отримати всю можливу інформацію, що має значення для відповідного кримінального провадження. Створення центрів за моделлю Барнахус одночасно забезпечує інтереси потерпілих та повну реалізацію завдань кримінального провадження. В Україні вже діє пілотний проєкт щодо запровадження центрів захисту дитини (за моделлю Барнахус), але варто розглянути запровадження даних центрів й для інших жертв насильства.

Окремої уваги потребує попередня підготовка слідчих, прокурорів, суддів та інших учасників процесу. Навички роботи з потерпілими від сексуального насильства, розуміння травми та відмова від стереотипного мислення є ключем до подолання вторинної віктимізації.

Водночас запровадження новітнього, людиноцентричного підходу не може бети ефективним без зміни суспільного підходу. Стереотипні питання про відвертий одяг, стан алкогольного сп'яніння, певну поведінку перекладають відповідальність з кривдника на жертву. Стигматизація потерпілих та фокусування на їхній поведінці чи зовнішньому вигляді в пошуках причини вчинених щодо неї певних дій, створює бар'єр, який змушує мовчати. Страх бути неприйнятим суспільством, зазнати суспільного осуду часто зупиняє жертву на шляху пошуку справедливості.

Право не бути жертвою вдруге є невід'ємною складовою права на гідність, безпеку, справедливий суд тощо. Держава повинна не лише забезпечувати правосуддя, а й гарантувати, що процес його досягнення не стане новим джерелом травматизації. Поки потерпілим доводиться обирати між мочанням та вторинною віктимізацією, це право існує лише на папері. Зміна застарілих підходів, розвиток суспільства та належна увага з боку учасників процесу може забезпечити не формальну, а реальну захищеність особи. Тільки тоді відповідь на питання «Чи маю я право не бути жертвою вдруге?» стане чітким «так» і зазначене право буде гарантоване не лише законом, а й практикою його застосування.

Слемньов І.А.
Державний університет
«Житомирська політехніка»
P14_sia@student.ztu.edu.ua
м.Житомир

«Чи маю я право бути анонімним в Інтернеті?»

У наш час інтернет став невід'ємною частиною життя**.** Кожного дня ми стикаємося з великим масивом питань та інформації яку потрібно переслати, віднайти чи перевірити у власних цілях. Та чи замислюємося ми над тим, хто може бачити інформацію, яку ми залишаємо в інтернеті? Чи не буде вона використана кимось у власних цілях? І чи справді наші особисті розмови залишаються приватними, чи, можливо, «по той бік екрану» їх все ж може прочитати хтось інший? Питання анонімності на сьогоднішній день одне з найважливіших з чим стикається суспільство. Кожен хоч якоюсь мірою хоче бути впевнений передусім у власній безпеці та контролю над власними даними. Передусім ми хочемо захистити своє особисте життя від стороннього втручання: щоб наші повідомлення не читалися третіми особами, щоб за нами не велося приховане стеження, а персональні дані, такі як: фото, паролі, банківські реквізити та інші, не потрапляли до рук зловмисників.

На превеликий жаль, в умовах війни, виразним прикладом в Україні, є необхідність анонімності для захисту журналістів та політичних активістів, які можуть зіткнутися з небезпекою через висловлювання своєї позиції.

То що ж таке та анонімність в інтернеті? Анонімність - це можливість людини не розкривати свою справжню особистість чи бути ідентифікованим іншими учасниками під час взаємодії у цифровому просторі. Переглядаючи фільм «Кіберсталкер» я виділив як Тео Фернандес дуже влучно промовив цитату: «Інтернет- це місце, де ніхто не знає, ким ти є насправді». Власне вона передає сучасне розуміння поняттю анонімності, проте чи дійсно “ніхто” нічого про нас не знає?

За даними інтернет-джерел, питання анонімності в інтернеті почало активно поширюватися ще у другій половині ХХ століття. Перші передумови з’явилися ще у 1970-х роках разом із розвитком мережі ARPANET та протоколу TCP/IP, авторами якого були американські вчені Вінтон Серф і Боб Кан. Саме ці технології заклали основу для передачі даних у мережі, однак на початковому етапі інтернет взагалі не передбачав анонімності або захисту даних. Тому на початку 90-их виникла потреба у захисті інформації. Однією з перших технологій шифрування став протокол **swIPe** (Software IP Encryption protocol**),** розроблений під керівництвом Джона Іоаннидіса. Він дозволяв шифрувати інформацію під час її передачі та став прототипом сучасних VPN. Згодом ці ідеї були розвинуті у протоколах IPsec, що значно посилило безпеку інтернет-комунікацій.

У сучасному цифровому просторі одним із найпоширеніших проявів анонімності є анонімні повідомлення та коментарі. Конституція України, статтею 34 закріпила гарантування кожному право на свободу думку і слова, на вільне вираження своїх поглядів та переконань.

З одного боку, вираження поглядів дозволяють користувачам відкрито висловлювати свою думку без страху осуду чи переслідування. Це особливо важливо під час обговорення суспільно важливих питань або особистих тем.

З іншого боку, анонімність у коментарях нерідко стає підґрунтям для зловживань. Відчуття безкарності спонукає окремих користувачів до поширення образ, використання нецензурної лексики, кібербулінгу та дезінформації, що негативно впливає як на окремих осіб, так і на суспільство загалом.

Водночас важливо підкреслити, що анонімність не означає повної відсутності відповідальності. Тому навіть з нікнеймом Hackerman_3000, особа в будь-якому випадку може бути ідентифікована та притягнута до відповідальності за вчинення різного роду правопорушень.

Юридичні вимоги в Україні наразі визначені статтею 32 Конституції України, яка унеможливлює втручання в особисте та сімейне життя особи, збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди на це, окрім випадків передбачених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Таким чином Українське законодавство, Конституцією, закріплює обов’язок у захисті інформації, цінностей людини та недопустимості привласнення та використання особистими даними без надання її згоди. Але такі права можуть порушуватися, якщо це може нашкодити державі, її громадянам та особам які перебувають на території цієї держави та коли це необхідно для захисту суспільних інтересів.

Водночас із конституційними гарантіями захисту існують спеціальні нормативно-правові акти. Зокрема, закон України "Про захист персональних даних", який визначає умови захисту та обробки персональних даних, у тому числі в мережі Інтернет. Та передбачає, що їх використання можливе лише за згодою особи або на інших законних підставах. Закон України" Про інформацію" - він закріплює право особи на інформацію про себе та гарантує її захист від неправомірного використання. А також, наказ омбудсмена "Про затвердження документів у сфері захисту персональних даних", що деталізує механізм контролю за дотриманням законодавства у сфері захисту персональних даних.

Окрім правового регулювання, важливу роль у забезпеченні анонімності відіграє і поведінка самого користувача. Дотримання базових правил цифрової безпеки, таких як: використання різних паролів, обмеження поширення персональних даних та застосування засобів захисту. Вони дозволяють зменшити ризики втрати приватності. Водночас це підтверджує, що анонімність в інтернеті залежить не лише від держави, а й від відповідальності самої особи. Надзвичайно важливим, на мій погляд є те, що законодавство України прямо не гарантує повної анонімності в інтернеті, а встановлює чіткі межі реалізації конфіденційності.

Питання анонімності в інтернеті дуже тісно пов’язано з «політикою конфіденційності» та обробкою персональних даних. Якщо подивитися поверхнево, то все виглядає просто: користувачі самі надають згоду на використання своїх даних, натискаючи всім відомі “дозволити” у спливаючих вікнах або погоджуються із умовами сайтів та соціальних мереж. Однак на практиці це означає, що значна частина інформації про людину починає використовуватися різними цифровими сервісами.

Однією з таких форм є файли cookies - невеликі текстові файлики, де зберігається інформація, на пристрої який використовується (телефоні, комп’ютері чи іншому пристрої користувача). Як правило, вони зберігають інформацію про наші захоплення, активність, час перебування на сайтах та історію відвідувань. Тобто ці файли дозволяють зробити інтернет персоналізованим та зручнішим, зберігаючи інформацію про нас. У результаті формується «цифровий слід» – це сукупність даних про особу, що може включати ім'я, вік, контакти, геолокацію та іншу інформацію.

З однієї сторони така форма збереження даних забезпечує комфорт у користуванні інтернетом. З іншої – це створює реальну загрозу для анонімності. Надмірне збирання та накопичення даних підвищує ймовірність їх витоку або використання третіми особами без власної згоди користувача. В такому випадку, мова йде вже не лише про втрату приватності, а й про можливі загрози: від доступу до особистих переписок до шахрайства з банківськими рахунками чи використанням паролів.

Якщо вам прийшла раптова ідея анонімізації і ви цілеспрямовано готові її реалізовувати, то ось кілька можливостей як забезпечити власну захищеність в інтернеті:

По-перше, залишитися анонімним на комп'ютері чи ноутбуці легше, ніж телефоні, де більшість сервісів тісно пов’язані з особистими даними користувача.

По-друге, слід використовувати засоби інформаційного захисту. Вони є різні, але найпоширенішими у інтернет-спільноті є:

1. VPN(Virtual Private Network) – його призначення це приховати вашу IP адресу та перенаправити інтернет-трафік через сервери інших країн. У такому випадку ні провайдери, ні інші особи не бачать вашого місцезнаходження чи відвідані ресурси, адже захищає передачу даних наскрізним шляхом. Проте це працює лише при використанні перевірених сервісів. Безкоштовні VPN часто просто перенаправляють дані іншим отримувачам і не завжди є безпечними. Тому краще використовувати надійні платні VPN, хоча навіть вони не дають 100% гарантії захисту даних.

2. Proxy сервери – також маскують IP-адресу та приховує реальне перебування або надає зловмисникам фальшиву геолокацію. На відміну від VPN, ці сервери не перенаправляють дані через окремий сервіс створюючи окрему IP-адресу. Використовуючи proxy сервери варто знати, що особисті дані перехопити цілком можливо.

3. Tor браузер (так звана “цибулева маршутизація”) – замість створення одного посередника сервісу між вами та ресурсом, пропускає трафік через цілу мережу взаємопов'язаних серверів-маршутизаторів. Це дозволяє значно підвищити рівень анонімності та ускладнює відстеження дій в інтернеті.

По-третє, використання однієї пошти та одного паролю робить нас вразливими до взлому та витоку даних. Тому варто розділяти свої акаунти: використовувати кілька поштових скринь, різні паролі, номери телефону, акаунти для різних цілей. Для підвищення захисту також можна застосовувати апаратні ключі (наприклад, YubiKey, NitroKey), які значно ускладнюють несанкціонований доступ. Крім того, доцільно використовувати альтернативні платформи для пошуку, такі як Firefox або DuckDuckGo, що значно орієнтовані на конфіденційність інформації користувача.

То чи можемо ми мати право бути анонімними в інтернеті? Абсолютно анонімним залишитися практично неможливо, адже в умовах цифровізації важко бути осторонь усього, що відбувається онлайн. Сучасне покоління постійно взаємодіє з інтернетом і повністю відмовитися від цього або залишатися при цьому невидимим майже не реально.

Водночас це є великою відповідальністю держави у забезпечені захисту громадян від вчинення незаконних правопорушень. В умовах повної анонімності, інкогніти можуть планувати теракти, продавати заборонені товари та послуги (яскравим прикладом є прихована мережа Darknet). Проте право на анонімність у тих випадках, де воно дійсно необхідне, не завжди реалізується належним чином, що залишається суттєвою проблемою. У сучасних реаліях світу, захист своєї онлайн-ідентичності є надзвичайно важливим. Інформація про особу збирається не лише з тих даних, які вона свідомо надає, а й із тих, що накопичуються без її прямої участі. Хоча й законодавство встановлює правила обробки персональних даних, їх практична реалізація та чітка гарантія ще не є досконалою. Саме тому мінімальний рівень анонімності слід розглядати як необхідну умову безпеки в інтернеті. А його забезпечення має бути спільною відповідальністю держави, провайдерів, інтернет-платформ і нами особисто, використовуючи різні засоби анонімності для захисту та власної безпеки.