

Марко Олексій Володимирович

Виклики демократії в епоху цифровізації

УДК 342.34

DOI <https://doi.org/10.24195/2414-9616.2025-3.13>

Марко Олексій Володимирович
аспірант
Інституту держави і права імені
В. М. Корецького Національної академії
наук України
вул. Трьохсвятительська, 4, Київ,
Україна
ORCID: 0009-0006-0461-8934

У статті розглянуто проблеми, що постають перед демократією у зв'язку з широким впровадженням новітніх інформаційно-комунікаційних технологій. Відзначено, що основний виклик цифрової епохи полягає у нівелюванні фундаментальних прав і цінностей, які покликана захищати і плекати демократія, що вимагає пошуку нових способів розуміння та захисту цих цінностей та фундаментальних прав і свобод. Відповідно, посилення демократії на сучасному етапі вимагає вжиття заходів у трьох напрямках: 1) адекватного нормативно-правового регулювання; 2) посилення захисту етичних цінностей, що лежать в основі демократії (автономії, справедливості, солідарності, рівності та недискримінації); 3) гарантування автономії та самовизначення окремих осіб та спільнот. Відзначено, що в епоху цифровізації найбільш вразливими характеристиками демократії є незалежні медіа, свобода слова, що підкреслює особливу роль етики, яка допомагає формувати інституції, політику, технології, закони та управління в цифрову епоху. Основні ризики цифровізації демократичним інституціям полягають у легкості поширення шкідливої інформації та браку прозорості, необхідності переосмислення приватності, впровадження тотального спостереження за особами та створення сприятливих умов для зовнішнього втручання у внутрішні справи держави, насамперед у виборчий процес. Для протидії дезінформації необхідно забезпечити захист, безпеку та розширення прав і можливостей журналістів та інших працівників медіа, а також визнати важливу роль аналітичних центрів та інших організацій громадянського суспільства у сприянні рефлексивним та поінформованим політичним дебатам. Приватність у цифрову епоху слід розуміти не лише як право особи на свободу від неправомірного втручання, а й як позитивне право на простір для розвитку та самовираження. Тотальне спостереження та широке використання алгоритмів у прийнятті рішень призводять до того, що громадяни позбавляються можливості від участі або оскаржити рішення, ухвалені у край непрозорий спосіб. Регуляторні заходи проти зловмисного іноземного втручання та їх застосування не повинні ослаблювати основу довіри та єдності в суспільстві, а спрямовуватися на підтримку та захист демократичних цінностей та інституцій.
Ключові слова: демократія, цифровізація, держава, громадянське суспільство, інформація, медіа, приватність, стеження, вибори, етика.

Вступ. Останніми роками демократія стикнулася з серйозними викликами, включаючи поширення неправдивої інформації та дезінформації. Разом з іншими проявами несправедливості вони посилюють політичну поляризацію та популізм, а також збільшують нерівність, негативно впливаючи на взаємовідносини між державою і громадянським суспільством. Низка найпередовіших інформаційно-комунікаційних технологій роблять ці виклики ще більш загрозливими.

Основний виклик цифрової епохи полягає у нівелюванні фундаментальних прав і цінностей, які покликана захищати і плекати демократія, насамперед такі як справедливість, рівність і солідарність. Нові виклики цифровізації вимагають пошуку нових способів розуміння та захисту цих цінностей та фундаментальних прав і свобод. Зокрема, приватність мало розуміти не лише як негативне право на свободу від необґрунтованого втручання в особисте життя, але і як позитивне право, яким володіє кожна особа без відстеження її діяльності та збору даних про неї. Держава має використовувати найкраще, що можуть запропонувати цифрові технології, для захисту і зміцнення верховенства народу в глибокому сенсі, а також для створення взаємної довіри між усіма особами, що проживають на її території, та посилення громадянської активності.

В епоху цифровізації особливу роль для належного функціонування демократичних інституцій мають громадянська свідомість і визнання соціальної, політичної та економічної рівності в суспільстві. Відповідно, демократія вимагає не лише простого визнання того, що інші можуть в кінцевому підсумку отримати більше користі від широко розповсюджених принципів розподільчої справедливості, а й громадянської солідарності та взаємності, які підтримують справедливі результати.

Мета і завдання. Метою статті є аналіз основних викликів демократії породжених цифровізацією, зокрема їх вплив на відносини між державою та громадянським суспільством. Відповідно завданням є виділення та розгляд основних ризиків, породжених повсюдним впровадженням найновіших інформаційно-комунікаційних технологій.

Методи дослідження. Для досягнення поставленої мети використано комплекс загальних та спеціальних методів дослідження, зокрема аналіз та синтез, системний аналіз для з'ясування впливу технологій на соціальні відносини, та порівняння для виявлення відмінностей між «паперовою» та «цифровою» епохами.

Результати. Цифрові трансформації останніх десятиліть мали амбівалентний вплив на демократію. З одного боку, цифрові технології створили нові майданчики для обміну думками та демокра-

тичної участі, але з іншого – вони також змінили поділ влади як на глобальному рівні, так і всередині країн. У результаті іноземні уряди, корпорації й мільярдери отримали нові можливості для втручання у виборчий процес, маніпулювання громадською думкою або поширення шкідливої інформації по всьому світу, що безпосередньо впливає на основні цінності демократії [5]. Загалом ризики та переваги цифрових технологій залежать від того, як вони розробляються та регулюються, а також від того, як використовуються. Іншими словами, на них також впливають домінуючі у суспільстві цінності.

Зміцнення демократії в епоху цифровізації вимагає вжиття заходів у трьох напрямках. По-перше, впровадження адекватного нормативно-правового регулювання, що має гарантувати, що передові технології слугуватимуть насамперед громадянам, а не лише приносять вигоду політичній еліті чи технократам.

По-друге, посилення захисту етичних цінностей, що лежать в основі демократії, зокрема автономії, справедливості, солідарності, рівності та недискримінації. Так у сучасний період значної асиметрії владних відносин між окремими особами, з одного боку, і приватними компаніями, які використовують дані користувачів, з іншого, згода на використання даних часто є передумовою доступу до (іноді навіть державних) товарів і послуг. Тому не можна вважати, що громадяни добровільно погоджуються на використання своїх даних іншими суб'єктами підприємницької діяльності.

По-третє, гарантування автономії та самовизначення окремих осіб та спільнот, які перебувають у небезпеці через втрату демократичними урядами контролю над основними державними функціями і наданням суспільних благ, оскільки вони дедалі частіше передаються, повністю або частково, приватним структурам.

При цьому слід пам'ятати, що світ онлайн структурно відрізняється від світу офлайн як з точки зору розміру мережі, так і з точки зору якості зв'язків між людьми, а також між користувачами й провайдерами. Для онлайн світу характерні слабкі зв'язки між людьми та відсутність чітких критеріїв достовірності поширюваної інформації. Корозія демократії посилюється ключовими особливостями економіки уваги та платформ з її методами персоналізації та сегментації аудиторії, маніпулятивним таргетингом і та непрозорими схемами власності вебсайтів. Стрімкий розвиток штучного інтелекту (ШІ) вже змінює виробництво та розповсюдження інформації, але оцінити наслідки широкомасштабного використання ШІ поки що досить складно. Так боти зі штучним інтелектом можуть створити безліч нових джерел дезінформації, відтворювати шкідливий та упереджений контент, призводити

до порушення права на приватність і завдавати значних екологічних збитків [12].

Можна стверджувати, що поки що наші суспільства не готові мати справу з технологією, яка переконливо видає себе за рупор істини, в той час, як вона не має наміру, волі, здатності створювати смисли й не може бути притягнута до відповідальності [19]. Тому слід ініціювати широке суспільне обговорення щодо таких соціотехнічних механізмів, які мають базуватися на основі загальноприйнятих цінностей.

У результаті бурхливого розвитку інформаційно-комунікаційних технологій демократія та основоположні права, які її підтримують і на які вона спирається, стикнулися з серйозною загрозою, що змусило дослідників навіть говорити про деконсолідацію звичного демократичного устрою на Заході [6]. У світі протягом останнього десятиліття неухильно зростає кількість авторитарних та інших форм гібридних режимів, про що свідчить ціла низка індексів розвитку демократії. Деякі з них виникають внаслідок занепаду існуючих демократій, як це відбувається при зростанні популізму. Такі режими включають демократичні елементи в те, що, по суті, є гібридними політичними системами. Їм бракує вільних і чесних виборів, загального виборчого права, незалежності судової влади, вільних медіа та інших засобів захисту прав людини, але їхні лідери видають їх за справжню волю народу. Популісти часто висловлюють своє захоплення такими авторитарними режимами, описуючи їх «чистішу» форму демократії, протиставляючи народ елітам [13]. Як слушно стверджують дослідники демократії С. Левітський та Д. Зіблатт, «трагічний парадокс електорального шляху до авторитаризму полягає в тому, що вбивці демократії використовують ті ж самі інститути демократії – поступово, тонко і навіть легально – для її вбивства» [11, р. 8].

Ознаками демократичної держави, які найшвидше піддаються корозії в останні роки, є «незалежні ЗМІ, що заслуговують на довіру», «свобода вираження поглядів» та «доступ до альтернативних джерел інформації» [7]. У кожному випадку зниження частково є наслідком зростаючого впливу цифрових медіа. У цьому контексті особлива роль відводиться етиці, яка з погляду моральних вимог і моральних міркувань допомагає формувати інституції, політику, технології, закони та управління в цифрову епоху. Донедавна робилися спроби звести етику до саморегулювання, що перетворили її на перешкоду для інновацій та призвело до скорочення фінансування досліджень у галузі соціальних і гуманітарних наук [18; 21]. Водночас стало цілком зрозуміло, що неможливо уникнути розв'язання фундаментальних етичних проблем та складних питань передових цифрових суспільств. Адже від відповідей на питання про те,

як ми хочемо жити й в якому суспільстві залежить майбутнє наших дітей.

У найбільш загальному вигляді ризику, які несе у собі цифровізація для демократичних інституцій зводиться до шкідливої інформації та браку прозорості, переосмислення приватності, тотального спостереження та зовнішнього втручання.

1. Шкідлива інформація та брак прозорості. Сьогодні, коли значна частина публічної сфери знаходиться в Інтернеті, наприклад, на платформах соціальних мереж, власники більшості цих платформ отримують вигоду від мови ненависті та поляризації поглядів. Чим більша брехня, обурливіші наклепи та переконливіші конспірологічні наративи, тим довше і більше людей залишаються на платформах, генеруючи прибутки для їх власників. Як показують нещодавні скандали, пов'язані з маніпулюванням виборцями та підбурюванням до насильства на расовому та сексуальному ґрунті, мережеві платформи, хоча й вони позиціонують себе як нейтральні інфраструктури, які не несуть відповідальності за поширюваний контент, можуть слугувати інтересам потужних політичних та економічних акторів [9; 15]. Чим більше приватних корпорацій перебирають на себе державні функції, тим більше непрозорими, нерівними і навіть небезпечними стають публічні простори.

Існують також ризики, пов'язані з використанням платформ як джерела новин. Якщо дедалі менше людей отримують новини з незалежних ЗМІ з контролем якості, а все більше – з платформ соціальних мереж, то спільна інформаційна реальність людей звужується. Вона розпадається на дедалі менші та фрагментованіші групи однодумців, оскільки алгоритми платформ визначають групи людей, які демонструють схожі поведінкові моделі (на основі «вподобайок» на вебсайтах і в соціальних мережах або даних про покупки), і пропонують їм персоналізовану інформацію, яка може бути для них релевантною та цікавою. У результаті громадяни отримують дедалі менше інформації про реальний стан справ, що ускладнює їхнє ставлення до розмаїття як такого. У результаті вони можуть мати викривлене уявлення про реальність і вважати, що їх оточують лише однодумці. Ми є свідками структурного зсуву влади від прозорих, немонополістичних публічних просторів до невідзвітних, орієнтованих на прибуток просторів, які можуть бути змінені, закриті або використані в особливих цілях за бажанням кількох впливових акторів [4].

У цьому контексті необхідно терміново забезпечити захист, безпеку та розширення прав і можливостей журналістів та інших працівників медіа [3], а також визнати важливу роль аналітичних центрів та інших організацій громадянського суспільства у сприянні рефлексивним та поінформованим політичним дебатам. Зміцнення ЗМІ та покращення журналістських стандартів передбачає надання

достатнього державного фінансування, програми підтримки журналістських розслідувань, а також покращення послуг з перевірки фактів та індексів довіри.

2. Переосмислення приватності. Вважається, що зростаюче документування життя і тіла людей, тобто все більша фіксація специфічно людських практик і характеристик у вигляді цифрових даних різного роду, змінило розуміння людьми приватності [8]. Однак це не означає, що люди стали менше піклуватися про неї: конфіденційність залишається важливою для громадян, але дехто вже змирився з тим, що повинен погодитися на використання даних про себе для отримання доступу до послуг та інструментів, необхідних у повсякденному житті [16]. Багато хто втратив надію на те, що їхнє приватне життя може бути повністю і ефективно захищене в сучасному світі. Крім того, не можна ігнорувати той факт, що інформація, яка описує, на що людина погоджується, коли приймає політику конфіденційності вебсайту, є невинуватено довгою, технічно складною і незрозумілою для багатьох людей. З цієї точки зору, можна сказати, що нинішня система згоди функціонує більше як відмова від відповідальності для тих, хто отримує дані, ніж як посилення права на приватність.

Відповідно, ефективний захист приватності в епоху цифровізації повинен виходити за рамки захисту, характерного для «паперового» періоду. Нині уже недостатньо забезпечити, щоб люди надавали згоду на використання їхніх даних. Згода на використання даних стала передумовою для отримання доступу до основних послуг, таких як комунікаційні та новинні платформи, а іноді навіть медичні послуги. Це може бути ефективним для компаній, але не є ефективним як усвідомлений вибір, оскільки оцінка та інформування про ризики, пов'язані з обробкою даних, пов'язані з труднощами. Конфіденційність у цифрову епоху слід розуміти як щось більше, ніж просто право особи на свободу від неправомірного втручання. Це також і позитивне право на простір для розвитку та самовираження.

Отже, приватність цінна не лише тому, що персональні дані, отримані компаніями, можуть бути використані для негативного впливу на життєві шанси людини (наприклад, підвищення страхових внесків для особи після отримання інформації про її спосіб життя чи стан здоров'я). Приватність – це простір для розвитку власної ідентичності, яка не продиктована виключно соціальними умовами.

3. Тотальне спостереження. Суспільствознавці десятиліттями вивчають згубний вплив технологій стеження на формування та функціонування особистості. Вони стверджують, що усвідомлення того, що за тобою наглядають, змінює поведінку людей [8]. Знаючи про «спостерігача» особа

починає змінювати свій спосіб життя, мислення та й свій характер, тобто нагляд обмежує автономію людини. Сьогодні він децентралізований, завдяки пристроям самоконтролю, інтернету речей та соціальним мережам. Таке спостереження здійснюється уже не лише вертикально (зверху), але й горизонтально, коли ми ділимося інформацією з іншими й стежимо самі за собою. Вона також є повсюдною, оскільки не обмежується мурами в'язниці, школи чи лікарні, а постійно проявляється у багатьох сферах суспільного життя. Приватність та пов'язані з нею цінності наразі перебувають під загрозою через постійний збір даних, профілювання, спонукання та прогнозування, що характеризують цифрову епоху.

Ситуація погіршується й тим, що алгоритми та автоматизовані системи прийняття рішень все частіше впроваджуються у сферах, які є життєво важливими для функціонування здорових демократій, зокрема в державному управлінні [17], правоохоронних органах, освіті [1], охороні здоров'я [10] та процедурах найму на роботу [20]. Хоча ці системи покликані підвищити ефективність і об'єктивність процедур прийняття рішень, однак вони навчаються на даних, які самі по собі містять упередження та забобони, а отже, неминуче впроваджують або відтворюють ці упередження. Досвід показує, що рішення та рекомендації, які виробляють ці системи, часто призводять до дискримінаційних наслідків, як правило, щодо вже вразливих груп суспільства, таких як різноманітні меншини, жінки та економічно незахищені групи. Більше того, оскільки ці системи стають дедалі більш інтегрованими в державні сектори, люди не завжди мають можливість відмовитися від участі або оскаржити рішення, ухвалені у вкрай непрозорий спосіб [14].

4. Іноземне втручання. Ще однією проблемою, яку створила для демократії цифровізація, є створення сприятливих умов для втручання приватних або державних акторів у внутрішні справи інших держав. Одним із прикладів є розробка і використання приватними компаніями і навіть іноземними спецслужбами шкідливого програмного забезпечення для промислового шпигунства або отримання доступу до конфіденційної інформації інших країн.

Тому особливо важливо розробити й впровадити заходи для зміцнення стійкості демократій на глобальному та міжнародному рівнях. Так шпигунство можна розглядати в рамках міжнародного публічного права, посилаючись на норми, що регулюють відносини між державами і поведінкою державних суб'єктів, такі як принцип невтручання або рамки, передбачені дипломатичним правом і правами людини.

Деякі країни розглядають державний суверенітет у кіберпросторі як норму міжнародного права, що може бути порушена як приватними, так і дер-

жавними акторами. В рамках державних кордонів такий суверенітет дозволяє державам самостійно регулювати питання, що стосуються кіберпростору, а поза ними – гарантує як територіальну цілісність держав, так і їхню політичну незалежність.

Регулювання іноземного втручання пов'язане з проблемою пошуку балансу між відкритістю й міжнародним співробітництвом та захистом демократичних систем і фундаментальних прав. Виявлення прихованих зловмисних дій вимагає підвищення прозорості та підзвітності в багатьох сферах – від платформ соціальних мереж до виробництва новин, а також науково-дослідних та інших організацій. Однак це не повинно відбуватися за рахунок послаблення цих інституцій, а також свобод і прав людей, багато з яких є ключовими для процвітання демократії, як підкреслюють організації громадянського суспільства [2]. Регуляторні заходи проти зловмисного іноземного втручання та їх застосування не повинні ослабляти основу довіри та єдності в суспільстві, а спрямовуватися на підтримку та захист демократичних цінностей та інституцій. Тут особливої уваги потребують непередбачувані наслідки заходів, а також заходи, які можуть бути інструменталізовані та використані для ослаблення демократичних інституцій.

Висновки. Епоха цифровізації несе у собі нові виклики демократичним інституціям, що проявляється насамперед у нівелюванні фундаментальних прав і цінностей, які покликана захищати і плекати демократія, насамперед такі як справедливість, рівність і солідарність. Відповідно, посилення демократії на сучасному етапі вимагає вжиття заходів у трьох напрямках: 1) адекватного нормативно-правового регулювання; 2) посилення захисту етичних цінностей, що лежать в основі демократії (автономії, справедливості, солідарності, рівності та недискримінації); 3) гарантування автономії та самовизначення окремих осіб та спільнот. Основні ризики цифровізації демократичним інституціям полягають у легкості поширення шкідливої інформації та браку прозорості, необхідності переосмислення приватності, впровадження тотального спостереження за особами та створення сприятливих умов для зовнішнього втручання у внутрішні справи держави, насамперед у виборчий процес.

ЛІТЕРАТУРА:

1. Bedginfield, W. (2020). Everything that went wrong with the botched A-Levels algorithm. Wired, <https://www.wired.co.uk/article/alevel-exam-algorithm>
2. Civil Society Europe & Philea (2023). Joint Civil Society Contribution to the Defence of Democracy Package. URL: <http://civilsocietyeurope.eu/we-need-a-new-pillar-on-civil-society-to-defend-democracy/>
3. Commission Recommendation (EU) 2021/1534 of 16 September 2021 on ensuring the protection, safety and empowerment of journalists and other media

professionals in the European Union. URL: https://www.stradalex.eu/en/se_src_publ_leg_eur_jo/toc/leg_eur_jo_3_20210920_331/doc/ojeu_2021.331.01.0008.01

4. European Parliament (2019). Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States. URL: [https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU\(2019\)608864](https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2019)608864)

5. European Parliament (2021) Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States. European Parliament, 2021. URL: [https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU\(2021\)653633](https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653633)

6. Foa, R.S., Mounk, Y. (2017). The signs of deconsolidation. *Journal of democracy*, vol. 28, no. 1, pp. 5–15.

7. Freedom in the World 2023: Marking 50 Years in the Struggle for Democracy. Freedom House, 2023. URL: <https://freedomhouse.org/report/freedom-world/2023/marking-50-years>

8. Friedewald, M., Burgess, J.P., Čas, J., Bellanova, R., Peissl, W. (2017). Surveillance, privacy and security. Taylor & Francis.

9. Hinds, J., Williams, E.J., Joinson, A.N. (2020). “It wouldn’t happen to me”: Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*, vol. 143, pp. 102498.

10. Ledford, H. (2019). Millions of black people affected by racial bias in health-care algorithms. *Nature*, vol. 574, pp. 608–609.

11. Levitsky, S., Ziblatt, D. (2019). *How democracies die*. London; Crown.

12. Marcus G. AI Platforms like ChatGPT Are Easy to Use but Also Potentially Dangerous. *Scientific American*, 2022. URL: <https://www.scientificamerican.com/article/ai-platforms-like-chatgpt-are-easy-to-use-but-also-potentially-dangerous/>

13. Mudde, C., Kaltwasser, C.R. (2017). *Populism: A very short introduction*. Oxford: Oxford University Press.

14. Pasquale, F. (2016). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard: Harvard University Press.

15. Tech Transparency Project, 2023. Meta Creates Pages for ISIS, Undermining Anti-Terrorism Efforts. URL: <https://www.techtransparencyproject.org/articles/meta-creates-pages-for-isis-undermining-anti-terrorism-efforts>

16. Turow, J., Hennessy, M., Draper, N. (2015). The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. A Report from the Annenberg School for Communication, University of Pennsylvania.

17. Van Bekkum, M., Borgesius, F.Z. (2021). Digital welfare fraud detection and the Dutch SyRI judgment. *European Journal of Social Security*, vol. 23, no. 4, pp. 323–340.

18. Van Dijk, N., Casiraghi, S., Gutwirth, S. (2021). The ‘Ethification’ of ICT Governance. *Artificial Intelligence and Data Protection in the European Union*. *Computer Law & Security Review*, vol. 43, p.105597.

19. Weil E. You Are Not a Parrot And a chatbot is not a human. And a linguist named Emily M. Bender is very worried what will happen when we forget this. *Intelligencer*, 2023. URL: <https://nymag.com/intelligencer/article/ai-artificial-intelligence-chatbots-emily-m-bender.html>

20. Whittaker, M., Alper, M., Bennett, C.L., Hendren, S., Kaziunas, L., Mills, M., Ringel Morris, M., Rankin, J., Rogers, E., Salas, M., Myers West, S. (2019). Disability, Bias, and AI. *AI Now Institute at NYU*, <https://ainowinstitute.org/disabilitybiasai-2019.pdf>

21. Yeung, K., Howes, A., Pogrebná, G. (2020). AI Governance by Human Rights–Centered Design, Deliberation, and Oversight. *The Oxford handbook of ethics of AI*, pp. 77–106.

Challenges to democracy in the digital age

Marko Oleksii Volodymyrovych

Postgraduate Student

V. M. Koretsky Institute of State and Law
of the National Academy of Sciences
of Ukraine

Trykhsvyatytelska str., 4, Kyiv, Ukraine
ORCID: 0009-0006-0461-8934

The article examines the problems faced by democracy in connection with the widespread introduction of the latest information and communication technologies. It is noted that the main challenge of the digital era is the levelling of fundamental rights and values that democracy is designed to protect and nurture, which requires finding new ways to understand and protect these values and fundamental rights and freedoms.

Accordingly, strengthening democracy at the present stage requires measures in three areas: 1) adequate regulatory and legal regulation; 2) strengthening the protection of ethical values underlying democracy (autonomy, justice, solidarity, equality and non-discrimination); 3) guaranteeing the autonomy and self-determination of individuals and communities. It is noted that in the digital era, the most vulnerable characteristics of democracy are independent media and freedom of speech, which emphasises the special role of ethics, which helps to shape institutions, policies, technologies, laws and governance in the digital era. The main risks of digitalisation to democratic institutions are the ease of dissemination of harmful information and lack of transparency, the need to rethink privacy, the introduction of total surveillance of individuals and the creation of favourable conditions for external interference in the internal affairs of the state, especially in the electoral process. To counter disinformation, the protection, safety and empowerment of journalists and other media professionals should be ensured, and the important role of think tanks and other civil society organisations in promoting reflective and informed political debate should be recognised. Privacy in the digital era should be understood not only as an individual's right to freedom from unlawful interference, but also as a positive right to space for development and self-

expression. Total surveillance and the widespread use of algorithms in decision-making lead to citizens being deprived of the opportunity to participate or challenge decisions made in a highly opaque manner. Regulatory measures against malicious foreign interference and their application should not weaken the basis of trust and unity in society, but should aim to support and protect democratic values and institutions.

Key words: democracy, digitalisation, state, civil society, information, media, privacy, surveillance, elections, ethics.