

První pododstavec písm. f) se netýká zpracování prováděného orgány veřejné moci při plnění jejich úkolů.

Útočníci, kteří bez svolení natáčejí a zveřejňují videa s osobními údaji oběti (její podobiznou, hlasem, projevy apod.), musejí pro takové zpracování mít alespoň jeden z právních titulů uvedených v čl. 6 odst. 1 písm. a)–f). Právě porušení této povinnosti přitom může být jedním z hlavních argumentů obětí cyberstalkingu. Nařízení GDPR obecně uznává následující právní základy pro zpracování osobních údajů:

- **Souhlas subjektu údajů**: Oběť obtěžování ve většině případů neudělila souhlas se záznamem či šířením svých údajů. Bez svobodného, informovaného souhlasu je tento právní základ vyloučen.

- **Plnění smlouvy**, **právní povinnost** či **ochrana životně důležitých zájmů**: Tyto důvody se na situaci obvykle nevztahují – oběť není ve smluvním vztahu s útočníkem a zveřejnění videa obvykle neslouží žádné právní povinnosti ani ochraně života či zdraví.

- **Veřejný zájem** nebo **výkon veřejné moci**: Útočník v námi sledovaných případech nikdy nebyl orgánem veřejné moci ani nejednal na základě zákonného zmocnění. I kdyby argumentoval „veřejným zájmem“ (např. odhalování pravdy o veřejné osobě), muselo by jít o úkol ve veřejném zájmu svěřený správci zákonem, což zde není splněno.

Jediným potenciálním titulem by teoreticky mohl být **oprávněný zájem správce** (útočníka) či třetí strany podle čl. 6 odst. 1 písm. f). Nařízení GDPR stanoví, že zpracování na základě oprávněných zájmů je přípustné pouze, pokud tyto zájmy nepřevažují nad zájmy nebo základními právy a svobodami subjektu údajů.

Recitál 47 Nařízení GDPR k tomu uvádí, že oprávněné zájmy mohou být právním základem zpracování jen za předpokladu řádného zvážení všech okolností a očekávání subjektu údajů. V kontextu obtěžování je zájem útočníka na zisku či „zviditelnění se“ v přímém konfliktu se zájmem oběti na ochraně soukromí, důstojnosti a bezpečí. Ve většině případů je zjevné, že základní práva a svobody oběti (např. právo na soukromý život a ochranu osobních údajů) převažují nad jakýmkoli tvrzeným zájmem útočníka. Obzvláště jde-li o obsah, jehož primárním cílem je oběť znevažovat či zastrašit a generovat zisk z tohoto útoku, stěží lze takové zpracování považovat za oprávněné či spravedlivé.

Recitál 39 GDPR zdůrazňuje, že jakékoli zpracování má být zákonné a spravedlivé a že osobní údaje mají být používány transparentně a pouze k legitimním účelům. V případě cyberstalkingu chybí legitimní účel a transparentnost. Naopak dochází ke zpracování zjevně proti vůli subjektu údajů a způsobem, který může způsobit újmu (což původci útoků nejenže vědí, ale je to i jedním z jejich hlavních motivů).

Zveřejnění záznamu útoku na oběť bez jejího svolení tedy v první řadě většinou nesplňuje podmínky zákonnosti dle čl. 6 Nařízení GDPR. Pro oběť to má významnou právní výhodu: pokud jsou její údaje zpracovávány protiprávně, vzniká jí právo požadovat okamžité ukončení takového zpracování a výmaz údajů (viz dále).

Samozřejmě, ani shora uvedené závěry nelze aplikovat bez dalšího, a to právě s ohledem na právo na informace a svobodu projevu, zejména při výkonu určitých činností, jakými jsou činnosti v oblasti žurnalistiky, vědeckého bádání či umělecké tvorby. Určitá omezení ochrany osobních údajů předpokládá Nařízení GDPR již v recitálu 153, kde výslovně uvádí: „*Právo členského státu by měly uvádět pravidla upravující svobodu projevu a informací, včetně novinářského, akademického, uměleckého nebo literárního projevu, do souladu s právem na ochranu osobních údajů podle*

tohoto nařízení. Na zpracování osobních údajů prováděné výhradně pro novinářské účely nebo pro účely akademického, uměleckého či literárního projevu by se měly vztahovat odchylky nebo výjimky z některých ustanovení tohoto nařízení, je-li to nutné za účelem uvedení práva na ochranu osobních údajů do souladu s právem na svobodu projevu a informací, jak je zakotveno v článku 11 Listiny." Platí to přitom zejména v audiovizuální oblasti. Nařízení GDPR ponechává úpravu těchto výjimek na členských státech. V České republice takovou výjimku obsahuje zákon č. 110/2019 Sb., o zpracování osobních údajů, konkrétně jeho § 17[10]. I ten ovšem akcentuje přiměřenost zpracování, která v námi analyzovaných případech cyberstalkingu hovoří ve prospěch obětí. Je totiž třeba vzít v úvahu, že ne každá „tvorba" naplňuje novinářský účel nebo znaky akademického, uměleckého či literárního projevu.

Zvláštní kategorie údajů a citlivé informace

Při hodnocení možného zásahu do práva na ochranu osobních údajů je nezbytné zkoumat i rozsah osobních údajů, které jsou útočníky zveřejňovány. Článek 9 Nařízení GDPR definuje zvláštní kategorie údajů (tzv. citlivé údaje), mezi něž patří např. údaje o rasovém či etnickém původu, politických názorech, náboženském přesvědčení, členství v odborech a dále genetické a biometrické údaje, údaje o zdravotním stavu, sexuálním životě nebo orientaci. Zpracování těchto údajů je obecně zakázáno s výjimkou taxativně stanovených případů.

Článek 9

Zpracování zvláštních kategorií osobních údajů

1. Zakazuje se zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

V kontextu veřejně činných osob může dojít k tomu, že útočník zveřejní např. informaci o zdravotním stavu, detail z jeho soukromého intimního života, případně využije politické názory či náboženskou příslušnost oběti k útoku. Tyto informace spadají pod zvláštní kategorie údajů a požívají přísnější ochrany. Pro jejich zákonné zpracování musí být naplněna některá z výjimek uvedených v čl. 9 odst. 2.

[10] (1) Osobní údaje lze zpracovávat také tehdy, slouží-li to přiměřeným způsobem pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu. Při posouzení přiměřenosti podle věty první se přihlédne také k tomu, jestli zpracování zahrnuje osobní údaje uvedené v čl. 9 odst. 1 nebo čl. 10 nařízení Evropského parlamentu a Rady (EU) 2016/679.

2. Odstavec 1 se nepoužije, pokud jde o některý z těchto případů:

a) subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů, s výjimkou případů, kdy právo Unie nebo členského státu stanoví, že zákaz uvedený v odstavci 1 nemůže být subjektem údajů zrušen;

b) zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany, pokud je povoleno právem Unie nebo členského státu nebo kolektivní dohodou podle práva členského státu, v němž se stanoví vhodné záruky týkající se základních práv a zájmů subjektu údajů;

c) zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas;

d) zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy tohoto subjektu nebo na osoby, které s ním udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt;

e) zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů;

f) zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo pokud soudy jednají v rámci svých soudních pravomocí;

g) zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů;

h) zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče na základě práva Unie nebo členského státu nebo podle smlouvy se zdravotnickým pracovníkem a při splnění podmínek a záruk uvedených v odstavci 4;

i) zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění přísných norem kvality a bezpečnosti zdravotní péče a léčivých přípravků nebo zdravotnických prostředků, na základě práva Unie nebo členského státu, které stanoví odpovídající a zvláštní opatření pro zajištění práv a svobod subjektu údajů, zejména služebního tajemství;

j) zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely v souladu s čl. 89 odst. 1 na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů.

Například, pokud by video z útoku obsahovalo i hanlivé komentáře o zdravotním stavu či sexuální orientaci oběti, útočník tím zpracovává zvláštní kategorie údajů protiprávně – pro zákonné zpracování zvláštní kategorie osobních údajů si nelze vystačit pouze s některým z právních základů, uvedených v článku 6 Nařízení GDPR. Takové zpracování může představovat závažné porušení Nařízení GDPR, neboť údaje spadající do zvláštní kategorie požívají vysoké ochrany z důvodu rizika vážných zásahů do práv a svobod (diskriminace, stigmatizace apod.).

Recitál 75 Nařízení GDPR výslovně zmiňuje, že zpracování osobních údajů, které vypovídají např. o politických názorech, zdravotním stavu či sexuálním životě, může vést k významné újmě (diskriminaci, poškození pověsti, ekonomické či společenské znevýhodnění atd.). Právě takové následky jsou u cyberstalkingu reálné – útočníci často míří na citlivé aspekty identity oběti (např. politické či osobní) s cílem způsobit jí co největší reputační či psychickou újmu (což v současné době stojí ruku v ruce se zájmem určité části veřejnosti o přístup k bulvárním informacím).

Pokud útočník při obtěžování zpracovává i citlivé údaje oběti, zpravidla jedná v rozporu s čl. 9 Nařízení GDPR. Oběť pak má o to silnější postavení při obraně. Může argumentovat nejen obecnou nezákonností, ale i porušením zákazu zpracování údajů zvláštní kategorie, což může vést k ještě přísnějším postihům pro pachatele i s nimi spolupracujících třetích osob.

„Právo být zapomenut“

Jedním z teoreticky nejmocnějších nástrojů, které Nařízení GDPR oběti poskytuje, je právo na výmaz osobních údajů (čl. 17), někdy označované jako „právo být zapomenut“. Toto právo umožňuje subjektu údajů domoci se odstranění svých osobních údajů u správce, a to bez zbytečného odkladu, jakmile jsou splněny nařízením stanovené podmínky. Pro situace cyberstalkingu jsou relevantní zejména následující důvody pro výmaz podle čl. 17 Nařízení GDPR:

- **Osobní údaje již nejsou potřebné pro daný účel:** I v případě, že se útočník skrývá za veřejným zájmem, je třeba odlišovat informační obsah a formu sdělení. Nepostačí tedy pouze argumentovat důležitostí toho, aby se veřejnost o určitém aspektu života sledované osoby dozvěděla. Je nutné posuzovat i formu (způsob), kterou je informace veřejnosti zprostředkovávána. Jakýkoliv urážlivý či obtěžující obsah nemá legitimní informační účel, a proto zpracování osobních údajů skandalizujícím způsobem není obvykle potřebné, a to ani v případě, kdy by snad šlo o zpracování oprávněné.

- **Odvolání souhlasu**: I v případech, že by snad oběť (subjekt údajů) poskytla v minulosti souhlas se zpracováním svých údajů, nelze jí upřít právo vzít takový souhlas zpět.

- **Námitka proti zpracování a neexistence převažujících důvodů správce:** Pokud oběť vznese námitku proti zpracování a útočník nemá převážný oprávněný důvod, musí být údaje oběti vymazány. V námi sledovaných případech útočník žádný převažující legitimní důvod zřejmě neměl, takže tento důvod k výmazu je naplněn.

- **Osobní údaje byly zpracovány protiprávně**: Pokud došlo v rámci cyberstalkingu ke zpracování osobních údajů nezákonně, má oběť nesporně právo na výmaz svých údajů již jen z tohoto jednoduchého důvodu.

Je-li splněn některý z důvodů pro uplatnění práva na výmaz, je správce osobních údajů povinen údaje bez odkladu vymazat. Oběť tedy může formálně požádat správce o výmaz videa, fotografií či jiných údajů z online platformy. Tato žádost by měla vycházet z konkrétního právního důvodu dle čl. 17 Nařízení GDPR.

Nařízení GDPR řeší i situace, kdy byly osobní údaje zveřejněny online více subjekty. Článek 17 odst. 2 stanoví, že pokud správce zveřejnil osobní údaje a je povinen je vymazat, musí s ohledem na dostupnou technologii učinit přiměřené kroky k informování dalších správců, kteří dané údaje zpracovávají, aby vymazali odkazy na ně či jejich kopie. Pokud tedy útočník nahrál video na platformu a to se objevuje ve vyhledávačích, měl by po obdržení žádosti o výmaz nejen smazat video, ale zajistit i odstranění indexace – např. informovat provozovatele vyhledávače. Tento mechanismus rozšiřuje účinnost „práva být zapomenut“ v prostředí internetu.

Recitál 66 Nařízení GDPR k tomu uvádí, že za účelem posílení práva být zapomenut v online prostředí má správce, který osobní údaje zveřejnil, povinnost informovat ostatní správce (např. provozovatele vyhledávačů) o žádosti subjektu údajů o výmaz všech odkazů na tyto údaje.

Delisting z vyhledávačů

Samotné internetové vyhledávače jsou ve většině případů správcem osobních údajů, protože indexují a poskytují odkazy na webové stránky obsahující osobní údaje. Oběť cyberstalkingu tak může využít právo na výmaz i přímo vůči vyhledávači a žádat stažení odkazů (delisting) na závadný obsah z výsledků vyhledávání. To je důležité, pokud původní online platforma obsah neodstranila nebo pokud byl obsah převzat na jiné weby – oběť může alespoň omezit šíření tím, že jej učiní hůře dohledatelným.

Evropský sbor pro ochranu osobních údajů (EDPB) ve svých *Pokynech 5/2019* upřesnil kritéria práva být zapomenut ve vztahu k vyhledávačům. Tyto pokyny (schválené v červenci 2020) potvrzují, že subjekt údajů může požadovat delisting, pokud je naplněn některý z důvodů podle čl. 17 Nařízení GDPR – v praxi typicky pokud jsou informace nepřesné, irelevantní, nadbytečné, nebo zpracované protiprávně.

Provozovatel vyhledávače musí každou žádost individuálně posoudit v kontextu kolize práva na soukromí a práva na informaci. U veřejně činných osob může hrát roli, zda je informace ve veřejném zájmu. Nicméně pokud jde o obsah obtěžující, urážlivý či zjevně sloužící k šikaně, veřejný zájem na indexaci takového obsahu je minimální.

Omezení práva na výmaz

I právo na výmaz má svá omezení. Zásadní výjimku upravuje čl. 17 odst. 3 písm. a) Nařízení GDPR. Podle něj se právo na výmaz neuplatní, pokud je zpracování nezbytné pro výkon práva na svobodu projevu a informace. To znamená, že v případech zpracování osobních údajů pro účely žurnalistické, umělecké či akademické může správce odmítnout smazat údaje, pokud by tím byla nepřiměřeně potlačena svoboda projevu. Dále jsou výjimky pro splnění právní povinnosti, veřejný zájem (archivace, výzkum) či uplatnění právních nároků.

Článek 17

Právo na výmaz („právo být zapomenut“)

1. Subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů:

a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;

b) subjekt údajů odvolá souhlas, na jehož základě byly údaje podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) zpracovány, a neexistuje žádný další právní důvod pro zpracování;

c) subjekt údajů vznese námitky proti zpracování podle čl. 21 odst. 1 a neexistují žádné převažující oprávněné důvody pro zpracování nebo subjekt údajů vznese námitky proti zpracování podle čl. 21 odst. 2;

d) osobní údaje byly zpracovány protiprávně;

e) osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Unie nebo členského státu, které se na správce vztahuje;

f) osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1.

2. Jestliže správce osobní údaje zveřejnil a je povinen je podle odstavce 1 vymazat, přijme s ohledem na dostupnou technologii a náklady na provedení přiměřené kroky, včetně technických opatření, aby informoval správce, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie či replikace.

3. Odstavce 1 a 2 se neuplatní, pokud je zpracování nezbytné:

a) pro výkon práva na svobodu projevu a informace;

b) pro splnění právní povinnosti, jež vyžaduje zpracování podle práva Unie nebo členského státu, které se na správce vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen;

c) z důvodů veřejného zájmu v oblasti veřejného zdraví v souladu s čl. 9 odst. 2 písm. h) a i) a čl. 9 odst. 3;

d) pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely v souladu s čl. 89 odst. 1, pokud je pravděpodobné, že by právo uvedené v odstavci 1 znemožnilo nebo vážně ohrozilo splnění cílů uvedeného zpracování;

e) pro určení, výkon nebo obhajobu právních nároků.

Právo vznést námitku proti zpracování

Právo na námitku dává subjektu údajů možnost kdykoli vznést námitku proti zpracování jeho osobních údajů, pokud je zpracování prováděno na základě oprávněných zájmů správce nebo pro účely veřejného zájmu či výkon veřejné moci. Námitku je třeba opřít o důvody týkající se konkrétní situace subjektu údajů. V námi analyzovaných případech by oběti mohly namítat, že správce nesmí nadále jejich údaje zpracovávat s ohledem na to, že tímto zpracováním vzniká oběti nepřiměřená újma.

Po vznesení námitky má správce povinnost ukončit zpracování, ledaže prokáže závažné oprávněné důvody, které převažují nad zájmy a právy subjektu údajů, nebo jde-li o určení či obhajobu právních nároků. V případě cyberstalkingu může oběť uplatnit řadu argumentů, které podporují oprávněnost námitky.

To nakonec vyplývá například z recitálu 47 Nařízení GDPR, který připomíná, že při posuzování námitek je třeba vzít v úvahu rozumná očekávání subjektu údajů a kontext. Oběť rozhodně neočekává, že bude potají nahrávána a zneužita ke komerční zábavě publika. Navíc ekonomická motivace správce není zvlášť chráněným zájmem ve srovnání s právem na soukromí či ochranu cti oběti (případně i jejích blízkých).

Pokud by správce namítal veřejný zájem nebo žurnalistický účel, musel by dokázat, že jeho záznam skutečně přináší veřejnosti relevantní informaci převyšující zásah do práv oběti, včetně toho, že tento účel nelze splnit způsobem mírnější co do zásahů do práv oběti. To by u zinscenovaných provokací a urážek bylo velmi obtížné. Ve většině případů tak námitka oběti bude oprávněná a správce nemá jak prokázat převažující důvody.

Podání stížnosti u dozorového úřadu (ÚOOÚ)

Nařízení GDPR dává subjektům údajů právo podat stížnost u nezávislého dozorového úřadu, pokud se domnívají, že zpracováním jejich osobních údajů došlo k porušení GDPR. V ČR je tímto úřadem Úřad pro ochranu osobních údajů (ÚOOÚ). Oběť cyberstalkingu se tedy může obrátit na ÚOOÚ se stížností, v níž popíše situaci (např. že jistá osoba/kanál zveřejnil/a video obsahující její osobní údaje bez souhlasu a přes její protesty je nesmazal/a). Dozorový úřad má povinnost stížnost prošetřit a informovat stěžovatele o výsledku.

Výhodou podání stížnosti je, že se věcí začne zabývat orgán veřejné moci nadaný pravomocí prověřit situaci a udělit sankce těm, kdo jednají v rozporu s Nařízením GDPR. Úřad může například nařídit různá opatření k nápravě, vč. odstranění obsahu, uložit pokutu apod. Jde o administrativně jednodušší postup, než je ochrana soudní cestou. Výhodou je rovněž to, že dojde-li k omezení přístupu k online obsahu na základě rozhodnutí správního úřadu, jde o postup, proti němuž se lze právně bránit (v případě možného zneužití Nařízení GDPR k omezení svobody projevu).

Tento postup lze doporučit i proto, že dojde-li ÚOOÚ k závěru o tom, že konkrétní online platforma je zneužívána pro účely cíleného zásahu do ochrany osobních údajů opakovaně, může jít o velice důležité vodítko i pro další orgány veřejné moci, zejména v oblasti trestního práva.

Soudní ochrana a náhrada újmy

Proti porušování ochrany osobních údajů se lze bránit i soudní cestou. Možné důsledky porušení práv zaručených Nařízením GDPR uvádí například recitál 85: ztráta kontroly nad osobními údaji, diskriminace, zneužití identity, poškození pověsti, jiné významné hospodářské či společenské znevýhodnění dotčených fyzických osob. V tomto případě lze o porušení práv stanovených v Nařízení GDPR doplnit civilněprávní žalobu, jak je popsána výše v kapitole ***Vnitrostátní právo***.

Role nevládního sektoru

Jak výslovně vyplývá z čl. 80 Nařízení GDPR, práva na ochranu proti nezákonnému zpracování osobních údajů vůči dozorovému úřadu či soudu lze uplatnit nejen individuálně, ale i prostřednictvím k tomu založených nevládních organizací.

Ochrana podle Nařízení DSA

V oblasti ochrany před cyberstalkingem bude jistě hrát důležitou roli i Nařízení DSA. Tento nástroj je v současné době předmětem mnoha diskusí. Kritizován (dle našeho názoru důvodně) je zejména proto, že pro podnikatele v oblasti provozování online platforem zavádí řadu administrativních povinností, nepřiměřeně přenáší na soukromý sektor povinnosti v oblasti ochrany před porušováním práva a může se stát i nástrojem cenzury. Jeho význam pro ochranu obětí cyberstalkingu však nelze ignorovat.

V recitálu 40 Nařízení DSA je výslovně zdůrazněna nutnost chránit uživatele před nenávistnými výroky, sexuálním obtěžováním či jinou diskriminací. Podobně jako Nařízení GDPR, i Nařízení DSA zmiňuje zásadu proporcionality, kdy opatření platforem proti škodlivému obsahu musejí být přiměřená, nezbytná a sledovat legitimní cíle veřejného zájmu.

Nezákonný vs. škodlivý obsah

Nařízení DSA zaměřuje hlavní pozornost na **nezákonný obsah**, tedy takový, jehož šíření je v rozporu s právními předpisy. Recitál 12 uvádí jako příklady mimo jiné **sdílení intimních snímků bez souhlasu** či **online pronásledování**. Pokud je obsah identifikován jako nezákonný (v souladu s příslušným vnitrostátním právem), mají provozovatelé online platforem povinnost jej **neprodleně odstranit nebo znemožnit přístup k němu** (tzv. notice-and-takedown).

Z pohledu demokratického právního státu je však sporné, do jaké míry je přípustné, aby o „nezákonnosti“ obsahu fakticky rozhodovali soukromí poskytovatelé služeb – a nesli i odpovědnost za případné chybné posouzení. Zatímco v některých případech (například dětská pornografie) je nezákonnost obsahu zřejmá, v oblasti cyberstalkingu je hranice mezi **nepřijatelným pronásledováním** a **tvrdou či bulvární, ale stále legitimní kritikou** mnohem jemnější.

Právě zde je podle našeho názoru nezbytné DSA **aplikovat zvlášť citlivě**, s respektem k ochraně svobody projevu a práva na informace, včetně práva na veřejnou kontrolu výkonu státní moci. Ne každý kritický (a třeba i nevkusně bulvární) obsah lze bez dalšího kvalifikovat jako cyberstalking. Nařízení DSA by nemělo být využíváno jako prostředek k umlčování žurnalistiky – ať už provozované tradičními médii, nebo jednotlivými blogery a tvůrci obsahu.

Nařízení DSA zároveň rozlišuje **nezákonný obsah** a **obsah škodlivý, ale zákonný**. Narozdíl od nezákonného obsahu nepožaduje Nařízení DSA přímý zásah provozovatelů proti škodlivému, ale zákonnému, obsahu. Provozovatelé mohou škodlivý obsah regulovat prostřednictvím svých smluvních podmínek a vnitřních pravidel.

Problematickou se zejména z tohoto hlediska jeví úprava vztahující se k tzv. velmi velkým online platformám (VLOP). Jim Nařízení DSA ukládá rozšířené povinnosti, a to nejen ve vztahu k nezákonnému a škodlivému obsahu, ale například i v souvislosti s krizovými situacemi,

ovlivňováním „veřejného diskurzu“ apod. S ohledem na předmět této analýzy se na problematické aspekty Nařízení DSA nezaměřujeme nad rámec, v němž se dotýká otázky cyberstalkingu.

Povinnosti platforem a reakce na nezákonný obsah

Podle článku 16 Nařízení DSA musí poskytovatelé hostingových služeb zřídit **mechanismus pro oznamování nezákonného obsahu** („notice and action“).

Článek 16

Mechanismy oznamování a přijímání opatření

1. Poskytovatelé hostingových služeb zavedou mechanismy, které osobám a subjektům umožňují oznamovat těmto poskytovatelům výskyt konkrétních informací v rámci jejich služby, které dotyčná osoba nebo subjekt považují za nezákonný obsah. Tyto mechanismy musí být snadno dostupné a uživatelsky přívětivé a musí umožňovat podávání oznámení elektronickými prostředky.

2. Mechanismy uvedené v odstavci 1 musí usnadňovat podávání dostatečně přesných a náležitě odůvodněných oznámení. Za tímto účelem přijmou poskytovatelé hostingových služeb nezbytná opatření, aby umožnili a usnadnili podávání oznámení obsahujících všechny tyto prvky:

a) dostatečně podložené vysvětlení důvodů, proč daná osoba či subjekt tvrdí, že dotčené informace představují nezákonný obsah;

b) jednoznačný údaj o přesném elektronickém umístění těchto informací, například přesnou jednotnou adresu URL nebo adresy URL, a v případě potřeby dodatečné informace umožňující identifikovat nezákonný obsah v závislosti na typu obsahu a konkrétním typu hostingové služby;

c) jméno osoby nebo název subjektu podávajících oznámení a jejich e-mailovou adresu, kromě případu informací, o nichž se usuzuje, že představují jeden z trestných činů uvedených v článcích 3 až 7 směrnice 2011/93/EU;

d) prohlášení potvrzující, že se osoba nebo subjekt podávající oznámení v dobré víře domnívají, že informace a tvrzení obsažené v oznámení jsou přesné a úplné.

3. Má se za to, že oznámení uvedená v tomto článku vedou ke zjištění dotčené informace či dozvědění se o ní pro účely článku 6, pokud pečlivému poskytovateli hostingových služeb umožňují odhalit nezákonnost dotyčné činnosti či informace bez podrobného právního přezkumu.

4. Pokud oznámení obsahuje elektronické kontaktní informace osoby nebo subjektu podávajících oznámení, zašle jim poskytovatel hostingových služeb bez zbytečného odkladu potvrzení o obdržení oznámení.

5. Poskytovatel bez zbytečného odkladu též uvědomí osobu či subjekt podávající oznámení o svém rozhodnutí s ohledem na informace, jichž se oznámení týká, a poskytne jim informace o dostupných možnostech nápravy v souvislosti s tímto rozhodnutím.

6. Poskytovatelé hostingových služeb vyřizují veškerá oznámení, která obdrží na základě mechanismů uvedených v odstavci 1, a přijímají rozhodnutí s ohledem na informace, jichž se oznámení týkají, včas, nesvévolně, objektivně a s náležitou péčí. Pokud při tomto vyřizování nebo rozhodování používají automatizované postupy, uvedou informace o jejich použití v potvrzení podle odstavce 5.

Zároveň jsou povinni zajistit, aby o každém rozhodnutí, jímž omezí obsah nebo služby (například odstraní příspěvek, omezí jeho viditelnost, pozastaví účet nebo demonetizují obsah), byl dotčený uživatel informován a měl k dispozici účinné opravné prostředky (čl. 17).

Recitál 54 a čl. 17 odst. 3 požadují, aby **každé takové rozhodnutí bylo odůvodněno** – musí obsahovat právní nebo smluvní důvod zásahu a být transparentně evidováno. Tato ustanovení jsou zásadní také v případech, kdy platforma omezí nebo zcela zablokuje **monetizaci obsahu útočníka**. Jde totiž o zásah do jeho hospodářských práv, který vyžaduje jasný právní základ a možnost přezkumu.

Každému příjemci služby (poskytovateli obsahu), jehož obsah je odstraněn, blokován, degradován nebo demonetizován, musí poskytovatel:

- srozumitelně vysvětlit důvod omezení,
- uvést, zda byl obsah posouzen jako nezákonný, nebo jen v rozporu s podmínkami služby,
- informovat o dostupných opravných prostředcích (interní stížnost, mimosoudní řešení sporu, soudní ochrana).

Článek 17

Odůvodnění

1. Poskytovatelé hostingových služeb poskytnou všem dotčeným příjemcům služby jasné a konkrétní odůvodnění kteréhokoli z následujících omezení uloženého z důvodu, že informace poskytnuté příjemcem služby mají nezákonný obsah nebo jsou neslučitelné s jejich smluvními podmínkami:

a) veškerá omezení viditelnosti konkrétních informací poskytnutých příjemcem služby, včetně odstranění obsahu, znemožnění přístupu k obsahu nebo přiřazení horší pozice tomuto obsahu ve vyhledávání;

b) pozastavení, ukončení nebo jiné omezení peněžních plateb;

c) úplné nebo částečné pozastavení nebo ukončení poskytování služby;

d) pozastavení nebo zrušení účtu příjemce služby.

2. Odstavec 1 se použije pouze tehdy, jsou-li poskytovateli známy příslušné elektronické kontaktní údaje. Použije se nejpozději ode dne, kdy je omezení uloženo, a bez ohledu na to, proč a jak bylo toto omezení uloženo.

Odstavec 1 se nepoužije, pokud se jedná o klamavý obchodní obsah ve velkém objemu.

3. Odůvodnění uvedené v odstavci 1 obsahuje alespoň tyto informace:

a) informace, zda rozhodnutí obnáší odstranění informací, znemožnění přístupu k nim, přiřazení horší pozice ve vyhledávání, omezení jejich viditelnosti nebo pozastavení či ukončení peněžních plateb souvisejících s těmito informacemi či ukládá jiná opatření podle odstavce 1 v souvislosti s těmito informacemi, a v relevantních případech územní působnost tohoto rozhodnutí a jeho dobu platnosti;

b) skutečnosti a okolnosti, z nichž rozhodnutí vychází, v relevantních případech včetně informací, zda bylo rozhodnutí přijato na základě oznámení podaného podle článku 16 nebo na základě dobrovolného šetření z vlastního podnětu, a je-li to nezbytně nutné, identitu oznamovatele;

c) v relevantních případech informace o použití automatizovaných postupů při přijímání rozhodnutí, včetně informace, zda bylo rozhodnutí přijato s ohledem na obsah zjištěný či identifikovaný automatizovanými postupy;

d) týká-li se rozhodnutí údajně nezákonného obsahu, odkaz na příslušný právní základ a vysvětlení, proč se informace z tohoto důvodu pokládají za nezákonný obsah;

e) jestliže se rozhodnutí zakládá na údajné neslučitelnosti informací se smluvními podmínkami poskytovatele hostingových služeb, odkaz na příslušný smluvní základ a vysvětlení, proč se informace pokládají za neslučitelné s příslušným(i) ustanovením(i);

f) jasné a uživatelsky vstřícné informace o možnostech nápravy, které má příjemce služby s ohledem na rozhodnutí k dispozici, zejména prostřednictvím případných interních mechanismů vyřizování stížností, mimosoudního řešení sporů a soudní nápravy.

4. Informace poskytnuté poskytovatelem hostingových služeb v souladu s tímto článkem musí být jasné, snadno srozumitelné a co nejpřesnější a nejkonkrétnější s ohledem na okolnosti. Informace musí být zejména takové, aby dotčenému příjemci služby přiměřeně umožnily účinně uplatnit dostupné možnosti nápravy uvedené v odst. 3 písm. f).

5. Tento článek se nevztahuje na příkazy podle článku 9.

Provozovatelé online platforem mají podle Nařízení DSA dále povinnost zavést **účinný interní systém vyřizování stížností** proti rozhodnutím o odstranění obsahu, pozastavení služby, zrušení účtu či omezení viditelnosti nebo zpeněžení. Tento systém musí být uživatelsky dostupný po dobu nejméně šesti měsíců od rozhodnutí a musí respektovat krátké lhůty pro vyřízení. Uživatelé tak mají možnost se **bránit proti „podregulaci“** (nečinnosti platformy) i **proti přehnaně tvrdým zásahům**.

Opatření proti ekonomickým stimulům útočníků

Nařízení DSA reflektuje i skutečnost, že jedním z motivů kyberútočníků může být **ekonomický zisk** (například z výnosů z reklamy, příspěvků fanoušků či jiných forem monetizace). Recitál 68 uvádí, že reklama na platformách může přispívat k „*finančním pobídkám ke zveřejňování či šíření nezákonného nebo jinak škodlivého obsahu*“.

Aby se těmto motivacím předešlo, uvádí Nařízení DSA mezi možnými opatřeními proti nezákonnému obsahu i možnost **pozastavit, ukončit nebo jinak omezit peněžní platby** (čl. 17 odst. 1 písm. b). Recitál 55 výslovně stanoví, že „*zpeněžení informací*“ lze omezit pozastavením nebo ukončením plateb příjemci.

V kontextu monetizovaného cyberstalkingu jde o **mimořádně významný nástroj**: je-li jasně identifikováno, že určitý obsah představuje nezákonný cyberstalking, může platforma – za splnění podmínek proporcionality a transparentnosti – přistoupit k odříznutí pachatele od finančních toků, které jeho jednání motivují a udržují.

Pokud poskytovatel tato opatření uplatní (například zablokuje platby nebo odstaví monetizační kanál), musí – s výjimkou výslovně stanovených případů – dotčeného uživatele **informovat** a

poskytnout mu **odůvodnění**. Nařízení tak usiluje o to, aby ani demonetizace nebyla svévolná, ale podléhala **kontrole a přezkumu**.

Další procesní práva a role koordinátora digitálních služeb

Vedle interního systému stížností vytváří Nařízení DSA prostor také pro **alternativní (mimosoudní) řešení sporů**. Spory mají být řešeny u subjektů, které k tomu získají zvláštní certifikaci od koordinátora digitálních služeb příslušného členského státu. V České republice plní funkci koordinátora digitálních služeb **Český telekomunikační úřad (ČTÚ)**.

Podle článku 53 Nařízení DSA mohou dotčené subjekty podat **stížnost přímo koordinátorovi digitálních služeb**, domnívají-li se, že platforma porušila své povinnosti podle Nařízení DSA. Koordinátor může ve věci provést šetření a přijmout vlastní opatření.

Nařízení DSA současně zavádí institut **„důvěryhodných oznamovatelů" (trusted flaggers)** – zvláštních právnických osob, které koordinátor digitálních služeb pověří dozorem nad obsahem na platformách. Oznámení těchto subjektů musí provozovatelé platforem vyřizovat **přednostně**. V kontextu cyberstalkingu mohou důvěryhodní oznamovatelé sehrát důležitou úlohu, pokud budou:

- jasně specializovaní na oblast online útoků a pronásledování,
- fungovat na základě transparentních kritérií,
- jejich činnost bude podléhat skutečnému veřejnému dohledu, aby se z tohoto institutu nestal nástroj selektivní cenzury.

Oznámení provozovateli online platformy a stížnost k ČTÚ (praktická rovina)

V praktické rovině lze Nařízení DSA využít zejména v rámci **postupu oběti monetizovaného cyberstalkingu**:

1. **Oznámení nezákonného obsahu provozovateli platformy**

   Oběť může (přímo nebo prostřednictvím právního zástupce) využít mechanismus podle čl. 16 Nařízení DSA a podat **oznámení nezákonného obsahu**. Provozovatel má povinnost na oznámení reagovat a v případě, že nevyhoví, poskytnout odůvodnění a umožnit podání stížnosti proti rozhodnutí. V závažných případech lze v oznámení výslovně upozornit i na možnost **demonetizace** daného obsahu či účtu útočníka.

2. **Stížnost ke koordinátorovi digitálních služeb (ČTÚ)**

Nedojde-li k nápravě ze strany provozovatele platformy, může oběť (je-li uživatelem služeb dotčené online platformy) podat **stížnost k Českému telekomunikačnímu úřadu** jako koordinátorovi digitálních služeb. ČTÚ je povinen věcí se zabývat, provést vlastní šetření a případně přijmout příslušná opatření vůči platformě.

Nařízení DSA tak vedle rizik, která přináší v oblasti svobody projevu a „privatizace" rozhodování o nezákonnosti obsahu, obsahuje i **využitelné procesní nástroje**, jež mohou oběti monetizovaného cyberstalkingu poskytnout konkrétní ochranu – zejména v kombinaci s prostředky vnitrostátního práva a Nařízení GDPR.

Další procesní práva

Vedle stížnosti podané proti rozhodnutí provozovatele online platformy vytváří Nařízení DSA i prostor pro obranu v rámci tzv. alternativního (mimosoudního) řešení sporů. Tento proces by měl probíhat u subjektů, které k tomu získají zvláštní certifikaci koordinátorem digitálních služeb příslušného členského státu (v České republice je tímto koordinátorem Český telekomunikační úřad). Ve smyslu článku 53 pak mohou dotčené subjekty podat stížnost na porušování Nařízení DSA i přímo koordinátorovi digitálních služeb.

Možný postup ochrany před komercionalizovanou šikanou

Jak vyplývá ze shora uvedeného, nástrojů obrany před monetizovaným cyberstalkingem nabízí české právo (jehož součástí je i právo EU) více. Zásadní otázkou jsou však rychlost a skutečná účinnost těchto nástrojů. V případě, že se oběť podobných útoků chce bránit, lze zvážit kombinaci několika kroků:

1. **Podnět k orgánům činným v trestním řízení**

   Praktické zkušenosti ukazují, že trestněprávní obrana proti dosavadním projevům kybernetického obtěžování či pronásledování se do jisté míry míjí účinkem. Důvodů může být více. Odhlédneme-li od mimoprávních teorií, lze za hlavní považovat princip tzv. subsidiarity trestní represe, tedy zásadu, že trestněprávní postih by měl nastoupit až v případě, že věc nelze řešit mírnějšími nástroji. I přesto lze podnět pro podezření ze spáchání trestného činu považovat za vhodné řešení. A to i pro případ, že by konkrétní útok policejní orgány nevyhodnotily jako trestný čin. Nelze totiž vyloučit, že v případě souběhu více takových podnětů již svůj přístup přehodnotí. Navíc, i kdyby konkrétní útok (nebo více útoků) nebyl vyhodnocen jako trestný čin, nelze vyloučit jeho kvalifikaci jako přestupku.

   Podání podobného podnětu je relativně jednoduché. Zákon nepředepisuje žádnou konkrétní formu, podání lze navíc učinit i osobně na policejní služebně. Podobný krok má výhodu i

v tom, že konkrétní útok bude touto cestou formálně zaznamenán, což může mít přínos i pro další (či následné) kroky.

2. Žaloba o ochranu osobnosti

Ochrana formou žaloby v občanskoprávním řízení je postupem již náročnějším, a to z hlediska formy i času. Přesto může jít o nástroj účinný, a to hned z několika důvodů. V první řadě může soud rozhodnout o odstranění škodlivého obsahu, případně rovněž o náhradě vzniklé nemajetkové újmy. Navíc, pravomocné rozhodnutí může sloužit i pro další jednání například s provozovatelem online platformy, jejímž prostřednictvím je škodlivý obsah monetizován.

V případě, že oběť požaduje i peněžitou náhradu nemajetkové újmy, dostává se do složitějšího postavení. Vedle vyššího soudního poplatku (a případné náhrady nákladů soudního řízení v případě neúspěchu ve věci) jsou na žalobce kladeny mnohem větší nároky pro prokázání skutečně vzniklé újmy. Bohužel, v českém právním řádu není stále příliš respektován názor, podpořený i nálezy Ústavního soudu, že v podstatě jakýkoliv zásah do lidské důstojnosti je jen stěží reparovatelný. Je tedy třeba počítat s nutností prokazovat vznik újmy například svědeckými výpověďmi rodinných příslušníků či jiných blízkých osob, lékařskými zprávami apod.

Je rovněž nutné počítat s nemalou časovou investicí. Soudní řízení v podobných sporech si často vyžádá dobu nejméně 6-12 měsíců, v případě, že se některá ze stran odvolá, pak dosahuje i dvou let.

3. Předběžné opatření

Časové nevýhody žaloby o ochranu osobnosti do jisté míry kompenzuje podání návrhu na nařízení předběžného opatření. Jím se poškozený může domoci toho, aby soud přijal určitá opatření do doby, než dojde k pravomocnému rozhodnutí ve věci. Poškozený se tak může domáhat například dočasného stažení škodlivého obsahu z platformy.

Podmínkou tohoto postupu je zaplacení tzv. jistoty ve výši 10.000 Kč. Jistota přitom musí být u soudu složena nejpozději v den, kdy je návrh na nařízení předběžného opatření k soudu podán. Tento návrh lze přitom podat i před podáním žaloby. Pokud soud návrhu vyhoví, uloží poškozenému, aby do určité lhůty podal ve věci žalobu samotnou, jinak předběžné opatření zruší.

Protože o předběžném opatření rozhoduje soud bez jednání, dokonce si ani nevyžádá stanovisko žalovaného, je nutné k němu připojit dostatek důkazů, z nichž soud může vyhodnotit důvodnost vydání předběžného opatření. Takové opatření je vykonatelné (tedy závazné) okamžikem, kdy je doručeno tomu, jehož se týká, a zavazuje ho až do pravomocného rozhodnutí soudu, případně na základě úspěšného odvolání žalovaného.

Před použitím tohoto nástroje je třeba zvážit i zvláštní důsledek, který je s nařízením předběžného opatření spojen. Zanikne-li totiž toto opatření jinak, než proto, že je žalobě nakonec vyhověno, je žalobce povinen nahradit škodu a jinou újmu každému, komu předběžným opatřením vznikla.

Závěrem je třeba doplnit, že návrh na nařízení předběžného opatření lze podat i proti jiné osobě, než je žalovaný (tedy v tomto případě původce cyberstalkingu). Vyloučit tak nelze ani předběžné opatření vůči provozovateli online platformy apod.

4. Žádost o výmaz a námitka provozovateli online platformy dle GDPR

Vedle shora uvedených instrumentů vnitrostátního práva je možné podat k provozovateli online platformy, jejímž prostřednictvím se záznam z útoků veřejně šíří, žádost o výmaz osobních údajů ve smyslu čl. 17 Nařízení GDPR, společně s námitkou proti takovému zpracování.

5. Stížnost k ÚOOÚ

Stejně tak lze proti nezákonnému zpracování podat stížnost k Úřadu pro ochranu osobních údajů, který je povinen se jí zabývat. Ve vztahu k provozovateli online platformy má smysl takovou stížnost podat zejména v situaci, kdy provozovatel sám na podněty poškozeného nereagoval.

6. Oznámení provozovateli online platformy dle DSA

Využít lze rovněž nástroje oznámení nezákonného obsahu (notice) dle čl. 16 Nařízení DSA. Provozovatel platformy má v tomto případě povinnost na oznámení reagovat a v případě, že mu nevyhoví, poskytnout stěžovateli odůvodnění a právo podat proti rozhodnutí stížnost. Nařízení DSA dokonce vytvořilo institut tzv. „důvěryhodných oznamovatelů“ (trusted flaggers) – jde o zvláštní právnické osoby, které jsou koordinátorem digitálních služeb oprávněny k jakémusi zvláštnímu dohledu nad obsahem zpracovávaným v online platformách. Ve smyslu Nařízení DSA jsou provozovatelé povinni vyřizovat jejich oznámení přednostně.

7. Stížnost k ČTÚ

Nedojde-li k nápravě ze strany provozovatele platformy, je možné při splnění podmínek čl. 53 DSA podat stížnost k Českému telekomunikačnímu úřadu, který ve věci může přijmout vlastní rozhodnutí.

Několik doporučení k dokazování

V souladu s úvodem této analýzy, kde je opakovaně zdůrazňován princip minimalizace regulace a princip osobní odpovědnosti, považujeme za vhodné v první řadě využít existujících možností právní obrany proti monetizovanému cyberstalkingu. Dlouhodobá praxe totiž ukazuje, že policejní

i další orgány často zahájí prověřování možného spáchání trestného činu v momentě, kdy se ukáže, že jde o opakované jednání, směřované proti více osobám, tedy že nejde o ojedinělý exces.

Příprava podání v podobných situacích však naráží na několik překážek. Tou první je překážka ekonomická a časová – sepis jakéhokoliv podání není triviální záležitostí, často vyžaduje asistenci právního specialisty, což je nákladná záležitost. Příprava podání rovněž vyžaduje určitý čas. Řada obětí tak raději volí cestu pasivní a mnoho útoků tak zůstane příslušným orgánům skryto.

Další bariérou je pak otázka dokazování. Je nanejvýš vhodné, aby si osoba, která se cítí být obětí podobného cyberstalkingového útoku, pořídila o takovém jednání dostatek důkazů. V opačném případě totiž pak často příslušné orgány čelí problému „slovo proti slovu“, nadto organizovaní útočníci nemají problém si vzájemně průběh incidentu dosvědčit tak, jak potřebují.

Je třeba poukázat na to, že jako důkaz může být použito vše, co může osvětlit (osvědčit) průběh nějakého děje.

V tomto směru se tak jako nejvhodnější jeví **nahrávka incidentu** (ale i toho, co po něm následovalo). České právo podobné pořizování zvukových či obrazových záznamů povoluje i bez souhlasu druhé strany, a to v ustanovení § 88 odst. 1 občanského zákoníku („*Svolení není třeba, pokud se podobizna nebo zvukový či obrazový záznam pořídí nebo použijí k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob.*“). Obdobně i Nařízení GDPR uvádí v čl. 6 odst. 1 mezi podmínkami zákonného zpracování osobních údajů bez souhlasu příslušné osoby (subjektu údajů) nezbytnost pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby (písm. d) a nezbytnost pro účely oprávněných zájmů toho, kdo údaje zpracovává, či třetí osoby (písm. f).

Důležitým důkazem může být také **svědectví** kolemjdoucích osob. V tomto případě je třeba vyžádat si hned po odeznění útoku od svědků kontaktní a identifikační údaje. Lze dále jen doporučit, aby si oběť vyžádala od svědka i písemné čestné prohlášení o incidentu. Ačkoliv takové prohlášení většinou (zejména pro účely soudů) nepostačí, je určitou zárukou, že svědek skutečně v budoucnu své svědectví poskytne a že například pod nátlakem druhé strany výpověď nezmění.

Zcela zásadní je pak zajistit si **dokumentaci obsahu**, který útočníci zveřejnili na sociálních sítích. Ideální (byť nákladnou) formou je pořízení notářského zápisu. Obvykle ale postačí i například videonahrávka, záznam obrazovky (tzv. screenshot) apod. Je rovněž vhodné evidovat si čas zveřejnění (nebo čas, kdy byl pořízen záznam o obsahu) a hypertextový odkaz na umístění předmětného obsahu (i kdyby držitel účtu na sociálních sítích obsah odstranil, provozovatelé online platforem jsou schopni ho zpětně dohledat, a to zejména, jsou-li k tomu vyzvány policejními orgány).

S cílem usnadnit obětem uplatnění shora uvedených právních nástrojů vnitrostátního práva i práva Evropské unie uvádíme v přílohách této analýzy několik příkladů podání. Upozorňujeme pouze, že jde o vzory, které je v každém konkrétním případě nutné upravit dle konkrétní věci, ve složitějších případech je vždy vhodné využít pomoci odborníka.

Praktické problémy obrany proti cyberstalkingu

Ačkoliv právo poskytuje řadu nástrojů pro obranu, jak je uváděno výše, ne vždy tyto nástroje poskytnou předpokládanou pomoc. Mezi hlavní reálné problémy lze uvést následující:

- skrytá identita pachatele – ne vždy je snadné zjistit, kdo je původcem útoku, což ztěžuje, případně znemožňuje postup prostřednictvím občanskoprávních nástrojů (žaloba, předběžné opatření)
- skrytá identita provozovatele online platformy – v některých případech se útočníci schovávají za platformami, jejichž vlastnictví je různými nástroji zakrýváno, což pak vede k tomu, že takový provozovatel nereaguje na podání, případně ani na pravomocná rozhodnutí orgánů veřejné moci
- nečinnost orgánů veřejné moci – je třeba počítat i s tím, že například policejní orgány nepřistupují k vyšetřování oznámených skutků tak rychle, jak by si oběť představovala
- faktická nevynutitelnost rozhodnutí – ani pravomocný rozsudek nemusí vést ke konečnému efektu, zejména pokud se útočník (příp. provozovatel platformy) prostě odmítne rozsudku podřídit; jde-li o osoby s určitým způsobem skrytou identitou (v případě platforem může jít o provozovatele registrovaného v cizím státu apod.), o osoby, které již čelí exekučním řízením apod., pak ani rozsudek nemusí vést k nápravě

S uvedenými riziky je třeba počítat. Je však rovněž třeba připomenout, že v případě opakovaných jednání s podobnými scénářem a podobnými aktéry (např. opakované využívání konkrétní platformy) nelze vyloučit, že se příslušné orgány věcí začnou opravdu zabývat.

Návrhy de lege lata (pro budoucí právní úpravu)

I ve světle shora uvedeného považujeme za nutné zahájit diskusi o revizi regulace v oblasti online prostoru, přičemž za klíčová považujeme dále uvedená témata:

1. **Preference směrnice před nařízeními Evropského parlamentu a Rady Evropské unie**
   Právě cyberstalking a jeho monetizace naznačují jeden z hlavních problémů současné regulace, jímž je určitá praktická neprovázanost právních řádů členských zemí Evropské unie a jejich čistě vnitrostátního práva. V důsledku přímé účinnosti nařízení EU dochází k situacím, kdy v členském státě vzniká paralelní struktura regulace. To lze ilustrovat na příkladu Nařízení DSA, které zavádí regulaci až na úroveň správních úřadů (koordinátorů digitálních služeb), aniž by se však odrazila například v oblasti výkonu rozhodnutí (viz dále).

   Směrnice oproti tomu klade na členské státy vyšší požadavky v podobě tzv. transpozice, tedy začlenění směrnicí stanovených požadavků do vnitrostátního práva. Právě tato

forma normativních právních aktů tak lépe odpovídá potřebě funkční provázanosti regulace. Členským státům rovněž umožňuje přijmout taková opatření, která jsou v souladu s jejich ústavním pořádkem a která respektují hospodářská, společenská, náboženská i kulturní specifika každého státu.

Dle našeho názoru by se tak orgány Evropské unie měly vrátit k dřívější praxi, a tou je harmonizace vnitrostátního práva členských států prostřednictvím směrnic.

2. **Minimalizace přenosu rozhodovacích pravomocí na soukromé subjekty**

Zejména právo Evropské unie v mnoha případech (viz právě Nařízení GDPR či Nařízení DSA) přenáší řadu pravomocí z orgánů veřejné moci na soukromoprávní subjekty. Jde typicky o rozhodování o tom, zda je konkrétní obsah nezákonný apod. K této „privatizaci" práva by mělo docházet pouze mírnějšími nástroji, které nepředstavují zásah do práv a svobod zaručených kromě jiného Listinou základních práv a svobod Evropské unie č. (2012/C 326/02), především práva na svobodu projevu a informace dle čl. 11 Listiny.

K zásadnějším zásahům, jakým je například odstranění či blokování obsahu, by, pokud vůbec, mělo bez ingerence veřejné moci docházet jen ve výjimečných, zcela jednoznačných případech, jakými jsou například šíření dětské pornografie, zásahy do nejintimnějších stránek soukromí apod., tedy v případech, kdy i krátkodobá veřejná dostupnost obsahu může způsobit skutečně dramatickou újmu na jiných právech, zaručených Listinou.

V tomto případě se jeví jako vhodný nástroj tzv. „*demonetizace obsahu*", tj. dočasné přerušení finančních toků mezi provozovateli online platforem a jejich uživateli. Ani tento nástroj nelze zavádět zcela nekriticky, a to zejména s ohledem na nutnost chránit fungování médií (viz čl. 11 odst. 2 Listiny).

Mělo by být pak úkolem členských států Evropské unie zavést ve svých právních systémech efektivní nástroje pro výkon veřejné moci, která bude schopna včas reagovat na (domnělá) porušení práva. Je totiž třeba přihlédnout k tomu, že právní řády i nástroje ochrany práv se v jednotlivých členských státech liší, ať již z hlediska procesních pravidel, tak i použitelných nástrojů (vč. například různé úrovně zavedení online forem soudních či správních řízení, různého praktického výkonu soudní moci, kdy řada zemí má dlouhodobou tradici využití tzv. arbitrážních/rozhodčích řízení, v jiných zemích dosud převažuje řešení sporů tradičními soudy apod.).

3. **Minimalizace preventivních povinností**

Jakkoliv je jistě nezbytné, aby i provozovatelé online platforem nesli určitou odpovědnost za obsah, který je prostřednictvím jejich platforem šířen, je třeba omezit povinnost těchto platforem vyhledávat nezákonný obsah a zasahovat proti němu preventivně. Jakkoliv si to snad lze představit v případě nejvážnějších forem trestné činnosti (dětská pornografie

apod.), v ostatních situacích (zejména civilněprávních) je třeba ponechat odpovědnost zejména na poškozených osobách, jimž však musí být poskytnuty nástroje veřejné moci, které budou účinné a rychlé.

4. **Revize nástrojů výkonu rozhodnutí**

   Je jistě vhodné zahájit širší diskusi o úpravě vnitrostátních pravidel v oblasti vynutitelnosti existujících pravomocných (vykonatelných) rozhodnutí. Právě v oblasti regulace online prostoru lze totiž pozorovat dlouhodobé zaostávání pravidel pro výkon rozhodnutí oproti regulaci, zaváděné nařízeními Evropského parlamentu a Rady Evropské unie. Příkladem může být úprava v České republice, kdy v oblasti výkonu soudního rozhodnutí, které se týká nepeněžitého plnění, lze v podstatě uplatnit jediný nástroj, a tím je ukládání pokut. To je právě v případě monetizovaného cyberstalkingu (ale i v dalších situacích) nástroj nepraktický a často i nefunkční.

   Nelze navíc odhlédnout od toho, že nejsou výjimečné (a zejména to platí pro prostředí internetu) situace, kdy osoba, která je vlastníkem provozovatele online platformy, sídlí ve státě mimo jurisdikci členských států Evropské unie, příp. kdy je internetová stránka, která je využívána pro nezákonnou činnost, registrována v takové jurisdikci. V takových případech se nelze domoci práva ani v případě, že existuje pravomocné a vykonatelné rozhodnutí soudního či správního orgánu.

   Je tak na zvážení (a to z hlediska právních, technických i ekonomických), zda v určité fázi vymáhání již soudem či správním orgánem určené povinnosti zapojit do procesu vymáhání práva i třetí strany, například tzv. ISPs (tedy poskytovatele služeb přístupu k internetu). Právě jejich prostřednictvím by mohlo dojít k blokaci samotného přístupu ke stránkám či platformám, jejichž provozovatelé se odmítají podrobit existujícímu rozhodnutí, případně takový přístup ztížit.

5. **Minimalizace regulace a právo na přezkum**

   Jakákoliv případná revize současného předpisového rámce v oblasti online prostoru by měla vždy respektovat základní principy demokratického právního státu. Za ty lze považovat zejména princip minimalizace zásahů státní moci do práv a svobod občanů, tedy přistoupit k regulaci teprve tam, kde nelze dosáhnout ochrany práv a svobod občanů jinou cestou a kdy si takovou regulaci vyžadují jiná práva či svobody.

   Druhým takovým nezadatelným principem je právo na účinný a spravedlivý soudní přezkum jakéhokoliv zásahu do práv, jak vyplývá v rámci práva EU zejména z článku 47 Listiny základních práv Evropské unie.

Závěr

Ochrana před monetizovaným cyberstalkingem je nesporně akutním tématem, jemuž je nezbytné se věnovat. Považujeme za nezbytné, aby jakákoliv právní regulace na úrovni Evropské unie (ale i členských států) obsahovala jasně specifikované cíle, odůvodnění jejich souladu s ústavním (právním) řádem a způsoby průběžného ověřování její skutečné efektivity. V oblasti monetizovaného cyberstalkingu lze sledovat snahu orgánů Evropské unie zavádět stále další regulatorní opatření, namísto toho, aby byla zhodnocena účinnost opatření existujících.

I s ohledem na to je nezbytné, aby občané byli seznámeni se svými právy a nástroji, které mají k dispozici pro jejich ochranu, a aby těchto nástrojů využívali. Jen díky praktické aplikaci práva lze získat informace o tom, nakolik předpisy Evropské unie v propojení s předpisy členských států skutečně plní cíle, s nimiž byly přijímány, nakolik nadále respektují hlavní pilíře, na nichž je postavena Evropská unie a na nichž spočívají i systémy jednotlivých členských států EU, a zda je možné takovou regulaci zrušit, případně zda je vhodné přistoupit k její revizi.

Nielsen Legal, advokátní kancelář, s.r.o.

JUDr. Tomáš Nielsen, advokát

V příloze této analýzy lze nalézt určité příklady jednodušších podání, která lze uplatnit v případě ochrany před monetizovaným cyberstalkingem. Upozorňujeme, že nenahrazují kvalifikovanou právní pomoc a že jsou zpracovány na základě praktických zkušeností s právem České republiky a právem Evropské unie (coby součástí práva České republiky).

Žlutě jsou označeny části, které jsou určeny k doplnění, případně které obsahují instrukce pro případné vyplnění informací (instrukce jsou uvozeny hranatými závorkami [ ] a z konečného textu je třeba je odstranit).

Příloha

Příklady podání

- trestní oznámení
- uplatnění práva na výmaz a námitka proti zpracování (GDPR)
- stížnost k ÚOOÚ
- oznámení (DSA)
- podnět k ČTÚ (DSA)

PODÁNÍ PODLE ČESKÉHO PRÁVA

TRESTNÍ OZNÁMENÍ

Okresní státní zastupitelství v [*]

Adresa

(podáno doporučeně/datovou schránkou/e-mailem)

[TRESTNÍ OZNÁMENÍ JE VHODNÉ SMĚŘOVAT K OKRESNÍMU STÁTNÍMU ZASTUPITELSTVÍ, PŘÍPADNĚ K POLICII, PŘÍSLUŠNÝM MÍSTU, KDE DOŠLO KE SPÁCHÁNÍ TRESTNÉHO ČINU – V TOMTO PŘÍPADĚ MŮŽE JÍT O SÍDLO PROVOZOVATELE PLATFORMY, JE-LI V ČESKÉ REPUBLICE, BYDLIŠTĚ ÚTOČNÍKA APOD. OBECNĚ LZE TRESTNÍ OZNÁMENÍ ALE PODAT K JAKÉMUKOLIV ORGÁNU. TRESTNÍ OZNÁMENÍ LZE PODAT I OSOBNĚ NA JAKÉMKOLIV ODDĚLENÍ POLICIE ČESKÉ REPUBLIKY. PŘI TAKOVÉM PODÁNÍ DOPORUČUJEME VYŽÁDAT SI OD POLICIE KOPII ÚŘEDNÍHO ZÁZNAMU O PODÁNÍ TRESTNÍHO OZNÁMENÍ]

Datum

Oznamovatel:

Jméno, příjmení, adresa, kontakt toho, kdo trestní oznámení podává

Oznámení o skutečnostech nasvědčujících spáchání trestného činu

I.

Tímto podávám podnět k prošetření, zda níže uvedeným jednáním nedošlo ke spáchání trestného činu.

II.

Dne X. Y. 2025 jsem byl fyzicky napaden neznámými osobami, a to na ulici na adrese XXXXXXXX. Napadení probíhalo tak, že jsem byl nejprve verbálně urážen výrazy jako „XXXXXX“, následně mě jedna z osob udeřila do hlavy.

Dne X. Y. 2025 došlo ze strany stejných osob k dalšímu incidentu, kdy jsem byl osloven na ulici na adrese XXXXXXXX a hrubě urážen, a to za přítomnosti mých dětí.

Uvedené osoby si průběh incidentů nahrávali na své telefony.

Důkazy:

- *Svědectví osoby [UVÉST JMÉNA, PŘÍJMENÍ A ADRESY SVĚDKŮ]*
- *Fotografie / videonahrávka*
- *Lékařská zpráva o důsledcích napadení*

Následně jsem zjistil, že nahrávky z incidentů jsou veřejně k dispozici na online platformě XXXXXXX, a to na URL adrese *[UVÉST URL ADRESU]*, přičemž přístup k tomuto obsahu je uvedenou platformou zpoplatněn.

Důkazy:

- *Videonahrávka / screenshot online obsahu*

[V TÉTO ČÁSTI JE POTŘEBNÉ CO NEJPODROBNĚJI POPSAT PRŮBĚH ÚTOKŮ, JEJICH SPECIFIKA, SKUTEČNOST, ZDA ŠLO OPAKOVANĚ O ÚTOKY STEJNÝCH OSOB, ZDA EXISTUJE DŮVOD SI MYSLET, ŽE POSTUPUJÍ KOORDINOVANĚ APOD. SOUČASNĚ JE TŘEBA NAVRHNOUT I PŘÍSLUŠNÉ DŮKAZY]

III.

V současné době mám obavu, že tyto útoky budou pokračovat, případně gradovat, že mohou být v budoucnu směrovány i vůči mým blízkým, vč. nezletilých dětí. Vyvinula se u mě navíc úzkostná reakce, kdy jakýkoliv pobyt venku pociťuji jako ohrožení.

Důkazy:

- *Svědectví osoby [UVÉST JMÉNA, PŘÍJMENÍ A ADRESY SVĚDKŮ]*
- *Lékařská zpráva / Zpráva psychologa*

[V TÉTO ČÁSTI JE POTŘEBNÉ CO NEJPODROBNĚJI POPSAT DOPADY ÚTOKU NA VAŠI OSOBU, PŘÍP. NA DALŠÍ OSOBY, PŘÍPADNĚ NAVRHNOUT DŮKAZY]

IV.

S ohledem na shora uvedené žádám příslušné orgány činné v trestním řízení, aby zahájily kroky k prověření, zda v uvedené věci nedošlo ke spáchání trestného činu, případně které osoby se takového trestného činu dopustily.

Jsem přesvědčen, že uvedeným jednáním mohlo dojít ke spáchání například trestného činu nebezpečné vyhrožování (§ 353 trestního zákoníku), nebezpečné pronásledování (§ 354 trestního zákoníku), vydírání (§ 175 trestního zákoníku), útisk (§ 177 trestního zákoníku), pomluva (§ 184 trestního zákoníku), ublížení na zdraví (§ 146 trestního zákoníku), o výtržnictví (§ 358 trestního zákoníku)[11], případně jiného trestného činu.

Žádám, aby příslušné orgány zejména vytěžily následující osoby, neboť mám důvodné podezření, že právě ony se mohly na shora popsaných útocích podílet, případně k nim mohou poskytnout relevantní informace:

[11] Popis základních skutkových podstat jednotlivých trestných činů najdete v kapitole „Vnitrostátní právo“.

- jméno, příjmení, adresa

[NAMÍSTO OBVINĚNÍ KONKRÉTNÍCH OSOB JE VHODNÉ UVÉST OSOBY, KTERÉ MOHOU BÝT PRO POSOUZENÍ VĚCI DŮLEŽITÉ A JEJICHŽ VÝSLECH BY PODLE VÁS MOHL VĚC OBJASNIT. NEZNÁTE-LI VEŠKERÉ ÚDAJE O TAKOVÝCH OSOBÁCH, JE VHODNÉ JE V MAXIMÁLNÍ MOŽNÉ, VÁM DOSTUPNÉ, PODOBĚ PŘIBLÍŽIT – NAPŘÍKLAD PŘEZDÍVKOU NA ONLINE PROFILU S URL ADRESOU TOHOTO PROFILU A POUŽITOU FOTOGRAFIÍ APOD.]

Žádám rovněž, aby si příslušné orgány vyžádaly informace o profilu na uvedené platformě prostřednictvím jejího provozovatele.

S ohledem na riziko, že k podobným útokům bude docházet i nadále, žádám, aby policejní orgán učinil příslušná opatření ve smyslu ustanovení § 78, 79, příp. 79a trestního řádu, tedy zejména aby po zjištění osob útočníků jim odebral mobilních telefony, jejichž prostřednictvím dochází k nahrávání útoků a které mohou sloužit jako důkazní prostředek v předmětné věci. Rovněž žádám, aby byla učiněna opatření k zablokování shora uvedeného obsahu na online platformě, a to k omezení dalšího vzniku újmy na mé straně a na straně mé rodiny.

V.

V případě potřeby jsem připraven doplnit shora uvedené informace či poskytnout ve věci jakoukoliv další součinnost.

Dojde-li příslušný orgán k závěru, že v tomto případě nebyly splněny znaky trestného činu, žádám, aby bylo prověřeno, že uvedená jednání nenaplňují znaky přestupku.

Rovněž žádám, abych byl informován o způsobu, jímž byl jeho podnět vypořádán, jakož i o dalším průběhu této věci.

_____

Podpis

PODÁNÍ DLE NAŘÍZENÍ GDPR

ŽÁDOST O VÝMAZ OSOBNÍCH ÚDAJŮ A NÁMITKA PROTI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Název platformy: XXXXXXXXXXXXXXXXX

Kontaktní adresa: **XXXXXXXXXXXXXXXXX**

[UVEĎTE NÁZEV PLATFORMY A KONTAKT, POKUD HO ZNÁTE – NAPŘ. E-MAIL APOD.

POZOR! VĚTŠINA PLATFOREM MÁ NA SVÝCH STRÁNKÁCH FORMULÁŘ PRO PODÁVÁNÍ PODOBNÝCH ŽÁDOSTÍ ČI STÍŽNOSTÍ. POKUD BUDETE ŽÁDOST POSÍLAT PŘES FORMULÁŘ, UJISTĚTE SE, ŽE VÁM BUDE DORUČENO POTVRZENÍ O JEJÍM ODESLÁNÍ, VČ. TEXTU ŽÁDOSTI. POKUD TAKOVOU JISTOTU NEMÁTE, PŘED ODESLÁNÍM SI POŘIĎTE ZÁZNAM OBRAZOVKY, PŘÍPADNĚ SI NAHRAJTE VIDEO POTVRZUJÍCÍ, ŽE ŽÁDOST S KONKRÉTNÍM TEXTEM ODESÍLÁTE, A TO PRO DOLOŽENÍ PODÁNÍ ŽÁDOSTI.]

V Praze dne X. X. 2025

Žádost o výmaz osobních údajů a námitka proti zpracování osobních údajů

Vážení,

Vaše online platforma *[NÁZEV PLATFORMY, NAPŘ. FACEBOOK/YOUTUBE...]* protiprávně zpracovává osobní údaje mé osoby, jak je podrobněji popsáno níže:

Odkaz na zpracovávané osobní údaje: *[UVEĎTE CELÝ ODKAZ, POD NÍMŽ LZE NALÉZT VIDEO-ZÁZNAM(Y)]*

Druh osobních údajů: Zobrazení mého obličeje, uvedení mého jména, zobrazení registrační značky mého vozidla, adresa mého bydliště, případně i další

Důvod žádosti: Osobní údaje jsou zpracovávány bez mého souhlasu a forma jejich zpracovávání mě poškozuje

Žádám tímto, aby uvedené osobní údaje byly z Vaší platformy bezodkladně vymazány, a to v souladu s článkem 17 odst. 1 písm. d) nařízení Evropského parlamentu a Rady EU 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (**GDPR**).

Žádám rovněž, abyste postupem dle článku 17 odst. 2 GDPR informovali ostatní správce, kteří tyto osobní údaje zpracovávají, o mé žádosti, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie či replikace.

Současně tímto vznáším námitku proti tomuto zpracování ve smyslu čl. 21 odst. 1 a 2 GDPR, a to, kromě jiného, i proto, že ke zpracování dochází k přímému marketingu zpoplatněného profilu, jímž k šíření uvedených osobních údajů dochází.

O výmazu, jakož i o dalších krocích, mě prosím v souladu s GDPR informujte prostřednictvím e-mailové adresy XXXXXXXXXXXXX do sedmi (7) dnů ode dne odeslání této žádosti.

V případě, že budete pro další postup vyžadovat jakoukoliv další součinnost, prosím, kdykoliv mě kontaktujte prostřednictvím uvedené e-mailové adresy.

S pozdravem

Jméno a příjmení

Adresa

Kontaktní údaje

PODNĚT K ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ

Pro podání podnětu použijte formulář uvedený na odkazu https://uoou.gov.cz/media/formulare/form-stiznost-zpracovani-ou1.pdf.

Podnět lze podat i písemně, datovou schránkou či e-mailem na adresu stiznosti@uoou.gov.cz:

Úřad pro ochranu osobních údajů

Pplk. Sochora 27

170 00 Praha 7

[PODNĚT PRO ÚČELY PODÁNÍ BEZ VYUŽITÍ FORMULÁŘE UVEDENÉHO NA STRÁNKÁCH ÚŘADU.]

V Praze dne X. X. 2025

Oznámení podezření na zpracování osobních údajů v rozporu s nařízením GDPR

Vážení,

žádám Vás tímto o prověření, zda níže uvedeným jednáním nedochází ze strany provozovatele online platformy XXXXXXXXXXXX ke zpracování mých osobních údajů v rozporu s nařízením Evropského parlamentu a Rady EU 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (GDPR):

Název platformy: XXXXXXXXXXXX

Provozovatel platformy: XXXXXXXXXXXX *[UVEĎTE, POKUD HO ZNÁTE.]*

Odkaz na zpracovávané osobní údaje: *[UVEĎTE CELÝ ODKAZ, POD NÍMŽ LZE NEZÁKONNÝ OBSAH NALÉZT]*

Druh osobních údajů: Zobrazení mého obličeje, uvedení mého jména, zobrazení registrační značky mého vozidla, adresa mého bydliště

Způsob zpracování: zejm. shromáždění, uspořádání, strukturování, uložení, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření veřejnosti

Dne X. X. XXXX jsem podal/a provozovateli předmětné online platformy žádost o výmaz dle čl. 17 GDPR a námitky proti zpracování dle čl. 21 GDPR (viz přiložená kopie žádosti). Do dnešního dne však osobní údaje nebyly odstraněny.

Podrobnější popis zpracování osobních údajů

Na uvedeném odkazu lze nalézt veřejně šířený video-záznam, kde je zobrazena moje podobizna, dále je zde uvedeno mé jméno, adresa a další osobní údaje. Veškeré osobní údaje byly pořízeny bez mého souhlasu a proti mé vůli. Účelem jejich zpracování je přitom difamace mé osoby a osobní obohacení subjektu, který uvedené video zveřejnil.

[POPIŠTE CO NEJPŘESNĚJI, JAKÉ OSOBNÍ ÚDAJE JSOU ZNEUŽÍVÁNY, JAKÝM ZPŮSOBEM A JAKÝ DOPAD TO NA VÁS MÁ. POKUD JSOU ZAZNAMENÁVÁNY I ÚDAJE VAŠICH BLÍZKÝCH, PŘÍP. NEZLETILÝCH OSOB, I TAKOVÉ INFORMACE POSKYTNĚTE.

JDE-LI O OPAKOVANOU SITUACI, DOPLŇTE I NÍŽE UVEDENÉ S ODKAZY NA DALŠÍ OBSAH, V NĚMŽ JSOU PODLE VÁS NEOPRÁVNĚNĚ ZPRACOVÁVANÉ VAŠE OSOBNÍ ÚDAJE.]

V předmětné věci přitom nejde o první případ. K podobnému neoprávněnému zpracování mých osobních údajů došlo na uvedené online platformě opakovaně – viz například odkazy zde:

- XXXXXXXXXXXXX
- XXXXXXXXXXXXX

Předmětné osobní údaje jsou zpracovávány nezákonně, bez mého souhlasu, způsobem, který hrubě porušuje má osobností práva a poškozuje mě v osobním i profesním životě. Pro zpracování přitom neexistuje ani žádný jiný právní základ ve smyslu článku 6 GDPR.

V případě, že budete pro další postup vyžadovat jakoukoliv další součinnost, prosím, kdykoliv mě kontaktujte prostřednictvím níže uvedené e-mailové adresy.

O řešení tohoto oznámení mě prosím informujte prostřednictvím e-mailové adresy XXXXXXXXXXXX.

S pozdravem

_____
(podpis)
Jméno a příjmení
Adresa
E-mail

Přílohy:

- *doklad o odeslání žádosti o výmaz a námitky proti zpracování*
- *reakce provozovatele online platformy*

PODÁNÍ DLE NAŘÍZENÍ DSA

OZNÁMENÍ NEZÁKONNÉHO OBSAHU

Název platformy: XXXXXXXXXXXXXXXXX

Kontaktní adresa: **XXXXXXXXXXXXXXXXX**

[UVEĎTE NÁZEV PLATFORMY A KONTAKT, POKUD HO ZNÁTE – NAPŘ. E-MAIL APOD.

POZOR! VĚTŠINA PLATFOREM MÁ NA SVÝCH STRÁNKÁCH FORMULÁŘ PRO PODÁVÁNÍ OZNÁMENÍ DLE DSA. POKUD BUDETE ŽÁDOST POSÍLAT PŘES FORMULÁŘ, UJISTĚTE SE, ŽE VÁM BUDE DORUČENO POTVRZENÍ O JEJÍM ODESLÁNÍ, VČ. TEXTU OZNÁMENÍ. POKUD TAKOVOU JISTOTU NEMÁTE, PŘED ODESLÁNÍM SI POŘIĎTE ZÁZNAM OBRAZOVKY, PŘÍPADNĚ SI NAHRAJTE VIDEO POTVRZUJÍCÍ, ŽE OZNÁMENÍ S KONKRÉTNÍM TEXTEM ODESÍLÁTE, A TO PRO DOLOŽENÍ PODÁNÍ OZNÁMENÍ.]

V Praze dne X. X. 2025

Oznámení nezákonného obsahu dle čl. 16 nařízení DSA

Vážení,

oznamuji Vám, že Vaše online platforma XXXXXXXXXXXX šíří nezákonný obsah, jak je podrobněji popsáno níže:

Odkaz na nezákonný obsah: *[UVEĎTE CELÝ ODKAZ, POD NÍMŽ LZE NEZÁKONNÝ OBSAH NALÉZT]*

Důvody oznámení:

- obtěžování, cyberstalking
- nahrávání bez souhlasu
- obtěžování, cyberstalking osoby mladší 18 let
- nahrávání osoby mladší 18 let bez souhlasu
- nezákonně získaný obsah zasahující do soukromí zobrazovaných osob

[VYBERTE, PŘÍPADNĚ I DOPLŇTE, V ČEM SHLEDÁVÁTE NEZÁKONNOST OBSAHU]

Toto oznámení podávám jako osoba, která je uživatelem služeb Vaší platformy a současně osoba, která je uvedeným obsahem velice zásadním způsobem dotčena.

Na uvedeném odkazu lze nalézt veřejně šířený video-záznam, kde je zobrazena moje podobizna, dále je zde uvedeno mé jméno, adresa a další osobní údaje. Záznam navíc zahrnuje i nezletilou osobu. Tento obsah byl pořízen bez mého souhlasu, proti mé vůli, obsahuje nepravdivé a urážlivé výroky a na veřejnosti vyvolává nenávist vůči mé osobě. Šíření tohoto obsahu navíc ohrožuje

bezpečnost nejen mou, ale i mé rodiny a dalších blízkých osob. Účelem šíření videa je přitom pouze difamace mé osoby a osobní obohacení osoby, která uvedené video zveřejnila.

[JDE-LI O OPAKOVANOU SITUACI, DOPLŇTE I NÍŽE UVEDENÉ S ODKAZY NA DALŠÍ NEZÁKONNÝ OBSAH, V NĚMŽ JSOU PODLE VÁS NEOPRÁVNĚNĚ ZPRACOVÁVANÉ VAŠE OSOBNÍ ÚDAJE.]

V předmětné věci přitom nejde o první případ. K podobnému šíření nezákonného obsahu došlo již v minulosti, a to nejen ve vztahu k mé osoby – viz například odkazy zde:

- XXXXXXXXXXXXXX
- XXXXXXXXXXXXXX

Vzhledem k tomu, že uvedený obsah je šířen nezákonně, žádám Vás o učinění příslušných opatření ve smyslu nařízení Evropského parlamentu a Rady EU o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (DSA).

Jak je patrné ze shora uvedeného odkazu, oznámený obsah je šířen prostřednictvím účtu, který je zpoplatněn. Proto zejména **žádám o přijetí okamžitých opatření, zejména o pozastavení jakýchkoliv plateb držiteli předmětného účtu**.

O postupu mě prosím v souladu s DSA informujte prostřednictvím níže uvedené e-mailové adresy XXXXXXXXXXXXX.

V případě, že budete pro další postup vyžadovat jakoukoliv další součinnost, prosím, kdykoliv mě kontaktujte prostřednictvím uvedené e-mailové adresy.

Prohlašuji, že toto oznámení podávám s tím, že se v dobré víře domnívám, že informace a tvrzení obsažené v tomto oznámení jsou přesné a úplné.

S pozdravem

Jméno a příjmení:

E-mail:

STÍŽNOST NA PORUŠENÍ DSA K ČESKÉMU TELEKOMUNIKAČNÍMU ÚŘADU

Český telekomunikační úřad

Sokolovská 58/219

19000 Praha 9

[PODNĚT PRO ÚČELY PODÁNÍ POŠTOU, PŘÍPADNĚ DATOVOU SCHRÁNKOU.]

V Praze dne X. X. 2025

Stížnost pro porušování nařízení DSA

Vážení,

obracím se na Vás jako uživatel online platformy XXXXXXXXXXXX. Jak jsem zjistil, na této platformě dochází k šíření dle mého názoru jednoznačně nezákonného obsahu. Tento obsah se přímo dotýká mé osoby, byl pořízen bez mého souhlasu, je užíván k obtěžování mé osoby a k šíření difamačních informací o mé osoby.

Uvedený nezákonný obsah jsem oznámil provozovateli online platformy dne X. X. XXXX. Do dnešního dne však nedošlo ze strany provozovatele online platformy k nápravě. Dle mého názoru tím, že provozovatel uvedené online platformy neučinil opatření k zamezení šíření nezákonného obsahu, porušil své povinnosti vyplývající mu, kromě jiného, z nařízení Evropského parlamentu a Rady EU o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (DSA).

Žádám Vás tímto o prošetření této stížnosti a učinění kroků ke zjednání nápravy, a to v souladu s článkem 53 DSA.

Dovoluji si uvést podrobnější informace k věci:

Odkaz na nezákonný obsah: *[UVEĎTE CELÝ ODKAZ, POD NÍMŽ LZE NEZÁKONNÝ OBSAH NALÉZT]*

Důvody oznámení:

- obtěžování, cyberstalking
- nahrávání bez souhlasu
- obtěžování, cyberstalking osoby mladší 18 let
- nahrávání osoby mladší 18 let bez souhlasu
- nezákonně získaný obsah zasahující do soukromí zobrazovaných osob

Na uvedeném odkazu lze nalézt veřejně šířený video-záznam, kde je zobrazena moje podobizna, dále je zde uvedeno mé jméno, adresa a další osobní údaje. Záznam navíc zahrnuje i nezletilou osobu. Tento obsah byl pořízen bez mého souhlasu, proti mé vůli, obsahuje nepravdivé a urážlivé výroky a na veřejnosti vyvolává nenávist vůči mé osobě. Šíření tohoto obsahu navíc ohrožuje

bezpečnost nejen mou, ale i mé rodiny a dalších blízkých osob. Účelem šíření videa je přitom pouze difamace mé osoby a osobní obohacení osoby, která uvedené video zveřejnila.

[POPIŠTE CO NEJPŘESNĚJI, V ČEM SPATŘUJETE NEZÁKONNOST DOTČENÉHO OBSAHU, JAK BYL POŘÍZEN, KOHO SE DOTÝKÁ APOD. POKUD JSOU ZAZNAMENÁVÁNY I ÚDAJE VAŠICH BLÍZKÝCH, PŘÍP. NEZLETILÝCH OSOB, I TAKOVÉ INFORMACE POSKYTNĚTE.

[JDE-LI O OPAKOVANOU SITUACI, DOPLŇTE I NÍŽE UVEDENÉ S ODKAZY NA DALŠÍ NEZÁKONNÝ OBSAH, V NĚMŽ JSOU PODLE VÁS NEOPRÁVNĚNĚ ZPRACOVÁVANÉ VAŠE OSOBNÍ ÚDAJE.]

V předmětné věci přitom nejde o první případ. K podobnému šíření nezákonného obsahu došlo již v minulosti, a to nejen ve vztahu k mé osoby – viz například odkazy zde:

- XXXXXXXXXXXXXX
- XXXXXXXXXXXXXX

V případě, že budete pro další postup vyžadovat jakoukoliv další součinnost, prosím, kdykoliv mě kontaktujte prostřednictvím níže uvedené e-mailové adresy.

O řešení tohoto oznámení mě prosím informujte prostřednictvím e-mailové adresy XXXXXXXXXXXX.

S pozdravem

_____
(podpis)

Jméno a příjmení
Adresa
E-mail

Přílohy:

- *doklad o odeslání oznámení provozovateli online platformy*
- *odpověď provozovatele online platformy*