ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ЧАС ВІЙНИ

2023

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ЧАС ВІЙНИ. СПИСКИ УКРАЇНЦІВ

Авторка: *Уляна Шадська,* юристка у сфері цифрового законодавства, експертка з питань захисту персональних даних та етики технологій

Літературна редакторка: *Мар'яна Добоні*

Дизайн та макет: *Ольга Золотар*

Висловлюємо окрему подяку за внесок у підготовку дослідження ***Вадиму Пивоварову, Тетяні Авдєєвій, Тетяні Дорошенко, Володимиру Батчаєву, Анастасії Малинці,*** а також усім іншим, хто порушує питання щодо права людини на захист персональних даних.

Дослідження «ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ЧАС ВІЙНИ. СПИСКИ УКРАЇНЦІВ» зроблено в рамках проєкту «Документування воєнних злочинів вчинених РФ» за фінансової підтримки НЕД, США (National Endowment for Democracy, USA) . Погляди авторів дослідження не обов'язково відображають офіційну позицію NED та Уряду США.

NED NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

Асоціація УМДПЛ UMDPL Association

Freerights ASSOCIATION

ЗМІСТ

КОРОТКЕ РЕЗЮМЕ

24 лютого 2022 року Російська Федерація розпочала повномасштабне вторгнення в Україну. Ця війна проти українців шокувала весь світ рівнем жорсткості до мирного населення та продемонструвала, що сучасні військові стратегії вже не обмежуються лише традиційними засобами ведення бойових дій. Застосовуються безпрецедентні технології для збору інформації про населення, інфраструктуру, зокрема використовуються системи штучного інтелекту та інші. Битва відбувається не тільки на землі, а ще в кіберпросторі, де традиційна зброя поєднується з новітніми технологіями.

Персональні дані стали засобом для досягнення ворожих цілей, включаючи вчинення воєнних злочинів проти людяності, та інших небезпечних явищ — переслідування, стеження та введення в оману, поширення дезінформації, ненависті тощо. Це війна, де кожна людина може стати жертвою, незалежно від її місця перебування. Цифрова лінія фронту не має географічних меж і кордонів. Вона проникає всюди — у будинки, офіси, у кишені особистих смартфонів, будь-де та будь-коли. Завдяки аналізу метаданих можна ідентифікувати конкретних осіб, прогнозувати військові операції, вивчати зв'язки між особами, проводити цілеспрямовані психологічні атаки проти населення. Сьогодні ще мало досліджень щодо загроз для людини або цілих спільнот від цілеспрямованого використання даних, зокрема в міжнародних збройних конфліктах. Відповідно недостатньо правових інструментів для протидії цьому.

Протягом 2022–2023 років наша команда зібрала факти, коли українці стали жертвами злочинів через використання персональних даних, а також випадки, які прямо вказують на порушення законодавства в цій сфері, тому що всі наслідки мають свої причини. Для цього опрацьовано понад 200 матеріалів, отриманих з відритих джерел: офіційні повідомлення українських органів правопорядку, публікації в медіа, коментарі очевидців порушень і громадських активістів. Усі ці дані ми узагальнили та представили в цьому аналітичному звіті.

Головна мета — показати причини та наслідки несанкціонованого використання персональних даних. Привернути увагу державної влади України, міжнародної та наукової спільноти до ризиків порушення приватності людини та необхідності проведення реформ у цій сфері.

Аналітичний звіт складається із шести розділів, у яких опубліковані історії:

- як за допомогою персональних даних формувалися детальні досьє про українців на тимчасово окупованих територіях. У змісті розкриті питання: які категорії осіб передусім зазнали переслідування; яким чином збираються персональні дані населення та для яких цілей;
- про несанкціоновані витоки персональних даних, які містяться в закритих державних закритих базах;
- про порушеннях законодавства у сфері захисту даних в органах місцевого самоврядування;
- про несанкціоновані витоки конфіденційної інформації в системі охорони здоров'я;
- про використання персональних даних українських дітей. У змісті розкриті гіпотези: для яких цілей збирається інформація та ризики для фізичної безпеки;
- про використання соціальних мереж та інших технологій для збору даних, переслідування, стеження та введення в оману населення, поширення дезінформації, ненависті тощо.

У висновках надано рекомендації, що можна зробити вже сьогодні, щоб вплинути на ситуацію, яка спровокувала негативні наслідки.

Загальна карта проблем і їхні причини, викладена в цьому документі:

- може дати поштовх до предметної дискусії щодо інформаційної безпеки населення. До початку повномасштабної збройної агресії Росії проти України проблеми захисту даних не мали широкого обговорення в суспільстві. Не тому, що їх не було, а тому, що більшість інцидентів були латентними. Тепер маємо достатньо аргументів, що захист особистих даних важливий не тільки для збереження фінансових активів на банківських картках, а ще й життя та здоров'я людини;
- допоможе експертам розробляти механізми захисту даних, зокрема проаналізувати, яка категорія осіб і вид інформації найбільш вразливі; здійснювати картування загроз і формувати гіпотези щодо методів контролю, щоб у майбутньому запобігти порушенням;

— може стати важливим матеріалом для дослідження взаємозв'язку між фізичним і «цифровим тілом» (або профілем) людини. Цифрові технології стали частиною практично всіх сфер життя. У науковому колі вже почали використовувати термін «цифрове тіло»[1], тобто інформація про людину, яка відображає її генетичну, соціальну, культурну та економічну ідентичність. Зображення, переконання, біометричні та інші дані, що зберігаються в цифровому просторі, — по суті, є відображенням особистості. Розуміння взаємозв'язку між фізичним і «цифровим тілом» необхідне для оцінювання можливих загроз як для окремого індивіда, так і цілих спільнот;

— допоможе визначити в правовому полі поняття «цифрова шкода» та її причинно-наслідковий зв'язок, зокрема в контексті міжнародного гуманітарного права. Можливість узгодження права на недоторканість приватного життя з нормами, що регулюють збройні конфлікти, а також політиками щодо зобов'язань осіб, які встановлюють факти для розслідувань воєнних злочинів;

— надасть змогу краще зрозуміти загрози, які можуть становити цифрові технології населенню, а також як реагувати на ці ризики та пом'якшувати їх. Потрібна теорія цифрової шкоди. Для того, щоб пов'язати теорію з практикою, потрібна концептуальна основа.

Сьогодні точиться багато дискусій про використання персональних даних. Глибоке розуміння всього спектру загроз для людини вимагатиме перегляду загальної концепції її захисту загалом. Зокрема, потрібно поставити питання:

— Які гарантії того, що дані, зібрані для захисту держави, не стануть засобом проти її громадян?

— Яка існує небезпека зловживання такою інформацією?

— Які методи забезпечення безпеки та збереження гідності людини в цифровому просторі?

— Як можна забезпечити відкритість і контроль над цим процесом?

1 Chris Shilling, «The Body in Sociology», цит. по: Claudia Malacrida and Jacqueline Low (eds), *Sociology of the Body, Oxford:* Oxford University Press, 2008; Carey Jewitt, Sara Price and Anna Xambo Sedo, «Conceptualising and Researching the Body in Digital Contexts: Towards New Methodological Conversations across the Arts and Social Sciences», *Qualitative research*, Vol. 17, No. 1, 2017.

ПЕРЕДМОВА

Під час російської збройної агресії страждає цивільне населення України. Окрім ракетних обстрілів, українці зазнають приниження, тортур і навіть убивств через національність, рідну мову, погляди, професію, інтереси, сімейні зв'язки, службу або навіть дружбу[2]. За словами очевидців, люди зникали на окупованих територіях України за певним алгоритмом. Спочатку військовослужбовці, правоохоронці, місцеві чиновники та їхні родичі. Далі — громадські активісти, журналісти та інші особи з проукраїнською позицією. Російські військові розшукували цих осіб за списками та з детальною інформацією про них — склад сім'ї, хто де працював, служив, навчався, яку власність має тощо. Водночас слід зазначити, що існування вищевказаних «груп ризику» не означало того, що всі інші жителі окупованих територій могли почувати себе в безпеці. Жорстокість окупантів мала не тільки прикладний характер (отримання інформації, примус до співпраці тощо), а й була спрямована на досягнення глобальної цілі війни — знищення української ідентичності. Тортури поряд з позасудовими стратами, депортацією та примусовою паспортизацією стали засобом примусу до відмови від українства[3].

Російські загарбники спільно з особами, які співпрацювали з ними, вели інформаційну підготовку, зокрема проводили пропагандистську роботу серед населення в різних регіонах України, збирали дані та складали списки українців. Окрему увагу треба звернути на те, що з різних джерел і під різним приводом вони також збирали та змінювали персональні дані українських дітей для виведення їх з правового, етнічного та культурного середовища.

Значну частину інформації про людей можна було отримати у відкритому доступі в інтернеті, але, окрім цього, протягом 2022–2023 років органи правопорядку все частіше викривали зрадників серед державних службовців, які добровільно пішли на співпрацю з росіянами та передавали їм необхідну інформацію. Зокрема, витоки зафіксовані в органах місцевого самоврядування та медичних установах. Окрім того, окупанти отримували дані через

2 Стаття 75 Додаткового протоколу до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів, забороняє тілесні покарання і катування всіх видів «у будь-який час і в будь-якому місці, незалежно від того, чиняться вони представниками цивільних чи воєнних органів».

3 Російська армія: приречені на жорстокість та катування. Режим доступу: *https://umdpl.info/news/rosijska-armiya-pryrecheni-na-zhorstokist-katuvannya/*

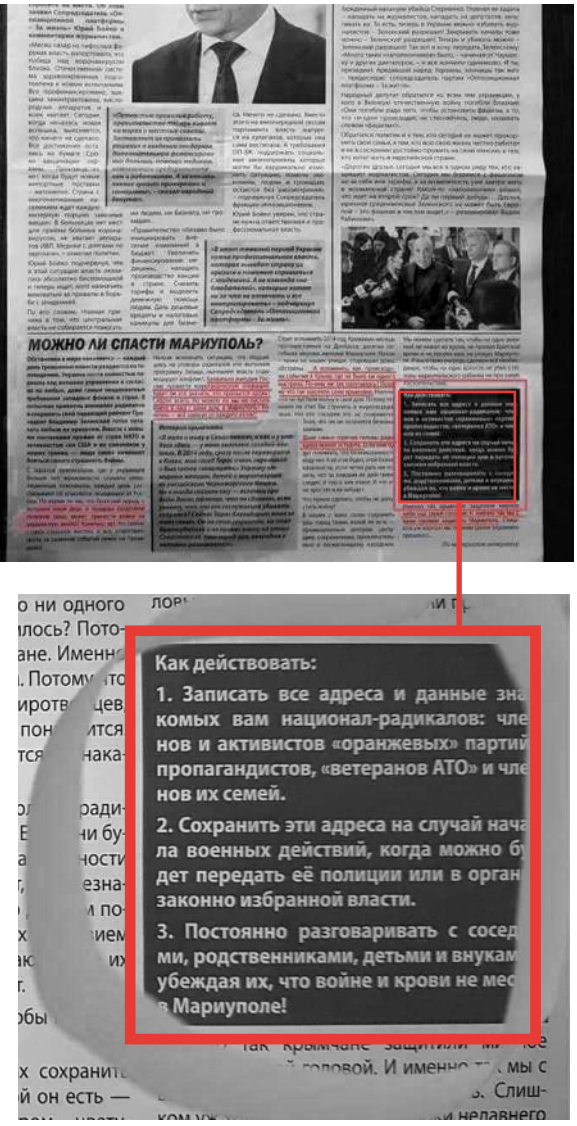
залякування, тортури та введення в оману населення.

Як уже було зазначено вище, усі наслідки мають свої причини. Опубліковані нижче факти прямо вказують на слабку систему захисту персональних даних. Не було забезпечено належних механізмів безпеки інформації закритих баз даних, зокрема під час окупації українських територій. У багатьох випадках державні службовці не були поінструктовані, що робити з інформацією. Це підтверджується в результатах перевірок, які здійснювали українські органи правопорядку та Уповноважений Верховної Ради України з прав людини. Хоч не всі події, наведені в цьому документі, є результатами розслідувань з достовірними доказами, але це достатні аргументи, щоб громадянське суспільство, державна влада та наукова спільнота звернули на них увагу.

Ми вдячні всім тим, хто порушує ці питання, наводить докази та аргументи, розслідує злочинну діяльність у цій сфері та притягає до відповідальності порушників. Такі факти не мають залишитися непоміченими або зникнути з просторів інтернету. Після прочитання цього звіту, сподіваємося, у вас не залишиться сумнівів у тому, що захист права на приватність має значення.

СПИСКИ УКРАЇНЦІВ НА ТИМЧАСОВО ОКУПОВАНИХ ТЕРИТОРІЯХ

(Джерело зображення: Anzhela Bets / unsplash.com)



Збір персональних даних українців здійснювався ще до повномасштабного вторгнення в Україну. У соціальних мережах люди ділилися різними даними та думками, що на сході вже давно проводилася пропагандистська діяльність серед населення. Один з фактів, опублікованих в інтернеті, який привернув нашу увагу, — це фотографія вирізки з газети[4], де в матеріалі під заголовком «Як врятувати Маріуполь» закликали жителів записувати дані ветеранів АТО, місцевих проукраїнських активістів, політичних діячів і членів їхніх сімей, щоб, як зазначено в газеті, коли розпочнуться воєнні дії, передати ці дані «новій владі», іншими словами — окупантам. Газети з логотипами опозиційної партії ОПЗЖ у поштові скриньки маріупольців розкидали невідомі люди[5]. Тоді представник фракції в Маріупольській міській раді, коментуючи зміст цієї публікації, сказав, що це провокація. Начебто хтось надрукував фальшиву газету. Незалежно від того, хто насправді розповсюдив це видання, факт збору інформації про осіб залишається незмінним.

За словами очевидців, російські військові або особи, що підтримують збройну агресію проти України, приходили до людей на окупованих територіях уже з повним досьє на них. Зі списками ходили по домах, вулицях,

4 У Маріуполі від імені ОПЗЖ поштовими скриньками розкидали антиукраїнські газети підривного характеру. Режим доступу: *https://www.0629.com.ua/news/3091656/v-mariupole-ot-imeni-opzz-po-poctovym-asikam-razbrosali-antiukrainskie-gazety-podryvnogo-haraktera-foto?fbclid=IwAR3FDWEjWH0aQVsgd1MJjGmdd8fRouFlOle6XDrQnDZCrGHIk9DTxJAzwm0*

5 «Опозиційна платформа — за життя» (ОПЗЖ) — заборонена в Україні проросійська політична партія соціального спрямування.

стояли на блокпостах, де влаштовували так звану «фільтрацію». Під час активної фази війни, зокрема на окупованих територіях, збирали інформацію про різні верстви населення загалом. Це робилося через тортури, шантаж або введення людей в оману. Наприклад, пенсіонерам за їхні персональні дані пропонували певну грошову винагороду, а дітям подарунки. Усі згадані в тексті випадки потребують подальшого детального з'ясування та розслідування.

1. КИЇВСЬКА ОБЛАСТЬ

Іванківська селищна громада, що в Київській області, була однією з перших, яка постраждала від повномасштабного вторгнення. Біля Чорнобильської зони точилися важкі бої з російськими військами, які намагалися прорватися до Києва. Звільнили колишній райцентр і навколишні села у квітні — до того часу вони перебували в блокаді. Мешканці села Коленці розповіли, що окупанти практично поіменно знали людей, які там живуть. Вони мали списки, у яких були зазначені адреси проживання українських військовослужбовців, зокрема учасників АТО. Розшукували та викрадали людей, тримали в полоні, когось відпустили, а когось убили. Також очевидці зазначили, що в них були списки власників зареєстрованої зброї, яких також шукали за адресами проживання.[6] Такі самі випадки зафіксовані в Бучі та Ірпені.

(Джерело зображення: palinchak / freepik.com)

6 ЗМІ, свідчення постраждалих та очевидців. Матерів хотіли розстріляти на очах у дітей. Як пережила окупацію найбільша громада України. Режим доступу: *https://lb.ua/society/2022/04/25/514634_materiv_hotili_rozstrilyati_ochah.html*

Жителі села під час інтерв'ю для медіа намагалися відповісти на питання, звідки в російських військових була інформація про місцеве населення. Зокрема, вони висловлювали підозри, що, можливо, саме серед односельців виявилися зрадники, які прямо вказали на розшукувані категорії осіб. Навіть якщо це так, усе одно залишається питання, чи це справді єдине джерело з огляду на масив інформації? Це ще доведеться з'ясувати.

2. ХЕРСОНСЬКА ОБЛАСТЬ

У квітні 2022 року міський голова на той час окупованого міста Херсон повідомив, що російські військові отримали персональні дані понад сотні місцевих активістів і майже всіх цих людей викрали.

«Доброзичливці» повністю злили базу даних на всіх активістів, які перебували в місті. У них виявились особисті справи на кожного мого профільного заступника, інформація умовно від родоводу дружини до прізвиська улюбленого собаки. Те саме стосується тероборони та херсонських учасників бойових дій, які були в Донецьку та Луганську, дані про те, де вони живуть і чим володіють», — зазначив міський голова в інтерв'ю для медіа[7].

Він був упевнений, що такі відомості міг надати лише той, хто мав доступ до конфіденційної інформації. За словами міського голови, викрали понад сто людей. Ізолятор тимчасового тримання в Херсоні на вулиці Теплоенергетиків — одне з місць, де російські військові катували українців. Місцеві жителі, які пройшли через цю катівню, розповідали, що в росіян уже були сформовані списки з персональними даними осіб. До цього ізолятора привозили всіх, хто служив у Збройних Силах України, органах правопорядку, а також активістів, журналістів та інших. Там їх допитували, щоб дізнатися, чи взаємодіють вони з українськими спецслужбами та чи мають плани з реалізації заходів Руху опору.[8]

7 ЗМІ, інтерв'ю з мером Херсона під час тимчасової окупації у 2022 році. Режим доступу: *https://zmina.info/news/mer-hersona-povidomyv-shho-okupanty-otrymaly-dani-ponad-sotni-misczevyh-aktyvistiv-lyudej-vykraly/?fbclid=IwAR1_iczqCGhHFIX7QwnxnHyhyR_im39xlKo_4zoc2ce2gdvdSy8FPYQBL3M*

8 ЗМІ з посиланням на свідчення постраждалих і дані органів правопорядку. Херсонці про катування в ізоляторі. Режим доступу: *https://suspilne.media/318636-ne-davali-spati-pidijmali-ta-vimagali-kricati-slava-rosii-hersonci-svidcat-pro-katuvanna-v-itt/*

Постійна представниця Президента України в Автономній Республіці Крим Таміла Ташева під час пресконференції зазначила, що на Херсонщині утримувалися в підвалах понад 500 українців. За її словами, наприклад, у селищі Новоолексіївка та в місті Геніческ окупаційні «адміністрації» або російські військові мали списки активістів, які брали участь у громадянській блокаді Криму у 2015 році.[9] Вони забирали людей з дому та вулиць.

Для того, щоб проїхати блокпост, потрібно було отримати спеціальну перепустку. За даними Центру національного спротиву, таким чином російські окупанти контролювали переміщення осіб і збирали дані про зв'язки між українцями, бо при заповненні перепустки люди вказували мету пересування та інформацію про тих, до кого їдуть[10]. Вікторія, жителька Херсонської області, розповіла, що її племінника затримали під час перевірки документів (так званої «фільтрації») на блокпості в Армянську. Його ім'я було в списках серед активістів, на яких полюють росіяни. Після затримання чоловіку на голову надягнули пакет і повезли на базу відпочинку, розташовану в районі Скадовська.[11]

З метою придушення опору російські війська проводили так звану «фільтрацію населення», спрямовану на виявлення та затримання українців, які могли б протидіяти процесам становлення нової проросійської влади або просто бути невдоволені її діями. На окупованих територіях створювали спеціальні фільтраційні табори й пункти утримання та катування затриманих. За даними[12] Єльського університету, станом на вересень 2022 року Росія створила на території України 21 локацію для фільтраційних заходів. Достеменну кількість «катівень» наразі визначити складно, але в червні 2023 року Національна поліція України заявила[13] про виявлення на деокупованих територіях 53 місць незаконного утримання та катування людей.

9 ЗМІ, заява постійного представника Президента України в АРК Таміли Ташевої. Режим доступу: *https://www.ukrinform.ua/rubric-regions/3476810-na-zahoplenij-hersonsini-vorogi-trimaut-u-pidvalah-i-katuut-majze-piv-tisaci-ludej.html*

10 Загарбники збирають дані про мешканців окупованих територій за допомогою спецперепусток. Режим доступу: *https://espreso.tv/zagarbniki-zbirayut-dani-pro-meshkantsiv-okupovanikh-teritoriy-za-dopomogoyu-spetsperepustok-tsns*

11 Фільтрація на Херсонщині і в Криму: куди зникають українці. Режим доступу: *https://mipl.org.ua/filtracziya-na-hersonshhyni-i-v-krymu-kudy-znykayut-ukrayinczi/*

12 U.S. report identifies 21 'filtration' locations run by Russia for processing Ukrainians. Режим доступу: *https://www.reuters.com/world/exclusive-us-report-identifies-21-filtration-locations-run-by-russia-processing-2022-08-25/*

13 Злочини, вчинені військовими рф під час повномасштабного вторгнення в Україну (станом на 15.06.2023). Режим доступу: *https://www.npu.gov.ua/news/zlochyny-vchyneni-viiskovymy-rf-pid-chas-povnomasshtabnoho-vtorhnennia-v-ukrainu-stanom-na-15062023*

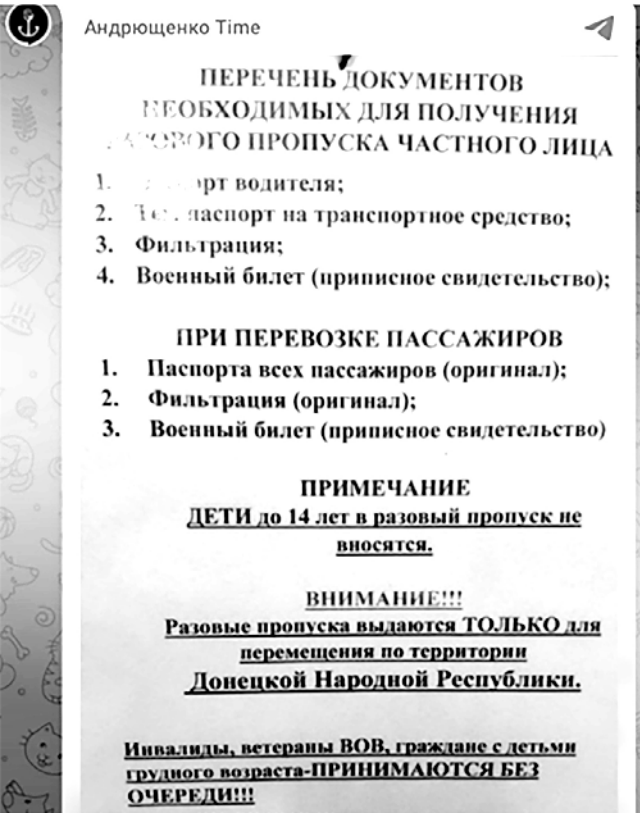
Окрім того, персональні дані населення збирали й іншими способами. Виконувач обов'язків голови Херсонської ОВА Дмитро Бутрій розповів виданню «Суспільні новини», що окупаційна влада виплачувала по 10 тисяч рублів на місяць пенсіонерам в обмін на їхні персональні дані. Українці похилого віку змушені були приймати ці виплати, адже інакше не мали на що жити. За словами мешканки Херсонщини, у її літньої матері немає банківської картки, тому вона деякий час після окупації не отримувала пенсійних виплат. Одного дня до неї прийшла поштарка й попросила паспорт, ідентифікаційний код і довго щось переписувала, нічого не пояснюючи. Потім вручила 20 тисяч російських рублів за два місяці. Коли жінка запитала: «Що ви там переписували?», їй відповіли, що це необхідно для підтвердження отримання пенсії. За даними управління Пенсійного фонду України, у Херсонській області понад 70 тисяч людей користувалися послугами пошти для отримання соціальних виплат[14].

(Джерело зображення: zinkevych / freepik.com)

3. ДОНЕЦЬКА ОБЛАСТЬ

Раніше вже було згадано, що на території Донецької області, зокрема в місті Маріуполі, ще до повномасштабного вторгнення закликали місцевих жителів записувати та передавати дані про ветеранів АТО, проукраїнських активістів, політичних діячів і членів їхніх сімей.

14 На Херсонщині представники окупаційної влади носять пенсії в рублях по домівках та збирають особисті дані. Режим доступу: *https://suspilne.media/267847-na-hersonsini-predstavniki-okupacijnoi-vladi-nosat-pensii-v-rublah-po-domivkah-ta-zbiraut-osobisti-dani/*



(Джерело зображення: Telegram-канал Андрющенко Time)

Водночас коли Маріуполь уже перебував під окупацією, за повідомленнями української влади, російські окупанти продовжували збирати дані місцевого населення. За словами радника міського голови Маріуполя Петра Андрющенка, одним з приводів для отримання інформації став збір заяв для начебто відновлення пошкодженого житла. Він пояснив, що дані були необхідні для проведення мобілізації та псевдореферендуму, і це було частиною підготовки. Наприклад, для отримання разової перепустки на виїзд або в'їзд у Маріуполь потрібно було обов'язково подати військовий квиток. Облік вела комендатура, звіряючи дані, надані в заявах на відновлення житла. У такий спосіб не тільки формували списки для підтасування референдуму, але й відновлювали військовий облік[15].

4. ХАРКІВСЬКА ОБЛАСТЬ

Мешканка міста Ізюм у Харківській області розповіла в інтерв'ю для медіа, що була змушена покинути свій дім перед окупацією, але там залишився її двоюрідний брат. Він не був військовим, а місцевим рятувальником. Попри це все одно потрапив у списки росіян, які викрали його з дому. Людину катували, але, на щастя, згодом відпустили.[16]

Прийшли і до 61-річного пана Миколи, електрика, футболіста-ветерана та тренера, який проживав у селі Веселе. В окупантів на нього також було повне досьє з інформацією про коло спілкування, осіб, яким він до-

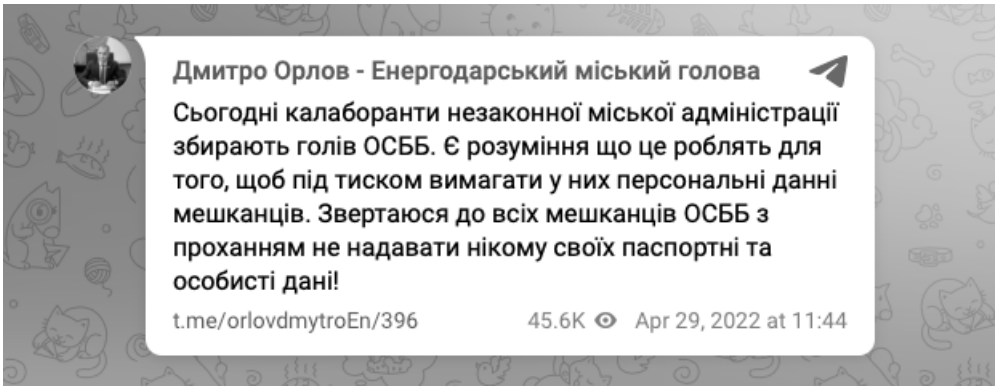
15 Телеграм-канал радника міського голови Маріуполя Петра Андрющенка.

16 ЗМІ, за словами очевидців. Режим доступу: *https://life.pravda.com.ua/society/2022/05/11/248583/*

помагав, і навіть про те, що у 2015-му як депутат місцевої ради він сприяв у виділенні землі учасникам АТО. Чоловіка катували, щоб дізнатися, з ким він співпрацював та яку інформацію й кому передавав.[17]Деяким паяльником випалювали на тілі хрести, щоб таким чином вибити з місцевих жителів імена й адреси учасників АТО, бійців територіальної оборони та осіб, які мали проукраїнську позицію. Затриманим українцям погрожували смертною карою на мінному полі та розправою над сім'ями, що перебували в окупованому місті[18].

5. ЗАПОРІЗЬКА ОБЛАСТЬ

У місті Енергодар у Запорізькій області інженер Запорізької АЕС повідомив у медіа про викрадення багатьох співробітників станції[19]. За словами очевидця, люди зникали, наче за певним алгоритмом. Спочатку громадські активісти Енергодара, далі — учасники АТО та їхні родичі, потім — усі, хто ідентифікує себе українцями.[20]



(Джерело зображення: Telegram-канал Дмитро Орлов - Енергодарський міський голова)

У березні 2022 року російські війська окупували місто Василівка й одразу почали шукати місцевих активістів. Українських журналістів, по-

17 ЗМІ з посиланням на свідчення постраждалого. Режим доступу: *https://www.youtube.com/watch?v=H0-zP49kVHI*

18 ЗМІ, за словами очевидців. Режим доступу: *https://glavcom.ua/country/incidents/bili-strumom-i-vipaljuvali-khresti-na-tili-rashisti-zhorstoko-katuvali-meshkantsiv-kupjanska-video-875931.html*

19 Запорізька атомна електростанція (***ЗАЕС***) — атомна електростанція в Україні, у степовій зоні на березі Каховського водосховища в Запорізькій області.

20 ЗМІ, повідомлення інженера ЗАЕС. Режим доступу: *https://www.unian.net/war/okkupanty-prevratili-proverku-zhenshchin-na-kpp-zaes-v-pytku-rabotnik-stancii-novosti-vtorzheniya-rossii-na-ukrainu-11940765.html?utm_source=viber&utm_medium=viber&utm_campaign=viber_site*

садовців катували особливо жорстоко[21]. У квітні 2022 року представники самопроголошеної міської адміністрації зібрали голів ОСББ[22] для того, щоб вимагати надати персональні відомості мешканців[23].

Міський голова міста Мелітополь Іван Федоров у своєму телеграм-каналі розповів, що росіяни змушували місцевих жителів оформлювати спеціальні перепустки. Таким чином вони збирали персональні дані, щоб відстежувати переміщення людей між населеними пунктами[24]. За даними звіту Запорізької ОВА від 20 травня 2022 року, у Мелітополі в центрі надання адміністративних послуг російські окупанти почали видавати пенсіонерам по 10 тисяч рублів в обмін на їхні дані *(паспорт, пенсійне посвідчення тощо)*. Так само обмінювали особисті дані за винагороду і в селищі міського типу Михайлівка. Окупанти реєстрували пенсіонерів нібито для виплати їм пенсій[25]. Тобто, окрім конкретних списків осіб, вони формували бази даних населення. Можна припустити, що це робилося для зміни даних, викривлення або подальшого знищення.

За даними Центру національного спротиву[26], згодом російські окупанти збільшили перелік соціальних груп населення, які намагалися підкупити для отримання паспортних даних. Зокрема, грошову допомогу пропонували малозабезпеченим родинам, матерям з дітьми до трьох років й іншим соціально незахищеним верствам населення. На людей чинили тиск, щоб вони були змушені брати російські документи. Також примусова паспортизація проводилася в місцях позбавлення волі.

Кожен із зазначених вище інцидентів потребує розслідування з боку українських органів правопорядку, зокрема з'ясування, звідки у російських військових опинилися детальні досьє про українців. У наступних розділах будуть розглянуті факти, що могло стати джерелом для отримання такої інформації.

21 ЗМІ з посиланням на органи правопорядку. Режим доступу: *https://www.slidstvo.info/news/okupanty-iaki-katuvaly-ukraintsiv-strumom-i-khimichnymy-reaktyvamy-vyiavylysia-biytsiamy-dahestanskoho-omonu/*

22 ***ОСББ*** — це об'єднання співвласників багатоквартирного будинку, яке створене, щоб спростити управління та використання майна.

23 Про це повідомив мер Енергодару Дмитро Орлов у своєму телеграм-каналі.

24 ЗМІ, повідомлення мера Мелітополя. Режим доступу: *https://espreso.tv/melitopol-stae-zakritim-mistom-ni-vikhati-do-nogo-ni-viikhati-zvidti-nemozhlivo-mer-fedorov*

25 Про це було повідомлено у звіті Запорізької ОВА. Режим доступу: *https://t.me/zoda_gov_ua/8041*

26 Окупанти збільшили масштаби підкупу населення для отримання паспортних даних. Режим доступу: *https://sprotyv.mod.gov.ua/okupanty-zbilshyly-masshtaby-pidkupu-naselennya-dlya-otrymannya-pasportnyh-danyh/?fbclid=IwAR3rtKVxFYhsILLGb2L0nezMmww4JXRq7wNF5ZpowdyEEb7QWNc1s9OFfYA*

ДЕРЖАВНІ ЗАКРИТІ БАЗИ ПЕРСОНАЛЬНИХ ДАНИХ

(Джерело зображення: pressfoto / freepik.com)

Сьогодні практично не існує організацій чи установ, які б не збирали персональні дані. Єдине, що їх відрізняє, — мета та вид інформації, яку вони обробляють. Наприклад, магазинам переважно потрібні електронні адреси та номери телефонів для просування продуктів. Інтернет-компанії збирають поведінкові дані людини: які сайти відвідує, що шукає, дивиться тощо, щоб у результаті отримати цифровий продукт, на основі якого формується реклама тощо. Банки, медичні, страхові, туристичні та інші сервіси взагалі не можуть вести свою діяльність без персональних даних. Але найширший спектр інформації про людину збирає держава.

Державні органи влади формують банки даних для здійснення своїх функцій у різних сферах — правоохоронній, медичній, соціальній, освітній тощо. Персональні дані можуть зберігатися на папері, в інформаційних системах або інших носіях. Це означає, що загрози для витоку інформації виникають не лише в разі кібератаки, а ще працівники самі можуть її розповсюджувати.

Головна проблема в тому, що в людини практично немає інструментів контролю за використанням своїх персональних даних. Якщо хтось вирішить про когось щось дізнатися, то за певну суму можна купити будь-яку інформацію. На жаль, сьогодні мало досліджень у цій сфері, тому складно сказати, наприклад, у яких секторах найбільше витоків даних. Ми можемо спиратися лише на випадки, які стали відомі та мали наслідки.

Протягом 2022–2023 років було досить багато повідомлень від органів правопорядку, громадських активістів і медіа про несанкціонований доступ і продаж державних баз, які містять персональні дані громадян України та країн Європейського Союзу. Ідеться про різні види інформації, яку за певну плату продають, зокрема, громадянам Росії. Головне питання: звідки в зловмисників доступ до закритих державних баз даних? Є повідомлення про викриття конкретних чиновників, які мали до них доступ. Але серед злочинців не всі були представниками влади.

У так званому даркнеті є величезна кількість пропозицій продажу різноманітних баз даних, включно із секретними. Такі бази можуть містити тисячі файлів з інформацією про будь-кого. Сьогодні процвітає ціла індустрія послуг, яка пропонує сформувати досьє на будь-яку людину. Тому не можна говорити, що проблема тільки у ворожих кібератаках. Уже є достатньо доказів, що значна частина витоків відбувається через соціальну інжене-

рію, коли люди, які мають доступ до інформації, навмисно або ненавмисно її поширюють. Поганий захист державних реєстрів, низький рівень цифрової грамотності працівників й відсутність належного контролю сприяють тому, що активно розвивається продаж персональних даних, які належать громадянам не тільки України, а й інших країн світу. Цей сегмент тіньового ринку послуг базується як на профільних андеграунд-майданчиках, так і таких платформах, як Telegram, Viber тощо. Знову ж таки, важливо те, що в багатьох випадках зловмисники не зламують бази, а просто купують вкрадені дані та використовують їх для пошуку інформації про конкретних людей[27]. Тому акцент робиться не стільки на проблемі технічного захисту даних, як організації процесу їх обробки загалом.

1. НЕСАНКЦІОНОВАНИЙ ДОСТУП ДО ДЕРЖАВНИХ БАЗ ДАНИХ

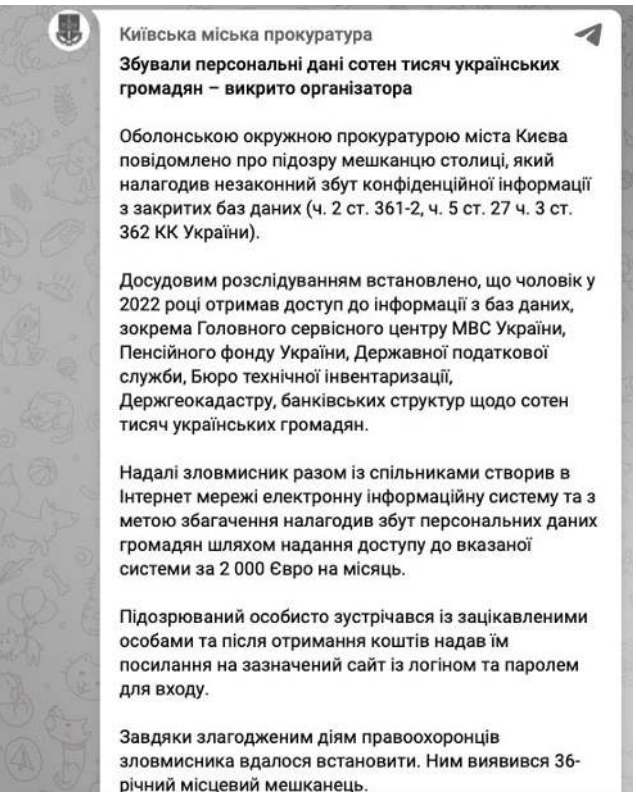
У квітні 2023 року Київська міська прокуратура повідомила, що викрила організатора, який продавав персональні дані українців. Оболонська окружна прокуратура міста Києва повідомила про підозру[28] мешканцю столиці, який здійснював незаконний продаж конфіденційної інформації із закритих баз даних.

Досудове розслідування встановило, що чоловік у 2022 році отримав доступ до інформації з баз даних, зокрема Головного сервісного центру Міністерства внутрішніх справ України, Пенсійного фонду України, Державної податкової служби, Бюро технічної інвентаризації, Держгеокадастру, банківських структур тощо. Зловмисник разом зі своїми спільниками створив в інтернеті інформаційну систему та з метою збагачення налагодив збут персональних даних громадян шляхом надання доступу до реєстрів за 2 000 євро на місяць. Підозрюваний[29] особисто зустрічався із зацікавленими особами та після отримання коштів надавав їм посилання на цей сайт з логіном і паролем для входу.

27 Вашу адресу, паспорт та рахунки можна легко купити в даркнеті за $ 100. Як працює ринок «пробиву» персональних даних. Режим доступу: *https://forbes.ua/inside/vashu-adresu-pasport-ta-rakhunki-mozhna-legko-kupiti-v-darkneti-za-100-yak-pratsyue-rinok-probivu-personalnikh-danikh-28012022-3431*

28 Частина 2 статті 361-2, частина 5 статті 27, частина 3 статті 362 Кримінального кодексу України.

29 Частина 2 статті 361-2, частина 5 статті 27, частина 3 статті 362 Кримінального кодексу України.



(Джерело зображення: Telegram-канал Андрющенко Time)

У ході обшуків за місцем проживання чоловіка вилучено системні блоки, жорсткі диски та інші пристрої, на яких зберігалася незаконно отримана конфіденційна інформація, а також номери телефонів, посвідчення, печатки, паспорти громадян Росії, документація про діяльність угруповання, грошові кошти на суму, еквівалентну 340 тисяч євро. Виникає питання: як ці особи отримали доступ до закритих державних баз даних? Саме тому під час підготовки цього тексту ми направили запит про надання роз'яснення в органи прокуратури. На момент публікації звіту відповіді так і не було.

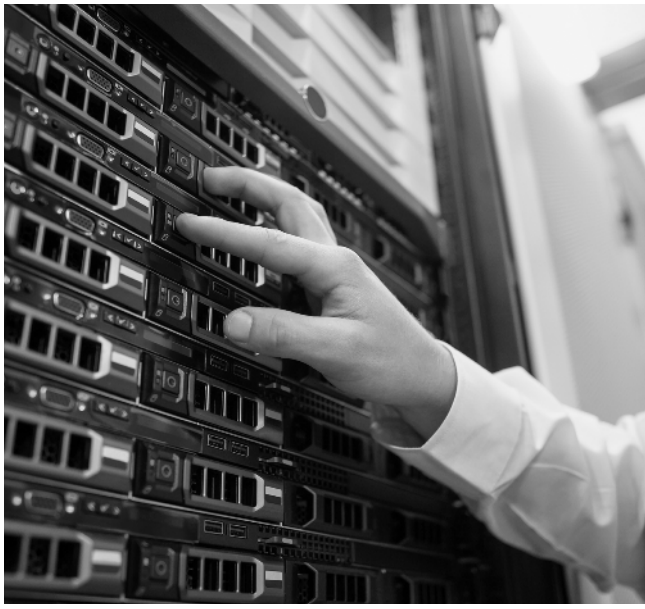
2. ПРОДАЖ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДЯН УКРАЇНИ ТА ЄВРОПЕЙСЬКОГО СОЮЗУ

Працівники кіберполіції розкрили масштабну операцію зі збуту персональних даних громадян України та Європейського Союзу. Злочинну діяльність організував 36-річний житель міста Нетішин у Хмельницькій області. Чоловік був адміністратором закритих груп у Telegram. Саме там переважно здійснювався продаж персональних даних за запитом. Серед інформації, яка пропонувалася на продаж, були паспортні дані, номери платників податків, свідоцтва про народження, водійські посвідчення та банківські рахунки. База даних містила особисту інформацію понад 300 мільйонів осіб, серед яких були громадяни України та країн Європейського Союзу. Залежно від обсягу інформації зловмисник вимагав від 500 до 2 000 доларів за доступ до даних. За виявленою інформацією, серед покупців даних були громадяни Росії. У його оселі правоохоронці

провели обшук і вилучили мобільні телефони, жорсткі диски, SIM-карти, комп'ютерну техніку та серверне обладнання, де виявили бази даних з обмеженим доступом[30]. Так само виникає питання: як ці особи отримали доступ до закритих баз даних?

Подібну схему також розкрила Служба безпеки України. Організатором виявився підприємець із Черкас, який придбав спеціалізоване серверне обладнання для збору та обробки персональних даних. До незаконної діяльності залучив двох мешканців столиці, які допомагали йому зі створенням й адмініструванням онлайн-сервісів. Зокрема, вони створили спеціалізовану інтернет-платформу й телеграм-бот, за допомогою яких продавали паспортні дані, номери телефонів й автомобілів, що належали мешканцям різних регіонів України. За даними слідства, для отримання доступу до електронних баз даних замовники купували підписку на відповідні інтернет-ресурси та пропонували придбати «абонемент» на місяць вартістю до 200 доларів. Для пошуку клієнтів використовували спеціально створені телеграм-канали, а оплату отримували на криптогаманці. Серед потенційних замовників таких інтернет-послуг були представники російських спецслужб, які шукали конфіденційну інформацію про військовослужбовців.

Під час обшуків за адресами проживання зловмисників було виявлено комп'ютерне обладнання та інші речові докази злочину. Організатору схеми повідомлено про підозру за частиною 1 статті 361-2 Кримінального кодексу України (несанкціонований збут інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), захищеної відповідно до чинного законодавства). На момент публікації цього матеріалу ще тривало розслідування для встановлення всіх обставин злочину та притягнення винних до відповідальності.



(Джерело зображення: wavebreakmedia / freepik.com)

30 Офіційна сторінка кіберполіції в соціальній мережі Фейсбук. Режим доступу: *https://www.facebook.com/cyberpoliceua/posts/pfbid0wATw3mv1Sw25ssF8QdJAHEMB8z4eKHyyLyDuAQREaPpHR2YnrpyoJt9iDZvenpxml*

3. ПРАЦІВНИК КАБІНЕТУ МІНІСТРІВ УКРАЇНИ ПЕРЕДАВАВ СЕКРЕТНУ ІНФОРМАЦІЮ ТА ПЕРСОНАЛЬНІ ДАНІ УКРАЇНЦІВ

У червні 2022 року Служба безпеки України на своєму офіційному сайті повідомила, що провела багатоетапну спецоперацію, щоб знешкодити агентурну мережу ФСБ, яка вела розвідувально-підривну діяльність в органах державної влади України. У результаті цієї операції затримано осіб, які займали посади — завідувача відділу Секретаріату Кабінету Міністрів України та керівника однієї з дирекцій Торгово-промислової палати.

(Джерело зображення: Racool_studio / freepik.com)

Ці посадовці передавали до країни-агресора інформацію: від стану обороноздатності до облаштування держкордону та персональних даних українських правоохоронців. Вони робили це не безкоштовно, їм платили за інформацію від 2 до 15 тисяч доларів за завдання. Суми залежали від рівня таємності й важливості зібраних даних. Секретні документи зловмисник роздруковував, фотографував і зберігав на флеш-накопичувачах. Для передачі файлів домовлявся через закритий телеграм-канал про зустріч зі своїм «зв'язковим» — одним з працівників Торгово-промислової палати. За даними слідства, схема передачі даних працювала так: урядовець передавав їх «зв'язківцю» з палати, а той — далі в Росію через зашифровані канали зв'язку. Обом зловмисникам повідомлено про підозру у вчиненні злочину за статтею 111 (державна зрада) Кримінального кодексу України. Суд обрав їм міру запобіжного заходу у вигляді тримання під вартою[31].

31 Офіційний сайт Служби безпеки України. Режим доступу: *https://ssu.gov.ua/novyny/sbu-vykryla-rosiisku-ahenturu-do-yakoi-vkhodyly-posadovtsi-kabminu-i-torhovopromyslovoi-palaty-ukrainy-video*

4. «ПРИВАТНІ ДЕТЕКТИВИ» ПРОДАВАЛИ КОНФІДЕНЦІЙНУ ІНФОРМАЦІЮ З ДЕРЖАВНИХ БАЗ ДАНИХ

У травні 2023 року Служба безпеки України повідомила[32], що їхні кіберфахівці «нейтралізували» в Києві злочинну діяльність приватного детективного агентства, яке продавало інформацію із закритих баз даних держаних установ. Незаконну діяльність організував колишній слідчий одного зі столичних райвідділів міліції, який відмовився проходити атестацію в лави поліції і у 2015 році звільнився з органу правопорядку. Згодом він спільно зі своїм знайомим створив приватне детективне агентство.

(Джерело зображення: офіційна сторінка Служби безпеки України)

Під виглядом легального бізнесу вони збирали для своїх клієнтів конфіденційну інформацію про громадян, у тому числі діставали дані, які зберігаються в закритих державних реєстрах. Для цього використовували «старі» зв'язки серед різних чиновників і представників органів правопорядку. Вартість «досьє» на одну людину сягала від 800 до 2,6 тисячі доларів. Сума залежала від обсягу персональних даних і терміновості «замовлення». Так, наприклад, до «розгорнутих анкет», окрім паспортних даних громадян, входила інформація про номери їхніх телефонів і автомобілів, а також відомості про перетин кордону та вчинення адміністративних правопорушень. Обох «детективів» було затримано під час отримання ними коштів за «папку» з установчими даними на жителя столиці. Під час обшуків за адресами проживання фігурантів виявлено мобільні телефони, комп'ютери з доказами протиправної діяльності. Також перевіряється інформація про можливий продаж конфіденційної інформації до країни-агресора[33].

32 Розслідування проводили слідчі Служби безпеки України у м. Києві та Київській області за процесуального керівництва Київської обласної прокуратури.

33 Офіційний сайт Служби безпеки України. Режим доступу: *https://ssu.gov.ua/novyny/sbu-zatrymala-u-kyievi-dvokh-pryvatnykh-detektyviv-yaki-torhuvaly-konfidentsiinoiu-informatsiieiu-iz-derzhavnykh-baz-danykh*

5. ПРАВООХОРОНЦІ НЕЗАКОННО ЗБИРАЛИ ПЕРСОНАЛЬНІ ДАНІ НАСЕЛЕННЯ В ТЕРНОПІЛЬСЬКІЙ ОБЛАСТІ

У червні 2023 року Державне бюро розслідувань повідомило про підозру працівнику органу правопорядку в Тернопільській області, який незаконно збирав персональні дані добровольців Сил територіальної оборони Збройних Сил України та членів їхніх сімей. Згодом ця інформація була оприлюднена на одному з російських ресурсів.

Підозрюваний систематизував і зберігав імена військових, дати їх народження, місце реєстрації та проживання, наявність у власності рухомого та нерухомого майна, вогнепальної зброї та спецзасобів, контактні номери телефонів родичів. Державне бюро розслідувань не зазначило, з якою метою збиралися ці дані та як надалі використовувалися, зокрема як потрапили до російських пропагандистів, але сам факт несанкціонованої обробки може мати значні наслідки. Правоохоронцю повідомлено про підозру[34] в незаконному збиранні, зберіганні та використанні конфіденційної інформації.[35]

Це не поодинокий випадок, адже в Тернопільській області виявлено ще одних працівників органів правопорядку, які незаконно збирали дані про жителів області. Зокрема систематизували детальну інформацію: про дати народження, місце реєстрації, проживання, наявність у власності рухомого та нерухомого майна, вогнепальної зброї, спецзасобів тощо. Про це повідомила пресслужба Тернопільської обласної прокуратури. Правоохоронцю було висунуто обвинувачення щодо незаконного збирання, зберігання, поширення конфіденційної інформації.[36] Досудове розслідування здійснювали слідчі Територіального управління Державного бюро розслідувань, розташованого у місті Львові.

34 Частина 1, 2 статті 182 Кримінального кодексу України

35 Офіційний вебсайт Державного бюро розслідувань. Режим доступу: *https://dbr.gov.ua/news/dbr-vikrilo-pravoohoroncya-na-nezakonnomu-zbirani-personalnih-danih-ternopilskih-teroboronivciv-yaki-potim-zyavilis-na-rosijskih-resursah*

36 Частина 1, 2 статті 182 Кримінального кодексу України

6. У СУМСЬКІЙ ОБЛАСТІ ВИКРИТО ПРАВООХОРОНЦЯ, ЯКИЙ ЗБУВАВ КОНФІДЕНЦІЙНУ ІНФОРМАЦІЮ З ДЕРЖАВНИХ БАЗ ДАНИХ

У Сумській області викрито правоохоронця, який продавав персональні дані українських громадян[37]. За даними слідства, співробітник оперативного підрозділу Національної поліції у Сумській області отримував з закритих державних баз даних, зокрема прикордонної та міграційної служб України, конфіденційну інформацію, яку потім продавав зацікавленим особам. Він діяв не один, а з іншими учасниками. Пошук потенційних покупців організатори схеми здійснювали на тематичних форумах в інтернеті. Зацікавлені особи замовляли у них потрібну інформацію, потім за таку послугу сплачували обумовлену суму у криптовалюті. Вартість кожного «замовлення» складала кількасот доларів, в залежності від обсягу. Після цього зловмисники несанкціоновано отримували та передавали «клієнтам» дані з інформаційних баз через закриті канали електронного зв›язку.

За даними слідства, серед «клієнтів», яким надавали такі «послуги», були, у тому числі громадяни та мешканці Росії та Казахстану. У ході проведення санкціонованих обшуків за місцем проживання та роботи одного з учасників схеми – співробітника поліції, було виявлено та вилучено: комп'ютерну техніку, флеш-накопичувачі, мобільні телефони, які містять докази протиправної діяльності. Триває досудове розслідування для притягнення до відповідальності усіх осіб, причетних до протиправної діяльності.

(Джерело зображення: freepik / freepik.com)

37 Повідомлення на офіційній сторінці Служби безпеки України у Сумській області в соціальній мережі Фейсбук.

7. АГРЕГАЦІЯ ЗАКРИТИХ ДЕРЖАВНИХ БАЗ ДАНИХ

У контексті випадків з витоками персональних даних потрібно також згадати про ініціативу створення єдиного державного реєстру призовників, військовозобов'язаних та резервістів, який буде наповнюватися шляхом взаємодії з іншими системами, базами даних про громадян[38]. Такі дії необхідні для прискорення процесу актуалізації даних про призовників, військовозобов'язаних і резервістів.

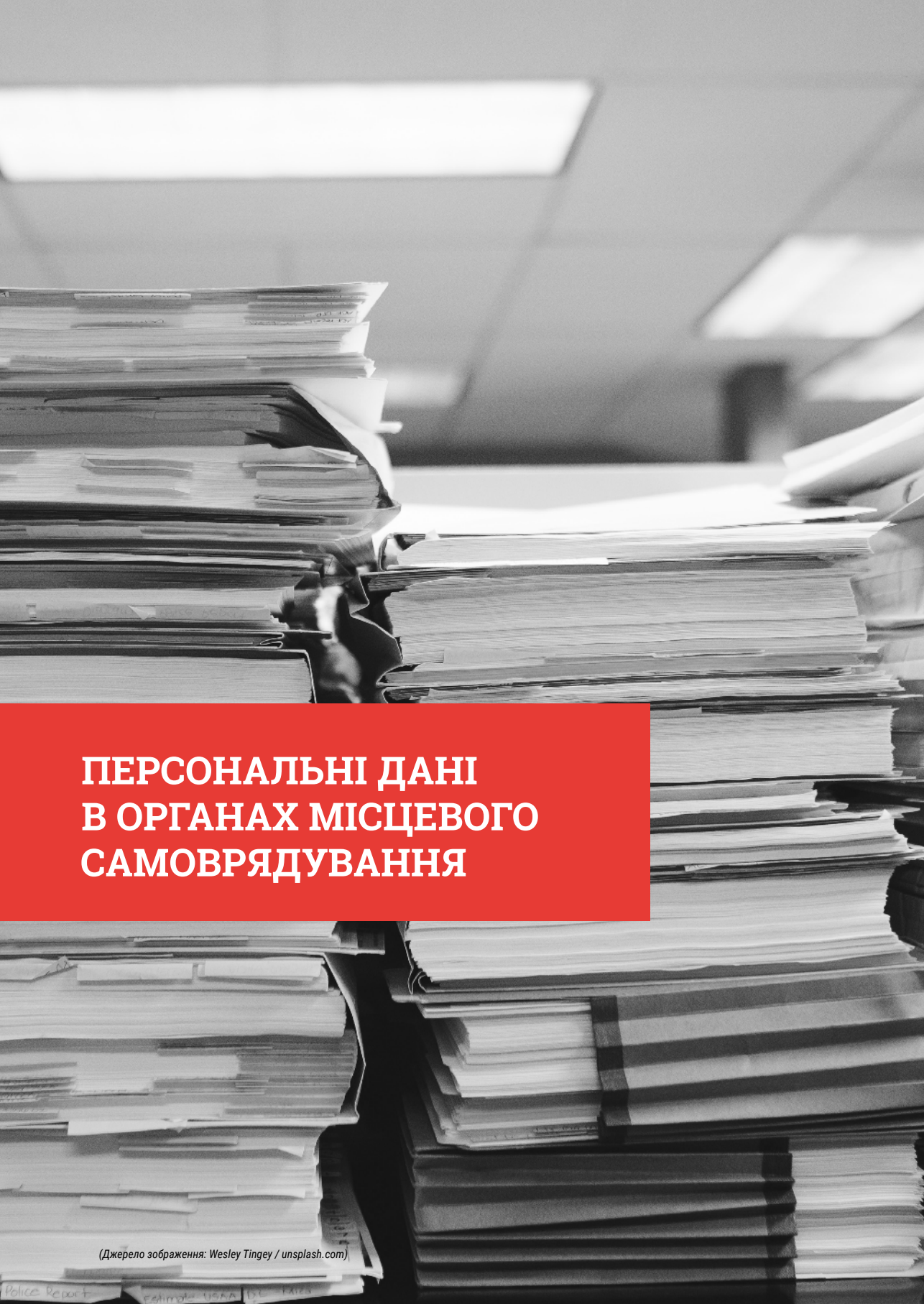
Зокрема, Кабінет Міністрів України постановою про проведення верифікації деяких реєстрових даних від 30 грудня 2022 року № 1493 передбачив проведення звірки персональних даних про фізичних осіб. Для цього було доручено провести верифікацію інформації про осіб на підставі даних, що обробляються в державних інформаційних ресурсах, а саме:

- Єдиному державному демографічному реєстрі;
- Державному реєстрі фізичних осіб — платників податків;
- Державному реєстрі актів цивільного стану громадян;
- реєстрі застрахованих осіб Державного реєстру загальнообов'язкового державного соціального страхування;
- Єдиній інформаційній базі даних про внутрішньо переміщених осіб;
- відомчій інформаційній системі Державної міграційної служби.

Можливо, інформаційна взаємодія між різними відомствами — є необхідним заходом для організації мобілізаційних питань та обороноздатності країни. Проте також важливо наголосити, що при ухваленні подібних рішень обов'язково потрібно враховувати чинне законодавство України з питань захисту персональних даних, яке потребує негайної реформи, наявну систему державного контролю в цій сфері, стан інформаційної безпеки державних систем й організацію роботи з конфіденційною інформацією загалом, зокрема широкий спектр ризиків, які існують сьогодні.

38 В Україні автоматизують та прискорять збір актуальних даних щодо призовників, військовозобов'язаних та резервістів. Режим доступу: *https://sud.ua/uk/news/publication/258417-v-ukraine-avtomatiziruyut-i-uskoryat-sbor-aktualnykh-dannykh-o-prizyvnikakh-voennoobyazannykh-i-rezervistakh*

ПЕРСОНАЛЬНІ ДАНІ В ОРГАНАХ МІСЦЕВОГО САМОВРЯДУВАННЯ



(Джерело зображення: Wesley Tingey / unsplash.com)

Органи місцевого самоврядування (далі — ОМС) здійснюють управління справами в інтересах певної територіальної громади. Повноваження виконавчих органів сільських, селищних, міських рад стосуються різних галузей — житлово-комунального господарства, освіти, охорони здоров'я, соціального захисту населення, оборони, бюджету, забезпечення правопорядку тощо. Виконання завдань зумовлює необхідність збирати та обробляти значні обсяги персональних даних населення.

З кожним роком ОМС ухвалюють нові рішення: впроваджують електронний документообіг; встановлюють комплексні системи відеоспостереження; створюють сучасні вебсайти з онлайн-послугами для мешканців. Розвиток технологій, окрім переваг, водночас створює певний спектр ризиків, які суттєво збільшуються у воєнний час.

У січні 2022 року експерти Асоціації УМДПЛ проводили зустрічі з представниками ОМС з різних регіонів України для того, щоб зрозуміти, з якими саме проблемами вони стикаються під час обробки персональних даних. Як виявилося, більшість з них були пов'язані з організаційними процесами обробки даних і відсутністю внутрішнього контролю. Під час розмови службовці визнавали, що потребують підвищення кваліфікації в цій сфері. Лише невелика кількість працівників цих підрозділів відвідувала спеціалізовані навчальні заходи.

Також ми з'ясували, що порівняно невелика кількість ОМС розробила та впровадила внутрішні розпорядчі документи, які регулюють питання в цій сфері. Навіть у тих ОМС, які ухвалили внутрішні політики у сфері приватності, такі документи часто були скопійовані з інших ресурсів і не адаптовані до діяльності конкретної установи. Відсутність внутрішньої регуляції всіх процесів роботи з даними призводить до ризиків — від порушення загального циклу їх обробки до можливого витоку інформації. Лишаються неврегульованими питання збору інформації та її зберігання. Частими є випадки, коли ОМС накопичують надлишковий обсяг інформації, ще одна поширена проблема — агрегація даних. Об'єднання різних баз даних у єдину становить ризики як для організації внутрішнього управління (ускладнює виконання вимог закону, наприклад диференціацію інформації або вчасне видалення даних), так і для особи, чия інформація міститься в базах даних, адже це може призвести до небажаної ідентифікації людини через її загальний профайл. Практично жоден ОМС не проводив роботи з оцінювання ризиків у сфері обробки даних.

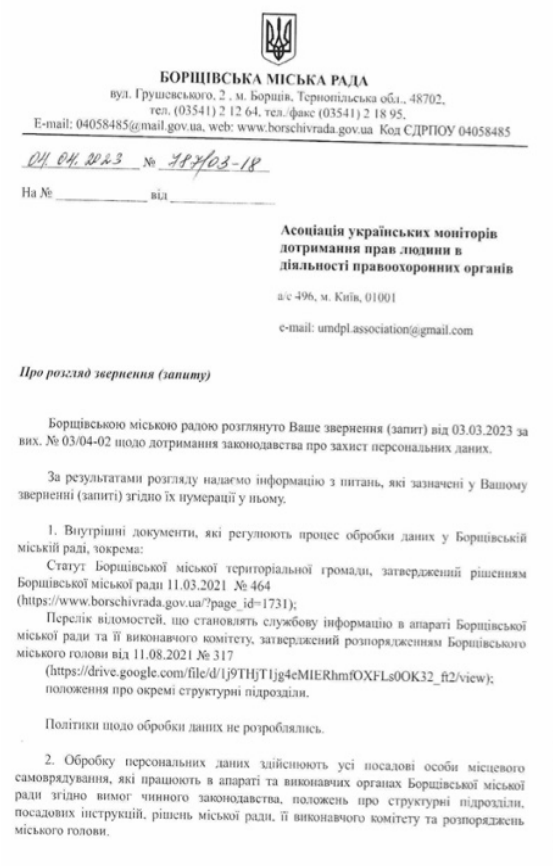
Переважна частина проблем, з якими стикнулися ОМС у воєнний час, не є новою або притаманною лише сьогоденню. Завдану шкоду й негативний вплив на ситуацію в країні внаслідок неналежного захисту персональних даних в ОМС під час війни оцінювати складно. Однак численні повідомлення в медіа свідчать про спроби отримати доступ до баз персональних даних, у тому числі тих, якими розпоряджалися ОМС, не гребуючи для цього викраденням посадовців, насильницькими діями або шантажем. Але, окрім цього, виявилося багато тих, хто самостійно різними способами надавав або оприлюднював інформацію, яку мають міськради.

1. МІСЬКИЙ ГОЛОВА ОПУБЛІКУВАВ ПЕРСОНАЛЬНІ ДАНІ ВІЙСЬКОВОСЛУЖБОВЦІВ

На початку жовтня 2022 року в медіа з'явилася інформація, що міський голова Борщівської міської ради опублікував заяви військовослужбовців, де були зазначені персональні дані військових, зокрема контактні телефони й прізвища. Фото документа з'явилося на сторінці міськради. Після цього на міського голову склали адмінпротокол за статтею про порушення використання документів, що призвело до розголошення службової інформації. Його дії кваліфікували за частиною 1 статті 212-5 Кодексу України про адміністративні правопорушення *(порушення порядку використання документів у сфері оборони, що призвело до розголошення інформації)*. Він, перебуваючи на посаді міського голови Борщівської міської ради, допустив порушення вимог Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів, що містять службову інформацію, [...] внаслідок чого відбулося розголошення службової інформації у сфері оборони країни — ідеться в постанові. Міський голова на судове засідання не з'явився. Водночас подав письмову заяву, у якій просив розглянути справу без його участі. Свою провину визнав, апеляцію не подавав. Суд також визнав чоловіка винним і призначив йому мінімальне за цією статтею покарання — 1 020 гривень штрафу. Окрім того, він повинен сплатити 496 гривень судового збору[39].

39 Zaxid.NET. Режим доступу: *https://zaxid.net/mera_borshheva_oshtrafuvali_za_rozgoloshennya_informatsiyi_pro_viyskovih_n1550640?fbclid=IwAR17aruvpsC7q5PeQEsQtX7Ehl2e98ZvxQrDDVgvUgOYqM9cMeO9Y3tB8Ps*

Наразі ми не можемо говорити про реальні мотиви дій міського голови, можливо, посадова особа ухвалила таке рішення, не усвідомлюючи потенційних наслідків, потім покаялася та понесла відповідальність. Але у цій ситуації важливо звернути увагу на організацію процесу захисту персональних даних в установі загалом. Тому під час підготовки цього документа ми надіслали запит до Борщівської міської ради, щоб з'ясувати, яким чином цей муніципалітет забезпечує безпеку даних, зокрема чи розроблені відповідні внутрішні документи та чи призначена в штаті відповідальна особа, як це зобов'язує закон. У відповідь нам повідомили, що в міській раді відсутні документи, які регулюють цю сферу, і не призначена відповідальна особа. Важливо зазначити, що подібна ситуація характерна не тільки для цієї міської ради. Про цей випадок стало відомо завдяки медіа. Є багато інших фактів, що свідчать про проблеми з виконанням закону.



БОРЩІВСЬКА МІСЬКА РАДА
вул. Грушевського, 2 , м. Борщів, Тернопільська обл., 48702,
тел. (03541) 2 12 64, тел./факс (03541) 2 18 95,
E-mail: 04058485@mail.gov.ua, web: www.borschivrada.gov.ua Код ЄДРПОУ 04058485

04.04.2023 № 787/03-18

На № _____ від _____

Асоціація українських моніторів дотримання прав людини в діяльності правоохоронних органів

а/с 496, м. Київ, 01001

e-mail: umdpl.association@gmail.com

Про розгляд звернення (запиту)

Борщівською міською радою розглянуто Ваше звернення (запит) від 03.03.2023 за вих. № 03/04-02 щодо дотримання законодавства про захист персональних даних.

За результатами розгляду надаємо інформацію з питань, які зазначені у Вашому зверненні (запиті) згідно їх нумерації у ньому.

1. Внутрішні документи, які регулюють процес обробки даних у Борщівській міській раді, зокрема:

Статут Борщівської міської територіальної громади, затверджений рішенням Борщівської міської ради 11.03.2021 № 464
(https://www.borschivrada.gov.ua/?page_id=1731);

Перелік відомостей, що становлять службову інформацію в апараті Борщівської міської ради та її виконавчого комітету, затверджений розпорядженням Борщівського міського голови від 11.08.2021 № 317
(https://drive.google.com/file/d/1j9THjT1jg4eMIERhmfOXFLs0OK32_ft2/view);
положення про окремі структурні підрозділи.

Політики щодо обробки даних не розроблялись.

2. Обробку персональних даних здійснюють усі посадові особи місцевого самоврядування, які працюють в апараті та виконавчих органах Борщівської міської ради згідно вимог чинного законодавства, положень про структурні підрозділи, посадових інструкцій, рішень міської ради, її виконавчого комітету та розпоряджень міського голови.

2. ОФІС ОМБУДСМАНА ПОВІДОМИВ ПРО ПОРУШЕННЯ В ОРГАНАХ МІСЦЕВОГО САМОВРЯДУВАННЯ

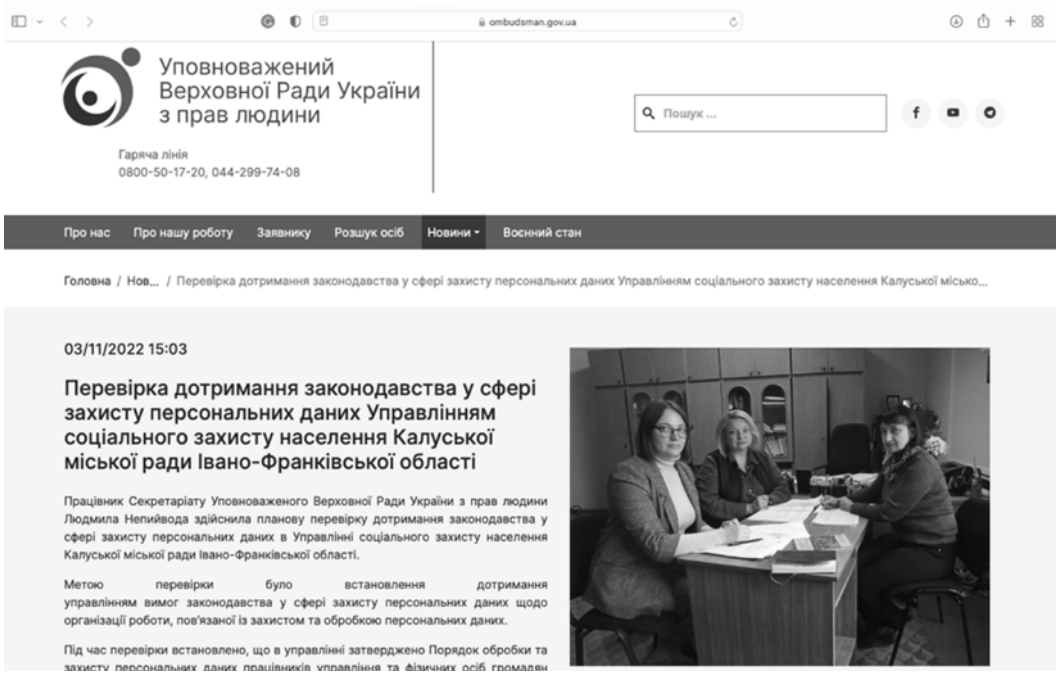
Протягом 2022 року на офіційному сайті Омбудсмена з'являлися повідомлення про планові та позапланові перевірки муніципалітетів щодо дотримання законодавства про захист персональних даних. Зокрема, було здійснено візити до управління соціального захисту населення Калуської міської ради Івано-Франківської області, управління соціального захисту

населення Дніпровської РВА, Перечинської міської ради та Ужгородської міської ради. Практично в усіх ОМС були виявлені порушення закону про захист персональних даних. У повідомленнях ідеться, що серед недоліків виявили такі:

- не повідомлено Уповноваженого з прав людини про обробку даних, яка становить особливий ризик для прав і свобод людини, і про відповідальну особу, що організовує роботу в цій сфері;[40]
- у Дніпровській районній військовій адміністрації не розроблено порядок обробки персональних даних; у працівників, які мають доступ до даних, не відбирають зобов'язання про нерозголошення конфіденційної інформації; не здійснюється облік працівників, які мають доступ до даних; не визначено процедуру видалення даних, строк зберігання яких закінчився; також не повідомлено Уповноваженого з прав людини про обробку особливих категорій даних і відповідальну за це особу; не ведеться облік операцій, пов'язаних з обробкою персональних даних;
- у Департаменті соціальної політики Ужгородської міської ради відсутні належні нормативно-правові акти, що регулюють обробку особливих категорій даних, а саме: інформацію про стан здоров'я та вчинення щодо особи домашнього насильства. У деяких особових справах отримувачів соціальних послуг містяться виписки з акта огляду медико-соціальною експертною комісією Міністерства охорони здоров'я України, у якій зазначено групу інвалідності та діагноз заявника. Департамент в електронному варіанті отримує у вигляді таблиць відомості про виявлені факти домашнього насильства. Також не розроблено окремого положення, яким визначено загальні вимоги до обробки та захисту даних, і не призначено відповідальну особу[41].

40 Перевірка дотримання законодавства у сфері захисту персональних даних Управлінням соціального захисту населення Калуської міської ради Івано-Франківської області. Режим доступу: *https://ombudsman.gov.ua/news_details/perevirka-dotrimannya-zakonodavstva-u-sferi-zahistu-personalnih-danih-upravlinnyam-socialnogo-zahistu-naselennya-kaluskoyi-miskoyi-radi-ivano-frankivskoyi-oblasti*

41 Моніторинг додержання права на звернення та планова перевірка додержання законодавства у сфері захисту персональних даних на Закарпатті. Режим доступу: *https://ombudsman.gov.ua/news_details/monitoring-doderzhannya-prava-na-zvernennya-ta-planova-perevirka-doderzhannya-zakonodavstva-u-sferi-zahistu-personalnih-danih-na-zakarpatti*



Можливо, на перший погляд, такі повідомлення виглядають дещо формальними. Але потрібно звернути увагу, що тут мова йде про причини (невиконання норм закону) уже тих наслідків, які описані в попередньому та інших розділах цього звіту.

3. ЧИНОВНИК З МІСТА МИКОЛАЇВ ОЧОЛЮВАВ РОСІЙСЬКУ АГЕНТУРУ

У Миколаєві контррозвідка Служби безпеки України нейтралізувала російського агента, одним із завдань якого було організувати потужну агентурну групу спецслужб Росії. Зрадником виявився начальник КП «Миколаївська ритуальна служба», якого було затримано просто в міськраді під час наради. Він збирав дані про дислокацію й переміщення підрозділів Збройних Сил України на території регіону. Іншим його завданням було «інформувати» агресора про роботу об'єктів критичної інфраструктури Миколаєва та інші питання, які обговорювалися під час робочих нарад у міськраді. Чиновник намагався залучити до розвідувально-підривної діяльності двох підлеглих і ще двох мешканців міста, серед яких — старший

оперуповноважений районного управління поліції. Також було встановлено, що зловмисник передавав росіянам персональні дані українських військовослужбовців, співробітників поліції, Служби безпеки України та прокуратури, списки загиблих українських захисників[42].

Складно уявити, що один посадовець міг мати доступ до всіх зазначених видів і категорій даних. Це скоріше наслідок неправильної екосистеми обробки інформації, де не були вжиті належні заходи для виконання законодавства у сфері захисту персональних даних і їх безпеки.

42 СБУ знешкодила російську агентуру, яку очолював чиновник із Миколаєва: зрадника затримали під час наради у мера. Режим доступу: *https://ssu.gov.ua/novyny/sbu-zneshkodyla-rosiisku-ahenturu-yaku-ocholiuvav-chynovnyk-iz-mykolaieva-zradnyka-zatrymaly-pid-chas-narady-u-mera-video*

МЕДИЧНІ ДАНІ

(Джерело зображення: Ante Samarzija / unsplash.com)

Питання захисту персональних даних має бути одним з ключових в системі охорони здоров'я. Перш за все приватність впливає на формування довіри суспільства до медичної сфери. Конфіденційність інформації про людину необхідна для її захисту від можливої стигматизації, дискримінації та іншими ризиками, що пов'язані з медичним діагнозом, лабораторними аналізами чи візитами до лікарів. Уже є багато випадків, коли через неправомірне використання медичної інформації (розголошення, викривлення, зміну тощо) було завдано значної психологічної та фізичної шкоди людині. Наприклад, у 2021 році стали відомі декілька історій, які демонструють ризики розголошення медичної інформації.

Олена[43] на той час проживала в невеликому містечку на сході України. Вона — громадська активістка, яка часто виступала за захист прав людини. Проте одного разу сама потребувала юридичної допомоги, коли дізналася, що інформація про її стан здоров'я була неправомірно розголошена. Олена мала серйозне захворювання й стояла на обліку в місцевій лікарні. Але через порушення безпеки персональних даних її медична інформація потрапила в недоброзичливі руки, після чого вона стала жертвою шантажу. Цю подію жінка пов'язувала зі своєю професійною діяльністю.

Інша історія про школярку Надію, яка мала певні проблеми зі здоров'ям. У клініці, де вона проходила реабілітацію, працювала мама одного з її однокласників, яка вирішила розповісти сину про медичні візити Надії. Таким чином, інформація про здоров'я дівчинки стала відома в школі. Спочатку це здавалося непорозумінням, але наслідки виявилися серйозними. Надія стикнулася зі стигмою, образами та дискримінацією. Однокласники почали уникали її, деякі навіть поширювали неправдиві чутки про діагнози, яких не існувало. Дівчинка пережила серйозний психологічний стрес, що надалі негативно вплинуло на її фізичний стан.

Ці приклади наведені лише для того, щоб показати, що проблема порушень захисту персональних у системі охорони здоров'я складається ось з таких складних життєвих історій. Саме тому згідно із законодавством медична інформація належить до особливої категорії даних, бо має високий ризик для прав і свобод людини. Відповідно потребує суворих заходів захисту.

43 Ім'я змінено з міркувань анонімності.

Окрім того, персональні дані можуть стати об'єктом полювання й для зовнішнього ворога. Це стосуються не тільки конкретної людини, а національної безпеки. Протягом 2022–2023 років траплялися повідомлення про витоки з медичних інформаційних систем, які є серйозним сигналом про проблеми в цій сфері, відсутність відповідальності для осіб, які мають доступ до інформації. Зловмисники, які незаконно отримують доступ до медичних баз даних, можуть використовувати ці дані для шахрайства, шантажу, чи передавати ворогу для вчинення воєнних злочинів.

1. У ХЕРСОНСЬКІЙ ОБЛАСТІ МЕДИЧНІ ПРАЦІВНИКИ НЕЗАКОННО ПЕРЕДАВАЛИ ПЕРСОНАЛЬНІ ДАНІ

У червні 2022 року було про притягнуто до відповідальності заступника генерального директора закладу охорони здоров'я з медичної частини Херсонської обласної дитячої лікарні за вчинення державної зради в умовах воєнного стану[44] [45]. За даними слідства, підозрюваний добровільно погодився на співпрацю зі співробітниками спецслужб Росії та представниками окупаційної влади країни-агресора.

(Джерело зображення: офіційна сторінка Служби безпеки України)

Чиновник з власної ініціативи повідомив представникам країни-агресора, що в архів дитячої лікарні була передана на зберігання медична документація з картками та особовими справами співробітників Головного управління Національної поліції в Херсонській області. Після цього російські військові отримали доступ до персональних даних співробітників поліції регіону.

44 Телеграм-канал Офісу Генерального прокурора. Режим доступу: *https://t.me/pgo_gov_ua/4460?fbclid=IwAR3eVEdJeV0zaepQt4pPeRalKpqbU0U2mknQno267p3E7gvfNfnKoxVlmGY*

45 Частина 2 статті 111 Кримінального кодексу України.

17 травня 2023 року Служба безпеки України повідомила,[46] що в Херсоні затримано медсестру однієї з місцевих лікарень, яка передавала ворогу конфіденційну інформацію про місцевих жителів. Навіть після звільнення міста від тимчасової окупації, вона залишилася та продовжила працювати в медичному закладі для проведення розвідувально-підривної діяльності проти України. Жінка збирала для агресора установчі дані українських захисників, які проходили лікування в медичній установі. Також вона шпигувала за місцями базування Сил оборони, які дислокувалися на території обласного центру. Як установили слідчі, у поле зору російської спецслужби жінка потрапила через публічну підтримку загарбників в одній з антиукраїнських груп у Telegram.

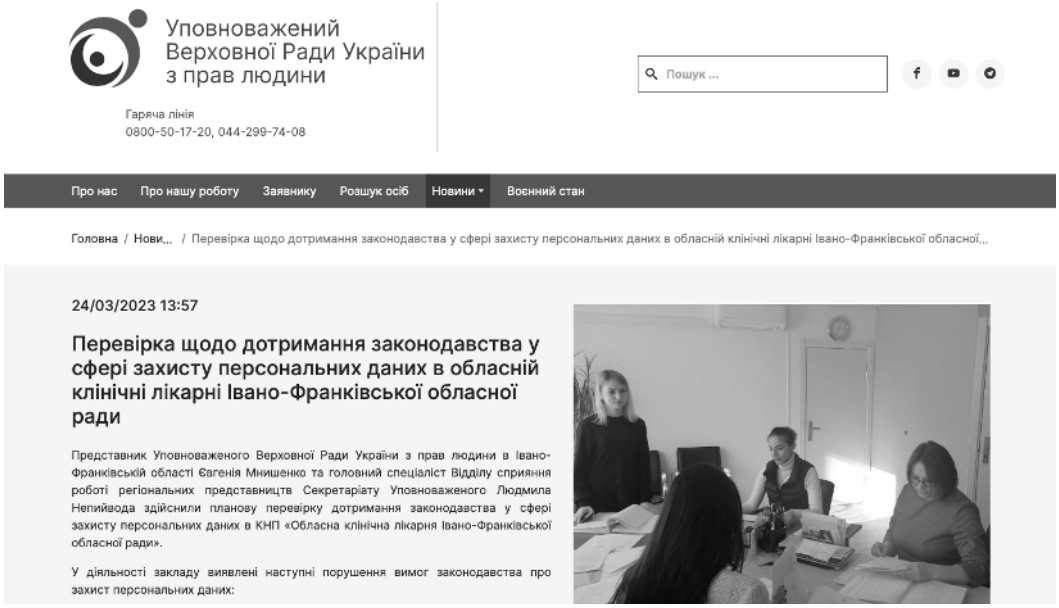
2. ПОРУШЕННЯ ЗАКОНОДАВСТВА В ОБЛАСНІЙ КЛІНІЧНІЙ ЛІКАРНІ ІВАНО-ФРАНКІВСЬКОЇ ОБЛАСНОЇ РАДИ

Протягом 2022–2023 років представники Офісу Омбудсмана здійснювали перевірку медичних закладів на предмет дотримання закону в цій сфері. У березні 2023 року повідомлено, що в Івано-Франківській області було здійснено планову перевірку в КНП «Обласна клінічна лікарня Івано-Франківської обласної ради», де виявлено такі порушення вимог законодавства про захист персональних даних:

- не ухвалено внутрішній розпорядчий документ, який визначає порядок обробки даних з урахуванням специфіки діяльності підприємства у сфері охорони здоров'я, трудових відносин тощо;
- не визначено відповідальну особу за захист та обробку персональних даних у лікарні;
- підприємство не повідомило Омбудсмана про обробку персональних даних, які становлять особливий ризик для прав і свобод людини, зокрема про стан здоров'я тощо;
- не розроблено план дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій[47].

46 Офіційний сайт Служби безпеки України. Режим доступу: *https://ssu.gov.ua/novyny/sbu-zatrymala-medsestru-yaka-pratsiuvala-na-fsb-i-zlyvala-vorohu-personalni-dani-ukrainskykh-zakhysnykiv?fbclid=IwAR0nocpE8aTUSL94SwCLsh06fhuWgtTYmDZC87xDIdxg3FRdAC2d6Wy2nzE*

47 Офіційний сайт Офісу Омбудсмана. Режим доступу: *https://www.ombudsman.gov.ua/news_details/perevirka-shchodo-dotrimannya-zakonodavstva-u-sferi-zahistu-personalnih-danih-v-oblasnij-klinichni-likarni-ivano-frankivskoyi-oblasnoyi-radi*


Уповноважений Верховної Ради України з прав людини

Гаряча лінія
0800-50-17-20, 044-299-74-08

Пошук ...

Про нас | Про нашу роботу | Заявнику | Розшук осіб | Новини | Воєнний стан

Головна / Нови... / Перевірка щодо дотримання законодавства у сфері захисту персональних даних в обласній клінічні лікарні Івано-Франківської обласної...

24/03/2023 13:57

Перевірка щодо дотримання законодавства у сфері захисту персональних даних в обласній клінічні лікарні Івано-Франківської обласної ради

Представник Уповноваженого Верховної Ради України з прав людини в Івано-Франківській області Євгенія Мнишенко та головний спеціаліст Відділу сприяння роботі регіональних представництв Секретаріату Уповноваженого Людмила Непийвода здійснили планову перевірку дотримання законодавства у сфері захисту персональних даних в КНП «Обласна клінічна лікарня Івано-Франківської обласної ради».

У діяльності закладу виявлені наступні порушення вимог законодавства про захист персональних даних:

За результатом перевірки було складено акт і припис про усунення порушення. З огляду на всі обставини, є всі підстави вважати, що це не єдиний заклад, який ігнорує закон у сфері захисту персональних даних.

На додаток, не можна ігнорувати й повідомлення, що Комітет Верховної Ради України з питань здоров'я нації рекомендує депутатам ухвалити законопроєкт № 9272 про внесення змін до деяких законодавчих актів України щодо верифікації відомостей про пацієнтів, яким пропонується передавати персональні дані пацієнтів з електронної системи охорони здоров'я до деяких реєстрів. Запропоновано внести зміни до статті 24-2 «Основи законодавства України про охорону здоров'я» та передбачити передання персональних даних пацієнтів, що зареєстровані в електронній системі охорони здоров'я, або тих, кого планується зареєструвати в ній, до:

- Єдиного державного демографічного реєстру;
- Державного реєстру актів цивільного стану громадян;
- Державного реєстру фізичних осіб — платників податків.

Основна мета такої передачі даних — звірка інформації про особу[48]. Знову ж таки, перед ухваленням будь-яких рішень про створення, агрегацію чи обмін інформацією між базами персональних даних необхідно обов'язково оцінити ризики щодо захисту.

48 Лікарі зможуть передавати ваші персональні дані: що потрібно знати. Режим доступу: *https://ogo.ua/articles/view/2023-05-15/132451.html?fbclid=IwAR0u4pE4Or-HT9DMUvjbzNJLIJHzplaCB1tYPHTM0lU0_RZdqF0sqG5XDus*

3. ПОРУШЕННЯ ПІД ЧАС ФУНКЦІОНУВАННЯ ЕЛЕКТРОННОЇ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я

На офіційному сайті Уповноваженого Верховної Ради України з прав людини[49] було повідомлено[50] про низку перевірок на дотримання вимог захисту персональних даних під час функціонування електронної системи охорони здоров'я. Зокрема, перевірено Національну службу охорони здоров'я України (далі — НСЗУ), ДП «Електронне здоров'я», ТОВ «ХЕЛСІ ЮА», КНП «Центр первинної медико-санітарної допомоги Печерського району», КПН «Центр первинної медико-санітарної допомоги «Русанівка» Дніпровського району м. Києва».

За даними Омбудсмена, перевірки встановили, що під час функціонування електронної системи охорони здоров'я неправильно застосовується законодавство у сфері захисту персональних даних. Власники електронних медичних інформаційних систем збирають персональні дані пацієнтів, у тому числі медичні дані, отримуючи згоду суб'єкта персональних даних. Така згода відбирається або під час звернення суб'єкта персональних даних до закладу охорони здоров'я та укладання декларації з лікарем, або під час реєстрації в електронній медичній інформаційній системі, зокрема для того, щоб записатися на прийом до лікаря. У першому випадку згода надається шляхом проставляння відмітки в електронній формі під час підписання декларації. Як установлено під час перевірок, у закладах охорони здоров'я не завжди повідомляють про надання згоди суб'єктові персональних даних, проставляючи згоду самостійно замість пацієнта і без його відома.

Окрім того, у такому випадку пацієнту не повідомляють про володільця персональних даних, мету збору, їх склад і зміст, кому вони можуть передаватися, його права, визначені законом. За даними Омбудсмена, таким чином, особа позбавляється можливості реалізації та захисту своїх прав як суб'єкта персональних даних. Також під час проведення перевірок вста-

49 Контролюючий державний орган у сфері захисту персональних даних.

50 Виявлено неправильне застосування законодавства в сфері захисту персональних даних під час функціонування електронної системи охорони здоров'я. Режим доступу: *https://www.ombudsman.gov.ua/uk/kontrol-za-doderzhannyam-vimog-zakonodavstva-zpd/rezultati-perevirok/viyavleno-nepravilne-zastosuvannya-zakonodavstva-v-sferi-zahistu-personalnih-danih-pid-chas-funkcionuvannya-elektronnoyi-sistemi-ohoroni-zdorovya*

новлено, що деякі власники медичних інформаційних систем неправильно визначають мету обробки персональних даних і відносини із закладами охорони здоров'я щодо обробки персональних даних пацієнтів.

Власник медичної інформаційної системи має обробляти персональні дані пацієнта з метою закладу охорони здоров'я і виступати в такому випадку розпорядником персональних даних, на що згода суб'єкта персональних даних не потрібна. Проте власники медичних інформаційних систем отримують згоду суб'єктів персональних даних з метою обробки персональних даних закладу охорони здоров'я, а свою власну мету обробки персональних даних зазначають занадто загально. У результаті пацієнти, надаючи згоду на обробку персональних даних, не знають, на що вони фактично погоджуються.

За результатами перевірок НСЗУ було рекомендовано доопрацювати технічні вимоги до електронної медичної інформаційної системи для її підключення до центральної бази даних електронної системи охорони здоров'я, затвердженої наказом НСЗУ від 6 лютого 2019 № 28; ТОВ «ХЕЛСІ ЮА» — доопрацювати документи та узгодити із законодавством у сфері захисту персональних даних відносини ТОВ «ХЕЛСІ ЮА» як розпорядника персональних даних пацієнтів закладів охорони здоров'я із закладами охорони здоров'я, з якими укладено договір про надання послуг користування інформаційно-телекомунікаційною системою «HELSI», і припинити отримувати згоду суб'єктів персональних даних на обробку персональних даних, володільцем яких є заклад охорони здоров'я. З метою з'ясування всіх обставин обробки персональних даних власниками медичних інформаційних систем плануються додаткові перевірки.

У цьому контексті згадаємо новину в медіа про те, що під час повномасштабного вторгнення компанія «Київстар» викупила 69,99 % акцій «Хелсі Україна». «HELSI» — масштабний приватний медтек-стартап, запущений у 2016 році, ключовий гравець на ринку медичних інформаційних систем, що працюють з державними та приватними лікарнями. Цей стартап має амбітні цілі — задовольнити всі потреби людини в її здоров'ї. Якісна, сучасна взаємодія лікарів і пацієнтів дозволить більше робити акцент на профілактику, ніж лікування серйозних хвороб. Сервіс справді якоюсь мірою полегшив доступ до державної медицини. Через нього можна знайти будь-якого лікаря та записатися на прийом, отримати електронне направлення тощо. Усі ці дані автоматично підтягуються в

особистий кабінет користувача із центральної бази Єдиної системи електронного здоров'я.

На травень 2023 року на платформі було зареєстровано понад 25 млн користувачів. До системи підключено медичні заклади по всій країні та приблизно 50 тисяч медпрацівників. Для багатьох українців стало несподіванкою те, що ця інформаційна система приватна, а не державна, і саме приватні структури отримують доступ до стану здоров'я українців. Згідно із Законом України «Про захист персональних даних» така інформація належить до спеціальної категорії даних і вимагає особливого захисту та процесу обробки.

У серпні 2022 року «HELSI» поглинув найбільший в Україні мобільний оператор «Київстар», який належить «Альфа Груп». Медичний стартап «HELSI» став частиною медичної інфраструктури в Україні. У громадськості почали з'являтися питання: хто побудував цей ІТсервіс, просуває його на державному рівні та навіщо він компанії «Київстар» під час війни? Особливе занепокоєння викликав той факт, що серед співвласників компанії «Київстар» є підприємці, які після початку повномасштабного вторгнення потрапили в санкційні списки Великої Британії.

«Київстар» і «HELSI» давно співпрацюють. Наприклад, оператор допомагав абонентам вакцинуватися, розсилаючи таргетовані SMS. Раніше на це особливо ніхто не звертав уваги, тільки зараз постало питання: як обробляються персональні дані мільйонів українців, хто здійснює контроль і має до них доступ?

На додаток до цього, у травні 2023 року в мережі спалахнув скандал навколо фейкових записів у Helsi-кабінетах. Українці в соціальних мережах ділилися історіями, що хтось без їхнього відома записував їх на консультації до лікарів, отримував направлення, діагнози тощо. Кількість акаунтів з фейковими записами у «HELSI» не уточнювали. Проблема могла існувати роками. Чому про неї стало відомо лише зараз? Більшість українців не часто заходить до особистого кабінету «HELSI», але публікації в соцмережах спричинили ефект лавини, і багато людей почали перевіряти свої облікові записи та виявляти, що хтось незаконно використовує їхні чутливі персональні дані.

Версію зламу керівництво медичного сервісу одразу відкинуло, запевняючи, що особисті дані пацієнтів не були скомпрометовані. Система пе-

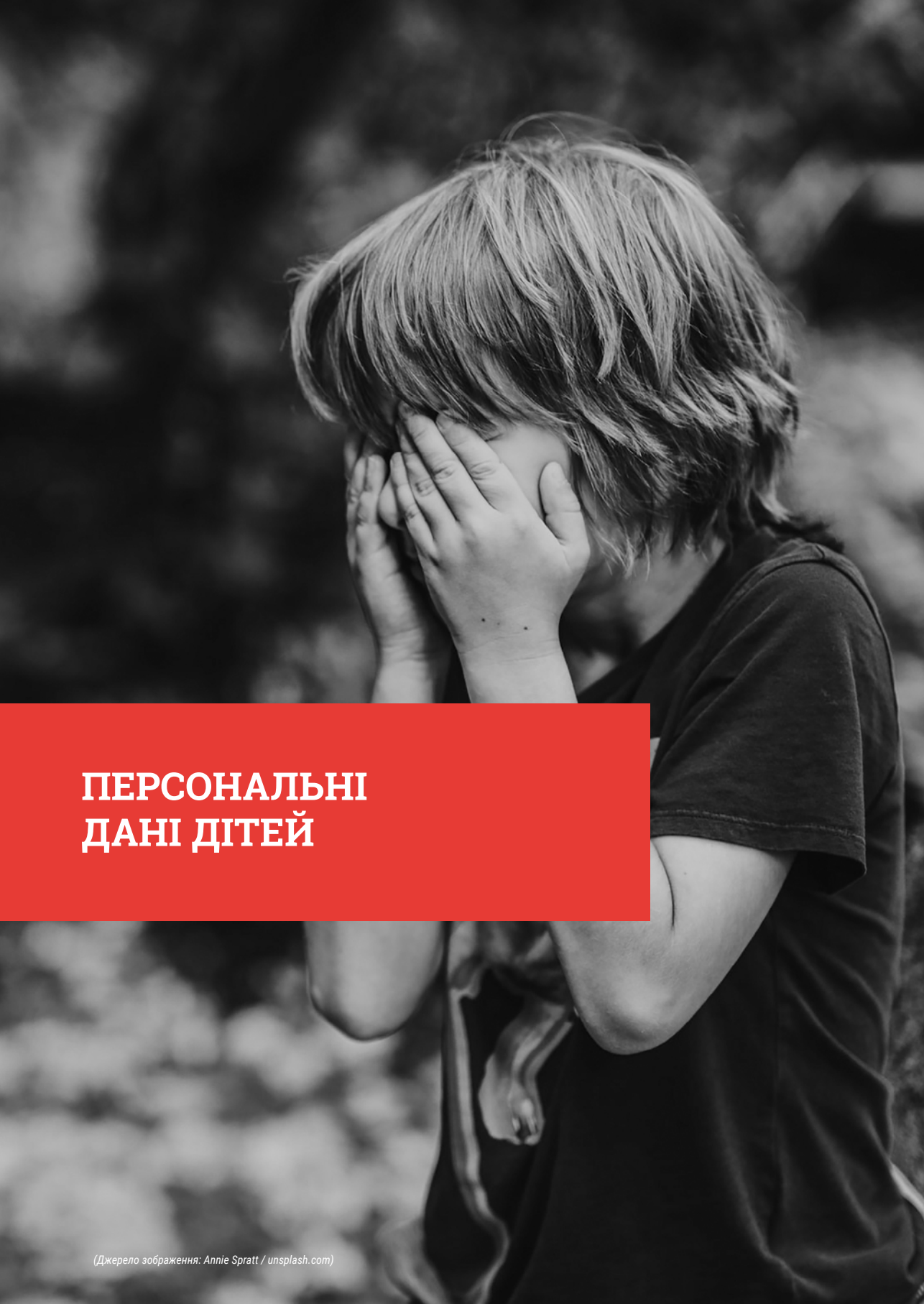
редбачає внесення інформації лише лікарями, тому треті особи начебто не можуть туди втрутитися. Тобто «віртуальні записи» — справа рук не хакерів, а медиків. Який сенс лікарям робити записи про прийоми, яких не було? Одна з можливих причин — це медична реформа, яка стартувала у квітні 2018 року. Її головний принцип — «гроші йдуть за пацієнтом». Більше пацієнтів і процедур — більше державного фінансування. Виділяє на це кошти НСЗУ за спеціальною програмою. Міністерство охорони здоров'я України теж знає про фейкові відвідування в «HELSI» та запевняє, що буде виявляти такі випадки та реагувати. Не відомо, яка вартість витрат і як довго держава платила за лікування, якого ніколи не було[51].

Обробка персональних даних, які зберігаються в медичних інформаційних системах, має велике значення не тільки для захисту приватності конкретної особи, а й національної безпеки загалом. Тому залишаються питання:

- Кому належить (хто є офіційно володільцем) медичної інформаційної системи helsi.me?
- Хто ухвалив рішення про формування цієї бази даних і зобов'язання громадян України (а також медичних закладів) передати дані до цієї системи? Зокрема, які були ухвалені нормативні акти, постанови та накази, що це дозволили?
- Хто конкретно контролює питання захисту персональних даних у цій системі?
- Які заходи із забезпечення захисту інформації в цій системі вжила держава?

Асоціація УМДПЛ надіслала запит до Міністерства охорони здоров'я України з проханням надати роз'яснення на ці та інші питання, проте, окрім загальної фрази «все здійснюється згідно законодавства про захист персональних даних», нічого не отримала.

51 У медичному сервісі Helsi лікарі роками створювали фейкові відвідування пацієнтів. Через це держава могла втрачати кошти. Як цю проблему вирішуватимуть МОЗ та Helsi. Режим доступу: *https://forbes.ua/innovations/ukraintsi-masovo-skarzhatsya-na-feykovi-zapisi-do-likariv-u-servisi-helsi-u-nogo-ponad-25-mln-koristuvachiv-u-chomu-problema-i-chomu-vona-vinikla-ne-sogodni-11052023-13607*



ПЕРСОНАЛЬНІ ДАНІ ДІТЕЙ

(Джерело зображення: Annie Spratt / unsplash.com)

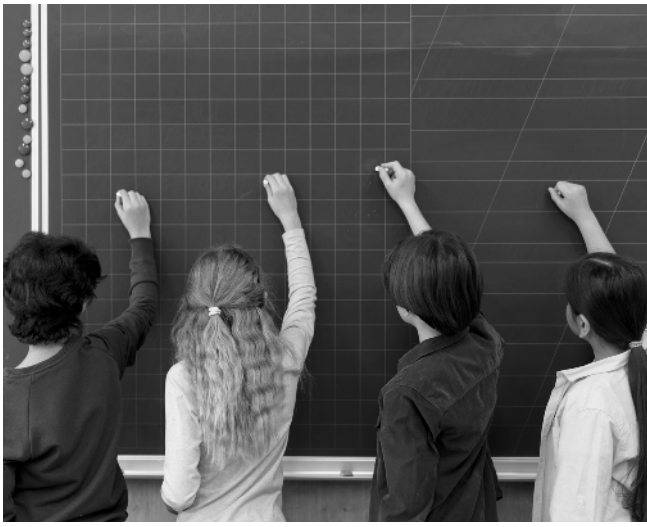
Проблему інформаційної безпеки дитини, як дорослої особи потрібно розглядати з різних аспектів. Персональні дані дитини можуть обробляти різні установи або організації, які своєю чергою зобов'язані забезпечити їхній надійний захист і не допустити несанкціонованих витоків і, як наслідок, злочинного використання інформації. Але також діти можуть самі надавати особисту інформацію в інтернеті або вільно ділитися нею іншими способами, тим самим наражаючи себе на небезпеку.

З одного боку, інтернет надає інструменти, які дозволяють дітям досліджувати навколишній світ. З іншого — відкриває нові можливості для відстеження, зберігання та аналізу даних про дії дітей з недосяжним раніше рівнем деталізації. Так, наприклад, тільки за інформацією із соціальної мережі можна скласти портрет дитини та дізнатися про її місцезнаходження, навчання, хроніку особистих подій, зовнішність, соціальні зв'язки, матеріально-економічне становище батьків, спосіб життя та поведінкові установки.

Джерелом інформації для цифрового профілю може стати будь-яка активність дитини в інтернеті та соціальних мережах: пости, лайки, фотографії, малюнки, онлайн-замовлення тощо. Кожна дія користувача залишає цифровий слід, й інформація, що публікується в інтернеті, може мати наслідки, які проявляться не відразу, а в довгостроковій перспективі. Розкриття особистої інформації дитини може призвести до неприйнятних контактів, різних фінансових махінацій чи навіть викрадення.

1. ГОЛОВА ГРОМАДИ В ХАРКІВСЬКІЙ ОБЛАСТІ ПЕРЕДАЛА ОКУПАНТАМ ПЕРСОНАЛЬНІ ДАНІ УКРАЇНСЬКИХ ШКОЛЯРІВ

23 липня 2022 року очільник Харківської ОВА Олег Синєгубов повідомив, що голова однієї на той час окупованої громади Харківщини пішла на співпрацю з росіянами та передала їм бази персональних даних школярів навчальних закладів. За його словами, цю інформацію було передано для видачі нових дипломів зразка окупаційного режиму. Також він наголосив, що державна зрада з боку держслужбовиці була свідомою, проте не зазначив її прізвище та ім'я[52].



(Джерело зображення: freepik / freepik.com)

Цей випадок вимагає ефективного розслідування з боку органів правопорядку, будемо сподіватися, що українське суспільство дізнається, як таке могло статися. Водночас, якщо подивитися, як функціонує процес обробки персональних даних, особливо в державних системах, то можна припустити, що інформація, яка містилася в базі навчального закладу, оброблялася з порушенням законодавства. Не були встановлені правила роботи, процедури обмеження доступу при загрозі окупації території тощо. Процес незаконної діяльності міг відбутися завчасно або із залученням інших осіб, які допомагали зібрати відомості з різних реєстрів. Це важливо враховувати під час розслідування або аналізу подібних ситуацій, бо основна увага може зміститися лише на злочинну діяльність конкретних осіб, а не належну систему захисту даних загалом. Для того, щоб у майбутньому мінімізувати подібні наслідки, потрібно детально досліджувати можливі причини.

52 Суспільні новини. Режим доступу: *https://suspilne.media/263657-golova-odniei-z-gromad-harkivsini-zdala-okupantam-personalni-dani-skolariv-sinegubov/?fbclid=IwAR1cPunJ-y4qBnM8b-3N5-139TRiWf4zWmUm_z8RvTDohE1J9aInaKTtU3g*

2. У ХЕРСОНСЬКІЙ ОБЛАСТІ ЗАКЛИКАЛИ ДІТЕЙ РЕЄСТРУВАТИСЯ НА РОСІЙСЬКОМУ САЙТІ НІБИТО ДЛЯ ОТРИМАННЯ ПОДАРУНКІВ

У соціальних мережах дітей закликали реєструватися на сайті, щоб отримати подарунки. Така інформація була розміщена на російському Telegram-каналі @VGA_Kherson, який позиціонував себе як офіційне джерело адміністрації Херсонської області. В оголошенні були зазначені чіткі параметри дитини, яка могла взяти участь у так званій «акції», — вік від 3 до 17 років і реєстрація на території саме цієї області. Потрібно було не тільки залишити на сайті заявку, а ще й додати копії своїх документів.

Водночас, як маніпулятивна тактика, дітям пропонували загадати бажання. Наприклад, іграшки та гаджети, а з нематеріального — зустріч з президентом Росії або «першими особами держави». *«Також, можливо, хтось забажає попрацювати журналістом, спробувати себе в цій новій ролі, хтось захоче поїхати на телебачення або на Байкал (перекладено з російської — ред.)»*, — ідеться в оголошенні.

Правозахисники висувають різні версії, зокрема, що росіянам могла бути потрібна ця інформація для підготовки депортації українських дітей перед імовірним відходом російських військ із захоплених українських територій[53].

(Джерело зображення: Telegram-канал Адміністрація Херсонської області)

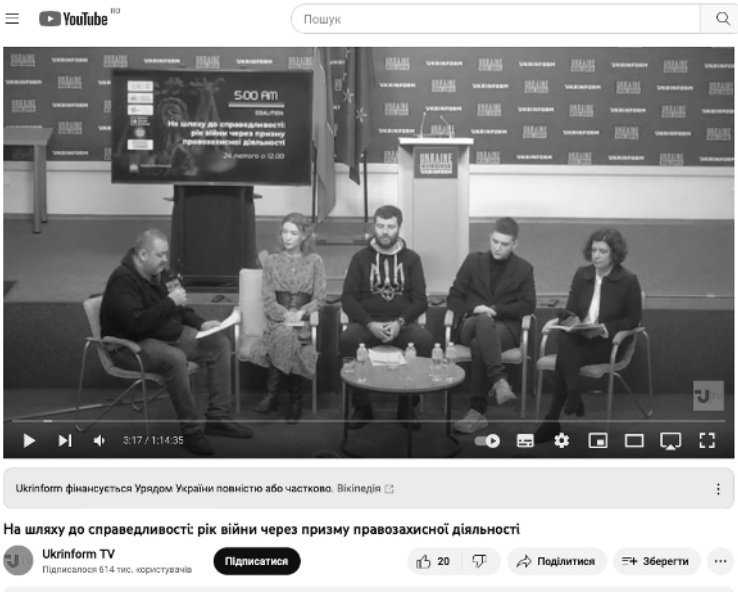
53 ZMINA. Режим доступу: *https://zmina.info/news/okupanty-proponuyut-dityam-hersonshhyny-podarunky-v-obmin-na-personalni-dani-pravozahysnyky-kazhut-pro-ryzyk-novyh-deportaczij/?fbclid=IwAR2YG6hIKOOFxHyUFWM0vgEBFGUpoafoyvmeRhsvzf4h-Bl53O_D5u_dlZU*

3. ЗМІНА ПЕРСОНАЛЬНИХ ДАНИХ ДІТЕЙ, ВИКРАДЕНИХ З УКРАЇНИ

Протягом 2022 року українські правозахисники неодноразово повідомляли про те, що росіяни змінювали особисті дані дітей перед депортацією. Наприклад, на одній з пресконференцій ішлося про таке:

«Росіяни фактично дописували їм вік, потім переміщували на територію Криму. Дитина там утримувалася, не маючи змоги повернутися, оскільки відповідно до їхніх документів вона більше не була дитиною, а її свобода пересування була протиправно обмежена Російською Федерацією», — зазначила правозахисниця Катерина Рашевська.

Уже вдалося ідентифікувати 16 тисяч депортованих дітей. У 2022 році в російські родини було відправлено 400 дітей. Щоб знайти таких дітей, знайти сім'ї, у які їх передали, і репатріювати в Україну, знадобляться значні зусилля, додає правозахисниця[54]. Також вона розповіла про російські «табори перевиховання» — своєрідні «табори русифікації, мілітаризації та індоктринації».



54 Відео з пресконференції українською мовою. Режим доступу: *https://www.youtube.com/watch?v=-c8uqGihYGk*

Ситуацію прокоментувала ще одна українська правозахисниця[55], яка у 2022 році перебувала на окупованих територіях Донецької області. Вона зазначила, що попри те, що війна триває вже багато років, їй по сьогодні складно усвідомити події, які відбуваються на території, де проходило її дитинство.

«Зміна персональних даних українських дітей є лише однією з безлічі жахливих тактик, якими окупанти намагаються затушувати істину та позбутися слідів своїх злочинів. Це не тільки порушення прав дитини, але й спроба витерти з її пам'яті своє коріння, культурну спадщину та історію. Маленькі долі були виштовхнуті в темряву невизначеності. Дітей перекидували з одного місця на інше.

Наполеглива робота правозахисних організацій, урядових структур та міжнародної спільноти повинна бути спрямована на встановлення істини, розслідування воєнних злочинів та покарання винних. Голоси повинні звучати гучно, вимагаючи справедливості. Нехай ця трагедія стане спонуканням для всіх народів світу зрозуміти важливість захисту прав дітей та мирного співіснування без будь-якої форми насильства. Нехай вона стане нагадуванням про те, що ніякі злочини та неправди не зможуть знищити духовну силу та бажання народу України боротися за справедливість і свободу».

55 Особа виявила бажання надати коментар анонімно.

СОЦІАЛЬНІ МЕРЕЖІ ТА МОБІЛЬНИЙ ЗВ'ЯЗОК

(Джерело зображення: freepik / freepik.com)

Серед загроз, які важливо виділити під час війни, — цифрове стеження, яке може здійснюватися за допомогою аналізу метаданих. Такі розробки досить прогресивні в оборонній, правоохоронній і розвідувальній діяльності. Для цього можуть застосовувати різні джерела інформації, зокрема соціальні мережі.

Уперше термін «соціальна мережа» запропонував соціолог Дж. Барнс у 1954 році, який описав його як систему зв'язків між агентами. Коли з'явилися інтерфейси для комунікації людей на онлайн-платформах, вони почали розглядатися як глобальний ресурс, що має великий набір соціально-психологічних функцій. У деяких з них більше користувачів, ніж жителів у більшості країн світу. Є багато платформ, де люди спілкуються онлайн, — від локальних, що притаманні певному регіону, до глобальних, таких як Facebook, Instagram. Сьогодні ведеться багато дискусій щодо наслідків їх використання. Існує думка, що соціальні мережі знають про людей більше, ніж вони самі про себе, бо через алгоритми прогнозування та обробки даних можуть дізнатися практично будь-яку інформацію, яка ґрунтується на аналізі поведінки в інтернеті.

Мікротаргетинг використовують для ідентифікації певного типу людей, щоб потім цілеспрямовано направляти їм потрібну інформацію для формування переконання. Уже існують механізми для визначення, які зображення або повідомлення подобаються певним людям або навпаки викликають негативні емоції. Це означає, що за допомогою технологій можна змусити одну особу або великі групи людей вчинити певні дії. У воєнний час знання про людей, їхні інтереси й потреби, геодані з графіком руху, фінансові операції набувають абсолютно іншого сенсу, ніж у мирний.

Проблема криється не в платформі як такій, а в контенті, розміщеному на ній. Соціальні медіа — це технологія, яка забезпечує «масштабованість» інформації, що може бути виражена через текст, картинку, відео або голос. Спочатку передбачалося, що людина самостійно може контролювати це, але пізніше виявилося, що немає кінцевого розуміння, як можна використовувати цей інструмент, які його переваги та ризики як для окремого індивіда, так і держав загалом. Багато вчених намагається з'ясувати реальний вплив таких технологій на пам'ять і поведінку людини[56]. Наприклад, наука антропологія вже вивчає онлайн-взаємодію, фокусуючись на культурному аналізі.

56 Boyd D. and Ellison, NB 2007 «Social Network Sites: Definition, History, and Scholarship» Journal of Computer Mediated-Communication, 13 (1) 210–2302.

Часто не треба застосовувати спеціальні засоби для отримання інформації, бо люди самі її оприлюднюють. Публікують дані в мережі не тільки про себе, а й про інших осіб: місцеперебування, тексти, фотографії тощо. Фіксують це на своїх мобільних пристроях. У перші місяці повномасштабної війни в Україні в соціальних мережах можна було помітити технології «підбурювання», наприклад повідомлення, що спонукали користувачів більше говорити про себе, розповідати про своє бачення ситуації тощо. Такі маніпуляції змушують людей начебто публічно виправдовуватися, надаючи потрібний контент. Фіксувати це на своїх мобільних пристроях. Найнебезпечніше те, що такими діями в інтернеті постраждалі можуть, самі того не знаючи, спричинити небезпеку заподіяння їм ушкодження у фізичній реальності, окрім усього іншого, стати об'єктом стеження, зіткнутися із загрозою насильства, злочинів на ґрунті ненависті. В епоху інформаційної революції військові операції, які впливають на дані, можуть завдати не меншої шкоди для мирного населення, ніж знищення об'єктів цивільної інфраструктури. Отже, онлайн-платформи, які обробляють великі обсяги даних практично з усіх країн світу, можуть бути інструментом для підготовки, підбурювання, розв'язання та ведення збройних конфліктів. Тому держава, особливо та, яка зазнає агресії, повинна мати спроможність аналізувати сценарії таких загроз і правові інструменти для їх урегулювання та протидії. Це стосується не тільки соціальних мереж, а ще й мобільних телефонів, додатків тощо.

У доповіді Міжнародного комітету Червоного Хреста за підсумками симпозіуму, присвяченого цифровому ризику в умовах збройних конфліктів, було наведено приклад про наслідки від кібератак на мобільні пристрої сирійських біженців[57]. Люди зазнали переслідування, декого вбили. Також було визнано, що *«використання цифрових технологій під час збройних конфліктів у цілях, відмінних від засобів і методів ведення війни»* — унікальна проблема, і наголошено, що робота з інформацією за допомогою технологій і соціальних платформ, де більшою мірою містяться персональні дані, під час збройних конфліктів, може завдавати значної шкоди населенню. Можливо, міжнародна спільнота ще не готова на офіційному рівні визнати та врегулювати цифрову зброю як новий засіб і метод ведення збройних конфліктів, але вже обережно говорить про наслідки та необхідність (пере)інтерпретації конкретного змісту прав на

57 Faine Greenwood, «Data Colonialism, Surveillance Capitalism and Drones», in Doug Specht (ed.), Mapping Crisis: Participation, Datafication and Humanitarianism in the Age of Digital Mapping, University of London Press, London, 2020.

недоторканість приватного життя та захист даних у світлі застосовних норм міжнародного гуманітарного права. В Україні також зафіксовані випадки використання мобільних телефонів, додатків та інших пристроїв для здійснення злочинної діяльності.

1. ЗБІР ПЕРСОНАЛЬНИХ ДАНИХ УКРАЇНЦІВ ЧЕРЕЗ СОЦІАЛЬНІ МЕРЕЖІ

У серпні 2022 року в медіа почала з'являтися інформація, що в локальних чатах у телеграмі в Чернігівській області було помічено розсилку на бот-акаунт, який начебто платить за проходження опитування.

Цей бот мав ім'я користувача — @money_for_polls_bot[58]. Після запуску бота країна-агресор отримувала історії листування в телеграмі, доступ до контактів і місцезнаходження осіб[59]. Оскільки в локальних онлайн-спільнотах місцеві мешканці діляться різними видами даних, це дозволяє отримувати детальну інформацію про те, що відбувається в регіоні. Зокрема, про наслідки воєнних злочинів, особисті дані людей, їхні настрої тощо. Подібні повідомлення були зафіксовані і в інших областях.

У Волинській області поширювали рекламу про грошову допомогу начебто від організації «Червоний

(Джерело зображення: freepik / freepik.com)

58 Було встановлено, що несанкціоновані сеанси відбуваються через додаток MoneyForPolls 1.24.0, пристрій PC 64bit, версія системи 5.10.0, геолокація пристрою — Російська Федерація, м. Москва, IP-адреса 109.172.113.59, хост 109.172.113.59, назва інтернет-провайдера RU-DATAMAX-M-20091118, Російська Федерація.

59 Зверніть увагу: росіяни збирають персональні дані жителів Чернігівщини через Telegram. Режим доступу: *https://cheline.com.ua/news/society/zvernit-uvagu-rosiyani-zbirayut-personalni-dani-zhiteliv-chernigivshhini-cherez-telegram-307168?fbclid=IwAR1T0ZF36Y-wTGRlpzucYSxy7UGTlVMhO6wdgNcT4MLgfETBzfngarYuaqM*

Хрест». Реклама скеровувала на телеграм-канал під назвою «Товариство «Червоного Хреста», який налічував до 200 підписників, хоча офіційний акаунт цієї організації має набагато більше читачів. Також користувачів занепокоїв той факт, що на сторінках указаних українських банків не було інформації про такі виплати. Шахраї маніпулювали часом виплат, зазначаючи, що їх оформлюють у короткий строк, щоб потенційна жертва через поспіх не змогла здогадатися про обман і не мала часу все обдумати. Оскільки для отримання фейкової допомоги потрібно було ввести свої персональні дані (номер рахунку банківської картки), можна зробити висновок, що зловмисники не тільки поширювали неправдиві повідомлення, але й займалися фішингом (вид шахрайства)[60].

2. ЗБІР ІНФОРМАЦІЇ ПРО УКРАЇНСЬКИХ ПОЛОНЕНИХ І ЇХНІХ РІДНИХ ЧЕРЕЗ МОБІЛЬНІ «SMS-АНКЕТИ»

У січні 2023 року Міністерство оборони України в телеграм-каналі повідомило[61], що російські вебресурси розсилають SMS-повідомлення родинам українських захисників з пропозицією заповнити анкету, яка начебто допоможе знайти полоненого на території Росії або на окупованих нею територіях України.

Тоді Координаційний штаб з питань поводження з військовополоненими застеріг, що під виглядом «допомоги» сім'ям, які розшукують зниклих безвісти, спецслужби Росії проводять збір персональних даних, що в підсумку може зашкодити становищу українських захисників у полоні й завадити їх звільненню. Він рекомендував ігнорувати будь-які сторонні неофіційні повідомлення; не надавати жодної особистої інформації про своїх родичів підозрілим особам, вебсайтам, месенджерам. Зокрема, обов'язково повідомляти про випадки незаконного збору персональних даних до органів правопорядку України. Заради безпеки українських військових усі питання необхідно обговорювати лише з Координаційним штабом з питань поводження з військовополоненими — єдиною про-

60 На Волині поширюють фейк про допомогу від «Червоного Хреста». Режим доступу: *https://rayon.in.ua/news/567749-na-volini-poshiryuyut-feyk-pro-dopomogu-vid-chervonogo-khresta?fbclid=IwAR0oSz5RlXzHdrMYVeRcQUiIKq8wRTIBfM6R_6QUDFPgki5dVDKNlIMqWE8*

61 Офіційний телеграм-канал Міністерства оборони України.

фільною державною інституцією, яка займається питаннями допомоги та звільнення з полону.

Це були непоодинокі випадки, подібні повідомлення надсилали масово. Також за допомогою соціальних мереж і повідомлень на мобільні номери телефонів «виманюють» інформацію під виглядом родичів українських військових, зокрема зниклих безвісти. Таким чином збирають контактні дані командирів військових підрозділів, інформацію про їхнє місцезнаходження тощо. Люди часто відгукуються на прохання «родичів і близьких» і, намагаючись їм допомогти, надають інформацію ворожим агентам.

3. ОФОРМЛЕННЯ КРЕДИТІВ НА ЗНИКЛИХ БЕЗВІСТИ ОСІБ І ПОЛОНЕНИХ ВІЙСЬКОВИХ

В Україні були зафіксовані випадки, коли шахраї здійснювали фінансові махінації з банківськими картками, які належать особам, зниклим безвісти, або полоненим українським військовим. Злочинці перевипускали SIM-картки й отримували доступ до онлайн-банкінгу таких осіб. З рахунків українських захисників знімали кошти, а також відкривали кредитні картки, привласнюючи собі суми позики.

(Джерело зображення: freepik / freepik.com)

Як зазначила[62] Олеся Данильченко, заступниця директора Української міжбанківської асоціації платіжної системи ЄМА, якщо людина тривалий час не виходила на зв'язок, то її номер використовували для того, щоб за різними схемами відновити SIM-картку. Важливо звернути увагу на те, що ця злочинна діяльність також передбачає збір персональних даних про людину. Зокрема, про те, що вона військовозобов'язана, знаходиться на службі, потрапила в полон або зникла безвісти, її сім'ю тощо.

62 Як в Україні шахраї оформлюють кредити на військових. Режим доступу: *https://www.obozrevatel.com/ukr/ekonomika-glavnaya/fea/yak-v-ukraini-shahrai-oformlyuyut-krediti-na-vijskovih-sut-shemi.htm?fbclid=IwAR0uzz0WH0vhgkO79wNeMQE4aHM8nSTnjdRYfkzKgCasJPH2vvg-JqYMnJ0*

4. ФЕЙКОВІ ЧАТ-БОТИ УКРАЇНСЬКИХ ДЕРЖАВНИХ СТРУКТУР

У липні 2022 року Центр національного спротиву повідомив[63] про нові елементи гібридної війни з боку Росії. Зокрема, створення фейкових чат-ботів українських державних структур. Приміром, у чат-бота «єВорог», через який можна передавати дані про розташування ворога, зафіксовано багато фейкових двійників. Поки одних блокують, з'являються інші. Відрізнити справжній чат-бот від фейкового майже неможливо.

На перший погляд, вони ідентичні. Ворожі чат-боти не лише блокують роботу основного, а й збирають персональні дані інформаторів. Тому Центр стратегічних комунікацій, Міністерство цифрової трансформації України, Держспецзв'язку та кіберполіція спільно розробили ботчекер, за допомогою якого можна перевірити чат-бот. Якщо він фейковий, ботчекер поінформує про це й дасть посилання на правильний. Якщо в базі немає цього бота, а в користувача залишилися підозри, то про такий випадок необхідно повідомити кіберполіцію. Так, лише впродовж одного місяця понад 35 тисяч людей поскаржилися до поліції на підозрілі канали та чат-боти в телеграмі. Завдяки небайдужості українців вдалося заблокувати загалом понад 300 ворожих профілів.

63 Інформаційний спротив. Як виявляти фейкові чат-боти в Телеграм. Режим доступу: *https://sprotyv.mod.gov.ua/informaczijnyj-sprotyv-yak-vyyavlyaty-fejkovi-chat-boty-v-telegram/*

ВИСНОВКИ

(Джерело зображення: freepik / freepik.com)

Право людини на повагу до її приватного та сімейного життя закріплене в Конституції України. У статті 32 визначено, що не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, окрім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Конституційний Суд України в рішенні[64] від 20 січня 2012 року, даючи офіційне тлумачення статті 32 Конституції України, вважає, що інформація про особисте та сімейне життя особи (персональні дані про неї) — це будь-які відомості чи сукупність відомостей про фізичну особу, за допомогою яких вона може бути ідентифікована.

Є багато різних банків персональних даних, їх умовно можна поділити на закриті та відкриті. До закритих належать державні бази, які збирають уповноважені на це органи влади, або приватні, які формують різні організації, комерційні установи, банки тощо. У разі відсутності належного правового регулювання та системи контролю, це створює ризик несанкціонованого використання даних для різних цілей. Звичайно, неможливо запобігти всім загрозам, але їх можна значно мінімізувати.

У цьому документі зазначені випадки, коли порушення приватності людини призвело до наслідків для її життя та здоров'я. Хоча водночас можуть траплятися й інші ситуації, де люди через порушення захисту персональних даних втрачають власність, стають жертвами кібершахрайства, дискримінації, стигматизації, переслідування та дезінформації. Можливо, ці випадки не стали відомі широкому загалу, бо люди намагаються самостійно впоратися зі своєю проблемою (особисте життя, чутлива інформація, яка може стосуватися близьких і дітей) або вони просто не знають про порушення їхніх прав і свобод. Тому забезпечення безпеки та приватності громадян — ключова місія держави, яка має на меті впроваджувати інноваційні цифрові рішення. Тому потрібно вже сьогодні говорити про конкретні кроки реформи в цій сфері та ставити питання: **що потрібно зробити просто зараз?**

64 Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України. Режим доступу: *http://zakon2.rada.gov.ua/laws/show/v002p710-12*

1. ПРАВОВЕ РЕГУЛЮВАННЯ

У січні 2011 року набрав чинності Закон України «Про захист персональних даних», який регулює правові відносини, пов'язані із захистом та обробкою персональних даних. Цей Закон написано за зразком Директиви ЄС 1995 року, коли користування технологіями ще не було настільки поширеним. Тому в Україні зараз фактично відсутні законодавчі стандарти регуляції захисту даних у мережі, зокрема електронної комерції та цифрової трансформації державних і приватних послуг. Неконтрольовані витоки даних створюють репутаційні ризики для держави щодо її сервісів та інформаційної безпеки людини загалом. Це означає, що щоб захистити суспільство від загроз XXI століття, необхідна комплексна реформа в цій сфері.

Невиконані обов'язки

У вересні 2017 року розпочала діяти Угода про асоціацію між Україною і ЄС, мета якої — відкрити ринки України і Європейського Союзу та налагодити співпрацю між ними. Стаття 15 Угоди вимагає узгодити захист персональних даних в Україні з європейськими та міжнародними стандартами; модернізувати національне законодавство та ратифікувати низку міжнародних актів: Конвенцію 108+ Ради Європи, а також впровадити рекомендації ОЕСР, які по сьогодні ще залишаються без уваги.

Фактично Україна, підписавши цю Угоду, погодилась на те, що потрібно ухвалення нового закону «Про захист персональних даних» та створення нової незалежної інституції, яка буде забезпечувати державний контроль у сфері цифрових прав українців. У 2021 році зроблені певні кроки — зареєстровано два законопроєкти № 5628 і № 6177, передбачені нові вимоги до забезпечення захисту даних та створення окремого наглядового органу. Згадані законопроєкти зазнали критики[65] з боку громадянського суспільства та потребували доопрацювання. Згодом було зареєстровано оновлений законопроєкт № 8153 від 25 жовтня 2022 року, який на момент написання цього матеріалу ще перебував на розгляді у Верховній Раді України.[66] Тобто пройшло вже більше року, проте змін у правовому регулюванні даної проблеми не відбулось, попри практично щоденні по-

65 Аналіз проєкту Закону України «Про захист персональних даних» № 5628. Режим доступу: *https://www.helsinki.org.ua/articles/analiz-proiektu-zakonu-ukrainy-pro-zakhyst-personalnykh-danykh-5628/*

66 Проєкт Закону про захист персональних даних. Режим доступу: *https://itd.rada.gov.ua/billInfo/Bills/Card/40707*

відомлення з боку українських органів правопорядку про масові витоки даних, зокрема з державних баз. Ухвалення нового закону про захист персональних даних, який буде відповідати міжнародним вимогам, — є вкрай необхідним кроком на шляху до того, щоб захисти права людини та національні інтереси в цілому, а також для того, щоб наша держава стала повноцінним членом ЄС.

2. ДЕРЖАВНА СТРАТЕГІЯ

На відміну від багатьох країну світу, в Україні не ухвалено національної стратегії щодо захисту персональних даних. Тобто на державному рівні немає відповіді на питання: які конкретні цілі та завдання забезпечення захисту персональних даних населення? Немає якісних і кількісних даних про поточну ситуацію; загрози; плани подолання викликів, необхідні на це ресурси тощо. Мова йде не про формальний документ, який буде припадати десь пилом, а конкретний фреймворк із чітким планом дій для всіх володільців баз даних, зокрема державних органів влади. Особливо під час воєнного стану.

Такий документ має щонайменше передбачати:

1. Якісний аналіз поточної ситуації

Складно ухвалювати правильні рішення у сфері захисту персональних даних, якщо не знати, у чому саме полягає проблема. Не можна орієнтуватися тільки на суб'єктивні думки, потрібен детальний аналіз, як відбувається загальний процес обробки даних у кожному окремому відомстві чи установі. Потрібна ефективна методологія аналізу та забезпечена незалежна система оцінювання таких результатів. Це дозволить визначити ключові проблеми, напрацювати індивідуальні механізми їх розв'язання, розробити відповідну внутрішню документацію — політики приватності, посадові інструкції, правила тощо.

2. Посилення спроможності системи державного контролю

Сьогодні за законом державний контроль за дотриманням інформаційних прав людини здійснює Офіс Омбудсмана. Вже давно ведуться розмови про те, що в Уповноваженого Верховної Ради України з прав

людини недостатньо повноважень та інституційних ресурсів ефективно виконувати цю функцію. Тому в Україні потрібно створити окремий незалежний орган, який буде реалізовувати державну політику у цій сфері.

Ми не знаємо, коли ці зміни відбудуться, тому варто підсилювати ті повноваження, які є сьогодні. Зокрема розглядати увесь спектр загроз в цифровому середовищі з різних питань та сфер відповідальності. Покращувати співпрацю різних інституцій та громадянського суспільства, наукової та студентської спільноти задля пошуку спільних рішень щодо забезпечення інформаційної безпеки людини та держави в цілому.

3. Правове регулювання нових технологічних рішень

За останній рік Україна зробила великий крок у напрямі цифрової трансформації. Багато державних послуг було диджиталізовано. Проте коли чиновники розповідають про новий додаток або цифрову екосистему, у юристів виникає питання: чим це врегульовано? Як у разі порушень будемо захищати права та законні інтереси людини?

Будь-яке технологічне рішення повинно впроваджуватися з пакетом відповідного законодавства. Хороший приклад Німеччини, яка формує свою систему права у світі технологій, застосовуючи практику регуляторних пісочниць. Вони поступово розв'язують питання в конкретних галузях, а не намагаються охопити все й одразу. Коли у них виникла необхідність урегулювати питання щодо використання автоматизованих машин, зокрема відповідальності в разі завдання збитків, там ухвалили поправки до Закону про дорожній рух. Щоб зрозуміти, де ми «відстали» з погляду правового регулювання, потрібно провести відповідний аналіз технологічного прогресу та ризиків, які у зв'язку із цим з'явилися.

4. Підвищення довіри суспільства до державних інститутів

Процес диджиталізації часто викликає спротив з боку суспільства, бо передусім люди не розуміють, яким чином будуть використовуватися їхні персональні дані. Тому, окрім належного правого регулювання, ще повинна бути сформована правильна стратегічна комунікація. Треба чесно говорити не тільки про переваги від технологій, а й ризики. Створити можливість спільного пошуку рішень у кризових ситуаціях. Загалом люди не проти розкривати інформацію про себе, але натомість хочуть отримати належні гарантії безпеки. Результати масштабного досліджен-

ня CES 2020 в США, Китаї та Франції показали, що захист персональних даних стає новим критерієм довіри, який буде турбувати людей нарівні з якістю наданих послуг.

Не треба й забувати про те, що цифрова трансформація відбувається не тільки в соціальній сфері, а й правоохоронній. Очевидно, що війна в Україні підштовхнула до розвитку нових технологічних рішень щодо контролю за населенням. Надалі ще більше будуть розвиватися міські системи відеоспостереження, програми ідентифікації осіб за допомогою штучного інтелекту та біометричної інформації, багато інших напрямів, які стосуються оборони, публічної та національної безпеки. Усі ці технології працюють на основі даних. Якщо не буде сформована правильна політика, то в майбутньому можуть виникнути протести. Технології повинні розвиватися, але з урахуванням усіх загроз і правого поля.

5. Просвітницька діяльність для населення та професійна підготовка

Одна з найпоширеніших причин, чому не виконується Закон про захист даних, — тому що в ньому складно розібратися. Незнання не позбавляє відповідальності, але потрібно визнати, що законодавство в цій сфері потребує детального роз'яснення, усвідомлення та адаптації. У країнах ЄС докладають багато зусиль, щоб населення, державні служби, муніципалітети, бізнес розуміли норми закону, що регулюють обробку даних, кібербезпеку та електронну комунікацію, знали практичні аспекти впровадження та ризики, пов'язані з невиконанням.

Ключове значення має професійна підготовка та відповідальність, особливо в системі державного управління. Існує помилкове уявлення, що вразливе місце — це технічний захист систем проти кібератак, але, як уже показали приклади, зокрема зазначені в цьому документі, проблема не стільки в програмах, скільки в людях. Відсутність контролю, бездіяльність, можливо, навіть якоюсь мірою байдужість, породжують соціальну інженерію. Немає сенсу витрачати великі ресурси на розроблення вірусної програми, якщо ті, хто має доступ до даних, можуть самі передавати, продавати чи поширювати потрібну інформацію.

Створення в суспільстві культури поваги до приватного та сімейного життя має бути стратегічною ціллю державної політики.

Стратегія — це орієнтир та амбіції України, як забезпечити безпечне майбутнє. Показати всьому світу свої цінності в цифровому світі та «розкрити значення персональних даних у діяльності уряду та загалом в економіці країни», а також сформувати довіру людей до інноваційних впроваджень.

3. ВИКОНАННЯ СВОЇХ ОБОВ'ЯЗКІВ ТИМИ, ХТО НЕСЕ ВІДПОВІДАЛЬНІСТЬ ЗА ЗАХИСТ ДАНИХ

Органи державної влади, приватні компанії та інші суб'єкти самостійно визначають процедури обробки персональних даних і заходи безпеки. Більшість порушень закону в цій сфері пов'язана з тим, що всі ці процеси не організовані відповідно до закону або не мають внутрішнього контролю.

Наприклад, вони можуть збирати надлишковий обсяг персональних даних; здійснювати їх обробку в цілях, несумісних з тими, для яких були зібрані спочатку; відсутні необхідні документи, які мають регулювати процедури обробки даних; не призначена відповідальна особа там, де обов'язково це потрібно зробити згідно із законом. Для забезпечення належного рівня захисту даних необхідно ухвалити низку заходів, які спочатку призведуть до поліпшення загальної ситуації, а в довгостроковій перспективі сприятимуть становленню суспільства, де право на повагу до приватного життя буде гарантовано.

Як уже було зазначено раніше, немає уніфікованого підходу, як організувати роботу з даними, бо кожна установа чи організація має свою специфіку діяльності. Але існують базові вимоги та процедури, передбачені законом і міжнародними стандартами, які необхідно зробити для захисту інформації. До основних організаційних заходів можна віднести такі:

— проведення загального аналізу діяльності (окремо кожного суб'єкта, що обробляє дані): проведення аудиту для визначення, які персональні дані збирає, обробляє та зберігає організація, а також ідентифікація можливих ризиків і слабких місць;[67]

67 Роз'яснення щодо того, як можна оцінювати ризики та які є міжнародні стандарти. Режим доступу: *https://decentralization.gov.ua/uploads/library/file/774/Posibnyk_ocinka-ryzykiv-ZPD.pdf*

- усвідомлення обов'язків: розуміння вимог відповідно до закону, включаючи принципи законності, справедливості та прозорості в зборі та обробці даних;
- мінімізація обробки даних: забезпечення того, щоб обробка даних була обмежена лише необхідною інформацією для виконання визначених цілей;
- розробка внутрішньої документації;
- упорядкування процедур передачі персональних даних, зокрема транскордонної;
- призначення та професійна підготовка відповідальної особи;
- встановлення механізмів для забезпечення прав суб'єктів даних, таких як доступ до даних, виправлення помилок, видалення даних і перенесення даних;
- впровадження правил внутрішнього контролю за обробкою персональних даних. Зокрема, впровадження моніторингу та виявлення порушень.

Кожна людина повинна мати чітке розуміння, як обробляються та захищаються її дані, зокрема бути впевненою в належній системі інформаційної безпеки.

4. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ДІТЕЙ

Міжнародні та національні положення встановлюють право дітей на недоторканість особистого життя. Згідно з Конвенцією про права дитини та іншими важливими документами, ніхто не може допускати порушення цих прав безпідставно та незаконно.[68] Особисте життя дитини охоплює їх фізичну недоторканість, особисту ідентичність, конфіденційність інформації, а також фізичну та просторову приватність.

Поняття «самовизначення» вказує на здатність особи вирішувати, які аспекти її особистого життя розголошувати та якою мірою. «Самостійність» означає здатність до саморегуляції в думках, почуттях і діях[69].

68 Комітет з прав дитини, зауваження загального порядку № 16 (2013), п. 12.

69 Abstract of the German Federal Constitutional Court's judgment of 15 December 1983, 1 BvR 209.

Конвенція ООН про права дитини визнає, що батьки повинні забезпечити виконання прав дітей, враховуючи їхні здібності й найкращі інтереси[70]. Раніше традиційно вважалося, що дорослі визначають, як дітям розпоряджатися своїм особистим життям. Проте потреби дітей в особистому житті можуть відрізнятися від потреб дорослих і водночас конфліктувати з ними.[71] Наприклад, практика «шерентингу» (розміщення батьками інформації про дитину в соціальних мережах) може суперечити праву дитини на недоторканість, тоді як право батьків на вираження думок конфліктує із цим правом. Визначення потреб дітей в особистому житті дорослими може обмежувати їхню самостійність і незалежність, а також зменшувати недоторканість їхнього приватного життя. Водночас діти все частіше стають об'єктами технологічного спостереження з боку різних суб'єктів, таких як уряди, приватні компанії та однолітки[72].

Дослідження показали, що, з одного боку, батьки турбуються про недоторканість і безпеку своїх дітей у цифровому просторі. З іншого — багато хто не контролює електронні пристрої своїх дітей або дозволяє користуватися цифровими сервісами без обмежень[73]. Зростаючи, діти вимагають більшої поваги до свого особистого життя від батьків, шкіл та інших суб'єктів. Вони розглядають особистий простір як важливий для творчого самовираження та розвитку незалежної думки. Важливо, щоб батьківський контроль був збалансованим і враховував потреби та думки дитини, зокрема її здатність до незалежного розвитку.

Сучасне покоління дітей — перше, народжене в епоху цифрових технологій. Ще до народження, в утробі, ідентичність дитини починає формуватися завдяки зображенням, які батьки розміщують в інтернеті. Ці зображення часто містять особисту інформацію. Наразі близько 80 % дітей у розвинених західних країнах залишають цифровий слід ще до досягнення дворічного віку[74]. Сучасних дітей усе більше залучають до онлайн-активностей в ранньому віці порівняно з минулим. З кожним роком кількість дітей, які спілкуються онлайн, збільшується. Багато дітей до

70 Tobin and Field, «Article 16».

71 Submissions from Parental Rights Foundation; Action Canada for Sexual Health and Rights, p. 4; Commission Nationale de l'Informatique et des Libertés (CNIL), p. 11.

72 Jane Bailey and Valerie Steeves, Defamation Law in the Age of the Internet: young people's perspectives (Law Commission of Ontario, Canada, 2017); submission from Ariel Foundation International.

73 Monica Anderson «A majority of teens have experienced some form of cyberbullying», Pew Research Center, 27 September 2018.

74 Submission from Hungarian National Authority for Data Protection and Freedom of Information, p. 42.

13 років має профіль у соціальних мережах (38 % дітей віком від 9 до 12 років, за європейськими дослідженнями), більшість з них — від двох до п'яти профілів[75]. Пандемія коронавірусної хвороби (COVID-19) посилила цю тенденцію.

Значно частіше самооцінка та самоповага, важливі для формування особистості та ідентичності, розвиваються в цифровому просторі під впливом цінностей і тенденцій, продиктованих там. Діти використовують інтернет для безперервного документування свого життя. Коли дитина здатна увімкнути смартфон раніше, ніж звикнути до азбуки, захист її особистих даних стає дуже важливим питанням, оскільки через свій вік вона ще не може оцінити можливі ризики. Нерідко діти діляться своїми персональними даними в соціальних мережах, ігрових чатах, форумах тощо.

У віртуальному світі персональні дані перетворилися в цифровий продукт, який може використовуватися по-різному:

- у маркетингових цілях, щоб формувати рекламу та продавати товари чи послуги;
- для спаму, підбору паролів, зламу облікових записів тощо;
- з метою шахрайства або шантажу, коли через дитину отримують фінансові дані батьків;
- для стеження, адже, знаючи де зазвичай перебуває дитина, злочинці можуть викрасти її або завдати шкоди;
- для психологічного впливу (цькування, кібербулінгу[76]), щоб спонукати дитину до певних дій;
- для вербування в різні структури, які мають на меті зашкодити життю та здоров'ю дитини (групи смерті, стримери та ін.).

В умовах війни кількість загроз для дітей значно збільшилася. У воєнних конфліктах діти можуть бути особливо вразливими. Зловмисники можуть використовувати їхні дані для поширення пропаганди та вербування, викрадення, політичної маніпуляції та навіть зміни їхньої національної ідентичності. Більшість порушень свідчать, що проблеми відбувалися через декілька причин:

75 Submission from Information and Data Protection Commissioner, Albania, p. 14.

76 Кібербулінг — погрози, образи та інші прояви агресії в інтернеті. Найчастіше це пов'язано з розкриванням інтимних фото чи інших подробиць у мережі. У результаті дитина опиняється в глибокій депресії, яка може призвести до незворотних наслідків.

- володільці баз персональних даних не забезпечили всі необхідні процедури для їх захисту відповідно до національного законодавства і міжнародних стандартів;
- слабка система цифрової грамотності населення.

В Україні необхідний комплексний підхід до захисту персональних даних дітей як на державному, так і місцевому рівні. Розпочати цей процес варто з якісного оцінювання ризиків. Тобто дослідити весь спектр потенційних загроз для дитини у зв'язку з неправомірним використанням її персональних даних в органах державної влади, бізнесі, приватними особами та навіть батьками. Якби діяльність усіх суб'єктів, які здійснюють обробку даних дітей, систематично аналізувалася, то сьогодні ми мали б відповідь на питання: яким чином голова однієї з громад Харківщини передала окупантам усі дані українських школярів? Яка система захисту баз даних та контролю там була?

Окрім державних органів, місцевого самоврядування, навчальних закладів тощо, великі масиви персональних даних обробляє бізнес. В одних випадках це робиться приховано, й отримані дані використовуються, наприклад, у маркетингових цілях, в інших їх прямо збирають для надання послуг дитині. Серед поширених сервісів, які можуть використовувати діти:

- освітні послуги (курси, творчі майстер-класи тощо);
- спортивні послуги (у тому числі обробка персональних даних при видачі абонементів та веденні відеоспостереження в залах);
- соціальні мережі;
- інтернет-магазини, поштові служби;
- онлайн-ігри, клуби та об'єднання за інтересами, розважальні платформи;
- послуги в галузі охорони здоров'я або соціальної підтримки тощо.

Тобто це великі масиви даних, обробку яких потрібно контролювати. Якщо подивитися на міжнародну практику, то досить жорсткі вимоги до обробки даних дітей встановлені в країнах ЄС, де діє Загальний регламент захисту даних (GDPR)[77]. У цьому документі визначено, що діти по-

77 Цей регламент Європейського Союзу містить положення про захист персональних даних, включаючи дітей. Він встановлює вимоги до збору, обробки та зберігання персональних даних дітей, включаючи вимогу отримувати згоду від батьків або опікуна дитини.

требують особливого захисту в питанні персональних даних, зокрема коли вони застосовуються для цілей маркетингу або створення профілю особи. У ЄС передбачені гарантії безпеки дитини в мережі та існує вимога отримання згоди батьків, якщо дитині надається послуга в режимі онлайн. Тому всім, хто обробляє в інтернеті дані дитини з ЄС, доводиться вигадувати, у який спосіб погоджувати це з батьками. Інакше загрожують санкції: штраф розміром до 4 % річного обігу (або до 20 мільйонів євро).

Наприклад, ірландський контролюючий орган (DPC) представив документ під назвою «Діти в центрі уваги: основні положення щодо обробки персональних даних дітей»[78]. Це результат більш ніж трьох років роботи, під час якої було проаналізовано ситуацію в цій сфері та думки багатьох зацікавлених сторін і самих дітей. У цьому документі викладені принципи захисту приватності та способи їх реалізації.

У США діє федеральний закон «Про захист конфіденційності дітей в Інтернеті», який зобов'язує встановлювати заходи для захисту дітей у мережі, які не досягли 13 років. Будь-яка інформація про дитину може оброблятися також тільки за згодою її законних представників. У низці штатів діють локальні закони, які встановлюють відповідальність за кіберпереслідування та знущання в соціальних мережах.

Влада Франції планує зобов'язати соціальні мережі перевіряти вік користувачів і вимагати дозвіл батьків у тих, кому ще не виповнилося 15 років. Якщо Єврокомісія схвалить цей документ, тоді компаніям дадуть два роки, щоб запровадити процедури перевірки користувачів під час реєстрації на їхніх вебресурсах. Закон дозволить батькам вимагати призупинення облікових записів своїх дітей віком до 15 років, а також вимагати від сайтів інструменти для обмеження часу перебування на конкретній платформі. У документі наголошено, що ці законодавчі зусилля є тільки частиною низки інших кроків уряду, спрямованих на захист дітей від кіберзалякування та інших злочинів[79].

Тобто заходи безпеки та захисту особистих даних дитини не можуть обмежуватися лише одним загальним законом. Цьому питанню треба

78 Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing. Режим доступу: *https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf*

79 France approves law requiring parental consent for minors on social media. Режим доступу: *https://www.france24.com/en/france/20230629-france-approves-law-requiring-parental-consent-for-minors-on-social-media*

приділити окрему увагу, у тому числі на законодавчому рівні. Наприклад, школи відіграють значну роль у повсякденному досвіді дітей з погляду недоторканості їхнього приватного життя. Пандемія COVID-19, а згодом повномасштабна війна в Україні змусили закрити деякі школи та перейти на онлайн-режим. Перехід до онлайн-освіти посилив наявний дисбаланс сил між компаніями, які надають доступ до онлайн-сервісів, і дітьми, а також між урядами та дітьми й батьками, при цьому кілька урядів відійшли від дотримання чинних законів про конфіденційність даних про дітей. Це означає, що недержавні суб'єкти регулярно контролюють цифрові записи дітей. Оцифрування та зберігання даних про навчання дітей охоплює характеристики мислення, траєкторію навчання, ступінь залучення, швидкість реакції, прочитані сторінки та переглянуті відеоматеріали. Більшість дітей і батьків не мають можливості оскаржувати правила конфіденційності компаній, які займаються освітніми технологіями, або відмовитися від надання даних, оскільки освіта обов'язкова. При виборі школами навчальних додатків і вебінструментів основна увага приділяється навчальній програмі та вартості, а не конфіденційності. У вересні 2020 року за результатами аналізу 496 додатків у галузі освітніх технологій у 22 країнах було встановлено, що багато з них збирають ідентифікатори пристроїв, багато прикладних програм збирають дані про місцезнаходження та обмінюються даними про користувачів з третіми сторонами. Безпека даних викликає занепокоєння. Наприклад, компанія «Microsoft» повідомила про 5,7 млн інцидентів зі шкідливим програмним забезпеченням, які торкнулися її користувачів з 24 серпня по 24 вересня 2020 року[80]. Самі школи зберігають значний обсяг інформації про дітей і все частіше відстежують їх, спостерігаючи за діяльністю учнів онлайн і за допомогою камер відеоспостереження. Використання всіх технологій вимагає підзвітності, осмисленої згоди, обмеження цілей, мінімізації даних, прозорості та гарантій безпеки. Освітні процеси не мають потреби й не повинні підривати здійснення права на недоторканість приватного життя та інших прав незалежно від того, де і як ведеться освітній процес, а також посилювати наявну цифрову нерівність[81].

Також велике має значення просвітництво серед населення. Часто ризики, пов'язані з інформацією про дитину, можуть з'являтися через

80 Submission from Human Rights Watch, para. 49.

81 Резолюція 75/166 Генеральної Асамблеї; Submissions from ombudsman of Autonomous City of Buenos Aires; ECLAC; Council of Europe.

незнання законодавства, недостатню поінформованість про потенційні проблеми та дії, які потрібно вчинити, щоб запобігти негативним наслідкам. Якщо дорослі люди будуть добре знати про свої права, обов'язки та можливі загрози, тоді це буде запорукою того, що цифрова грамотність стане частиною виховання дитини. Це може допомогти запобігти проблемам, пов'язаним із цифровою залежністю, психологічними розладами через цькування в соціальних мережах або кіберзлочинами.

Батькам варто разом з дітьми знайомитися з новими технологіями або програмами, обговорювати їхні переваги та ризики. Стежити за контентом, щоб бути в курсі, чим цікавляться їхні діти. «Стати друзями» в соціальних мережах, щоб розуміти основну аудиторію та як складаються з нею стосунки (наприклад, чи є негативні коментарі, які реакції переважають, підписки тощо). Розповісти, що фотографії або інший опублікований контент залишаються в інтернеті назавжди. Якщо публікація певної світлини сьогодні буде здаватися дуже веселою, то чи буде це так виглядати, скажімо, через десять років. Пояснити, що недопустимо передавати свої або батьківські особисті дані в обмін на подарунки, як це робили росіяни в Херсонській та інших областях. Надзвичайно важливо спільно визначити межі особистої приватності та обговорити, публікація яких даних може мати наслідки не тільки для самої дитини, а й усієї сім'ї.

Суть цифрових прав у тому, що людина повинна сприймати персональні дані як свою власність і не боятися ставити питання стороннім особам, чому вони їх збирають і що з ними буде далі. Цього вже треба вчити змалечку. Наприклад, коли батьки бачать, що без дозволу фотографують або публікують якусь інформацію про їхню дитину, вони мають право заперечити проти цього. Якщо такі ситуації виникають у школі, дитячому садочку, варто попереджати вихователів і вчителів про свою позицію заздалегідь. Також можна запропонувати керівництву закладу розробити внутрішні правила обробки даних дітей. Після чого ознайомити з ними інших батьків.

Якщо дитина вже може самостійно поширювати інформацію про себе, то треба попередити, що не варто повідомляти стороннім людям або залишати на різних сайтах свої персональні дані *(наприклад, паролі, місце проживання, банківські реквізити тощо).* Поведінку в мережі аналізують і потім можуть використати в тому числі і в злочинних цілях. Що більше людей будуть категорично ставитися до будь-яких проявів порушення у

сфері приватності, незалежно від того, чи неправомірні дії вчинили органи державної влади, бізнес чи приватна особа, тоді є шанс, що загальна картина зміниться.

Повага до приватного життя дітей — найважливіший засіб забезпечення їхніх інтересів. Підхід, орієнтований на забезпечення інтересів, вимагає, щоб дорослі активно з'ясовували думки дітей і ставилися до них максимально серйозно. Усі сторони — уряд, компанії, громади, приватні особи та батьки — повинні визнавати дітей як носів своїх прав. Однак лише цифрової грамотності недостатньо без рішучих і послідовних дій держави щодо забезпечення недоторканості приватного життя, захисту даних і безпеки дитини.

NED
NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

Асоціація УМДПЛ UMDPL Association

Freerights ASSOCIATION