Богдан Даниленко,
кандидат юридичних наук,
адвокат
ORCID: 0000-0003-4314-9051

<https://doi.org/10.32782/2306-9082/2021-41-2>

УДК 342.72

Порушення права на недоторканість особистого життя: прихований наступ на свободу людини

*«Мене звуть майор Міра Кіліан,
я даю свою згоду на знищення цих даних.»*

Художній фільм «Привид у броні»
(США, Японія, 2017)

Постановка проблеми. Відповідно до частини першої статті 32 Конституції України [1] ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Згідно з частиною другою цієї статті не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Проте з часу ухвалення Конституції України порушення права на недоторканість особистого життя набули масового характеру, що вимагає відповідних наукових досліджень.

Аналіз останніх досліджень та публікацій. Право на недоторканість особистого життя було предметом досліджень представників науки конституційного права: Н.Г. Беляєвої,

М. С. Петросяна, Ф.М. Рудинського та інших. Серед представників науки конституційного права України можна особливо відзначити В.О. Серьогіна, який здійснив глибоке дослідження прайвесі на рівні дисертації на здобуття наукового ступеня доктора юридичних наук. Водночас, на наш погляд, у правовій науці досі недостатньо уваги приділяється проблемі порушення права на недоторканість особистого життя, особливо з огляду на масовість таких порушень. Також стрімкий розвиток суспільних відносин, в першу чергу, зумовлений технічним прогресом у сфері інформаційних технологій, вимагає окремого дослідження права на недоторканість особистого життя в контексті збору та використання персональних даних.

Під час здійснення наукової та практичної діяльності нами було виявлено стійку тенденцію із порушення прав людини в Україні [2]. На підставі здійсненого дослідження ми дійшли висновку про масовий характер порушення права людини на особисте життя, які здійснюються завдяки використанню

сучасних інформаційних технологій. Порухення права на особисте життя було визначено нами як один із напрямків подальших досліджень [2, с. 9].

Постановка завдання. Метою цієї статті є дослідження сучасного стану дотримання права людини на особисте життя в аспекті збору та використання персональних даних.

Виклад основного матеріалу дослідження. Сьогодні порушення права на недоторканість особистого життя мають тотальний характер. Це глобальне явище, яке має свої прояви в Україні, так само, як і в інших країнах світу. Завдяки нещодавнім скандалам щодо витоку конфіденційної інформації користувачів Facebook та її використання фактично всупереч їх інтересам [3; 4], масовим зломом електронної пошти сервісу Gmail, відеодзвінків сервісу ZOOM та іншим випадкам ця проблема набула висвітлення у пресі та стала предметом широкого громадського обговорення. Все частіше можна зустріти публікації в ЗМІ про торгівлю особистими даними з боку поліцейських [5; 6], працівників банків [7] та інших осіб. В інтернеті можна зустріти досить докладні огляди таких подій [8]. Проте ані Верховна Рада України, ані Президент України – гарант Конституції України, ані інші уповноважені органи державної влади не вживають адекватних заходів для захисту права людини на особисте життя.

Більше того. Політика держави сприяє порушенню цього права.

Демографічний реєстр. Згідно з частиною третьою статті 32 Конституції України кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею. Законом України від 20 листопада 2012 року № 5492-VI «Про Єдиний державний демографічний реєстр та документи, що

підтверджують громадянство України, посвідчують особу чи її спеціальний статус» було запроваджено Єдиний державний демографічний реєстр [9]. Чимало положень цього закону викликають занепокоєння. Проте ще більше занепокоєння викликає те, що переважна більшість громадян України навіть не чула про існування такого державного реєстру. Хоча, на нашу думку, це найбільш важливий для людини реєстр, оскільки він призначений для зберігання даних про людину, зокрема, біометричних, які, до речі, завжди збиралися лише щодо злочинців. Що цікаво, так це те, що, на відміну від інших державних реєстрів, які рекламуються державою та широко висвітлюються у ЗМІ, цей реєстр не набув висвітлення у засобах масової інформації.

Законопроект про демографічний реєстр було піддано обґрунтованій критиці з боку Головного науково-експертного управління та Головного юридичного управління апарату Верховної Ради України. Зокрема, стосовно порушень прав людини [10; 11]. Проте це, вже традиційно, не зупинило народних депутатів України.

Закон уже був предметом ґрунтовного наукового дослідження в аспекті дотримання прав людини. У своєму дослідженні, з яким можна ознайомитись на сайті Української Гельсінської спілки з прав людини, Олександр Волох дійшов висновку про здійснення конкретних кроків у бік розбудови системи таємного спостереження за фізичними особами-держателями платіжних карток та користувачами ідентифікаційних документів з платіжним додатком. Надання державним органам повноважень щодо обробки (збирання, зберігання, використання, поширення, тощо) непропорційно великого обсягу конфіденційної інформації про особу, як це передбачено Законом № 5492, становить порушення статті 8 Конвенції за всіма

критеріями, згідно яких можна було б виправдати втручання у приватність (крім вимоги доступності закону) [12].

Цікаво подивитися, чим же керувалися народні депутати України, коли голосували за проект цього закону. Як вказано у пояснювальній записці до законопроекту, ціллю прийняття законопроекту є запровадження загальноприйнятої Європейської практики щодо створення та забезпечення функціонування реєстру населення, а також виконання Україною своїх зобов'язань перед Європейською спільнотою на шляху до членства в Європейському союзі, в частині, що стосується забезпечення в державі обігу документів з електронним носієм інформації [13]. Схоже, для народних депутатів України вимоги ЄС вище за Конституцію України. Також їх не збентежило і те, що «загальноприйнята Європейська практика» суперечать практиці Європейського суду за прав людини [12]. Але і тут автори законопроекту злукали. Адже закон передбачає внесення біометричних даних до документів, що не використовуються для виїзду за кордон (наприклад, паспорт громадянина України, посвідчення водія) [10, с. 2].

Бізнес намагається не відставати від влади в напрямку стеження за людиною. Роботодавці вже давно вважають за норму таємно слідкувати за своїми працівниками та збирати на них інформацію. Ця практика набула такого поширення, що навіть юристи не соромляться публічно говорити про такі речі. Так, представники юридичної компанії Alexandrov&Partners радять своїм клієнтам, що на кожного співробітника компанії має бути сформоване та регулярно поновлюватись окреме дос'є [14, с. 70].

Боротьба із корупцією. Держава не обмежилася запровадженням згаданого вище реєстру. 14 жовтня 2014 року було прийнято Закон України «Про запобігання корупції» [15]. Законом

передбачене оприлюднення декларацій про майно, доходи та витрати широкого кола осіб.

Відповідно до частини першої статті 47 чинного Закону України «Про запобігання корупції» подані декларації включаються до Єдиного державного реєстру декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування, що формується та ведеться Національним агентством.

Національне агентство забезпечує відкритий цілодобовий доступ до Єдиного державного реєстру декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування, на офіційному веб-сайті Національного агентства.

Положення проекту чинного Закону України «Про запобігання корупції» було детально проаналізовано та піддано обґрунтованій критиці у висновку Головного науково-експертного управління апарату Верховної Ради України [16].

Зокрема, вказано, що у проекті не взято до уваги ту обставину, що на членів сім'ї суб'єкта декларування, які проживають окремо від нього, неможливо покласти обов'язок надавати відомості про свої доходи та витрати. Внаслідок цього виявляється, що проект вимагає від суб'єкта декларування вчинення дій, які не залежать від його волі, а у разі, коли такі дії не вчинено – передбачає за це юридичну відповідальність, що є юридично некоректним. За змістом ч. 1 ст. 32 Конституції України ніхто не може зазнавати втручання в його особисте і сімейне життя (а майновий стан особи є частиною його особистого життя) крім випадків, передбачених Конституцією України [15, с. 11]. Проте ці норми набули чинності (ст. 46 Закону).

На думку Головного науково-експертного управління апарату Верховної Ради України, досить дискусійною є ідея оприлюднення декларацій мільйонів

громадян, які є суб'єктами декларування, відповідно до положень проекту. Адже цілком зрозуміло, що високі корупційні ризики притаманні здебільшого відповідальним посадам [16, с. 12].

З огляду на наведені вище висновки особливо цинічним виглядає ствердження авторів законопроекту про те, що законопроект «не належить до сфери правового регулювання Конвенцією про захист прав людини і основоположних свобод» [17, с. 5].

Народні депутати України не дослухалися до порад фахівців.

На нашу думку, оприлюднення декларацій – масове порушення права на особисте життя.

Всі реформи влади, зокрема антикорупційна, подаються під соусом прозорості влади. Прозора влада має діяти відповідно до Конституції України та Законів України в інтересах народу України. Інакше вона діяти просто не може, оскільки будь-які зловживання одразу помітні суспільству. Але на практиці відбувається дещо інше.

Отже, насправді влада не стала прозорою. Проте все більш прозорою стає людина. Публічний доступ до декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування, робить прозорими цих осіб, а не органи публічної влади. Що насправді стоїть за такою «прозорістю» чудово продемонстровано в художньому фільмі «Сфера» (США, ОАЕ, 2017 р.).

Деяким особам не вистачає публічних декларацій, і вони замовляють збір конфіденційної інформації на державних службовців. Часом таких осіб вдається викрити правоохоронним органам [18]. Проте, на наше переконання, це лише верхівка айсбергу.

Індивідуальний ідентифікаційний номер. Час від часу в мережі з'являються викиди конфіденційної інформації про необмежене коло осіб. Так, на початку 2000-их років працював сайт Radarix.com, що містив дані

про громадян України та деяких інших країн. За допомогою цього сайту будь-хто бажавчий за ім'ям особи міг отримати дані з податкової бази: адресу, телефони, номер автомобілів та документів, відомості про судимість та розмір заробітної плати [19].

Проте найбільше вразило користувачів інше. Законом України від 22 грудня 1994 року № 320/94ВР «Про Державний реєстр фізичних осіб – платників податків та інших обов'язкових платежів» [20] (на даний час втратив чинність) запроваджено присвоєння індивідуальних ідентифікаційних номерів фізичним особам – платникам податків. Це викликало рішучий протест певної частини суспільства.

Законом України від 16 липня 1999 року «Про внесення змін до Закону України «Про Державний реєстр фізичних осіб – платників податків та інших обов'язкових платежів» [21] (втратив чинність) таким людям була надана можливість не присвоювати ідентифікаційний номер.

Чинний Податковий кодекс України [22] містить таке формулювання: реєстраційний номер облікової картки платника податків та серію та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган і мають відмітку у паспорті) (пункт 48.3 статті 48). Це громіздке формулювання повторюють численні Закони України та підзаконні акти.

Не дивлячись на це, користувачі сайту Radarix.com з величезним подивом дізналися про те, що особи, які відмовилися від прийняття реєстраційного номера облікової картки платника податків, все одно його мають. Просто вони, на відміну від інших громадян, не знають його. Ніяких пояснень з боку компетентних органів державної влади не було.

Таємниця кореспонденції. Згідно зі статтею 31 Конституції України [1] кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо.

У 2018 році в Україні стався масовий злам поштового сервісу Google Gmail. Сторонні особи могли з легкістю отримати доступ до листів чужої електронної поштової скриньки. Сервіс Gmail вважається, на відміну від українських поштових сервісів, надійним та захищеним. А тому багато людей в Україні довіряло не лише особисте, але й ділове листування цьому сервісу. Злам електронної пошти став справжнім потрясінням для таких людей. Цей випадок яскраво продемонстрував всю ціну уявної надійності Gmail. Проте в українській аудиторії дуже коротка новинна пам'ять. Тому навіть таку подію, що безпосередньо торкнулася мільйонів українців, до кінця року вже майже ніхто не пам'ятав. Ніякої реакції з боку правоохоронних органів на масове порушення права людини на таємницю кореспонденції в українському інформаційному просторі автором зафіксовано не було.

Психологічне тестування та інші сучасні методи прихованого збору персональних даних. Тести проникають все глибше у наше життя: в освіту, державну службу, трудові відносини, тощо. Зараз у рамках проведення співбесіди роботодавця із найманим працівником під час відбору працівників все більшої популярності набуває проходження працівником різноманітних психологічних тестів. Під час карантину, викликаного поширенням вірусу COVID-19 навесні 2020 року, дійшло до того, що деякі рекрутингові

агентства почали надсилали пошукачам психологічні тести електронною поштою. Мабуть, не треба й казати про те, що той, хто шукає роботу, ніколи не визнає результатів своїх тестів.

На нашу думку, така практика вкрай сумнівна, подібні дії за певних обставин можуть навіть містити склад злочину. Адже психологічне тестування – особливий вид збору інформації про людину. У такий спосіб можна дізнатися про людину те, чого вона і сама про себе не знає. Ця інформація потенційно може бути використана зовсім не з тією метою, для якої її збирали. Наприклад, під приводом пошуку працівників хтось може проводити наукові дослідження. У такому випадку матимемо порушення права людини на повагу до його гідності. Згідно з частиною другою статті 28 [1] Конституції України жодна людина без її вільної згоди не може бути піддана медичним, науковим чи іншим дослідженням.

Якщо ідеться про тестування суддів, тут виникають й інші питання. Як відомо, в межах кампанії із реформування судової влади судді усіх судів України пройшли тестування. За приватними відгуками суддів зміст запитань у тестах був вкрай дивним, а результати тестів взагалі зникли. Таким чином, була зібрана особиста інформація невідомого характеру про усіх персональних носіїв судової влади в Україні. Така інформація може бути використана проти України іноземними державами. Подібні дії вже виходять за межі площини порушення прав людини і сягають сфери національної безпеки.

Мода на психологічні тести прийшла до України із Америки. У США тестування почало проникати в життя американців набагато раніше, ніж у нас. У контексті нашого дослідження дуже цікаво навести свідчення відомого американського вченого статистика Дарела Хафа, викладені ним у книзі «Як брехати за допомогою статистики» 1954 року: «У наші дні із різного

роду тестів на розумові здібності створили просто-таки фетиш та розводять навколо них шаманські танки. І не виключено, що Вам доведеться витримати невелику словесну баталію, щоб здобути результати тесту. Це відомості вельми езотеричного характеру, що недоступні для розуміння непосвячених, і тому прийнято вважати, що вони будуть краще збережені, якщо залишатимуться в лише в руках психологів та педагогів. Ймовірно, це не позбавлене сенсу...» [23, с. 65].

Багатьом роботодавцям тестування працівників здається недостатнім і вони звертаються також до інших методів збору інформації особистого характеру: як заснованим на сучасних технологіях, так і дуже давнім. Так, наприклад, у Москві, деякі компанії вже почали залучати до роботи із персоналом астрологів, яким ставлять деталізовані вимоги щодо роботи із персоналом. Звісно, не для того, щоб створити для кожного працівника більш комфортні умови праці: навпаки, роботодавці шукають нові можливості для пошуку слабких місць людей, що і так від них залежні економічно. Все більшого поширення серед українських роботодавців набуває використання поліграфу при прийомі на роботу [14, с. 108]. Звісно, без будь-яких правових підстав. Результати дослідження з використанням поліграфу наймані працівники ніколи не побачать, так само, як і психологічного тестування.

Таким чином, ми бачимо, що існує тенденція до того, щоб розширювати застосування психологічних тестів і не надавати результати тестів тому, хто їх проходив. Те саме стосується і використання поліграфу та інших методів прихованого збору персональних даних. У такій ситуації вже можемо констатувати порушення права людини на приватність, адже згідно з частиною третьою статті 32 Конституції України кожний громадянин має право знайомитися в органах державної влади,

органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею.

Проте самі факти збору інформації про людину та приховання її від самої людини не такі небезпечні, як їх можливі наслідки. Адже маємо ситуацію, коли якісь невідомі особи можуть знати про людину більше, ніж вона сама про себе знає. Такі знання можуть бути використані проти людини. Якщо хтось здійснює цілеспрямований збір даних про людину, він знає, для чого він це робить. А якщо він приховує зміст цих даних, є всі підстави вважати, що його цілі суперечать інтересам тих, на кого він збирає інформацію.

Правова охорона персональних даних. Як же держава реагує на масові порушення конституційного права громадян?

1 січня 2011 року набув чинності Закон України «Про захист персональних даних» [24]. Відповідно до положень цього закону збір, зберігання, обробка та використання персональних даних про фізичну особу, за загальним правилом, вимагає згоди цієї особи. І закон виконується. Будь-які дії, що вимагають отримання персональних даних від людини, незалежно від того, ким вони здійснюються (органами публічної влади чи юридичними особами приватного права), супроводжуються процедурою надання згоди на отримання персональних даних від суб'єкта персональних даних. Такі згоди ми підписуємо під час отримання адміністративних послуг, відвідування банків, тощо.

Проте все викладене вище свідчить про те, що Ваша згода нікому не потрібна. Держава, банки, мобільні оператори та інші організації вже давно збирають на Вас будь-яку інформацію, яку вони лише забажають, і в значно більшому обсязі, ніж Ви даєте на це дозвіл. На наш погляд, Закон України «Про захист персональних даних»

достатньо вдалий як з погляду змісту, так і з погляду юридичної техніки. Проте практика його застосування, яка полягає в тому, що відповідні суб'єкти дотримуються лише формальних вимог і повністю ігнорують дух цього закону, лише створює ілюзію захисту персональних даних і нічого, крім шкідливої звички ставити особистий підпис на документи, не думаючи, людині не дає. Застосування чинний закон за умов повсюдного грубого порушення права на приватність перетворилося на відверту профанацію. Це прикриття, за яким здійснюється наступ на свободу людини.

Згідно із чинним законодавством України право на приватність підлягає кримінально-правовій охороні: стаття 182 Кримінального кодексу України передбачає кримінальну відповідальність за порушення недоторканості приватного життя [25]. Стаття була ще у первісній редакції чинного Кримінального кодексу України, тобто діє із 2001 року. У 2011 році до цієї статті було внесено зміни щодо посилення кримінальної відповідальності за порушення недоторканості приватного життя. Також було внесено відповідні зміни і до Кодексу України про адміністративні правопорушення [26]. Практика застосування статті 182 Кримінального кодексу України вкрай обмежена і явно не відповідає масштабу повсякденного здійснення діяльності, що містить склад злочину, передбаченого вказаною статтею. У більшості випадків до кримінальної відповідальності притягають окремих осіб, які вчиняють такі злочини із метою збагачення чи з особистих мотивів. Проте справжню небезпеку в контексті прав людини становлять не окремі шахраї або навіть групи шахраїв, які є завжди.

Високу суспільну небезпеку має діяльність держави (в особі відповідних посадових осіб) та представників крупного бізнесу. У першу чергу це

стосується бізнесу у сфері інформаційних технологій: операторів мобільного зв'язку; розробників, власників та адміністраторів пошукових систем у мережі Інтернет та інших програмних продуктів, соціальних мереж, тощо (програмне забезпечення – software). Те саме стосується і розробників, власників та тих, хто здійснює експлуатацію апаратного забезпечення (hardware) та іншого обладнання і техніки: мобільних телефонів, комп'ютерів, вишок зв'язку, тощо. Також варто приділити увагу діяльності банків, страхових компаній та інших юридичних осіб, діяльність яких передбачає постійний збір персональних даних великої кількості людей. Проте правоохоронні органи чомусь дуже кволі у цьому напрямку діяльності. За 20 років дії чинного Кримінального кодексу України, за умов повсякденного грубого порушення права на приватність, постійного вдосконалення та стрімкого поширення нових технічних засобів збору персональних даних, в Україні досі не сформувалася належна судова практика.

На нашу думку, чинне законодавство України дозволяє здійснювати ефективний захист права людини на приватність. Проте правоохоронні органи з якихось причин фактично ігнорують злочинну діяльність у цій сфері.

Деякі прояви протиправного використання персональних даних. Протиправне збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди не лише порушує право людини на особисте життя, але й може призвести до порушень практично будь-яких інших конституційних прав людини. Більше того, ця проблема вже вийшла з площини ймовірного до площини дійсного.

Сьогодні для того, щоб стежити за людиною, достатньо отримати доступ до даних її оператора мобільного зв'язку, адже можна легко простежити всі пересування цієї людини.

Цей спосіб вже широко використовується правоохоронними органами, і далеко не завжди в межах їх повноважень. Під час акцій протесту у Києві в січні 2014 року учасникам акцій приходили повідомлення такого змісту: «Шановний абоненте, Ви зареєстровані як учасник масових заворушень» [27]. Тоді це набуло широкого розголосу. Навіть далеко за межами нашої країни ця подія використовується як приклад застосування інформаційних технологій у політичних цілях проти громадян країни. Проте це була лише скромна демонстрація того, як персональні дані, якими володіють мобільних оператори, можуть бути використані проти їх власників.

Зовсім не відома широкому загалу історія, яка трапилася у Харкові. Після зникнення відомого журналіста за фактом зникнення було розпочато кримінальне провадження. Під час досудового слідства було викликано на допити як свідків безпрецедентну кількість осіб. Єдиною підставою для цього було те, що мобільні телефони цих людей перебували приблизно в тому районі і в той час, де, за версією слідства, зник журналіст. Що може трапитися поруч з мобільним телефоном будь-якої людини і як це може бути використано правоохоронними органами, організованими злочинними угрупованнями чи будь-якими іншими особами? Потенційно будь-хто може стати жертвою кримінального переслідування чи злочинного нападу.

Наведені вище приклади можуть пролити світло на дивну бездіяльність правоохоронних органів у напрямку захисту права на недоторканість особистого життя: правоохоронцям надзвичайно вигідна така ситуація. По-перше, тотальний збір інформації про всіх і все значно полегшує розслідування злочинів. По-друге, він значно полегшує можливості для тиску на тих чи інших осіб за потреби. Можливість швидкого доступу до величезного обсягу

інформації про будь-яку людину і в будь-який момент виглядає аж надто спокусливою, щоб нею не скористатися.

Соціальні мережі. На жаль, більшість користувачів пострадянського простору почали своє знайомство з інтернетом з ICQ, «Вконтакті», «Однокласників» та інших «друзів», довіра до яких була настільки високою, що їх просто перестали помічати та повністю інтегрували до свого життя.

Невдовзі інтернет знав про людей все, і цю інформацію почали використовувати проти її власників, починаючи із хакерів, котрі зламували аккаунти та вимагали грошей за персональні дані, та завершуючи великими комерційними компаніями, котрі знали вподобання користувачів, розуміли, який продукт їм краще продати та як можна вплинути на їх мозок [8].

Проте так відбувається не лише на пострадянському просторі. Так відбувається в усьому світі. І особливо яскраво це видно на прикладі батьківщини сучасних інформаційних технологій – Сполучених Штатів Америки.

Найбільш популярна у світі соціальна мережа Facebook була створена для спілкування студентів. З часом нею почали користуватися, як-то кажуть, широкі маси американського населення. І непомітно для громадян США Facebook перекочував із суто приватної до публічної площини.

Декілька років тому світ сколихнув скандал, викликаний використанням даних американських користувачів Facebook фактично проти них самих. Але цього разу це було здійснено не з метою нав'язати людям якийсь черговий непотрібний їм товар, а, ні багато, ні мало, з метою перемоги на виборах Президента США потрібного кандидата! Чимало оглядачів стверджують, що саме завдяки застосуванню майстерно продуманої системи маніпуляцій через соціальні мережі Дональд Трамп і став новим президентом США [28].

Сьогодні у США, які, до речі, вважаються демократичною країною, починають відкрито використовувати соціальні мережі для порушення прав як своїх громадян, так і іноземців. Так, для отримання візи Державний департамент США вимагатиме в іноземних громадян дані про їх соціальні мережі [29]. Відповідно до офіційного повідомлення, розміщеного на сайті Бюро консульських відносин Державного департаменту США від 4 червня 2019 року, 31 травня 2019 року Державний департамент США оновив форми заявок для отримання візи. Додано нову інформацію, зокрема, дані про соціальні мережі для осіб, що бажають отримати візу [30]. В онлайн-аплікаційній формі для отримання візи США вже міститься дві графи: назва соціальної мережі та назва Вашого персонального акаунту.

Згідно з новими правилами особа, яка бажає отримати візу, повинна надати інформацію про акаунти у соціальних мережах, які вона використовувала протягом останніх 5 років. Така інформація дасть уряду доступ до фото, місцезнаходження, дати народження, важливих дат у житті та іншої персональної інформації, якою зазвичай діляться в соціальних мережах. Державний департамент США заявляє, що «ми постійно працюємо над тим, щоб знайти механізми, які покращать наш процес перевірки заради захисту громадян Сполучених Штатів, водночас ми підтримуємо легальний туризм до Сполучених Штатів» [31].

Проте з такою логікою незгодні правозахисники. Так, Американський Союз захисту громадянських свобод заявляє, що «немає жодних доказів, що такий моніторинг соціальних мереж є ефективним чи справедливим та призведе до самоцензури в інтернеті» [31]. Надумку Елори Мухірі, директору Клініки Прав Мігрантів при Школі Права Колумбії, схоже, що це частина спроби мати надзвичайно широку систему спостереження за громадянами та

негромадянами. Вона вважає, що, з огляду на обсяг спостереження, важко знайти раціональну основу для широкого спостереження, що його здійснює Державний департамент та Департамент Внутрішньої Безпеки впродовж вже майже двох років [31].

Фаїза Патель, співдиректор програми свободи та національної безпеки центру імені Бренанна при Університеті Нью-Йорку звертає увагу на те, що згідно нових правил моніторингу підлягають люди, які вже перебувають у США – наприклад, власники грін карт. Є недостатність відкритості в тому, як саме уряд використовує такі дані [32].

Ситуація дуже схожа із прийняттям Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус», про який йшлося на початку статті. Держава збирає все більше даних на людину і не пояснює, як насправді вони будуть використовуватись.

І як тут не згадати про те, що американська соціальна мережа Facebook на сьогодні буквально заповонила життя мільйонів українців. У ній люди висловлюють свої думки, об'єднуються в групи, вступають у конфлікти. На тлі бурхливого громадського життя в сучасній Україні люди довіряють цьому ресурсу масу інформації про себе та свої зв'язки з іншими людьми. Навряд чи така інформація чимось зарадить безпеці громадян США. А от використати її для впливу на громадян України дуже навіть можна.

У період карантинних заходів в Україні, викликаних поширенням у світі коронавірусу, різко зросло і без того велике значення інформаційних технологій. Ділові комунікації максимально зосередилися у технологічній площині. Заклади освіти перейшли на дистанційне навчання. Особливої популярності набув сервіс для відеоконференцій ZOOM. Але не встиг цей сервіс

опанувати простори української освіти, як пресу сколихнув скандал із викладенням у вільний доступ тисяч відеодзвінків, що здійснювалися через ZOOM [33]. Проте люди, занепокоєні поширенням інфекції, а, можливо, ще більшою мірою, зміною звичного ритму життя, не надали належної уваги цій новині.

Правовий нігілізм. Ми вже наводили приклади відкритих порушень права на недоторканість особистого життя. Проте буквально з кожним роком ситуація стрімко погіршується. Люди отримують повідомлення та дзвінки на мобільні телефони від найрізноманітніших суб'єктів: банків, торговельних мереж, таксі, тощо. У більшості випадків людина і гадки не має, звідки у них з'явився її номер мобільного телефону. А варто лише переступити поріг інтернету, і на Вас одразу посиплється цілеспрямована реклама та інша інформація, відібрана спеціально для Вас на підставі використання Ваших особистих персональних даних, про що Ви, звісно, ніколи і нікого не просили. Звідки і як це все береться? Але ще гірше те, що більшість людей уже навіть не задає собі таких питань. Люди вже звикли до того, що їх персональні дані живуть своїм окремим життям і завжди доступні необмеженому колу осіб. У людей виникає ілюзія, що це все нормально. А також ілюзія безпеки.

На нашу думку, не усвідомлення глибини суспільної небезпеки порушення права на приватність – одна з основних проблем захисту прав та свобод людини.

Отже, в Україні проблема порушення права на недоторканість особистого життя завдяки використанню сучасних інформаційних технологій, не те що назріла, а вже давно перезріла. Проте, на відміну від США, українські правозахисники не приділяють уваги цій проблемі.

Скандали, спричинені масовим витоком персональних даних в соціальних мережах, даних мобільних

операторів, електронній пошті і навіть державних реєстрах, виникають досить часто і висвітлюються у ЗМІ. Проте дуже коротка пам'ять аудиторії дозволяє буд-якій зміні інформаційного порядку денного відволікти увагу від гучних скандалів та масштабних проблем [8].

Висновки. Здійснене дослідження дає підстави зробити висновок про існування стійкої тенденції із порушення права людини на недоторканість особистого життя. Ця тенденція має глобальний характер, тому її основні прояви в Україні близькі до тих, які можна спостерігати в інших країнах світу. Порушення права на приватність спирається на застосування сучасних інформаційних технологій. Також виявлено тенденцію до постійного зростання збору та накопичення інформації про людину, розширення та поглиблення такої інформації завдяки науковому прогресу, з одночасною заборобою людині знайомитися з такою інформацією. Особливістю порушення права на недоторканість особистого життя є його непомітність для більшості людей. Водночас порушення цього права створює широкі можливості для порушення інших прав людини. Не дивлячись на це, цій проблемі не приділяється належної уваги як з боку практиків, так і з боку науковців.

Напрямки подальших досліджень. Стрімкий розвиток інформаційних технологій, активна правотворчість, спрямована на створення умов для посилення негласного збору особистих даних як на національному, так і на міжнародному рівні, а також непомітність порушення права на приватність та недостатня увага до нього як з боку суспільства, так і з боку фахівців, створює сприятливі умови для розвитку нових форм порушення права на недоторканість особистого життя. Вони і мають стати предметом майбутніх досліджень. Крім того, викликають

науковий інтерес шляхи використання порушення інших прав людини, а персональних даних, оскільки вони також з іншими суспільно небезпеч- можуть бути використані з метою ними цілями.

Список використаних джерел

1. Конституція України. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
2. Даниленко Б. Обмеження прав людини: небезпечна тенденція. *Вісник Київського університету імені Тараса Шевченка*. 2019. Випуск № 1. С. 5–12.
3. Цукерберг розповів сенаторам США про «гонку озброєнь» з Росією. URL : [https://www.dw.com/uk/цукерберг-розповів-сенаторам-сша-про-гонку-озброєнь-з-росією/a-43334365?maca=ukr-rss-ukrnet-ukr-all-3816-xml\\$](https://www.dw.com/uk/цукерберг-розповів-сенаторам-сша-про-гонку-озброєнь-з-росією/a-43334365?maca=ukr-rss-ukrnet-ukr-all-3816-xml$).
4. ВЕСанонсировали «жесткие меры» против Facebook. URL: <https://apostrophe.ua/news/politics/foreign-policy/2018-03-25/v-es-anonsirovali-jestkie-meryi-protiv-facebook/125215>.
5. Офицер патрульной полиции Харькова задержан за торговлю служебной информацией. URL : https://censor.net.ua/photo_news/3066246/ofitser_patrulnoyi_politsii_harkova_zaderjan_za_torgovlyu_slujebnoyi_informatsieyi_natspolitsiya_foto.
6. Двое сотрудников уголовного розыска задержаны в Виннице за торговлю служебной информацией. URL : https://censor.net.ua/photo_news/3055825/dvoe_sotrudnikov_ugolovnogo_rozyska_zaderjany_v_vinnitse_za_torgovlyu_slujebnoyi_informatsieyi_natspolitsiya.
7. Менеджер ПриватБанка продавал данные клиентов по 400 гривен. URL : https://zn.ua/ECONOMICS/sotrudnik-privatbanka-prodaval-dannye-klientov-cherez-telegram-295682_.html.
8. «Теория большого слива». Как не стать жертвой утечки личных данных в интернете. URL : <http://politica.com.ua/teoriya-bolshogo-sliva-kak-ne-stat-zhertvoj-utechki-lichnykh-dannykh-v-internete/>.
9. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус : Закон України від 20 листопада 2012 року № 5492-VI. *Голос України*. 2012. № 231 (з наступними змінами та доповненнями).
10. Висновок на проект Закону України «Про Єдиний державний демографічний реєстр». URL : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=43462.
11. Зауваження до проекту Закону України «Про Єдиний державний демографічний реєстр та документи, які підтверджують громадянство України, посвідчують особу чи її спеціальний статус». URL : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=43462.
12. Олександр Волох. Право на приватність та Закон «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус». URL : <http://hro.org.ua/index.php?id=1519312627>.
13. Пояснювальна записка до проекту Закону України «Про Єдиний державний демографічний реєстр». URL : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=43462.
14. Антирейдерство. Захист агробізнесу. Київ: Видавничий дім «КІЙ», 2017. 176 с.
15. Про запобігання корупції : Закон України від 14 жовтня 2014 року № 1700-VII. *Голос України*. 2014. № 206.
16. Висновок на проект Закону України «Про запобігання корупції». URL : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=52247.
17. Пояснювальна записка до проекту Закону України «Про запобігання корупції». URL : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=52247.
18. 36-летний продавец программного обеспечения из Хмельницкого украл личные данные госслужащих, киберполиция. URL : https://censor.net.ua/news/3103953/36letniyi_prodavets_programmnogo_obespecheniya_iz_hmelnitskogo_ukral_lichnye_dannye_gosslujaschih_kiberpolitsiya.

19. Radarix. URL : <https://ru.wikipedia.org/wiki/Radarix>.
20. Про Державний реєстр фізичних осіб – платників податків та інших обов'язкових платежів: Закон України від 22 грудня 1994 року № 320/94-ВР. *Відомості Верховної Ради України*. 1995. № 2. С. 21. Ст. 10.
21. Про внесення змін до Закону України «Про Державний реєстр фізичних осіб – платників податків та інших обов'язкових платежів»: Закон України від 16 липня 1999 року № 1003-XIV. *Голос України*. № 156.
22. Податковий кодекс України : Закон України від 2 грудня 2010 року № 2755-VI. *Голос України*. № 229 (з наступними змінами та доповненнями).
23. Как лгать при помощи статистики / Дарелл Хафф; Пер. с англ. 4-е изд. Москва : Альпина Паблишер, 2018. 163 с.
24. Про захист персональних даних : Закон України від 1 червня 2010 року № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. С. 1188. Ст. 481.
25. Кримінальний кодекс України : Закон України від 5 квітня 2001 року № 2341-III. *Голос України*. 2001. № 107 (з наступними змінами та доповненнями).
26. Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних : Закон України від 2 червня 2011 року № 3454-VI. *Голос України*. 2011. № 116.
27. Мобильные операторы «идентифицируют» участников протестов. URL : <https://www.pravda.com.ua/rus/news/2014/01/21/7010294/>.
28. Year one: how Donald Trump used social media to win (and maintain) the presidency. URL : <https://medium.com/rta902/year-one-how-donald-trump-used-social-media-to-win-and-maintain-the-presidency-fef7f7175d2c>.
29. Хотите американську візу? Будьте чемними до США у соцмережах. URL : <https://www.radiosvoboda.org/a/30005481.html>.
30. Collection of Social Media Identifiers from U.S. Visa Applicants. URL : https://travel.state.gov/content/travel/en/News/visas-news/20190604_collection-of-social-media-identifiers-from-U.-S.-visa-applicants.html.
31. U.S. Requiring Social Media Information From Visa Applicants. URL : <https://www.nytimes.com/2019/06/02/us/us-visa-application-social-media.html>.
32. U.S. to Collect Social Media Data on All Immigrants Entering Country. URL : <https://www.nytimes.com/2017/09/28/us/politics/immigrants-social-media-trump.html>.
33. Thousands of Zoom recordings exposed because of the way Zoom names recordings. URL: <https://www.theverge.com/2020/4/3/21207134/zoom-recordings-exposed-thousands-identical-naming-search>.

Даниленко Б. В. Порушення права на недоторканість особистого життя: прихований наступ на свободу людини

Стаття присвячена дослідженню стану дотримання права на недоторканість особистого життя в Україні. Зроблено висновок про масовий характер порушень права на приватність як із боку держави, так і із боку приватних осіб. Верховна Рада України ухвалює закони, які порушують Конституцію України в частині охорони права на недоторканість особистого життя. Закони України, спрямовані на правову охорону цього права, не виконуються належним чином. Правоохоронні органи фактично ігнорують численні порушення з боку різних суб'єктів, що лише заохочує до подальших правопорушень.

Особливу роль у контексті даного дослідження відіграє використання сучасних інформаційних технологій. Саме завдяки ним порушення права на приватність набули тотального характеру. Із розвитком цих технологій ситуація лише стрімко погіршується. Інформаційні технології використовуються як інструмент протиправного стеження за людиною з боку розробників та адміністраторів відповідної техніки (операторів мобільного зв'язку, розробників програмного забезпечення, тощо), банків, страхових компаній, інших організацій, діяльність яких пов'язана з обробкою персональних даних, та, нарешті, самих працівників правоохоронних органів.

Також важливу роль у контексті даної проблеми відіграють соціальні мережі. Коли їх запроваджували, то вони подавалися як засіб для виключно приватного спілкування. Проте коли соціальні мережі вже глибоко проникли у життя суспільства, їх почали переводити у публічну площину. У даний час соціальні мережі активно використовують із економічними та політичними цілями всупереч інтересам користувачів.

Масовість порушень права на недоторканість особистого життя та бездіяльність із боку правоохоронних органів породили глибокий правовий нігілізм. Навіть правники суттєво недооцінюють ступеню суспільної небезпеки порушення права на приватність: зневаження недоторканості приватного життя може бути використано як основа для порушення усіх інших прав та свобод людини.

Ключові слова: Конституція, право на недоторканість особистого життя, приватність, реєстр, корупція, персональні дані, тести, інформаційні технології, соціальні мережі, бездіяльність, правовий нігілізм.

Даниленко Б. В. Нарушения права на неприкосновенность частной жизни: скрытое наступление на свободу человека

Статья посвящена исследованию состояния соблюдения права на неприкосновенность частной жизни в Украине. Сделано заключение о массовом характере нарушения права на неприкосновенность частной жизни как со стороны государства, так и со стороны частных лиц. Верховная Рада Украины принимает законы, которые нарушают Конституцию Украины в части охраны права на неприкосновенность частной жизни. Законы Украины, направленные на защиту этого права, не исполняются надлежащим образом. Бездействие правоохранительных органов лишь поощряет дальнейшие правонарушения.

Особая роль в контексте данного исследования принадлежит использованию современных информационных технологий. Именно благодаря им нарушения права на приватность приобрели тотальный характер. По мере развития этих технологий ситуация лишь усугубляется. Информационные технологии используются как инструмент противоправного наблюдения за человеком со стороны разработчиков и администраторов соответствующей техники (операторов мобильной связи, разработчиков программного обеспечения, и т.п.), банков, страховых компаний, иных организаций, деятельность которых предусматривает обработку персональных данных, и, наконец, работников правоохранительных органов.

Также важную роль в контексте рассматриваемой проблемы играют социальные сети. Когда их внедряли, их подавали как средство для исключительно частного общения. Однако после того как социальные сети глубоко проникли в жизнь общества, их стали переводить в публичную плоскость. В настоящее время социальные сети активно используются для достижения экономических и политических целей, которые противоречат интересам пользователей.

Масовость нарушений права на неприкосновенность частной жизни, а также бездействие со стороны правоохранительных органов стали причиной возникновения глубокого правового нигилизма. Даже правоведы существенно недооценивают степень общественной опасности нарушения права на приватность: пренебрежение неприкосновенностью частной жизни может быть использовано как основание для нарушения всех остальных прав и свобод человека.

Ключевые слова: Конституция, право на неприкосновенность частной жизни, приватность, реестр, коррупция, персональные данные, тесты, информационные технологии, социальные сети, бездействие, правовой нигилизм.

Danylenko B. The violation of right to privacy: the hidden attack on civil liberties

This article is devoted to the research of violations of right to privacy in Ukraine. The author demonstrates that such violations are permanent and massive. Both state and private persons constantly violate right to privacy. The state legislative policy is contradictory. On

one hand, the Ukrainian state makes laws that protect privacy. But on the other hand, the parliament makes laws, that violate Constitution of Ukraine concerning right to privacy. It is important to admit, that National Police does not protect privacy of Ukrainian citizens. So protective laws simply does not work. This encourages private persons to violate the law.

The violation of privacy is based on the usage of modern informational technologies. The uncontrolled spread of IT is a real threat to human rights. In Ukraine the political groups have already used mobile phones to threaten the citizens. Mobile phones are used by police to track people. The employers violate rights of their employees: collect private data, use psychological testing, polygraph and other methods. It is important to admit, that according to Constitution of Ukraine everyone has the right of access to the information about himself. But employers hide such information. Different organizations, such as banks, mobile network operators and other collect private information in such a way, that contradicts the legislation of Ukraine.

Social media is one of the most important tools that are used to violate privacy and other civil rights. The cause of the problem is that at first social media were used only for private communication. They were widely advertised as a private space. But once people get used to them, social media suddenly became a public resource with all the consequences of such a change.

All these created a problem of legal nihilism. People are get used to the violation of privacy and underestimate the threat. The lawyers, both scientists and practitioners, also do not pay due attention to the problem. The main issue is that fact, that violation of privacy is used to violate other civil rights.

Key words: Constitution, civil rights, privacy, violation, register, corruption, informational technologies, social media, legal nihilism.