УДК 343.4
DOI https://doi.org/10.32782/1813-338X-2023.3.18

Е. Г. Стоматов
кандидат юридичних наук, доцент,
суддя Комунарського районного суду м. Запоріжжя
https://orcid.org/0000-0002-3955-3337

КРИМІНАЛЬНО-ПРАВОВА ОХОРОНА КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ЗА КРИМІНАЛЬНИМ КОДЕКСОМ РЕСПУБЛІКИ ПОЛЬЩА (НА ПРИКЛАДІ СТ. 267 КК)

В статті проаналізовано стан кримінально-правової охорони конфіденційної інформації за Кримінальним кодексом Республіки Польща, на підставі аналізу відповідної кримінально-правової норми, її конституційних засад, доктринальних положень науки та доступної правозастосовної практики.

Установлено, що конфіденційність інформації міжособистісного спілкування розглядається невід'ємною складовою приватного життя особи на конституційному рівні. Відтак, основу кримінально-правової охорони такої інформації складає Конституція Республіки Польща, Загальна Декларація прав людини, Міжнародний Пакт про громадянські і політичні права, Конвенція про захист прав людини і основоположних свобод, Конвенція Ради Європи про захист осіб у зв'язку автоматичною обробкою персональних даних, Генеральний регламент ЕС про захист персональних даних (General Data Protection Regulation- GDPR), Закон РП «Про захист персональних даних» та інші нормативні джерела, зокрема й ті, які визначають підстави та межі втручання у приватне життя особи з боку органів державної влади. Наведено приклади тлумачення інформаційної автономії особи Конституційним Трибуналом Польщі, яка визнається важливою складовою права на захист приватного життя, і полягає в тому, щоби за власним рішенням розкривати інформацію про себе іншим особам, а також здійснювати контроль над інформацію, навіть якщо нею володіють інші. В межах статті проаналізовано доктрину кримінального права Польщі та правозастосовну практику щодо розуміння, передбачених ст. 267 КК Польщі форм незаконного отримання інформації, оскільки ця стаття в її чинній редакції стала результатом імплементації положень (вимог) Рамкового рішення ЄС 2005/222, які акцентують на необхідності вироблення загального підходу до складових елементів кримінальних правопорушень в сфері захисту конфіденційної інформації (персональних даних) шляхом введення загальних складів злочинів. На підставі чого зроблено висновок, що як для Польщі, так і для України актуальним питанням залишається застосування конституційних та міжнародно-правових норм, що забезпечують свободу та захист таємниці спілкування при використанні ІТ-мереж, особливо в частині необхідності узгодження конституційної охорони таємниці спілкування з безсумнівною потребою державного контролю інформації, що знаходиться в мережах, зокрема в цілях охорони державної безпеки та громадського порядку.

Ключові слова: *приватність, конфіденційна інформація, таємниця спілкування, таємниця листування, захист персональних даних, незаконне отримання інформації.*

Постановка проблеми. Науковий інтерес до моделі кримінально-правової охорони недоторканності приватного життя особи саме в Республіці Польща (далі – РП) пояснюється рядом факторів: Польща на сьогодні є членом у багатьох міжнародних організаціях та об'єднань (ООН, МВФ, Європейського Союзу, НАТО, Ради Європи, Єврозони, Вишеградської групи та інших); країна є важливим союзником нашої держави у міжнародних організаціях та регіональних об'єднаннях, а також послідовно підтримує євроінтеграційні та євроатлантичні прагнення України; між Україною та Польщею укладено більше 150 міжнародних договорів в сфері співробітництва, у тому числі, в сфері кримінального права (зокрема Договір між Україною і Республікою Польща про правову допомогу та правові відносини у цивільних і кримінальних справах, згідно з яким видача особи з метою виконання покарання відбувається

тільки у випадку вчинення діянь, які є злочинами згідно з законодавством обох країн); Польща приєдналась до загальноєвропейського регуляторного документу – Загального регламенту про захист персональних даних (GDPR), включена до переліку країн, яка забезпечує належний захист персональних даних і в 2020 році посіла 11 місце (Україна відповідно 25 місце) в Національному індексі кібербезпеки, (що є важливим фактором отримання громадянами України публічних послуг за межами України на підставі передачі персональних даних іноземним суб'єктам відносин, пов'язаних з персональними даними); наразі в Польщі за різними даними проживає більше 1 млн громадян України, які можуть стати потерпілими від порушення недоторканності приватного життя та ін.

Аналіз останніх досліджень і публікацій. В контексті порівняльного аналізу норм про захист приватності вітчизняними науковцями було досліджено кримінальне законодавство Швейцарії, Австрії, Іспанії, ФРН, Данії, Норвегії Італії [1, с. 918-920], також Модельний кримінальний кодекс США, кримінальне законодавство Іспанії, Франції, Швеції, Болгарії, згадувалися і норми кримінального кодексу РП, на підставі стислого аналізу відповідного законодавства запропоновано нову редакцію ст. 182 КК України [2, с. 139] та визнано позитивним правовим досвідом Польщі розміщення норм про охорону приватності в одному розділі та встановлення кримінальної відповідальності за незаконні дії з приватною інформацією службових осіб чи осіб, яким інформація стала відомою у зв'язку з виконанням професійного обов'язку в одній загальній нормі [3, с. 10]. Незважаючи на досить презентативну кількість компаративних досліджень в галузі кримінального права за часів незалежності України, і надалі підходи щодо їх проведення різняться (зокрема щодо визначення об'єктів порівняння, принципів, рівнів, методів, правил тощо). Адже дійсно, на практиці, використання порівняльного методу дослідження супроводжується рядом методологічних правил, які регулюють відповідну наукову діяльність [4, с. 6], а в вітчизняних компаративних кримінально-правових дослідженнях зустрічаються певні недоліки з відбором матеріалу для порівняння (вибірковість, безсистемність, обмеження лише аналізом джерельної бази, без звернення до відповідної доктрини та практики), що не йде на користь дослідженню [5, с. 37-38]. Слушність цієї думки підтверджується самою сутністю порівняльно-правового методу, який «…дозволяє вийти за межі своєї національної правової системи, проаналізувати проблеми юридичної науки та практики з кримінального права інших держав, розширити рамки юридичних пошуків, здійснити обмін правовою інформацією, науковими ідеями, врахувати як позитивний, так і негативний юридичний досвід у законотворчості й у правозастосуванні» [6, с. 35]. Зрозуміло, що рамки такого юридичного пошуку не можуть обмежуватись аналізом виключно норм кримінального законодавства будь якої країни, мають бути досліджені також доктрина та правозастосовна практика.

Отже ***мета статті*** полягає в з'ясуванні стану кримінально-правової охорона конфіденційної інформації за Кримінальним кодексом Республіки Польща, у порівнянні з Україною, на підставі аналізу відповідної кримінально-правової норми, її конституційних засад, доктринальних положень науки та доступної правозастосовної практики.

Виклад основного матеріалу. Право особи на правову охорону різних проявів приватного та сімейного життя передбачено в ряді норм Конституції РП, зокрема ст. 47 (право кожного на охорону приватного, сімейного життя, честі і доброго імені, а також рішень про своє особисте життя), ст. 49 (право на свободу та охорону таємниці комунікації), недоторканність житла (ст. 50) [7]. У рішенні від 30.07.2014 р. K 23/11 Конституційний трибунал пояснив, що конституційний орган розглядає приватне життя особи не як конституційно надане суб'єктивне право, а як захищену конституцією свободу з усіма наслідками, що звідси випливають наслідки. Перш за все, це свобода дій для окремих осіб в межах свободи, встановлених законом. Невід'ємним елементом усіх конституційних свобод людини визнається обов'язок держави поважати і захищати їх законним шляхом, а також утримуватися від втручання у свободи як з боку держави, так і приватних осіб (ст. 31 Конституції РП). Цей стандарт поширюється на усі конституційні свободи людини, зокрема особисті свободи, до яких, крім приватного життя, належать, серед іншого: свобода спілкування (ст. 49 Конституції Республіки Польща), недоторканність житла (ст. 50 Конституції Республіки Польща) або широко розуміти інформаційну автономію (Стаття 51 Конституції Республіки Польща) [8]. Отже приватність життя людини, недоторканність її житла разом із свободою спілкування визнаються складовими її свободи.

Захист таємниці спілкування не є абсолютним, проте обмеження цього особистого інтересу вимагає регулювання має бути визначено на нормативному рівні [9]. Тому, регулюючи питання свободи спілкування та його захисту, законодавець не може посилатися на загальні положення, а має конкретизувати ці обмеження та визначити спосіб їх реалізації. На це вказує судова практика Конституційного Трибуналу, який у своєму рішенні від 12.12.2005 р. зазначив, що «в межах ст. 49 Конституції Республіки Польща (свобода спілкування) ця свобода може бути обмежена у випадках, передбачених звичайним законодавством» [9]. У конструктивному розумінні таємниця листування є складовою права на недоторканність приватного життя». Як і у випадку ст. 50 і 51 Конституції РП, тлумачення ст. 49 не можна відокремити від ст. 47 Конституції РП [10, с. 258]. Відповідно до ст. 47 Конституції РП має кожен право на правовий захист особистого та сімейного життя, честі та доброго імені, приймати рішення щодо свого особистого життя. *Таємниця спілкування* визнається одним з проявів недоторканності приватного життя за ст. 47 конституції РП [11, с. 41].

Відповідно до ст. 51 Конституції РП, ніхто не може бути зобов'язаний інакше, як на підставі Закону, розголошувати відомості про особу, а ст. 51 передбачає, що органи державної влади не можуть здобувати, збирати та ділитися іншою інформацію про громадян, ніж необхідна в демократичній правовій державі. Положення ст. 51 Конституції РП виражає т. зв. інформаційна автономія. Судова практика Конституційного трибуналу наголошує на збереженні людської гідності, це вимагає поваги до його суто особистої сфери, де він не примушується до необхідності «бути з іншими» або «ділитися з іншими» своїм досвідом або відчуттями [12]. У судовій практиці Конституційний Трибунал виходить з того, що ст. 47 і 51 Конституції Республіки Польща захищають це однакову конституційну цінність, тобто сферу приватного життя. Інформаційна автономність є важливою складовою права на захист приватного життя, і воно полягає у тому, щоби за власним рішенням розкривати інформацію про себе іншим особам, а також здійснювати контроль над інформацію, навіть якщо нею володіють інші [13].

У Конституції РП вживається термін «*таємниця спілкування*», яка включає не тільки зміст повідомлень, а й факт та обставини спілкування. Конфіденційність кореспонденції як право, яке має кожна людина, захищається Конституцією Польщі, кримінальним правом, а також цивільним, авторським та адміністративним правом. Одна з класичних, традиційних свобод індивідуальна і здавна гарантована конституцією [14, с. 11].

У чинному КК РП злочин проти конфіденційності кореспонденції було перенесено до нової глави «Злочини проти захисту інформації (глава XXXIII КК), з колишньої глави XXII КК «Злочини проти свободи». Він також був описаний більш сучасно, з урахуванням технічного прогресу в галузі телекомунікацій та того, що злочини у сфері захисту персональних даних є надзвичайно поширеною і водночас дуже небезпечною формою комп'ютерної злочинності в Польщі. Зі створенням ІТ-систем виникла необхідність правового захисту інформації, що обробляється в цих системах. Така безпека визначається в доктрині за допомогою трьох основних критеріїв: доступність, цілісність і конфіденційність [14, с. 3]. Польські науковці вказують, що серед найпоширеніших злочинів, скоєних останніми роками в кіберпросторі, є зокрема й ті, що посягають на інформаційну конфіденційність, зокрема: використання електронних платіжних засобів, найчастіше це фішинг (англ. phishing), несанкціоноване отримання інформації (злом), комп'ютерне прослуховування (сніфінг) [15, с. 7].

Об'єктом охорони за § 1 ст. 267 Кримінального кодексу розуміється право розпоряджатися інформацією, що має характер суб'єктивного права, фактично інформація, не призначена для правопорушника, яка міститься в закритому листі, передається через телекомунікаційну мережу або захищена електронним, магнітним, ІТ чи іншим спеціальним способом. Мова йде про конфіденційну інформацію, конфіденційність визначається як «виключний доступ осіб, уповноважених на певну інформацію та захист даних від їх читання або копіювання неавторизованими особами» [16, с. 40-41].

Стаття 267 КК Республіки Польща передбачає відповідальність за незаконне отримання інформації в наступних формах: несанкціоноване отримання доступу до не призначеної для нього інформації шляхом відкриття закритого листа, підключення до телекомунікаційної мережі або зламу чи обходу її електронного, магнітного, ІТ чи іншого спеціального захисту (§ 1); отримання доступу до всієї ІТ-системи або її частини без авторизації (§ 2); встановлення або використання пристрою для прослуховування, візуального пристрою або

іншого пристрою чи програмного забезпечення (§ 3); розкриття інформації, отриманої у спосіб, зазначений у § 1-3, іншій особі (§4). Переслідування правопорушення, зазначеного в § 1-4, здійснюється за клопотанням потерпілої сторони (§ 5) [17].

Розглянемо доктринальні положення та практику кримінально-правової оцінки зазначених вище зазіхань на приватне життя особи через незаконне отримання інформації про особу. Щодо такої форми незаконного отримання інформації як несанкціоноване отримання доступу до не призначеної для нього інформації шляхом *відкриття закритого листа, підключення до телекомунікаційної мережі або зламу чи обходу її електронного, магнітного, ІТ чи іншого спеціального захисту* (§ 1 ст. 267 КК).

Об'єктивна сторона цього злочину полягає в отриманні доступу до не призначеної для особи інформації. В даний час в доктрині кримінального права Польщі прийнято широке розуміння поняття листування. Крім, суто листування, ним визнаються також всі способи ведення розмов (спілкування) за допомогою відомих знаків письма, малюнка, світла, засобів телекомунікації. Таким чином, захист конфіденційності листування також поширюється на сучасні засоби передачі інформації, такі як телефон, телекс, радіотелефон, магнітна стрічка, телепринтер, електронна пошта тощо. Під поняттям *отримання* польські фахівці пропонують розуміти не лише заволодіння носієм, на якому записана інформація (аркуш паперу, магнітна стрічка, плівкова стрічка, комп'ютерна флешка тощо), а й копіювання запису інформації (шляхом переписування, фотокопіювання чи копіювання запису на комп'ютерний носій) або читання інформації у спосіб, який дозволяє її зрозуміти [18].

Порушення конфіденційності листування може відбуватися різними способами. Воно може полягати в неправомірному ознайомленні з кореспонденцією, адресованою іншої особи (розкриття та читання чужого листа), захоплення та привласнення чужої кореспонденції, знищення чужої кореспонденції, розповсюдження чужої кореспонденції, вторгнення в систему електронного зв'язку. Порушення конфіденційності кореспонденції може полягати в розповсюдженні кореспонденції без згоди одержувача, навіть якщо відправник поширює свою кореспонденцію. Охорона кореспонденції надається не тільки адресату кореспонденції, а й її відправнику (автору). Відправник, направляючи кореспонденцію конкретному адресату, має право розраховувати на те, що адресат дотримуватиметься принципу конфіденційності та зберігатиме в таємниці отриману з кореспонденції інформацію, що стосується сфери його приватного життя [19, с. 180]. Тому для поширення потрібна їхня згода обох [20].

Відкриті форми спілкування, тобто листівки, та ті, що передаються по радіо на загальнодоступній частоті, не охороняються, оскільки наявність таємниці листування передбачає приховування повідомлення від третіх осіб, крім адресата у спосіб, який зазвичай перешкоджає доступу до інформації, що міститься в листі, наприклад, шляхом склеювання, зшивання, запечатування конверта, використання власної радіочастоти або коду. Зокрема, Верховний суд Польщі в своєму рішенні від 3 лютого 2004 р., II KK 388/02, зазначив, що «Хоча ст. 267 КК РП кримінальним порушенням таємниці листування має лише відкриття «закритих листів», однак ці положення визначають аксіологічний напрямок дій з усім листуванням. Широко використовується в етичних термінах і суспільно прийнятим є принцип не читати чужу кореспонденцію, навіть якщо остання у формі листівок» [21]. Також Верховний Суд РП наголосив, що суть злочину, передбаченого ст. 267 § 1 КК РП полягає в отриманні інформації, не призначеної для винного [22, с. 128].

В доктрині існує позиція, що КК Польщі не захищає кореспонденцію, яка вже була доставлена, відповідальність винного за порушення таємниці кореспонденції поширюється лише на ситуації, коли порушення сталося до того, як адресат ознайомився зі змістом його листа. Утім пані Дудка вважає таку позицію помилковою, оскільки змістом предмету охорони в такому разі є не право власності на лист, а право, яке за своїм змістом існує незалежно від того, чи знав адресат цей зміст чи ні [23, с. 83].

Захист таємниці спілкування, що стосується як письмового, так і електронного листування, тісно пов'язаного з конфіденційністю зазначеного між конкретними особами і передбачає зокрема: заборону примушувати адресатів до розкриття змісту отриманих ними повідомлень; заборону спроби отримання інформації про цей контент без згоди адресата (це стосується всіх суб'єктів, включаючи органи влади публічний); захист самого факту того, що хтось взагалі є адресатом певних повідомлень. Таким чином, «таємниця спілкування» полягає у «приховуванні змісту повідомлення (інформації, вислов-

лювань, зізнань, вражень, почуттів тощо) від інших осіб, які не є обраним автором повідомлення адресатом (іншими адресатами). Йдеться не про таємницю, що міститься у змісті повідомлення, а про ставлення до цього змісту людей, які спілкуються. Це породжує розрізнення між конфіденційним спілкуванням та загальнодоступною міжособистісною комунікацію. Отже конфіденційність міжособистісного спілкування визначається волею сторін. У зв'язку з таким розумінням, як і в кримінальному праві України, актуалізується питання яким чином і в якій формі має відбуватись подібне волевиявлення суб'єктів листування.

Польські науковці зауважують, що «в актах міжнародного права вживається поняття таємниці листування, а не спілкування. Положення ст. 17 МПГПП передбачає, що «ніхто не може зазнавати свавільного чи незаконного втручання в його особисте життя, сім'ю, недоторканність житла чи кореспонденції, а також незаконних нападів» за його честь і добре ім'я». Тоді як ст. Стаття 8 ЄКПЛ говорить, що «кожен має право на повагу до свого особистого та сімейного життя, дому і ваше листування» (пункт 1). Кореспонденція захищена з метою запобігання несанкціонованому перехопленню повідомлень (повідомлень, що надсилаються через неї) та забезпечення досягнення інформації адресатом [24, с. 99].

Виходячи і з того, і з іншого, в країні склалася багата судова практика, яка розуміє поняття кореспонденції якомога ширше [25, с. 12]. Так, в рішенні районного суду у Білостоці № VII K 922/14 від 22.04.2015 р., зазначається, що захист також поширюється на електронну пошту – «(...) отже, чи листування є письмовим і міститься у закритому листі або чи є воно в електронній формі та міститься в особистих даних облікового запису іншої особи на сайті соціальної мережі, це не має значення для висновку, що воно підлягає захисту відповідно до ст. 267 § 1 КК [26]. Вищезазначене з очевидністю демонструє широке розуміння поняття «відкриття закритого листа» як способу несанкціонованого отримання доступу до не призначеної для особи інформації, відповідно до тенденцій тлумачення сутності таємниці листування в міжнародно-правових документах, і в кримінально-правові доктрині Польщі і в правозастосовній (судовій) практиці.

Наступними способами несанкціонованого отримання доступу до інформації закон визнає *підключення до телекомунікаційної мережі або злам чи обхід її електронного, магнітного, IT чи іншого спеціального захисту.* Підключення до телекомунікаційної мережі – в якості нормативного джерела визначення цього поняття посилаються на п. 35 ст. 2 «Закону про телекомунікації» Республіки Польща, за яким телекомунікаційної мережі це «системи передачі та пристрої комутації або перенаправлення, а також інші ресурси, включаючи неактивні елементи мережі, які дозволяють передачу, прийом або передачу сигналів за допомогою проводів, радіохвиль, оптичних хвиль або інших засобів з використанням електромагнітної енергії, незалежно свого типу» [27]. Мова йде як про дротові з'єднання, так і бездротові або оптичні з'єднання як еквівалентні. Під час підключення до мережі мережева карта (і, отже, користувач) отримує багато детальних параметрів (які є інформацією) щодо її конфігурації, необхідних для того, щоб зв'язок взагалі був можливим. Серед них, зокрема, IP-адреса з маскою підмережі, призначена маршрутизатором (точніше встановленим на ньому сервером DHCP), адреси DNS- серверів, час оренди адреси, призначеної DHCP-сервером (тобто період, протягом якого ми отримуємо задану IP-адресу від маршрутизатора під час підключення до бездротової мережі), MAC-адресу маршрутизатора (що, у свою чергу, дозволяє перевірити, що виробник пристрою, що може бути важливим при спробі зламати безпеку самого маршрутизатора) або, нарешті, інформацію про Інтернет-провайдера, який підтримує з'єднання. Уся ця інформація має кваліфікуватися як інформація, отриманню якої має передувати згода адміністратора, а отримання без його згоди (шляхом підключення до бездротової мережі) безсумнівно виконує характер «отримання доступу до інформації», передбачений § 1 ст. 267 КК Польщі [28].

Останнім зазначеним в ст. 267 § 1 способом вчинення цього злочину є обхід безпеки, що полягає в тому, що винний не зламує систему безпеки, а обходить її. Злам безпеки є лише одним із багатьох методів (і навіть не найпоширенішим), які використовують хакери для проникнення в систему комп'ютера і може проявлятись в наступних формах: введення людини в оману (соціальна інженерія, тобто соціальна інженерія, що полягає, наприклад, у видаванні іншої особи з метою вимагання паролю або доступу до приміщення, де знаходиться сервер, і фізичне підключення до нього); введення системи в оману – серед методів обходу заходів безпеки таким способом, т.зв. спуфінг, тобто

підробка адреси з метою введення в оману про те, куди надсилати повідомлення. Найчастіше фальсифікуються IP-адреси користувачів (логічна адреса комп'ютера, яку призначає адміністратор мережі), але також можна підробити, наприклад, адреси WWW (щоб спрямування жертви на веб-сайт, створений злочинцем, наприклад, який видає себе за веб-сайт банку); використання вразливостей (багів) в операційних системах, додатках або протоколи (це набори правил, що визначають комунікаційні процеси що відповідає, серед інших для ідентифікації комп'ютерів у мережі), для чого вони призначені програми під назвою exploits [29, с. 168-176]. Подібні проблеми характерні і для України, адже як вказують фахівці з інформаційної безпеки, «найбільш поширеними напрямами загроз інформаційній безпеці є шахрайські шкідливі платіжні програми, що ускладнюють, порушують або блокують роботу банківських терміналів, використовуються для крадіжки даних громадян, взлому паролей від банківських карток для заволодіння коштами цих громадян…» [30, с. 115]. Правопорушення, передбачене ст. 267 § 1 КК Польщі має загальний характер. Воно може бути вчинене будь-якою особа, яка може нести кримінальну відповідальність і не є власником інформації.

Отримання доступу до всієї IT-системи або її частини без авторизації, передбачене диспозицією § 2 ст. 267 КК Польщі утворює склад, так званого хакерства, що полягає в несанкціонованому проникненні (зломі) в комп'ютерну систему чи мережу [31]. Простого підключення без авторизації до незахищеної телекомунікаційної мережі, на думку фахівців, «очевидно, недостатньо для здійснення ознак забороненої дії, описаної в ст. 267 § 2 Кримінального кодексу також необхідний «доступ до інформації», який є результатом такої поведінки», під яким розуміють створення можливості ознайомлення з інформацією [32].

В той же час інші польські дослідники акцентують увагу, що положення ст. 267 § 2 КК Польщі досить місткі за змістом і задаються питанням, чи не намагався таким чином законодавець створити основний вид хакерського злочину (ст. 267 § 2 Кримінального кодексу) та його кваліфікований вид (ст. 267 § 1 Кримінального кодексу), що вимагає дії, що полягає в подоланні безпеки, а отже – дії, більш суспільно шкідливої. І надалі припускають, що положення ст. 267 § 2 КК буде застосовуватися у випадках, коли основним елементом діяння винного був простий доступ до всієї інформаційної системи або її частини, а не отримання доступу до інформації (наприклад, у разі злому облікового запису на аукціоні з метою використання вчинення злочину шахрайства, доступ до профілю на порталі соціальної мережі, а потім зміна даних, що містяться в ній) [22, с. 132]. Головною умовою притягнення особи до кримінальної відповідальності за статтею 267 § 2 Кримінального кодексу є отриманні доступу до системи без дозволу. Прикладом такого зламу є наступний випадок з судової практики. Будучи одруженим, J. використовував для приватних цілей обліковий запис електронної пошти, створений для облікового запису електронної пошти своєї дружини. Після розлучення для безпечного використання електронної пошти, колишня дружина ввела нові ідентифікатор користувача та пароль автентифікації (…), які нікому не повідомляла. Під час перебування в цій квартирі використовуючи невизначене шпигунське програмне забезпечення, J. розшифрував пароль електронної пошти своєї дружини і таким чином, зламавши захист, отримав доступ до її електронної скриньки. Розшифрувавши пароль, він увійшов у систему та отримав, не маючи авторизації, доступ до не призначеної для нього інформації, що міститься в електронній скриньці його колишньої дружини. Потім він скопіював її листування з CJ (...) і PS. ((...)). Як було встановлено, він робив це багато разів, при цьому також копіював файли з різних документів та її приватне листування електронною поштою. Про те, що відповідач зламав захист у вигляді пароля, який необхідно було ввести для входу в обліковий запис електронної пошти, потерпіла дізналася під час другого слухання в окружному суді у справі про розлучення. Тоді представник обвинуваченого, як відповідача, надав до суду лист, з якого вбачається, що це листування між потерпілою та її новим партнером. Щоб дістатися до цієї кореспонденції, обвинувачений мав потрапити на електронну скриньку жертви, а отже, зламати пароль [33].

Встановлення або використання пристрою для прослуховування, візуального пристрою або іншого пристрою чи програмного забезпечення (§ 3 ст. 267 КК Польщі). Положення ст. 267 § 3 КК РП санкціонує конституційні гарантії права на захист приватне життя (ст. 47 Конституції), свободи спілкування та захисту таємниці цього спілкування (ст. 49 Конституції), а також недоторканність житла (ст. 51 Конституції). На підставі цієї статті можуть визнаватися

протиправними ряд дій, пов'язаних з втручанням у приватне життя. Наприклад, порушення безоплатного користування квартирою шляхом спостереження з використанням підслуховувальних чи візуальних пристроїв або перехоплення інформації, надісланої через телекомунікаційну мережу [34, с. 57]. Не викликає в польських науковців сумніву, що з огляду на положення ст. 267 § 3 КК можна розглядати дії хакера, що полягають у встановленні програми на комп'ютері особи, яка відстежує передачу даних, таких як: троянський кінь (trojan); програма «back door» [22, с. 134].

Встановлення зображення або звукозаписувального пристрою з метою перехоплення інформації про перебіг розмови є забороненим діянням, ознаки якого визначені ст. 267 § 3 Кримінального кодексу, зазначається в Постанові Верховного Суду Республіки Польща від 27 квітня 2016 р., III KK 265/15) [35]. Натомість запис розмови між двома особами в громадському місці, яку могли чути без будь-яких перешкод й інші люди, не містить ознак цього злочину [36].

Загальні ознаки засобів вчинення цього злочину, наведені в диспозиції ст. 267 § 3 КК РП, дозволяють визнавати такими не лише пристрої, спеціально призначені для отримання інформації під час процесу зв'язку, але й будь-які пристрої, за допомогою яких можна отримати інформацію [37, с. 442], тобто будь-якого пристрою, який використовується для запису зображення або звуку, і тому призначений для цієї мети аналоговий або цифровий пристрій, наприклад фотоапарат, магнітофон, диктофон [38, с. 4]. Властивості цієї форми порушення конфіденційності вичерпуються встановленням або використанням підслуховуючого пристрою, візуального чи іншого спеціального пристрою з метою несанкціонованого отримання інформації. Відповідні дії можуть вчинятися тільки на основі закону компетентними органами (правоохоронні органи, прокуратура, суду) за наявності до того підстав.

Заборонене діяння, визначене ст. 267 § 4 Кримінального кодексу полягає в розкритті іншій особі відомостей, отриманих у спосіб, описаний у ст. 267 § 1-3 Кримінального кодексу. Суб'єктом цього злочину є будь яка особа, яка надає незаконну інформацію, знаючи про її джерело походження (тобто не лише виконавець злочину згідно зі ст. 267 § 1, § 2 або § 3 Кримінального кодексу, який отримав це безпосередньо).

Висновки. Як і в Україні основу кримінально-правової охорони конфіденційності інформації, спілкування як невід'ємних складових приватного життя особи складають Конституція Республіки Польща, Загальна Декларація прав людини (стаття 12), Міжнародний Пакт про громадянські і політичні права (стаття 17), Конвенція про захист прав людини і основоположних свобод (стаття 8), Конвенція Ради Європи про захист осіб у зв'язку автоматичною обробкою персональних даних, Генеральний регламент ЕС про захист персональних даних (General Data Protection Regulation, GDPR), Закон РП «Про захист персональних даних». Важливим практичним висновком польських науковців є той, що тлумачення положень ст. 267 КК Республіки Польща, пов'язані з відповідальністю за поведінку в Інтернеті в широкому розумінні та спрямовані на інформаційну безпеку, не повинні проводитися окремо від такої динамічно змінної технологічна реальність, яка вимагає постійного пошуку та опису нових форм зазіхань на конфіденційну інформацію в контексті захисту приватного життя людини. Варто погодитися з думками польських колег, які вважають, що стосовно цього виду злочину кримінальне право повинно допускати певний ступінь гнучкого тлумачення, щоб гарантувати, що ці положення фактично застосовуються до технологічної реальності, яка постійно випереджає законодавця, що допускає порушення законно охоронюваних благ, іноді невідомими нам способами. Актуальним питанням залишається застосування конституційних та міжнародно-правових норм, що забезпечують свободу та захист таємниці спілкування при використанні ІТ-мереж, особливо в частині необхідності узгодження конституційної охорони таємниці спілкування з безсумнівною потребою державного контролю інформації, що знаходиться в мережах, зокрема в цілях охорони державної безпеки та громадського порядку.

Цінним висновком аналізу польської кримінально-правової доктрини можна визнати те, що, як і вітчизняні фахівці, польські науковці нарікають на проблемах, пов'язаних з імплементацією положень міжнародних актів в національне законодавство. Так, вони вважають, що ряд поправок, внесених до ст. 267 КК Польщі в 2008 році, зокрема § 2 – положення про кримінальну відповідальність діяння винного, що полягає в отриманні несанкціонованого доступу до всіх або частини інформаційної системи, є фактично автоматичним й буквальним переписуванням змісту ст. 2 Рамкового рішення 2005/222, в п. 11 якого зазначено на необхідності вироблення загального підходу до складових елементів кри-

мінальних правопорушень шляхом введення таких загальних складів злочинів як: незаконний доступ до інформаційної системи, недоторканність системи та порушення недоторканності даних. Сутність критичних зауважень першочергово зводиться до того, що національний законодавець має імплементувати правові норми, а не нормативні акти, а відтак рамкові рішення гармонізують матеріальне кримінальне право не підходять для дослівної транспозиції до тексту КК. Ураховуючи активну роботи над текстом нового Кримінального кодексу України, вважаємо подальші наукові дослідження проблеми кримінально-правової охорони конфіденційної інформації особи з метою забезпечення охорони її приватного життя в країнах, які раніше почали процес гармонізації власного кримінального законодавства до вимог міжнародно-правових стандартів у сфері захисту персональних даних, вельми цінним для України.

Список використаної літератури:

1. Хавронюк М.І. Кримінальне законодавство України та інших держав континентальної Європи: порівняльний аналіз, проблеми гармонізації. Монографія. К.: Юрисконсульт, 2006. 1048 с.
2. Yuliia Khrystova, Valentyn Liudvik. Foreign experience of criminal legal protection of privacy. *Scientific Bulletin of Dnipropetrovsk State University of Internal Affairs*. 2021. Special Issue № 1. P. 136-139.
3. Горпинюк О.П. Кримінально-правова охорона інформаційного аспекту приватності в Україні. Автореф. дис. на здоб. наук. ступ. канд. юрид. наук за спец. 12.00.08. Львівський державний університет внутрішніх справ. Львів, 2011. 20 с.
4. Хавронюк М.І. Компаративний метод у сучасному кримінально-правовому дослідженні: мета застосування. *Право.ua*. Вип. 1. 2017. С. 5-9.
5. Туляков В.О. Порівняльний метод у науці кримінального права. Правова доктрина України: у 5 т.: Кримінально-правові науки Україні: стан, проблеми та шляхи розвитку / За заг. ред. В. Я. Тація, В. І. Борисова. Харків : Право, 2013. Т. 5. С. 30-40.
6. Панов М.І. Проблеми методології науки кримінального права : вибр. наук. пр. Харків: Право. 2018. 472 с.
7. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. URL: https://www.sejm.gov.pl/prawo/konst/polski/kon1.htm
8. Wyrok TK z 30.7.2014 r., K 23/11. URL: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20140001055/T/D20141055TK.pdf
9. Wyrok TK z 12.1.2000 r., P11/98 URL: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20000030046/T/D20000046L.pdf
10. Recenzje Konstytucja RP. Red. Marek Safjan, Leszek Bosek t. I, Komentarz do art. 1–86. *Przegląd Sejmowy.* 6 (143). 2017. s. 257-264.
11. Jabłoński, M, Wygoda, K. Dostęp do informacji i jego granice, Wrocław 2002, 326 s.
12. Wyrok TK z:12.12.2005 r., K 32/04. URL: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20052502116/T/D20052116TK.pdf
13. Wyrok TK z: 19.2.2002 r., U 3/01. URL: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20020560763/T/M20020763TK.pdf
14. Jarosz-Żukowska Sylwia. Konstytucyjnoprawne aspekty ochrony tajemnicy komunikowania się w internecie. *Przegląd Prawa i Administracji* 78, 2008. s. 12-29.
15. H. Fedewicz, V. Paleolog-Demetraki. Cyberprzestępczość – nowym rodzajem zagrożeń dla bezpieczeństwa państwa. *Теоретичні та практичні засади протидії злочинності в сучасних умовах*: тези доповідей та повідомлень учасників Міжнародної науково-практичної конференції 16 жовтня 2015 р. Львів: Львівський державний університет внутрішніх справ, 2015. С. 5-9.
16. Prawo karne komputerowe / Andrzej Adamski. Autorzy: Adamski, Andrzej. Wydano: Warszawa : Wydaw. C. H. Beck, 2000. s. 40–41
17. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny. URL:https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970880553/U/D19970553Lj.pdf
18. Bogacki Piotr. Hacking w ujęciu art. 267 KK. *Monitor Prawniczy* | 2013. № 17. URL:https://czasopisma.beck.pl/monitor-prawniczy/artykul/emhackingem-wujeciu-art267-kk/
19. Agnieszka Kubiak-Cyrul. Dobra osobiste osób prawnych. Kantor Wydawniczy "Zakamycze", 2005. 299 s
20. Prawo cywilne część ogólna, red. Marek Safjan, t. 1. 215-236. Warszawa: Wydawnictwo C.H. Beck. Serwin, Bożena. 2012. s. 1135.
21. W y r o k imieniu Rzeczypospolitej Polskiej. Sygn. akt II KK 388/02. Dnia 3 lutego 2004 r. URL: http://www.sn.pl/sites/orzecznictwo/Orzeczenia2/II%20KK%20388-02.pdf
22. Filip Radoniewicz. Odpowiedzialność karna za przestępstwo hackingu. *Prawo w działaniu sprawy karne* . 2013. № 13. S. 121-128.
23. K. Dudka. Ochrona prawa do prywatności i jej ograniczenia w polskim prawie karnym. *Czasopismo Prawa Karnego i Nauk Penalnych.* 2000. № 4. S. 83.
24. Hofmański P., Komentarz do wybranych przepisów Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności [w:] E. Zielińska (red.), Standardy prawne Rady

Europy. Tekst i komentarze. T. 3, Prawo karne, Oficyna Naukowa, Warszawa 1997. 368 s.
25. Jarosz-Żukowska Sylwia. Konstytucyjnoprawne aspekty ochrony tajemnicy komunikowania się w internecie. *Przegląd Prawa i Administracji*. 2008. 78. S. 11-29.
26. Sygn. akt VII K 922/14 WYROK Dnia 22 kwietnia 2015 roku. Sąd Rejonowy w Białymstoku. URL:https://www.saos.org.pl/judgments/151214
27. U S T AWA z dnia 16 lipca 2004 r. Prawo telekomunikacyjne1 https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20041711800/U/D20041800Lj.pdf
28. AdamBehan.Współczesnesystemyinformatyczne a typy przestępstw z art. 267 kodeksu karnego Palestra 2/2020. 21-36. URL:https://palestra.pl/pl/czasopismo/wydanie/2-2020
29. F. Radoniewicz. Odpowiedzialność karna za hacking i inne przestępstwa przeciwko komputerowym i systemom informatycznym, Warszawa 2016, S. 278-282.
30. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внут. справ, 2020. 144 с.
31. Sparrow Włodzimierz , Zoll Andrzej. Kodeks karny. Część Specjalna. T. II. Komentarz do art. 117-277D VIP. 5. Wolters Kluwer SA. 2017. 1884 s.
32. Kodeks karny Komentarz / redakcja naukowa Tadeusz Bojarski Tadeusz Bojarski, Aneta Michalska-Warias Joanna Piórkowska-Flieger, Maciej Szwarczyk. Wolters Kluwer. Warszawa 2016. S. 794-800.
33. Rozwód, włamanie i logowanie na konto e-mail żony albo męża. URL: https://kancelaria-prawo-rodzinne.com/wlamanie-logowanie-konto-e-mail
34. Adamski A. Prawo karne. C.H. Beck, 2000. 269 s.
35. Postanowienie Sądu Najwyższego z dnia 27 kwietnia 2016 r. II KK 265/15. URL: http://www.sn.pl/sites/orzecznictwo/Orzeczenia3/III%20KK%20265-15.pdf
36. Postanowienie Sądu Apelacyjnego w Gdańsku z dnia 28 września 2016 r., II AKa 111/16).
37. Sakowicz A. Kodeks karny. Część szczególna. Komentarz. Tom II, pod red. M. Królikowskiego i R. Zawłockiego, Wydawnictwo CH Beck, 2013. S. 410-456.
38. Postanowienie dnia 27 kwietnia 2016 r Sygn. akt III KK 265/15. URL: http://www.sn.pl/sites/orzecznictwo/Orzeczenia3/III%20KK%20265-15.pdf

Stomatov E. H. Criminal law protection of confidential information under the Polish Penal Code (on the example of Article 267 of the Penal Code)

The article analyzes the state of criminal law protection of confidential information under the Polish Penal Code based on the analysis of the relevant criminal law norm, its constitutional foundations, doctrinal provisions of science and available law enforcement practice.

It is found that confidentiality of interpersonal communication information is considered to be an integral part of a person's private life at the constitutional level. Therefore, the basis for criminal law protection of such information is the Constitution of the Republic of Poland, the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the Convention for the Protection of Human Rights and Fundamental Freedoms, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the EU General Data Protection Regulation (GDPR), the Personal Data Protection Act of the Republic of Poland on and other regulatory sources, including those that define the grounds and limits of interference with a person's private life by public authorities. The article provides examples of the interpretation of information autonomy of a person by the Constitutional Tribunal of Poland, which is recognized as an important component of the right to privacy, and consists in the right to disclose information about oneself to other persons at one's own discretion, as well as to exercise control over information, even if it is possessed by others. The article analyzes the doctrine of Polish criminal law and law enforcement practice with regard to understanding the forms of illegal obtaining of information provided for in Article 267 of the Polish Penal Code, since this Article in its current edition is the result of implementation of the provisions (requirements) of the EU Framework Decision 2005/222, which emphasize the need to develop a common approach to the constituent elements of criminal offenses in the field of protection of confidential information (personal data) by introducing general corpus delicti. On this basis, the author concludes that for both Poland and Ukraine, the application of constitutional and international legal norms ensuring freedom and protection of the secrecy of communication when using IT networks remains a topical issue, especially with regard to the need to reconcile the constitutional protection of the secrecy of communication with the undoubted need for state control over information contained in networks, in particular for the purposes of protecting state security and public order.

Key words**:** *privacy, confidential information, secrecy of communication, secrecy of correspondence, protection of personal data, illegal obtaining of information.*