DOI: https://doi.org/10.21564/2707-7039.1.275644
УДК 341.231.14+342.7+008

Петро Сухорольський*

МАЙБУТНЄ ПРИВАТНОСТІ КРІЗЬ ПРИЗМУ ТЕОРІЇ ПОСТНОРМАЛЬНОСТІ

Вступ

Сучасні правові дослідження приватності нерідко зосереджені винятково на низинному рівні і спрямовані передусім на вивчення загроз та засобів забезпечення відповідних прав людини у конкретних життєвих реаліях. Водночас зміни на макрорівні (включаючи трансформацію й еволюцію технологічного та соціального середовища упродовж кількох останніх десятиліть) настільки масштабні і всеохоплюючі, що їх вже аж ніяк не можна далі ігнорувати. Ці зміни дуже важко науково описати і тим паче спрогнозувати їхній розвиток на майбутнє. Тому багато хто просто закриває на них очі, обмежившись дослідженнями приватності в рамках звичної парадигми. Такий підхід не можна вважати надійним і адекватним, адже невідповідність між регулятивними механізмами та реальністю лише зростає, а невирішені проблеми проявляються все частіше.

Описана ситуація змушує звернути увагу на всеосяжніші теорії, автори яких намагаються вловити суть сучасних цивілізаційних перетворень. Одна з найбільш вдалих з-поміж них – теорія постнормального часу, розроблена визначним науковцем, письменником, інтелектуалом і поліматом Зіяуддіном Сардаром. Хоча ця теорія була оприлюднена ще у 2010 р., справжнє визнання вона отримала аж у 2020-ті рр., коли стало зрозуміло, що за допомогою неї Сардару вдалося передбачити чимало феноменів, знакових саме для останніх років, включаючи глобальну пандемію та активізацію протестного руху афроамериканців у США. Сам Сардар у своїй роботі зазначає, що приватність належить до систем, які вже зараз знаходяться у стані постнормальності[1]. Тому невипадково у цій статті проблема зникнення приватності[2] розглянута саме

* Петро Михайлович Сухорольський, кандидат юридичних наук, доцент кафедри політології та міжнародних відносин Інституту гуманітарних та соціальних наук Національного університету "Львівська політехніка" (Україна).
Petro Sukhorolskyi, Candidate of Legal Sciences, Associate Professor at the Department of Political Science and International Relations of the Institute of Humanities and Social Sciences, Lviv Polytechnic National University (Ukraine).
e-mail: sukhorolsky@gmail.com
ORCID ID: https://orcid.org/ 0000-0002-1689-3283

[1] Ziauddin Sardar and John A. Sweeney, "The Three Tomorrows of Postnormal Times," *Futures* 75 (2016): 4.

[2] Сам термін "приватність" у цій статті для зручності вжито у широкому значенні. Тобто правовий захист приватності тут охоплює і право на недоторканність приватного життя, і право на захист персональних даних, а також інші суміжні права, які визнані в окремих правових системах. Проте це

крізь призму його теорії. Зокрема, у ній зроблена спроба окреслити сучасний стан і перспективи розвитку процесів у сфері приватності на основі методології, розробленої у межах теорії постнормального часу. Головною метою статті є привернення уваги науковців та експертів до проблем і суперечностей, які не вдається вирішити за допомогою звичних та дієвих у минулому засобів, а також стимулювання пошуку альтернативних способів узгодження та забезпечення усіх важливих інтересів у цій сфері.

I. Епоха постнормальності

Основи теорії постнормальності висвітлені у працях Сардара та його співавторів. З-поміж них ключовими є роботи "Ласкаво просимо у постнормальні часи,"[3] "Три варіанти майбутнього у постнормальні часи,"[4] "Знову про постнормальні часи,"[5] опубліковані у "Futures" – найавторитетнішому науковому футурологічному журналі світу.

Сардар створив свою теорію послуговуючись ідеями Сільвіо Фунтовича та Джерома Равеца про постнормальну науку, час якої приходить тоді, коли невизначеності набувають епістемологічного чи етичного характеру, ставки при прийнятті рішень високі, а позиції зацікавлених сторін – суперечливі.[6] На думку Сардара, характеристики, які згадані автори приписували науці у 1990-ті рр., у 2010-их підходять не лише для багатьох інших видів людської діяльності, але й для суспільства загалом. Отже, постнормальні часи – це проміжний період, який наступає, коли старі теорії, уявлення і практики помирають, а нові ще не народилися, і здається, що дуже небагато речей взагалі мають сенс. У колишні "нормальні часи" коли виникала нова проблема, її можна було легко виділити та ідентифікувати, після чого застосувати усі наявні інтелектуальні ресурси для її вирішення на основі ґрунтовних і доведених теорій з усіх наукових дисциплін. І найголовніше – усе це працювало. Тепер більшість з того, що вважалося нормальним, звичним, традиційним, поступово стає безсилим перед новими викликами, які насуваються одночасно великою лавиною та охоплюють багато явищ, починаючи від зміни клімату і закінчуючи проблемами з ідентичністю.[7]

не означає критику поширених у Європі підходів, які розмежовують інститут захисту персональних даних та право на повагу до приватного й сімейного життя. Швидше навпаки – проведений аналіз учергове доводить, що політичні, економічні та інші аспекти захисту персональних даних все більше виходять за межі приватності і приватного життя та вже зараз прямо стосуються чи не усіх граней суспільного буття. Більше про це у роботі: Петро Сухорольський, "Право на захист персональних даних як нове фундаментальне право людини в інформаційному суспільстві," in *Wyzwania społeczeństwa informacyjnego. Polskie i ukraińskie doświadczenia* (Lublin: Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, 2018), 15–25.

[3] Ziauddin Sardar, "Welcome to Postnormal Times," *Futures* 42 (2010): 435–44.

[4] Sardar and Sweeney, "The Three Tomorrows of Postnormal Times," 1–13.

[5] Ziauddin Sardar, "Postnormal Times Revisited," *Futures* 67 (2015): 26–39.

[6] Silvio O. Funtovicz and Jerome R. Ravetz, "Science for the Post-Normal Age," *Futures* 25, issue 7 (1993): 750.

[7] Sardar, "Welcome to Postnormal Times," 435–36.

Трьома ключовими ознаками постнормальності є: складність, хаос і суперечності (скорочено "3С" від англ.: complexity, chaos, contradictions). Щодо першої – то мабуть ні для кого не є секретом, що усі важливі проблеми сьогодення надзвичайно складні, а прості задачі і рішення практично відсутні. Причинами цього є як довготривале ускладнення процесів у різних сферах, так і їх вихід на глобальний рівень. Ба більше, все з усім може бути взаємопов'язане, а зміни наступають раптово й одночасно. За таких умов науковцям, які намагаються змоделювати ці процеси, доводиться вдаватися до суттєвого зниження складності систем у своїх теоріях, але це неодмінно призводить до значних прогалин та відхилень, і результат виходить зовсім не таким, як очікували.[8]

Ті ж самі чинники є передумовами другого елемента постнормальності – *хаосу*. Взаємопов'язаність усього і постійне прискорення ведуть до ситуації, коли невеликі зміни спричиняють величезні наслідки, і спрогнозувати розвиток цих процесів практично неможливо. За останній час звичними для усіх стали надзвичайно рідкісні у минулому явища: раптові злети і падіння політичних фігур; нові мільярдери з космічними статками, заробленими за кілька років; неочікувані вибухи протестних рухів і революцій;[9] медіа-зірки, інфлуенсери та випадкові люди, які з'являються нізвідки, стають всесвітньовідомими і відправляються в нікуди, а також багато іншого.

У складному і хаотичному світі, де мережі поєднують все і кожного, не можна уникнути загострення багатьох *суперечностей*. Вони можуть бути деструктивними, спричиняючи руйнівну боротьбу, що завершується колапсом. З іншого боку, суперечності виконують важливу функцію – вони привертають увагу до проблем у всій їхній повноті й багатогранності і таким чином стимулюють суспільство до трансформації та переходу на новий рівень розвитку. Оскільки усі проблеми і чинники, які їх зумовлюють, взаємопов'язані, намагання ізольовано вирішити лише частину з них призводить до того, що поза увагою залишаються інші. І часто люди усвідомлюють це надто пізно.[10]

Стан постнормальності не настає одночасно в усіх сферах і місцях. Саме майбутнє починається безпосередньо від теперішнього моменту. За Сардаром воно може включати різнорідні елементи, які належать до: 1) розширеного теперішнього, 2) знайомих майбутніх,[11] 3) немислимих майбутніх. У часи постнормальності усі ці компоненти існують паралельно, проте лише останній з них безпосередньо пов'язаний з постнормальними процесами і є їхнім результатом. *Розширене теперішнє* – це продовження у майбутнє трендів, походженням із минулого і теперішнього. Певний час (різний для різних сфер, явищ та місць) ці тренди ще залишатимуться актуальними, проте згодом вони неодмінно ослабнуть і стануть надбанням історії. Майбутнє у межах розширеного теперішнього можна спрогнозувати і спланувати. Інакше кажучи, воно відноситься

[8] Ibid, 437.

[9] З-поміж іншого Сардар вважає ілюстративним прикладом хаотичних процесів постнормальності й Помаранчеву революцію в Україні у 2004 р.

[10] Sardar, "Welcome to Postnormal Times," 437–39.

[11] У футурології (futures studies) слово "майбутнє" часто вживають у множині, підкреслюючи багатоваріантність можливого розвитку подій.

швидше до нормальності, ніж до постнормальності. Оскільки розпад колишньої нормальності неможливо зупинити, а невідомість і непевність постнормальних часів усіх лякає, виникає феномен штучно сконструйованої нормальності (manufactured normalcy). Вона з'являється як в результаті спроб домінантних світових гравців спрямувати усі процеси в зрозуміле русло капіталістичних відносин, так і внаслідок реакцій простих людей, які зіштовхнувшись із невідомим намагаються втиснути його у рамки звичних уявлень та минулого досвіду.

Знайомі майбутні охоплюють неіснуючі у теперішньому процеси і явища, які, однак, вже стали звичними для людей через присутність у різноманітних образах майбутнього, поширених у масовій культурі. *Немислимі майбутні* включають щось настільки далеке від загальноприйнятих уявлень, що це заважає нам зосередитися на таких варіантах майбутнього розвитку подій. Або це настільки незвичні можливості, що ми просто не надаємо їм значення.[12]

Оскільки, на думку Сардара, ситуація у сфері приватності вже зараз є постнормальною, усі згадані характеристики цього стану повинні чітко тут проявлятися. Спробуємо їх ідентифікувати та описати. Окремо звернемо увагу на звичні теорії та підходи, що стосуються приватності, які у цьому випадку повинні відповідати критеріям розширеного теперішнього, включаючи штучно сконструйовану нормальність.

II. Прояви постнормальності у сфері приватності

Насамперед важливо встановити, наскільки характерними для сфери приватності є три головні ознаки постнормальності – складність, хаос та суперечності.

Складність

Кількість збережених даних у світі зростає з шаленою швидкістю. Значну кількість із них можна використати для втручання у приватність. Швидко зростає і кількість джерел надходження цих даних – камер, мікрофонів, різноманітних датчиків. Наприклад, ідентифікація за допомогою відбитків пальців за останні роки вже стала нормою. Ні бізнес, ні влада не збираються відмовлятися від теперішньої стратегії акумуляції усе більшої кількості даних у великих базах, до того ж часто ці дані пов'язані між собою. Існує також величезна кількість неструктурованої інформації. Не менш важливо, що алгоритми опрацювання цих даних також постійно ускладнюються і, на думку багатьох експертів, незабаром можуть вийти з-під контролю людини.[13]

У Посібнику з європейського права у сфері захисту персональних даних, підготовленому Радою Європи та ЄС, стверджується, що персональні дані обробляються "все більш складними і непрозорими способами." У контексті проблем, пов'язаних з упро-

[12] Sardar and Sweeney, "The Three Tomorrows of Postnormal Times," 1–13.
[13] James Dawes, "Speculative Human Rights: Artificial Intelligence and the Future of the Human," *Human Rights Quarterly* 42.3 (2020): 573–93; Mathias Risse, "Human Rights and Artificial Intelligence: An Urgently Needed Agenda," *Human Rights Quarterly* 41.1 (2019): 1–16.

вадженням технологій штучного інтелекту, говориться про випадки, коли "складність і кількість оброблюваних даних не можуть бути визначені з певністю." Також зазначено про складність, або й неможливість, процесу оцінки впливу великих даних на приватність та ризиків, пов'язаних з опрацюванням персональних даних.[14] Окрім вказаних, у Посібнику міститься ще чимало схожих формулювань, що свідчать про надзвичайне ускладнення процесів, які відбуваються у сфері персональних даних, а також про поступову втрату контролю і зростаючу непевність – дві виділені Сардаром характеристики постнормальності, які безпосередньо пов'язані з ускладненням життя.[15]

Показовим є і постійне збільшення кількості та ускладнення правових норм, пов'язаних із приватністю. Наприклад, обсяг Загального регламенту захисту даних (GDPR), прийнятого ЄС у 2016 р., приблизно у 4 рази перевищує обсяг Директиви 95/46/ЕС. Проте це зовсім не означає, що норм GDPR вистачає для забезпечення ефективного захисту персональних даних в усіх сферах. Як мінімум, у Регламенті відсутні спеціальні положення щодо технологій штучного інтелекту, великих даних та явно недостатніми є лише кілька загальних згадок про генетичні дані, які є дуже специфічними в плані своїх характеристик та загроз для приватності людини.[16] У численних рішеннях міжнародних організацій, які стосуються впливу інформаційних технологій на права людини, відзначено гостру необхідність розроблення правових норм на національному і міжнародному рівнях, які дозволили б врахувати новітні загрози та узгодити й забезпечити усі важливі індивідуальні та суспільні інтереси.[17] Однак, чи не перешкоджатиме сама складність такої нормативної бази її ефективному впровадженню, враховуючи ще й те, що у світі існують багато різних правових систем, у межах яких втілюються цілковито відмінні підходи до вирішення проблем приватності (вже не кажучи про альтернативні регулятори відносин у суспільстві, про які йтиметься нижче, а саме: ринок, технологічне середовище, а також соціальні норми, що формуються під впливом медіа).

Хаос

Як зазначає Сардар, потенціал хаосу зростає під впливом великих даних, а поєднаність у мережі зумовлює те, що маленькі зміни спричиняють великі наслідки.[18] Усе це безпосередньо стосується і приватності. Індивіди за короткий час стали міцно прив'язані

[14] *Handbook on European Data Protection Law* (Luxembourg: Publications Office of the European Union, 2018), 347–60.
[15] Sardar, "Welcome to Postnormal Times," 440, 442.
[16] Див. більше: Petro Sukhorolskyi and Valeriia Hutsaliuk, "Processing of Genetic Data under GDPR: Unresolved Conflict of Interests," *Masaryk University Journal of Law and Technology* 14, no. 2 (2020): 151–76.
[17] UN, The right to privacy in the digital age, Resolution adopted by the Human Rights Council on 26 September 2019, A/HRC/RES/42/15; Council of Europe, Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes, Decl (13/02/2019)1.
[18] Sardar, "Postnormal Times Revisited," 33.

до мережі. Багато людей відчувають залежність від смартфонів і намагаються її позбутися, проте звичним способом подолання тривоги від непевності сучасного світу часто є занурення у той самий смартфон.[19] Складається парадоксальна ситуація: ховаючись від постнормальності люди все більше перетворюються на елементи складних глобальних мереж, які самі посилюють хаос і є одним із головних джерел постнормальності.

Згідно з законодавством, персональні дані нібито є захищеними, але насправді мало хто у це вірить. Великі витоки даних мільйонів людей вже нікого не дивують, але незважаючи на це, вони можуть стати причиною неконтрольованої реакції. Показовою є ситуація з компанією *Cambridge Analytica*, яка і до скандалу не приховувала цілей і методів своєї діяльності та відкрито цим хизувалася. Аж раптом у 2018 р. вона перетворилася на об'єкт прискіпливої уваги медіа та правоохоронних органів, і це спричинило ланцюгову реакцію й масштабні наслідки (зокрема ринкова вартість *Facebook* впала на 19% або на 119 млрд доларів за рекордно короткий час). Ще ілюстративніше те, що після затухання скандалу ситуація загалом залишилася такою ж самою (тобто характерною для постнормальних часів). Численні компанії неконтрольовано збирають дані про людей та використовують їх для політичних цілей (у тому числі й дочірні компанії *SCL Group*, якій належала *Cambridge Analytica*). Те ж саме стосується і продовження неконтрольованого втручання у приватність з боку органів державної безпеки у різних країнах навіть після викриттів Едварда Сноудена.

На нижчому рівні прикладом хаотичних процесів є випадки раптового загострення інтересу мільйонів до окремих осіб, які часто зовсім не мали наміру ввійти в глобальні інформаційні тренди, або принаймні не під таким інформаційним приводом. Так, один невеликий пост, фотографія, колаж чи відеоролик може зробити людину відомою на весь світ. У такому разі не доводиться і мріяти про збереження чи відновлення її приватності, і навіть право бути забутим тут безсиле. Насамкінець варто відзначити, що хаотичні процеси в суспільстві відбувалися і в "нормальні" часи, проте лише в часи постнормальності вони стають настільки поширеними й звичними, що їх фактично можна назвати новим мейнстрімом.

Суперечності

Третій складовий елемент "3С" у нашому випадку є найцікавішим, оскільки сфера приватності та персональних даних переповнена суперечностями, багато з яких проявилися лише в останні роки. Розглянемо деякі з них детальніше.

Законодавство визначає згоду суб'єкта даних як одну з головних підстав для опрацювання персональних даних. Згідно з цим, звичним для усіх стало надання такої згоди через підписування спеціальних документів чи проставлення галочок і натискання

[19] Mary Holland, "How to Take a Digital Detox during the Covid-19 Pandemic," *BBC Worklife*, last modified May 18, 2020, https://www.bbc.com/worklife/article/20200513-how-to-take-a-digital-detox-during-the-covid-19-pandemic.

кнопок на сайтах. Проте лише дуже невеликий відсоток людей справді читає умови використання даних. Крім того, часто не існує жодних прийнятних альтернатив, оскільки надання послуги чи користування ресурсом залежить від згоди суб'єкта даних на їх опрацювання. У більшості випадків люди просто не здатні розібратися з ризиками, пов'язаними із наданням згоди, і це не дивно, адже адекватно оцінити ці ризики інколи не спроможна навіть велика група експертів, задіяних у спеціальній процедурі оцінювання впливу. Візьмемо для прикладу генеалогічні сайти, які пропонують людям інформацію на основі аналізу їхньої ДНК (*MyHeritage*, *23andMe*, *Ancestry* та інші). Приватні компанії, що є власниками цих сайтів, пропонують фізичним особам надіслати біологічні зразки для аналізу, погодитися на опрацювання їхніх генетичних даних та подальше їх включення у величезні масиви генетичних даних мільйонів людей. Отже, фізичні особи повинні оцінити усі переваги та ризики і прийняти зважене рішення. Але чи здатні вони це зробити, якщо на думку фахівців, що вивчають це питання, оцінювання усіх ризиків[20] у цьому випадку є настільки складним завданням, що воно вимагає масштабного міждисциплінарного дослідження із залученням спеціалістів у галузі етики, права, генетики та соціології?[21]

Метою створення законодавства у сфері захисту персональних даних було надання людині можливостей контролювати межі своєї приватності і мати вплив на опрацювання персональних даних, що її стосуються. Проте сучасний механізм згоди особи на опрацювання даних все менше сприяє досягненню цієї мети. З цим погоджуються і експерти ЄС та РЄ – автори згаданого вище Посібника, які стверджують, що сучасні умови вимагають "переосмислення ідей особистого контролю персональних даних," враховуючи з-поміж іншого й недостатню обізнаність з боку людей. Натомість вони пропонують спрямувати зусилля на "більш складний процес множинних оцінок впливу ризиків, пов'язаних з використанням персональних даних."[22] Отже, сучасна система захисту прав суб'єкта даних, що базується на його згоді, дуже часто створює лише ілюзію контролю над даними, не забезпечуючи реальний контроль, і це є першою важливою суперечністю. Її можна сформулювати у вигляді твердження (яке не обов'язково повинне виконуватися в усіх випадках для того, щоб свідчити про постнормальність): "*чим більше формальних можливостей надають суб'єкту даних, тим слабшою стає система забезпечення його права на захист персональних даних.*"

Іншою важливою стратегією захисту персональних даних, яку можна виокремити аналізуючи сучасні нормативно-правові акти, є анонімізація та псевдонімізація даних.[23] Вона базується на припущенні, що чим більше даних будуть анонімними або захище-

[20] Така процедура передбачена для чутливих даних згідно зі ст. 35 Загального регламенту захисту даних Європейського Союзу.

[21] Paul Quinn and Liam Quinn, "Big Genetic Data and Its Big Data Protection Challenges," *Computer Law & Security Review* 34, no. 5 (2018): 1008.

[22] *Handbook on European Data Protection Law*, 359.

[23] 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

ними псевдонімами, тим більше будуть забезпечені інтереси суб'єкта даних. Проте це припущення справджується далеко не в усіх випадках, а з часом воно може взагалі втратити актуальність. Йдеться про те, що в епоху великих даних стає все простіше ідентифікувати людину навіть на основі знеособленої інформації. Чіткої межі між персональними даними та анонімізованою інформацією не існує.[24] Все набагато складніше. Вже зараз у різних дослідженнях автори виділяють декілька рівнів анонімізації, і віднесення інформації до певного рівня зовсім не означає, що ситуація не може змінитися з часом. Стосовно ж окремих видів персональних даних висловлюються сумніви, чи рівень їхньої абсолютної анонімності може бути в принципі досягнутий.[25]

Згідно з загальноприйнятим у Європі визначенням, персональні дані – це інформація, що стосується фізичної особи, яку ідентифіковано або можна ідентифікувати. Тобто для встановлення того, що є персональними даними, на які поширюється правовий захист, важливо зрозуміти зміст словосполучення "можна ідентифікувати." Щодо цього у GDPR міститься таке формулювання: "Щоб встановити можливість ідентифікації фізичної особи, необхідно взяти до уваги всі способи, що можуть бути використані з високою ймовірністю…," при цьому потрібно врахувати "всі об'єктивні фактори, такі як витрати та період часу, необхідні для ідентифікації, з огляду на технології, наявні станом на момент опрацювання, і технологічні розробки."[26] Інакше кажучи, дані можуть виявитися зовсім не такими анонімними, як очікувалося, якщо витратити більше часу і зусиль для ідентифікації. Якщо ж врахувати факт, що технології у наш час дуже швидко вдосконалюються, то з кожним днем імовірність ідентифікації особи на основі так званої деперсоніфікованої чи анонімної інформації лише зростатиме. А отже, дані, які сьогодні вільно збирають і використовують приватні компанії, можуть завтра раптово перетворитися у персональні, але відновити приватність зацікавлених осіб буде вже практично неможливо. Щодо таких випадків виправдано стверджувати, що відносна деперсоніфікація даних лише відкладає загрози у майбутнє, а не усуває їх. І судячи з розміру інвестицій, які скеровують на розвиток відповідних технологій, це дуже недалеке майбутнє.

Ще цікавіша ситуація зі стратегією мінімізації персональних даних. Довгий час мінімізацію даних вважали чи не найдієвішим засобом забезпечення приватності та інших суміжних прав людини.[27] Інакше кажучи, припускали, що чим менше збирають персональних даних, тим краще забезпечені відповідні права. Наприклад, у Кодексі про захист

of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJL 119, 4.5.2016, pp. 1–88), recitals 26, 28, 29, 78, 156, articles 6, 32, 40.

[24] EU, Opinion 05/2014 on Anonymisation Techniques, Article 29 Data Protection Working Party (April 10, 2014, 0829/14/EN WP216), 4–5.

[25] Mark Taylor, *Genetic Data and the Law: A Critical Perspective on Privacy Protection* (Cambridge: Cambridge University Press, 2012), 138.

[26] General Data Protection Regulation, recital 26.

[27] Giusella Finocchiaro, "Anonymity and the Law in Italy," in *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford University Press, 2009), 526.

персональних даних Італії у редакції 2003 р.[28] був закріплений як основоположний (на самому початку документа в окремій статті) принцип мінімізації даних, згідно з яким

> [і]нформаційні системи і програмне забезпечення мають бути налаштовані для мінімізації використання персональних чи ідентифікаційних даних, так щоб виключити їх опрацювання, якщо мети у конкретному випадку можна досягти, використовуючи анонімні дані, або через відповідні заходи, які дозволяють ідентифікувати суб'єкта даних лише у випадку необхідності.[29]

Утім, розглянувши принцип мінімізації крізь призму теорії постнормальності, стає зрозуміло, що він швидше втілює бажання повернутися у часи нормальності, ніж справді може змінити ситуацію. І справа тут не лише в технологічних та бізнесових трендах. Набагато цікавіше, що в умовах постнормальності мінімізація може зумовлювати протилежний очікуваному ефект, і це виявляє ще одну важливу суперечність. Йдеться про те, що завдяки новим технологіям деякі втручання у права людини, які базуються на використанні персональних даних, стали можливими і без них. Уявімо собі алгоритм, який може з високою ймовірністю встановити політичні погляди чи сексуальну орієнтацію (чутливі дані) користувача на основі аналізу його профілю в соціальних мережах. У процесі навчання алгоритму найімовірніше використовували чутливі дані багатьох осіб, проте після цього для його роботи не потрібно опрацьовувати чи зберігати ці дані, необхідний лише доступ до профілів користувачів, багато з яких є відкритими.

Якщо ж метою алгоритму є не просто встановити факти, а сформулювати рішення щодо людини, яке має для неї правові наслідки, то цей алгоритм зовсім не обов'язково повинен розкривати той факт, що рішення зумовлене відомостями про сексуальну орієнтацію чи політичні погляди індивіда. Коли це стосується штучного інтелекту, то навіть самі розробники можуть не здогадуватися про такий дискримінаційний ефект. З іншого боку, щоб встановити цей ефект, нам необхідно зіставити результати роботи алгоритму з чутливими даними, але таких даних у нас немає, бо вони не потрібні для роботи алгоритму і до того ж створюють зайві правові проблеми для контролера даних.[30] Отже, принцип мінімізації даних може мати негативний ефект для приватності, і у такому разі буде справджуватися закономірність: *"чим менше зібрано персональних даних, тим важче встановити втручання у права індивіда."*

Суперечності, які стосуються приватності, не вичерпуються неоднозначним впливом стратегій захисту персональних даних. У світі поширені кардинально протилежні оцінки щодо загальної ситуації у цій сфері, корені яких зводяться до відмінностей на рівні цінностей та світогляду. У той час як багато експертів у сфері прав людини стверджують,

[28] У новій значно переробленій редакції Кодексу 2018 р., яка була прийнята для його узгодження з GDPR, цю статтю вилучили.

[29] Italian Personal Data Protection Code (Legislative Decree #196, June 30, 2003), http://www.privacy.it/privacycode-en.html, article 3.

[30] Michiel Rhoen and Qing Yi Feng, "Why the 'Computer Says No': Illustrating Big Data's Discrimination Risk through Complex Systems Science," *International Data Privacy Law* 8, issue 2 (2018): 153.

що приватність поступово зникає і ситуація внаслідок цього стає катастрофічною,[31] представники високотехнологічного бізнесу та державні менеджери доводять, що хвилюватися, загалом, немає про що, а реальні загрози для людини і суспільства без особливих труднощів можна мінімізувати. У цьому плані показовою є оцінка GDPR у процесі його створення та після прийняття. Представники бізнесу, численні медіаресурси та окремі науковці (особливо американські) створювали навколо цього акта імідж "драконівського закону," який пов'язаний із марними витратами для підприємців і запроваджує невиправдано великі обмеження для економіки, а деякі його положення (наприклад, про право бути забутим) називали нерозсудливими.[32] Хоча якщо проаналізувати цей документ з точки зору забезпечення прав суб'єкта даних, то неважко відшукати у ньому значні послаблення саме в інтересах розвитку економіки, вже не говорячи про прогалини щодо багатьох аспектів, які дозволяють обійти правила.[33]

Усі ці розбіжності можна пояснити за допомогою припущення, що існує загальна і практично нерозв'язна суперечність між приватністю і глибинними тенденціями розвитку бізнесу та публічного управління в індустріальному/постіндустріальному суспільстві.[34] З цим погоджуються і чимало відомих представників високотехнологічного бізнесу, які, наприклад, спокійно прогнозують, що приватність і конфіденційність буде добровільно замінена на переваги цифрового світу, і називають це "новим суспільним договором."[35] Використовуючи модель динаміки приватності фінського дослідника Матті Мінккінена, можна побачити, що головними чинниками у цій сфері є інтереси контролерів даних (здебільшого стосуються економіки та забезпечення контролю), культурні і правові норми та наявні технологічні системи.[36] Приблизно те ж саме, але

[31] Один із авторів, які пишуть на цю тему, порівнює близьке майбутнє приватності зі світом, у якому продають лише повністю прозорі будівельні матеріали, і прозорими стали навіть віконні штори (Ivan Szekely, "Building Our Future Glass Homes – An Essay about Influencing the Future through Regulation," *Computer Law & Security Review* 29 (2013): 540). Це нам нагадує антиутопію Євгенія Замятіна, проте там штори все ж є непрозорими і їх можна закрити в одному випадку.

[32] Christiana Markou, "The 'Right to Be Forgotten:' Ten Reasons Why It Should Be Forgotten," in *Reforming European Data Protection Law* (Springer, 2015), 224.

[33] Наприклад, у GDPR відсутні спеціалізовані норми щодо опрацювання генетичних даних та недостатньо враховані втручання в інтереси суб'єкта даних, пов'язані з масштабним використанням великими IT-компаніями технологій штучного інтелекту й аналітики великих даних (Michael Butterworth, "The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework," *Computer Law & Security Review* 34.2 (2018): 257–68). Також у Регламенті запроваджені значні винятки з правил не на користь суб'єкта даних, які стосуються наукових досліджень (research exemption), при тому, що суб'єктами таких досліджень можуть бути і приватні комерційні структури (Kärt Pormeister, "Genetic Data and the Research Exemption: Is the GDPR Going Too Far?" *International Data Privacy Law* 7.2 (2017): 137–46).

[34] Більше про те, чому наша постіндустріальна реальність є швидше прямим розширенням індустріальної, а не її запереченням, у роботі: Петро Сухорольський, *Основи футурології* (Львів: Апріорі, 2021), 295–392.

[35] Ерік Шмідт та Джаред Коен, *Новий цифровий світ* (Львів: Літопис, 2015), 265.

[36] Matti Minkkinen, "Futures of Privacy Protection: A Framework for Creating Scenarios of Institutional Change," *Futures* 73 (2015): 54.

в набагато ширшому контексті доводить відомий американський вчений та політичний діяч Лоуренс Лессіг, який твердить про існування чотирьох паралельних регуляторів відносин у суспільстві. До них належать: право, інші соціальні норми, ринок та архітектура. Останній елемент у цьому переліку включає технологічне середовище (так зване регулювання кодом).[37]

Розглянемо, який загальний вплив на приватність мають вказані регулятори у теперішні часи. Правові норми, як мінімум у Європі, але також і в багатьох інших країнах світу, стоять на сторожі приватності. Включення у конституції держав, а також у міжнародні каталоги прав людини права на захист персональних даних поряд із правом на недоторканність приватного життя як ключових основоположних прав стало вже загальним стандартом у XXI ст. Хоча зрозуміло, що у межах демократичних систем ці права повинні бути збалансовані з іншими конкуруючими правами та інтересами, а в авторитарних державах приватність часто приносять у жертву забезпеченню державного контролю. Вплив другого регулятора – інших соціальних норм – не такий однозначний. Хоча у ліберальних демократіях приватність і далі вважають важливою суспільною цінністю, ставлення до неї змінюється під впливом медіа та споживацьких практик. Не буде перебільшенням стверджувати, що вагомі гравці на ринку інтернет-послуг, як і система капіталістичних відносин загалом, здатні у теперішній час суттєво впливати на суспільні норми у сфері приватності. Свідченням цього є значні зміни у поведінці людей, що стосуються добровільного розкриття персональної інформації про себе, які відбулися за останні десятиліття.

Третій регулятор – ринок, як правило, у сучасних умовах працює прямо проти приватності. Зокрема, бізнес відкрито заявляє, що big data, включаючи різноманітну інформацію про споживачів, гостро необхідні для економічного зростання. Компанії, які максимально ефективно збирають та опрацьовують дані про якнайбільшу кількість користувачів, здобувають неоціненну перевагу на ринку і витісняють конкурентів. Тому не дивно, що кожен великий бізнес прагне стати "гуглом" у своїй сфері діяльності.[38] Під впливом економічних гравців та органів влади упродовж останніх десятиліть в онлайн-просторі, а нерідко і поза ним, була сформована архітектура тотального спостереження.[39] Отже, четвертий регулятор (архітектура) також здебільшого налаштований на усунення приватності, хоча Лессіґ переконаний, що теоретично його можна

[37] Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books, 2006), 123.

[38] Так, наприклад, бізнес компаній, які за гроші пропонують людям певну інформацію, отриману з їхньої ДНК (direct-to-consumer genetic testing companies), має двоїсту природу. Далеко не усім відомо, що головна їхня мета – зовсім не продаж якомога більшої кількості тестів фізичним особам, а накопичення величезних баз генетичних даних. Тоді можна продавати доступ до цих баз великим компаніям, які здійснюють медичні та фармацевтичні дослідження, та отримувати набагато більші прибутки і можливості для зростання (Miriam C. Buiten, "'Your DNA Is One Click Away:' The GDPR and Direct-to-Consumer Genetic Testing," in *Consumer Law and Economics*, eds. Klaus Mathis and Avishalom Tor (Springer, 2021), 209).

[39] Lessig, *Code: Version 2.0*, 4.

було б спроектувати принципово по-іншому. Теорія чотирьох регуляторів дозволяє пояснити, чому проблему з приватністю не можна вирішити просто задіявши більше технологій чи ресурсів (тобто характерними для нормальності засобами), та ілюструє фундаментальну суперечність між приватністю і чинними на сьогодні трендами розвитку цивілізації.

III. Традиційні заходи реагування та перспективи

Постнормальність не настає одномоментно. Сардар характеризує цей процес терміном "сповзання в постнормальність" (postnormal creep). Під час цього багато хто не помічає чи не хоче помічати незворотні зміни. Зокрема, якщо говорити про приватність, то переважна більшість людей не надають великого значення її поступовому зникненню. Тобто у масах домінує ставлення "don't care,"[40] і це створює ілюзію у багатьох захисників приватності, що за допомогою просвітницьких заходів серед населення можна що-небудь кардинально змінити. Натомість впливові економічні та політичні гравці схильні ігнорувати нові реалії[41] і надіються, що стратегія "business as usual" буде і надалі ефективною. Крім того, вони намагаються вживати заходів для того, щоб все працювало, як і раніше, тобто фактично займаються конструюванням штучної нормальності. Усе це призводить до "лагу постнормальності" (розрив між реальністю і тим, як її сприймають люди), який за Сардаром може зникнути лише внаслідок "постнормального прориву," коли система стає тотально постнормальною, і від цього неможливо сховатися.[42]

Детально простежимо, як усі ці процеси відбуваються (чи можуть відбуватися) у сфері приватності. Насамперед, потрібно ще раз наголосити, що звичні для нормальності підходи у такій ситуації не лише не сприяють нормалізації, а заганяють систему ще далі в стан постнормальності. Основними такими підходами у нашому випадку можна вважати: 1) повернення назад, 2) ускладнення заходів реагування, 3) збільшення контролю.

Звичною інтуїтивною реакцією на шок від постнормальності є бажання відкотити ситуацію назад до часу, коли все злагоджено працювало, чи принаймні зупинити прискорення і заглиблення в хаос. Ілюстрацією такого підходу є закріплення у законодавстві згаданого раніше принципу мінімізації даних, який, як тепер уже зрозуміло, перетворився на надбання історії. Ще одним промовистим прикладом є деякі положення Резолюції Європейського парламенту про норми цивільного права щодо робототехніки

[40] Szekely, "Building Our Future Glass Homes," 545–46.

[41] У зв'язку з цим пов'язана з приватністю реальність наповнена так званими "чорними слонами" – явищами, які настільки значні, що їх мало б бути так само легко помітити, як і слона в кімнаті. Проте багато кому все ж вдається їх не помічати. Поняття "чорні слони" поряд із поняттями "чорні лебеді" та "чорні медузи" вживають для характеристики різних стадій настання постнормальності. (John A. Sweeney, "Infectious Connectivity: Illustrating the Three Tomorrows," in *The Postnormal Reader*, ed. Ziauddin Sardar (International Institute of Islamic Thought, 2020), 18–19).

[42] Sardar and Sweeney, "The Three Tomorrows of Postnormal Times," 5.

2017 р. З-поміж іншого у документі відзначено, що необхідно у всіх випадках забезпечити можливість "звести обчислення системи штучного інтелекту до форми, зрозумілої для людей," і оснастити складних роботів " 'чорною скринькою,' яка записує дані про кожну здійснену машиною трансакцію, включаючи логіку, яка зумовила її рішення."[43] Такі позиції суттєво розходяться із прогнозами про розвиток робототехніки, які озвучують лідери цієї галузі.

Другий традиційний підхід, який залишається домінантним у розвинутих країнах Заходу, – ускладнення заходів реагування. Він означає прийняття численних нових норм, які регулюють вузькі випадки опрацювання персональних даних, започаткування нових процедур, створення додаткових органів. Проте така стратегія все далі відводить систему від суб'єкта даних. Нюанси складного законодавства доступні лише вузькому колу експертів, а комплексні ризики адекватно оцінити не може практично ніхто. Людина залишається осторонь процесів,[44] а доля її приватності залежить від хитких компромісів між владою і бізнесом. Ще важливіше, що забезпечити виконання складних норм стає все важче, і для цього потрібно все більше ресурсів, включаючи посилення контролю (третій підхід).

Про необхідність жорсткішого контролю над персональними даними говорить все більше посадовців та експертів. Авторитарна влада правомірними і неправомірними способами намагається зібрати максимальну кількість персональних даних і не дозволити, щоб вони потрапили в руки інших. У демократичних державах йдеться про пропозиції запровадити незалежне оцінювання впливу певної діяльності у сфері опрацювання персональних даних на права людини, тобто про потребу встановлення зовнішнього контролю. Приватні компанії мріють мати в своєму розпорядженні масиви персональних даних, до яких не має доступу ніхто інший. Наприклад, Ерік Шмідт та Джаред Коен, які певний час працювали на топ-посадах у Google, вважають привабливим варіант, коли технологічні гіганти будуть ділитися даними один з одним та зобов'яжуться не передавати їх нікому іншому.[45]

Проблема у тому, що намагання поставити під контроль систему, що вже "вагітна потенціалом стати постнормальною" за Сардаром повинні спричинити лише зворотний ефект.[46] Те ж саме потрібно очікувати і від ускладнення регулювання – суперечності лише загострюватимуться, а хаос наростатиме. Традиційні заходи в умовах постнормальності схожі на намагання помістити масу різнорідних елементів в один мішок, який уже тріщить по швах і в якому повно дірок. Цей мішок – це в тому числі і єдині теорії,

[43] EU, Civil Law Rules on Robotics, European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) (OJC 252, 18.7.2018, pp. 239–57), 244.

[44] Це припущення фактично підтверджують автори Посібника РЄ та ЄС у сфері захисту персональних даних, вказуючи на необхідність "переосмислення ідей особистого контролю персональних даних" (*Handbook on European Data Protection Law*, 388).

[45] Шмідт та Коен, *Новий цифровий світ*, 74.

[46] Sardar and Sweeney, "The Three Tomorrows of Postnormal Times," 5.

концепції, моделі та підходи. Для того, щоб охопити реальність, чи певну її частину, в межах єдиної моделі, неможливо не вдаватися до спрощень. Якщо ж ця реальність надскладна, як це є у теперішній час, то спрощення такі значні, що модель стає неадекватною реальності.[47]

Розглянемо деякі з таких спрощень, що зроблені в межах сучасної системи захисту приватності. Насамперед, це сам поділ даних на персональні та усі інші. Через нього виникає ілюзія нібито між першими і другими можна провести більш-менш чітку межу. Насправді за сучасних технологій така межа все більше розмивається аж до стану її повного зникнення. Свідченням цього є те, що інтернет-компанії кожної секунди опрацьовують величезні масиви даних, не вважаючи їх персональними, хоча реальний і потенційний вплив цих процесів на приватність дуже значний. Пол Квінн у спеціалізованому дослідженні відзначає, що в епоху великих даних також стає все важче розрізнити й чутливі та усі інші персональні дані, і це утруднює забезпечення передбаченого законодавством особливого захисту чутливих даних.[48]

Ще одним спрощенням є загальноприйняте розмежування публічних і приватних просторів, хоча при цьому незрозуміло, куди віднести різноманітні сайти в інтернеті, хмарні середовища, смартфон, або й навіть власну квартиру, якщо вона перетворилася в офіс для віддаленої роботи під зовнішнім наглядом. Щодо публічних просторів, то законодавство встановлює, що здійснювати відеозйомку особи можна лише за її згодою, але така згода припускається, якщо зйомка проводиться відкрито в публічних місцях.[49] Однак, коли камер стає занадто багато, вони знімають з великою роздільною здатністю, і більше того – хтось має до них чи до їхніх записів повний доступ, то кожна людина перетворюється на об'єкт для загального нагляду, і неважливо, що рішення щодо спостереження за нею не було прийняте наперед.

Вивчення впливу використання генетичних даних людини на її права розкриває низку слабких місць інституту захисту персональних даних. Зокрема руйнується переконання, що персональні дані можуть стосуватися лише одного суб'єкта даних. Коли людина дає згоду на розкриття своїх генетичних даних, цим самим вона, ймовірно, розкриває дані необмеженого кола осіб, які з нею генетично споріднені.[50] Сучасне передове законодавство покладається на анонімізацію і псевдонімізацію як ключові стратегії захисту персональних даних. Проте ефективна анонімізація генетичних даних, так щоб від них залишилася хоч якась користь, практично неможлива.[51] Ще одна новація в галузі персональних даних – право бути забутим – передбачає розмежування між приватними і публічними особами та на основі цього балансування інтересів для фор-

[47] Sardar, "Welcome to Postnormal Times," 437.
[48] Paul Quinn and Gianclaudio Malgieri, "The Difficulty of Defining Sensitive Data – The Concept of Sensitive Data in the EU Data Protection Framework," *German Law Journal* 22 (2021): 1583–612.
[49] Цивільний кодекс України, ст. 307.
[50] EU, Working Document on Genetic Data, Article 29 Data Protection Working Party (12178/03/EN WP 91, March 17, 2004): 4, 8–9.
[51] Quinn and Quinn, "Big Genetic Data," 1002.

мулювання рішення. Однак Президент України Володимир Зеленський, який наприкінці 2018 року залишався у статусі приватної особи, за кілька місяців зміг стати на чолі протилежного табору. І такі приклади зараз непоодинокі. Загалом, право бути забутим ілюструє, що темпоральний чинник має величезне значення для приватності та конкуруючих із нею інтересів, і тепер, коли час стискається і за лічені тижні можуть відбутися лавиноподібні зміни, важко залишатися впевненим щодо будь-яких впливів і ризиків.

Висновки (рішення у дусі постнормальності)

Що ж залишається робити, коли ефективність звичних підходів стрімко падає? Перш за все, потрібно визнати масштаби, неконтрольованість і незворотність змін, що відбулися, а також те, що вони ще далекі від завершення. Позитивно, що усвідомлення цього поступово з'являється не лише у роботах противників мейнстріму, але й в офіційних документах. Зокрема, у Декларації Комітету міністрів Ради Європи про маніпулятивні здатності алгоритмічних процесів 2019 р. відзначено "потребу додаткових захисних рамок, що стосуються даних, які виходять за межі сучасних понять захисту персональних даних і приватності та стосуються важливих впливів на суспільство цілеспрямованого використання даних, а також здійснення прав людини у широкому контексті."[52]

Сьогодні більшість дослідників приватності переконані, що потрібно вже зараз вживати заходи для удосконалення правового регулювання у цій сфері, інакше зовсім скоро буде вже запізно.[53] Але теорія постнормальності дає нам зрозуміти, що якщо такі заходи будуть здійснюватися винятково в межах старої парадигми, то шансів щось виправити може стати ще менше. Отже, необхідно створювати і просувати інноваційні підходи, які включають реформи у сфері регулювання приватності та поза нею. Щодо перших – варто використовувати інструментарій стратегічного форсайту із залученням стейкхолдерів, проведенням симуляцій і використанням для цього комп'ютерних технологій.

Однак усе це буде марним, якщо контекст залишиться тим самим. Тому важливо зосередити увагу на вивченні ролі інших вагомих у цій сфері регуляторів – ринку, архітектури і соціальних норм – та навчитися їх використовувати й налаштовувати в інтересах прав людини. На ринку, як мінімум, потрібно позбутися монополізації та високотехнологічних маніпуляцій, які унеможливлюють автономію учасників і баланс між інтересами продавців та покупців. Оздоровлення ринку (або винайдення його наступника) разом із розумними стратегіями влади створять сприятливі умови для виникнення альтернативних технологічних середовищ та руйнації архітектури тотального спостереження і контролю. Не менш важливо виявляти і викривати маніпуляції громадською думкою, які призводять до утвердження нових соціальних норм, вигідних

[52] Council of Europe, Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes (Decl(13/02/2019)1).
[53] Szekely, "Building Our Future Glass Homes," 550.

насамперед технологічним-гігантам і технократичній владі, що все більше віддаляється від ідеалів ліберальної демократії. У будь-якому разі теорія постнормальності вказує, що вихід потрібно шукати у децентралізації та посиленні автономності на різних рівнях, а не у створенні та зміцненні монструозних централізованих і всеохопних структур. А сфера приватності і персональних даних є хорошими індикатором того, у якому із зазначених двох напрямків рухається цивілізація.

Bibliography

Buiten, Miriam C. "'Your DNA Is One Click Away:' The GDPR and Direct-to-Consumer Genetic Testing." In *Consumer Law and Economics*, edited by Klaus Mathis and Avishalom Tor, 205–23. Springer, 2021.

Butterworth, Michael. "The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework." *Computer Law & Security Review* 34.2 (2018): 257–68.

Dawes, James. "Speculative Human Rights: Artificial Intelligence and the Future of the Human," *Human Rights Quarterly* 42.3 (2020): 573–93.

Finocchiaro, Giusella. "Anonymity and the Law in Italy." In *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, 523–37. Oxford University Press, 2009.

Funtovicz, Silvio O., and Jerome R. Ravetz. "Science for the Post-Normal Age." *Futures* 25, issue 7 (1993): 739–824.

Handbook on European Data Protection Law. Luxembourg: Publications Office of the European Union, 2018.

Holland, Mary. "How to Take a Digital Detox during the Covid-19 Pandemic." *BBC Worklife*, last modified May 18, 2020. https://www.bbc.com/worklife/article/20200513-how-to-take-a-digital-detox-during-the-covid-19-pandemic

Lessig, Lawrence. *Code: Version 2.0*. New York: Basic Books, 2006.

Markou, Christiana. "The 'Right to Be Forgotten:' Ten Reasons Why It Should Be Forgotten." In *Reforming European Data Protection Law*, 203–26. Springer, 2015.

Minkkinen, Matti. "Futures of Privacy Protection: A Framework for Creating Scenarios of Institutional Change." *Futures* 73 (2015): 48–60.

Pormeister, Kärt. "Genetic Data and the Research Exemption: Is the GDPR Going Too Far?" *International Data Privacy Law* 7.2 (2017): 137–46.

Quinn, Paul, and Gianclaudio Malgieri. "The Difficulty of Defining Sensitive Data – The Concept of Sensitive Data in the EU Data Protection Framework." *German Law Journal* 22 (2021): 1583–612.

Quinn, Paul, and Liam Quinn. "Big Genetic Data and Its Big Data Protection Challenges." *Computer Law & Security Review* 34, no. 5 (2018): 1000–18.

Rhoen, Michiel, and Qing Yi Feng. "Why the 'Computer Says No:' Illustrating Big Data's Discrimination Risk through Complex Systems Science." *International Data Privacy Law* 8, issue 2 (2018): 140–59.

Risse, Mathias. "Human Rights and Artificial Intelligence: An Urgently Needed Agenda." *Human Rights Quarterly* 41.1 (2019): 1–16.

Sardar, Ziauddin, and John A. Sweeney. "The Three Tomorrows of Postnormal Times." *Futures* 75 (2016): 1–13.

Sardar, Ziauddin. "Postnormal Times Revisited." *Futures* 67 (2015): 26–39.

Sardar, Ziauddin. "Welcome to Postnormal Times." *Futures* 42 (2010): 435–44.

Schmidt, Eric, and Jared Cohen. *The New Digital Age*. [In Ukrainian.] Lviv: Litopys, 2015.

Sukhorolskyi, Petro, and Valeriia Hutsaliuk. "Processing of Genetic Data under GDPR: Unresolved Conflict of Interests." *Masaryk University Journal of Law and Technology* 14, no. 2 (2020): 151–76.

Sukhorolskyi, Petro. *Foundations of Futures Studies*. [In Ukrainian.] Lviv: Apriori, 2021.

Sukhorolskyi, Petro. "Right to the Protection of Personal Data as a New Fundamental Human Right in Information Society." In *Wyzwania społeczeństwa informacyjnego. Polskie i ukraińskie doświadczenia*, 15–25. [In Ukrainian.] Lublin: Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, 2018.

Sweeney, John A. "Infectious Connectivity: Illustrating the Three Tomorrows." In *The Postnormal Reader*, edited by Ziauddin Sardar, 17–21. International Institute of Islamic Thought, 2020.

Szekely, Ivan. "Building Our Future Glass Homes – An Essay about Influencing the Future through Regulation." *Computer Law & Security Review* 29 (2013): 540–53.

Taylor, Mark. *Genetic Data and the Law: A Critical Perspective on Privacy Protection*. Cambridge: Cambridge University Press, 2012.

Петро Сухорольський. Майбутнє приватності крізь призму теорії постнормальності

Анотація. Теорія постнормального часу авторства Зіяуддіна Сардара є спробою пояснити процеси, що відбуваються у суспільстві, в умовах, коли традиційні моделі, теорії та парадигми виявляються безсилими перед новими викликами, які насуваються на світ одночасно великою лавиною. Постнормальні часи – це проміжний період, який наступає тоді, коли старі уявлення, теорії та практики помирають, а нові ще не сформувалися, і здається, що увесь світ занурюється у непевність, хаос та суперечності. Приватність є однією зі сфер, ситуація у яких вже зараз є постнормальною. Тому у статті зроблена спроба окреслити сучасний стан і перспективи розвитку процесів, що стосуються приватності та захисту персональних даних, на основі методології, розробленої у межах теорії постнормального часу.

Трьома головними ознаками постнормальності є складність, хаос та суперечності. Усі вони значною мірою характерні для сфери приватності. Зокрема, вплив головних сучасних стратегій правового захисту персональних даних (до яких відносять покладання на згоду суб'єкта даних як одну з основних підстав для опрацювання даних, а також використання анонімізації та псевдонімізації, чи запровадження механізму зовнішньої оцінки ризиків) зовсім не є однозначним. Окрім того, стверджується, що у сучасному світі існує базова суперечність між приватністю і глибинними тенденціями розвитку бізнесу та публічного управління, причини якої допомагає зрозуміти теорія чотирьох регуляторів суспільних відносин Лоуренса Лессіґа.

За таких умов традиційні підходи реагування на виклики – намагання повернути назад, ускладнення заходів реагування, збільшення контролю – не лише не сприяють нормалізації, а заганяють систему ще далі у стан постнормальності. Це супроводжується загостренням існуючих та виявленням все нових і нових критичних суперечностей і збільшує ймовірність колапсу діючої системи захисту приватності у близькій перспективі. Тому необхідно розробляти і просувати інноваційні підходи, які включають як реформи у сфері регулювання приватності, так і зусилля щодо зміни зовнішнього середовища.

Ключові слова: захист персональних даних; права людини; інформаційне право; генетичні дані; постнормальні часи; футурологія; регулювання кодом; штучно сконструйована нормальність.

Петр Сухорольский. Будущее приватности сквозь призму теории постнормальности

Аннотация. Теория постнормального времени авторства Зияуддина Сардара является попыткой объяснить происходящие в обществе процессы в условиях, когда традиционные модели, теории и парадигмы оказываются бессильными перед новыми вызовами, которые надвигаются на мир одновременно большой лавиной. Постнормальные времена – это промежуточный период, наступающий тогда, когда старые представления, теории и практики умирают, а новые еще не сформировались, и кажется, что весь мир погружается в неуверенность, хаос и противоречия. Приватность является одной из сфер, ситуация в которых уже сейчас является постнормальной. Поэтому в статье предпринята попытка очертить современное состояние и перспективы развития процессов, касающихся приватности и защиты персональных данных, на основе методологии, разработанной в рамках теории постнормального времени.

Тремя главными признаками постнормальности являются сложность, хаос и противоречия. Все они во многом характерны для сферы приватности. В частности, влияние главных современных стратегий правовой защиты персональных данных (к которым относятся закрепление согласия субъекта данных как одного из основных оснований обработки данных, а также использование анонимизации и псевдонимизации, или создание механизма внешней оценки рисков) вовсе не однозначно. Кроме того, утверждается, что в современном мире существует базовое противоречие между приватностью и глубинными тенденциями развития бизнеса и публичного управления, причины которого раскрывает теория четырех регуляторов общественных отношений Лоуренса Лессига.

В таких условиях традиционные способы реагирования на вызовы – попытки повернуть назад, усложнение мер реагирования, увеличение контроля – не только не способствуют нормализации, а загоняют систему еще дальше в состояние постнормальности. Это сопровождается обострением существующих и обнаружением все новых и новых критических противоречий и увеличивает вероятность коллапса действующей системы защиты приватности в ближайшей перспективе. Поэтому необходимо разрабатывать и продвигать инновационные подходы, включающие как реформы в сфере регулирования приватности, так и усилия по изменению внешней среды.

Ключевые слова: защита персональных данных; права человека; информационное право; генетические данные; постнормальные времена; футурология; регулирование кодом; искусственно сконструированная нормальность.

Petro Sukhorolskyi. The Future of Privacy Through the Lens of Postnormal Times Theory

Abstract. The theory of postnormal times by Ziauddin Sardar is an attempt to explain the social processes occurring when traditional models, theories, and paradigms seem powerless in the face of looming challenges. Postnormal times are an intermediate period when old ideas, theories, and practices are dying and new ones have not yet been formed, and the whole world seems to be plunged into uncertainty and chaos. Privacy is one of the areas where the situation is considered to be already postnormal. Therefore, the article attempts to outline the current state and prospects related to privacy and personal data protection, based on the methodology developed within the theory of postnormal times.

Complexity, chaos, and contradictions are the main forces propelling postnormal times. All of them are very perceptible in the sphere of privacy. In particular, the outcomes of the major current

strategies for the legal protection of personal data are ambiguous and controversial. It relates to the consent of the data subject as one of the main legal grounds for personal data processing, as well as the use of data anonymization and pseudonymization techniques, or the introduction of mechanisms of external risk assessment. In addition, it is argued that in the present world there is a fundamental contradiction between privacy and underlying trends in business and governance, the causes of which are revealed by applying Lawrence Lessig's theory of four regulators.

Under such conditions, traditional ways of responding to challenges – turning back, increasing control and complexity of measures – not only contribute to normalization, but drive the system even further into a state of postnormalcy. It is accompanied by the exacerbation of identified critical contradictions and revealing of the new ones that increases the likelihood of collapse of the existing system of privacy protection in the near future. Therefore, it is necessary to develop and promote innovative approaches which include both reforms in the field of privacy regulation and efforts to change the external environment.

Keywords: personal data protection; human rights; information law; genetic data; postnormal times; futures studies; regulation by code; manufactured normalcy.

Одержано/Received 10.04.2022