

**БАЛАНС МІЖ ПРАВОМ НА БЕЗПЕКУ І ПРАВОМ НА ПРИВАТНІСТЬ:
ТЕОРЕТИЧНИЙ АНАЛІЗ У КОНТЕКСТІ ЦИФРОВОЇ ЕПОХИ****BALANCE BETWEEN THE RIGHT TO SECURITY AND THE RIGHT TO PRIVACY:
A THEORETICAL ANALYSIS IN THE CONTEXT OF THE DIGITAL ERA**

**Добкіна К.Р., д.ю.н., професор,
заступник директора**

Навчально-науковий

інститут управління, технологій та правових наук

Національного транспортного університету

ORCID ID: 0000-0003-2627-8871

У цифрову епоху фундаментальні права людини – зокрема право на приватність – зазнають значних трансформацій під впливом технологічного прогресу та зростання ролі приватних корпорацій у сфері регулювання інформаційного простору. Традиційна модель, за якою держава виступає єдиним гарантом безпеки і прав людини, поступово втрачає монополію: цифрові платформи дедалі частіше виконують функції, що раніше належали виключно державним інституціям.

Корпорації, які володіють інфраструктурою для збору, обробки та модерації даних, фактично формують власні нормативні порядки – правила поведінки, алгоритми контролю, стандарти доступу. Відповідна діяльність має ознаки «цифрового суверенітету», що дозволяє говорити про появу нових суб'єктів регуляторної влади. У цьому контексті постає питання: чи можуть приватні платформи бути визнані суб'єктами правозахисної відповідальності?

Стаття присвячена аналізу трансформації правового статусу приватних корпорацій у цифрову епоху, зокрема їхньої участі у регулюванні прав на безпеку та приватність. У фокусі – зсув від державної монополії на гарантування прав людини до ситуації, коли цифрові платформи фактично виконують квазі-нормативні функції.

Сучасна правова доктрина лише частково реагує на ці виклики. Відсутність чіткої моделі відповідальності корпорацій за порушення цифрових прав, нечіткість меж їхньої правосуб'єктності та достатньо слабка інтеграція етичних критеріїв у правову оцінку їхньої діяльності створюють нормативну прогалину. Автором пропонується доктринальна категорія «приватного регулятора з публічною відповідальністю» – як інструмент правового осмислення меж корпоративної дії у сфері фундаментальних прав.

У підсумку зроблено висновок, що цифрове середовище потребує оновлення правових підходів, які враховують не лише технічні аспекти, а й трансформацію владних повноважень у руках недержавних суб'єктів. Разом з тим, формування нової законодавчої рамки має ґрунтуватися на принципах прозорості, підзвітності та прав людини як вищої цінності цифрового порядку.

Ключові слова: права людини, цифрові права, приватність, безпека, корпорації, правозахисна відповідальність, цифровий суверенітет, публічна відповідальність, захист прав людини, міжнародні стандарти.

In the digital age, fundamental human rights – in particular, the right to privacy – are undergoing significant transformations under the influence of technological progress and the growing role of private corporations in regulating the information space. The traditional model, in which the state acts as the sole guarantor of security and human rights, is gradually losing its monopoly: digital platforms are increasingly performing functions that previously belonged exclusively to state institutions.

Corporations that own the infrastructure for collecting, processing, and moderating data are effectively forming their own regulatory frameworks – rules of conduct, control algorithms, and access standards. Such activities have the characteristics of “digital sovereignty,” which suggests the emergence of new regulatory authorities. In this context, the question arises: can private platforms be recognized as subjects of legal responsibility?

This article analyzes the transformation of the legal status of private corporations in the digital age, in particular their participation in regulating the rights to security and privacy. The focus is on the shift from a state monopoly on guaranteeing human rights to a situation where digital platforms effectively perform quasi-regulatory functions.

Contemporary legal doctrine only partially responds to these challenges. The absence of a clear model of corporate liability for violations of digital rights, the vagueness of the boundaries of their legal personality, and the rather weak integration of ethical criteria into the legal assessment of their activities create a regulatory gap. The author proposes the doctrinal category of a “private regulator with public responsibility” as a tool for legal understanding of the limits of corporate action in the sphere of fundamental rights.

The conclusion is that the digital environment requires an update of legal approaches that take into account not only technical aspects but also the transformation of power in the hands of non-state actors. At the same time, the formation of a new legislative framework should be based on the principles of transparency, accountability, and human rights as the highest value of the digital order.

Key words: human rights, digital rights, privacy, security, corporations, human rights accountability, digital sovereignty, public accountability, human rights protection, international standards.

Постановка проблеми. У сучасному правовому порядку, що формується під впливом цифрової трансформації, відбувається докорінна зміна суб'єктного складу гарантування прав людини. Якщо класична теорія держави і права виходила з презумпції, що саме держава є головним носієм обов'язку щодо захисту прав на безпеку і приватність, то в умовах цифрової епохи ці функції дедалі частіше реалізуються – або порушуються – приватними корпораціями, насамперед технологічними. При цьому правова доктрина не виробила узгодженого підходу до визначення меж відповідальності таких суб'єктів, їх

правового статусу, а також критеріїв легітимності їхньої діяльності у сфері обробки даних, алгоритмічного управління та цифрового нагляду.

Особливої складності набуває проблема правового балансу між безпекою та приватністю, коли корпоративні платформи фактично здійснюють регуляторну функцію, встановлюючи правила доступу, модерації, збору та використання інформації без належного демократичного контролю. Водночас, національні правові системи демонструють фрагментарність у регулюванні цього питання, а міжнародні стандарти – зокрема, Guiding Prin-

ciples on Business and Human Rights – залишаються рекомендаційними, не створюючи обов'язкових механізмів відповідальності.

У цьому контексті постає низка невирішених теоретичних і прикладних питань: чи можуть приватні корпорації вважатися суб'єктами правозахисної відповідальності? Які межі їхнього втручання в особисту сферу є допустимими з точки зору конституційного права? Які критерії добросовісності мають застосовуватися до їхньої діяльності?

Очевидна відсутність системного теоретичного осмислення цих питань у вітчизняній доктрині, а також нормативна невизначеність у міжнародному праві, зумовлюють необхідність всебічного дослідження ролі приватних корпорацій у гарантуванні та порушенні прав на безпеку і приватність, з метою формування нової правової парадигми, що відповідатиме викликам цифрової епохи.

Стан опрацювання. В межах української правової доктрини проблема ролі приватних корпорацій у гарантуванні або порушенні прав на безпеку і приватність досліджується переважно в контексті конституційного права, інформаційного права, цифрової безпеки та прав людини. Так, В. Шаповал аналізує межі допустимого втручання держави в особисту сферу, акцентуючи на конституційних гарантіях приватності, що опосередковано стосується і діяльності приватних суб'єктів, які діють за делегованими повноваженнями [1]. Б. Фасій аналізує взаємозв'язок між захистом персональних даних і національною безпекою, наголошуючи на ризиках цифрового середовища та необхідності правового реагування на діяльність приватних операторів даних [2]. О. Довгань, своєю чергою, розглядає участь приватного сектору в забезпеченні цифрової стійкості, зокрема в контексті транснаціональних ризиків, алгоритмічного управління та нормативної фрагментації [3]. О. Коваленко та О. Тихомиров досліджують трансформацію поняття приватності в цифрову епоху, аналізуючи вплив технологій Big Data та цифрових платформ на інформаційну автономію особи [4]. Тим не менш, попри наявність окремих досліджень, в українській доктрині відсутня системна концептуалізація приватних корпорацій як суб'єктів правозахисної відповідальності, що створює прогалину в теоретичному обґрунтуванні їх статусу.

Разом з тим, у зарубіжній доктрині проблема ролі корпорацій у сфері прав людини досліджується значно глибше, хоча й не без суперечностей. Зокрема, S. Zuboff обґрунтовує тезу про трансформацію приватності в товар, що підриває автономію особи в умовах цифрового ринку [5]. L. Lessig доводить, що цифровий код є формою регулювання, що не менш впливова, ніж закон, і тому має бути предметом правового контролю [6]. J. Cohen пропонує концепцію контекстуальної приватності, яка враховує соціальні та технологічні чинники, що формують індивідуальну автономію [7]. Нарешті, у рамках ініціативи ООН Guiding Principles on Business and Human Rights визнається обов'язок бізнесу поважати права людини, хоча ці принципи залишаються рекомендаційними [8]. Водночас слід звернути увагу, що основними невирішеними питаннями залишаються: відсутність обов'язкової правової моделі відповідальності корпорацій, нечіткість меж їхньої правосуб'єктності у сфері прав людини, а також недостатня інтеграція етичних критеріїв у правову оцінку їхньої діяльності. Очевидним є і те, що наведені аспекти потребують доктринального осмислення та нормативного закріплення.

Метою статті є здійснення аналізу трансформації ролі приватних корпорацій у сфері гарантування та порушення прав на безпеку і приватність у цифрову епоху, з урахуванням зміни суб'єктного складу правозахисної відповідальності, еволюції технологічних ризиків та нормативної фрагментації міжнародних стандартів. Стаття спрямована на виявлення теоретичних прогалин у вітчизняному та зарубіжному праві, обґрунтування необхідності перео-

смислення меж правосуб'єктності недержавних суб'єктів, а також формулювання концептуальних засад для розробки нормативної моделі цифрової добросовісності як критерію легітимності корпоративної діяльності в контексті прав людини.

Виклад основного матеріалу. У сучасній теорії держави і права дедалі більшої уваги набуває проблема співвідношення права на безпеку та права на приватність, що постає як одне з найважливіших питань у добу цифрової трансформації. Окреслені два права, хоча й мають спільну мету – забезпечення гідності особи, – нерідко вступають у конфлікт, особливо в умовах посилення державного контролю, алгоритмічного управління та зростання ризиків кіберзагроз. Принагідно зауважимо, що класичні моделі правового балансу, сформовані в епоху індустріального суспільства, виявляються недостатніми для пояснення нових форм втручання, які не мають фізичних меж, але мають глибокі наслідки для автономії особи.

В даному аспекті варто звернутися до концепції Е. Бекенаферде, який стверджував, що держава є одночасно умовою і загрозою свободи. Його теза про «парадокс свободи» є надзвичайно релевантною для аналізу балансу між безпекою та приватністю, оскільки вона висвітлює, що будь-яке посилення безпекових механізмів потенційно містить ризик надмірного втручання в особисту сферу [9]. Водночас, погоджуючись із загальним напрямом думки автора, вважаємо за необхідне уточнити, що в умовах цифрової епохи держава не лише загрожує свободі, а й делегує частину своїх повноважень приватним технологічним корпораціям, які фактично здійснюють квазі-державне регулювання приватності [5, с. 502].

Конституція України від 28.06.1996 р. гарантує кожному право на невтручання в особисте і сімейне життя, а також захист персональних даних (ст. 32) [10]. Водночас допускається обмеження цього права в інтересах національної безпеки – за умови дотримання принципів законності, необхідності та пропорційності. У контексті цифрової трансформації ці положення набувають особливої актуальності, оскільки приватні суб'єкти дедалі частіше виконують функції, що раніше були виключно державною прерогативою.

В той же час Закон України «Про захист персональних даних» від 01.06.2010 р. №2297-VI [11] встановлює обов'язки як державних, так і приватних розпорядників даних щодо забезпечення конфіденційності, безпеки та прав суб'єктів. Проте Закон не містить чіткої моделі відповідальності транснаціональних корпорацій, що діють поза межами української юрисдикції, створюючи тим самим нормативну прогалину в контексті глобального цифрового ринку. Своєю чергою, Закон України «Про електронні комунікації» від 16.12.2020 р. №1089-IX [12] передбачає обов'язки провайдерів щодо збереження трафіку, доступу до даних правоохоронними органами, а також технічної взаємодії з державними структурами. Проте, як видається, подібний режим створює ризики для приватності без належних процедурних гарантій, особливо в умовах відсутності незалежного контролю за обробкою даних.

Як зазначалося вище, у вітчизняній доктрині питання балансу між безпекою та приватністю досліджувалося, зокрема, у працях В. Шаповала, який наголошував на необхідності конституційного обмеження втручання держави в особисту сферу. Концепція «конституційної межі допустимого втручання», запропонована автором [1, с. 485], є надзвичайно важливою для аналізу сучасних викликів, пов'язаних із масовим збором даних, відеоспостереженням, біометричним контролем та алгоритмічним прогнозуванням поведінки. Проте, на нашу думку, окреслена концепція потребує доповнення категорією «технологічної прозорості», яка має стати новим критерієм легітимності державного втручання.

В даному аспекті слід звернутися до положень Регламенту ЄС 2016/679, який встановлює принципи обробки персональних даних, включаючи обов'язок приватних компаній забезпечувати прозорість, мінімізацію даних, право на забуття та захист від автоматизованого прийняття рішень [13]. Разом з тим, його імплементація в Україні є частковою, що обумовлює потребу в доктринальному осмисленні адаптації європейських стандартів до національного законодавства.

Доцільно зазначити, що право на безпеку, як і право на приватність, не є абсолютним. Вони підлягають обмеженню за умов дотримання принципу пропорційності, який, згідно з практикою Європейського суду з прав людини (S. and Marper v. the United Kingdom [14]), вимагає, щоб втручання було не лише законним, але й необхідним у демократичному суспільстві. Водночас, при аналізі цифрових форм втручання, постає питання про нову якість ризиків – алгоритмічну дискримінацію, втрату автономії, маніпуляцію поведінкою – які не були враховані в класичних доктринах прав людини.

Особливої уваги заслуговує концепція «цифрового конституціоналізму», яку розвиває E. Celeste [15]. Автор обґрунтовує, що цифрові платформи дедалі більше виконують нормативну функцію, формуючи власні правила поведінки, модерації, збору та обробки даних – фактично створюючи «квазі-конституції» для мільйонів користувачів. У цьому контексті корпорації не просто обробляють інформацію, а здійснюють регуляторну діяльність, що наближає їх до статусу недержавних нормотворців. Відповідна трансформація зумовлює необхідність доктринального осмислення: насамперед, варто розробити категорію «приватного регулятора з публічною відповідальністю», яка б визначала межі дії цифрових платформ у сфері прав людини та демократичного контролю.

У межах подальшого теоретичного розвитку запропонованої концепції доцільно здійснити порівняльно-правовий аналіз аналогічних доктринальних конструкцій, що функціонують у зарубіжних правових системах. Зокрема, категорія «приватного регулятора з публічною відповідальністю» може бути зіставлена з концептами «quasi-public actor» у американському праві [16], «platform governance» у європейських дослідженнях цифрової політики [17] [18], а також із моделлю «normative intermediaries», що застосовується в контексті транснаціонального регулювання [19] [20].

У практичному вимірі особливо показовими є кейси, пов'язані з діяльністю компаній Meta, Google, Amazon, які неодноразово ставали об'єктом критики за порушення приватності, маніпуляцію даними та непрозорість алгоритмів. Зокрема, у рішенні Суду Європейського Союзу у справі Schrems II (C-311/18) було визнано недейсним механізм Privacy Shield, що регулював передачу персональних даних між ЄС і США [21]. Суд поставив під сумнів здатність американських корпорацій гарантувати належний рівень захисту даних громадян ЄС, що створює прецедент для перегляду транснаціональних потоків даних та посилення контролю за діяльністю приватних суб'єктів. Така судово-практика засвідчує, що навіть у межах усталених правових режимів транснаціональні корпорації можуть уникати належного контролю, що актуалізує потребу в додаткових нормативних орієнтирах.

В даному аспекті особливого значення набувають універсальні рамки корпоративної відповідальності, зокрема ті, що сформульовані у Керівних принципах ООН з питань бізнесу і прав людини [8], які визнають обов'язок приватного сектору поважати права людини, включаючи право на приватність. Слід наголосити, що документ формулює три ключові положення: обов'язок держави захищати права людини, відповідальність бізнесу за їх повагу та необхідність забезпечення доступу до засобів правового захисту.

Проте, констатуємо, наведені принципи мають рекомендаційний характер і не створюють юридично обов'язкових норм, що обмежує їх ефективність у регулюванні діяльності корпорацій.

Окрему увагу слід приділити концепції «інформаційного самовизначення», запропонованій Федеральним конституційним судом Німеччини у справі про перепис населення (BVerfGE 65, 1, 1983), яка передбачає, що кожна особа має право самостійно вирішувати, які дані про неї збираються, зберігаються та використовуються [22]. Означене, на нашу думку, є основним для формування сучасної теорії приватності, оскільки поєднує індивідуальну автономію з вимогами цифрової безпеки. Проте, слід критично зауважити, що в умовах алгоритмічного управління та штучного інтелекту інформаційне самовизначення дедалі більше перетворюється на декларативну норму, позбавлену реального механізму реалізації.

Продовжуючи наукову аргументацію, слід зазначити, що концепція інформаційного самовизначення, попри її нормативну обґрунтованість, стикається з низкою структурних обмежень у цифровому середовищі. По-перше, як слушно зауважує D. Solove, сучасна приватність не зводиться до контролю над даними, а є складним соціальним конструктом, що охоплює в тому числі контекстуальну взаємодію, інформаційні асиметрії та структурну нерівність між суб'єктами даних і технологічними операторами [23]. Відтак, самостійне волевиявлення особи щодо обробки її даних не гарантує фактичного захисту, якщо не супроводжується інституційними гарантіями та процедурною прозорістю.

По-друге, M. Gharib у своїй праці про інформовану згоду як механізм реалізації інформаційного самовизначення доводить, що модель «notice and choice» є вразливою: більшість користувачів не мають реального вибору, а згода часто є формальною, неусвідомленою і нав'язливою [24]. Наведене, як видається, ставить під сумнів ефективність самовизначення як інструменту захисту приватності в умовах цифрової економіки. По-третє, H. Nissenbaum пропонує концепцію «контекстуальної цілісності», яка критикує універсалізм самовизначення і наголошує на необхідності врахування соціальних норм, ролей і очікувань у конкретному інформаційному контексті [25]. Окреслений підхід дає можливість розглядати приватність не як індивідуальне право в ізоляції, а як елемент соціального порядку.

Ба більше, S. Zuboff у своїй теорії «наглядового капіталізму» демонструє, що сучасні цифрові корпорації не просто збирають дані, а конструюють поведінкові моделі, які підпорядковують індивідуальну автономію логіці прогнозування і комерційного контролю [5]. У цьому контексті інформаційне самовизначення втрачає свою нормативну силу, оскільки особа не здатна передбачити або вплинути на алгоритмічні наслідки власної цифрової активності. Критика авторки «економіки поведінкових даних» є надзвичайно важливою для правової теорії, оскільки вона висвітлює, що право на приватність більше не може розглядатися виключно як захист від держави – воно має бути переосмислене як захист від корпоративного алгоритмічного контролю.

Погоджуючись із загальним напрямом її критики, вважаємо за необхідне доповнити її концепцію правовим механізмом – зокрема, через запровадження обов'язкової доктрини «цифрової доброчесності» для суб'єктів, які обробляють персональні дані. Своєю чергою, під *цифровою доброчесністю* доцільно розуміти нормативно-етичний принцип, що визначає межі допустимої поведінки суб'єктів цифрового середовища – насамперед приватних платформ, які здійснюють обробку персональних даних, алгоритмічне управління та модерацію інформаційного простору. Наведений принцип передбачає не лише формальне дотримання законодавчих вимог, а й забезпечення

прозорості цифрових процесів, пропорційності втручання в особисту сферу, контекстуальної обґрунтованості алгоритмічних рішень та пріоритетності людської гідності як вищої цінності цифрового порядку.

У межах подальшого теоретичного осмислення доцільно порушити питання про формування цифрової конституційної етики – як міждисциплінарного концепту, що охоплює правові, філософські та технологічні засади легітимності цифрового порядку. Йдеться не лише про нормативне регулювання поведінки корпорацій, а про встановлення етичних меж допустимого втручання в автономію особи, алгоритмічного прогнозування та модерації соціального простору. Етика має ґрунтуватися на презумпції людської гідності як непереборного критерію цифрової доброчесності, а також на принципі «некомодифікованої приватності» – тобто такої, що не може бути об'єктом ринкового обігу.

Висновки. У результаті проведеного дослідження встановлено, що цифрова трансформація суспільства зумовлює докорінну зміну суб'єктного складу гарантування прав людини, зокрема прав на безпеку та приватність. Традиційна модель, за якою держава виступає єдиним носієм правозахисної відповідальності, виявляється недостатньою для пояснення сучасних викликів, пов'язаних із діяльністю приватних корпорацій, які дедалі частіше виконують квазі-нормативні функції у цифровому середовищі.

З'ясовано, що правова доктрина, як на національному, так і на міжнародному рівні, не виробила усталеного підходу до визначення меж правосуб'єктності приватних платформ, критеріїв легітимності їхньої діяльності

та механізмів відповідальності за порушення цифрових прав.

У межах подальшого правового осмислення цифрової доброчесності як правового принципу доцільно розглянути її не лише як етичну декларацію, а як потенційний елемент позитивного права, здатний виконувати функцію нормативного обмежувача корпоративної дискреції. Разом з тим, зазначений принцип має бути інтегрований у правові режими, що регулюють обробку персональних даних, алгоритмічне управління, модерацію контенту та систему цифрового вибору. Своєю чергою, його нормативна сила полягає у здатності встановлювати межі допустимого втручання в інформаційну автономію особи, виходячи з презумпції гідності як конституційного ядра цифрового порядку.

В даному аспекті правова кваліфікація платформ як «приватних регуляторів з публічною відповідальністю» набуває особливого значення, оскільки наведена конструкція дозволяє вийти за межі класичної моделі суб'єктності, визнаючи, що приватні цифрові оператори здійснюють нормативну діяльність, яка має прямий вплив на реалізацію прав і свобод. Відтак, їхня поведінка повинна оцінюватися не лише з позиції договірної права чи комерційної доброчесності, а й крізь призму конституційних положень, що регулюють діяльність публічної влади.

З огляду на це, правова доктрина має в подальшому сформулювати критерії легітимності цифрового регулювання, які охоплюють, зокрема: прозорість алгоритмічних процесів, контекстуальну обґрунтованість рішень, процедурну підзвітність, а також здатність суб'єкта забезпечити ефективний доступ до засобів правового захисту.

ЛІТЕРАТУРА

1. Шаповал В.М. Сучасний конституціоналізм. *Монографія*. К.: Юридична фірма «Салком»; Юрінком Інтер, 2005. 560 с.
2. Фасій Б. Національна безпека та захист персональних даних в епоху цифрових технологій. *Society and Security*. 2024. №6 (6). С. 76–82.
3. Кібербезпека в інформаційному суспільстві: *Інформаційно-аналітичний дайджест* / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПРН України»; Національна бібліотека України ім. В.І. Вернадського. К., 2024. № 5 (травень). 316 с.
4. Коваленко О.О., Тихомиров О.О. Право на приватність в умовах сучасних комунікацій. *Юридичний науковий електронний журнал*. 2020. №5. С. 133–136.
5. Zuboff S. The age of surveillance capitalism: the fight for a human future at the new frontier of power. New York: *Public Affairs*. 2019. 704 pp.
6. Lessig L. Code and Other Laws of Cyberspace. New York: *Basic Books*, 1999. 320 p. URL: https://www.academia.edu/11685582/Code_and_other_laws_of_cyberspace
7. Cohen J. E. Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. New Haven: *Yale University Press*, 2012. 352 p. URL: <https://scholarship.law.georgetown.edu/facpub/804/>
8. Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework. New York and Geneva: *Office of the High Commissioner for Human Rights*, 2011. URL: https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
9. Böckenförde E.-W. Der Staat als Voraussetzung der Freiheit. Böckenförde E.-W. Recht, Staat, Freiheit: *Studien zur Rechtsphilosophie, Staatstheorie und Verfassungsgeschichte*. Frankfurt am Main: Suhrkamp, 1991. P. 92–114.
10. Конституція України від 28.06.1996 №254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>
11. Про захист персональних даних: Закон України від 01.06.2010 №2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17>
12. Про електронні комунікації: Закон України від 16.12.2020 №1089-IX. URL: <https://zakon.rada.gov.ua/laws/show/1089-20>
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
14. S. and Marper v. the United Kingdom. App 30562/04. Judgement 04.12.2008. URL: <https://hudoc.echr.coe.int/fre?i=001-117816>
15. Celeste E. Constitutionalism in the Digital Age. Berlin: *Alexander von Humboldt Institute for Internet and Society*, 2020. 15 p. URL: <https://www.hiig.de/wp-content/uploads/2020/11/2020-Celeste-Constitutionalism-in-the-Digital-Age.pdf>
16. Quasi-Governmental Entities and Legislative Power Delegations. Constitution Annotated. *Library of Congress*. URL: https://constitution.congress.gov/browse/essay/artI-S1-6-4/ALDE_00001323/
17. Europe fit for the Digital Age: new online rules for platforms. *European Commission*. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act/europe-fit-digital-age-new-online-rules-platforms_en
18. Digital Platform Governance. April 2025. Competition Policy International. URL: <https://www.pymnts.com/wp-content/uploads/2025/04/TechREG-Chronicle-Digital-Platform-Governance-APRIL-2025.pdf>
19. Kourula A., Paukku M., Peterman A., Koria M. Intermediary roles in regulatory programs: Toward a role-based framework. *Regulation & Governance*. 2018. URL: <https://onlinelibrary.wiley.com/doi/epdf/10.1111/rego.12226>
20. Brès L., Mena S., Salles-Djelic M.-L. Exploring the formal and informal roles of regulatory intermediaries in transnational multi-stakeholder regulation. *Regulation & Governance*. 2019. Vol. 13, № 2. P. 127–140. DOI: <https://doi.org/10.1111/rego.12249>
21. Court of Justice of the European Union. Data Protection Commissioner v. Facebook Ireland and Maximilian Schrems (Schrems II). (C-311/18) Judgment of the Court (Grand Chamber) of 16.07.2020. URL: <https://curia.europa.eu/juris/liste.jsf?num=C-311/18>
22. Bundesverfassungsgericht. Volkszählungsurteil – Urteil vom 15. Dezember 1983, 1 BvR 209/83 u.a. BVerfGE 65, 1. URL: https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/EN/1983/12/rs19831215_1bvr020983en.pdf

23. Solove D. J. Understanding Privacy. Cambridge, Mass.: *Harvard University Press*, 2008. 257 p. URL: <https://archive.org/details/understandingpri0000solo>
24. Gharib M. Privacy and Informational Self-determination Through Informed Consent: The Way Forward. ESORICS 2021 International Workshops. Springer, 2022. P. 171–184. URL: <https://www.researchgate.net/publication/357573456>
25. Nissenbaum H. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: *Stanford University Press*, 2010. 288 p. URL: <https://archive.org/details/privacyincontext0000niss>

Дата першого надходження рукопису до видання: 18.08.2025
Дата прийнятого до друку рукопису після рецензування: 23.09.2025
Дата публікації: 26.09.2025