AMERICANBARASSOCIATION

Лабораторія Цифрової Безпеки

Наскільки «прозора» законність діяльності Clearview AI в Україні?

Анна Людва
Тетяна Авдєєва

2023

Зміст

В епоху постійної цифровізації масове стеження стало популярним інструментом органів влади для підтримки громадського порядку серед населення. Одним з найбільш часто використовуваних інструментів спостереження є технологія розпізнавання облич (далі – FRT) – біометрична система, яка використовує автоматизовані методи для перевірки або ідентифікації людини. У зв›язку з цим Україна є однією з держав, які часто вдаються до методів FRT. Її потреба в біометричних технологіях стала ще більш очевидною після повномасштабного вторгнення Росії в Україну. У відповідь на ситуацію, що виникла, держава звернулася до використання технології Clearview AI. Початково розроблена для правоохоронних цілей, технологія Clearview зіставляє зображення з базою даних загальнодоступних зображень, зібраних з веб-сайтів, включаючи платформи соціальних мереж. При цьому, незважаючи на відсутність уніфікованих законодавчих норм щодо використання системи, Україна, як і раніше, вдається до цифрових заходів без правової бази та гарантій для суб'єктів даних. Беручи до уваги тривалий період дії воєнного стану, довільне використання технологій FRT органами влади може негативно вплинути на недоторканність приватного життя громадян, якщо FRT продовжить застосовуватися навіть після припинення дії надзвичайного стану. Таким чином, необхідно провести комплексну правову оцінку з точки зору прав людини і знайти належний баланс між правом українців на недоторканність приватного життя і національними інтересами держави, в той час як FRT застосовуються під час надзвичайного стану.

I. Хто може захистити права людини під час надзвичайного стану?

Важливо дотримуватися прав та обов›язків людини навіть у виняткових обставинах, включаючи війну чи інші надзвичайні ситуації. У зв›язку з цим стаття 15 ЄКПЛ дозволяє державі відступати від своїх зобов›язань за Конвенцією, тим самим вводячи додаткові обмеження на охоронювані права там, де це необхідно. Тут влада може призупинити звичайні процедури і отримати більше повноважень. Проте, навіть при наявності більш широких дискреційних повноважень, свобода розсуду держав не може бути необмеженою і повинна залишатися в рамках «необхідності та пропорційності». У зв›язку з цим ЄСПЛ встановлює загальні вимоги для того, щоб відступ вважався «дійсним», а саме:

- наявність війни чи іншого надзвичайного стану, що загрожує життю нації;
- відсутність обмежень щодо прав, які не допускають відступів (стаття 2, за винятком випадків смерті внаслідок законних військових дій, або статті 3, 4 (1) та 7 ЄКПЛ);

- абсолютна необхідність відступу в силу гостроти ситуації;
- повідомлення Генерального секретаря Ради Європи про відступ.

Водночас практика Європейського суду з прав людини (далі – ЄСПЛ) демонструє, що індивідуальна оцінка залишається необхідною для кожного випадку відступу, щоб уникнути потенційних зловживань і довільного втручання в права людини. Причина в тому, що досі незрозуміло, наскільки далеко можуть поширюватися дискреційні повноваження влади, навіть якщо відступ дозволяє призупинити певні права та звичайні процедури. Тут Суд наголошує, що навіть за часів надзвичайного стану права людини не перестають існувати: отже, відповідні зобов›язання залишаються покладеними на державу. Наприклад, у справі Лоулесс проти Ірландії (№3), стосовно введення спеціальних повноважень щодо утримання під вартою, ЄСПЛ виправдав наявність таких повноважень, оскільки останні використовувалися для конкретної надзвичайної мети, і на них поширювався ряд правових гарантій від зловживань (пункт 38). Аналогічним чином, у справі Бранніган *і* Макбрайд проти Великобританії Суд підтвердив, що національна влада не вийшла за межі своєї свободи розсуду завдяки існуючим правовим гарантіям, таким як право консультуватися з адвокатом, а також можливість оскаржити рішення в судовому порядку (пункти 64, 61).

Повертаючись до поточної проблеми з використанням технологій FRT, існує побоювання, що під час надзвичайної ситуації влада може використовувати ще більш інтрузивні цифрові технології, мотивуючи це необхідністю захисту національних інтересів. Відступ повинен бути особливо обережним щодо неабсолютних прав, таких як право на приватність: оскільки положення про обмеження відповідно до статті 8(2) ЄКПЛ вже передбачає виправдане втручання влади, відступ йде ще далі і дозволяє державі ширшу свободу дій. Однак тут Суд Європейського Союзу віддзеркалює практику ЄСПЛ щодо пропорційності та підкреслює, що відступи щодо персональних даних «повинні застосовуватися тільки в тій мірі, в якій це абсолютно необхідно». Нарешті, говорячи про воєнний контекст, навіть якщо певні обмеження і будуть встановлені, необхідно гарантувати, що такі надмірні обмеження будуть зняті як тільки умови надзвичайного стану перестануть діяти.

Україна та технології розпізнавання облич

Україна бере активну участь у розвитку сучасних технологій. Як і багато інших держав, Україна також вдається до заходів спостереження, серед яких FRT – як у цивільних, так і у військових цілях. Її політика в значній мірі спирається на цифровізацію, що вбачається з мобільного додатку «Дія», створеного як база даних електронних документів, або програми «Safe. City», винайденій як інноваційний спосіб забезпечення місцевої безпеки.

Однак використання цифрових технологій в Україні тільки зросло після повномасштабного російського вторгнення. Таким чином, в наступних підрозділах буде проаналізовано, чи надає українське законодавство достатні гарантії суб'єктам даних, які активно взаємодіють з FRT.

II. Законодавча та політична база для технологій FRT в Україні

В принципі, Україна не має єдиної правової бази, пов›язаної з заходами масового стеження. Конкретні положення, що стосуються цифрових технологій, можна знайти в окремих законодавчих положеннях або підзаконних актах. Таким чином, незважаючи на відсутність регулювання, деякі закони можуть бути проаналізовані.

Закони про захист даних. Хоча Україна вважається «цифровою державою», як не дивно, її законодавство про приватність та захист даних залишається вкрай застарілим. Діючий Закон України «Про захист персональних даних» (далі – Закон) був введений в дію у 2010 році. Після вступу в силу Загального регламенту захисту даних ЄС (далі – GDPR) у Закон неодноразово вносилися поправки, однак він все ще не регулює специфіку механізму захисту даних. Ба більше, чинний Закон нездатний іти в ногу з усіма передовими цифровими технологіями, що спростовує твердження про те, що правові норми повинні бути актуальними. Зокрема, Закон не адресує питань недотримання термінів обробки даних, механізму правового захисту, несанкціонованого збору даних тощо. Важливо відзначити, що наразі не створено контролюючого органу для здійснення ефективного нагляду за використанням новітніх технологій у сфері приватності. Незважаючи на те, що в українському парламенті було запропоновано кілька нових законопроєктів (таких як № 5628 або № 8153), мало що було досягнуто з точки зору їх розгляду та імплементації.

Стосовно вмісту та захисту приватного життя, то Закон сформульований в основному в загальних і нечітких термінах. В цілому Закон окреслює вичерпний перелік підстав для збору даних та надає суб›єктам даних суттєві права на захист від будь-якої незаконної поведінки або довільного збору даних. Крім того, Закон зобов›язує органи влади обробляти дані лише в конкретних і легітимних цілях, надаючи особі ряд прав, включаючи доступ до інформації, а також право на видалення даних. Слідуючи GDPR, Закон забороняє обробку біометричних даних, оскільки останні становлять особливу категорію даних. Водночас Закон виокремлює винятки, коли така обробка вважається законною, серед яких надання попередньої згоди та явне оприлюднення особою персональних даних. Останній випадок надає

органам влади свободу дій для збору інформації, включаючи використання технології Clearview AI (яка збирає загальнодоступні фотографії з соціальних мереж). У зв›язку з цим ніякого дозволу від суб›єкта даних не потрібно, оскільки Закон де-факто дозволяє збір даних із публічних ресурсів. Що стосується контролюючих повноважень, то Закон України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» уповноважив Омбудсмена України здійснювати контроль за дотриманням законодавства про захист персональних даних. Однак такі наглядові повноваження не можуть вважатися достатніми для забезпечення дотримання положень у разі вчинення порушення, оскільки в Законі відсутній належний санкційний механізм.

Стосовно останніх ініціатив, то Законопроєкт № 8153 «Про захист персональних даних» спрямований на гармонізацію законодавства зі стандартами ЄС та заповнення існуючих законодавчих прогалин. Законопроєкт значно деталізує існуючі процедури, посилюючи механізми захисту у разі обробки біометричних даних та автоматичного процесу прийняття рішень. Однак навіть запропонована редакція закону не містить будь-яких положень, що стосуються заходів спостереження. Зокрема, на відміну від Пропозиції ЄС щодо Закону про штучний інтелект, яка розмежовує три різні системи, Законопроєкт не розрізняє звичайне спостереження та технології FRT, які є більш інтрузивними. Оскільки Законопроєкт не передбачає жодних обмежень, він фактично дає владі «зелене світло» на використання будь-якого виду FRT без запобіжних заходів. На жаль, зазначений законопроєкт навряд чи буде прийнятий найближчим часом, враховуючи мовчання парламенту протягом півроку з моменту його реєстрації.

Закони про правозастосування. Закон України «Про Національну поліцію» є ще одним законом, який варто згадати в контексті стеження. Стаття 40 Закону дозволяє поліції використовувати «фото - і відеотехніку, у тому числі техніку, *що працює в автоматичному режимі*», а також «спеціалізоване програмне забезпечення для здійснення аналітичної обробки фото - та відеоінформації». У цьому випадку на правоохоронні органи не накладається жодних обмежень, окрім зобов›язання використовувати спостереження для чітко визначеної мети. У березні 2022 року українські законодавці внесли поправки до вищезазначеного Закону, уповноваживши поліцію керувати реєстром та базами даних, які містять дані про підозрюваних злочинців, обвинувачуваних, підсудних, осіб, які переховуються від правосуддя, тощо. Примітно, що така база даних також містить біометричні дані осіб (включаючи цифрове зображення обличчя людини), які поліція зобов›язана збирати у осіб. У зв›язку з внесеними поправками слід підкреслити два важливих моменти.

- По-перше, згідно з новими поправками, період зберігання біометричних даних та інших матеріалів відеоспостереження встановлюється Міністерством внутрішніх справ України. Цей орган уповноважений видавати виключно внутрішні накази, які зазвичай не мають обов›язкової юридичної сили. Це, в свою чергу, може призвести до потенційного зловживання з боку правоохоронних органів біометричними даними, які можуть зберігатися протягом невизначеного періоду часу.
- По-друге, поправки були запроваджені під час воєнного стану, коли допускається більш широка свобода дій. Однак закон не надає жодних вказівок щодо того, чи обмежується він періодом воєнного стану, припускаючи, що закон може застосовуватися і в мирний час, якщо до нього знову не буде внесено поправок. У зв'язку з цим існує небезпека, що поліція буде наділена надмірними повноваженнями навіть після припинення дії воєнного стану.

Кримінальні процесуальні закони. В Кримінальному процесуальному кодексі наявні положення про доступ слідчого або прокурора до інформаційно-комунікаційних систем. У цьому випадку останні уповноважені збирати інформацію з технічних пристроїв, таких як пристрої для фото - або відеозапису, що функціонують у загальнодоступних місцях, у тому числі в автоматичному режимі, за винятком приватних будинків. Зазначене положення надає особливо широку дискрецію правоохоронним органам з огляду на такі причини:

- Збір інформації здійснюється на підставі постанови слідчого або прокурора та не вимагає попереднього судового наказу. Оскільки ті самі люди і схвалюють, і виконують функції, а зовнішнього наглядового органу не існує, така практика не лише надає надмірну свободу дій, а й піднімає питання потенційного упередження у процесі прийняття рішень.
- У цьому положенні не обумовлюється вид інформації, яка може бути отримана, що надає правоохоронним органам практично необмежені повноваження в зборі будь-яких видів персональних даних.

III. Україна виводить штучний інтелект на поле бою

Що стосується практичного застосування методів FRT, у березні 2022 року український уряд оголосив про свою співпрацю з американською компанією Clearview AI. Ця система ідентифікує людей за допомогою зображень, які раніше були зібрані онлайн з платформ соціальних мереж (таких як Google,

Facebook, Twitter, Вконтакте і т.д.). Іншими словами, для ідентифікації особи, його/її фотографію потрібно завантажити в базу даних, і алгоритм встановить відповідність. Біометрична база даних компанії налічує близько 10 мільярдів зображень у своїй власності, і компанія часто продає ці дані органам влади, переважно поліції та агентствам. В Україні технологія Clearview AI використовується для ідентифікації потенційних російських солдатів та диверсантів на контрольно-пропускних пунктах, росіян, підозрюваних у скоєнні військових злочинів (для збору доказів міжнародних злочинів), ідентифікації загиблих солдатів та повідомлення їх сімей (для боротьби з міфом про те, що російське вторгнення – це «спеціальна операція»). Проте наразі Clearview AI в основному ідентифікує загиблих російських солдатів (щоб повідомити про це їх сім'ї), а також жертв війни (як серед росіян, так і серед українців).

IV. «Охолоджуюча» приватність: загрози системи Clearview

Важливо відзначити, що до технології Clearview AI існує особливо негативне ставлення на міжнародній арені. Як правозахисні організації, так і науковці визнали систему Clearview надзвичайно інтрузивною технологією, яка не відповідає вимогам GDPR. Так, організація Privacy International наголосила, що використання Clearview AI «є значним розширенням сфери спостереження з дуже реальним потенціалом для зловживань». У зв'язку з цим Privacy International, разом з іншими регіональними організаціями (включаючи Digital Human Rights, Homo Digitalis і т. д.), подала кілька юридичних позовів проти компанії Clearview AI та направила їх регулюючим органам Франції, Австрії, Італії, Греції та Великобританії. Заявники стверджували, що Clearview AI порушила численні положення GDPR, а саме обробку чутливих даних, відсутність прозорості та законних підстав для обробки даних. В результаті розпочатого внутрішнього розслідування французький регулюючий орган наклав на Clearview штраф у розмірі 20 мільйонів євро, наказавши зупинити збір та обробку даних, а також видалити вже зібрані дані. Італія прийняла аналогічне рішення, заборонивши метод скрапінгу («scraping») веб-сторінок та зобов›язавши Clearview видалити всі дані. Така реакція міжнародного співтовариства є більш ніж зрозумілою. Відповідно, використання Clearview AI несе велику кількість ризиків для суб›єктів даних і їх подальшого застосування.

По-перше, під час використання Clearview завжди існує небезпека повної залежності від алгоритму системи, яка замінює прийняття рішень людиною. Хоча Тест Постачальника Засобів Розпізнавання Облич продемонстрував

точність алгоритму Clearview на рівні 99,85%, така сама точність ніколи не може бути гарантована протягом майбутніх співставлень. При автоматичному прийнятті рішень машина залишається всього лише машиною, що створює постійну проблему неправильного розпізнавання. У контексті війни в Україні це тягне за собою постійну небезпеку того, що система Clearview може видавати фатальні помилки, такі як прийняття цивільних осіб за солдатів, тяжкопоранених солдатів за загиблих, або навіть прийняття українців за російських диверсантів. Таким чином, правоохоронні органи та військові, які використовують систему, мабуть, повинні утримуватися від використання Clearview як єдиного джерела доказів.

По-друге, технологія Clearview піднімає питання приватності особи. Приватність – це концепція, яка включає «*як* право контролювати, чи ділитися інформацією, *так і з ким* нею ділитися». Таким чином, існує ризик, що очікування людей щодо приватності можуть мати охолоджуючий ефект при усвідомленні, що їх фотографії можуть збиратися та зберігатися. Більше того, Clearview порушує правила GDPR і національне українське законодавство, особливо щодо особливих категорій даних. Нагадаємо, що база даних складається із загальнодоступних фотографій із соціальних мереж. Дослідники запевняють, що Clearview збирає фотографії навіть з приватних акаунтів (де людина не бажає оприлюднювати інформацію), таким чином, припускаючи, що немає необхідності для отримання згоди людини в першу чергу. Однак база даних містить навіть ті зображення, «яких більше немає, але які колись були загальнодоступними», що дозволяє технології збирати навіть колись видалені зображення. Також не існує офіційного способу перевірити, чи знаходиться чиєсь зображення в базі даних Clearview AI, і, таким чином, вимагати видалення звідти таких даних.

Нарешті, FRT створює серйозні ризики при використанні у воєнних умовах в Україні. Оскільки компанія Clearview самостійно вирішує, кому пропонувати свої послуги, немає гарантії, що в якийсь момент часу інша сторона збройного конфлікту не отримає цю саму технологію. Враховуючи тривалі бойові дії та окупацію певних українських територій, існує ймовірність, що держава-агресор може захопити цифрові інструменти разом з фізичною інфраструктурою. Більше того, будь-яка приватна компанія може використовувати пошукову базу даних Clearview за умови оплати доступу до неї. Це може мати негативний вплив на українське інформаційне поле. У контексті війни в Україні це може призвести до небезпечних наслідків: оскільки Clearview AI також використовує зображення з російської соціальної мережі «ВКонтакте», Росія може посилити свою онлайн-маніпуляцію веб-сторінками, таким чином, спотворюючи результати для Clearview. Нарешті, сам факт ефективного використання послуг Clearview під час збройного конфлікту передбачає певний ступінь легітимізації небезпечної технології,

яка, ймовірно, створює ризики при її подальшому використанні в мирний час або в рамках інших конфліктів, де баланс сил не такий чіткий (наприклад, немає різниці між агресором та стороною, що захищається).

Всі вищезгадані занепокоєння створюють надзвичайно серйозний ризик при подальшому використанні Clearview AI. Незважаючи на те, що генеральний директор компанії заохочує використання тільки «тренованими слідчими», останнє не має сенсу, якщо не передбачені правові підстави для регулювання біометричних технологій. Зокрема, це залежить виключно від добросовісного підходу компанії та відповідних державних органів. Більше того, в основному сама компанія вирішує, кому може бути наданий доступ до її послуг, та регулює це замість законодавця. Це було проблемою для європейських держав і залишається головною проблемою для України в контексті війни. Таким чином, важливо здійснювати адвокацію за належне регулювання спостереження, здійснюваного як у військових, так і цивільних цілях. Важливо також підкреслити, що будь-які обмеження, накладені в умовах війни, повинні бути зняті негайно після припинення дії надзвичайного стану.

Незважаючи на вищезазначені проблеми, важко заперечити ефективність запровадженої системи Україні. Українська влада наголосила, що система Clearview допомогла в ідентифікації 125 тисяч російських військових злочинців. Серед них система ідентифікувала 50 осіб, причетних до вивезення дітей з України. Очікується, що через такі відчутним результати співпраця між Україною та Clearview AI в найближчому майбутньому стане ще тіснішою: компанія Clearview планує відкрити свій місцевий офіс в Україні для розвитку цифрової інфраструктури.

V. Рекомендації українським законодавцям

З розвитком цифрових технологій та їх впровадженням на полі бою важливо виступати за внесення змін до українського законодавства. Якщо надзвичайні засоби будуть застосовані без належних гарантій, це з великою ймовірністю може призвести до тяжких наслідків. Важливо також приділяти особливу увагу особливим категоріям даних, оскільки всі технології, які використовує Україна, обробляють дані за допомогою спеціальних технічних засобів, що дозволяють здійснювати унікальну ідентифікацію або аутентифікацію фізичної особи. У цьому випадку основною рекомендацією, яку пропонує ця робота, є внесення змін до чинного законодавства шляхом заповнення законодавчих прогалин та надання особам, що піддаються спостереженню, мінімальних гарантій. Такі гарантії повинні надаватися як у воєнний, так

і в мирний час, коли надзвичайна ситуація перестає існувати. Таким чином, для забезпечення належного захисту та дотримання прав людини, а також законного використання цифрового інструменту, дана робота рекомендує українським законодавцям наступне:

В мирний час:

1) Внести зміни до Закону України «Про захист персональних даних»:
   - додати статтю про технології FRT, в якій описується механізм їх роботи, вичерпний перелік підстав для їх використання, а також правила подальшої обробки біометричних даних;
   - розмежувати звичайне спостереження та спостереження, кероване штучним інтелектом, системи «високого ризику» та «низького ризику», біометричне та небіометричне спостереження;
   - надати додаткові гарантії проти незаконної обробки особливих категорій даних, зокрема:
     - встановити часові обмеження для зберігання біометричних даних в базах даних, вказавши чіткий список легітимних цілей (наприклад, підозра в скоєнні кримінального злочину, триваюче кримінальне розслідування і т.д.).,
     - надати суб›єкту даних право на забуття,
     - розробити спеціальний механізм повідомлення після того, як спостереження було проведене і досягло своєї мети;
   - встановити механізм санкцій за порушення правил захисту персональних даних шляхом запровадження пропорційних фінансових штрафів з урахуванням легких, серйозних та тяжких порушень, які можуть мати місце;
   - надати омбудсмену правозастосовні функції (наприклад, можливість накладати дисциплінарні або адміністративні санкції);
   - встановити додатковий контролюючий орган для поліпшення функціонування системи захисту даних.

2) Внести зміни до Кримінального кодексу України:
   - криміналізувати несанкціоноване використання засобів спостереження (особливо систем, керованих штучним інтелектом).

3) Внести зміни до Закону України «Про Національну поліцію»:
   - додати статтю, що надає визначення масового стеження, описує механізм його використання та надає вичерпний перелік цілей, для яких може бути застосовано спостереження.

4) Внести зміни до Кримінального процесуального кодексу:
   - передбачити судовий наказ як передумову для доступу правоохоронних органів до інформаційно-комунікаційних систем;
   - уточнити вид інформації, яка може збиратися за допомогою технічних пристроїв слідчим та прокурором.

У воєнний час:

1) Внести зміни до Закону України «Про захист персональних даних»:
   - передбачити можливість накладення більш суворих санкцій за недотримання правил захисту даних (наприклад, шляхом збільшення існуючої суми фінансових штрафів) з чіткою вказівкою, що така політика застосовна виключно у воєнний час;
   - збільшити періоди зберігання біометричних даних правоохоронними органами лише у воєнний час;
   - розширити перелік легітимних цілей для обробки біометричних даних (наприклад, національна безпека або територіальна цілісність) з виключною застосовністю цього положення у воєнний час;
   - уточнити види та обсяг додаткових заходів і технологій, дозволених до застосування виключно у воєнний час.

2) Внести зміни до Закону України «Про Національну поліцію»:
   - уточнити, до яких інтрузивних технологій (таких як автоматизовані системи прийняття рішень, системи, керовані штучним інтелектом) можуть вдаватися органи влади, вказавши, що такі цифрові інструменти можуть використовуватися таким чином лише у воєнний час;
   - передбачити механізм співпраці між правоохоронними органами та Clearview AI, перерахувавши цілі, для яких використовується система, функції, які має виконувати Clearview, та обмеження на її використання з урахуванням приватності суб›єктів даних (наприклад, запобігти збиранню системою Clearview зображень з приватних акаунтів у соціальних мережах).

Аналітичний звіт підготовлено в рамках програми “Сприяння Інтернет свободі в Україні”, яку реалізує Американська Асоціація Юристів в Україні / Ініціатива верховенства права.

Лабораторія цифрової безпеки — громадська організація, що працює над створенням сприятливого середовища для реалізації цифрових прав людини через проведення аналізу та розробку рекомендацій щодо державної політики у сфері інтернет свобод та врядування, а також надає підтримку з цифрової безпеки правозахисникам, журналістам, медійним та іншим організаціям громадянського суспільства в Україні та Східній Європі.

Лабораторія
Цифрової
Безпеки

2023