ВИБОРИ
ЦИФРОВІ ТЕХНОЛОГІЇ
ПРАВА ЛЮДИНИ

Документи
Ради Європи

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

ВИБОРИ
ЦИФРОВІ ТЕХНОЛОГІЇ
ПРАВА ЛЮДИНИ

Документи
Ради Європи

Рада Європи

Ця збірка розроблена Управлінням з виборів і громадянського суспільства Ради Європи та перекладена українською мовою за сприяння та в рамках проєкту Ради Європи «Підтримка прозорості, інклюзивності та чесності виборчої практики в Україні».

Неофіційний переклад документів здійснено за редакцією д.ю.н. Ключковського Ю.Б., Президента Інституту виборчого права.

Збірка має на меті підвищення громадської обізнаності про стандарти та політики Ради Європи у відповідній сфері. Документи, які увійшли до збірки, не обов'язково всеохоплюючі, повні, точні та оновлені. Цю збірку розроблено виключно для цілей інформування. Щоб отримати професійну або правову пораду, будь ласка, звертайтеся до належно кваліфікованого професіонала.

Усі права захищено. Заборонено перекладати, відтворювати та розповсюджувати в будь-якій формі чи будь-якими засобами, електронними (на компакт-дисках, у мережі Інтернет тощо) або механічними, включно з фотокопіюванням, записом чи збереженням на будь-якому з інформаційних носіїв чи систем відтворення, якусь із частин цієї публікації без попереднього письмового дозволу Директорату комунікацій (F-67075 Strasbourg Cedex або publishing@coe.int).

Оформлення обкладинки та верстка: Катерина Кисла

Фото на обкладинці: Shutterstock

Видавництво Ради Європи (F-67075 Strasbourg Cedex book.coe.int).

© Рада Європи, березень 2020 р., англійська версія: "Elections. Digital Technologies. Human Rights"
© Рада Європи, березень 2020 р., переклад українською мовою

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Зміст

Резолюція 1459 (2005)[1]
Парламентської Асамблеї Ради Європи

Про усунення обмежень на право голосу

1. Парламентська Асамблея відповідно до своєї Рекомендації 1500(2001) «Про участь іммігрантів та іноземців-резидентів у політичному житті держав-членів Ради Європи» підкреслює значення права голосу й права на висування своєї кандидатури на виборах як основоположної передумови збереження інших основних громадянських і політичних прав, що захищаються Радою Європи. Виборчі права – це основа для демократичної легітимації та представницького характеру політичного процесу. Тому вони повинні розвиватися, щоб відповідати поступу сучасних суспільств на шляху до більш інклюзивної демократії.

2. Із цією метою, відповідно до висновку Європейської комісії «За демократію через право» (Венеційської комісії), прийнятого у грудні 2004 року, Асамблея запрошує держави-члени і спостерігачів організації переглянути всі існуючі обмеження виборчих прав та скасувати ті з них, які більше не є необхідними і пропорційними для досягнення законної мети.

3. Асамблея вважає, що пріоритетом, зазвичай, повинно бути надання ефективних вільних і рівних виборчих прав максимально великій кількості громадян, незалежно від їхнього етнічного походження, місця проживання, стану здоров'я, статусу військовослужбовця чи наявності судимості. Належно варто брати до уваги право голосу тих громадян, які проживають за кордоном.

4. Відповідно до практики Європейського суду з прав людини будь-які винятки з цього правила повинні бути передбачені законом, мати законну мету та не бути свавільними або непропорційними.

---

1. Дебати Асамблеї 24 червня 2005 року (24-е засідання) (див. Док. 10553, доповідь Комітету з правових питань та прав людини, доповідач: пан Екер, та Док. 10577, висновок Комітету з політичних питань, доповідач: лорд Джон Томільсон). Текст ухвалено Асамблеєю 24 червня 2005 року (24-е засідання).

   Оригінал тексту доступний на веб-сторінці за посиланням: www.assembly.coe.int.

5. Усі резиденти зобов'язані платити місцеві податки, а рішення місцевих органів влади безпосередньо впливають на їхнє життя. Тому право голосувати та брати участь як кандидати у місцевих виборах повинно надаватися всім легальним резидентам незалежно від їхнього громадянства чи етнічного походження. У зв'язку з цим Асамблея закликає відповідні країни виконувати рекомендації Комісара з прав людини про надання такого права резидентам, які мають особливий статус «негромадян» відповідно до Конвенції про участь іноземців у суспільному житті на місцевому рівні (ETS № 144).

6. З огляду на можливість конфлікту лояльності між державою, громадянином якої є відповідна особа, і країною проживання особи, право голосувати та балотуватися на національних виборах (парламентських або президентських) загалом повинно бути пов'язаним із громадянством. Особи, які мають множинне громадянство, повинні мати право вільно обирати, у якій країні вони бажають реалізувати своє право голосу.

7. Враховуючи значення права голосу в демократичному суспільстві, держави-члени Ради Європи повинні забезпечувати своїм громадянам, які проживають за кордоном, можливість голосувати на національних виборах з урахуванням складності різних виборчих систем. Вони повинні вжити відповідних заходів із тим, щоб максимально полегшити реалізацію такого права голосу, зокрема, розглядаючи можливість дистанційного голосування (поштою), голосування у консульських установах чи електронного голосування, відповідно дотримуючись Рекомендації Rec(2004)11 Комітету Міністрів державам-членам про правові, операційні та технічні стандарти е-голосування. Держави-члени мають співпрацювати між собою з цією метою та утримуватися від створення непотрібних перешкод на шляху ефективного здійснення права голосу з боку іноземних громадян, які проживають на їх території.

8. Беручи до уваги, що кінцевою метою кримінального покарання є перевиховання ув'язнених із метою повернути їх до суспільства з усіма правами та обов'язками, які мають інші громадяни, Асамблея висловлює жаль щодо того, що в багатьох країнах особи, засуджені за вчинення злочинів, позбавлені можливості голосувати, у деяких випадках навіть протягом певного часу після закінчення терміну ув'язнення. Більш сучасний підхід повинен полягати в тому, щоб позбавлення права голосу наставало лише за злочини проти демократичного процесу (наприклад, фальсифікація виборів, протиправний тиск на виборців чи кандидатів, участь у збройному путчі, участь у терористичній діяльності, встановлені рішенням суду). У будь-якому випадку, беручи до уваги рішення Європейського суду з прав людини у справі «Герст проти Сполученого Королівства» (Hirst v. the United Kingdom) (від 30 червня 2004 року), національні парламенти повинні переглянути наявні обмеження та визначити, чи дійсно вони все ще спрямовані на досягнення законної мети та чи не є свавільними або непропорційними.

9. Як підкреслювала Венеційська комісія, потреба демократичного контролю за збройними силами не повинна використовуватися як виправдання для автоматичного позбавлення військовослужбовців їхнього права голосу.

10. Асамблея також підкреслює важливість захисту права голосу вразливих категорій населення, таких як особи, які проживають у будинках для людей похилого віку, ув'язнені, солдати та особи з інвалідністю. Повинні бути вжиті відповідні заходи для того, щоб уникнути необґрунтованого впливу осіб, які доглядають за людьми похилого віку, а також наглядового персоналу чи вищих керівників, зокрема шляхом забезпечення таємниці голосування.

11. У зв'язку з цим Асамблея пропонує:

відповідним державам-членам і спостерігачам Ради Європи:

- *a. знизити мінімальні вікові вимоги для здійснення активного та пасивного виборчих прав до 18 років для права голосу і до 25 років для права бути кандидатом на виборах;*
- *b. надати виборчі права всім своїм громадянам, не встановлюючи вимог щодо місця проживання;*
- *c. полегшити здійснення права голосу громадянам, які проживають за межами країни, передбачивши можливість дистанційного голосування (поштою та/або в консульських установах) та розглянувши можливість запровадження е-голосування відповідно до Рекомендації Rec(2004)11 Комітету Міністрів, а також співпрацювати між собою з цією метою;*
- *d. підписати та ратифікувати Конвенцію Ради Європи 1992 року про участь іноземців у суспільному житті на місцевому рівні та надати активне й пасивне виборчі права на місцевих виборах усім легальним резидентам;*
- *e. переглянути існуючі обмеження виборчих прав ув'язнених чи військовослужбовців із метою скасувати ті обмеження, які більше не є необхідними та пропорційними для досягнення законної мети;*
- *f. вжити відповідних заходів щодо захисту виборчих прав вразливих груп виборців (зокрема осіб, які проживають у будинках для людей похилого віку, ув'язнених, військовослужбовців, кочових груп) у відповідності до Кодексу належної практики у виборчих справах, прийнятого в липні 2003 року Венеційською комісією;*

Раді Європи та, зокрема, Венеційській комісії – надалі активізувати свою діяльність, спрямовану на поліпшення умов для ефективного здійснення виборчих прав, звертаючи особливу увагу на співпрацю з метою полегшення реалізації виборчих прав для тих громадян, які проживають за межами своєї країни.

Резолюція 1970 (2014)[1]
Парламентської Асамблеї Ради Європи

Інтернет та політика: вплив нових інформаційно-комунікаційних технологій на демократію

1. Парламентська Асамблея зазначає, що поширення Інтернету спричинило значні наслідки у контексті здійснення основоположних прав, які відіграють центральну роль у побудові нашого демократичного суспільства, зокрема права на свободу інформації, вираження поглядів, думки, зібрань та об'єднань, а також права на захист приватності індивіда.

2. Таке поширення та експоненціальне прискорення пропускної здатності Мережі поклали край концентрації інформаційної влади та змінили парадигму комунікації. Публічний простір розширився, а Мережа стала величезним необмеженим полем, справжнім глобальним форумом, де всі індивіди можуть шукати інформацію, ділитися знаннями, висловлювати думки на будь-яку тему та присвячувати себе ідеї чи справі.

3. Потрясіння, спричинені Інтернетом, змінили відносини між політичним світом та громадянами, а також порушили рівновагу між представницькою та прямою демократією. Вони зобов'язують нас обговорювати як нові перспективи, які відкриваються для більш сильної та динамічної форми демократії, так і нові небезпеки, що можуть підірвати її, а також роль, яку в цьому процесі мають відігравати законодавці.

4. Інтернет допомагає громадянам гуртуватися і забезпечує більшу видимість їхніх дій. Він також радикально змінює інституційне спілкування та структуру взаємовідносин між виборцями та політичними партіями, а також між громадянами, обраними представниками та урядовими департаментами. Більш загально, він розширив можливості участі в політичному житті. Отже, Інтернет є істотною складовою сучасної демократії, і політичні інститути повинні враховувати безліч ініціатив щодо участі громадян, які формуються в мережі.

1. Обговорення Асамблеї 29 січня 2014 року (5-е засідання) (див. Док. 13386, Доповідь Комітету з питань культури, науки, освіти та медіа, доповідач: пані Енн Брассер; та Док. 13399, висновок Комітету з політичних питань та демократії, доповідач: пан Ганс Франкен). Текст ухвалено Асамблеєю 29 січня 2014 року (п'яте засідання). Див. також Рекомендацію 2033 (2014).
Оригінал тексту доступний на веб-сторінці за посиланням: www.assembly.coe.int.

5. Розвиток комунікаційних технологій у майбутньому дозволить використовувати електронне голосування для розширення традиційних механізмів демократії. Цей процес повинен бути поступовим.

6. Однак Асамблея не вважає, що в сучасному складному світі можна було б замінити засновану на загальному виборчому праві модель політичного представництва будь-якою іншою моделлю, що ґрунтується передусім на процесах прямої демократії за допомогою електронних каналів, навіть якщо й припустити, що кожна особа має доступ до процедури консультацій та голосує через Інтернет, а також що буде знайдено відповідні засоби для усунення всіх перешкод задля загального використання електронного голосування.

7. Для визначення та реалізації політики необхідна низка довготермінових рішень, що потребують складних переговорів та залучення конфліктуючих інтересів, які важко збалансувати; така складність недостатньо оцінена в контексті процесів прийняття рішень у Мережі, що неминуче має спростити зміст дискусій. Публічна політика також вимагає внутрішньої узгодженості та координації, для якої фрагментація процесу прийняття рішень у Мережі створює непереборні перешкоди.

8. Нарешті, у такій системі ті люди, які мають більше ресурсів і яких обов'язково значно менше, які ***de facto*** диктуватимуть остаточні рішення, ані не будуть відомими, ані не будуть мати обов'язку звітувати про свої рішення, а тому вони матимуть такий тип влади, який буде і нелегітимним, і непідзвітним. У такому разі ми вже не можемо говорити про демократію.

9. Участь та представництво є нероздільними; це вимагає, щоб представницька демократія була дійсно учасницькою. Уже протягом декількох років Асамблея регулярно спостерігає поступову ерозію суспільної довіри до політичних інститутів. Щоб зупинити цю тенденцію, політики повинні більше слухати, розвивати участь громадян та сприяти активній громадянській позиції.

10. У зв'язку з цим Асамблея зазначає, що Інтернет та соціальні медіа відкривають нові двері для розширеного діалогу між громадянами і виборними представниками та стимулюють більш динамічну участь у демократичному житті. Ми повинні скористатися цією можливістю для возз'єднання демократичних інституцій із громадянами, які віддалилися від них, за допомогою Інтернету та розвивати, зокрема в наших парламентах, спроможності й компетенції, необхідні для використання того позитивного потенціалу, який наданий Інтернетом.

11. Поряд із виборними представниками політичні партії повинні відігравати надзвичайно важливу роль; Асамблея заохочує їх замислитися над їхніми взаєминами із електоральними базами та над використанням нових інформаційно-комунікаційних технологій із метою розвитку постійного діалогу з виборцями та залучення їх до розробки й подальшого впровадження своїх політичних програм.

12. Проте Асамблея усвідомлює, що Інтернет збільшує ризики зловживань та спотворень, здатних загрожувати правам людини, верховенству права й демократії: Мережа акумулює в собі прояви нетерпимості, ненависті та насильства щодо дітей і жінок; вона підживлює організовану злочинність, міжнародний тероризм і диктатури; Інтернет також посилює ризик упередженої інформації й маніпулювання поглядами та спрощує підступний моніторинг нашого приватного життя.

13. Контроль за правомірним використанням даних, які обробляються в Мережі, є складним: національне законодавство про захист даних у різних країнах неоднакове, а політика захисту приватності, що прийнята транснаціональними корпораціями Інтернету, які є найбільшими світовими операторами персональних даних, підпорядкована законодавству тих держав, у яких такі корпорації зареєстровано. Особливо турбує те, що персональні дані стають товарами, які стають предметом торгівлі, і їх неналежно використовують у комерційних чи політичних цілях, що становить серйозну загрозу захисту приватного життя. Крім того, посилене використання нових семантичних методів опитування може призвести до маніпулювання громадською думкою та спотворення політичних процесів.

14. Інтернет належить кожному; отже, він не належить нікому та не має меж. Ми повинні зберегти його відкритість та нейтральність. Однак не можна дозволити Інтернету стати гігантським механізмом добування приватної інформації, що діє поза будь-яким демократичним контролем. Ми повинні не допустити, аби мережа стала ***de facto*** «гетто», сферою, де панують приховані сили, відповідальність за володіння якими чітко покласти на когось буде неможливо.

15. Тому підзвітність операторів Інтернету є ключовим питанням, яким Асамблея на цей час займається, працюючи над двома доповідями – про право доступу до Інтернету та про узгоджені стратегії ефективного управління Інтернетом. На рівні Європейського Союзу цієї проблеми також стосуються «Кодекс ЄС щодо прав онлайн» та «Цифрового порядку денного для Європи».

16. Веб-користувачі можуть допомогти зробити Інтернет більш безпечним середовищем, у якому поважають права людини, а оператори повинні брати на себе відповідальність у боротьбі зі зловживаннями та спотвореннями. У цьому контексті життєво важливим є саморегулювання, щоб гарантувати нейтральність Інтернету, і його варто заохочувати; проте, як виявляється, цього недостатньо.

17. Держави повинні вживати узгоджених дій та приймати спільні норми, гарантуючи, що механізми нагляду самі собою не загрожуватимуть основоположним свободам, щоб захищати Інтернет як сферу свободи. Одкровення про діяльність оперативно-розшукових органів, які виходять за межі будь-яких правових рамок, шляхом систематичного вторгнення в приватне життя, є неприйнятним; це повинно змусити нас серйозно замислитися над ціною, яку ми платимо за нашу безпеку, і поміркувати про запобіжні

заходи, які ми повинні вжити, щоб уникнути знищення простору свободи в Інтернеті.

18. Національні парламенти є ключовими форумами для обговорення демократії та можливого оновлення демократичної системи в епоху Інтернету; проте вони повинні відкривати та активно залучати всіх зацікавлених суб'єктів, таких як державні інституції, приватні суб'єкти та підприємницькі компанії, а також мобілізувати все громадянське суспільство для дискусій про демократію, політику та Інтернет.

19. Відповідно, Асамблея рекомендує державам-членам, зокрема їх національним парламентам:

    - 19.1. збільшити спроможність політичних (і, зокрема, парламентських) інституцій використовувати нові інформаційно-комунікаційні технології для підвищення прозорості процесу прийняття рішень та діалогу з громадянами, зокрема через соціальні мережі, парламентські канали в Інтернеті та інші платформи, що дозволяють громадянам надавати зворотний зв'язок;

    - 19.2. продовжувати розробляти в цьому контексті цільові програми інтернет-навчання для виборних представників, модернізувати сайти парламентів та урядів і вдосконалювати використання засобів онлайн-консультацій та участі;

    - 19.3. не просто відтворювати традиційні інструменти онлайн, а досягти уваги громадян у межах створених віртуальних просторів та творчо обдумувати потенціал Інтернету як платформи для залучення й поширення знань;

    - 19.4. більш ефективно використовувати Інтернет як джерело сукупних даних, які можна застосувати для визначення преференцій та потреб громадян так, щоб політичний порядок денний на всіх рівнях влади краще відображав проблеми, що хвилюють суспільство, з огляду на довготермінові наслідки в контексті загального інтересу;

    - 19.5. скористатися функціями Інтернету для активізації співробітництва між органами влади, громадянським суспільством та університетами з метою розробки й реалізації ініціатив щодо поширення політичного та демократичного залучення серед громадян;

    - 19.6. боротися із соціально-культурними нерівностями, які закріплюють цифровий поділ суспільства, зокрема й шляхом запровадження освітніх програм, орієнтованих на підлітків та молодих студентів, щоб вони отримали необхідні компетенції для використання Інтернету та були добре інформованими вебкористувачами;

    - 19.7. просувати конвергенцію освіти в нових медіа й освіти для демократичної громадянської свідомості та прав людини, яка повинна належним чином враховувати переваги й проблеми Інтернету, а також розробляти програми, здатні охопити різні вікові межі та соціальні

групи; ці програми мають мобілізувати шкільні й університетські кола, соціальних партнерів та медіа;

- 19.8. закликати університети розробляти академічні курси у галузі науки про обробку даних, зокрема й щодо етичних, технічних, юридичних, економічних та суспільних аспектів;

- 19.9. ініціювати як на національному рівні, так і в рамках Ради Європи, обговорення норм та механізмів, які б відповідали розвитку технологій, потрібних для:

    - 19.9.1. створення безпечного простору в Мережі, із гарантіями також свободи вираження поглядів, передбаченої статтею 10 Європейської конвенції з прав людини (ETS № 5), та захисту приватного життя, передбаченого статтею 8;

    - 19.9.2. запобігання ризику спотворення інформації та маніпулювання громадською думкою, для чого необхідно розглянути:

    - 19.9.2.1. розробку узгоджених норм та/або стимулів для саморегулювання щодо підзвітності основних інтернет-операторів;

    - 19.9.2.2. створення незалежної інституції з достатніми повноваженнями, технічними компетенціями та ресурсами для надання експертних висновків щодо алгоритмів пошукових систем, які фільтрують і регулюють доступ до інформації та знань у Мережі з уникненням водночас ризику, що така установа може підривати саму природу свободи вираження поглядів;

    - 19.9.2.3. розробку принципів та загальних стандартів регулювання нових семантичних практик опитування громадської думки;

    - 19.9.2.4. розробку регулювання, що має застосовуватися компаніями, які пропонують системи інтернет-зв'язку з метою запобігання негативному впливу на особисте або сімейне життя індивідів внаслідок тролінгу, зберігаючи в той же час баланс із свободою вираження поглядів;

- 19.10. забезпечення, з одного боку, поваги до прав людини у Мережі та, з другого – свободи Інтернету, і вжиття заходів в рамках міжнародних органів, відповідальних за управління Інтернетом, щоб захистити ці права та цю свободу в усьому світі, особливо там, де демократія є ослабленою, загрожена або повалена;

- 19.11. безумовної підтримки пропозиції розпочати підготовку Білої книги Ради Європи про демократію, політику та Інтернет, яку було викладено Асамблеєю в Рекомендації 2033(2014) «Інтернет та політика: вплив нових інформаційно-комунікаційних технологій на демократію».

- 19.12. продовження дискусій у тісній співпраці з Європейською комісією за демократію через право (Венеційська комісія) з метою розробки протоколу до Європейської конвенції з прав людини щодо права людини на участь в управлінні публічними справами, як це було наголошено в Резолюції 1746(2010) та Рекомендації 1928(2010) «Демократія в Європі: криза та перспективи», і звернути особливу увагу на роль Інтернету та інших цифрових інструментів участі, таких як соціальні мережі, онлайнові дискусійні платформи, електронне голосування та відкриті урядові ініціативи.

Рекомендація CM/Rec(2017)5[1]

Комітету Міністрів Ради Європи державам-членам щодо стандартів е-голосування

Ухвалена Комітетом Міністрів Ради Європи 14 квітня 2017 року на 1289-му засіданні заступників міністрів

ПРЕАМБУЛА

Комітет Міністрів, відповідно до положень статті 15.b Статуту Ради Європи,

Зважаючи на те, що метою Ради Європи є досягнення більшого єднання між її членами для збереження та втілення в життя ідеалів і принципів, які є їхнім спільним доробком;

Підтверджуючи свою впевненість у тому, що представницька і пряма демократія є частиною цього спільного доробку та основою для участі громадян в політичному житті на рівні Європейського Союзу, а також на загальнонаціональному, регіональному і місцевому рівнях;

З огляду на зобов'язання, узяті в рамках наявних правових актів і документів, серед яких:

- Загальна декларація прав людини;
- Міжнародний пакт про громадянські та політичні права;
- Конвенція ООН про ліквідацію всіх форм расової дискримінації;
- Конвенція ООН про ліквідацію всіх форм дискримінації щодо жінок;
- Конвенція ООН про права осіб з інвалідністю;

1. Під час ухвалення цієї рекомендації Постійний представник Російської Федерації зазначив, що, згідно з підпунктом 2(c) статті 10 Регламенту засідань заступників міністрів, за його урядом залишається право дотримуватися чи не дотримуватися рекомендації.
Оригінал тексту доступний на веб-сторінці за посиланням: www.coe.int/cm.

- Конвенція ООН проти корупції;
- Конвенція про захист прав людини та основоположних свобод (ETS № 5), зокрема, Протокол до неї (ETS № 9);
- Європейська хартія місцевого самоврядування (ETS № 122);
- Конвенція про кіберзлочинність (ETS № 185);
- Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS № 108);
- Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних (ETS № 181);
- Конвенція про стандарти демократичних виборів, виборчих прав і свобод у державах-учасницях Співдружності Незалежних Держав (CDL-EL(2006) 031rev);
- Рекомендація Rec(99)5 Комітету Міністрів Ради Європи державам-членам щодо захисту недоторканності приватного життя в Інтернеті;
- Рекомендація Rec(2004)15 Комітету Міністрів Ради Європи державам-членам щодо електронного врядування (е-врядування);
- Рекомендація CM/Rec(2009)1 Комітету Міністрів Ради Європи державам-членам щодо електронної демократії (е-демократії);
- Документ Копенгагенської наради Конференції ОБСЄ щодо людського виміру;
- Хартія основних прав Європейського Союзу;
- Кодекс належної практики у виборчих справах, ухвалений Радою з демократичних виборів Ради Європи та Європейською комісією за демократію через право (Венеційською комісією) і підтриманий Комітетом Міністрів, Парламентською Асамблеєю та Конгресом місцевих і регіональних влад Ради Європи;

Беручи до уваги, що право голосу належить до підвалин демократії, і що, як наслідок, усі механізми голосування, зокрема е-голосування, повинні відповідати принципам демократичних виборів і референдумів;

Визнаючи, що використання державами-членами інформаційно-комунікаційних технологій під час виборів значно зросло останніми роками;

Зазначаючи, що деякі держави-члени вже використовують або розглядають можливість використання е-голосування з різними цілями, зокрема:

- надання виборцям можливості подавати свій голос з іншого місця, аніж приміщення для голосування на їх виборчих дільницях;
- сприяння поданню голосу виборцями;

- сприяння участі у виборах та референдумах громадян, що мають право голосу і проживають чи перебувають за кордоном;
- розширення доступу до процесу голосування виборцям з інвалідністю чи особам, які стикаються з іншими труднощами, пов'язаними з фізичною присутністю на виборчій дільниці та використання наявних на ній пристроїв;
- підвищення рівня участі виборців через надання додаткових механізмів голосування;
- узгодження голосування із нововведеннями у суспільстві та активніше використання нових технологій як засобу комунікації, та залучення громадськості у реалізації демократії;
- поступове скорочення загальних витрат органів адміністрування виборів на проведення виборів чи референдумів;
- забезпечення надійнішого та швидшого отримання результатів голосування;
- забезпечення кращого обслуговування електорату через надання різноманітних механізмів голосування;

Високо оцінюючи досвід, накопичений державами-членами, що останніми роками використовували е-голосування, та уроки, здобуті з цього досвіду;

Усвідомлюючи також досвід, отриманий внаслідок застосування Рекомендації Rec(2004)11 Комітету Міністрів Ради Європи державам-членам щодо правових, операційних і технічних стандартів е-голосування, Керівних принципів розроблення процесів, що засвідчують відповідність встановленим вимогам і стандартам (Сертифікація систем е-голосування), і Керівних принципів забезпечення прозорості виборів із застосуванням електронних технологій;

Знову підтверджуючи свою переконаність у тому, що суспільна довіра до органів, відповідальних за організацію виборів, є передумовою для запровадження е-голосування;

Розуміючи стурбованість щодо потенційних проблем із захистом, надійністю та прозорістю систем е-голосування;

Усвідомлюючи, відповідно, що лише захищені, надійні, ефективні, технічно стійкі, відкриті для незалежної перевірки та легкодоступні для виборців системи е-голосування здатні сформувати суспільну довіру, що є передумовою для проведення е-голосування;

Розуміючи потребу для держав-членів зважати на середовище, в якому запроваджується е-голосування;

Усвідомлюючи, що, з огляду на останні технічні та правові нововведення, пов'язані з проведенням у державах-членах Ради Європи виборів із застосуванням електронних технологій, положення Рекомендації Rec(2004)11 потребують ретельного перегляду та оновлення;

З огляду на роботу Спеціального комітету експертів з питань правових, операційних і технічних стандартів е-голосування (CAHVE), створеного Комітетом Міністрів із завданням оновлення Рекомендації Rec(2004)11,

1. Рекомендує, щоб уряди держав-членів, залежно від обставин, у разі запровадження, перегляду або оновлення національного законодавства та практики у сфері е-голосування:

   i. дотримувалися всіх принципів демократичних виборів і референдумів;

   ii. оцінювали ризики та протидіяли їм відповідними заходами, особливо тим ризикам, що характерні лише для механізму е-голосування;

   iii. керувалися у своєму законодавстві, політиці та практиці стандартами, наведеними в Додатку I до цієї рекомендації. Водночас варто враховувати взаємозв'язок між зазначеними вище стандартами й тими, що містяться в Керівних принципах виконання цієї рекомендації;

   iv. постійно здійснювали аналіз та перегляд своєї політики та досвіду е-голосування, зокрема того, як і наскільки реалізуються положення цієї рекомендації, щоб надавати Раді Європи підстави для проведення засідань з огляду стану виконання цієї рекомендації принаймні кожні два роки після її прийняття;

   v. обмінювалися досвідом у цій сфері;

   vi. забезпечили переклад і якомога ширше розповсюдження цієї рекомендації, Пояснювальної записки до неї та Керівних принципів, особливо серед виборчих органів, їх посадових осіб, громадян, політичних партій, національних та міжнародних спостерігачів, НУО, ЗМІ, науковців, постачальників рішень у сфері е-голосування та спеціальних органів, що здійснюють контроль у сфері е-голосування;

2. Погоджується регулярно оновлювати положення Керівних принципів, що супроводжують цю рекомендацію;

3. Скасовує Рекомендацію Rec(2004)11 щодо правових, експлуатаційних і технічних стандартів е-голосування та Керівні принципи до неї.

ДОДАТОК I. СТАНДАРТИ Е-ГОЛОСУВАННЯ

I. Загальне право голосу

1. Інтерфейс виборця в системі е-голосування є простим для розуміння та використання для усіх виборців.

2. Система е-голосування повинна бути розроблена в такий спосіб, щоб, наскільки це практично може бути реалізовано, забезпечувати особам з інвалідністю та з особливими потребами можливість голосувати самостійно.

3. Якщо механізми дистанційного е-голосування не є загальнодоступними, вони становлять лише додатковий і необов'язковий засіб голосування.

4. Перед поданням голосу через систему дистанційного е-голосування увага виборця повинна бути прямо звернута на те, що е-вибори, у яких вони

подають своє рішення з використанням електронних засобів, є реальними виборами або референдумом.

II. Рівне виборче право

5. Вся офіційна інформація про голосування має надаватися однаково в рамках і через усі механізми голосування.

6. У разі використання як електронних, так і неелектронних механізмів голосування під час тих же виборів або референдуму повинен існувати захищений і надійний спосіб зібрати разом усі голоси і підрахувати результати.

7. Повинна бути забезпечена однозначна ідентифікація виборців у такий спосіб, що їх можна безпомилково відрізнити від інших осіб.

8. Система е-голосування повинна надавати користувачеві доступ лише після автентифікації її/його як особи з правом голосу.

9. Система е-голосування повинна забезпечувати, щоб кожен виборець міг подати лише належну кількість голосів, і щоб лише така кількість голосів кожного виборця зберігалася в електронній виборчій скриньці та була врахована у результатах виборів.

III. Вільні вибори

10. Намір виборця проголосувати не повинен зазнавати впливу ані системи голосування, ані будь-якого суб'єкта неналежним чином.

11. Повинно бути забезпечене надання виборцю системою е-голосування автентичного виборчого бюлетеня та автентичної інформації.

12. Спосіб, яким виборці повинні проходити через процес е-голосування, не може призводити до голосування ними раптово чи без отримання підтвердження.

13. Система е-голосування повинна надавати виборцю засоби участі у виборах або референдумі без створення умов, щоб виборець віддавав перевагу будь-якій з опцій г олосування.

14. Система е-голосування повинна повідомляти виборця про те, що він чи вона подає недійсний е-голос.

15. Виборець повинен мати можливість пересвідчитися в тому, що його чи її наміри точно відображені у змісті поданого голосу та що запечатаний голос без змін надійшов до електронної виборчої скриньки. Будь-який протиправний вплив, який би модифікував зміст голосу, повинен піддаватися виявленню.

16. Виборець має отримати від системи підтвердження того, що голос був успішно поданий і що вся процедура голосування завершена.

17. Система е-голосування повинна надавати надійні докази того, що кожен автентичний голос точно включений до результатів відповідних виборів.

Повинні існувати незалежні від системи е-голосування способи перевірки цих доказів.

18. Система повинна надавати надійні докази того, що лише голоси, подані повноважними виборцями, включено до відповідних остаточних результатів. Повинні існувати незалежні від системи е-голосування способи перевірки цих доказів.

IV. Таємне голосування

19. Е-голосування повинно бути організованим у такий спосіб, щоб забезпечувати дотримання таємності голосування на всіх етапах процедури голосування.

20. Система е-голосування повинна обробляти і зберігати протягом потрібного часу лише ті персональні дані, які необхідні для проведення е-виборів.

21. Система е-голосування та будь-який уповноважений суб'єкт повинні захищати дані автентифікації так, щоб неуповноважені суб'єкти не мали можливості зловживати використанням, перехоплювати, змінювати чи іншим способом отримувати відомості про ці дані.

22. Доступ до реєстрів виборців, що зберігаються або передаються системою е-голосування, має надаватися лише уповноваженим суб'єктам.

23. Система е-голосування не повинна надавати виборцю підтвердження змісту поданого голосу для використання третіми особами.

24. До моменту закриття електронної виборчої скриньки система е-голосування не повинна дозволяти розкриття будь-кому кількості голосів, поданих за будь-яку опцію голосування. До завершення часу голосування ці відомості не підлягають оприлюдненню.

25. Е-голосування повинно забезпечувати дотримання таємності попередніх варіантів, записаних і видалених виборцем до подання ним чи нею свого остаточного голосу.

26. Процес е-голосування, особливо етап підрахунку голосів, повинен бути організованим у такий спосіб, щоб унеможливити відстеження зв'язку між розпечатаним голосом та виборцем. Подані голоси є та залишаються анонімними.

V. Нормативні та організаційні вимоги

27. Держави-члени, які запроваджують е-голосування, повинні здійснювати це поетапно та поступово.

28. Перш ніж запроваджувати е-голосування, держави-члени повинні внести необхідні зміни до відповідного законодавства.

29. Відповідне законодавство повинно регулювати відповідальність за функціонування систем е-голосування і забезпечувати контроль за ними з боку органу адміністрування виборів.

30. Кожен спостерігач повинен мати можливість спостерігати за підрахунком голосів. Відповідальність за процес підрахунку голосів покладається на орган адміністрування виборів.

VI. Прозорість і спостереження

31. Держави-члени зобов'язані забезпечувати прозорість усіх аспектів е-голосування.

32. Задовго до початку голосування громадськість, зокрема, виборці повинні бути поінформовані чіткою і простою мовою про:

    - будь-які дії, які мав би вчинити виборець, щоб узяти участь у виборах і проголосувати;
    - належне використання і функціонування системи е-голосування;
    - часовий графік е-голосування включно з усіма його етапами.

33. Складові системи е-голосування повинні бути відкритими для цілей верифікації та сертифікації.

34. Кожен спостерігач у межах, встановлених законом, повинен мати можливість спостерігати за е-виборами та коментувати їх, зокрема й встановлення результатів.

35. Для забезпечення взаємодії між різними технічними складовими чи послугами, можливо, отриманими з різних джерел, повинні використовуватися відкриті стандарти.

VII. Підконтрольність

36. Держави-члени повинні розробити технічні, оцінювальні та сертифікаційні вимоги й бути переконаними в тому, що вони повністю відображають відповідні правові та демократичні принципи. Держави-члени повинні підтримувати ці вимоги в актуальному стані.

37. Перед запровадженням системи е-голосування та з належною періодичністю після її запровадження, зокрема, після внесення до системи будь-яких істотних змін, повинна бути здійснена оцінка незалежним і компетентним органом щодо відповідності технічним вимогам системи е-голосування і будь-яких її компонентів, що використовують інформаційно-комунікаційні технології (ІКТ). Це може набувати форми офіційної серти-фікації або іншого належного контролю.

38. Сертифікат чи будь-який інший відповідний виданий документ повинні містити чітке зазначення об'єкта оцінювання та заходи із запобігання таємним чи ненавмисним змінам до нього.

39. Система е-голосування повинна забезпечувати можливість свого аудиту. Система аудиту має бути відкритою і всеосяжною та оперативно сповіщати про можливі проблеми й загрози.

VIII. Надійність і захищеність системи

40. Орган адміністрування виборів повинен бути відповідальним за дотримання всіх вимог і відповідність цим вимогам навіть у разі відмов і атак. Орган адміністрування виборів повинен бути відповідальним за доступність, надійність, придатність до використання і безпеку системи е-голосування.

41. Тільки особам, уповноваженим органом адміністрування виборів, повинен надаватися доступ до центральної інфраструктури, серверів і даних про вибори. Призначення на посаду осіб, уповноважених працювати у сфері забезпечення е-голосування, повинно бути чітко регламентованим.

42. Перед будь-якими е-виборами орган адміністрування виборів повинен пересвідчитися, що система е-голосування справжня і функціонує належно.

43. Повинен бути визначений порядок періодичного встановлення оновлених версій і виправлень усього відповідного програмного забезпечення.

44. У разі зберігання чи передання поза межі контрольованого середовища голоси повинні бути зашифровані.

45. До початку процесу підрахунку голоси виборців та відомості про них повинні зберігатися в запечатаному вигляді.

46. Орган адміністрування виборів повинен забезпечити захист при роботі з усіма криптографічними матеріалами.

47. У разі виникнення інцидентів, що можуть загрожувати цілісності системи, відповідальні за експлуатацію обладнання особи повинні негайно сповістити про це орган адміністрування виборів.

48. Автентичність, доступність і цілісність реєстрів виборців і списків кандидатів повинна бути забезпечена. Автентичність джерел даних має підтверджуватися. Положення про захист даних повинні бути дотримані.

49. Система е-голосування повинна ідентифікувати голоси, що зазнали впливу порушень.

ДОДАТОК II. ГЛОСАРІЙ ТЕРМІНІВ

Наведені в цій рекомендації та Пояснювальній записці терміни використовуються у таких значеннях:

- контроль доступу – запобігання несанкціонованому використанню ресурсу;
- оцінювання – здійснення оцінки осіб, апаратного забезпечення, програмного забезпечення та процедур з метою перевірити їхню придатність до виконання певних завдань;

- аудит – незалежне передвиборче чи післявиборче оцінювання особи, організації, системи, процесу, суб'єкта, проєкту чи продукту, яке включає кількісний та якісний аналіз;
- автентифікація – забезпечення достовірності заявленої ідентичності особи чи даних;
- доступність – стан, що дозволяє доступ і використання на вимогу;
- бюлетень – юридично визнаний засіб, яким виборець може виразити свій голос;
- кандидат – опція голосування, що складається з однієї особи, групи осіб та/або політичної партії;
- подання голосу – внесення голосу до виборчої скриньки;
- сертифікат – документ, що є результатом офіційної сертифікації, яким засвідчується чи підтверджується певний факт;
- сертифікація – процес підтвердження того, що система е-голосування відповідає встановленим вимогам і стандартам і що вона містить, щонайменше, засоби, які дозволяють пересвідчитися в належному функціонуванні системи. Це може здійснюватися різними заходами, від тестування та аудиту і до офіційної сертифікації. Кінцевим результатом є звіт та/або сертифікат;
- орган сертифікації (або сертифікатор) – організація, уповноважена здійснювати процес сертифікації та видавати сертифікат після завершення процесу;
- звіт про сертифікацію – документ, який роз'яснює, що саме засвідчує сертифікат і як саме здійснена сертифікація;
- ланцюжок довіри – процес у комп'ютерній безпеці, що здійснюється шляхом валідації кожного компонента апаратного та програмного забезпечення знизу вгору. Він покликаний забезпечити використання лише надійного програмного та апаратного забезпечення, водночас зберігаючи гнучкість;
- покомпонентне тестування – метод тестування окремих блоків коду системи для визначення їх придатності до використання;
- конфіденційність – стан, що характеризує інформацію, до якої не повинен надаватися доступ або яка не може бути розголошена неуповноваженим особам, суб'єктам чи процесам;
- контрольоване середовище – приміщення, що перебувають під наглядом посадових осіб органів адміністрування виборів, наприклад, приміщення для голосування, посольства чи консульства;
- е-вибори – політичні вибори чи референдум, на яких використовується е-голосування;

- орган адміністрування виборів – інституція, уповноважена на організацію підготовки і проведення виборів у конкретній країні на загальнонаціональному чи нижчому рівні;
- електронна виборча скринька – електронні засоби, за допомогою яких зберігаються голоси в очікуванні їх підрахунку;
- е-голос – голос, поданий в електронному вигляді;
- е-голосування – використання електронних засобів для подання та/або підрахунку голосів;
- система е-голосування – апаратне, програмне забезпечення та процеси, що надають можливість виборцям голосувати за допомогою електронних засобів на виборах чи референдумі;
- офіційна сертифікація – сертифікація, що здійснюються офіційними органами тільки до дня виборів і результатом якої є видача сертифіката;
- керівні принципи – будь-який документ, покликаний скерувати певні процеси згідно зі встановленою методикою. За визначенням, керівні принципи не є юридично зобов'язальними;
- угода про нерозголошення (УПН) – юридична угода між двома чи більше сторонами, що окреслює конфіденційні матеріали, знання чи інформацію, якими сторони бажають обмінюватися з певними цілями, але прагнуть обмежити до них доступ для третіх сторін;
- відкритий доступ – онлайновий доступ до матеріалів, читання яких вільне для всіх та які можуть вільно використовуватися (чи повторного використовуватися) всіма у певних межах;
- профіль захисту – незалежний від реалізації набір вимог до захищеності певної категорії продуктів, який відповідає конкретним безпековим потребам споживачів;
- вимога – окрема документально оформлена потреба щодо того, якими повинні бути конкретний продукт чи сервіс або як вони повинні функціонувати;
- дистанційне е-голосування – використання електронних засобів для подання голосу поза межами приміщення, в якому в загальному випадку відбувається голосування;
- запечатування – захист інформації у такий спосіб, що вона не може бути використана або інтерпретована без допомоги іншої інформації чи засобів, доступних лише певним особам чи органам, зокрема й за допомогою шифрування;
- зацікавлений суб'єкт – особа, група осіб, організація чи система, які чинять вплив на дії уряду чи організації або можуть зазнавати впливу від таких дій. Це поняття охоплює громадян, посадових осіб органів адміністрування виборів, політичні партії, уряди, національних і міжнародних

спостерігачів, ЗМІ, науковців, міжнародні та внутрішні НУО, організації-опоненти е-голосування та спеціальні органи сертифікації е-голосування;

- стандарт (правовий) – стосується положень, що містяться в Додатку I до Рекомендації CM/Rec(2017)5;
- стандарт (технічний) – встановлена норма, зазвичай, у формі офіційного документа, що встановлює єдині інженерні чи технічні критерії, методи, процеси та практику;
- тестування – процес перевірки того, що система працює так, як очікувалося;
- голос – вираження вибору опції голосування;
- виборець – особа, що має право голосу на певних виборах чи референдумі;
- механізм голосування – спосіб, яким виборець може подати свій голос;
- опції голосування – перелік варіантів, з-поміж яких можна здійснити вибір шляхом подання голосу на виборах чи референдумі;
- реєстр виборців – список осіб, що мають право голосу (виборців).

Пояснювальна записка[1]
до Рекомендації CM/Rec(2017)5 Комітету Міністрів державам-членам щодо стандартів е-голосування

(Схвалено Комітетом Міністрів Ради Європи 14 червня 2017 року на 1289-му засіданні заступників міністрів)

Спеціальний комітет експертів з питань правових, операційних і технічних стандартів е-голосування (CAHVE)

(Питання розглянуто Групою доповідачів з питань демократії (GR-DEM) на її засіданнях, що відбулися 20 квітня та 1 червня 2017 року)

ЗАСАДИ

1. Ця Рекомендація щодо стандартів е-голосування та Пояснювальна записка є оновленою редакцією «Рекомендації Rec(2004)11 Комітету Міністрів Ради Європи державам-членам щодо правових, операційних і технічних стандартів е-голосування» та Пояснювальної записки до неї, затверджених 30 вересня 2004 року. 2010 року були прийняті два додаткові документи: «Керівні принципи розробки процесів, що засвідчують відповідність встановленим вимогам і стандартам (Сертифікація систем е-голосування)» і «Керівні принципи щодо прозорості виборів із застосуванням електронних технологій».

2. Рекомендація Rec(2004)11 та супровідні Керівні принципи слугували правовими орієнтирами для країн та інституцій регіону під час запровадження, експлуатації та оцінювання систем е-голосування. Відповідно до висновків 2012 і 2014 року щодворічних засідань щодо Рекомендації Rec(2004)11, а також засідання експертів, проведеного у Відні в грудні 2013 року, Комітет Міністрів 1 квітня 2015 року вирішив, відповідно до Статті 17 Статуту Ради Європи та згідно з Резолюцією CM/Res(2011)24 щодо міжурядових комітетів і підпорядкованих органів, створити «Спеціальний комітет експертів з питань правових, операційних і технічних стандартів е-голосування» (CAHVE).

3. CAHVE було доручено підготувати нову Рекомендацію, яка б оновлювала Rec(2004)11 і пояснювальний меморандум до неї у світлі останніх технічних і правових новел, пов'язаних із проведенням у державах-членах Ради

1. Оригінал тексту доступний на веб-сторінці за посиланням: www.coe.int/cm.

Європи виборів із застосуванням електронних технологій. Оновлення мало полягати у вдосконаленні та подальшому розвитку чинної Рекомендації Rec(2004)11. Робота мала бути спрямована на усунення виявлених у Рекомендації недоліків, спираючись на останній досвід проведення е-голосування в регіоні та беручи до уваги наслідки від використання новітніх технічних концепцій і рішень. Процес оновлення мав ґрунтуватися на оцінюванні потреб, особливу увагу приділяючи думкам держав-членів і неурядових зацікавлених суб'єктів. І в межах своїх повноважень CAHVE підготував такі документи: Рекомендація Rec(2017)XX щодо стандартів е-голосування, яка викладає в новій редакції та замінює собою Рекомендацію Rec(2004)11 щодо правових, операційних і технічних стандартів е-голосування, та цей пояснювальний меморандум. На додаток до цих повноважень CAHVE підготувала «Керівні принципи імплементації положень Рекомендації Rec(2017)XX щодо стандартів е-голосування».

4. Ця Рекомендація містить стандарти е-голосування, що відображають і застосовують до е-голосування принципи демократичних виборів і референдумів. Стандарти спрямовані на те, щоб забезпечити дотримання цих принципів під час використання е-голосування, зміцнюючи у такий спосіб довіру до національних механізмів е-голосування та впевненість у них.

5. Принципи демократичних виборів і референдумів випливають з чинних документів Ради Європи та інших міжнародних документів у сфері виборів. Стандарти виражають цілі, яких має досягти е-голосування, щоби відповідати принципам демократичних виборів і референдумів. Стандарти є спільними для регіону Ради Європи.

6. Ця Рекомендація не впливає на повноваження держав-членів Ради Європи у виборчих справах і щодо референдумів. Рекомендація охоплює використання е-голосування на політичних виборах і референдумах. Політичні вибори та референдуми проводяться на різних рівнях. У деяких країнах референдуми не проводяться. Стандарти застосовуються однаково, незалежно від того, чи е-голосування використовується під час політичних виборів, чи політичних референдумів.

7. Причини запровадження або розгляду можливості запровадження е-голосування відрізняються для різних країн та залежать від конкретних внутрішніх умов. Стало очевидним, що система е-голосування може впроваджуватися лише тоді, коли у виборців наявна довіра і впевненість у свої виборчій системі та виборчій адміністрації. Ця Рекомендація не вимагає від держав-членів запровадження е-голосування. Вона зауважує, що останнім часом дедалі більше число країн певною мірою використовує е-голосування або планує робити це в найближчому майбутньому. Рекомендація запроваджує стандарти, спрямовані на узгоджену реалізацію принципів демократичних виборів і референдумів під час використання е-голосування в державах-членах.

8. У цій Рекомендації термін «е-голосування» означає використання електронних засобів для цілей голосування і підрахунку голосів у контрольованих і

неконтрольованих середовищах. Він охоплює машини для е-голосування у приміщеннях для голосування, використання оптичних сканерів для реєстрації та/або підрахунку паперових виборчих бюлетенів, а також дистанційне е-голосування. Якщо окремо не застережено, стандарти стосуються всіх форм е-голосування. Якщо стандарти стосуються лише однієї чи декількох форм, це зазначається окремо. Детальні положення щодо імплементації, в яких часто розглядається лише одна з форм е-голосування, містяться в «Керівних принципах імплементації положень Рекомендації CM/Rec(2017)5 щодо стандартів е-голосування».

9. Виборчі системи можуть включати в себе як недистанційні, так і дистанційні форми голосування. Дистанційне голосування може проводитися як у контрольованих (наприклад, голосування в посольствах чи консульствах, голосування у поштових відділеннях або муніципальних управліннях), так і неконтрольованих (тобто без нагляду з боку посадовців) середовищах (наприклад, голосування з дому поштою чи з персонального комп'ютера через інтернет). У кожній державі-члені склалася своя практика щодо видів механізмів голосування, доступних виборцям[2]. Для цілей цієї Рекомендації дистанційне е-голосування означає використання електронних засобів для подання голосу поза межами приміщення, де в загальному випадку відбувається голосування.

10. Рекомендація спрямована на відповідні аспекти е-голосування, пов'язані з різними етапами виборів і референдумів, а саме, етап перед голосуванням, подання голосів, етап після голосування, а також на роль та повноваження різних зацікавлених суб'єктів. Наведені тут стандарти можуть бути застосовані до використання е-голосування так, як визначено цією Рекомендацією. Додаткові системи, які стосуються е-голосування, але у технічному сенсі не є його частиною, як, наприклад, системи реєстрації виборців, потребують спеціального регулювання. Викладені стандарти е-голосування можуть дати поштовх до розробки такого регулювання. Держави-члени, які розглядають можливість запровадження е-голосу-вання, можуть також звернути увагу на посібник Ради Європи з е-голосування «Ключові етапи запровадження виборів із застосуванням електронних технологій» (2010 р.), який надає допомогу та слугує порадником з цього питання.

11. Докладні керівні принципи щодо реалізації цілей (наведених у стандартах) можна знайти у «Керівних принципах імплементації положень Рекомендації CM/Rec(2017)5 щодо стандартів е-голосування», доданих до цієї Рекомендації. Нові Керівні принципи містять оновлену редакцію положень цього рівня з попередньої Рекомендації Rec(2004)11 та пов'язаних із нею двох документів, а саме: «Керівних принципів розробки процесів, що

2. Європейська комісія за демократію через право (Венеційська комісія) видала Доповідь про сумісність дистанційного голосування та електронного голосування з вимогами документів Ради Європи (прийнята Венеційською комісією на 58-й пленарній сесії. Венеція, 12-13 березня 2004 р. Дослідження № 260, 2003 р., Страсбург, 18 березня 2004 р., CDL-AD (2004)012, оригінал французькою мовою). Венеційська комісія дійшла висновку, що дистанційне голосування сумісне зі стандартами Ради Європи за умови дотримання певних запобіжних заходів у процедурах голосування поштою чи електронного голосування.

засвідчують відповідність встановленим вимогам і стандартам (Сертифікація систем е-голосування)» і «Керівних принципів забезпечення прозорості виборів із застосуванням електронних технологій». Нові Керівні принципи замінюють собою ці два документи з керівними принципами.

12. Ця редакція Керівних принципів потребує доповнення через подальшу роботу, щоб стосуватися всіх форм і всіх аспектів е-голосування, охоплених Рекомендацією CM/Rec(2017)5 щодо стандартів е-голосування. Навіть більше, у зв'язку з постійним розвитком в правовій і технічній сферах положення Керівних принципів потрібно регулярно оновлювати, тоді як Рекомендація покликана забезпечувати стабільну основу. Оновлення Керівних принци-пів повинні розглядатися та затверджуватися державами-членами на засіданнях, що періодично проводяться з метою огляду стану виконання цієї Рекомендації.

РЕКОМЕНДАЦІЇ

13. Демократія немислима без виборів і референдумів, які проводяться відповідно до певних принципів, що надають їм демократичності. Ці принципи становлять окремий аспект «європейського конституційного доробку», також відомий як «європейський виборчий доробок». У 2002 році Європейська комісія за демократію через право (Венеційська комісія) прийняла Кодекс належної практики у виборчих справах[3], який хоча й не є зобов'язальним, однак становить еталонний документ Ради Європи в цій галузі, визначаючи «європейський виборчий доробок» через два аспекти: фундаментальні конституційні принципи виборчого права та деякі основні умови, необхідні для їх застосування. Кодекс визначає такі принципи: загальне, рівне, виборче право, вільні та прямі вибори, таємне голосування та періодичність виборів. Основні умови – це верховенство права, повага до основоположних прав, стабільність виборчого законодавства та дієві процедурні гарантії[4]. Усі механізми голосування, що використовуються під час виборів і референдумів, зокрема й е-голосування, мають бути розроблені та впроваджені з дотриманням цих принципів та умов.

---

3. Кодекс належної практики у виборчих справах (CDL-AD(2002)023rev), схвалений резолюцією 1320(2003) Парламентської Асамблеї та резолюцією 148 (2003) КМРВЄ, предмет Декларації Комітету Міністрів (114-та сесія, 13 травня 2004 р.).

4. – Пункт 7 Документа Копенгагенської наради Конференції ОБСЄ щодо людського виміру від 29 червня 1990 р. явно зазначає про загальне та рівне виборче право, вільні вибори при таємному голосуванні, а пункт 6 – про прямі вибори, хоча і з певними застереженнями;

– Стаття 25(b) Міжнародного пакту про громадянські та політичні права безпосередньо передбачає всі ці принципи, за винятком прямих виборів, хоча останній передбачається неявно (стаття 21 Загальної декларації прав людини);

– Стаття 3 Додаткового протоколу до Європейської конвенції про права людини прямо передбачає право на вільні вибори з розумною періодичністю шляхом таємного голосування; інші принципи також визнаються судовою практикою у сфері прав людини (загальність: рішення ЄСПЛ у справі «Матьє-Моен і Клерфей проти Бельгії» від 2 березня 1997 р., заява № 9267/81, Серія A, том 113, с. 23; рішення в справі «Гітонас та інші проти Греції» від 1 липня 1997 р., заяви №№ 18747/91, 19376/92, 19379/92, 28208/95 і 27755/95, Збірник судових рішень і постанов 1997-IV, с. 1233; рівність: зазначене вище рішення у справі «Матьє-Моен і Клерфей проти Бельгії», с. 23). Право на прямі вибори також в порядку презумпції визнається Страсбурзьким судом (§ 64 рішення ЄСПЛ у справі «Метьюз проти Сполученого Королівства» від 18 лютого 1999 р., заява № 24833/94, Збірник судових рішень і постанов 1999-I).

14. Відповідно до Кодексу належної практики у виборчих справах 2002 року зміст цих принципів і умов можна коротко викласти так:

   - ***Загальне виборче право:*** кожна людина має право голосу і право бути кандидатом на виборах за дотримання певних умов, таких як вік чи громадянство;
   - ***Рівне виборче право:*** кожен виборець має рівну кількість голосів, кожен голос має однакову вагу, має забезпечуватися рівність можливостей;
   - ***Вільні вибори:*** виборець має право формувати та виражати свою думку вільно, без жодного примусу чи протиправного впливу;
   - ***Таємне голосування:*** виборець має право проголосувати таємно як індивід, і держава зобов'язана захищати це право;
   - ***Прямі вибори:*** подані виборцями бюлетені безпосередньо визначають обраних особу чи осіб;
   - ***Періодичність виборів:*** вибори мають проводитися через регулярні проміжки часу;
   - ***Повага до основоположних прав:*** демократичні вибори вимагають поваги до прав людини, таких як свобода вираження поглядів, свобода пересування, свобода зібрань, свобода об'єднань;
   - ***Рівні регулювання та стабільність виборчого законодавства:*** норми виборчого права повинні бути закріплені принаймні на рівні закону; норми, що регламентують технічні питання та подробиці, можуть міститися в підзаконних актах виконавчої влади. Основні складові виборчого права не повинні переглядатися пізніше ніж за один рік до виборів, або ж повинні бути закріплені в конституції чи на рівні, вищому за звичайний закон;
   - ***Процедурні гарантії:*** включають, серед іншого, процедурні запобіжники, спрямовані на забезпечення організації виборів безстороннім органом, спостереження за виборами національними та міжнародними спостерігачами, наявності дієвої системи оскарження;
   - ***Виборча система:*** за умови дотримання зазначених вище принципів може бути обрана будь-яка виборча система.

15. Стандарти, наведені в Додатку I до цієї Рекомендації, ставлять цілі, яких має дотримуватися е-голосування, щоби відповідати принципам і вимогам «європейського виборчого доробку». Однак не всі зазначені вище принципи та умови потребують особливої уваги та встановлення окремих цілей для е-голосування. Це, наприклад, стосується «періодичного проведення виборів», яке не потребує особливої уваги під час розробки чи запровадження е-голосування, крім очевидної вимоги щодо готовності механізмів голосування, зокрема й е-голосування, до періодичного проведення виборів. Наведені в цій Рекомендації стандарти адресовані лише тим проблемам, які вважаються особливо актуальними для е-голосування.

Пункт I, рекомендації i–vi
Рекомендації i та ii. Дотримання принципів і протидія ризикам

16. Е-голосування, як і будь-який інший спосіб голосування, повинно дотримуватися принципів демократичних виборів і референдумів. Стрімкі зміни в базовій технології породжують виклики для такого дотримання, оскільки вони безперервно створюють нові можливості та загрози. Це вимагає відповідного менеджменту. Зрештою, важливо, щоб зазначені принципи не порушувалися через запровадження рішень на основі електронних технологій у процесах голосування та/або підрахунку голосів чи внаслідок їхньої еволюції.

17. Відповідно, системи е-голосування, повинні розроблятися та функціонувати у такий спосіб, щоб забезпечувати постійне дотримання цих принципів. Держави-члени повинні приділяти особливу увагу ризикам, притаманним обраному методу е-голосування. Специфічні для е-голосування ризики необхідно постійно контролювати, вживаючи в разі потреби належних контрзаходів. З огляду на стрімкі темпи змін у сфері нових технологій, державам-членам рекомендовано запровадити засади політики управління ризиками.

18. Можуть існувати винятки з принципів; на умови реалізації принципів можуть накладатися обмеження. До того ж у контексті е-голосування може бути необхідним більш строге застосування одного принципу і більш м'яке – другого. Такі рішення приймаються компетентним національним органом (парламентом, верховним судом, органом адміністрування виборів чи урядовим відомством) і залежать від конкретних умов країни. Важливо, щоб ці рішення приймалися відповідно до основних вимог, таких як, зокрема, прийняття компетентним органом, наявність законних підстав, відповідність загальним інтересам, дотримання пропорційності. Повинно забезпечуватися дотримання загальної мети демократичних виборів і референдумів.

19. Принципи демократичних виборів, на які посилається Рекомендація, – це принципи європейського виборчого доробку, включені до Кодексу належної практики у виборчих справах Венеційської комісії. Вони становлять мінімальні вимоги та застосовуються по всій території регіону. Окрема країна може запроваджувати додаткові принципи або встановлювати більш строге тлумачення наведених тут принципів. У цьому разі е-голосування має відповідати жорсткішим принципам і стандартам, ніж наведеним у цій Рекомендації.

Рекомендація iii. Вказівки в Рекомендації щодо перегляду національного законодавства, взаємозв'язок між Додатком I та Керівними принципами

20. Дотримання принципів забезпечується різними способами та різними засобами, залежно від механізму голосування та базової технології. Стандарти, наведені в Додатку I до Рекомендації, перетворюють ці принципи на конкретні цілі. Керівні принципи містять вказівки щодо реалізації цих цілей. Передбачається, що надалі Керівні принципи будуть

регулярно доповнюватися та оновлюватися, щоб бути узгодженими з практичним досвідом і розвитком нових технологій.

21. Між новою Рекомендацією та новими Керівними принципами існує тісний взаємозв'язок. Додаток I до Рекомендації містить базові стандарти високого рівня, що виражають цілі, яким має відповідати система е-голосування, щоби були дотримані принципи демократичних виборів. Стандарти повинні бути стабільними протягом усього часу. Детальні приписи щодо того, як імплементувати цілі (стандарти) включені до Керівних принципів. Вони ґрунтуються на досвіді та новелах у державах-членах, а також пропозиціях за результатами наукових досліджень.

22. Рекомендація радить державам-членам при запровадженні е-голосування, керуватися у своєму відповідному національному законодавстві її положеннями. Потрібно приділяти ретельну увагу аспектам законодавства, відмінним від тих, що стосуються просто потрібного електронного обладнання та його використання. Ступінь потрібного перегляду повинен залежати від чинного законодавства відповідної держави-члена. Приклади включають положення, пов'язані з методами голосування, норми кримінального законодавства щодо виборчих справ, законодавство про захист даних або законодавство про спостереження за виборами.

23. Державам-членам рекомендовано розглянути можливість внесення інших змін до законодавства, що можуть бути необхідними внаслідок запровадження е-голосування.

Рекомендації iv та v. Аналіз стану імплементації та політика оновлення на основі обміну досвідом у цій сфері

24. Е-голосування – це новий напрям, що стрімко розвивається. Стандарти й керівні принципи запровадження не повинні відставати від правових і технічних новел. З огляду на це рекомендовано, щоб кожна держава-член аналізувала свій розвиток у сфері е-голосування, повідомляла Раду Європи про результати такого аналізу та брала участь в роботі з оновлення Рекомендацій і Керівних принципів (див. пункт II). Рада повинна розглядати стан виконання цієї Рекомендації принаймні кожні два роки після її прийняття, а держави-члени мають обмінюватися усім досвідом у цій сфері.

Рекомендація vi. Переклад і розповсюдження

25. Рекомендація та Керівні принципи, що додані до неї, повинні бути перекладені та розповсюджені в кожній державі-члені місцевою мовою, щоб належним чином поінформувати органи адміністрування виборів та їх посадових осіб, громадян, політичні партії, національних і міжнародних спостерігачів, НУО, ЗМІ, науковців, постачальників рішень у сфері е-голосування та спеціальні контрольні органи у цій сфері.

Пункт II. Оновлення Керівних принципів

26. Керівні принципи імплементації положень Рекомендації CM/Rec(2017)5 щодо стандартів е-голосування – це «живий» документ, який має регулярно

оновлюватися, якщо цього вимагають правові, операційні чи технічні новели. Зазначений вище аналіз (пункт 24) надає можливість оцінювати таку потребу.

Пункт III. Скасування Рекомендації Rec(2004)11

27. Нова Рекомендація CM/Rec(2017)5 Комітету Міністрів державам-членам щодо стандартів е-голосування і Керівні принципи імплементації положень Рекомендації CM/Rec(2017)5 скасовують і замінюють собою чинну Рекомендацію Rec(2004)11 Комітету Міністрів Ради Європи державам-членам щодо правових, операційних і технічних стандартів е-голосування, «Керівні принципи розробки процесів, що засвідчують відповідність встановленим вимогам і стандартам (Сертифікація систем е-голосування)», а також «Керівні принципи забезпечення прозорості виборів із застосуванням електронних технологій». Це дозволить уникнути будь-якої плутанини в тому, які саме принципи, стандарти чи рекомендації відтепер стосуються е-голосування в державах-членах Ради Європи.

СТАНДАРТИ

28. Додаток I до Рекомендації містить перелік стандартів е-голосування, що виражають цілі, яким має відповідати е-голосування, щоб були дотримані принципи демократичних виборів і референдумів. Вони становлять мінімальні стандарти, котрі, якщо вони дотримані в системі е-голосування, сприятимуть відповідності принципам демократичних виборів і референдумів. Проте сама лише відповідність цим стандартам не гарантує демократичної якості е-виборів чи е-референдуму. Національне законодавство може містити додаткові вимоги. Е-вибори або е-референдум мають оцінюватися в цілому і зокрема, у конкретному контексті. Проте дотримання стандартів – це важливий елемент підвищення демократичної якості системи е-голосування.

ВИЗНАЧЕННЯ І ТЛУМАЧЕННЯ

29. Додаток II наприкінці документа містить визначення термінів, що використовуються в Рекомендації, Додатку I до неї та цій Пояснювальній записці. До цих визначень також потрібно звертатися, коли Рекомендації або окремі її частини перекладаються іншими мовами.

ДОДАТОК I. СТАНДАРТИ Е-ГОЛОСУВАННЯ

ЗАГАЛЬНЕ ВИБОРЧЕ ПРАВО

Стандарт № 1. «Інтерфейс виборця системи е-голосування…»[5]

30. Задля дотримання принципу загального виборчого права держави-члени повинні забезпечувати, щоб інтерфейс виборця системи е-голосування був зрозумілим і зручним для якомога більшої кількості виборців. Під час розробки інтерфейсу е-голосування потрібно враховувати міркування

5. Скорочені формулювання цього і подальших стандартів узгоджені з їх редакцією у перекладі Рекомендації CM/Rec(2017)5.

ергономіки, щоб узяти до уваги взаємодію між інтерфейсом і виборцем. Мета полягає в тому, щоб виборець міг легко користуватися системою та виконувати вказівки, зокрема ті, що стосуються захисту.

31. Необхідно взяти до уваги різні обмеження з боку користувачів, пов'язані з віком, мовою, способом життя тощо. Інструкції, що надаються виборцям, мають бути чіткими, легко зрозумілими та такими, які можуть бути виконані якомога більшою кількістю виборців.

Стандарт №2. «Система е-голосування повинна бути розроблена у такий спосіб…»

32. Не всі особи з інвалідністю можуть бути здатними користуватися е-голосуванням. Конструкція системи е-голосування повинна, однак, прагнути до максимального використання потенціалу доступності, що надає їм цей механізм голосування. У зіставленні з іншими доступними механізмами голосування, е-голосування спрямоване на те, щоби забезпечити якомога ширшому колу осіб з інвалідністю та особливими потребами можливість голосувати самостійно.

33. На рівні реалізації відповідальний орган вирішує, як задовольняти запити людей з інвалідністю та особливими потребами. Наприклад, індивідам з порушеннями зору або з дислексією можуть знадобитися пристрої читання з екрана, різко контрастні текст і фон, а також функція регулювання розміру тексту у їх веб-браузері або машинах для голосування. Користувачі з комунікативними розладами можуть віддавати перевагу графічно представленій інформації. Особи з порушеннями координації можуть віддавати перевагу використанню клавіатури, а не миші. Інтерфейси голосування повинні бути адаптованими до потреб користувачів з обмеженими можливостями пересування.

34. Зручні для користувачів рішення, адаптовані для осіб з інвалідністю, можуть виявитися менш стійкими до загроз безпеці е-голосування. Саме з цієї причини відповідальному органу належить приймати рішення щодо їхньої розробки й використання у міру практичної можливості, тобто настільки, наскільки досягатиметься прийнятний баланс між зручністю та захистом.

Стандарт №3 «Якщо механізми дистанційного е-голосування не є загальнодоступними…»

35. Доповнення традиційних форм голосування додатковими механізмами, тобто е-голосуванням, може зробити вибори та референдуми більш доступними й у такий спосіб зміцнити принцип загальності. Проте пропонування виключно дистанційного механізму е-голосування обмежує доступність, зважаючи на те, що механізм, тобто інтернет, не є загальнодоступним на цей час. Це положення покликане захистити виборця, щоб йому чи їй пропонувався дійсно доступний засіб голосування.

Стандарт №4 «Перед поданням голосів через систему дистанційного е-голосування…»

36. При запровадженні цілком нових методів голосування, особливо дистанційного е-голосування, увагу виборців особливо потрібно звертати на те, що це є офіційний механізм, який використовується в реальних виборах чи референдумі. Мета полягає в запобіганні тому, щоб виборці помилково вважали, що беруть участь у несправжніх виборах або референдумі чи будь-якому іншому тестуванні. Такі самі комунікаційні зусилля повинні вживатися під час використання демонстраційної чи пробної версії, щоб у виборців не склалося враження, що вони вже проголосували. Навіть більше, вибори чи референдум варто чітко відрізняти від опитувань громадської думки та навпаки.

РІВНЕ ВИБОРЧЕ ПРАВО

Стандарт №5 «Вся офіційна інформація про голосування має надаватися однаково…»

37. Вся офіційна інформація про голосування, зокрема про опції голосування, повинна надаватися рівною мірою по різних механізмах голосування. Це означає рівність змісту. Повинні бути вжиті заходи, які запобігають як пропуску інформації, що має з'являтися на електронному бюлетені, так і внесенню будь-яких додаткової інформації, яка не повинна з'являтися на офіційному бюлетені, як це передбачено законом.

38. Це також означає, що повинна бути рівність щодо того, як інформація виводиться на дисплей. Проте повної рівності на дисплеї може виявитися важко або неможливо досягти, оскільки різні пристрої (наприклад, мобільний телефон, цифрове телебачення, машини для е-голосування або персональний комп'ютер) по-різному виводять інформацію на свої екрани. У такому разі потрібно визнати, що це не суто технічне питання і що його не варто залишати на рішення лише технічного персоналу. Вказівки з цього питання має надати орган адміністрування виборів.

Стандарт №6 «У разі використання як електронних, так і неелектронних механізмів голосування…»

39. Е-голоси спочатку розшифровуються і підраховуються. Тоді результати об'єднуються з тими, що отримані за паперовими бюлетенями, та підраховується остаточний результат. Для цього потрібен метод об'єднання, ймовірно, програмний. Він повинен задовольняти ті самі вимоги безпеки та надійності, що й програмне забезпечення для е-голосування.

40. Якщо кількість е-голосів або паперових бюлетенів особливо невелика, існує ризик порушення таємності голосування в разі розголошення результатів, отриманих за цими небагатьма бюлетенями. Метод об'єднання повинен включати необхідні технічні та процедурні запобіжники, які б забезпечували об'єднання результатів, отриманих через різні механізми голосування, перед оголошенням результатів виборів, у такий спосіб забезпечуючи

таємність. Крім того, процедурні норми, пов'язані саме з втручанням персоналу в процес підрахунку голосів, повинні враховувати такі випадки.

Стандарт № 7 «Повинна бути забезпечена однозначна ідентифікація виборців…»

41. Однозначна ідентифікація стосується перевірки ідентичності конкретної особи за одним чи кількома параметрами, так що особу можна безпомилково відрізняти від усіх інших. Тому реєстри виборців потрібні, щоб уникати цифрових близнюків, тобто осіб, які мають однакові ідентифікаційні дані. У разі використання централізованих реєстрів виборців однозначна ідентифікація може здійснюватися неявно під час внесення даних особи в базу даних. Для взаємопов'язаних реєстрів виборців можуть знадобитися додаткові засоби.

42. Оскільки дехто може бути як виборцем, так і кандидатом, важливо запобігати тому, щоб така особа мала однакову ідентифікацію в системі для всіх своїх функцій. Те саме стосується осіб, які можуть бути як адміністраторами системи е-голосування, так і виборцями. Автентифікація може здійснюватися на основі як ідентичності, так і виконуваних функцій. Тоді як для виборців, які реєструються чи подають голос, або під час висування кандидатів, доцільно використовувати автентифікацію на основі ідентичності, застосування автентифікації на основі виконуваних функцій може виявитися достатнім для адміністраторів, аудиторів тощо.

Стандарт № 8 «Система е-голосування повинна надавати користувачеві доступ…»

43. У разі, якщо маркери анонімного голосування свідчать про те, що виборець має право голосу, ідентифікація виборця на цьому етапі може не вимагатися, оскільки вона вже відбулася на більш ранньому етапі, тобто під час присвоєння окремого маркера конкретному виборцю.

Стандарт № 9 «Система е-голосування повинна забезпечувати, щоб кожен виборець…»

44. Усі голоси, подані електронними чи неелектронними механізмами голосування, підраховуються. Має бути забезпечено, щоб до результатів виборів зараховувалися голоси лише повноважних виборців. Повинен бути дотриманий принцип «одна людина – один голос», і для кожного виборця повинна враховуватися лише належна кількість голосів, передбачена законодавством.

ВІЛЬНІ ВИБОРИ

Стандарт № 10 «Намір виборця проголосувати не повинен зазнавати впливу…»

45. Система голосування не повинна впливати на наміри повноважних виборців. Особисте здійснення права голосу є базовим принципом. Оскільки воно особливо вразливе в ситуації дистанційного е-голосування, до цієї обставини повинна бути привернута особлива увага. Цей стандарт не забороняє дистанційного е-голосування, однак на нормативному рівні та на рівні реалізації повинні бути запроваджені адекватні положення,

щоб забезпечити дотримання особистого й вільного голосування. Те саме стосується недистанційного е-голосування.

46. У контексті дистанційного е-голосування повинні бути взяті до уваги такі моменти: можливість імітації офіційного сервера через маніпулювання системою доменних імен (DNS); використання доменного імені, подібного до доменного імені офіційного сервера е-голосування; здійснення атаки типу «незаконний посередник»; або наявність шкідливої програми в системі виборця, яка замінює оригінальний бюлетень чи подає фальсифікований бюлетень.

47. Залежно від національного законодавства та політики та забезпечення доступності принцип загального виборчого права може отримувати перевагу над принципом особистого голосування, і тому, наприклад, може дозволятися голосування за довіреністю. Такі самі умови застосовні також до механізму е-голосування. Проте і тут повинні бути дотримані норми та умови, що допускають голосування за довіреністю.

48. Електронні підписи, коди перевірки чи інші технології, що застосовуються до бюлетеня, дозволяють пересвідчитися в тому, що голос не зазнав маніпуляцій. Проте використання цих технологій повинно забезпечувати дотримання таємності голосування. Водночас повинно існувати чітке регулювання дій у випадку, коли перевірка виявляє заборонені маніпуляції з поданим голосом.

Стандарт № 11 «Повинно бути забезпечено надання виборцю системою е-голосування автентичного виборчого бюлетеня…»

49. Окрім технологій, передбачених стандартами № 5 і № 10, стандарт № 11 вимагає запровадження процедурних заходів, які мають забезпечити, що вся інформація, введена в систему е-голосування і надана виборцю через інтерфейс е-голосування, є автентична, тобто ідентична до наданої компетентним органом.

Стандарт № 12 «Спосіб, яким виборці повинні проходити через процес…»

50. Під час процесу голосування важливо, щоб рішення не могли бути прийняті шляхом ненавмисного натискання на кнопку чи посилання, а дійсно відображали волю виборця. Зокрема, якщо е-голосування відбувається у неконтрольованому середовищі, виборцю на початку цього процесу потрібно нагадати, що він чи вона бере участь у реальному голосуванні. Протягом усього процесу, як у контрольованих, так і в неконтрольованих формах е-голосування, виборець повинен мати достатньо часу на роздуми та реагування, так що він чи вона не повинні бути змушеними голосувати без роздумів щодо зробленого вибору. Дизайн інтерфейсу, повідомлення виборцеві та всі інші відповідні аспекти мають бути запрограмовані у такий спосіб, щоб дозволяти виборцеві вираження своєї справжньої волі. Наприкінці процесу голосування обрані виборцем варіанти повинні узагальнюватися, і виборця мають попросити підтвердити, чи таке узагальнення відображає його чи її справжню волю.

Лише після цього голос повинен відсилатися на сервер голосування або вноситися до електронної виборчої скриньки. Проте детальна реалізація цього положення може мати варіанти залежно від специфіки системи е-голосування, що використовується.

Стандарт № 13 «Система е-голосування повинна надавати виборцю…»

51. У системах голосування з використанням паперових бюлетенів виборці мають можливість брати участь у виборах, але не віддавати перевагу запропонованим опціям. Цей стандарт передбачає, що така можливість повинна забезпечуватися і в е-голосуванні.

52. Цей стандарт не впливає на правомірність і наслідки подання незаповненого бюлетеня чи навмисного подання недійсного голосу. Ці питання регламентуються на національному рівні. Країни вирішують, наприклад, чи такі голоси є прийнятними, як (якщо так) їх треба підраховувати, або який їх правовий вплив на результат. Кожна держава-член самостійно вирішує, чи такі опції повинні бути дозволеними також при е-голосуванні. Там, де опція «порожнього голосу» вже передбачена для паперового бюлетеня, достатньо, щоб ця опція також була наявна у бюлетені для е-голосування. Цей стандарт просто забороняє системи, в яких виборець змушений обирати одну опцію (іншу, аніж незаповнений бюлетень), щоб завершити процес голосування. Як такий, він покликаний забезпечувати ті самі гарантії, що й система, заснована на паперових бюлетенях, коли виборець, наприклад, має можливість не обирати жодного із запропонованих кандидатів.

Стандарт № 14 «Система е-голосування повинна повідомляти виборця…»

53. Як було роз'яснено в попередніх пунктах, ця Рекомендація не перешкоджає державам-членам запроваджувати інші опції голосування, такі як можливість умисного подання недійсного голосу. Навіть більше, умисно подані дійсні голоси за певних обставин можуть бути визнані недійсними через технічні труднощі без обов'язкового ознайомлення виборця з цим фактом. Цей стандарт не вимагає того, щоб можливість подання недійсного голосу запроваджувалася як опція голосування. Він вимагає лише того, аби щоразу, коли система е-голосування з будь-яких причин отримує недійсний голос, виборець, який подав такий голос, був про це відповідно поінформований. Мета полягає в тому, щоб уникнути ненавмисного подання недійсних е-голосів. Це застосовується до всіх випадків, незалежно від того, дозволяє чи забороняє система е-голосування подання недійсних голосів. Звичайно, це стосується лише голосів, поданих в електронному вигляді.

54. Повідомляючи виборця про те, що його чи її голос недійсний, система повинна також інформувати його чи її про наслідки такої недійсності (враховується чи ні такий голос тощо), а також про можливість знову подати голос, якщо недійсний голос був поданий ненавмисно. Якщо система не приймає недійсні голоси, у поданні бюлетеня може бути відмовлено, або ж він може бути прийнятий та анульований. Якщо система приймає

недійсні голоси, то такий голос буде прийнято за результатами реакції з боку виборця: якщо недійсний голос подано ненавмисно, виборець може знову проголосувати; в іншому разі, виборець, навмисно подавши недійсний голос, підтверджує цей вибір. Багато тут залежить від національного регулювання недійсних голосів. Перевага системи е-голосування полягає в тому, що у виборця є можливість отримати повідомлення та відреагувати на таку недійсність, якщо вона не відображає його справжньої волі.

Стандарт № 15 «Виборець повинен мати можливість пересвідчитися в тому, що…»

55. Стандарти № 15–18 запроваджують механізми перевірюваності, що розвивають концепцію ланцюжка довіри у виборах з використанням електронних технологій. Стандарт № 15 посилається на інструменти перевірюваності, які надають можливість виборцю пересвідчитися в тому, що його чи її е-голос було подано відповідно до бажання та зафіксовано так, як він поданий, що також відоме як індивідуальна перевірюваність. Інструменти індивідуальної перевірюваності можуть бути різними залежно від конкретного рішення в сфері е-голосування. Прикладами таких інструментів є доступний для перевірки виборцями паперовий контрольний журнал, що формується машиною для е-голосування, яка використовується у приміщенні для голосування, або зворотні коди, що використовуються в інтернет-голосуванні.

56. Стандарт №16 стосується підтвердження системою того, що процедура голосування була завершена успішно. Стандарт № 17 звертає увагу на інструменти перевірюваності, які дозволяють усім зацікавленим суб'єктам пересвідчитися в тому, що голоси підраховані так, як були зафіксовані (загальна перевірюваність), а стандарт № 18 передбачає можливість перевірки того, що лише голоси повноважних виборців були включені до остаточних результатів, тим самим замикаючи ланцюжок довіри.

Стандарт № 16 «Виборець має отримати від системи підтвердження…»

57. Процедура голосування успішно завершена, якщо електронний голос надійшов до електронної виборчої скриньки. У контексті дистанційного е-голосування це означає, що процедура голосування успішно завершена лише тоді, коли голос відісланий з пристрою виборця для голосування (персонального комп'ютера, телефону тощо) через інтернет або іншу мережу і досяг свого призначення, тобто сервера з виборчою скринькою.

58. Система підтверджує виборцю, що його чи її голос надійшов до виборчої скриньки та буде підрахований і що процес голосування успішно завершений. Як тільки виборець дізнається про це, він чи вона може спокійно вийти з системи або розірвати зв'язок. Обидва повідомлення про успішне подання голосу та про завершення процедури можуть об'єднуватися в одне повідомлення, якщо ці дві події збігаються. До належної практики відноситься супровід цих повідомлень нагадуванням і вказівками виборцю про те, як знищити сліди голосування, якщо голос подавався через неконтрольований пристрій.

Стандарт № 17 «Система е-голосування повинна надавати надійні докази того, що кожен автентичний голос…»

59. Система голосування забезпечує коректне внесення кожного голосу до результатів виборів. Це вимагає спроможності надавати виборцям і третім сторонам переконливі докази того, що отримані результати є достовірним і точним відображенням поданих автентичних голосів та відповідають правовим вимогам до демократичних виборів і референдумів. Термін «переконливі докази» стосується критеріїв, за якими ці докази можуть загалом бути визнаними. Термін «автентичні голоси» стосується згаданих вище стандартів, які забезпечують, що голос відображає вільне волевиявлення виборця.

60. Крім того, повинна існувати можливість контролю доказів з метою перевірки їхньої правильності за допомогою інструментів, зовнішніх щодо і незалежних від системи е-голосування. Для цього система е-голосування має забезпечувати інтерфейси з можливостями комплексного спостереження та аудиту, підпорядковану потребі таємності та анонімності голосу.

61. Відсоток голосів, поданих електронно, та порівняння результатів е-голосування з результатами голосування за допомогою інших механізмів можна використовувати, щоби визначити ймовірність правильності результатів е-голосування.

Стандарт № 18 «Система повинна надавати надійні докази того, що лише голоси, подані повноважними виборцями…»

62. Виборці та треті сторони повинні мати можливість перевірити, що лише голоси повноважних виборців включені до результатів. Водночас підраховані голоси мають бути анонімними. У разі інтернет-голосування існують методи шифрування, що не потребують декодування до підрахунку голосів (гомоморфне шифрування). Підрахунок може проводитися без розкриття змісту зашифрованих голосів.

ТАЄМНЕ ГОЛОСУВАННЯ

Стандарт № 19 «Е-голосування повинно бути організованим у такий спосіб, щоб…»

63. Цей стандарт встановлює загальну вимогу щодо таємності голосування, яка поширюється на всю процедуру: на етап до голосування (наприклад, передання виборцям персональних (ПІН) кодів або електронних маркерів), протягом заповнення виборчого бюлетеня, подання та передання виборчого бюлетеня, а також на підрахунок і будь-який повторний підрахунок голосів.

64. Потрібні заходи, звичайно, включають до себе шифрування, а також, наприклад, перемішування поданих голосів в електронній виборчій скриньці, щоб послідовність, у якій вони надходять на етапі підрахунку голосів, не дозволяла б реконструювати послідовність їхнього подання.

Стандарт № 20 «Система е-голосування повинна обробляти і зберігати…»

65. Система голосування повинна обробляти та зберігати лише ті персональні дані, без яких ця система не може належно функціонувати. Це вимога, відома також як «мінімізація даних», стосується даних, потрібних для задоволення правових вимог до процесу голосування. Орган адміністру-вання виборів, відповідальний за організацію е-голосування, визначає такі дані та повинен бути здатним пояснити, які правові норми і міркування мають наслідком їх необхідність. Тривалість обробки, зберігання тощо також залежить від правових вимог, а саме тих, що стосуються оскарження. Мінімізація даних покликана забезпечувати захист даних і є частиною таємності голосування.

Стандарт № 21 «Система е-голосування та будь-який уповноважений суб'єкт повинні захищати…»

66. Національне законодавство може передбачати різні способи ідентифікації та автентифікації для різних механізмів голосування (зазначення імені виборця, подання паспорта (ID-card), використання кодів, унікальних для кожного виборця тощо). Загальна мета полягає в тому, щоб забезпечити, що лише особи, які мають право голосу, можуть реально проголосувати, а також щоб запобігти багаторазовому голосуванню чи іншим зловживанням.

67. Стандарт передбачає, що сама система і будь-який уповноважений суб'єкту певний момент здійснює обробку інформації автентифікації. Прикладом уповноваженого суб'єкта є суб'єкт, який друкує матеріали для голосування, що містять інформацію автентифікації. Система і будь-який уповноважений суб'єкт повинні захищати цю інформацію за допомогою технічних і організаційних засобів. Усі інші, за визначенням неуповноважені суб'єкти, не повинні мати доступу до цих даних чи використовувати їх в інший спосіб.

68. Інші сервіси, такі як інформаційні послуги, що надаються виборцям до початку процесу голосування та які очевидно не потребують автентифікації, перебувають поза сферою дії цього стандарту.

Стандарт № 22 «Доступ до реєстрів виборців, що зберігаються або передаються системою е-голосування…»

69. Цей стандарт передбачає, що спеціальний доступ до реєстрів виборців мають лише уповноважені особи.

Стандарт № 23 «Система е-голосування не повинна надавати виборцю…»

70. Мета цього стандарту полягає в тому, щоб запобігти порушенням таємності голосування, а також продажу голосів. Проте індивідуальна перевірюваність може бути реалізована за умови наявності достатніх запобіжних заходів, що унеможливлюють примус або купівлю голосів.

71. Повинні існувати нормативні положення щодо випадків порушення таємності голосування або продажу голосів. У багатьох країнах відповідальність за такі порушення встановлюється нормами кримінального за-

кону. Ці норми охоплюють всі використовувані механізми голосування і повинні також застосовуватися у разі використання е-голосування. У разі необхідності вони мають бути оновлені з огляду на специфіку е-голосування.

72. Там, де виготовляється паперове підтвердження змісту поданого голосу, як це має місце у контрольованих середовищах, де використовують електронні машини для голосування, повинні застосовуватися технічні та організаційні заходи, які б запобігали будь-якому іншому використанню виборцем цього підтвердження, ніж звичайне використання, передбачене процесом голосування. Наприклад, виборцю не дозволяється використовувати це підтвердження, порушуючи таємність голосування, або виносити його за межі приміщення, що перебуває під спостереженням.

73. У системі дистанційного е-голосування з використанням інтернету виборець має бути поінформований про потребу в знищенні на пристрої, що використовувався для подання голосу, слідів операції голосування, а також про те, як це зробити. Такі сліди можуть зберігатися, наприклад, у пам'яті персонального комп'ютера, кеші браузера, відеопам'яті, файли підкачки, тимчасових файлах тощо.

74. Особливу увагу треба приділяти способу, яким реалізуються анонімність і таємність голосування, у процесі проєктування системи е-голосування. Щодо дистанційного е-голосування існує щонайменше три рівні, які потрібно розглянути: веб-застосунок, браузер і службові програми на комп'ютері виборця.

    - a. Веб-застосунок не повинен дозволяти користувачеві зберігати копію свого голосу. Він не має пропонувати функції роздруку, запису чи зберігання голосу або (фрагменту) вмісту екрану, на якому видно поданий голос.

    - b. Браузер не має пропонувати можливості роздруку екрану, на якому видно поданий голос. Варто зазначити, що браузери можуть зберігати та фактично зберігають інформацію кількома способами. Наприклад, за допомогою кнопки «назад» у браузері можна вивести на екран одну чи більше попередніх сторінок. Наскільки це можливо, така загальна функція браузерів повинна блокуватися веб-застосунком. Принаймні, інформація не повинна зберігатися після того, як виборець завершив голосування.

    - c. Потрібно також брати до уваги елементи програмного забезпечення, здатні певним чином записувати дії конкретного користувача комп'ютера. Трьома звичайними прикладами є: програми скриншоту; програми, що роблять відео з послідовності екранів; програми, що записують натискання користувачем клавіш. Такі програми можуть існувати на комп'ютері користувача без його відома як шкідливі програми. Система е-голосування може виявитися нездатною запобігти присутності таких зловмисних програм. Виборець має бути поінформований про можливу присутність цих шкідливих програм, пов'язані

з ними потенційні ризики, належну практику, якої йому чи їй варто дотримуватися, щоби звести ці ризики до мінімуму, та загалом про доступні йому чи їй альтернативні й більш захищені механізми голосування.

Стандарт № 24 «До моменту закриття електронної виборчої скриньки система е-голосування…»

75. Цей стандарт покликаний запобігти встановленню та публікації проміжних результатів через механізм е-голосування. Інформація про рівень участі виборців у голосуванні перебуває поза сферою дії цього стандарту і може збиратися та публікуватися відповідно до положень національного регулювання.

Стандарт № 25 «Е-голосування повинно забезпечувати дотримання таємності попередніх варіантів…»

76. Цей стандарт вимагає того, щоб таємниця попередніх варіантів вибору, введених і знищених виборцем у процесі голосування, мала такий самий захист, як і таємниця остаточно поданого голосу.

Стандарт № 26 «Процес е-голосування, особливо етап підрахунку голосів…»

77. Цей стандарт передбачає неможливість встановлення зв'язку між голосом і виборцем, який його подав, запобігаючи у такий спосіб порушенню таємності голосування.

78. У процесах недистанційного е-голосування автентифікація виборців і подання голосу можуть бути розділені також фізично і в разі використання систем е-голосування. Це фізичне розділення, у принципі, може контролюватися посадовцями органів адміністрування виборів і спостерігачами на виборах, якщо припускати наявність навмисної чи випадкової помилки в системі е-голосування (і відсутність шкідливих програм).

79. У процесі дистанційного голосування інформація, пов'язана з виборцем (зазвичай це код), і подані голоси до певного етапу пов'язані між собою. У країнах, що допускають багаторазове голосування, така прив'язка потрібна для опрацьовування послідовності поданих голосів та наслідків такого подання (наступний голос усуває попередній). Розділення має здійснюватися електронними засобами на заздалегідь визначеному етапі перед тим, як розпочнеться підрахунок голосів. Це потребує спеціальних технічних рішень.

80. Там, де національне законодавство вимагає наявності постійної прив'язки голосу до виборця, а також її зберігання під час виборів чи референдуму і певний час після цього, потрібно пересвідчуватися в тому, що прив'язка виборця до його чи її бюлетеня достатньо захищена протягом цього періоду, щоб забезпечити таємність голосування. Така прив'язка може розкриватися лише за наказом компетентного судового органу, і водночас потрібно забезпечувати, щоб навіть у разі розкриття цього зв'язку виборець не був змушений розголошувати, як саме він чи вона проголосував(-ла).

81. Система аудиту має постійно зберігати анонімність виборця, якщо інше окремо не передбачене положеннями національного законодавства. У будь-якому разі, зібрана системою аудиту інформація має бути захищена від несанкціонованого доступу.

НОРМАТИВНІ ТА ОРГАНІЗАЦІЙНІ ВИМОГИ

Стандарт № 27 «Держави-члени, які запроваджують е-голосування…»

82. Технології електронного голосування повинні запроваджуватися поступово, поетапно та випробуватися в реальних умовах заздалегідь перед днем виборів. Як свідчить досвід держав-членів, поступове впровадження необхідне з огляду на правові та технічні проблеми й можливості, що несе з собою е-голосування. Деякі основні етапи описані в керівних принципах, що стосуються цього стандарту.

83. Зокрема, перед запровадженням дистанційного е-голосування інші форми дистанційного голосування, такі як голосування поштою (листом), повинні бути вже добре усталеними та користуватися довірою. Багато пов'язаних із дистанційним е-голосуванням проблем, що стосуються операційних аспектів і довіри з боку користувачів, пов'язаних із дистанційним е-голосуванням, подібні до пов'язаних із голосуванням поштою і можуть легше вирішуватися в контексті голосування поштою.

Стандарт № 28 «Перш ніж запроваджувати е-голосування, держави-члени…»

84. Хоча цей стандарт може на перший погляд здаватися очевидним, він покликаний привернути увагу держав-членів до того, що, окрім регулювання деталей е-голосування, у них може виникнути потреба у внесенні змін до законів або навіть конституції, щоб дозволити е-голосування. Чинне законодавство не пишуть з урахуванням автоматизації, і воно може виявитися неоднозначним при застосуванні до е-голосування.

85. Інший урок, почерпнутий з досвіду, накопиченого в регіоні, полягає в тому, що нормативне регулювання е-голосування має бути деталізованим, щоб надати усім відповідним зацікавленим суб'єктам можливість розуміти е-голосування та здійснювати щодо нього свої власні функції. Навіть більше, наявність детального регулювання важливе для гарантування того, що запровадження технологій відповідає принципам демократичних виборів і референдумів.

86. Нормативна база повинна передбачати можливість судового перегляду е-голосування, що дозволяє громадянам оскаржувати чинний метод, що використовується для е-голосування, а також імплементацію цього методу, збільшуючи так суспільну довіру до е-голосування та довіру до нього.

Стандарт № 29 «Відповідне законодавство повинно регулювати відповідальність…»

87. Існують численні зацікавлені суб'єкти, які відіграють роль і несуть певну відповідальність у розробці, тестуванні, сертифікації, розгортанні, засто-

суванні, підтримці систем е-голосування, спостереженні за ними та їх аудиті. Проте, зрештою, саме уряд несе загальну відповідальність за голосування і, відповідно, за систему е-голосування. Рекомендується, щоби відповідне законодавство передбачало здійснення функції нагляду за е-голосуванням з боку органу адміністрування виборів. Роль та повноваження інших залучених суб'єктів варто уточнювати на відповідному регуляторному чи договірному рівні.

88. Одним із аспектів, який допоможе впевнитися в тому, що орган адміністрування виборів здійснює дієвий контроль щодо е-голосування, є те, щоб держави-члени не були надто залежними від лише небагатьох постачальників, оскільки це може призвести до включення постачальників у систему. Дійсно, програмне та апаратне забезпечення системи е-голосування потребує постійного обслуговування. До цього додаються процедури, пов'язані зі спеціальними заходами, наприклад, формуванням виборчих бюлетенів. Якщо розглядається можливість аутсорсингу, то вкрай важливо, аби ті хто відповідальний за вибори, розуміли, що саме й чому передається на аутсорсинг, які методи та процеси має намір застосовувати постачальник. Законодавчо встановлені повноваження органу, уповноваженого здійснювати організацію підготовки і проведення виборів, у жодному разі не повинні передаватися на аутсорсинг, оскільки саме цей орган має повноваження щодо виборів.

Стандарт № 30 «Кожен спостерігач повинен мати можливість спостерігати за підрахунком голосів. Відповідальність за процес підрахунку голосів покладається на орган адміністрування виборів».

89. Цей стандарт покликаний підкреслити роль органу адміністрування виборів у процесі підрахунку голосів, причому не лише як одного з учасників, а і як суб'єкта, що організує підрахунок голосів та здійснює за ним нагляд. Повинна бути передбачена можливість присутності спостерігачів при цьому процесі. Такі спостерігачі повинні включати представників як політичних партій, так і широкої громадськості.

ПРОЗОРІСТЬ І СПОСТЕРЕЖЕННЯ

Стандарт № 31 «Держави-члени зобов'язані забезпечувати прозорість…»

90. Система е-голосування може бути запроваджена лише тоді, коли виборці мають довіру і впевненість у свої виборчій системі та виборчій адміністрації. Однак довіра не наступає просто так, і держави повинні робити все можливе, щоб забезпечити її збереження. Сприяння прозорій практиці в державах-членах – це ключовий елемент у розбудові суспільної довіри та впевненості. Прозорість у питаннях системи е-голосування, процесах навколо неї та підставах запровадження е-голосування сприятимуть обізнаності та розумінню з боку виборців, водночас формуючи довіру і суспільну впевненість.

91. Цей стандарт передбачає широку прозорість усіх аспектів усіх форм е-голосування. Зокрема, повинна бути гарантована прозорість системи, тобто можливість перевіряти її належне функціонування. Держави-чле-

ни повинні внормувати, кому, до чого, коли й за яких обставин надається доступ.

92. Прозорості також можна досягнути через відкритість щодо процедури е-голосування. Окрім системи електронного голосування, держави-члени також повинні забезпечувати прозорість усіх процедур (перед, під час і після дня/періоду виборів), пов'язаних з е-голосуванням. Цього можна досягти публікацією на офіційному сайті наочних прикладів (наприклад, фотографій, відео тощо), які б роз'яснювали е-голосування всім зацікавленим суб'єктам. Задля подолання комунікативних бар'єрів навколо питання е-голосування варто також використовувати мову жестів і субтитри.

93. У процес запровадження виборів із застосуванням електронних технологій потрібно залучати представників осіб з інвалідністю, щоб побачити, як саме це може впливати на людей, яких вони представляють.

Стандарт № 32 «Задовго до початку голосування громадськість, зокрема, виборці…»

94. Е-вибори відрізняються від виборів або референдуму тим, що проводяться без е-голосування, зокрема, процедурами, яких повинні дотримуватися виборці. Прикладами можливих відмінностей є: проміжок часу, протягом якого можуть бути подані голоси; кроки, які має здійснити виборець, щоб узяти участь в е-виборах; те, як фактично відбувається е-голосування. Ці відмінності потрібно довести до відома кожного виборця, щоб уникнути будь-якого неправильного розуміння процедур і щоб надати виборцю всю інформацію, необхідну для використання механізму е-голосування. Особливу увагу потрібно приділити проблемі, скільки часу необхідно виборцеві, щоб дійти до цього рішення. Варто також приділити увагу проблемі надання виборцю можливості перевірити придатність свого обладнання, перш ніж він чи вона вирішить скористатися конкретним каналом е-голосування.

Стандарт № 33 «Складові системи е-голосування повинні бути відкритими…»

95. Істотне значення має оцінювання того, чи системи е-голосування функціонують належно і чи забезпечується захист. Засобами реалізації цього є незалежне оцінювання або сертифікація системи як цілого чи її окремих компонентів, що потребує розкриття інформації про критичні елементи системи. Оцінювання може здійснюватися, наприклад, через розкриття дизайну системи, надання дозволу на перевірку робочої документації, розкриття вихідних кодів, надання дозволу на перевірку звітів про оцінювання та сертифікації компонентів, проведення поглибленого тестового проникнення тощо. Фактичний рівень розкриття елементів системи, потрібний для отримання належних гарантій, залежить від особливостей системи, її компонентів і сервісів, які вона надає.

Стандарт № 34 «Кожен спостерігач в межах, встановлених законом, повинен мати можливість…»

96. Хоча публічна доступність документів важлива, не всі будуть здатні зрозуміти систему е-голосування. Щоб мати довіру, виборці покладаються на інших, хто здатний зрозуміти відповідні матеріали і процеси. Тому вкрай важливо, щоб спостерігачі мали якнайширший доступ до відповідних документів, засідань, заходів тощо.

97. Існують різноманітні міжнародні та внутрішні спостереження за виборами. Спостерігачі повинні включати представників як кандидатів і політичних партій, так і широкої громадськості, а також незалежних внутрішніх та міжнародних спостерігачів. Усі держави-члени взяли на себе зобов'язання відповідно до Документу Копенгагенської наради Конференції з людського виміру ОБСЄ від 29 червня 1990 року «запрошувати спостерігачів від будь-яких держав-учасниць ОБСЄ та інших відповідних приватних інституцій та організацій, які мають таке бажання, спостерігати за перебігом їхніх загальнонаціональних виборів [… і…] сприяти аналогічному доступу до виборчих процесів, що проводяться на рівні, нижчому за загальнонаціональний». Порядок прийняття спостерігачів, а також права та обов'язки спостерігачів визначаються законодавством відповідної країни та мають відповідати міжнародним зобов'язанням цієї країни.

98. В обсязі, дозволеному законом, спостерігачі повинні мати можливість пересвідчитися в тому, що сама система е-голосування спроєктована та функціонує з дотриманням основних принципів демократичних виборів і референдумів. Отже, держави-члени повинні мати чіткі правові норми щодо доступу спостерігачів до документації та даних аудиту системи е-голосування.

99. Е-голосування становить особливу проблему для спостерігачів, характерну для електронного проведення виборів чи референдуму. Відповідно спостерігачі повинні бути забезпечені, зокрема, доступом до відповідної інформації про програмне забезпечення, можливістю вивчати фізичні та електронні заходи безпеки на серверах, перевіряти та тестувати сертифіковані пристрої, мати доступ до сайтів та інформації, що надаються для дистанційного е-голосування, і тестувати їх, а також спостерігати за поданням електронних голосів та їх підрахунком. Проте заходи безпеки можуть вимагати заборони присутності спостерігачів безпосередньо у самому комп'ютерному приміщенні. У такому разі повинні бути вжиті заходи, щоб надати спостерігачам можливість вести моніторинг діяльності.

Стандарт № 35 «Для забезпечення взаємодії між різними технічними…»

100. Щоб мати можливість використовувати системи чи сервіси е-голосування від різних постачальників, вони мають бути функціонально сумісні. Функціональна сумісність означає, що вхідні та вихідні параметри відповідають відкритим стандартам і, особливо, відкритим стандартам е-голосування. Такі стандарти потрібно регулярно оновлювати, щоб враховувати правові та технічні новели.

101. Основними перевагами від використання відкритих стандартів є такі:

- Ширший вибір продукції та постачальників;
- Менша залежність від одного постачальника;
- Можливість уникнути бар'єрів для зміни постачальника;
- Стабільність або зниження витрат;
- Простіше пристосування до змін у майбутньому.

102. Країни, зокрема децентралізовані, у складі декількох штатів/суб'єктів і, відповідно, з різноманітністю виборчої практики, можуть вирішити приймати такі стандарти на рівні країни[6]. На регіональному рівні, країни можуть приймати рішення про запровадження регіональних стандартів.

103. На міжнародному рівні OASIS, міжнародний консорціум з питань функціональної сумісності е-бізнесу, розробив стандарти виборів та інформаційних сервісів для виборців з використанням XML. OASIS розробив Election Markup Language (EML). EML – це набір визначень даних і повідомлень, описаних у вигляді XML-схем. Це був перший міжнародний стандарт структурованого обміну даними між постачальниками апаратного, програмного забезпечення та сервісів, залученими до будь-якого напряму забезпечення виборів чи сервісів для виборців. Його функцією є забезпечення відкритих захищених, стандартизованих та функціонально сумісних інтерфейсів між компонентами виборчих систем. Додаткові відомості про діяльність OASIS у сфері виборів (яка завершилася в середині 2015 року) можна знайти за посиланням www.oasis-open.org/committees/election.

ПІДКОНТРОЛЬНІСТЬ

Стандарт № 36 «Держави-члени повинні розробити технічні, оцінювальні…»

104. Органи адміністрування виборів або призначені ними суб'єкти повинні розробити технічні вимоги до систем е-голосування. Вони повинні далі розробити вимоги до технологій оцінювання від тестування і до офіційної сертифікації систем е-голосування. Такого типу вимоги містяться в «Загальних критеріях оцінки безпеки інформаційних технологій» CC/ISO 15408.

105. Обидва види вимог спрямовані на забезпечення, вже перед реальним використанням системи е-голосування на виборах чи референдумі, того, що ця система спроєктована відповідно до вимог щодо демократичних виборів і що вона працює належно, тобто робить те, що мала б робити.

106. Саме орган адміністрування виборів чи призначений ним суб'єкт повинні пересвідчитися в тому, що всі зазначені вимоги повною мірою відображають відповідні правові принципи демократичних виборів. Це означає, що вимоги оновлюються щоразу, як виникає потреба в тому, щоб внести до них можливі правові новели. Наприклад, організаційні норми щодо типу виборів можуть з часом змінюватися; і так само мають зміню-

6. Як, наприклад, у Швейцарії, де стандарти були впроваджені eCH – Асоціацією встановлення стандартів е-врядування. Подальші відомості про стандарти, пов'язані з е-голосуванням, доступні за посиланням www.ech.ch під рубрикою eCH Documents > nach Themenbereich > Politische Aktivitäten.

ватися й відповідні вимоги, що перекладають ці правила на мову технічних інструкцій до системи або до її сертифікації.

Стандарт № 37 «Перед запровадженням системи е-голосування та з належною періодичністю…»

107. Належний контроль за системою е-голосування забезпечує докази відповідності системи технічним вимогам, які, як вже згадувалося в попередньому положенні, є похідними від принципів демократичних виборів і спрямовані на їх реалізацію. Додаткова вартість такого контролю полягає не лише у визначенні того, чи система е-голосування відповідає встановленим вимогам і стандартам; це також важливий інструмент у встановленні довіри до системи е-голосування.

108. Орган адміністрування виборів повинен забезпечувати відповідність системи е-голосування технічним вимогам. Для цього він має уповноважити незалежний і компетентний орган на проведення оцінювання системи. Поняття незалежного органу охоплює незалежність як від виробника системи чи постачальника послуг, так і від політичного втручання.

109. Незалежний орган може бути урядовим, наприклад, відомством, уповноваженим здійснювати національну сертифікацію ІТ-захисту. Він може бути приватною (національною чи міжнародною) організацією, такою як лабораторією з оцінювання або органом сертифікації (наприклад тим, що акредитований проводити оцінювання за національними чи міжнародними схемами оцінювання, такими як BS7799/ISO17799, Загальні критерії (Common Criteria) або ITSEC). У будь-якому разі такий орган, окрім незалежності від виробника/сервіс-провайдера і від політичного втручання, повинен бути компетентним, щоб вести сертифікаційну діяльність. Навіть більше, його призначення (як органу сертифікації) має здійснюватися прозоро.

110. Сертифікація чи будь-який інший належний контроль здійснюється перед запровадженням системи е-голосування, а також через певні необхідні проміжки часу, а саме після важливих змін у системі. Сертифікація може проводитися різними способами. Держави-члени на власний розсуд можуть, наприклад, сертифікувати всю систему або лише її компоненти, враховуючи потребу в забезпеченні того, щоб система і процедури голосування були здатні реагувати на можливі загрози та ризики, а також відповідали стандартам демократичних виборів і референдумів.

Стандарт № 38 «Сертифікат чи будь-який інший відповідний виданий документ…»

111. Будь-який відповідний виданий документ має забезпечувати прозорість і відтворюваність процесу оцінювання для третіх осіб, особливо для тих, які мають доступ до системи. Повинна існувати можливість пересвідчуватися на основі сертифіката в тому, що система, яка використовується на виборах, є саме тою, яка була сертифікованою. Відповідно, сертифікат має містити (або посилатися на) принаймні таку інформацію:

- Суб'єкт, що видав сертифікат;
- Період/дата/умови проведення перевірки (наприклад, наявність угоди про нерозголошення);
- Опис призначення сертифіката. Чи заявлено в сертифікаті, що система є доступною, захищеною, придатною до використання, функціонує належно та якою мірою?;
- Опис методу, що застосовувався в процесі сертифікації. Які стандарти використовувалися? Які методи застосовувалися при перевірці та оцінюванні системи? Як аналізувався вихідний код? Як перевірялися апаратні компоненти?;
- Опис сертифікованої системи. Щоб забезпечити відтворюваність для третіх осіб, він повинен містити цифрові ідентифікаційні мітки компонентів програмного забезпечення, детальні характеристики версій апаратно-програмного забезпечення, компонентів апаратного забезпечення тощо;
- Результат процесу сертифікації;
- Зауваження щодо операційних вимог або інших передумов;
- Цифрову ідентифікаційну мітку сертифіката чи аналогічну систему.

Стандарт № 39 «Система е-голосування повинна забезпечувати можливість свого аудиту…»

112. Проведення аудиту процесу, ресурсів чи інфраструктури е-голосування є засобом встановлення довіри та впевненості в роботі ІКТ-систем(и), що використовується при е-голосуванні. Воно потребує цілісності та автентичності інформації аудиту та розгорнутих систем аудиту.

113. Метою аудитів є виявлення можливих атак на системи. Незалежний і всебічний моніторинг захисту, проведення аудиту, перехресні перевірки та звітність є критично важливими частинами систем е-голосування. Тому системи е-голосування повинні мати засоби аудиту для кожного з основних компонентів (голосування, підрахунку голосів тощо) і на різних рівнях системи: логічному, програмному, технічному.

114. Засоби аудиту на логічному рівні мають надавати звіти про використання системи. Засоби аудиту на рівні застосування мають надавати інформацію про діяльність, яку підтримує система, щоб надавати можливість реконструювати функціонування системи. Засоби аудиту на технічному рівні мають надавати інформацію про діяльність, яку підтримує інфраструктура, що використовується. Сюди входить інформація від поточних відомостей, наприклад, конкретної інформації про завантаження і несправності в системі, і до конкретної інформації про сигнали, що надходять від системи виявлення вторгнень (IDS) щодо можливих атак.

115. Контрольні журнали критично важливі для систем е-голосування, тому вони повинні бути якомога повними та відкритими для перевірки уповноваженими третіми особами. Перевірені дані мають надаватися в різних вузлах і на різних рівнях системи електронного голосування, наприклад, дані можуть перевірятися на рівнях EML, IT-системи або комунікаційної інфраструктури.

116. На рівні EML, наприклад, існує багато стандартизованих відкритих вузлів інтерфейсу. Потоки даних на цих вузлах інтерфейсу можна легко спостерігати та контролювати. Системи аудиту мають також охоплювати інтерфейси, що не використовують EML, наприклад, інтерфейси комунікаційної інфраструктури, баз даних і функцій управління системою.

117. Повинні існувати процедурні вимоги до використання систем аудиту під час проведення виборів або референдумів, а також заздалегідь визначені процедури для сценаріїв швидкого реагування.

118. Система аудиту має забезпечувати будь-якому спостерігачеві можливість здійснювати моніторинг у реальному часі перебіг виборів чи референдуму без розкриття можливих кінцевих підрахунків чи результатів. Наприклад, спостерігачі повинні мати можливість бачити в реальному часі загальну кількість поданих бюлетенів, щоб могли проводитися незалежні перехресні перевірки.

119. Система аудиту має бути здатною виявляти виборчі фальсифікації та надавати докази того, що всі підраховані голоси автентичні. Всі випадки спроб виборчих фальсифікацій повинні реєструватися в журналах; журнали системи аудиту повинні містити дані, що забезпечують можливість перехресної перевірки параметрів доступу, які дають право голосувати, а також гарантувати, що всі підраховані голоси були подані виборцями, які мають на це право, і що всі автентичні голоси були підраховані як такі.

120. Система аудиту має включати в себе всі дані виборів чи референдуму, потрібні посадовим особам органів адміністрування виборів, щоб здійснювати перехресну перевірку та облік усіх поданих бюлетенів, перевіряючи так належне функціонування системи голосування і легітимність результатів. Результати підрахунку виборчих бюлетенів повинні відповідати загальній кількості поданих голосів, включно з дійсними та недійсними голосами. Система аудиту має надавати інформацію, яка б сприяла незалежній перехресній перевірці та підтвердженню належного функціонування системи е-виборів чи е-референдуму і точності результатів. Система аудиту повинна забезпечувати, щоб жоден автентичний голос не був втрачений і щоб не було жодного непідрахованого голосу.

121. Перехресна перевірка даних незалежного аудиту збільшує ймовірність виявлення прихованих атак на системи е-голосування, оскільки атаки здійснюють приховано як на систему е-голосування, так і на дані незалежного аудиту.

122. Система аудиту повинна відповідати тим самим вимогам щодо захисту, які встановлені щодо запровадження самої системи е-голосування.

123. Система аудиту сама має бути захищена від атак, що мають на меті або здатні пошкодити, змінити чи знищити записи. Про виявлення будь-яких внутрішніх або зовнішніх атак на систему аудиту необхідно негайно повідомляти та вживати заходів.

НАДІЙНІСТЬ І ЗАХИЩЕНІСТЬ СИСТЕМИ

Стандарт № 40 «Орган адміністрування виборів повинен бути відповідальним за дотримання…»

124. На додаток до доступності та придатності до використання механізм е-голосування має бути надійним і захищеним, щоби відповідати принципам демократичних виборів. Гарантувати це зобов'язана держава-член. Загальна відповідальність покладається на орган адміністрування виборів, який здійснює нагляд за е-голосуванням, і не може бути делегована, наприклад, постачальникові системи голосування.

125. Дотримання принципів повинно також забезпечуватися у разі відмов чи атак. Це означає, що система е-голосування має бути захищеною, тобто стійкою щодо навмисних атак, і надійною, тобто здатною функціонувати самостійно, незалежно від відмов апаратного чи програмного забезпечення.

126. Технічні рішення, що відображають найновіші технології, пройшли експертне оцінювання і загалом схвалені відповідною науковою спільнотою, допомагають забезпечувати доступність, надійність, придатність до використання та захист системи е-голосування навіть у разі відмови та атак.

Стандарт № 41 «Тільки особам, уповноваженим органом адміністрування виборів…»

127. Будь-яке втручання в апаратне чи програмне забезпечення несе технічні і суб'єктивні ризики, які потрібно зводити до мінімуму під час експлуатації. Саме тому варто віддавати перевагу автоматичному управлінню та встановлювати обмеження на здійснення дистанційних маніпуляцій без офіційного нагляду. Якщо виникає потреба у втручанні, то ризики проникнення, суб'єктивних помилок, саботажу тощо потрібно мінімізувати, наскільки це можливо. Такі заходи варто реалізувати через встановлення робочого порядку, що підлягає дотриманню та підтвердженню, який обмежує кількість осіб, уповноважених виконувати роботу, до невеликої контрольованої групи та вимагає перевіряти кожну дію через фізичну присутність двох чи більше кваліфікованих осіб. Ці особи повинні дотримуватися правил безпеки, встановлених компетентним органом.

Стандарт № 42 «Перед будь-якими е-виборами орган адміністрування виборів…»

128. Перед проведенням будь-яких е-виборів орган адміністрування виборів повинен пересвідчитися, що використовувана система е-голосування –

це система, використання якої дійсно передбачається, тобто програмне забезпечення справжнє (тобто те, що попередньо перевірялося та було дозволене до використання) і працює належно.

129. Перевірка має запобігати встановленню будь-якої системи е-голосування, якщо система чи будь-який її компонент зазнав недозволеного втручання або заміни. Орган адміністрування виборів повинен гарантувати, що в експлуатацію введено належну систему. Крім того, цей стандарт вимагає належного функціонування системи.

Стандарт № 43 «Повинен бути визначений порядок періодичного…»

130. Постійний розвиток інформаційно-комунікаційних технологій викликає потребу в регулярних оновленнях, зокрема програмного забезпечення. Це означає потребу в оновленні центральних систем і засобів голосування, що використовуються у контрольованому середовищі (наприклад, машин для голосування). Усі важливі оновлення мають бути сертифіковані подібно до первинної сертифікації, яка проводилася перед введенням в експлуатацію.

131. Суттєво, щоб системи електронного голосування залишалися максимально прозорими, наскільки це можливо, для органів влади та громадян. Точні, повні, актуальні описи апаратних і програмних компонентів повинні бути опубліковані, надаючи можливість у такий спосіб зацікавленим групам самостійно пересвідчуватися в тому, що системи, які використовуються, відповідають тим, що були сертифіковані компетентними органами. Результати сертифікації мають бути доступними для органів влади, політичних партій і, залежно від нормативного регулювання, для громадян.

Стандарт № 44 «У разі зберігання чи передання поза межі контрольованого середовища…»

132. З моменту подання голосу ніхто не повинен мати можливості змінити його або пов'язати цей голос із виборцем, який його подав. Це досягається, окрім інших заходів, процесом запечатування виборчої скриньки, а якщо виборча скринька розташована дистанційно від виборця, запечатуванням голосу протягом його передання від виборця до виборчої скриньки, використовуючи шифрування. Голос вважається запечатаним, коли його зміст зазнав заходів, які гарантують неможливість його прочитання, зміну або пов'язування з виборцем, який його подав.

133. Для запечатування та захисту електронної виборчої скриньки можуть бути необхідними заходи фізичного та технічного характеру, такі як контроль доступу, механізми авторизації та брандмауери.

Стандарт № 45 «До початку процесу підрахунку голоси виборців та відомості про них повинні зберігатися в запечатаному вигляді»

134. Цей стандарт роз'яснює момент, коли завершується запечатування: безпосередньо перед початком підрахунку голосів. Як вже зазначалося

раніше (та за аналогією з фізичною виборчою скринькою), перед розпечатуванням голоси перемішують.

Стандарт № 46 «Орган адміністрування виборів повинен забезпечити захист при роботі…»

135. Цей стандарт нагадує, що для опрацювання криптографічних матеріалів потрібно передбачати наявність адекватних і сучасних процедур.

Стандарт № 47 «У разі виникнення інцидентів, що можуть загрожувати цілісності системи…»

136. Важливо негайно повідомляти про інциденти, що загрожують цілісності системи, відповідальному за комунікації компетентному суб'єкту, який має забезпечувати вжиття потрібних заходів та оперативне інформування всіх зацікавлених суб'єктів, тобто політичні партії та виборців.

Стандарт № 48 «Автентичність, доступність і цілісність реєстрів виборців…»

137. У повністю електронних процесах автентифікація джерел даних може забезпечуватися, наприклад, електронними підписами. У напів-електронних процесах автентифікація джерел даних також може застосовувати звичайні заходи безпеки, такі як власноручні підписи, печатки, кур'єри тощо.

138. У системі е-голосування може не вимагатися наявність реєстру виборців, якщо у двоетапній моделі застосовують маркер анонімного голосування, щоб встановити наявність права голосу. Варто зауважити, що реєстри виборців у приміщенні для голосування можуть бути потрібними, щоб запобігти багаторазовому голосуванню (в електронному вигляді та паперовими бюлетенями), або там, де голосування є обов'язковим. Отже, список тих, хто проголосував, є істотним.

Стандарт № 49 «Система е-голосування повинна ідентифікувати голоси…»

139. Порушення повинні бути ідентифіковані, щоб було вжито необхідних заходів та щоб зацікавлені сторони (виборці, орган адміністрування виборів) були поінформовані і могли реагувати у відповідний спосіб.

Керівні принципи[1]

імплементації положень Рекомендації CM/Rec(2017)5 Комітету Міністрів державам-членам щодо стандартів е-голосування

(Схвалено Комітетом Міністрів Ради Європи 14 квітня 2017 року на 1289-му засіданні заступників міністрів)

Спеціальний комітет експертів з питань правових, операційних і технічних стандартів е-голосування (CAHVE)

(Питання розглянуто Групою доповідачів з питань демократії (GR-DEM) на її засіданнях, що відбулися 20 квітня та 1 червня 2017 року)

ПРЕАМБУЛА

Комітет Міністрів, відповідно до положень статті 15.b Статуту Ради Європи,

Зважаючи на те, що метою Ради Європи є досягнення більшого єднання між її членами для збереження та втілення в життя ідеалів і принципів, які є їхнім спільним доробком;

Підтверджуючи свою впевненість у тому, що представницька і пряма демократія є частиною цього спільного доробку та основою для участі громадян в політичному житті на рівні Європейського Союзу, а також на загальнонаціональному, регіональному і місцевому рівнях;

З огляду на зобов'язання, узяті в рамках наявних правових актів і документів, серед яких:

- Загальна декларація прав людини;
- Міжнародний пакт про громадянські та політичні права;
- Конвенція ООН про ліквідацію всіх форм расової дискримінації;
- Конвенція ООН про ліквідацію всіх форм дискримінації щодо жінок;
- Конвенція ООН про права осіб з інвалідністю;
- Конвенція ООН проти корупції;

1. Оригінал тексту доступний на веб-сторінці за посиланням: www.coe.int/cm.

- Конвенція про захист прав людини та основоположних свобод (ETS № 5), зокрема, Протокол до неї (ETS № 9);
- Європейська хартія місцевого самоврядування (ETS № 122);
- Конвенція про кіберзлочинність (ETS № 185);
- Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS № 108);
- Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних (ETS № 181);
- Конвенція про стандарти демократичних виборів, виборчих прав і свобод у державах-учасницях Співдружності Незалежних Держав (CDL-EL(2006)031rev);
- Рекомендація R(99)5 Комітету Міністрів Ради Європи державам-членам щодо захисту недоторканності приватного життя в інтернеті;
- Рекомендація Rec(2004)15 Комітету Міністрів Ради Європи державам-членам щодо електронного врядування (е-врядування);
- Рекомендація CM/Rec(2009)1 Комітету Міністрів Ради Європи державам-членам щодо електронної демократії (е-демократії);
- Документ Копенгагенської наради Конференції ОБСЄ щодо людського виміру;
- Хартія основних прав Європейського Союзу;
- Кодекс належної практики у виборчих справах, ухвалений Радою з демократичних виборів Ради Європи та Європейською комісією за демократію через право (Венеційською комісією) і підтриманий Комітетом Міністрів, Парламентською Асамблеєю та Конгресом місцевих і регіональних влад Ради Європи;

Беручи до уваги, що право голосу належить до підвалин демократії і що, як наслідок, усі механізми голосування, зокрема е-голосування, повинні відповідати принципам демократичних виборів і референдумів;

Визнаючи, що використання державами-членами інформаційно-комунікаційних технологій під час виборів значно зросло останніми роками,

Зазначаючи, що деякі держави-члени вже використовують або розглядають можливість використання е-голосування з різними цілями, зокрема:

- надання виборцям можливості подавати свій голос з іншого місця, аніж приміщення для голосування на їх виборчих дільницях;
- сприяння поданню голосу виборцями;
- сприяння участі у виборах та референдумах громадян, що мають право голосу і проживають чи перебувають за кордоном;

- розширення доступу до процесу голосування виборцям з інвалідністю чи особам, для яких фізична присутність у приміщенні для голосування та користування доступними у ньому пристроями інакше ускладнені;

- підвищення рівня участі виборців через надання додаткових механізмів голосування;

- узгодження голосування із нововведеннями у суспільстві та активніше використання нових технологій як засобу комунікації, та залучення громадськості у реалізації демократії;

- поступове скорочення загальних витрат органів адміністрування виборів на проведення виборів чи референдумів;

- забезпечення надійнішого та швидшого отримання результатів голосування;

- забезпечення кращого обслуговування електорату через надання різноманітних механізмів голосування;

Високо оцінюючи досвід, накопичений державами-членами, що останніми роками використовували е-голосування, та уроки, здобуті з цього досвіду;

Усвідомлюючи також досвід, отриманий за результатами застосування Рекомендації Rec(2004)11 Комітету Міністрів Ради Європи державам-членам щодо правових, операційних і технічних стандартів е-голосування, Керівних принципів розроблення процесів, що засвідчують відповідність встановленим вимогам і стандартам (Сертифікація систем е-голосування), і Керівних принципів прозорості виборів із застосуванням електронних технологій;

Знову підтверджуючи свою переконаність у тому, що суспільна довіра до органів, відповідальних за організацію виборів, є передумовою для запровадження е-голосування;

Розуміючи стурбованість щодо потенційних проблем із захистом, надійністю та прозорістю систем е-голосування;

Усвідомлюючи, відповідно, що лише ті системи е-голосування, які є захищеними, надійними, ефективними, технічно стійкими, відкритими для незалежної перевірки та легкодоступними для виборців, здатні сформувати суспільну довіру, що є передумовою для проведення е-голосування;

Розуміючи потребу для держав-членів зважати на середовище, в якому запроваджується е-голосування;

Усвідомлюючи, що з огляду на останні технічні та правові нововведення, пов'язані з проведенням у державах-членах Ради Європи виборів із засто-

суванням електронних технологій, положення Рекомендації Rec(2004)11 потребують ретельного перегляду та оновлення;

З огляду на роботу Спеціального комітету експертів з питань правових, експлуатаційних і технічних стандартів е-голосування (CAHVE), створеного Комітетом Міністрів із завданням оновлення Рекомендації Rec(2004)11;

Приймає наведені нижче керівні принципи щодо стандартів е-голосування, які мають слугувати практичним інструментом для урядів держав-членів у схваленні, прийнятті, запровадженні та контролі підходу до е-голосування, описаного тут, та адаптації їхніх систем е-голосування;

Заохочує уряди держав-членів забезпечити широке розповсюдження цих керівних принципів серед органів адміністрування виборів, їх посадових осіб, громадян, політичних партій, національних і міжнародних спостерігачів, неурядових організацій (НУО), ЗМІ, науковців, постачальників рішень у галузі е-голосування та спеціальних органів, що здійснюють контроль за е-голосуванням.

ВСТУП

1. Ці керівні принципи є оновленою редакцією Керівних принципів розробки процесів, що засвідчують відповідність встановленим вимогам і стандартам (Сертифікація систем е-голосування) та Керівних принципів прозорості виборів із застосуванням електронних технологій. Первісні редакції обох документів з керівними принципами було схвалено 2011 року з метою надання вказівок щодо реалізації положень про сертифікацію і прозорість, що містилися в Рекомендації Rec(2004)11 Комітету Міністрів Ради Європи державам-членам щодо правових, операційних і технічних стандартів е-голосування від 30 вересня 2004 року.

2. Рекомендація Rec(2004)11 і первинні версії керівних принципів переглядалися та оновлювалися в 2015 і 2016 роках Спеціальним комітетом експертів з питань правових, операційних і технічних стандартів е-голосування (CAHVE), створеним Комітетом Міністрів 1 квітня 2015 року.

3. Ці керівні принципи надають вказівки щодо реалізації положень Рекомендації CM/Rec(2017)5. Кожен керівний принцип позначений номером, що відсилає до відповідного положення рекомендації.

4. Ця редакція керівних принципів не є остаточною і буде далі завершена, щоб стосуватися усіх форм е-голосування, охоплених Рекомендацією CM/Rec(2017)5. Відповідно, постійні новації у правовій і технічній сферах вимагатимуть регулярного оновлення положень цих керівних принципів.

5. Ці керівні принципи призначені для використання під час політичних виборів та референдумів на всіх рівнях управління. Вони не мають за мету бути не сукупністю суворих норм для держав-членів, нав'язуючи певний спосіб реалізації положень оновленої рекомендації, а радше спрямовані на надання державам-членам загальних настанов та підтримки в цій сфері.

6. Ці керівні принципи, як і оновлена рекомендація, не становлять вичерпних нормативних рамок для е-голосування. Державам-членам потрібно надалі розвивати ці положення, зважаючи на національну специфіку у сфері виборів. Ці керівні принципи також містять приклади ефективної імплементації стандартів у певних контекстах, тобто так звану «належну практику». Приклади належної практики наведено в інформаційних цілях.

I. Керівні принципи імплементації рекомендацій щодо загального виборчого права

1. Інтерфейс виборця в системі е-голосування є простим для розуміння та використання для усіх виборців.

- a. Виведення варіантів голосування на пристрій, що використовується виборцем, має бути оптимізоване для пересічного виборця, який не має спеціальних комп'ютерних знань.

  Продукти та послуги повинні бути пристосовними до функціональних обмежень і конкретних умов користувачів, не порушуючи такі принципи, як рівність. Це може досягатися шляхом пропонування різних версій того самого продукту, змін у ключових параметрах, модульну конструкцію, допоміжне обладнання чи інші методи.

- b. До проєктування систем е-голосування варто залучати виборців, зокрема, для того, щоб виявляти обмеження й тестувати зручність використання на кожному основному етапі в процесі розроблення.

  Доступність означає, що системи спроєктовані так, що ними може користуватися якомога більша кількість виборців. ІТ-продукти та сервіси повинні бути функціональними та враховувати потреби громадськості, не будучи надмірно ускладненими. Ці вимоги можуть бути задоволені через підхід, що передбачає співпрацю із включенням групи розробників і представницької групи користувачів.

- c. При розробці нових ІТ-продуктів, варто зважати на їхню сумісність з уже наявними.

2. Система е-голосування повинна бути розроблена в такий спосіб, щоб, наскільки це практично може бути реалізовано, забезпечувати особам з інвалідністю та з особливими потребами можливість голосувати самостійно.

- a. У кожному випадку, де це необхідно та можливо, виборців варто забезпечувати додатковими засобами, зокрема спеціальними інтерфейсами чи іншими аналогічними ресурсами, наприклад, особистою допомогою.

  Е-голосування може бути альтернативним способом голосування, що надає додаткові можливості голосувати самостійно особам з інвалід-

ністю та з особливими потребами. Варто знаходити прийнятний баланс між наданням таких можливостей доступу і дотриманням інших вимог, особливо щодо захищеності е-голосування.

- b. Інтерфейс голосування через інтернет має максимальною мірою відповідати керівним принципам, визначеним в Ініціативі веб-доступності (Web Accessibility Initiative – WAI).

  Консорціум WWW (World Wide Web Consortium – W3C) було створено 1994 року, щоб через розробку спільних протоколів уможливити розкриття Всесвітньою павутиною (World Wide Web – WWW) свого повного потенціалу. Він ініціював WAI з метою сприяння високому рівню доступності для осіб з інвалідністю. WAI спрямована на забезпечення веб-доступності за п'ятьма основними напрямами діяльності: технології, керівні принципи, інструменти, освітня та просвітницька діяльність, а також дослідження та розвиток. WAI розробила набір стандартів і керівних принципів на підтримку доступності (наприклад, керівні принципи доступності веб-контенту, інструменти створення контенту, керівні принципи щодо доступності, агента користувача, керівні принципи щодо доступності XML). Додаткова інформація доступна на сайті WAI за посиланням www.w3.org/WAI.

  WAI широко використовується у контексті браузерних рішень для інтернет-голосування. Навіть якщо в інтернет-голосуванні використовують альтернативні рішення (наприклад, коли застосунок для голосування – це сам по собі окремий унікальний «браузер»), існує можливість дотримуватися загальних принципів WAI.

II. Керівні принципи імплементації рекомендацій щодо рівного виборчого права

5. Вся офіційна інформація про голосування має надаватися однаково в рамках і через усі механізми голосування.

- a. Електронний виборчий бюлетень, що використовується для е-голосування, не має містити жодної інформації про опції голосування, крім встановленої законом.

  Інтерфейс е-голосування не має містити більше інформації про варіанти вибору, ніж офіційні (зазвичай паперові) виборчі бюлетені. Такі елементи, як спливаючі екрани, що підтримують конкретного кандидата чи позицію або звукові елементи, пов'язані з конкретним кандидатом чи точкою зору, а також будь-яка інша інформація, відсутня на паперовому виборчому бюлетені (рівність механізмів голосування), не повинні з'являтися на інтерфейсі е-голосування. Це не перешкоджає викладу офіційної інформації про опції голосування.

- b. Якщо інформація про опції голосування доступна на сайті е-голосування, вона має подаватися неупереджено.

  Інформація про опції голосування повинна подаватися у неупереджений спосіб у рамках усіх механізмів голосування.

9. Система е-голосування повинна забезпечувати, щоб кожен виборець міг подати лише належну кількість голосів, і щоб лише така кількість голосів кожного виборця зберігалася в електронній виборчій скриньці та була врахована у результатах виборів.

- a. Якщо виборцю дозволено подавати електронний голос декілька разів, повинні бути вжиті належні заходи, щоби забезпечувати врахування лише одного голосу.

- b. Якщо виборцю дозволено подавати голос через більше ніж один механізм голосування, повинні бути вжиті належні заходи, щоб забезпечувати врахування лише одного голосу.

Керівні принципи 9a та 9b: Якщо дозволене багаторазове голосування, це має бути також відображено в е-голосуванні. Наприклад, деякі системи голосування дозволяють виборцям подавати достроково голос один чи декілька разів і пізніше змінювати свою думку. Лише останній голос вноситься до виборчої скриньки, і, отже, є поданим голосом. Так прийнято в Андоррі, Данії та Швеції.

Варіант багаторазового голосування (подання декількох е-голосів або через декілька механізмів голосування) може запроваджуватися одночасно з е-голосуванням як захід протидії примусу виборців, який залишається можливим, якщо голосування відбувається поза контрольованим середовищем (дистанційне голосування). Так відбувається в Естонії.

Визначення того, який голос має враховуватися, має бути здійснене на національному рівні. У контексті е-голосування країна може вирішити, що пріоритет має паперовий виборчий бюлетень. В інших місцях враховується лише останній поданий голос. Третя країна може вирішити, що врахуванню підлягає перший голос, поданий належним чином. Щоб відповідати принципам демократичних виборів, система е-голосування (або одночасне використання паперового виборчого бюлетеня та методів е-голосування) повинна забезпечувати рівне право голосу. Національне законодавство визначає, який із поданих голосів враховується. Принцип «один виборець – один голос» має бути дотриманий.

Рішення про те, який саме голос враховується, залежить від національної політики щодо дистанційного голосування. Країни, які здійснюють більш сувору політику щодо дистанційного голосування, матимуть тенденцію до надання пріоритету паперовому виборчому бюлетеню, якщо це голос, поданий у приміщенні для голосування (у контрольованому середовищі). Країни, більш прихильні до дистанційного голосування, можуть вирішити, що врахуванню підлягає перший голос, поданий належним чином, і в цьому разі е-голос, поданий в неконтрольованому середовищі, може мати перевагу над голосом, що був поданий пізніше за допомогою паперового бюлетеня. Рішення про те, як загалом боротися з примусом виборців у разі дистанційного голосування, взагалі кажучи, має приймати національний законодавчий орган. Такі рішення не мають залишатися на розсуд самого

лише органу адміністрування е-голосування, оскільки вони стосуються політики щодо дистанційного голосування в цілому, а не лише запровадження е-голосування.

- с. У всіх інших випадках повинні бути вжиті належні заходи, щоб запобігти поданню виборцем більше ніж одного голосу.

У країнах, де багаторазове голосування не допускається, подання декількох голосів розглядається як спроба проголосувати більше, ніж дозволено окремому виборцю. Цей ризик може виникати, наприклад, коли виборець сам намагається проголосувати декілька разів або коли інша особа намагається скористатися ідентифікаційним документом виборця, щоб проголосувати від імені цього виборця після того, як він чи вона проголосували.

У контексті голосування за допомогою паперових бюлетенів цим ризикам протидіють за допомогою організаційних заходів. Наприклад, у Сполученому Королівстві, якщо особа прибула у приміщення для голосування, щоб проголосувати, і виявила, що хтось вже проголосував від його чи її імені, така особа має право подати окремий голос за допомогою спеціального виборчого бюлетеня. Цей бюлетень не опускається до виборчої скриньки, а запечатується у конверт і розглядається лише в разі оскарження дійсності виборів та відповідно до вказівок суду. Аналогічне положення застосовується у разі отримання двох голосів, поданих поштою від одного й того самого виборця. У контексті е-голосування повинні бути забезпечені належні заходи. Важливою є наявність захищеної ідентифікації. Одним зі таких заходів може бути збереження прив'язки ідентифікаційних кодів виборця до його чи її запечатаного бюлетеня протягом певного часу.

Запровадження дистанційного е-голосування породжує питання про те, як пов'язані між собою періоди часу, встановлені для голосування у приміщенні для голосування та для дистанційного е-голосування. На перший погляд, видається логічним, щоб для обох способів голосування були призначені ті самі періоди часу, щоб уникнути ускладнень і відмінностей. Однак причини, які можуть призводити до проведення такого голосування у різний час, включають такі:

- *якщо для виборців, що перебувають у межах країни, голосування у приміщенні для голосування є запасним варіантом у разі відмови системи е-голосування, час закінчення е-голосування треба встановити більш раннім відносно часу закриття приміщення для голосування;*
- *якщо система розроблена та експлуатується у такий спосіб, що виборці можуть обирати механізми голосування, але наявні механізми не забезпечують доступу до єдиного реєстру, в якому можна знайти імена виборців, які вже проголосували, то періоди доступності цих механізмів загалом не повинні перетинатися.*

У будь-якому разі підрахунок голосів повинен розпочинатися лише після закриття голосування за всіма механізмами.

▸ d. У всіх випадках виборці мають бути чітко поінформовані про можливості голосування, що пропонуються, і про правила підрахунку голосів.

Особливо важливо інформувати виборця про його чи її можливості голосування, включно з можливістю подавати більше одного е-голосу або голосувати більше ніж один раз послідовно за допомогою різних механізмів голосування, якщо багаторазове голосування дозволено.

У будь-якому разі, виборець має бути поінформований про чинні правила підрахунку голосів, зокрема щодо того, який його голос буде остаточно врахованим.

III. Керівні принципи імплементації рекомендацій щодо вільних виборів

10. Намір виборця проголосувати не повинен зазнавати впливу ані з боку системи голосування, ані будь-яким іншим неналежним чином.

▸ a. У разі дистанційного е-голосування виборець повинен бути поінформованим про засоби, якими можна пересвідчитися у встановленні підключення до офіційного сервера та в наданні автентичного виборчого бюлетеня.

У контексті дистанційного е-голосування варто врахувати такі можливі сценарії, як, серед іншого, створення фальшивих серверів, наприклад, таких, що імітують офіційний сервер через фальсифікації з допомогою системи доменних імен (DNS); використання доменного імені, подібного до доменного імені офіційного сервера; або пошкодження серверного коду (зокрема з використанням зловмисного програмного забезпечення). Виборці повинні отримувати інформацію про те, як перевірити сертифікат офіційного сайту е-голосування. Справжність бюлетеня дозволяють перевірити електронні підписи, проставлені органом адміністрування виборів на виборчому бюлетені. Це, однак, не має порушувати таємності голосування.

▸ b. Система е-голосування має не допускати здійснення будь-якого маніпулятивного впливу на виборця під час голосування. Зокрема, електронний виборчий бюлетень, за допомогою якого подається електронний голос, не повинен містити жодної неофіційної інформації.

Подібно до положення 5a, цей керівний принцип вимагає, щоб виборцю була надана лише офіційна інформація для голосування і щоб був виключений будь-який маніпулятивний вплив з боку неуповноважених сторін.

▸ c. Система е-голосування повинна запроваджувати всі можливі заходи, щоб уникнути вчинення будь-якого маніпулятивного впливу на голос після його подання, і це також включає заходи, які дозволять пересвідчуватися, що жоден такий вплив не здійснювався.

Поняття вільних виборів також захищає голос від будь-якого маніпулятивного впливу після того, як його було подано. Будь-який маніпулятивний

вплив на голос чи несанкціоноване втручання у його зміст мають бути виключені. Звичайно, багаторазове голосування, якщо воно дозволене, не впливає на це положення, і виборцю має бути дозволено голосувати декілька разів.

Це положення спрямоване на запобігання будь-яким несанкціонованим змінам у змісті голосу після того, як його було подано. Воно захищає від атак, що здійснюються ззовні системи, а також від внутрішніх загроз. Індивідуальна та загальна перевірюваність (див. стандарти № 15 і № 17) – це засоби контролю, покликані виявляти будь-яке несанкціоноване втручання такого роду.

▸ d. Якщо це вважається за потрібне, система е-голосування має пропонувати механізми (наприклад, багаторазове голосування) для захисту виборців від примусу голосувати певним чином.

Багаторазове голосування розглядається як механізм, що захищає виборця від осіб, які здійснюють примус, надаючи йому чи їй можливість переголосувати.

12. Спосіб, яким виборці повинні проходити через процес е-голосування, не може приводити до голосування ними раптово чи без отримання підтвердження.

▸ a. Виборці повинні мати можливість змінити свій вибір у будь-який момент під час дистанційного е-голосування, перш ніж подати свій голос, або перервати цю процедуру.

Це положення передбачає можливість припинення процедури голосування перед тим, як голос подано, тобто до його надходження до електронної виборчої скриньки. Після реєстрації голосу це стає неможливим. Тому інтерфейс повинен бути запрограмованим так, щоб привернути до цього увагу виборців, наприклад, пропонуючи їм підтвердити свій вибір перед поданням голосу. Було б корисно також нагадувати виборцям, що ця операція означатиме підтвердження голосу та його остаточне подання у разі, якщо багаторазове голосування не дозволене.

15. Виборець повинен мати можливість пересвідчитися в тому, що його чи її намір точно відображений у змісті поданого голосу та що запечатаний голос без змін надійшов до електронної виборчої скриньки. Будь-який протиправний вплив, який би модифікував зміст голосу, повинен піддаватися виявленню.

▸ a. У разі застосування машин для е-голосування у приміщеннях для голосування держави-члени повинні розглянути можливість використання паперових бюлетенів як другого носія для зберігання голосів з метою перевірки.

Відомий також під назвою «доступний для перевірки виборцями паперовий контрольний журнал» (voter-verified paper audit trail – VVPAT), цей метод покликаний забезпечувати вільні вибори там, де голоси подають

через машини для е-голосування в контрольованому середовищі. Якщо е-рішенням, що застосовується на виборчих дільницях, є сканер виборчих бюлетенів, то наявність другого носія не обов'язкова, оскільки виборчий бюлетень у цьому разі паперовий за визначенням.

Інші рішення, що передбачають наявність другого носія, можуть бути пов'язані, наприклад, з використанням відривних частин бюлетеня (як модель scantegrity[2] Д. Чома), що допускає можливість індивідуальної перевірки. Вони можуть бути дуже подібними до VVPAT чи мати іншу форму. Їх треба виготовляти з паперу, який є одночасно незмінюваним та таким, що може розпізнаватися і перевірятися людиною.

Критерії дійсності (достовірності) цього другого носія мають встановлюватися національним регулюванням, яке також має встановлювати, що саме робити у разі розбіжностей між електронними результатами та тими, що отримані з використанням другого носія.

- b. Потрібно проводити обов'язковий підрахунок голосів, поданих на другому носії, на статистично значущій кількості випадково обраних виборчих дільниць, зокрема, при використанні машин для е-голосування та оптичних сканерів.

Такі критерії, як відсоток голосів або кількість виборчих дільниць, де відбувається такий підрахунок, їхнє призначення тощо мають встановлюватися на національному рівні. Вони мають забезпечувати досягнення загальної мети – проведення вільних виборів.

IV. Керівні принципи імплементації рекомендацій щодо таємності голосування

19. Е-голосування повинно бути організованим у такий спосіб, щоб забезпечувати дотримання таємності голосування на всіх етапах процедури голосування.

- a. Дані реєстру виборців повинні бути чітко відокремлені від компонентів голосування.

Це положення особливо повинно застосовуватися тоді, коли у приміщеннях для голосування, крім машин для е-голосування чи сканерів для голосування, для ідентифікації виборців використовуються біометричні методи. Відокремлення двох компонентів забезпечує таємність голосування.

Якщо голоси та знеособлені дані виборців зберігаються разом, цю інформацію потрібно захищати наскрізним шифруванням.

2. Під такою назвою відомий один із засобів посилення безпеки та достовірності систем голосування з оптичним скануванням, розроблений Д. Чомом (David Chaum) та Р. Рівестом (Ron Rivest). – *Прим. ред.*

21. Система е-голосування та будь-який уповноважений суб'єкт повинні захищати дані автентифікації так, щоб неуповноважені суб'єкти не мали можливості зловживати використанням, перехоплювати, змінювати чи іншим способом отримувати відомості про ці дані.

- a. Автентифікація повинна використовувати криптографічні механізми.

  Це положення потребує використання новітніх технічних рішень для захисту даних автентифікації.

23. Система е-голосування не повинна надавати виборцю підтвердження змісту поданого голосу для використання третіми особами.

- a. Якщо виборцю видається паперове підтвердження змісту електронного голосу в контрольованому середовищі, виборцю не має бути дозволено показувати його будь-якій іншій особі або виносити таке підтвердження за межі приміщення для голосування.

  Е-голосування не повинно надавати виборцеві підтвердження змісту поданого голосу. Якщо це запрограмовано на певному етапі процедури голосування, як, наприклад, при використанні машин для е-голосування на виборчих дільницях, повинні існувати організаційні заходи, які б запобігали будь-якому використанню цього підтвердження для порушення таємності голосування. Метою є захист таємності голосування та запобігання практики продажу голосів. Звичайно, це не може повністю утримати виборця від розголошення змісту свого голосу, наприклад, через його фотографування. Національне кримінальне та адміністративне законодавство, яке також поширюється на е-голосування, повинно передбачати покарання за такі порушення таємності голосування.

- b. Після подання голосу на екран не повинна виводитися жодна залишкова інформація, пов'язана з рішенням виборця.

  Поняття «залишкова інформація» означає інформацію, що залишається доступною в різних місцях (у пам'яті персонального комп'ютера, кеші браузера, відеопам'яті, файли підкачки, тимчасових файлах і т. ін.) після подання голосу і можуть розкривати рішення виборця.

  Це положення рекомендує розробникам систем або постачальникам послуг проєктувати системи е-голосування у такий спосіб, щоб залишкова інформація знищувалася після подання голосу. З технічного погляду, засоби забезпечення цього в дистанційному середовищі голосування можуть виявитися обмеженими. Однак варто вживати всіх можливих заходів, щоб знищувати таку залишкову інформацію після подання голосу. Проте можна реалізувати індивідуальну перевірюваність за умови наявності достатніх запобіжних заходів, що унеможливлюють примус або купівлю голосів.

- c. У випадку дистанційного е-голосування виборець має бути поінформований перед голосуванням про можливі ризики для таємності голосування та рекомендовані засоби їхнього зменшення.

▸ d. У випадку дистанційного е-голосування виборець має бути поінформований про те, як знищити, де це можливо, сліди від поданого голосу на пристрої, з якого здійснювалося голосування.

Керівні принципи 23c і 23d: у разі дистанційного е-голосування виборець має бути ясно поінформований про ризик порушення таємності голосування та про заходи й належну практику, які потрібно застосовувати задля врахування цього ризику, використовуючи, наприклад, брандмауери, знищення слідів тощо. Сама система повинна автоматично знищувати якомога більше таких слідів.

Е-голосування з дистанційного, неконтрольованого середовища передбачає поділ обов'язків між виборцем і системою е-голосування/органом адміністрування виборів. До обов'язків виборця входить вжиття рекомендованих заходів (зазначених у цьому положенні). Обов'язком органу адміністрування виборів є чітке інформування виборця щодо принаймні трьох моментів: про принцип поділу обов'язків; про різні заходи, яких має вжити виборець задля зменшення ризиків (встановлення на комп'ютері антивірусного програмного забезпечення, брандмауера, знищення слідів голосування тощо); про решту ризиків і техніки перевірюваності.

Ця інформація повинна досягти виборця заздалегідь до періоду голосування. Виходячи з цього, виборець має можливість вирішити, використовувати дистанційне е-голосування чи ні.

Попереджувальні повідомлення можуть з'являтися на початку процедури е-голосування; повідомлення про рекомендовані дії, до яких виборець має вдатися після голосування (зокрема, знищення слідів), може бути необхідним надати виборцю наприкінці процедури е-голосування. Проте такі повідомлення є лише нагадуваннями і не замінюють собою початкову повну інформацію, яку виборець має отримати до настання періоду е-голосування.

26. Процес е-голосування, особливо етап підрахунку голосів, повинен бути організованим у такий спосіб, щоб унеможливити відстеження зв'язку між розпечатаним голосом і виборцем. Подані голоси є та залишаються анонімними.

▸ a. Відомості про виборця мають бути відокремленими від зробленого ним рішення на заздалегідь визначеному етапі процесу підрахунку голосів.

▸ b. Будь-яке декодування, необхідне для підрахунку голосів, повинно бути здійснене якнайшвидше, наскільки це можливо, після завершення часу голосування.

Термін «відомості про виборця» означає знеособлену інформацію про виборця, таку як ідентифікаційні коди, що використовуються у дистанційному е-голосуванні. Хоча прив'язка такої інформації до запечатаного голосу повинна певний час зберігатися під відповідним захистом, щоб, серед іншого, уможливити багаторазове голосування з дотриманням

принципу «одна людина – один голос», ця прив'язка має бути ліквідована до початку підрахунку голосів.

Шифрування голосів, взагалі кажучи, має бути необхідним для забезпечення анонімності голосування. У багатьох випадках голос шифрується ще до початку передачі через комп'ютерні мережі. Він зберігається в зашифрованому стані у виборчій скриньці та розкодовується перед підрахунком голосів. Підрахунок проводиться з декодованими голосами, які неможливо прив'язати до конкретних виборців.

Однак існують методи шифрування, що не потребують декодування перед підрахунком голосів (гомоморфне шифрування). У цьому випадку підрахунок може проводитися без розкриття змісту защифрованих голосів. У деяких випадках задля забезпечення анонімності може навіть виникати потреба в проведенні підрахунку, поки голоси перебувають у зашифрованому стані.

- c. Держави-члени повинні вжити необхідних заходів, щоб гарантувати конфіденційність будь-якої інформації, отриманої будь-яким суб'єктом під час виконання аудиторських функцій.

Окрім захисту інформації, зібраної системою аудиту, від несанкціонованого доступу, повинні бути вжиті правові та організаційні заходи із перевірки осіб, які мають санкціонований доступ до системи аудиту. Такі заходи, наприклад, можуть бути включені до процесу акредитації.

V. Керівні принципи імплементації нормативних та організаційних рекомендацій

27. Держави-члени, які запроваджують е-голосування, повинні здійснювати це поетапно та поступово.

- a. Перед добором і впровадженням будь-якої технології е-голосування варто здійснити та опублікувати офіційне обґрунтування доцільності. Воно повинно включати підстави для прийняття цієї системи, аналіз ризиків, оцінку нормативної бази, план пілотної експлуатації та оцінювання її результатів, а також аналіз затрат-користі.
- b. Будь-яке пілотне застосування системи е-голосування має починатися задовго до виборів і передбачати всі необхідні підготовчі заходи, такі як прийняття, у разі потреби, детального регулювання пілотного застосування та тестування системи.
- c. Остаточна версія системи е-голосування повинна пройти випробування перед її використанням у регулярних, зобов'язальних виборах.
- d. Пілотне застосування має бути проведене на основі чітких і вичерпних критеріїв оцінки ефективності та цілісності системи е-голосування включно з переданням результатів.

28. Перш ніж запроваджувати е-голосування, держави-члени повинні внести необхідні зміни до відповідного законодавства.

- a. Нормативна база має включати регулювання процедур імплементації е-голосування від налагодження та функціонування до підрахунку голосів.

  Докладні приписи мають, можливо, міститися в підзаконних актах та інструкціях. Це має бути передбачено законодавством вищого рівня, яке повинно також визначити чіткі повноваження щодо прийняття такого деталізованого регулювання.

- b. Нормативна база повинна містити правила визначення дійсності е-голосу.

- c. Нормативна база має містити норми, що стосуються проблем, відмов і розбіжностей, які виникають внаслідок використання інструментів верифікації.

  Якщо держави-члени використовують другий носій для зберігання голосу та проводиться їх обов'язковий підрахунок, то між результатами голосування можуть виникати розбіжності. У таких випадках норми мають чітко визначати, який саме голос (електронний чи на альтернативному носії) має перевагу. Аргументом на користь електронного голосування є те, що виборці подали свої голоси цим способом. Міркуванням на користь другого носія є те, що цей голос міг бути перевірений самим виборцем, особливо якщо розглядуваний носій передбачає паперову фіксацію.

  Отже, у разі будь-якої розбіжності відповідний випадок має бути ретельно вивчений, а будь-яке рішення щодо результату врахування такого голосу має залежати від результатів розгляду. Державам-членам пропонується встановити норми, що визначали б, який саме голос використовується в офіційному підрахунку, коли та за яких умов перерахунок вважається необхідним, коли і як проводиться обов'язковий підрахунок, за яких обставин підраховують усі другі голоси й коли мають проводитися повторні вибори.

- d. Нормативна база повинна містити регулювання процедур процесу знищення даних, особливо задля узгодження обробки, зберігання і знищення даних (та обладнання) в технології голосування із законодавством про захист персональних даних.

  Носій інформації, що містить голоси (жорсткий диск, карти пам'яті тощо), має знищуватися.

- e. Нормативна база має містити положення щодо вітчизняних і міжнародних спостерігачів.

  Держави-члени повинні передбачати роль вітчизняних і міжнародних спостерігачів у процесі е-голосування та регулювати це відповідно до міжнародних зобов'язань і належної практики. Тип доступу до е-голосування, наданого спостерігачам, має залежати від положень національного законодавства. Ці положення мають відображати міжнародні

зобов'язання, зокрема ті, що стосуються Бюро з демократичних інститутів і прав людини Організації з безпеки та співробітництва в Європі (ОБСЄ/БДІПЛ). Спостерігачі мають всключати представників політичних партій і широкої громадськості.

- f. Законодавство має передбачати чіткий часовий графік проведення всіх етапів е-виборів.

  Е-вибори можуть відрізнятися від виборів або референдуму в аспекті процедур, яких повинні дотримуватися виборці. Прикладами можливих відмінностей є період часу, протягом якого можуть бути подані голоси, кроки, які має здійснити виборець, щоб узяти участь в е-виборах, та спосіб, у який фактично відбувається е-голосування. Ці відмінності варто чітко доводити до відома виборців для того, щоб уникнути будь-якого неправильного розуміння процедур і щоб надати виборцю всю інформацію, потрібну для того, щоб він міг зробити обґрунтоване рішення щодо того, який механізм голосування використати. Особливу увагу потрібно приділяти тому, скільки часу потрібно виборцю для такого рішення.

- g. Період часу, протягом якого може бути поданий електронний голос, не може починатися оголошенням про проведення виборів або референдуму.

  Доведення до відома виборців інформації про період часу, встановлений для голосування, особливо важливе тоді, коли період часу е-голосування відрізняється від часу, встановленого для інших механізмів голосування. Ця різниця виникає особливо у разі дистанційного е-голосування, де для голосування з використанням електронних механізмів може бути потрібний інший період часу внаслідок специфіки цих механізмів.

- h. Дистанційне е-голосування може розпочинатися та/або завершуватися раніше, ніж відкриється будь-яка виборча дільниця.

- i. Період часу, протягом якого може бути поданий електронний голос, не повинен продовжуватися після завершення періоду голосування.

  Керівні принципи 28h і 28i: З різних причин проміжок часу дистанційного е-голосування може бути тривалішим, аніж проміжок часу, протягом якого відкриті виборчі дільниці. Ці причини включають забезпечення кращого обслуговування громадян і підвищення доступності.

  Проте дистанційне е-голосування не повинно продовжуватися після завершення періоду голосування на виборчих дільницях. У разі недоступності системи е-голосування (наприклад, якщо персональний комп'ютер виборця не працює через порушення енергопостачання), виборець, який проживає або перебуває в країні, де проходять вибори чи референдум, все ще повинен мати можливість прибути до приміщення для голосування на виборчій дільниці, щоб проголосувати. Якщо е-голосування продовжуватиметься після закриття виборчих дільниць, у виборця не буде такої можливості.

- j. Надходження електронних голосів до електронних виборчих скриньок має бути дозволене протягом достатнього часу після завершення

періоду е-голосування, щоб допустити будь-які затримки з проходженням повідомлень через механізм дистанційного е-голосування.

- k. Після завершення періоду е-голосування жодному виборцю не може бути надано доступу до системи е-голосування.

Керівні принципи 28j і 28k: Ці положення стосуються сеансів інтернет-голосування, що починаються незадовго до закриття механізму е-голосування. Виборча скринька має залишатися відкритою, щоби могти зібрати ці голоси. Тривалість має бути аналогічною до звичайної тривалості сеансу е-голосування, щоб надати можливість тим виборцям, які здійснюють доступ до системи за декілька секунд до її закриття, нормально завершити процес е-голосування.

Інша ситуація, знову ж таки в умовах інтернет-голосування, пов'язана зі зростанням попиту на послуги, який може виникати протягом короткого періоду, що безпосередньо передує завершенню голосування. Це може призвести до затримок із надходженням голосів до електронної виборчої скриньки. Своєчасно надіслані голоси не треба відкидати через такі затримки. Опрацювання голосів не має зупинятися негайн після закриття сервісу е-голосування. Однак початок сесії е-голосування після того, як систему закрито, повинен бути неможливим.

29. Відповідне законодавство повинно регулювати відповідальність за функціонування систем е-голосування і забезпечувати контроль за ними з боку органу адміністрування виборів.

- a. Процеси закупівель для е-голосування мають проходити прозоро.

- b. Мають бути встановлені норми, які б запобігали конфліктам інтересів приватних зацікавлених сторін, залучених до цього процесу.

- c. Необхідно підтримувати та документально оформлювати чіткий поділ повноважень.

- d. Держави-члени повинні вжити належних заходів для уникнення ситуацій, коли вибори протиправно залежать від постачальників.

30. Кожен спостерігач повинен мати можливість спостерігати за підрахунком голосів. Відповідальність за процес підрахунку голосів покладається на орган адміністрування виборів.

- a. Обов'язковим є ведення протоколу процесу підрахунку електронних голосів, який би містив, зокрема й відомості про початок і завершення підрахунку та про осіб, які його проводили.

- b. Має бути забезпечена відтворюваність підрахунку голосів. Повинна існувати можливість отримання надійних доказів того, що процедуру підрахунку було здійснено задовільно, зокрема через незалежний повторний підрахунок.

Мета тут полягає в тому, що має існувати можливість отримання надійних доказів правильного виконання процедури підрахунку. Одним зі способів реалізувати це є незалежний повторний підрахунок голосів, якщо він здійснюється з використанням іншої системи з іншого джерела. Однак цього можна досягти іншими засобами, наприклад, використовуючи криптографічні докази (загальна перевірюваність).

- c. Можливість перевірки також має бути забезпечена для інших характеристик, які можуть впливати на точність результатів системи е-голосування.

Залежно від використовуваної системи, можуть існувати інші складові, окрім повторного підрахунку, що позначаються на точності результату. Прикладом може бути підтвердження того, що всі подані голоси були підраховані.

Окрім інструментів верифікації, потрібно розглядати можливість використання даних про відсоток голосів, поданих електронно, та про порівняння результатів е-голосування з результатами голосування за допомогою інших механізмів, щоб визначити правдоподібність результатів е-голосування та підтвердити їхню точність.

- d. Система е-голосування повинна зберігати доступність і цілісність електронної виборчої скриньки та результатів процесу підрахунку голосів стільки, скільки це потрібно.

Інформація, що зберігається в електронній виборчій скриньці, повинна бути захищеною доти, доки це необхідно з огляду на можливість повторного підрахунку, подання правового оскарження або інших правових вимог, що існують у відповідній державі-члені.

VI. Керівні принципи імплементації рекомендацій щодо прозорості та спостереження

31. Держави-члени зобов'язані забезпечувати прозорість усіх аспектів е-голосування.

- a. Компетентні органи адміністрування виборів повинні опублікувати офіційний перелік програмного забезпечення, що використовується під час е-виборів. У цьому переліку варто зазначати принаймні назву, версію, дату інсталяції та короткий опис програмного забезпечення, що використовується.

Постійний розвиток інформаційно-комунікаційних технологій потребує частих оновлень апаратного та програмного забезпечення і його регулярної адаптації до центральних систем і засобів голосування, використовуваних у контрольованому середовищі (наприклад, машин для голосування). Для того, щоб е-голосування залишалося прозорим, потрібно публікувати точні, повні, актуальні описи апаратних і програмних компонентів, дозволяючи таким способом зацікавленим групам самостійно пересвідчуватися в тому, що використовувані системи відповідають тим, які були сертифіковані компетентними органами. Результати сертифікації мають бути доступними для органів влади,

політичних партій і, залежно від чинного правового регулювання, для громадян.

- b. Публічний доступ до компонентів системи е-голосування та інформації, що у них міститься, зокрема документації, вихідних кодів та угод про нерозголошення, мають бути відкритими для зацікавлених сторін та широкої громадськості задовго до початку виборчого процесу.

Коли електронний пристрій чи система надає зобов'язальні результати, технічні подробиці щодо того, що і як підраховувати, легко можуть стати настільки ж важливі, як і виборче законодавство, котре визначає правила підрахунку на виборчих дільницях. Для забезпечення суспільної довіри через прозорість вихідні коди, конфігурація, а також перелік усіх апаратних і програмних компонентів системи е-голосування мають бути частиною результатів аудиту. Протоколи перевірених процесів, таких як процедури установки та налаштування, підтвердження того, що сертифікований вихідний код є тим, що використовується під час виборів, і процес підрахунку електронних виборчих бюлетенів також мають бути частиною результатів аудиту. Це повинно допомогти державам-членам у наданні відповідної документації виборцям і третім особам, включно з національними й міжнародними спостерігачами та ЗМІ.

Вираз «задовго» означає, що національними нормативними актами мають бути встановлені чіткі строки для такого розкриття і що планові кінцеві терміни дозволяють зацікавленим сторонам реалізувати свої права, реагувати на таке розкриття і подавати запити щодо внесення змін. Орган адміністрування виборів повинен мати час і можливість реагувати на такі відгуки, зокрема через оновлення системи. Публікація такої інформації за дванадцять місяців до голосування задовольнятиме критерію «задовго». Для оперативних змін можуть бути необхідними коротші строки. Проте основні елементи повинні бути відкритими задовго до виборів, а не безпосередньо перед ними.

- c. Розгортання технологій електронного голосування має передбачати розробку всеохопних, детальних, покрокових рекомендацій включно з посібником з процедури.

32. Задовго до початку голосування громадськість, зокрема, виборці повинні бути поінформовані чіткою і простою мовою про:
- будь-які дії, які мав би вчинити виборець, щоб узяти участь у виборах і проголосувати;
- належне використання і функціонування системи е-голосування;
- часовий графік е-голосування включно з усіма його етапами.

- a. Виборцям мають бути доступними допоміжні та інструктивні матеріали щодо процедур голосування.

Допоміжні та інструктивні матеріали щодо процедур голосування повинні бути наявними незалежно від конкретного використовуваного механізму. Для кожного використовуваного каналу електронного

голосування така інформація має бути доступна принаймні на тому самому каналі електронного голосування. Інакше кажучи, якщо каналом е-голосування є інтернет, то має бути доступним принаймні сайт з довідковою інформацією та засобами електронної пошти, а якщо можливе голосування телефоном, то має бути доступною телефонна гаряча лінія.

- b. У разі дистанційного е-голосування інформаційні матеріали для виборців повинні також бути доступними через інший загальнодоступний канал зв'язку.

  Інформація про дистанційне е-голосування має бути доступною також на резервному, іншому, загальнодоступному каналі зв'язку для ситуацій, коли канал дистанційного е-голосування виходить із ладу. Наприклад, для інтернет-голосування таким альтернативним каналом зв'язку може бути телефонна гаряча лінія.

- c. Виборцям має бути надана можливість попрактикуватися до моменту подання електронного голосу та відокремлено від його подання. У такому разі увага учасників цих дій має бути чітко привернута до того, що вони не беруть участі в реальних виборах або референдумі.

  Традиційні механізми голосування вже добре відпрацьовані в державах-членах, і виборці знайомі з загальними нормами, що їх регулюють. Запровадження е-голосування породжує труднощі для виборця. Такі системи та спосіб їхньої роботи не так легко зрозуміти. Щоб забезпечити розуміння та довіру з боку виборця, потрібно вжити заходів з ознайомлення виборців із системою. Такі заходи можуть вимагати застосування протягом тривалого часу.

  Для того, щоб зміцнити розуміння та довіру до будь-якої (нової) системи е-голосування, можливості попрактикуватися в її використанні потрібно надавати до моменту подання електронного голосу та відокремлено від його подання (наприклад, через демонстраційні системи або пробні вибори). Особливу увагу потрібно приділити категоріям виборців, у яких скоріше за все виникатимуть значні труднощі (наприклад, особам похилого віку), та їхнім особливим потребам.

33. Складові системи е-голосування повинні бути відкритими для цілей верифікації та сертифікації.

- a. Системи е-голосування мають генерувати надійні й достатньо докладні дані спостережень, щоб уможливити спостереження за виборами. Має існувати можливість надійно визначати момент, коли подія згенерувала дані спостереження. Повинна забезпечуватися автентичність, доступність і цілісність цих даних.

- b. Національні та міжнародні спостерігачі повинні мати доступ до всієї відповідної документації щодо процесів е-голосування.

  Доступ до документації, включно з протоколами, сертифікацією, звітами про випробування та аудити, а також докладною документацією,

що роз'яснює функціонування системи, має важливе значення для національних і міжнародних спостерігачів. Такі спостерігачі включають представників політичних партій і широкої громадськості. Їх потрібно запрошувати на відповідні засідання. Де це можливо, держави-члени, постачальник або сертифікаційний орган повинні надавати інформацію всім зацікавленим сторонам, наприклад, розміщуючи відповідні документи в інтернеті задовго до початку виборчого процесу.

Держави-члени повинні розробити порядок, який би визначав, хто, до чого й коли має доступ. Такий порядок потрібно розробити як для національних і міжнародних спостерігачів, так і для ЗМІ. Потрібно також встановити порядок доступу для інших зацікавлених сторін, зокрема громадян, політичних партій і НУО. Центральною ідеєю зазначених порядків має бути відкритий доступ.

Держави-члени повинні чітко викладати ці вимоги до потенційних постачальників, які також мають розуміти, що зацікавленим сторонам, особливо національним і міжнародним спостерігачам, потрібен доступ до певної документації під час проведення тендерів. Угоди про нерозголошення, що не дозволяють спостерігачам публікувати оцінки та факти, на яких ґрунтуються ці оцінки, позбавляють всіх зацікавлених сторін і, що найважливіше, спостерігачів важливої інформації.

- c. Держави-члени повинні надавати спостерігачам доступ до відповідної документації, наскільки це можливо, мовою, якою часто користуються в міжнародних відносинах.

Відповідна інформація, що потрібна національним і міжнародним спостерігачам для того, щоб задовільно виконувати свою роботу, має бути доступною державною мовою (чи мовами) відповідної країни. Таку інформацію, наскільки це можливо, варто також забезпечувати однією з офіційних мов Ради Європи (англійською та французькою). Зокрема, доступ до документації, виконаної однією з цих мов, потрібен міжнародним спостерігачам.

- d. Держави-члени повинні надавати програми підготовки для груп національних і міжнародних спостерігачів.

Системи е-голосування нелегкі для розуміння особам, які не є експертами з е-голосування. Щоб поліпшити розуміння зацікавленими сторонами системи, що використовується, потрібні тренінги, зокрема, для національних, але також і для міжнародних спостерігачів. Такі тренінги мають надавати базові та прості інструменти для використання в роботі спостерігачів, зокрема й способи перевірки запечатування, читання роздруку машин для голосування та файлу аудиту.

- e. Національні та міжнародні спостерігачі, а також ЗМІ повинні мати можливість спостерігати за тестуванням програмного та апаратного забезпечення.

Зацікавлені сторони, зокрема й групи акредитованих спостерігачів, повинні мати не лише доступ до документів, а й можливість спостерігати за перевіркою пристроїв і систем е-голосування. Спостереження за таким тестуванням та/або аудитом не має перешкоджати виборчому процесу. Тому такий моніторинг має здійснюватися тільки під керівництвом осіб, відповідальних за організацію виборів. Як вже зазначалося, такі спостерігачі повинні включати представників політичних партій і широкої громадськості. Навіть більше, особи, що спостерігають за тестуванням та/або аудитом, повинні заздалегідь пройти тренінги. Процес має бути достатньо відкритим, щоб дозволяти спостерігачам отримувати повне уявлення про роботу системи.

- f. Спостерігачі на виборах повинні мати доступ до всіх етапів процесу оцінювання та сертифікації.

Останні двадцять років спостереження за виборами засвідчило, що воно є успішним методом забезпечення прозорості виборів та доступу до них. З появою електронного голосування виникає потреба в оновленні усталених методик спостереження за виборами. Для того, щоб спостерігачі були спроможними спостерігати за сертифікацією систем електронного голосування, тривалість місій зі спостереження за виборами повинна бути збільшена. Вирішальне значення має те, щоб жодна з процедур, необхідних для сертифікації е-голосування, не проходила за закритими дверима, оскільки це викликатиме підозри.

Спостерігачам, зокрема й представникам політичних партій і широкої громадськості, має бути наданий доступ до будь-якої відповідної інформації протягом усього процесу сертифікації, щоб вони могли виконувати свої обов'язки. Спостерігачі, зі свого боку, повинні розкривати методологію, яку вони збираються застосовувати.

VII. Керівні принципи імплементації рекомендацій щодо звітності

36. Держави-члени повинні розробити технічні, оцінювальні та сертифікаційні вимоги й бути переконаними в тому, що вони повністю відображають відповідні правові та демократичні принципи. Держави-члени повинні підтримувати ці вимоги в актуальному стані.

- a. Держави-члени повинні встановити цілі та методи сертифікації.

При розгляді питання про сертифікацію систем місцевого чи дистанційного е-голосування перший крок полягає у чіткому визначенні цілей сертифікації та вимог до процедури сертифікації. При розробці цих вимог важливо пересвідчитися в тому, що вони відповідають національному законодавству та міжнародним стандартам, включно з будь-якими процедурами оскарження, пов'язаними з проведенням виборів. Хоча докладний перелік вимог спочатку може здаватися надійним способом гарантувати належний сертифікаційний аналіз, строгі нормативні рамки можуть викликати парадоксальні ефекти. Наприклад, аудиторів піддаватимуть детальному нагляду, однак постачальники можуть мати можливість адаптувати свою продукцію до обмеженої мети – просто задовольнити вимоги, встановлені конкретною виборчою адміністрацією. За цих обставин постачальники можуть не оптимі-

зувати продукцію, а виборча адміністрація буде зобов'язана відповідно до власних правових норм прийняти недостатньо оптимальну продукцію. Уникнути цієї пастки повинно допомогти використання договорів, у яких критерієм відбору переможця є якість, а не ціна.

Визначення цілей і вимог у плані програмного забезпечення, операційної системи, апаратного забезпечення та процесу е-голосування, а також обсягу та методів сприятиме ефективності процесу сертифікації, зручності режиму сертифікації та загальній прозорості систем е-голосування.

Сертифікація систем е-голосування не обмежується первинною сертифікацією; вона також включає процедури десертифікації та повторної сертифікації програмного забезпечення, операційних систем, апаратного забезпечення та процесів.

Соціально-політичні чинники можуть зумовлювати ступінь довіри громадян і становити серйозну проблему. Оскільки ці чинники також здатні позначатися на процесах сертифікації; держави-члени повинні заохочувати наукові дослідження в цій галузі, включно з міжнародним обміном відповідною інформацією.

Мають бути встановлені рамки, які б гарантували, що всі сторони обізнані про систему і добре її розуміють. Робота має проводитися з дотриманням встановлених методик, як підтверджувальне тестування, тестування компонентів, тестування продуктивності та функціональне тестування.

37. Перед запровадженням системи е-голосування та з належною періодичністю після її запровадження, зокрема, після внесення до системи будь-яких істотних змін, повинна бути здійснена оцінка незалежним і компетентним органом щодо відповідності технічним вимогам системи е-голосування і будь-яких її компонентів, що використовують інформаційно-комунікаційні технології (ІКТ). Це може набувати форми офіційної сертифікації або іншого належного контролю.

▸ а. Держави-члени повинні визначити розподіл коштів, потрібних для процесу сертифікації. Вони повинні визначити відповідальність, зокрема фінансову, сертифікаційного органу за якість його роботи.

Будь-хто, хто уповноважений брати участь у сертифікації системи е-голосування, зокрема й сертифікатори, оцінювачі та аудитори, повинен бути незалежним та кваліфікованим. Тому критерії, способи та компетентні установи, залучені до вибору органів сертифікації, повинні бути чітко визначені національним законодавством. Держави-члени відповідальні за розробку норм і керівних принципів процесів відбору.

Ці процедури мають бути відомі та оприлюднені задовго до дня виборів. Це полегшить завдання постачальників і посилить довіру виборців до процедур. Кількість органів сертифікації не повинна обмежуватися;

кожен, хто є незалежним та кваліфікованим, повинен бути уповноваженим проводити сертифікацію. Перевагу варто віддавати використанню європейського відкритого тендеру або проведенню консультацій із групою потенційних сертифікаторів, щоб визначити кваліфікованих сертифікаторів.

Держави-члени мають розглянути можливість здійснення процедури добору міжнародними сертифікованими професійними аудиторами. Наприклад, CISA (Сертифіковані аудитори інформаційних систем) є стандартом досягнень для тих, хто здійснює аудит, контроль, моніторинг та оцінювання інформаційних технологій і бізнес-систем організації. Потрібно приділити увагу вартості таких процедур. Іншим важливим чинником є те, що використання міжнародних сертифікатів не має ставати перешкодою для використання державами-членами конкретної системи е-голосування чи навіть унеможливлювати використання країнами конкретної надійної системи е-голосування.

Держави-члени повинні від самого початку ясно визначати, які органи відповідальні за витрати, пов'язані з процедурою сертифікації. Вони можуть вирішувати, що всі витрати, включно з вартістю офіційної сертифікації, несуть постачальники, що може привести до більшої залученості останніх. Витрати можуть також покладатися на відповідні держави-члени, а третім варіантом є розподіл витрат. Витрати на сертифікацію за жодних обставин не мають робити предметом компромісу незалежність, цілісність і якість процесу сертифікації. Незалежно від обраного варіанту, держави-члени повинні мати достатнє фінансування, а рішення варто оприлюднювати.

- b. Органи оцінки і сертифікації повинні мати повний доступ до всієї відповідної інформації та мати достатньо часу на здійснення процесу сертифікації до початку виборів.

Органи сертифікації повинні мати доступ до інформації та даних, які є необхідними і достатніми для виконання ними своїх обов'язків, а саме, дійти висновку про систему голосування, яка розглядається; ці органи повинні мати достатньо часу, щоб проаналізувати всі відомості та дані.

Громадяни мають право знати, яку інформацію не було визнано необхідною і достатньою для проведення сертифікації. Крім того, норми, що регулюють відносини між постачальником і сертифікатором, наприклад, угоди про нерозголошення (УПН) чи інші аналогічні документи провинні бути опублікованими.

У деяких випадках, як дострокові вибори чи запровадження нової системи голосування, процеси сертифікації можуть відбуватися лише незадовго до початку виборів. Це має наслідком ризик браку часу на проведення ретельної процедури сертифікації, а це, у свою чергу, може підірвати довіру до виборів. Тому процедура сертифікації повинна бути завершена задовго до виборів, забезпечуючи достатній час на розгляд висновків.

Одним із рішень, яке дозволяє зекономити час і гроші, є сертифікація лише змінених модулів і встановлення послідовності модулів для майбутньої сертифікації відразу після завершення первинного процесу сертифікації

та після того, як був сертифікований компонент е-голосування. Це можна зробити лише тоді, коли визначено відмінність між значними змінами (модифікаціями) та незначними змінами в системі е-голосування.

- с. Повноваження органів оцінки і сертифікації повинні бути регулярно підтверджуваними через встановлені проміжки часу.

Держави-члени повинні розробити порядок проведення не лише процедури первинного відбору, але й подальших процедур, таких як повторні перевірка та підтвердження повноважень чи позбавлення повноважень. Повноваження, надані будь-якому органу сертифікації на сертифікування системи е-голосування, повинні бути надані лише на обмежений строк. Тендери потрібно проводити з регулярною періодичністю, і ці тендери мають бути відкритими. Має бути чітко визначено, чи рішення про те, щоб довірити сертифікацію системи конкретному вибраному органу сертифікації, може бути прийняте постачальником, чи таке рішення належить до компетенції органу адміністрування виборів.

- d. Висновки, наведені у звіті про сертифікацію, мають бути цілком зрозумілими з урахуванням інформації, що міститься в цьому звіті.

Звіт про сертифікацію має бути таким, що не потребує пояснень, тобто його висновки мають спиратися лише на інформацію, що міститься в ньому, дозволяючи третій стороні повторити ці дослідження і тим самим підтвердити, що висновки звіту про сертифікацію є дійсні.

- е. Держави-члени повинні встановити та опублікувати чіткі правила щодо розкриття остаточного звіту про сертифікацію та всіх відповідних документів, враховуючи важливість прозорості.

Держави-члени мають розробити та опублікувати порядок, яким визначається, хто, коли й до якої інформації має доступ. Особливу увагу потрібно приділити потребам національних і міжнародних спостерігачів та ЗМІ. Також мають бути визначені процедури для інших зацікавлених суб'єктів, таких як громадяни, політичні партії, НУО та, не в останню чергу, посадові особи органів адміністрування виборів. Ці процедурні норми важливі для того, щоб зміцнити довіру громадян до захищеності та надійності систем е-голосування та наглядову функцію органів адміністрування виборів. Можливість нерозголошення звіту про сертифікацію повністю або частково, чи всіх відповідних документів має розглядатися лише за виняткових обставин.

Особливу увагу потрібно приділити компонентам програмного забезпечення, важливим для безпеки системи. Цього можна досягти, включивши тестування безпеки до планів випробувань, щоб читач звіту розумів, як перевірялася безпека. Також можна розглядати можливість маркування всіх документів державами-членами та постачальниками.

Постачальники і навіть сертифікатори можуть не погоджуватися з публікацією деякого чи значного обсягу документації на систему е-голосування, оскільки бажають захистити права інтелектуальної

власності. Відповідно, щоб уникнути надмірної секретності під час процесів сертифікації, до відома потенційних постачальників і сертифікаторів потрібно довести під час тендерної процедури, що зацікавлені суб'єкти повинні отримати доступ до конкретної документації. Угоди про нерозголошення, що перешкоджають спостерігачам публікувати оцінки та факти, на яких ґрунтуються ці оцінки, дуже ускладнюють ведення повноцінного спостереження.

Нарешті, щоб здійснювати нагляд за процесом сертифікації або компенсувати будь-яке часткове та неповне розкриття інформації для громадськості, держави-члени можуть засновувати спеціальні комітети у складі експертів, науковців та/або політиків. Наприклад, у Бельгії колегія експертів відповідальна за нагляд над усім виборчим процесом від імені повноважного законодавчого органу.

39. Система е-голосування повинна забезпечувати можливість свого аудиту. Система аудиту має бути відкритою і всеосяжною та оперативно сповіщати про можливі проблеми й загрози.

- a. Система аудиту має реєструвати час, події та дії, зокрема:
  - будь-яку інформацію, пов'язану з голосуванням, зокрема й кількість повноважних виборців, кількість поданих голосів, кількість дійсних і недійсних голосів, підрахунок і повторний підрахунок тощо;
  - будь-які атаки на функціонування системи е-голосування та її комунікаційну інфраструктуру;
  - системні відмови, несправності та інші загрози системі.

Автоматизовані інструменти та системні процедури мають забезпечувати швидкий і точний аналіз даних та звітування про них, створюючи таким способом можливість швидких коригувальних дій. Система аудиту має забезпечувати доступні для перевірки звіти про:

- *повторну перевірку даних;*
- *атаки на системи чи мережі;*
- *виявлення вторгнень і повідомлення про них;*
- *маніпуляції даними;*
- *фальсифікації та спроби фальсифікацій.*

Система аудиту повинна зберігати записи про всі атаки на функціонування системи виборів чи референдуму або на її комунікаційну інфраструктуру. Система обов'язково має містити функцію виявлення та звітування про спроби зламу, вторгнення чи маніпулювання. Виявлені атаки на систему голосування мають реєструватися, про них має негайно повідомлятися та до них мають негайно вживатися заходи.

Система аудиту має реєструвати всі підрахунки та повторні підрахунки, зокрема й усі прийняті рішення, вчинені дії чи винятки, допущені в процесі підрахунку голосів.

- b. Система е-голосування має містити надійні синхронізовані джерела часу. Точність джерела часу має бути достатньою для того, щоб забезпечувати мітки часу для звітів аудиту і даних спостережень, а також для забезпечення строків реєстрації, висування, голосування або підрахунку.

  Можуть існувати різні вимоги щодо точності для різних користувачів джерела часу, зокрема різні допустимі відхилення, встановлені для події реєстрації та подання голосу. Тому можуть використовуватися кілька джерел часу або одне джерело часу, що забезпечує найвищу точність. Термін «мітка часу» використовується як вказівка того, що дані позначено. Залежно від ситуації, існує декілька доступних засобів: для критичних подій можуть знадобитися захищені мітки часу, водночас для записів у журналі достатніми можуть виявитися безперервна послідовність номерів або збереження такої послідовності. Зауважимо, що наявність міток часу на поданих голосах може нести загрозу таємності голосування. Тому потрібний ретельний розгляд питання про те, як і чи варто використовувати такі мітки для бюлетенів або поданих голосів.

- c. Висновки, отримані в процесі аудиту, повинні бути взяті до уваги під час майбутніх е-виборів.

VIII. Керівні принципи імплементації рекомендацій щодо надійності та захисту

40. Орган адміністрування виборів повинен бути відповідальним за дотримання всіх вимог і відповідність цим вимогам навіть у разі відмов і атак. Орган адміністрування виборів повинен бути відповідальним за доступність, надійність, придатність до використання і безпеку системи е-голосування.

- a. Доступність сервісів е-голосування для всіх виборців має забезпечуватися протягом усього процесу е-голосування.

  Система е-голосування має бути захищена від неполадок і аварій. Однак можливість аварії неможливо виключити повністю. Повинні бути передбачені процедури та альтернативні рішення для екстрених випадків.

- b. Виборці повинні бути невідкладно поінформованими належними засобами про переривання, припинення чи перезавантаження системи е-голосування.

- c. Система голосування не повинна позбавляти повноважних виборців можливості подати свій голос.

- d. Система е-голосування повинна забезпечувати доступність і цілісність голосів.

З моменту, коли голос подано, ніхто не повинен мати можливості який його подав. Це досягається процесом запечатування виборчої скриньки, а якщо виборча скринька розташована на дистанції від виборця, – запечатуванням голосу протягом усьому його передання від виборця до виборчої скриньки. За деяких обставин запечатування повинно бути здійснене шляхом шифрування.

Щоб запечатати будь-яку виборчу скриньку, потрібні заходи фізичного та організаційного характеру. Вони можуть передбачати фізичне замикання скриньки та забезпечення її охорони більш ніж однією особою. У разі електронної виборчої скриньки потрібні додаткові заходи, такі як контроль доступу, механізми авторизації та брандмауери.

Голос є запечатаним, коли його зміст зазнав заходів, які гарантують неможливість його прочитання, зміну або співвідношення з виборцем, який його подав.

Показники доступності та частоти відмов зазвичай встановлюються в угодах про рівень сервісу (SLA). Певний рівень деградації сервісу може бути прийнятним протягом періодів відмов, наприклад, у разі пошкодження сервера в кластері. Під час процесів реєстрації можуть навіть допускатися короткочасні періоди збоїв у сервісі або періоди технічного обслуговування.

Розробники систем, однак, враховують можливість відмови внаслідок атак на сервіси та повинні зазначати в документації особливий резерв діяльності системи, призначений для цього. Незалежне тестування на проникнення може зменшити ймовірність успіху навмисних спроб викликати збої сервісів.

Сервіси, захищені в доступі, залежать від етапу: перед, під час чи після голосування. На етапі перед голосуванням мають бути доступні процеси та сервіси номінації й реєстрації кандидатів; на етапі голосування – процеси та сервіси голосування; а на етапі після голосування – процеси та сервіси підрахунку й звітності. Процеси аудиту мають бути доступними на всіх етапах. Проте попередньо визначені обмеження для угод про рівень сервісу, допустима частота відмов або зниження продуктивності сервісів можуть відрізнятися для окремих етапів чи сервісів.

- e. Повинні бути вжиті технічні й організаційні заходи, щоб унеможливити необоротну втрату даних внаслідок аварії чи несправності в системі е-голосування.

- f. Держави-члени повинні брати до уваги практичність використання у процесі розроблення механізмів захисту.

Керівні принципи 40e і 40f: Це не означає, що має бути використано кожен доступний метод захисту. У кожному окремому випадку необхідно робити вибір щодо природи й обсягу заходів захисту, що мають бути застосованими. Потрібно досягти належного балансу між різними однаково важливими чинниками, наприклад, між загальною важливою потребою забезпечення захисту та прагненням мати системи, котрими легко користуватися виборцям. У цьому випадку легкість у користуванні не заперечує потреби у високому рівні захисту, але може бути чинником

при визначенні того, які заходи безпеки мають бути вжитими. Подібні міркування можуть бути застосовані, якщо дуже незначні додаткові переваги в плані захисту досягаються надмірно високою ціною щодо легкості в користуванні.

- g. Повинні проводитися регулярні перевірки, щоб забезпечити функціонування компонентів системи е-голосування відповідно до технічних характеристик системи та доступності її сервісів.

- h. Ключове обладнання для е-голосування повинно бути розміщене в захищеному приміщенні, і це приміщення повинно протягом усього виборчого процесу чи процесу референдуму перебувати під охороною від усіх спроб несанкціонованого втручання або доступу.

- i. Протягом виборчого процесу чи процесу референдуму має діяти аварійний план відновлення.

Керівні принципи 40h і 40i: Для забезпечення своєї безпеки центральні системи мають бути встановлені в захищених, контрольованих місцях. Фізичний доступ має бути контрольованим та обмеженим. Повинно бути підготоване також альтернативне місце розташування, щоб існувала можливість реагувати на фізичні аварії, заздалегідь створивши резерв відповідного обладнання (планування відновлення в аварійній ситуації).

Органи адміністрування виборів повинні визначити конкретний рівень сервісу перед запуском системи. Виходячи з бажаного рівня сервісу, має бути здійснений аналіз ризиків і визначені можливі сценарії. Це передбачає встановлення порядку дій, механізмів дублювання, резервування ресурсів тощо.

- j. Повинна існувати можливість у будь-який момент перевіряти стан захисту обладнання для голосування. Суб'єкти, відповідальні за обладнання, мають використовувати спеціальні процедури моніторингу, щоб забезпечувати протягом періоду голосування відповідність обладна-ння для голосування та його використання встановленим вимогам.

- k. Мають бути в наявності та постійно доступними достатні механізми резервування, щоб забезпечувати безперебійність процесу голосування. Будь-яка резервна система має відповідати тим самим стандартам і вимогам, що й основна система.

- l. Відповідний персонал має бути готовий до швидкого втручання згідно з процедурою, розробленою компетентними органами адміністрування виборів.

i. Особи, відповідальні за функціонування обладнання, мають розробити порядок дій у надзвичайних ситуаціях.

ii. Усі технічні операції мають бути підпорядковані офіційній процедурі контролю. Про будь-які істотні зміни в ключовому обладнанні повинно бути повідомлено.

Керівні принципи 40j, 40k і 40l: Система електронного голосування потребує формалізованих процедур моніторингу своєї захищеності й надійності та вирішення проблем, а також достатніх ресурсів для усунення несправностей в інфраструктурі.

Органи адміністрування виборів повинні бути обізнані з усіма критичними змінами, внесеними до системи, щоб передбачати всі наслідки та обрати відповідну політику повідомлення про такі зміни.

- m. Усі дані, що залишилися після виборчого процесу чи процесу референдуму, повинні надійно зберігатися.

Всі дані про вибори або референдум, що підлягають збереженню, повинні зберігатися надійно. Це означає, що потрібно зберігати декілька копій даних на різних типах носіїв інформації (жорсткий диск, магнітні стрічки, оптичні носії, такі як DVD або мікрофіші, USB-накопичувачі та роздруки), і вони повинні зберігатися в різних місцях.

41. Тільки особам, уповноваженим органом адміністрування виборів, повинен надаватися доступ до центральної інфраструктури, серверів і даних про вибори. Призначення на посаду осіб, уповноважених працювати у сфері забезпечення е-голосування, повинно бути чітко регламентованим.

- a. Призначені особи повинні мати обмежений доступ до сервісів е-голосування залежно від свого ідентифікатора користувача чи своєї ролі користувача. Автентифікація користувача має бути здійснена, перш ніж може бути виконана будь-яка дія. Розподіл обов'язків має бути чітким і суворо забезпечуватися технічними заходами.
- b. Коли електронна виборча скринька відкрита, будь-яке санкціоноване втручання, що впливає на систему, повинно здійснюватися групами принаймні з двох осіб, підлягати звітуванню, спостерігатися представниками органу адміністрування виборів та будь-якими спостерігачами за виборами.
- c. Уся інша критична технічна діяльність має вестися групами в складі щонайменше двох осіб. Склад груп повинен регулярно змінюватися. Наскільки можливо, така діяльність повинна здійснюватися поза періодом виборчого процесу. Ця діяльність має підлягати звітуванню.

42. Перед будь-якими е-виборами орган адміністрування виборів повинен пересвідчитися, що система е-голосування справжня і функціонує належно.

- a. Перед кожними виборами обладнання має перевірятися та затверджуватися згідно з протоколом, розробленим компетентними органами

адміністрування виборів. Обладнання повинно перевірятися, щоб забезпечити його відповідність технічним характеристикам. Результати мають бути подані до компетентних органів адміністрування виборів.

Варто проводити чітку відмінність між регулярними перевірками після кожних виборів чи референдуму і перевірками, що здійснюються щоразу після модифікації системи у будь-якому відношенні. У першому випадку перевірку можуть виконувати працівники суб'єкта, що забезпечує роботу системи виборів чи референдуму. Однак у другому випадку перевірку має здійснювати зовнішній орган, оскільки така перевірка ближча до процедури сертифікації.

43. Повинен бути визначений порядок періодичного встановлення оновлених версій і виправлень усього відповідного програмного забезпечення.

- a. Мають бути розроблені офіційні процедури розгортання програмного забезпечення та конфігурації технологій голосування. Повинні бути встановлені крайні строки для оновлень. Розповсюджувані оновлення мають бути автентифіковані (підписані).

46. Орган адміністрування виборів повинен забезпечити захист при роботі з усіма криптографічними матеріалами.

- a. Приватні криптографічні ключі повинні генеруватися на відкритому засіданні та мають бути поділені на окремі частини, що видаються принаймні двом особам, які навряд чи вступлять у змову.

47. У разі виникнення інцидентів, що можуть загрожувати цілісності системи, відповідальні за експлуатацію обладнання особи повинні негайно сповістити про це орган адміністрування виборів.

- a. Типи інцидентів повинні бути заздалегідь визначеними органом адміністрування виборів.
- b. У разі інциденту компетентний орган адміністрування виборів повинен вжити необхідних заходів для усунення наслідків інциденту.

48. Автентичність, доступність і цілісність реєстрів виборців і списків кандидатів повинна бути забезпечена. Автентичність джерел даних має підтверджуватися. Положення про захист даних повинні бути дотримані.

- a. Друкування ідентифікаційних даних виборців, таких як картки виборців, повинно здійснюватися під наглядом для забезпечення захищеності чутливих даних.

49. Система е-голосування повинна ідентифікувати голоси, що зазнали впливу порушень.

▸ а. Повинна існувати можливість пересвідчитися в тому, що голос був поданий у межах встановленого проміжку часу.

У контексті інтернет-голосування вираз «у межах встановленого проміжку часу» стосується терміну закриття інтернет-каналу голосування. Це може бути реалізовано за допомогою міток часу або надійним підтвердженням, наданим системою. Мітка часу, яку додають до голосу, не повинна, однак, використовуватися для розкриття голосу.

ДОДАТОК

ВИЗНАЧЕННЯ

Наведені в цих керівних принципах терміни використовуються у таких значеннях:

- контроль доступу – запобігання несанкціонованому використанню ресурсу;
- оцінювання – здійснення оцінки осіб, апаратного забезпечення, програмного забезпечення та процедур з метою перевірити їхню придатність до виконання певних завдань;
- аудит – незалежне передвиборче чи післявиборче оцінювання особи, організації, системи, процесу, суб'єкта, проєкту чи продукту, яке включає кількісний та якісний аналіз;
- автентифікація – забезпечення достовірності заявленої ідентичності особи чи даних;
- доступність – стан, що дозволяє доступ і використання на вимогу;
- бюлетень – юридично визнаний засіб, яким виборець може виразити свій голос;
- кандидат – опція голосування, що складається з однієї особи, групи осіб та/або політичної партії;
- подання голосу – внесення голосу до виборчої скриньки;
- сертифікат – документ, що є результатом офіційної сертифікації, якою засвідчується чи підтверджується певний факт;
- сертифікація – процес підтвердження того, що система е-голосування відповідає встановленим вимогам і стандартам і що вона містить, щонайменше, засоби, які дозволяють пересвідчитися в належному функціонуванні системи. Це може здійснюватися різними заходами – від тестування та аудиту і до офіційної сертифікації. Кінцевим результатом є звіт та/або сертифікат;
- орган сертифікації (або сертифікатор) – організація, уповноважена здійснювати процес сертифікації та видавати сертифікат після завершення процесу;

- звіт про сертифікацію – документ, який роз'яснює, що саме засвідчує сертифікат і як саме проведена сертифікація;
- ланцюжок довіри – процес у комп'ютерній безпеці, що здійснюється шляхом валідації кожного компонента апаратного та програмного забезпечення знизу вгору. Він покликаний забезпечити використання лише надійного програмного та апаратного забезпечення, водночас зберігаючи гнучкість;
- компонентне тестування – метод тестування окремих блоків коду системи для визначення їх придатності до використання;
- конфіденційність – стан, що характеризує інформацію, до якої не повинен надаватися доступ або яка не може бути розголошена неуповноваженим особам, суб'єктам чи процесам;
- контрольоване середовище – приміщення, що перебувають під наглядом посадових осіб органів адміністрування виборів, наприклад, приміщення для голосування, посольства чи консульства;
- е-вибори – політичні вибори чи референдум, на яких використовується е-голосування;
- орган адміністрування виборів – інституція, уповноважена на організацію підготовки і проведення виборів у конкретній країні на загальнонаціональному чи нижчому рівні;
- електронна виборча скринька – електронні засоби, за допомогою яких зберігаються голоси в очікуванні їх підрахунку;
- е-голос – голос, поданий в електронному вигляді;
- е-голосування – використання електронних засобів для подання та/або підрахунку голосів;
- система е-голосування – апаратне, програмне забезпечення та процеси, що надають можливість виборцям голосувати за допомогою електронних засобів на виборах або референдумі;
- офіційна сертифікація – сертифікація, що здійснюються офіційними органами тільки до дня виборів і результатом якої є видання сертифіката;
- керівні принципи – будь-який документ, покликаний скеровувати певні процеси згідно зі встановленою методикою. За визначенням, керівні принципи не є юридично зобов'язальними;
- угода про нерозголошення (УПН) – юридична угода між двома чи більше сторонами, що окреслює конфіденційні матеріали, знання чи інформацію, якими сторони бажають обмінюватися з певними цілями, але прагнуть обмежити до них доступ для третіх сторін;
- відкритий доступ – доступ онлайн до матеріалів, читання яких вільне для всіх та які можуть вільно використовуватися (чи повторно використовуватися) всіма у певних межах;

- профіль захисту – незалежний від реалізації набір вимог до захищеності певної категорії продуктів, який відповідає конкретним безпековим потребам споживачів;
- вимога – окрема документально оформлена потреба щодо того, якими повинні бути конкретний продукт чи сервіс або як вони повинні функціонувати;
- дистанційне е-голосування – використання електронних засобів для подання голосу поза межами приміщення, в якому в загальному випадку відбувається голосування;
- запечатування – захист інформації у такий спосіб, що вона не може бути використана або інтерпретована без допомоги іншої інформації чи засобів, доступних лише певним особам чи органам, зокрема й за допомогою шифрування;
- зацікавлений суб'єкт – особа, група, організація чи система, які чинять вплив або можуть зазнавати впливу через дії уряду чи організації. Це поняття охоплює громадян, посадових осіб органів адміністрування виборів, політичні партії, уряди, національних і міжнародних спостерігачів, ЗМІ, науковців, міжнародні та внутрішні НУО, організації-опонентів е-голосування, та спеціальні органи сертифікації е-голосування;
- стандарт (правовий) – стосується положень, що містяться в Додатку I до Рекомендації CM/Rec(2017)5;
- стандарт (технічний) – встановлена норма, зазвичай, у формі офіційного документа, що встановлює єдині інженерні чи технічні критерії, методи, процеси та практику;
- тестування – процес перевірки того, що система працює так, як очікувалося;
- голос – вираження вибору опції голосування;
- виборець – особа, що має право голосувати на певних виборах чи референдумі;
- механізм голосування – спосіб, яким виборець може подати свій голос;
- опції голосування – перелік варіантів, з-поміж яких можна здійснити вибір шляхом подання голосу на виборах чи референдумі;
- реєстр виборців – список осіб, що мають право голосу (виборців).

Декларація Decl(13/02/2019)1[1]

Комітету Міністрів Ради Європи щодо маніпулятивних можливостей алгоритмічних процесів

(ухвалена Комітетом Міністрів Ради Європи на 1337-му засіданні заступників міністрів 13 лютого 2019 року)

1. Держави-члени Ради Європи зобов'язалися розбудовувати суспільства, що ґрунтуються на цінностях демократії, прав людини та верховенства права. Це зобов'язання існує і повинно дотримуватися упродовж нинішнього процесу суспільної трансформації, який підживлюється технологічним прогресом. Держави-члени повинні забезпечити права та свободи, закріплені в Конвенції про захист прав людини і основоположних свобод (ETS № 5), кожному, хто перебуває під їхньою юрисдикцією, однаково в реальних відносинах та онлайн, в умовах безпрецедентної політичної, економічної та культурної глобалізації і пов'язаності.

2. Цифрові послуги використовуються сьогодні як важливий інструмент сучасної комунікації, зокрема й для політичної комунікації між урядами та між публічними інституціями і громадянами. Навіть більше, ці послуги стають основними для щораз більшої кількості користувачів у контексті споживання новин, освіти, розваг, комерційних операцій та багатьох інших форм повсякденної діяльності. Така ситуація має наслідком безпрецедентні обсяги нових даних, які безперервно продукуються із великою швидкістю та в чимраз більших масштабах.

3. Передові технології відіграють ключову роль у підтримці ефективності та цінності громадських послуг через цифрові технології, у зміцненні індивідуальної автономії та самовизначення, а також у підвищенні рівня людського розквіту через формування оптимальних умов для здійснення прав людини. У цьому контексті важливо вказати Рекомендацію CM/Rec(2007)16 Комітету Міністрів державам-членам щодо заходів із метою пропагування цінності Інтернету для надання суспільних послуг; Рекомендацію CM/Rec(2014)6 Комітету Міністрів державам-членам щодо Посібника з прав людини для інтернет-користувачів; а також Рекомендацію CM/Rec(2018)2 Комітету Міністрів державам-членам про ролі та обов'язки інтернет-посередників.

1. Оригінал тексту доступний на веб-сторінці за посиланням: www.coe.int/cm.

4. Рівень присутності технологій у нашому повсякденному житті постійно зростає, що спонукає користувачів надавати доступ до своїх відповідних, зокрема персональних, даних добровільно з отриманням відносно невеликої особистої зручності. Проте обізнаність суспільства залишається обмеженою щодо обсягу величезної кількості даних, щоденно збираних та генерованих різними пристроями. Ці дані використовують для підготовки технологій машинного навчання з метою визначення пріоритетності результатів пошуку, прогнозування та формування особистих уподобань, зміни інформаційних потоків, а іноді для проведення над індивідами поведінкових експериментів.

5. Тривалі дискусії щодо застосування та посилення законів про захист даних повинні зважати на особливі ризики й інтереси тих осіб, які особливо не обізнані про небезпеки використання даних. До таких осіб належать діти, а також особи, які належать до маргіналізованих груп, які можуть зіштовхнутися з мовними бар'єрами або іншими структурними перешкодами. До таких осіб також можуть належати ті, хто через їхній особливо великий цифровий слід особливо зазнають нових форм впливу спостереження, заснованого на таких даних.

6. Щораз більше обчислювальні засоби надають можливість виводити інтимну та детальну інформацію про індивідів із легкодоступних даних. Це сприяє сортуванню індивідів за категоріями, тим самим підсилюючи різні форми соціальної, культурної, релігійної, правової та економічної сегрегації та дискримінації. Це також полегшує мікротаргетування індивідів на основі їхніх профілів способами, які можуть глибоко вплинути на життя цих людей.

7. Навіть більше, технології та системи, засновані на обробці даних, розроблено для неперервного досягнення оптимальних рішень за певними заданими параметрами, визначеними їх розробниками. При широкому застосуванні такі процеси оптимізації неминуче надаватимуть пріоритет певним цінностям перед іншими, формуючи таким способом контексти та середовища, у яких індивіди, як користувачі, так і некористувачі, оброблятимуть інформацію і прийматимуть свої рішення. Такі зміни в конфігурації середовищ можуть приносити вигоду для одних індивідів і груп та водночас бути згубними для інших, що породжує серйозні питання щодо отриманих результатів поділу. Вплив цілеспрямованого використання узагальнених даних, обсяги яких невпинно зростають, на реалізацію прав людини в широкому розумінні виходить далеко за межі сучасних уявлень про захист персональних даних та приватного життя, залишається недостатньо вивченим та потребує серйозного розгляду.

8. Сучасні інструменти машинного навчання мають щораз вищу спроможність не тільки передбачати вибір, а й впливати на емоції та думки і змінювати очікуваний перебіг дій, іноді підсвідомо. Небезпека для демократичних суспільств, яка випливає з можливості використання такої спроможності для маніпулювання та управління не лише економічним вибором, але й соціальною та політичною поведінкою, лише нещодавно стала явною. У цьому контексті особливу увагу потрібно звернути на ту серйозну владу,

що її надає технологічний прогрес тим – чи то державним інституціям, чи приватним суб'єктам, – хто може використовувати такі алгоритмічні інструменти без адекватного демократичного нагляду чи контролю.

9. Детально структуровані, підсвідомі та персоналізовані рівні алгоритмічного навіювання можуть мати суттєвий вплив на когнітивну автономію індивідів та їхнє право формувати думки і приймати незалежні рішення. Ці ефекти залишаються недостатньо вивченими, але їх не можна недооцінювати. Вони не тільки здатні послабити здійснення та користування правами людини, але й можуть призвести до корозії самої основи Ради Європи. Її центральні опори – права людини, демократія та верховенство права – ґрунтуються на засадничій вірі в рівність і гідність усіх людей як незалежних моральних суб'єктів.

З огляду на зазначене вище, Комітет Міністрів:

- звертає увагу на щораз більшу небезпеку для права людини формувати думки та приймати рішення незалежно від автоматизованих систем, що нерозривно пов'язані з передовими цифровими технологіями. Особливу увагу потрібно звернути, зокрема, на їхню спроможність використовувати персональні та неперсональні дані для сортування й мікротаргетування людей, виявлення окремих вразливих ситуацій та використання точних прогностичих знань, а також переформування соціальних середовищ для задоволення специфічних цілей і корисливих інтересів;

- закликає держави-члени взяти на себе відповідальність за подолання цієї загрози шляхом:

  - a) забезпечення адекватної пріоритетної уваги на вищому рівні до такої міжгалузевої проблеми, яка часто потрапляє у прогалини між визначеними сферами повноважень відповідних органів;

  - b) розгляду потреби додаткових захисних рамок, пов'язаних з даними, які лежать за межами сучасних понять про захист персональних даних та приватного життя, які б більш широко стосувалися істотних наслідків цілеспрямованого використання даних на суспільство та на реалізацію прав людини;

  - c) започаткування у відповідних інституційних рамках відкритих, поінформованих та інклюзивних публічних дискусій із метою надання рекомендацій, де варто провести межу між формами припустимого навіювання та неприйнятними маніпуляціями. Останні можуть набирати вигляду впливу, який є підсвідомим, використовує наявні вразливості чи когнітивні упередження та/або зазіхає на незалежність і автентичність індивідуального прийняття рішень;

- d) вжиття відповідних та пропорційних заходів для забезпечення ефективних правових гарантій, доречних проти таких форм протиправного втручання; і

- e) розширення можливостей користувачів шляхом підтримки найважливіших навичок цифрової грамотності та завдяки значному підвищенню поінформованості суспільства про те, наскільки багато даних генерується та обробляється персональними пристроями, мережами та платформами через алгоритмічні процеси, пристосовані для використання даних. Особливо варто підвищити поінформованість суспільства щодо того, що алгоритмічні інструменти широко застосовуються для комерційних цілей і щораз частіше з політичних міркувань, а також у зв'язку з прагненнями анти- або недемократичного отримання влади, ведення війни чи заподіяння безпосередньої шкоди;

- рівною мірою підкреслює відповідальність держав-членів за проведення та підтримку досліджень та вивчення проблем незалежності, рівності та якості життя, що посилює потенціал передових технологій обробки даних і машинного навчання. Зокрема, потрібно створювати стимули щодо розробки сервісів, які зміцнюють рівний доступ до прав людини та користування ними, а також формують загальні цінності для суспільства, спонукаючи, зокрема, задовольняти потреби історично маргіналізованих або досі недостатньо забезпечених спільнот. З цією метою потрібно сприяти структурному розмаїттю інновацій та досліджень;

- визнає необхідність розглядати як на національному, так і на міжнародному рівнях чимраз вищий рівень відповідальності, яка покладається на індустрію у різних секторах у контексті виконання власних важливих функцій та впливу на сумірні рівні підвищеної справедливості, прозорості та підзвітності відповідно до їх відповідальності за повагу до прав людини й основоположних свобод та під керівництвом публічних інституцій;

- наголошує на суспільній ролі наукових кіл щодо проведення незалежних, доказових та міждисциплінарних досліджень і консультацій для осіб, які приймають рішення, щодо здатності алгоритмічних інструментів посилювати когнітивну незалежність індивідів чи втручатися в неї. Таке дослідження має брати до уваги існуючу різноманітність у суспільстві та повинно охоплювати всі соціальні прошарки й вікові категорії користувачів не лише в контексті їхньої поведінки як споживачів, а й з урахуванням ширшого впливу на емоційне самопочуття й особистий вибір у суспільному, інституційному та політичному контексті;

- звертає увагу на необхідність критично оцінити потребу посилення регуляторних чи інших заходів із метою забезпечити адекватний та демократично легітимізований нагляд за створенням, розробкою, розгортанням і використанням алгоритмічних інструментів з огляду на гарантованість існування ефективного захисту від недобросовісної практики або зловживання становищем ринкової влади;

- наголошує, зокрема, на потребі оцінки нормативної бази, пов'язаної з політичною комунікацією та виборчими процесами, щоб захистити справедливість і доброчесність виборів як у режимі офлайн, так і в режимі онлайн відповідно до встановлених принципів. Зокрема, необхідно забезпечити, щоб виборці мали доступ до інформації щодо усього політичного спектру, яку можна порівнювати, щоб виборці усвідомлювали небезпеку політичної практики «червоних ліній», яка виникає, коли політична агітація обмежується тими, хто найбільше зазнає впливу, а також гарантувати, що виборці ефективно захищені від недобросовісної практики та маніпуляцій;

- підкреслює життєво важливу роль, яку відіграють незалежні та плюралістичні засоби масової інформації у нагляді за публічними справами й процесами від імені електорату, тим самим виступаючи вартовими суспільства та сприяючи змістовній і поінформованій дискусії;

- закликає держави-члени підтримувати відкритий та інклюзивний діалог з усіма відповідними зацікавленими сторонами в усьому світі, щоб уникнути залежностей від обраного шляху та повністю розглянути всі наявні способи ефективного врегулювання цієї нової і поки що недостатньо вивченої та, можливо, недооціненої проблеми.

Модернізована Конвенція[1]
про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108+)

Зведений текст [2]

Страсбург, 28 січня 1981 року **– Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (угода ETS № 108), відкрита для підписання державамичленами Ради Європи та приєднання держав, які не є членами Ради Європи**

Страсбург, 08 листопада 2001 року **– Угода зі змінами, внесеними Додатковим Протоколом (ETS № 181), відкритим для підписання державами, які підписали угоду ETS № 108, та Європейським Союзом, а також для приєднання держав, які приєдналися до угоди ETS № 108**

Страсбург, 10 жовтня 2018 року **– Угода зі змінами, передбаченими Протоколом (CETS № 223), відкрита для підписання державами-Сторонами угоди ETS № 108**

ПРЕАМБУЛА

Держави-члени Ради Європи та інші підписанти цієї Конвенції,

беручи до уваги те, що метою Ради Європи є досягнення більшого єднання між її членами, яке ґрунтується, зокрема, на дотриманні верховенства права, а також прав людини й основоположних свобод;

беручи до уваги необхідність забезпечувати гідність та захист прав й основоположних свобод для кожної особи і з огляду на диверсифікацію, інтенсифікацію і глобалізацію обробки даних і потоків персональних даних, особисту незалежність, засновану на праві особи контролювати його або її персональні дані та обробку таких даних;

нагадуючи, що право на захист персональних даних має розглядатися у зв'язку з його роллю у суспільстві і що воно повинне узгоджуватися з іншими правами людини та основоположними свободами, включаючи свободу вираження поглядів;

беручи до уваги, що в ході виконання правил, встановлених цією Конвенцією, вона дозволяє враховувати принцип права на доступ до офіційних документів;

визнаючи необхідність підтримувати основоположні цінності поваги до приватного життя та захисту персональних даних на глобальному рівні, тим самим сприяючи безперешкодному обміну інформацією між людьми;

---

1. Оригінал тексту доступний на веб-сторінці за посиланням: conventions.coe.int.
2. Текст зі змінами, які будуть внесені відповідно до Протоколу CETS № 223, коли останній вступить в силу.

визнаючи зацікавленість у зміцненні міжнародного співробітництва між Сторонами Конвенції,

домовилися про таке:

РОЗДІЛ I – ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1 – Предмет і мета

Метою цієї Конвенції є забезпечення захисту для кожної особи, незалежно від його чи її громадянства або місця проживання, щодо обробки їх персональних даних, сприяючи тим самим дотриманню його або її прав й основоположних свобод, зокрема права на приватне життя.

Стаття 2 – Визначення

Для цілей цієї Конвенції:

- a. «персональні дані» означає будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною (далі – «суб'єкт даних»);
- b. «обробка даних» означає будь-яку операцію або набір операцій, що виконуються щодо персональних даних, такі як збір, зберігання, збереження, зміна, вибірка, розкриття, надання доступу, стирання або знищення, або здійснення логічних та/або арифметичних операцій з такими даними;
- c. у випадках, коли не використовується автоматизована обробка, «обробка даних» означає операцію або набір операцій, що виконуються щодо персональних даних в структурованому наборі таких даних, які є доступними або такими, що піддаються вибірці відповідно до чітких критеріїв;
- d. «контролер» означає фізичну або юридичну особу, орган влади, службу, установу чи будь-який інший орган, що самостійно або спільно з іншими має право приймати рішення щодо обробки даних;
- e. «одержувач» означає фізичну або юридичну особу, орган влади, службу, установу або будь-який інший орган, для яких дані розкривають або надають до них доступ;
- f. «оброблювач» означає фізичну або юридичну особу, орган влади, службу, установу чи будь-який інший орган, що обробляє персональні дані від імені контролера.

Стаття 3 – Сфера застосування

1. Кожна Сторона зобов'язується застосовувати цю Конвенцію до обробки даних, що підпадає під її юрисдикцію у публічному та приватному секторах, забезпечуючи тим самим право кожної особи на захист його або її персональних даних.
2. Ця Конвенція не поширюється на процес обробки даних, що здійснюється особою в ході суто особистої або побутової діяльності.

РОЗДІЛ II – ОСНОВНІ ПРИНЦИПИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Стаття 4 – Обов'язки Сторін

1. Кожна Сторона вживає необхідних заходів щодо свого законодавства для імплементації положень цієї Конвенції та забезпечення їх ефективного застосування.

2. Такі заходи уживаються кожною Стороною і вони мають набути чинності до моменту ратифікації або приєднання до цієї Конвенції.

3. Кожна Сторона зобов'язується:

   - a. дозволити Комітету Конвенції, передбаченому у Розділі VI, здійснювати оцінку ефективності заходів, які вона вжила щодо свого законодавства для виконання положень цієї Конвенції; та

   - b. активно сприяти цьому процесу оцінки.

Стаття 5 – Легітимність обробки даних та якість даних

1. Обробка даних має бути пропорційною відносно легітимних цілей, що переслідуються, і відображати на всіх етапах обробки справедливий баланс між усіма інтересами, яких вона стосується, як публічних, так і приватних, та правами і свободами, про які йдеться.

2. Кожна Сторона повинна забезпечити здійснення обробки даних на підставі вільної, точно визначеної, інформованої і чітко вираженої згоди суб'єкта даних або на іншій легітимній підставі, встановленій законом.

3. Персональні дані, що піддаються обробці, повинні оброблятися правомірно.

4. Персональні дані, що піддаються обробці, повинні:

   - a. оброблятися чесно та прозоро;

   - b. збиратись для чітко виражених, точно визначених і легітимних цілей та не оброблятись у спосіб, несумісний з такими цілями; подальша обробка для цілей архівування в суспільних інтересах, в наукових чи історичних або статистичних цілях, з урахуванням відповідних гарантій, сумісна з такими цілями;

   - c. бути адекватними, відповідними та ненадмірними щодо цілей, для яких вони обробляються;

   - d. бути точними та, в разі потреби, оновлюватися;

   - e. зберігатись у формі, яка дозволяє ідентифікацію суб'єктів даних не довше, ніж це необхідно для цілей, для яких такі дані обробляються.

Стаття 6 – Особливі категорії даних

1. Обробка:

   - генетичних даних;
   - персональних даних, що стосуються правопорушень, кримінальних проваджень та судимості, а також пов'язаних із цим заходів безпеки;
   - біометричних даних, які однозначно ідентифікують особу;
   - персональних даних, що містять інформацію про расову або етнічну приналежність, політичні переконання, членство в профспілках, релігійні чи інші переконання, про здоров'я або сексуальне життя,

   дозволяється лише тоді, коли закон закріплює відповідні гарантії, що доповнюють ті, які передбачені цієї Конвенцією.

2. Такі запобіжні заходи повинні захищати від ризиків, які може представляти обробка чутливих даних для інтересів, прав та основоположних свобод суб'єкта даних, зокрема, від ризику дискримінації.

Стаття 7 – Безпека даних

1. Кожна Сторона забезпечує, щоб контролер та, де це необхідно, оброблювач, вживав належні заходи безпеки щодо таких ризиків, як випадковий або несанкціонований доступ, знищення, втрата, використання, зміна або розкриття персональних даних.

2. Кожна Сторона забезпечує, щоб контролер без затримки повідомляв, принаймні компетентний наглядовий орган у розумінні статті 15 цієї Конвенції про ті порушення обробки даних, які можуть становити серйозне втручання в права і основоположні свободи суб'єктів даних.

Стаття 8 – Прозорість обробки

1. Кожна Сторона забезпечує інформування суб'єктів даних контролером про:

   - a. його або її ідентифікаційні дані, постійне місце розташування або діяльності;
   - b. юридичні підстави та цілі запланованої обробки;
   - c. категорії оброблених персональних даних;
   - d. одержувачів або категорії одержувачів персональних даних, якщо такі є; та
   - e. засоби реалізації прав, викладених у Статті 9,

   а також будь-яку необхідну додаткову інформацію для забезпечення чесної та прозорої обробки персональних даних.

2. Пункт 1 не застосовується, якщо суб'єкт даних вже має відповідну інформацію.

3. В разі, якщо персональні дані не відбираються у суб'єктів даних, контролер не зобов'язаний надавати таку інформацію, якщо така обробка чітко передбачена законом, або якщо це виявляється неможливим, або передбачає докладання непропорційно значних зусиль.

Стаття 9 – Права суб'єкта даних

1. Кожна особа має право:

- a. не бути суб'єктом рішення, що має значний вплив на нього або неї, прийнятого виключно на основі автоматизованої обробки даних, без врахування його або її думки;

- b. отримувати на вимогу через розумні інтервали часу та без надмірної затримки або витрат, підтвердження обробки персональних даних, що стосуються його або її; отримувати в доступній для розуміння формі дані, що обробляються, всю наявну інформацію про їх походження, період зберігання, а також будь-яку іншу інформацію, надання якої вимагається від контролера для забезпечення прозорості обробки відповідно до пункту 1 Статті 8;

- c. отримувати на вимогу обґрунтування, що є підставою обробки даних, якщо результати такої обробки застосовуються до нього або неї;

- d. у будь-який час заперечувати на підставах, що стосуються його або її ситуації, проти обробки персональних даних, що стосуються його або її, крім випадків, коли контролер демонструє легітимні підстави для обробки, які переважають його або її інтереси чи права і основоположні свободи;

- e. отримувати на вимогу, безоплатно і без надмірної затримки виправлення або знищення таких даних у відповідних випадках, якщо вони обробляються або оброблялися всупереч положень цієї Конвенції;

- f. мати засоби захисту, передбачені в Статті 12, якщо його або її права за цією Конвенцією були порушені;

- g. мати користь незалежно від його або її громадянства або місця проживання від допомоги наглядового органу у розумінні Статті 15 при реалізації його або її прав за цією Конвенцією.

2. Підпункт «a» пункту 1 не застосовується, якщо рішення було прийняте на підставі закону, який поширюється на контролера і який також передбачає відповідні засоби захисту прав, свобод і легітимних інтересів суб'єкта даних.

Стаття 10 – Додаткові зобов'язання

1. Кожна Сторона забезпечує, щоб контролери та, де це необхідно, обробляючі, вживали всіх відповідних заходів з метою виконання зобов'язань

згідно з цією Конвенцією та були здатні продемонструвати з урахуванням національного законодавства, прийнятого відповідно до пункту 3 Статті 11, зокрема, компетентному наглядовому органу, який передбачено в Статті 15, що обробка даних, яка відбувається під їх контролем, відповідає положенням цієї Конвенції.

2. Кожна Сторона забезпечує, щоб контролери та, де це необхідно, оброблювачі досліджували ймовірний вплив запланованої обробки даних на права та основоположні свободи суб'єктів даних до початку такої обробки і розробляли так процес обробки даних, щоб запобігти або мінімізувати ризик втручання в ці права та основоположні свободи.

3. Кожна Сторона забезпечує, щоб контролери та, де це необхідно, оброблювачі, впроваджували технічні та організаційні заходи, які враховують вплив права на захист персональних даних на всіх етапах обробки даних.

4. Беручи до уваги ризики, що виникають щодо інтересів, прав і основоположних свобод суб'єктів даних, Кожна Сторона може встановити застосування положень пунктів 1, 2 і 3 в своєму законі, імплементуючи положення цієї Конвенції відповідно до характеру і обсягу даних, характеру, обсягу і цілей обробки і, там де це є належним, величини контролера або оброблювача.

Стаття 11 – Винятки та обмеження

1. Жодних винятків з положень, викладених у цьому Розділі, не дозволено за винятком положень пункту 4 Статті 5, пункту 2 Статті 7, пункту 1 Статті 8, а також Статті 9, якщо такі винятки передбачено законом, поважають сутність основоположних прав і свобод та є необхідними і пропорційними заходами в демократичному суспільстві для:

   - a. захисту національної безпеки, оборони, громадської безпеки, важливих економічних та фінансових інтересів Держави, безсторонності та незалежності судової влади або запобігання, розслідування кримінальних правопорушень та притягнення до відповідальності за їх вчинення і для виконання покарань за вчинення кримінальних правопорушень, а також для інших важливих цілей в загальних інтересах суспільства;

   - b. захисту суб'єкта даних або прав і основоположних свобод інших осіб, зокрема права на свободу вираження поглядів.

2. Обмеження щодо виконання положень, визначених в Статтях 8 і 9, можуть передбачатись законом щодо обробки даних для цілей архівування в інтересах суспільства, для наукових або історичних досліджень чи для статистичних цілей у випадках відсутності небезпеки порушення прав та основоположних свобод суб'єктів даних.

3. На додаток до винятків, дозволених пунктом 1 цієї Статті, в частині діяльності з обробки даних для цілей національної безпеки та оборони, кожна Сторона може передбачити в законі і лише настільки, наскільки це є необхідним і пропорційним в демократичному суспільстві для досягнення

цієї мети, винятки щодо пункту 3 Статті 4, пунктів 5 і 6 Статті 14 та підпунктів «a», «b», «c» та «d» пункту 2 Статті 15.

Це аж ніяк не обмежує вимогу про те, що діяльність з обробки даних з метою національної безпеки та оборони має підлягати незалежному та ефективному контролю і нагляду відповідно до національного законодавства відповідної Сторони.

Стаття 12 – Санкції та засоби правового захисту

Кожна Сторона зобов'язується встановити відповідні судові і позасудові санкції та засоби юридичного захисту щодо порушень положень цієї Конвенції.

Стаття 13 – Розширення захисту

Жодне з положень цього Розділу не тлумачиться як таке, що обмежує можливості Сторони забезпечувати суб'єктам даних більший ступінь захисту, ніж передбачений цією Конвенцією, або як таке, що іншим чином впливає на таку можливість.

РОЗДІЛ III – ТРАНСКОРДОННІ ПОТОКИ ПЕРСОНАЛЬНИХ ДАНИХ

Стаття 14 – Транскордонні потоки персональних даних

1. Сторона не може лише з метою захисту персональних даних забороняти чи зумовлювати спеціальними дозволами передачу таких даних одержувачу, який підпадає під дію юрисдикції іншої Сторони Конвенції. Однак, така Сторона може зробити це, якщо існує реальний і серйозний ризик того, що передача до іншої Сторони, або від цієї іншої Сторони до суб'єкта, що не є стороною Конвенції, призведе до уникнення виконання положень Конвенції. Сторона також може так вчинити, якщо вона має зобов'язання за гармонізованими правилами захисту, що є спільними для держав, які належать до регіональної міжнародної організації.

2. Якщо одержувач підпадає під дію юрисдикції держави або міжнародної організації, яка не є Стороною цієї Конвенції, передача персональних даних може здійснюватися лише за умови забезпечення відповідного рівня захисту на основі положень цієї Конвенції.

3. Відповідний рівень захисту може бути забезпечений:

   - a. законодавством цієї держави або міжнародної організації, включаючи застосовні міжнародні договори або угоди; або

   - b. ad hoc або прийнятими стандартизованими гарантіями, що забезпечуються юридично зобов'язуючими та такими, що можуть бути виконаними, інструментами, прийнятими та запровадженими особами, залученими до передачі та подальшої обробки даних.

4. Незважаючи на положення попередніх пунктів, кожна зі Сторін може передбачити, що передача персональних даних може здійснюватися, якщо:

   - a. суб'єкт даних дав ясну, чітко визначену і добровільну згоду після того, як був поінформований про ризики, що виникають у разі відсутності відповідних гарантій; або
   - b. особливі інтереси суб'єкта даних вимагають цього в окремому випадку; або
   - c. переважаючі легітимні інтереси, зокрема, важливі суспільні інтереси є передбаченими законом, і така передача є необхідним і пропорційним заходом в демократичному суспільстві; або
   - d. це є необхідним і пропорційним заходом в демократичному суспільстві для свободи вираження поглядів.

5. Кожна Сторона забезпечує отримання компетентним наглядовим органом у значенні Статті 15 цієї Конвенції всієї відповідної інформації, що стосується випадків передачі даних, передбачених у підпункті «b» пункту 3, а також за вимогою щодо випадків, передбачених у підпунктах «b» та «c» пункту 4.

6. Кожна Сторона також забезпечує, щоб наглядовий орган був повноважним вимагати, щоб особа, яка передає дані, продемонструвала ефективність гарантій або існування переважаючих легітимних інтересів, і щоб наглядовий орган міг з метою захисту прав і основоположних свобод суб'єктів даних заборонити, призупинити такі передачі або встановлювати умови такої передачі.

РОЗДІЛ IV – НАГЛЯДОВІ ОРГАНИ

Стаття 15 – Наглядові органи

1. Кожна Сторона передбачає один або декілька органів влади, які є відповідальними за забезпечення дотримання положень цієї Конвенції.

2. З цією метою дані органи повинні:

   - a. мати повноваження проводити розслідування та здійснювати втручання;
   - b. виконувати функції, пов'язані з передачею даних, передбаченою Статтею 14, зокрема, погодження стандартизованих гарантій;
   - c. мати повноваження приймати рішення щодо порушень положень цієї Конвенції і, зокрема, можливість накладати адміністративні санкції;
   - d. бути повноважними брати участь у судовому проваджені або доводити факти порушень положень цієї Конвенції до відома компетентних судових органів;

▸ e. сприяти:

i. поінформованості громадськості про свої функції та повноваження, а також про свою діяльність;

ii. поінформованості громадськості про права суб'єктів даних та їх реалізацію;

iii. поінформованості контролерів та оброблювачів про їх обов'язки згідно з цією Конвенцією;

особлива увага повинна приділятися праву на захист даних дітей та інших вразливих осіб.

3. Пропозиції щодо будь-яких законодавчих або адміністративних заходів, які передбачають обробку персональних даних, повинні узгоджуватись з компетентними наглядовими органами.

4. Кожен компетентний наглядовий орган розглядає запити та скарги, подані суб'єктами даних щодо їх права на захист даних, і інформує суб'єктів даних про стан їх розгляду.

5. В ході виконання своїх обов'язків та здійснення своїх повноважень, наглядові органи діють з повною незалежністю та безсторонністю, і тому не повинні ні просити, ні приймати жодних вказівок.

6. Кожна Сторона забезпечує наглядові органи ресурсами, необхідними для ефективного виконання ними своїх функцій та здійснення їхніх повноважень.

7. Кожен наглядовий орган готує та публікує періодичну доповідь з інформацією про його діяльність.

8. Члени та персонал наглядових органів зобов'язані дотримуватись конфіденційності щодо конфіденційної інформації, до якої вони мають або мали доступ під час виконання своїх обов'язків та повноважень.

9. Рішення наглядових органів можуть підлягати судовому оскарженню.

10. Наглядові органи не є компетентними в питаннях обробки даних органами, які здійснюють судові повноваження.

РОЗДІЛ V – СПІВРОБІТНИЦТВО ТА ВЗАЄМОДОПОМОГА

Стаття 16 – Призначення наглядових органів

1. Сторони погоджуються співпрацювати та надавати одна одній взаємну допомогу для реалізації цієї Конвенції.

2. Для цього:

- a. кожна Сторона призначає один чи більше наглядових органів у значенні Статті 15 цієї Конвенції, назву та адресу яких вона повідомляє Генеральному секретарю Ради Європи;
- b. кожна Сторона, яка призначила більше одного наглядового органу, зазначає компетенцію кожного органу у своєму повідомленні, згаданому в попередньому підпункті.

Стаття 17 – Форми співпраці

1. Наглядові органи співпрацюють один з одним в обсязі, необхідному для виконання їхніх обов'язків і здійснення повноважень, зокрема шляхом:

- a. надання взаємної допомоги шляхом обміну відповідною та корисною інформацією і шляхом співпраці один з одним за умови дотримання всіх правил та гарантій цієї Конвенції щодо захисту персональних даних;
- b. координації своїх розслідувань, чи втручань або проведення спільних дій;
- c. надання інформації та документації про своє законодавство та адміністративну практику щодо захисту даних.

2. Інформація, зазначена в пункті 1, не повинна містити персональні дані, які обробляються, крім випадків, коли такі дані є важливими для співпраці або коли суб'єкт даних, про якого йде мова, надав чітко виражену, визначену, добровільну та поінформовану згоду на її надання.

3. Наглядові органи Сторін формують мережу для організації співпраці і виконання обов'язків, викладених в попередніх пунктах.

Стаття 18 – Допомога суб'єктам даних

1. Кожна Сторона надає допомогу будь-якому суб'єкту даних, незалежно від його або її громадянства чи місця проживання, у реалізації його або її прав відповідно до Статті 9 цієї Конвенції.

2. Якщо суб'єкт даних проживає на території іншої Сторони, йому або їй надається можливість подати вимогу за посередництвом наглядового органу, призначеного цією Стороною.

3. Вимога про надання допомоги повинна містити всі необхідні відомості, що стосуються, зокрема:

- a. ім'я, адреси та будь-яких інших відповідних відомостей, які ідентифікують суб'єкта даних, що звертається з вимогою;
- b. обробки, якої стосується вимога, або її контролера;
- c. мети вимоги.

Стаття 19 – Гарантії

1. Наглядовий орган, який отримав інформацію від іншого наглядового органу, що супроводжує вимогу або інформацію у відповідь на його вимогу, використовує цю інформацію лише для цілей, зазначених у вимозі.

2. Наглядовому органу у жодному випадку не дозволяється на власний розсуд і без чітко вираженого схвалення суб'єкта даних звертатися з вимогою від імені такого суб'єкта даних.

Стаття 20 – Відхилення вимог

Наглядовий орган, до якого адресовано вимогу згідно зі Статтею 17 цієї Конвенції, може відмовити у задоволенні такого прохання, якщо:

- a. вимога є не сумісною з його повноваженнями;
- b. вимога не відповідає положенням цієї Конвенції;
- c. виконання вимоги буде несумісним з суверенітетом, національною безпекою або громадським порядком Сторони, якою він був призначений, або з правами та основоположними свободами осіб, які перебувають під юрисдикцією цієї Сторони.

Стаття 21 – Витрати та процедура

1. Співпраця і взаємна допомога, яку Сторони надають одна одній згідно зі Статтею 17, та допомога, яку вони надають суб'єктам даних згідно зі Статтями 9 і 18, не може бути підставою для сплати жодних витрат або зборів, за винятком тих, що сплачуються у зв'язку з діяльністю експертів і перекладачів. Витрати або збори у зв'язку з діяльністю останніх сплачуються Стороною, яка звертається з проханням.

2. На суб'єкта даних не може покладатися сплата витрат або зборів, пов'язаних із заходами, яких було вжито від його або її імені на території іншої Сторони, крім витрат або зборів, які на законних підставах сплачуються резидентами такої Сторони.

3. Інші подробиці щодо співпраці і надання допомоги, що стосуються, зокрема, форм і процедур, а також використання мов, визначаються безпосередньо між відповідними Сторонами.

РОЗДІЛ VI – КОМІТЕТ КОНВЕНЦІЇ

Стаття 22 – Склад Комітету

1. Комітет Конвенції створюється після набуття чинності цією Конвенцією.

2. Кожна Сторона призначає до Комітету одного представника та заступника представника. Будь-яка держава-член Ради Європи, яка не є Стороною Конвенції, має право бути представленою в Комітеті спостерігачем.

3. Комітет Конвенції може відповідно до рішення, прийнятого більшістю, тобто двома третинами голосів представників Сторін, запросити спостерігача бути представленим на засіданнях Комітету.

4. Будь-яка Сторона, яка не є членом Ради Європи, робить внесок у фінансування діяльності Комітету Конвенції відповідно до умов, встановлених Комітетом Міністрів за погодженням з цією Стороною.

Стаття 23 – Функції Комітету

Комітет Конвенції:

- a. може вносити рекомендації для сприяння застосуванню або поліпшення застосування Конвенції;
- b. може вносити пропозиції щодо внесення змін до цієї Конвенції відповідно до Статті 25;
- c. робить свій висновок щодо будь-якої пропозиції про внесення змін до цієї Конвенції, яка передається йому на розгляд відповідно до пункту 3 Статті 25;
- d. може робити висновок з будь-якого питання, що стосується тлумачення або застосування цієї Конвенції;
- e. перед будь-яким новим приєднанням до Конвенції готує висновок Комітету Міністрів щодо рівня захисту персональних даних кандидата на приєднання і, якщо необхідно, надає рекомендації щодо вжиття заходів для забезпечення відповідності положенням цієї Конвенції;
- f. може на прохання держави або міжнародної організації оцінити, чи відповідає рівень захисту персональних даних, який забезпечує держава, положенням цієї Конвенції, і, якщо необхідно, рекомендувати вжити заходів для досягнення такої відповідності;
- g. може розробляти або затверджувати зразки стандартизованих гарантій, зазначених у Статті 14;
- h. перевіряє виконання цієї Конвенції Сторонами та рекомендує вжити заходів у випадку, якщо Сторона не дотримується цієї Конвенції;
- i. у разі необхідності сприяє дружньому врегулюванню всіх труднощів, пов'язаних із застосуванням цієї Конвенції.

Стаття 24 – Процедура

1. Комітет Конвенції скликається Генеральним секретарем Ради Європи. Його перше засідання відбувається у межах дванадцяти місяців після набрання

чинності цією Конвенцією. Надалі він збирається принаймні раз на рік й у будь-якому разі, коли одна третина представників Сторін вимагає його скликання.

2. Після кожного свого засідання Комітет Конвенції подає Комітетові Міністрів Ради Європи доповідь про свою роботу та про стан виконання Конвенції.

3. Механізм голосування в Комітеті Конвенції наводиться в положеннях Регламенту, який додається до Протоколу CETS № [223].

4. Комітет Конвенції розробляє інші положення свого Регламенту та встановлює, зокрема, процедури оцінки та перевірки, згаданих в пункті 3 Статті 4 та підпунктах «e», «f» та «h» Статті 23, на підставі об'єктивних критеріїв.

РОЗДІЛ VII – ЗМІНИ

Стаття 25 – Зміни

1. Зміни до цієї Конвенції можуть пропонуватися Стороною, Комітетом Міністрів Ради Європи або Комітетом Конвенції.

2. Будь-яка пропозиція про внесення зміни надсилається Генеральним секретарем Ради Європи Сторонам цієї Конвенції, іншим державам-членам Ради Європи, Європейському Союзу та кожній державі, що не є членом Ради Європи, або міжнародній організації, яку було запрошено приєднатися до цієї Конвенції відповідно до положень Статті 27.

3. Крім того, будь-яка зміна, запропонована Стороною або Комітетом Міністрів, надсилається Комітету Конвенції, який подає Комітетові Міністрів свій висновок щодо цієї запропонованої зміни.

4. Комітет Міністрів розглядає запропоновану зміну та будь-який висновок, поданий Комітетом Конвенції, і може затвердити зміну.

5. Текст будь-якої зміни, затвердженої Комітетом Міністрів відповідно до пункту 4 цієї Статті, надсилається Сторонам для прийняття.

6. Будь-яка зміна, затверджена відповідно до пункту 4 цієї Статті, набуває чинності на тридцятий день після того, як усі Сторони повідомили Генеральному секретарю про її прийняття.

7. Крім того, Комітет Міністрів, після консультацій з Комітетом Конвенції, може вирішити одноголосно, що конкретна зміна набирає чинності після закінчення трирічного періоду з дати, коли вона була відкрита для прийняття, якщо Сторона не повідомить Генеральному секретарю Ради Європи про те, що вона заперечує проти набуття цією зміною чинності. В разі виникнення такого заперечення зміна набирає чинності в перший день місяця, що настає після дати, коли Сторона цієї Конвенції, яка повідомила про

заперечення, здала на зберігання Генеральному секретарю Ради Європи свій документ про прийняття.

РОЗДІЛ VIII – ЗАКЛЮЧНІ ПОЛОЖЕННЯ

Стаття 26 – Набуття чинності

1. Ця Конвенція відкрита для підписання державами-членами Ради Європи та Європейським Союзом. Вона підлягає ратифікації, прийняттю або схваленню. Ратифікаційні грамоти або документи про прийняття чи схвалення здаються на зберігання Генеральному секретарю Ради Європи.

2. Ця Конвенція набуває чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати, коли п'ять держав-членів Ради Європи висловили свою згоду на обов'язковість для них цієї Конвенції відповідно до положень попереднього пункту.

3. Для будь-якої Сторони, яка надалі висловлює свою згоду на обов'язковість для неї цієї Конвенції, вона набуває чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати здачі на зберігання ратифікаційної грамоти або документа про прийняття чи схвалення.

Стаття 27 – Приєднання держав, що не є членами Ради Європи, або міжнародних організацій

1. Після набуття чинності цією Конвенцією Комітет Міністрів Ради Європи, після консультацій зі Сторонами цієї Конвенції та отримання їх одностайної згоди, та у світлі висновку, підготовленого Комітетом Конвенції відповідно до пункту «e» Статті 23, може запропонувати будь-якій державі, яка не є членом Ради Європи, чи міжнародній організації приєднатися до цієї Конвенції шляхом ухвалення рішення більшістю голосів, як це передбачено в пункті «d» Статті 20 Статуту Ради Європи, і шляхом одностайного голосування представників Договірних держав, які мають право засідати в Комітеті Міністрів.

2. Для будь-якої держави або міжнародної організації, що приєдналася до цієї Конвенції відповідно до вищезазначеного пункту 1, Конвенція набуває чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати здачі на зберігання документа про приєднання Генеральному секретарю Ради Європи.

Стаття 28 – Територіальні положення

1. Будь-яка держава, Європейський Союз чи інша міжнародна організація під час підписання або здачі на зберігання своєї ратифікаційної грамоти або свого документа про прийняття, схвалення чи приєднання, може визначити територію або території, до яких застосовується ця Конвенція.

2. Будь-яка держава, Європейський Союз чи інша міжнародна організація може будь-коли після цього, шляхом подання декларації на ім'я Генерального секретаря Ради Європи поширити дію цієї Конвенції на будь-яку іншу територію, визначену в цій декларації. Конвенція набуває чинності щодо

такої території в перший день місяця, що настає після закінчення тримісячного періоду від дати отримання такої декларації Генеральним секретарем.

3. Будь-яка заява, подана відповідно до двох попередніх пунктів, може бути відкликана щодо будь-якої території, визначеної в цій заяві, шляхом подання відповідного повідомлення на ім'я Генерального секретаря.

   Відкликання набуває чинності в перший день місяця, що настає після закінчення шестимісячного періоду від дати отримання такого повідомлення Генеральним секретарем.

Стаття 29 – Застереження

Жодне застереження щодо положень цієї Конвенції не дозволяється.

Стаття 30 – Денонсація

1. Будь-яка Сторона може будь-коли денонсувати цю Конвенцію шляхом подання відповідного повідомлення на ім'я Генерального секретаря Ради Європи.

2. Така денонсація набуває чинності в перший день місяця, що настає після закінчення шестимісячного періоду від дати отримання такого повідомлення Генеральним секретарем.

Стаття 31 – Повідомлення

Генеральний секретар Ради Європи повідомляє державам-членам Ради Європи та будь-якій Стороні цієї Конвенції про:

- a. будь-яке підписання;
- b. здачу на зберігання будь-якої ратифікаційної грамоти чи будь-якого документа про прийняття, схвалення або приєднання;
- c. будь-яку дату набуття чинності цією Конвенцією відповідно до Статей 26, 27 та 28;
- d. будь-яку іншу дію, повідомлення або комунікацію, що стосуються цієї Конвенції.

ДОДАТОК ДО ПРОТОКОЛУ:
ЕЛЕМЕНТИ ПОЛОЖЕНЬ РЕГЛАМЕНТУ КОМІТЕТУ КОНВЕНЦІЇ

1. Кожна Сторона має право голосу і має один голос.

2. Більшість у складі двох третин представників Сторін становить кворум, необхідний для проведення засідань Комітету Конвенції. У випадку, якщо Протокол про внесення змін до Конвенції набуває чинності відповідно до пункту 2 Статті 37 до набуття ним чинності щодо всіх Договірних держав Конвенції, для засідань Комітету Конвенції необхідний кворум в кількості не менше 34 Сторін Протоколу.

3. Рішення відповідно до Статті 23 приймаються більшістю у чотири п'ятих голосів. Рішення відповідно до підпункту «h» Статті 23 приймається більшістю у чотири п'ятих голосів, включаючи більшість голосів держав-Сторін, які не є членами організації регіональної інтеграції, яка є стороною Конвенції.

4. У разі, якщо Комітет Конвенції приймає рішення відповідно до підпункту «h» статті 23, Сторона, якої стосується перевірка, – не голосує. Якщо таке рішення стосується питання, що підпадає під компетенцію організації регіональної інтеграції, не голосують ані організація, ані її держави-члени.

5. Рішення щодо процедурних питань приймаються простою більшістю голосів.

6. Організації регіональної інтеграції у питаннях, що входять до їх компетенції, можуть реалізувати своє право голосу в Комітеті Конвенції з кількістю голосів, що дорівнює кількості держав-членів організації, які є Сторонами Конвенції. Така організація не може використовувати своє право голосу, якщо будь-яка з її держав-членів здійснює своє право.

7. У разі голосування всі Сторони повинні бути поінформовані про предмет і час голосування, а також про те, чи голосування здійснюватимуться Сторонами окремо, чи регіональною організацією інтеграції від імені її держав-членів.

8. Комітет Конвенції може надалі вносити зміни до свого Регламенту більшістю у дві третіх голосів, за винятком процедури голосування, яка може бути змінена лише одностайним голосуванням Сторін і до якої застосовується Стаття 25 Конвенції.

Конвенція про кіберзлочинність[1]
(Будапештська конвенція)

***Будапешт, 23 листопада 2001 року* – Угода, відкрита для підписання державами-членами Ради Європи та державами не членами Ради Європи, які брали участь у її розробці, та для приєднання інших держав, що не є членами Ради Європи**

ПРЕАМБУЛА

Держави-члени Ради Європи та інші держави, які підписали цю Конвенцію,

Вважаючи, що метою Ради Європи є досягнення більшої єдності між її членами;

Визнаючи цінність налагодження співробітництва з іншими державами, які є Сторонами цієї Конвенції;

Впевнені у першочерговій необхідності спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, між іншим, шляхом створення відповідного законодавства і налагодження міжнародного співробітництва;

Усвідомлюючи глибокі зміни, спричинені переходом на цифрові технології, конвергенцією і глобалізацією комп'ютерних мереж, яка продовжується;

Стурбовані ризиком того, що комп'ютерні мережі та електронна інформація може також використовуватися для здійснення кримінальних правопорушень, і того, що докази, пов'язані з такими правопорушеннями, можуть зберігатися і передаватися такими мережами;

Визнаючи необхідність співробітництва між державами і приватними підприємствами для боротьби з кіберзлочинністю і необхідність захисту законних інтересів у ході використання і розвитку інформаційних технологій;

1. Оригінал тексту доступний на веб-сторінці за посиланням: conventions.coe.int.
Офіційний переклад українською мовою доступний за посиланням: zakon.rada.gov.ua/laws/show/994_575.

Вважаючи, що ефективна боротьба з кіберзлочинністю вимагає більшого, швидкого і ефективно функціонуючого міжнародного співробітництва у кримінальних питаннях;

Впевнені, що ця Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це описано у Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва;

Пам'ятаючи про необхідність забезпечити належний баланс між правоохоронними інтересами і повагою до основних прав людини, як це передбачено Конвенцією Ради Європи про захист прав людини і основних свобод 1950 р., Міжнародною Хартією ООН про громадянські і політичні права 1966 р. і іншими відповідними міжнародними угодами з прав людини, які підтверджують право кожного безперешкодно дотримуватись поглядів, а також право на свободу слова, включаючи право на пошук, отримання і передачу будь-якої інформації та ідей, незважаючи на кордони, а також права на повагу до приватного життя;

Також пам'ятаючи про право на захист особистої інформації, як це передбачено Конвенцією Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 р.;

Посилаючись на Конвенцію ООН про права дитини 1989 р. і Конвенцію МОП про найгірші форми дитячої праці 1999 р.;

Беручи до уваги існуючі конвенції Ради Європи про співробітництво у кримінальній сфері іподібні угоди, що існують між державами-членами Ради Європи та іншими державами, і підкреслюючи, що ця Конвенція має на меті доповнення цих конвенцій для підвищення ефективності кримінальних розслідувань і переслідувань, що стосуються кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, і для надання можливості збирання доказів, що стосуються кримінального злочину, в електронній формі;

Вітаючи нещодавні події, які сприяють міжнародному порозумінню і співробітництву у боротьбі з кіберзлочинністю, включаючи заходи ООН, ОЕСР, ЄС і «Великої вісімки»;

Посилаючись на Рекомендації Комітету Міністрів № R(85)10, що стосується практичного застосування Європейської Конвенції про взаємодопомогу у кримінальних справах по відношенню до листів, які створюють необхідність перехоплення телекомунікацій, № R(88)2 про піратство у сфері авторських і суміжних прав, № R(87)15, яка регулює використання особистих даних у поліцейській галузі, № R(95)4 про захист особистих даних у сфері телекому-

нікаційних послуг, з особливим посиланням на телефонні послуги, а також № R(89)9 про злочини, пов'язані з комп'ютерами, яка надає орієнтири для національного законодавства щодо визначення певних комп'ютерних злочинів, і № R(95)13, що стосується проблем кримінально-процесуального права, пов'язаних з інформаційними технологіями;

Посилаючись на Резолюцію N1, прийняту європейськими міністрами юстиції на своїй 21-й Конференції (Прага, 10-11червня 1997 р.), яка рекомендувала Комітету Міністрів підтримати роботу, що проводиться Європейським комітетом з проблем злочинності (ЄКПЗ) щодо кіберзлочинності для зближення внутрішньодержавних положень кримінального права і створення можливостей для застосування ефективних засобів розслідування таких правопорушень, а також на Резолюцію № 3, прийняту на 23-й Конференції європейських міністрів юстиції (Лондон, 8-9 червня 2000 р.), яка заохочувала сторони переговорів до пошуку відповідних рішень для надання можливості якомога більшій кількості держав стати учасниками цієї Конвенції, і визнала необхідність швидкодіючої і ефективної системи міжнародного співробітництва, яка б належним чином враховувала специфічні вимоги боротьби з кібер-злочинністю;

Також посилаючись на План дій, прийнятий головами держав та урядів Ради Європи з нагоди їх Другого Саміту (Страсбург, 10-11 жовтня 1997 р.), для пошуку спільних відповідей на розвиток нових інформаційних технологій, які базуються на стандартах і цінностях Ради Європи;

Домовились про таке:

РОЗДІЛ I – ВИКОРИСТАННЯ ТЕРМІНІВ

Стаття 1 – Визначення

Для цілей цієї Конвенції:

- a. «комп'ютерна система» означає будь-який пристрій або групу взаємно поєднаних або пов'язаних пристроїв, один чи більш з яких, відповідно до певної програми, виконує автоматичну обробку даних;

- b. «комп'ютерні дані» означає будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою;

- c. «постачальник послуг» означає:

  i. будь-яку державну або приватну установу, яка надає користувачам своїх послуг можливість комунікацій за допомогою комп'ютерної системи, та

ii. будь-яку іншу установу, яка обробляє або зберігає комп'ютерні дані від імені такої комунікаційної послуги або користувачів такої послуги.

- d. "дані про рух інформації" означає будь-які комп'ютерні дані, пов'язані з комунікацією за допомогою комп'ютерної системи, які були створені комп'ютерною системою, що складала частину ланцюга комунікації, і які зазначають походження, кінцевий пункт, маршрут, час, дату, розмір і тривалість комунікації або тип основної послуги.

РОЗДІЛ II – ЗАХОДИ, ЯКІ МАЮТЬ ЗДІЙСНЮВАТИСЯ НА НАЦІОНАЛЬНОМУ РІВНІ

Частина 1 – Матеріальне кримінальне право

Заголовок 1 – Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем

Стаття 2 – Незаконний доступ

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисний доступ до цілої комп'ютерної системи або її частини без права на це. Сторона може вимагати, щоб таке правопорушення було вчинене шляхом порушення заходів безпеки з метою отримання комп'ютерних даних або з іншою недобросовісною метою, або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою.

Стаття 3 – Нелегальне перехоплення

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне перехоплення технічними засобами, без права на це, передач комп'ютерних даних, які не є призначе ними для публічного користування, які проводяться з, на або всередині комп'ютерної системи, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить в собі такі комп'ютерні дані. Сторона може вимагати, щоб таке правопорушення було вчинене з недобросовісною метою або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою.

Стаття 4 – Втручання у дані

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це.

2. Сторона може залишити за собою право вимагати, щоб поведінка, описана у пункті 1, завдавала серйозну шкоду.

Стаття 5 – Втручання у систему

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це.

Стаття 6 – Зловживання пристроями

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це:

   - a. виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином:

     i. пристроїв, включаючи комп'ютерні програми, створених або адаптованих, в першу чергу, з метою вчинення будь-якого зі злочинів, перерахованих у статтях 2-5 вище;

     ii. комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у статтях 2-5; та

   - b. володіння предметом, перерахованим у підпунктах a.i або ii вище, з наміром його використання для вчинення будь-якого зі злочинів, перерахованих у статтях 2-5. Сторона може передбачити у законодавстві, що для встановлення кримінальної відповідальності необхідно володіти певною кількістю таких предметів.

2. Ця стаття не тлумачиться як така, що встановлює кримінальну відповідальність у разі, якщо виготовлення, продаж, придбання для використання, розповсюдження чи надання для використання іншим чином або володіння, зазначені у пункті 1 цієї статті, не призначені для вчинення будь-якого зі злочинів, перерахованих у статтях 2-5 цієї Конвенції, такі як дозволене випробування або захист комп'ютерної системи.

3. Кожна Сторона може залишити за собою право не застосовувати пункт 1 цієї статті, за умови, що таке застереження не стосується продажу, розповсюдження або надання для використання іншим чином предметів, перерахованих у підпункті 1.a.ii цієї статті.

Заголовок 2 – Правопорушення, пов'язані з комп'ютерами

Стаття 7 – Підробка, пов'язана з комп'ютерами

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, введення, зміни, знищення або приховування комп'ютерних даних, яке призводить до створення недійсних даних з метою того, щоб вони вважались або відповідно до них проводилися б законні дії, як з дійсними, незалежно від того, можна чи ні такі дані прямо прочитати і зрозуміти. Сторона може вимагати наявність наміру обману або подібної нечесної поведінки для встановлення кримінальної відповідальності.

Стаття 8 – Шахрайство, пов'язане з комп'ютерами

Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом:

- a. будь-якого введення, зміни, знищення чи приховування комп'ютерних даних,
- b. будь-якого втручання у функціонування комп'ютерної системи,

з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи.

Заголовок 3 – Правопорушення, пов'язані зі змістом

Стаття 9 – Правопорушення, пов'язані з дитячою порнографією

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, наступних дій:
   - a. вироблення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем;
   - b. пропонування або надання доступу до дитячої порнографії за допомогою комп'ютерних систем;
   - c. розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем;
   - d. здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи;
   - e. володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації.
2. Для цілей пункту 1 вище «дитяча порнографія» включає в себе порнографічний матеріал, який візуально зображує:

- a. неповнолітню особу, задіяну у явно сексуальній поведінці;

- b. особу, яка виглядає як неповнолітня особа, задіяну у явно сексуальній поведінці;

- c. реалістичні зображення неповнолітньої особи, задіяної у явно сексуальній поведінці.

3. Для цілей пункту 2 вище термін «неповнолітня особа» включає в себе усіх осіб до18 років. Сторона може, однак, передбачити нижчий віковий поріг, який має бути не меншим за 16 років.

4. Кожна Сторона може залишити за собою право не застосовувати, частково чи повністю, підпункти 1.d, 1.e, 2.b та 2.c.

Заголовок 4 – Правопорушення, пов'язані з порушенням авторських та суміжних прав

Стаття 10 – Правопорушення, пов'язані з порушенням авторських та суміжних прав

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за порушення авторських прав, як це визначено законодавством такої Сторони відповідно до її зобов'язань за Паризьким Актом від 24 липня 1971 р. щодо Бернської Конвенції про захист літературних та художніх творів, Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про авторське право, за винятком будь-яких моральних прав, які надаються такими Конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем.

2. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за порушення суміжних прав, як це визначено законодавством такої Сторони відповідно до її зобов'язань за Міжнародною Конвенцією про захист виконавців, виробників фонограм і організацій мовлення (Римська конвенція), Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про виконання і фонограми, за винятком будь-яких моральних прав, які надаються такими Конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем.

3. Кожна Сторона може залишити за собою право не встановлювати кримінальну відповідальність відповідно до пунктів 1 і 2 цієї статті у обмежених випадках, за умови існування інших ефективних засобів впливу, і за умови того, що таке застереження не порушує міжнародних зобов'язань Сторони відповідно до міжнародних документів, на які містяться посилання у пунктах 1 і 2 цієї статті.

Заголовок 5 – Додаткова відповідальність і санкції

Стаття 11 – Спроба і допомога або співучасть

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисну допомогу чи співучасть у вчиненні будь-якого зі злочинів, перерахованих у статтях 2-10 цієї Конвенції, з метою вчинення такого злочину.

2. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисну спробу вчинити будь-який зі злочинів, перерахованих у статтях 3-5, 7, 8, 9.1.a та 9.1.c цієї Конвенції.

3. Кожна Сторона може залишити за собою право не застосовувати, повністю чи частково, пункт 2 цієї Статті.

Стаття 12 – Корпоративна відповідальність

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення того, щоб юридична особа могла нести відповідальність за кримінальне правопорушення, встановлене відповідно до цієї Конвенції, яке було вчинене на її користь будь-якою фізичною особою, як індивідуально, так і в якості частини органу такої юридичної особи. Така фізична особа має займати керівну посаду в рамках юридичної особи, в силу:

   - a. повноважень представляти цю юридичну особу;
   - b. повноважень приймати рішення від імені цієї юридичної особи;
   - c. повноважень здійснювати контроль в рамках цієї юридичної особи.

2. На додаток до випадків, вже передбачених у пункті 1 цієї статті, кожна Сторона вживає заходів для забезпечення того, щоб юридична особа могла понести відповідальність у разі, коли недостатній нагляд чи контроль, який мав здійснюватися особою, вказаною у пункті 1, створив можливість вчинення кримінального правопорушення, встановленого відповідно до цієї Конвенції, на користь такої юридичної особи фізичною особою, яка діяла під її контролем.

3. Відповідно до юридичних принципів Сторони, відповідальність юридичної особи може бути кримінальною, цивільною або адміністративною.

4. Така відповідальність не впливає на кримінальну відповідальність фізичних осіб, які вчинили правопорушення.

Стаття 13 – Санкції і заходи

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення того, щоб кримінальні правопорушення,

встановлені відповідно до статей 2-11, каралися ефективними, пропорційними і переконливими санкціями, включаючи позбавлення волі.

2. Кожна Сторона забезпечує, щоб юридичні особи, які несуть відповідальність відповідно до статті 12, каралися ефективними, пропорційними і переконливими кримінальними або некримінальними санкціями або заходами, включаючи грошові санкції.

Частина 2 – Процедурне право

Заголовок 1 – Загальні положення

Стаття 14 – Сфера процедурних положень

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для визначення повноважень і процедур, передбачених цією частиною, з метою конкретних кримінальних розслідувань або переслідувань.

2. За винятком обставин, конкретно передбачених статтею 21, кожна Сторона застосовує повноваження і процедури, передбачені у пункті 1 цієї статті, до:

   - a. кримінальних правопорушень, встановлених відповідно до статей 2-11 цієї Конвенції;

   - b. інших кримінальних правопорушень, вчинених за допомогою комп'ютерних систем; та

   - c. збору доказів у електронній формі стосовно кримінального правопорушення.

3. - a. Кожна Сторона може залишити за собою право застосовувати заходи, які містяться у статті 20, тільки до правопорушень або до категорій правопорушень, зазначених у застереженні, за умови, що обсяг таких правопорушень або категорій правопорушень не менший за обсяг правопорушень, до яких вона застосовує заходи, які містяться у статті 21. Кожна Сторона розгляне можливість обмеження такого застереження з метою якомога ширшого застосування заходів, які містяться у статті 20.

   - b. Якщо Сторона внаслідок обмежень, встановлених її чинним законодавством під час прийняття цієї Конвенції, не може застосовувати заходи, які містяться у статтях 20 і 21, до комунікацій, які передаються всередині комп'ютерної системи постачальника послуг, причому така система

     i. використовується на користь закритої групи користувачів, та

     ii. не використовує мережі зв'язку загального доступу, і не пов'язана з іншою комп'ютерною системою, відкритою для загального доступу чи приватною,

така Сторона може залишити за собою право не застосовувати ці заходи для таких комунікацій. Кожна Сторона розгляне можливість обмеження такого застереження з метою якомога ширшого застосування заходів, які містяться у статтях 20 і 21.

Стаття 15 – Умови і запобіжні заходи

1. Кожна Сторона забезпечує, щоб встановлення, імплементація і застосування повноважень і процедур, передбачених цією частиною, регулювалися умовами і запобіжними заходами, передбаченими її внутрішньо-державним правом, які б забезпечували адекватний захист прав і свобод людини, включаючи права, що випливають із зобов'язань за Конвенцією Ради Європи про захист прав людини і основних свобод 1950 р., Міжнародною Хартією ООН про громадянські і політичні права 1966 р., та інших відповідних міжнародних угод з прав людини, і які б включали в себе принцип пропорційності.

2. Такі умови і запобіжні заходи включатимуть, між іншим, як це є доречним з огляду на природу відповідного повноваження або процедури, судовий або інший незалежний нагляд, підстави, які виправдовують застосування, і обмеження сфери застосування і терміну таких повноважень або процедур.

3. У тій мірі, наскільки це відповідає суспільним інтересам, зокрема, належному відправленню правосуддя, кожна Сторона розгляне вплив повноважень і процедур, які містяться у цій частині, на права, відповідальність і законні інтереси третіх сторін.

Заголовок 2 – Загальні положення

Стаття 16 – Термінове збереження комп'ютерних даних, які зберігаються

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання можливості своїм компетентним органам видавати ордери або іншим подібним шляхом спричиняти термінове збереження визначених комп'ютерних даних, включаючи дані про рух інформації, які зберігалися за допомогою комп'ютерної системи, зокрема у випадку, коли існують підстави вважати, що такі комп'ютерні дані особливо вразливі до втрати чи модифікації.

2. Якщо Сторона застосовує пункт 1 вище шляхом видачі ордеру особі, яким така особа зобов'язується зберігати визначені комп'ютерні дані, які зберігаються і знаходяться у власності або під контролем такої особи, вона вживає такі законодавчі та інші заходи, які можуть бути необхідними для того, щоб зобов'язати таку особу зберігати і підтримувати цілісність таких комп'ютерних даних протягом такого періоду, який буде необхідним для того, щоб компетентні органи мали можливість отримати дозвіл на їхнє розкриття, з максимальним терміном у 90 днів. Сторона може передбачити можливість наступного продовження терміну дії такого ордеру.

3. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для того, щоб зобов'язати особу, яка має зберігати ком-

п'ютерні дані, зберігати конфіденційність факту проведення таких процедур протягом періоду, визначеного її внутрішньодержавним законодавством.

4. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.

Стаття 17 – Термінове збереження і часткове розкриття даних про рух інформації

1. Кожна Сторона вживає по відношенню до даних про рух інформації, які мають зберігатися відповідно до статті 16, такі законодавчі та інші заходи, які можуть бути необхідними для:

   - a. забезпечення того, щоб таке термінове збереження даних про рух інформації могло проводитися, незважаючи на те, один чи більше постачальників послуг було залучено до передачі такої інформації; та

   - b. забезпечити термінове розкриття компетентному органові Сторони або особі, призначеній таким органом, обсягу даних про рух інформації, достатнього для ідентифікації постачальників послуг і маршруту, яким була передана інформація.

2. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.

Заголовок 3 – Порядок представлення
Стаття 18 – Порядок представлення

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання повноважень своїм компетентним органам видавати ордери:

   - a. особі, яка знаходиться на її території – про надання зазначених комп'ютерних даних, якими така особа володіє або контролює, і які зберігаються у комп'ютерній системі або на комп'ютерному носії інформації; та

   - b. постачальнику послуг, який пропонує свої послуги на території Сторони – про надання інформації про користувача послуг, пов'язаної з такими послугами, яка знаходиться у власності або під контролем такого поста-чальника послуг.

2. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.

3. Для цілей цієї статті термін «інформація про користувача послуг» означає будь-яку інформацію, у формі комп'ютерних даних чи у іншій формі, яка

знаходиться у постачальника послуг, відноситься до користувачів його послуг, не є даними про рух даних або власне даними змісту інформації, та за допомогою якої можна встановити:

- a. тип комунікаційної послуги, яка використовувалася, її технічні положення і період користування послугою;
- b. особистість користувача послуг, поштову або географічну адресу, телефони та інший номер доступу, інформацію про рахунки і платежі, яку можна отримати за допомогою угоди або домовленості про постачання послуг;
- c. будь-яку іншу інформацію про місце встановлення комунікаційного обладнання, яку можна отримати за допомогою угоди або домовленості про постачання послуг.

Заголовок 4 – Обшук і арешт комп'ютерних даних, які зберігаються

Стаття 19 – Обшук і арешт комп'ютерних даних, які зберігаються

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання повноважень своїм компетентним органам для обшуку або подібного доступу до:
   - a. комп'ютерної системи або її частини і комп'ютерних даних, які зберігаються в ній; та
   - b. комп'ютерного носія інформації, на якому можуть зберігатися комп'ютерні дані на її території.
2. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення того, щоб у випадку, коли її компетентні органи здійснюють обшук або подібний доступ до конкретної комп'ютерної системи або її частини відповідно до підпункту 1.a, і мають підстави вважати, що дані, які розшукуються, зберігаються у іншій комп'ютерній системі чи її частині, яка знаходиться на її території, і до таких даних можна здійснити законний доступ з першої системи чи вони є доступними першій системі, такі компетентні органи мали право терміново поширити обшук або подібний доступ на іншу систему.
3. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання своїм компетентним органам повноважень арештовувати або вчиняти подібні дії щодо комп'ютерних даних, до яких був здійснений доступ відповідно до пунктів 1 або 2. Такі заходи включатимуть повноваження на:
   - a. арешт або подібні дії щодо комп'ютерної системи або її частини або комп'ютерного носія інформації;
   - b. копіювання і збереження копії таких комп'ютерних даних;
   - c. збереження цілісності відповідних збережених комп'ютерних даних;

- d. заборону доступу або вилучення цих комп'ютерних даних з комп'ютерної системи, до якої здійснювався доступ.

4. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання своїм компетентним органам повноважень вимагати від будь-якої особи, яка знає про функціонування комп'ютерної системи або про заходи, які були здійснені для захисту комп'ютерних даних, які містяться у ній, надавати, наскільки це можливо, необхідну інформацію для проведення дій, які містяться у пунктах 1 і 2.

5. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.

Заголовок 5 – Збирання комп'ютерних даних у реальному масштабі часу

Стаття 20 – Збирання даних про рух інформації у реальному масштабі часу

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання своїм компетентним органам повноважень:

   - a. збирати або записувати технічними засобами на території такої Сторони, та

   - b. зобов'язувати постачальника послуг, в межах його існуючих технічних можливостей:

     i. збирати або записувати технічними засобами на території такої Сторони; або

     ii. співробітничати і допомагати компетентним органам у зборі або запису даних про рух інформації у реальному масштабі часу, які пов'язані з визначеною передачею інформації на її території, яка передається за допомогою комп'ютерних систем.

2. Якщо Сторона, в силу встановлених принципів її юридичної системи, не може застосувати заходи, на які містяться посилання у пункті 1.a, вона замість цього може вжити такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення збору або запису даних про рух інформації у реальному масштабі часу, які пов'язані з визначеною передачею інформації на її території, шляхом застосування технічних засобів на такій території.

3. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для того, щоб зобов'язати постачальника послуг зберігати конфіденційність факту використання будь-якого з повноважень, зазначених у цій статті, і будь-якої інформації, пов'язаної з цим.

4. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.

Стаття 21 – Перехоплення даних змісту інформації

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними стосовно певних серйозних злочинів, які визначаються внутрішньодержавним законодавством, для надання повноважень своїм компетентним органам:

   - a. збирати або записувати технічними засобами на території такої Сторони, або
   - b. зобов'язувати постачальника послуг, в межах його існуючих технічних можливостей:

     i. збирати або записувати технічними засобами на території такої Сторони; або

     ii. співробітничати і допомагати компетентним органам у зборі або запису даних змісту інформації у реальному масштабі часу, які належать до визначеної передачі інформації на її території, яка здійснюється за допомогою комп'ютерних систем.

2. Якщо Сторона, в силу встановлених принципів її юридичної системи, не може застосувати заходи, на які містяться посилання у пункті 1.a, вона замість цього може вжити такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення збору або запису даних змісту інформації у реальному масштабі часу, які належать до визначеної передачі інформації на її території, шляхом застосування технічних засобів на такій території.

3. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для того, щоб зобов'язати постачальника послуг зберігати конфіденційність факту використання будь-якого з повноважень, зазначених у цій статті, і будь-якої інформації, пов'язаної з цим.

4. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.

Частина 3 – Юрисдикція

Стаття 22 – Юрисдикція

1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення юрисдикції стосовно будь-якого злочину, встановленого відповідно до статей 2-11 цієї Конвенції, у випадках, коли таке правопорушення вчинене:

   - a. на її території; або
   - b. на борту судна, яке плаває під прапором такої Сторони; або
   - c. на борту літака, зареєстрованого відповідно до законодавства такої Сторони; або
   - d. одним з її громадян, якщо таке правопорушення карається кримінальним законодавством у місці його вчинення, або якщо правопору-

шення вчинено поза межами територіальної юрисдикції будь-якої держави.

2. Кожна держава може залишити за собою право не застосовувати або застосовувати лише у окремих випадках або за окремих умов правила юрисдикції, викладені у пунктах 1.b-1.d цієї статті або у будь-якій їх частині.

3. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення юрисдикції стосовно злочинів, встановлених відповідно до пункту 1 статті 24 цієї Конвенції, у випадках, коли підозрюваний правопорушник знаходиться на її території, і після запиту про екстрадицію не передається іншій Стороні лише на підставі його громадянства.

4. Ця Конвенція не виключає будь-якої кримінальної юрисдикції, яка здійснюється Стороною відповідно до її внутрішньодержавного законодавства.

5. Якщо більш ніж одна Сторона заявляє про юрисдикцію стосовно підозрюваного правопорушення, встановленого відповідно до цієї Конвенції, заінтересовані Сторони, де це можливо, проводять консультації з метою визначення найбільш придатної для переслідування юрисдикції.

РОЗДІЛ III – МІЖНАРОДНЕ СПІВРОБІТНИЦТВО

Частина 1 – Загальні принципи

Заголовок 1 – Загальні принципи міжнародного співробітництва

Стаття 23 – Загальні принципи міжнародного співробітництва

Сторони співробітничають між собою у найширших обсягах відповідно до принципів цього розділу шляхом застосування відповідних міжнародних документів щодо міжнародного співробітництва у кримінальних питаннях, угод, укладених на основі єдиного чи взаємного законодавства, і внутрішньодержавного законодавства, з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними або з метою збирання доказів у електронній формі, які стосуються кримінальних правопорушень.

Заголовок 2 – Принципи екстрадиції

Стаття 24 – Екстрадиція

1. ▸ a. Ця стаття застосовується до екстрадиції, що має місце між Сторонами у зв'язку з кримінальними правопорушеннями, встановленими відповідно до статей 2-11 цієї Конвенції, за умови, що вони підлягають покаранню позбавленням волі, максимальний строк якого складає щонайменше один рік, або більш суворому покаранню, відповідно до законодавства обох заінтересованих Сторін.

▸ b. У випадках, коли відповідно до домовленості, укладеної на основі єдиного чи взаємного законодавства, або договору про екстрадицію, включаючи Європейську Конвенцію про екстрадицію (ETS № 24), які застосовуються між двома або більше сторонами, має застосовуватися різне мінімальне покарання, застосовується мінімальне покарання відповідно до такої домовленості чи угоди.

2. Кримінальні правопорушення, описані у пункті 1 цієї статті, вважаються такими, що включаються як правопорушення, які спричиняють екстрадицію, до будь-якої угоди про екстрадицію, яка існує між Сторонами. Сторони зобов'язуються включати такі правопорушення, як такі, що спричиняють екстрадицію, до будь-якого договору про екстрадицію, який буде укладено між ними.

3. Якщо Сторона, яка здійснює екстрадицію за умови існування договору, отримує запит про екстрадицію від іншої Сторони, з якою в неї нема договору про екстрадицію, вона може вважати цю Конвенцію юридичною основою для екстрадиції відносно будь-якого кримінального правопорушення, на яке міститься посилання у пункті 1 цієї статті.

4. Сторони, які не ставлять існування договору умовою для екстрадиції, визнають для себе кримінальні правопорушення, на які міститься посилання у пункті 1 цієї статті, такими, що спричиняють екстрадицію.

5. Екстрадиція підлягає умовам, передбаченим законодавством Сторони, яку запитують про екстрадицію, або відповідними договорами про екстрадицію, включаючи підстави, на яких Сторона, яку запитують, може відмовити в екстрадиції.

6. Якщо в екстрадиції стосовно кримінального правопорушення, на яке міститься посилання у пункті 1 цієї статті, відмовлено виключно на підставі громадянства особи, стосовно якої надходить запит про екстрадицію, або тому, що Сторона, яку запитують, вважає, що вона має юрисдикцію стосовно такого правопорушення, Сторона, яку запитують, на запит Сторони, яка запитує, надсилає справу своїм компетентним органам з метою переслідування правопорушення, і належним чином повідомляє його результат Стороні, яка запитує. Такі органи приймають свої рішення і проводять свої розслідування і переслідування таким же чином, як і у випадку будь-якого іншого правопорушення подібної природи відповідно до законодавства такої Сторони.

7. ▸ a. Кожна Сторона під час підписання або передачі на зберігання своєї ратифікаційної грамоти або документа про прийняття, схвалення чи приєднання повідомляє Генеральному секретарю Ради Європи назви і адреси усіх компетентних органів, які відповідають за надсилання чи отримання запитів про екстрадицію або тимчасовий арешт у випадку відсутності договору.

▸ b. Генеральний секретар Ради Європи створює і вносить відповідні зміни у реєстр компетентних органів, відповідно призначених Сторо-

нами. Кожна Сторона забезпечує правильність відомостей, які містяться у такому реєстрі.

Заголовок 3 – Загальні принципи взаємної допомоги

Стаття 25 – Загальні принципи взаємної допомоги

1. Сторони надають одна іншій взаємну допомогу у найширшому обсязі з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі щодо кримінального правопорушення.

2. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для виконання зобов'язань, що містяться у статтях 27-35.

3. Кожна Сторона за надзвичайних умов може зробити запит про взаємну допомогу або про повідомлення, пов'язані з такою допомогою, які здійснюються терміновими засобами комунікації, включаючи факс і електронну пошту, у тому обсязі, в якому такі засоби комунікацій можуть забезпечити належні форми безпеки і підтвердження достовірності (включаючи використання кодування, де це необхідно), за яким має слідувати формальне підтвердження, якщо таке вимагається Стороною, яку запитують. Сторона, яку запитують, приймає і відповідає на запит шляхом будь-якого з таких термінових засобів комунікації.

4. Якщо інше не передбачене статтями цього розділу, взаємна допомога надається відповідно до законодавства Сторони, яку запитують, або до відповідних договорів про взаємну допомогу, включаючи підстави, на яких Сторона, яку запитують, може відмовити у співробітництві. Сторона, яку запитують, не використовує право відмовити у взаємній допомозі відносно правопорушень, які містяться у статтях 2-11, тільки на підставі того, що запит стосується правопорушення, яке вона вважає фіскальним правопорушенням.

5. У разі, якщо відповідно до положень цього розділу, Стороні, яку запитують, дозволяється надавати взаємну допомогу за умови існування подвійного визнання правопорушення, ця умова вважається виконаною, незалежно від того, чи відносить її законодавство таке правопорушення до тієї ж категорії правопорушень або визначає його тією ж термінологією, як і Сторона, яка запитує, у разі, якщо поведінка, яка визначає правопорушення, стосовно якого запитується допомога, є кримінальним правопорушенням відповідно до законодавства Сторони, яку запитують.

Стаття 26 – Добровільно надана інформація

1. Сторона може в рамках свого законодавства без попереднього запиту надіслати іншій Стороні інформацію, отриману в ході її власного розслідування, якщо вона вважає, що розкриття такої інформації може допомог-

ти Стороні, яка отримує інформацію, у відкритті або проведенні розслідування чи переслідування стосовно кримінальних злочинів, встановлених відповідно до цієї Конвенції або може спричинити запит про співробітництво від такої Сторони відповідно до цього розділу.

2. До надання такої інформації Сторона, яка надає інформацію, може вимагати, щоб вона залишалася конфіденційною або використовувалася за певних умов. Якщо Сторона, яка отримує інформацію, не може задовольнити вимоги такого запиту, вона повідомляє про це Сторону, яка надає інформацію, яка після цього визначає, чи надавати інформацію, незважаючи на це. Якщо Сторона, яка отримує інформацію, приймає її за певних умов, вона має їх дотримуватися.

Заголовок 4 – Процедури, пов'язані із запитами про взаємну допомогу у разі відсутності відповідних міжнародних угод

Стаття 27 – Процедури, пов'язані із запитами про взаємну допомогу у разі відсутності відповідних міжнародних угод

1. У разі відсутності між Стороною, яка запитує, і Стороною, яку запитують, чинних договорів про взаємну допомогу чи угод на основі єдиного чи взаємного законодавства, застосовуються положення пунктів 2-10 цієї статті. Положення цієї статті не застосовуються у разі наявності такого договору, угоди або законодавства, якщо тільки заінтересовані Сторони не погоджуються застосовувати замість них, частково або повністю, нижчевикладені положення цієї статті.

2. ▸ a. Кожна Сторона призначає центральний уповноважений орган або органи, які відповідають за надсилання та відповідь на запити про взаємну допомогу, виконання таких запитів або їх передачу уповноваженим органам, компетентним виконувати їх.

   ▸ b. Ці центральні уповноважені органи здійснюють прямі зносини між собою.

   ▸ c. Кожна Сторона під час підписання або передачі на зберігання ратифікаційної грамоти або документа про прийняття, схвалення чи приєднання повідомляє Генеральному секретарю Ради Європи назви і адреси усіх компетентних органів, призначених відповідно до цього пункту.

   ▸ d. Генеральний секретар Ради Європи створює і вносить відповідні зміни у реєстр компетентних органів, відповідно призначених Сторонами. Кожна Сторона забезпечує правильність відомостей, які містяться у такому реєстрі.

3. Запити про взаємну допомогу відповідно до цієї статті здійснюються згідно процедур, зазначених Стороною, яка запитує, якщо тільки вони не суперечать законодавству Сторони, яку запитують.

4. Сторона, яку запитують, може, на додаток до підстав для відмови, передбачених у пункті 4 статті 25, відмовити у допомозі, якщо:

- a. запит стосується правопорушення, яке Сторона, яку запитують, вважає політичним правопорушенням або правопорушенням, пов'язаним з політичним правопорушенням; або

- b. вона вважає, що виконання запиту може зашкодити її суверенітету, безпеці, суспільному порядку або іншим важливим інтересам.

5. Сторона, яку запитують, може відкласти свої дії щодо запиту, якщо такі дії можуть зашкодити кримінальному розслідуванню чи переслідуванню, яке здійснюється її уповноваженими органами.

6. До відмови або відкладення допомоги Сторона, яку запитують, після консультацій з Стороною, яка запитує, розгляне, якщо це доречно, можливість часткового задоволення запиту або його задоволення за умов, які вона вважає доречними.

7. Сторона, яку запитують, терміново інформує Сторону, яка запитує, про результат виконання запиту про допомогу. Якщо у допомозі відмовлено чи вона відкладена, надаються причини відмови чи відкладення. Сторона, яку запитують, також інформує Сторону, яка запитує, про будь-які причини, які унеможливлюють виконання запиту або можуть значною мірою затримати його виконання.

8. Сторона, яка запитує, може вимагати від Сторони, яку запитують, зберігати конфіденційним факт і зміст будь-якого запиту, зробленого відповідно до цього розділу, за винятком того обсягу, який є необхідним для виконання запиту. Якщо Сторона, яку запитують, не може виконати запит за умов його конфіденційності, вона терміново інформує про це Сторону, яка запитує, яка після цього визначає, чи необхідно виконати запит, незважаючи на це.

9. - a. У термінових випадках запити про взаємну допомогу або про повідомлення, пов'язані з нею, можуть надсилатися безпосередньо судовими органами Сторони, яка запитує, до відповідних органів Сторони, яку запитують. В будь-якому такому випадку копія одночасно надсилається центральному уповноваженому органу Сторони, яку запитують, через центральний уповноважений орган Сторони, яка запитує.

   - b. Будь-який запит або повідомлення відповідно до цього пункту може здійснюватися через Міжнародну організацію кримінальної поліції (Інтерпол).

   - c. Якщо запит здійснено відповідно до підпункту a. цієї статті, і орган не має компетенції розглядати такий запит, він передає запит до компетентного національного органу, і безпосередньо повідомляє про це Сторону, яка запитує.

- d. Запити або повідомлення, здійснені відповідно до цього пункту, які не стосуються примусових дій, можуть передаватися безпосередньо компетентними органами Сторони, яка запитує, компетентним органам Сторони, яку запитують.

- e. Кожна Сторона під час підписання або передачі на зберігання ратифікаційної грамоти або документа про прийняття, схвалення чи приєднання може повідомити Генерального секретаря Ради Європи про те, що з метою ефективності усі запити відповідно до цього пункту мають надсилатися її центральному органу.

Стаття 28 – Конфіденційність і обмеження у використанні

1. У разі відсутності між Стороною, яка запитує, і Стороною, яку запитують, чинних договорів про взаємну допомогу чи угод на основі єдиного чи взаємного законодавства, застосовуються положення цієї статті. Положення цієї статті не застосовуються у разі наявності такого договору, угоди або законодавства, якщо тільки зацікавлені Сторони не погоджуються застосовувати замість них, частково або повністю, нижчевикладені положення цієї статті.

2. Сторона, яку запитують, може ставити умовою для надання інформації або матеріалів у відповідь на запит, вимогу, що таке надання інформації:

   - a. залишиться конфіденційним, якщо запит про взаємну правову допомогу не можна було б виконати за відсутності такої умови, або

   - b. не використовуватиметься для розслідувань або переслідувань, що не зазначені у запиті.

3. Якщо Сторона, яка запитує, не може виконати умову, що міститься у пункті 2, вона терміново інформує про це іншу Сторону, яка після цього визначає, чи може інформація бути надана, незважаючи на це. Якщо Сторона, яка запитує, приймає умову, вона є обов'язковою для неї.

4. Будь-яка Сторона, яка надає інформацію або матеріали за умови, що міститься у пункті 2, може вимагати, щоб інша Сторона надала пояснення про використання такої інформації у зв'язку із такою умовою.

Частина 2 – Конкретні принципи

Заголовок 1 – Взаємна допомога щодо тимчасових заходів

Стаття 29 – Термінове збереження комп'ютерних даних, які зберігаються

1. Сторона може запитати іншу Сторону видати ордер чи іншим чином провести термінове збереження комп'ютерних даних, які зберігаються за допомогою комп'ютерної системи, яка знаходиться на території такої іншої Сторони, і відносно якої Сторона, яка запитує, має намір надіслати запит про взаємну допомогу щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких даних.

2. У запиті про збереження відповідно до пункту 1 зазначається:

- a. компетентний орган, який робить запит про збереження;
- b. правопорушення, яке підлягає кримінальному розслідуванню або переслідуванню, і короткий опис відповідних фактів;
- c. комп'ютерні дані, які необхідно зберегти, та їх зв'язок з правопорушенням;
- d. будь-яка доступна інформація для ідентифікації особи, яка зберігає такі комп'ютерні дані, або розташування комп'ютерної системи;
- e. необхідність збереження; та
- f. положення про те, що така Сторона має намір надіслати запит про взаємну допомогу щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких комп'ютерних даних, які зберігаються.

3. Після отримання запиту від іншої Сторони, Сторона, яку запитують, вживає усіх належних заходів для термінового збереження зазначених даних відповідно до її внутрішньодержавного законодавства. Для цілей відповіді на запит, подвійне визнання правопорушення не вимагається як підстава для проведення такого збереження.

4. Сторона, яка вимагає подвійне визнання правопорушення як умову виконання запиту про взаємну допомогу щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких даних, може відносно правопорушень, які не є правопорушеннями, встановленими статтями 2-11 цієї Конвенції, зберегти за собою право відмовити у виконанні запиту про збереження відповідно до цієї статті у випадках, коли вона має підстави вважати, що на час розголошення умову щодо подвійного визнання правопорушення не можна задовольнити.

5. На додаток до цього, у виконанні запиту про збереження можна відмовити лише у випадках, коли:
   - a. запит стосується правопорушення, яке Сторона, яку запитують, вважає політичним правопорушенням або правопорушенням, пов'язаним з політичним правопорушенням; або
   - b. Сторона, яку запитують, вважає, що виконання запиту може зашкодити її суверенітету, безпеці, суспільному порядку або іншим важливим інтересам.

6. Якщо Сторона, яку запитують, вважає, що таке збереження не забезпечить майбутню доступність даних або загрожуватиме їх конфіденційності чи іншим чином зашкодить розслідуванню, яке проводить Сторона, яка запи-

тує, вона терміново інформує про це Сторону, яка запитує. Після цього остання визначає, чи необхідно виконувати запит, незважаючи на це.

7. Будь-яке збереження, проведене у відповідь на запит відповідно до пункту 1, продовжується не менше ніж 60 днів, для того, щоб надати можливість Стороні, яка запитує, надіслати запит щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких даних. Після отримання такого запиту, дані зберігаються до винесення рішення стосовно такого запиту.

Стаття 30 – Термінове розкриття збережених даних про рух інформації

1. Якщо в ході виконання запиту, зробленого відповідно до статті 29, щодо збереження даних про рух інформації, які стосуються конкретної передачі інформації, Стороні, яку запитують, стає відомо, що постачальник послуг в іншій Державі був залучений до передачі такої інформації, Сторона, яку запитують, терміново повідомляє Стороні, яка запитує, обсяг інформації про рух даних, достатній для ідентифікації такого постачальника послуг і шляху передачі такої інформації.

2. У розкритті інформації про рух даних відповідно до пункту 1 може бути відмовлено тільки якщо:

   - a. запит стосується правопорушення, яке Сторона, яку запитують, вважає політичним правопорушенням або правопорушенням, пов'язаним з політичним правопорушенням; або

   - b. Сторона, яку запитують, вважає, що виконання запиту може зашкодити її суверенітету, безпеці, суспільному порядку або іншим важливим інтересам.

Заголовок 2 – Взаємна допомога щодо повноважень на розслідування

Стаття 31 – Взаємна допомога щодо доступу до комп'ютерних даних, які зберігаються

1. Будь-яка Сторона може запитати іншу Сторону провести обшук чи подібний доступ, арешт чи подібні дії або розголошення даних, які зберігаються за допомогою комп'ютерної системи, яка знаходиться на території Сторони, яку запитують, включаючи дані, збережені відповідно до статті 29.

2. Сторона, яку запитують, відповідає на запит шляхом застосування відповідних міжнародних документів, угод і законодавства, на які містяться посилання у статті 23, а також відповідно до інших положень цього розділу.

3. На запит надається термінова відповідь, якщо:

   - a. існують підстави вважати, що відповідні дані особливо вразливі для втрати або змін; або

   - b. документи, угоди і законодавство, на які містяться посилання у пункті 2, передбачають термінове співробітництво.

Стаття 32 – Транскордонний доступ до комп'ютерних даних, які зберігаються, за згодою або у випадку, коли вони є публічно доступними

Будь-яка Сторона може, не отримуючи дозвіл іншої Сторони:

- a. здійснювати доступ до публічно доступних (відкрите джерело) комп'ютерних даних, які зберігаються, незважаючи на те, де такі дані знаходяться географічно; або

- b. здійснювати доступ або отримувати за допомогою комп'ютерної системи, яка знаходиться на її території, комп'ютерні дані, які зберігаються і знаходяться в іншій Стороні, якщо Сторона отримує законну і добровільну згоду особи, яка має законні повноваження розкривати дані такій Стороні за допомогою такої комп'ютерної системи.

Стаття 33 – Взаємна допомога у збиранні даних про рух інформації у реальному масштабі часу

1. Сторони надають взаємну допомогу одна одній у збиранні даних про рух інформації у реальному масштабі часу, пов'язаних із зазначеною передачею інформації на їх території, яка передається за допомогою комп'ютерної системи. Відповідно до положень пункту 2, ця допомога регулюється умовами і процедурами, які передбачені внутрішньодержавним законодавством.

2. Кожна Сторона надає таку допомогу щонайменше відносно кримінальних правопорушень, стосовно яких проводиться збирання даних про рух інформації у реальному масштабі часу у випадку подібної внутрішньодержавної справи.

Стаття 34 – Взаємна допомога у перехопленні даних змісту інформації

Сторони надають взаємну допомогу одна одній у збиранні або записі у реальному масштабі часу даних змісту інформації у зазначених передачах інформації, які здійснюються за допомогою комп'ютерної системи, у обсягах, які дозволяються відповідними договорами між ними і внутрішньодержавним законодавством.

Заголовок 3 – Цілодобова мережа
Стаття 35 – Цілодобова мережа

1. Кожна Сторона призначає орган для здійснення контактів цілодобово впродовж тижня з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення. Така допомога включає сприяння або, якщо це дозволяється її внутрішньодержавним законодавством і практикою, пряме:

- a. надання технічних порад;
- b. збереження даних відповідно до статей 29 і 30; та
- c. збирання доказів, надання юридичної інформації і встановлення місцезнаходження підозрюваних.

2. - a. Орган Сторони, визначений нею для здійснення контактів, має можливість терміново встановлювати контакт з органом іншої Сторони, визначеним нею для здійснення контактів.
   - b. Якщо орган Сторони, визначений нею для здійснення контактів, не є частиною уповноваженого органу або органів такої Сторони, які відповідають за міжнародну взаємну допомогу або екстрадицію, то орган, визначений для здійснення контактів, забезпечує свою здатність проводити термінову координацію з таким уповноваженим органом або органами.
3. Кожна Сторона забезпечує кваліфікований персонал і відповідне обладнання для сприяння роботі мережі.

РОЗДІЛ IV – ПРИКІНЦЕВІ ПОЛОЖЕННЯ

Стаття 36 – Підписання та набуття чинності

1. Ця Конвенція відкрита для підписання державами-членами Ради Європи та державами, які не є членами Ради Європи, але брали участь у її розробці.
2. Ця Конвенція підлягає ратифікації, прийняттю або схваленню. Ратифікаційні грамоти або документи про прийняття або схвалення передаються на зберігання Генеральному секретарю Ради Європи.
3. Ця Конвенція набуває чинності в перший день місяця, який наступає після закінчення тримісячного періоду від дати, на яку п'ять держав, серед яких принаймні три держави-члена Ради Європи, висловлять свою згоду на обов'язковість для них цієї Конвенції згідно з положеннями пунктів 1 та 2.
4. Для будь-якої держави, яка підписала Конвенцію та згодом висловила згоду на її обов'язковість для себе, ця Конвенція набуває чинності в перший день місяця, який наступає після закінчення тримісячного періоду від дати висловлення такою державою згоди на обов'язковість для неї цієї Конвенції згідно з положеннями пунктів 1 та 2.

Стаття 37 – Приєднання до Конвенції

1. Після набуття чинності цією Конвенцією, Комітет Міністрів Ради Європи, після консультацій з державами, які є Сторонами цієї Конвенції, та отримання їхньої одностайної згоди, може запросити будь-яку державу, яка не є членом Ради та не брала участь у розробці цієї Конвенції, приєднатися до неї. Таке рішення ухвалюється більшістю, передбаченою у статті 20.d Статуту Ради Європи, та одностайним голосуванням представників Договірних держав, які мають право брати участь у засіданнях Комітету Міністрів.

2. Для будь-якої держави, яка приєднується до Конвенції відповідно до пункту 1 вище, Конвенція набуває чинності в перший день місяця, який наступає після закінчення тримісячного періоду від дати здачі на зберігання документа про приєднання Генеральному секретарю Ради Європи.

Стаття 38 – Територіальне застосування

1. Будь-яка держава під час підписання або здачі на зберігання своєї ратифікаційної грамоти або документа про прийняття, схвалення або приєднання може визначити територію або території, до яких застосовуватиметься ця Конвенція.

2. Будь-яка держава у будь-який пізніший час шляхом направлення заяви на ім'я Генерального секретаря Ради Європи може поширити дію цієї Конвенції на будь-яку іншу територію, визначену в заяві. Для такої території Конвенція набуває чинності в перший день місяця, який наступає після закінчення тримісячного періоду від дня одержання заяви Генеральним секретарем.

3. Будь-яка заява, зроблена згідно з двома попередніми пунктами щодо будь-якої території, визначеної у такій заяві, може бути відкликана шляхом направлення повідомлення Генеральному секретарю Ради Європи. Відкликання набуває чинності в перший день місяця, який наступає після закінчення тримісячного періоду від дати отримання такого повідомлення Генеральним секретарем.

Стаття 39 – Цілі Конвенції

1. Мета цієї Конвенції полягає у доповненні застосовних двосторонніх або багатосторонніх договорів або домовленостей між Сторонами, зокрема положень:

   - Європейської конвенції про екстрадицію, відкритої для підписання у Парижі 13 грудня 1957 року (ETS № 24);
   - Європейської конвенції про взаємну допомогу у кримінальних справах, відкриту для підписання у Страсбурзі 20 квітня 1959 року (ETS № 30);
   - Додаткового протоколу до Європейської конвенції про взаємну допомогу у кримінальних справах, відкритого для підписання у Страсбурзі 17 березня 1978 року (ETS № 99).

2. Якщо дві або більше Сторони вже уклали угоду або договір щодо питань, які регулюються цією Конвенцією, або іншим чином встановили відносини з таких питань, або якщо вони роблять це у майбутньому, вони також матимуть право застосовувати таку угоду або договір або відповідно регулювати такі відносини. Однак у разі, якщо Сторони встановлюють свої відносини щодо питань, які регулюються цією Конвенцією, в інший

спосіб, ніж передбачається нею, вони роблять це у такий спосіб, що не суперечить цілям та принципам Конвенції.

3. Ніщо в цій Конвенції не зачіпає інших прав, обмежень, зобов'язань та відповідальності Сторони.

Стаття 40 – Заяви

Шляхом направлення письмового повідомлення на ім'я Генерального секретаря Ради Європи будь-яка держава під час підписання або здачі на зберігання своєї ратифікаційної грамоти або документа про прийняття, схвалення або приєднання може заявити, що вона користується можливістю вимагати додаткові елементи, передбачені згідно зі статтями 2 та 3, пунктом 1.b статті 6, статтею 7, пунктом 3 статті 9 та пунктом 9.e статті 27.

Стаття 41 – Клаузула щодо федеральних держав

1. Федеральна держава може залишити за собою право брати на себе зобов'язання, передбачені у розділі II цієї Конвенції, відповідно до її основних принципів регулювання відносин між центральним урядом та штатами, що входять до складу федерації, або іншими подібними територіальними одиницями за умови, що вона все-таки спроможна співпрацювати відповідно до розділу III.

2. Роблячи застереження відповідно до пункту 1, федеральна держава не може застосовувати умови такого застереження для того, щоб виключити або значно зменшити свої зобов'язання щодо передбачення заходів, встановлених у розділі II. Загалом вона забезпечує широкі та ефективні правоохоронні можливості щодо таких заходів.

3. Щодо положень цієї Конвенції, застосування яких входить до юрисдикції штатів, що утворюють федерацію, або інших подібних територіальних одиниць, які згідно з конституційною системою федерації не зобов'язані вживати законодавчих заходів, федеральний уряд інформує компетентні органи таких штатів про згадані положення, висловлюючи свою схвальну думку, та заохочує їх до вжиття відповідних заходів для введення в дію таких положень.

Стаття 42 – Застереження

Шляхом направлення письмового повідомлення на ім'я Генерального секретаря Ради Європи будь-яка держава під час підписання або здачі на зберігання своєї ратифікаційної грамоти або документа про прийняття, схвалення або приєднання може заявити, що вона користується застереженням(и), передбаченим(и) у пункті 2 статті 4, пункті 3 статті 6, пункті 4 статті 9, пункті 3 статті 10, пункті 3 статті 11, пункті 3 статті 14, пункті 2 статті 22, пункті 4 статті 29 та пункті 1 статті 41. Не може бути зроблено жодних інших застережень.

Стаття 43 – Статус та відкликання застережень

1. Будь-яка Сторона, яка зробила застереження відповідно до статті 42, може повністю або частково відкликати його, направивши повідомлення на ім'я

Генерального секретаря. Таке відкликання набуває чинності в день отримання такого повідомлення Генеральним секретарем. Якщо у повідомленні зазначається, що відкликання застереження має набути чинності у визначений у повідомленні день, та така дата є пізнішою, ніж дата отримання повідомлення Генеральним секретарем, відкликання набуває чинності у такий пізніший день.

2. Сторона, яка зробила застереження, згадане у статті 42, відкликає таке застереження повністю або частково, як тільки це дозволяють обставини.

3. Генеральний секретар Ради Європи може періодично запитувати Сторони, які зробили одне або декілька застережень, згаданих у статті 42, про можливості відкликання такого застереження (таких застережень).

Стаття 44 – Зміни

1. Зміни до цієї Конвенції можуть пропонуватися будь-якою Стороною; вони направляються Генеральним секретарем Ради Європи державам-членам Ради Європи, а також державам, які не є членами Ради Європи, але брали участь у її розробці, та всім державам, які приєдналися або були запрошені приєднатися до цієї Конвенції згідно з положеннями статті 37.

2. Будь-яка зміна, запропонована Стороною, передається до Європейського комітету з проблем злочинності (ЄКПЗ), який надає Комітетові Міністрів свою думку щодо такої запропонованої зміни.

3. Комітет Міністрів розглядає запропоновану зміну і думку, представлену ЄКПЗ, та після консультацій з державами, які не є членами Ради Європи, але є Сторонами цієї Конвенції, може прийняти зміну.

4. Текст будь-якої зміни, прийнятої Комітетом Міністрів згідно з пунктом 3 цієї статті, направляється Сторонам для прийняття.

5. Будь-яка зміна, прийнята відповідно до пункту 3 цієї статті, набуває чинності після того, як всі Сторони повідомлять Генерального секретаря про їх прийняття.

Стаття 45 – Вирішення спорів

1. Європейський комітет з проблем злочинності (ЄКПЗ) інформується про тлумачення та застосування цієї Конвенції.

2. У разі спору між Сторонами щодо тлумачення або застосування цієї Конвенції, вони намагаються вирішити спір шляхом переговорів або будь-яких інших мирних засобів на свій вибір, включаючи подання спору до ЄКПЗ, до арбітражного суду, рішення якого є обов'язковим для виконання Сторонами, або до Міжнародного суду, за домовленістю заінтересованих Сторін.

Стаття 46 – Консультації Сторін

1. Сторони у разі необхідності періодично консультуються з метою сприяння:

   - a. ефективному використанню та застосуванню цієї Конвенції, включаючи виявлення будь-яких її проблематичних питань, а також наслідків будь-якої заяви або застереження, зробленого згідно з цією Конвенцією;
   - b. обміну інформацією про суттєві зміни у галузі права, політики або технології, що стосуються кіберзлочинності, та збору інформації в електронній формі;
   - c. розгляду можливих додатків або змін до цієї Конвенції.

2. Європейський комітет з проблем злочинності (ЄКПЗ) регулярно інформується про результати консультацій, згаданих у пункті 1.

3. ЄКПЗ у разі необхідності сприяє проведенню консультацій, згаданих у пункті 1, та вживає необхідних заходів для надання допомоги Сторонам у їхніх зусиллях щодо внесення змін або доповнень до Конвенції. Щонайпізніше через три роки після набуття чинності цією Конвенцією Європейський комітет з проблем злочинності (ЄКПЗ) у співпраці зі Сторонами проводить перегляд усіх положень Конвенції та, у разі необхідності, пропонує будь-які відповідні зміни.

4. Витрати, пов'язані з виконанням положень пункту 1, сплачуються Сторонами у визначений ними спосіб, крім випадків, коли такі витрати сплачуються Радою Європи.

5. Секретаріат Ради Європи допомагає Сторонам у виконанні ними їхніх функцій за цією статтею.

Стаття 47 – Денонсація

1. Будь-яка Сторона може в будь-який час денонсувати цю Конвенцію шляхом направлення письмового повідомлення Генеральному секретарю Ради Європи.

2. Така денонсація набуває чинності в перший день місяця, який наступає після завершення тримісячного періоду від дня отримання повідомлення Генеральним секретарем.

Стаття 48 – Повідомлення

Генеральний секретар Ради Європи повідомляє держави-члени Ради Європи та держави, які не є членами Ради Європи, але брали участь у розробці цієї Конвенції, а також всі держави, які приєдналися або були запрошені приєднатися до цієї Конвенції, про:

- a. будь-яке підписання;
- b. здачу на зберігання будь-якої ратифікаційної грамоти або документа про прийняття, схвалення або приєднання;

- c. будь-яку дату набуття чинності цією Конвенцією відповідно до статей 36 і 37;

- d. будь-яку заяву, зроблену відповідно до статті 40, або застереження, зроблене відповідно до статті 42;

- e. будь-який інший акт, повідомлення або інформацію, що стосується цієї Конвенції.

На посвідчення чого нижчепідписані, належним чином на це уповноважені представники підписали цю Конвенцію.

Вчинено в Будапешті 23 листопада 2001 року англійською та французькою мовами, причому обидва тексти є рівно автентичними, в одному примірнику, який зберігатиметься в архівах Ради Європи. Генеральний секретар Ради Європи надсилає завірені копії цієї Конвенції кожній державі-члену Ради Європи, державам, які не є членами Ради Європи, але брали участь у розробці цієї Конвенції, а також будь-якій державі, запрошеній приєднатися до неї.

Настанова T-CY № 9[1]

Аспекти втручання у вибори за допомогою комп'ютерних систем, охоплені Будапештською конвенцією

Ухвалена Комітетом з питань Конвенції про кіберзлочинність (T-CY) на його 21-ому засіданні 8 липня 2019 року

1. ВСТУП

Комітет із питань Конвенції про кіберзлочинність (T-CY) на своєму 8-му пленарному засіданні (грудень 2012 року) постановив видати Настанови, спрямовані на сприяння ефективному використанню та реалізації положень Будапештської конвенції про кіберзлочинність, зокрема в світлі правових, політичних і технологічних нововведень[2].

Настанова відображає спільне розуміння Сторін цього договору щодо застосування Конвенції.

Втручання у вибори через зловмисну кібердіяльність, спрямовану проти комп'ютерів і даних, що використовуються у виборах і виборчих кампаніях, підриває вільні, чесні й чисті вибори та довіру до демократії. Дії з дезінформації, як це, зокрема, спостерігалося після 2016 року, можуть використовувати зловмисну кібердіяльність і мати аналогічний ефект. Може виникнути потреба адаптувати національні виборчі процедури до реалій інформаційного суспільства, а комп'ютерні системи, що використовуються під час виборів і пов'язаних із ними кампаній, зробити більш захищеними.

У цьому контексті потрібно докладати більше зусиль, щоб притягати до відповідальності за таке втручання, якщо воно становить кримінальне правопорушення: ефективне реагування кримінальної юстиції здатне стримати від втручання у вибори та заспокоїти виборців щодо використання інформаційно-комунікаційних технологій у виборах.

У цій Настанові розглянуто, як саме статті Конвенції можуть бути застосовані до різних аспектів втручання у вибори за допомогою комп'ютерних систем.

1. Оригінал тексту доступний на веб-сторінці за посиланням: www.coe.int/TCY.
2. Див. повноваження T-CY (стаття 46 Будапештської конвенції).

Передбачені Конвенцією суттєві кримінальні правопорушення можуть вчинятися як дії з втручання у вибори або як підготовчі дії, що сприяють такому втручанню.

Крім того, для проведення розслідувань та притягнення до відповідальності за втручання у вибори існують національні процесуальні та міжнародні інструменти взаємної правової допомоги, надані Конвенцією. Обсяг і межі процесуальних повноважень та інструментів міжнародного співробітництва визначаються статтями 14.2 і 25.1 Будапештської конвенції:

Стаття 14.2

2. За винятком обставин, конкретно передбачених статтею 21, кожна Сторона застосовує повноваження і процедури, передбачені у пункті 1 цієї статті, до:

   - a. кримінальних правопорушень, встановлених відповідно до статей 2-11 цієї Конвенції;
   - b. інших кримінальних правопорушень, вчинених за допомогою комп'ютерних систем; та
   - c. збору доказів у електронній формі щодо кримінального правопорушення.

Стаття 25.1

Сторони надають одна другій взаємну допомогу в найширшому обсязі з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі щодо кримінального правопорушення.

На передбачені Конвенцією процесуальні повноваження поширюються умови та запобіжники, встановлені статтею 15.

2. ВІДПОВІДНІ ПОЛОЖЕННЯ БУДАПЕШТСЬКОЇ КОНВЕНЦІЇ ПРО КІБЕРЗЛОЧИННІСТЬ (ETS № 185)

2.1. Процесуальні положення

Процесуальні повноваження, передбачені Конвенцією (статті 14-21), можуть бути застосовані в конкретному кримінальному розслідуванні або провадженні за фактом втручання у вибори будь-якого типу, як це встановлено статтею 14.

Спеціальні процесуальні заходи можуть бути дуже корисними під час кримінального розслідування втручання у вибори. Наприклад, у випадках втручання у вибори комп'ютерна система може бути використана для вчинення чи сприяння у вчиненні злочину; докази цього злочину можуть зберігатися в електронному вигляді, або підозрюваного можна ідентифікувати через абонентські дані, зокрема й за адресою інтернет-протоколу. Так само протиправне політичне фінансування можна простежити через збережені електронні повідомлення; відповідно, голосове спілкування між змовниками можна зафіксувати через належним чином дозволене перехоп-

лення, а зловживання даними можна засвідчити за допомогою електронних слідів.

Отже, при кримінальному розслідуванні щодо втручання у вибори, Сторони можуть скористатися терміновим збереженням записаних комп'ютерних даних, судовими наказами про надання інформації, пошуком і вилученням наявних комп'ютерних даних, а також іншими інструментами збирання електронних доказів, потрібних у розслідуванні та притягненні до відповідальності за вчинення злочинів, пов'язаних із втручанням у вибори.

2.2. Положення про взаємну міжнародну правову допомогу

Передбачені Конвенцією повноваження щодо міжнародного співробітництва (статті 23-35) охоплюють аналогічні питання й здатні допомогти Сторонам в розслідуванні втручання у вибори.

Отже, Сторони повинні забезпечувати можливість термінового збереження записаних комп'ютерних даних, видання судових наказів про надання інформації, пошук та вилучення наявних комп'ютерних даних, а також вчинення інших дій у рамках міжнародного співробітництва.

2.3. Матеріальні норми кримінального права

Насамкінець, як зазначалося вище, втручання у вибори може бути пов'язане з зазначеними нижче видами протиправної поведінки, криміналізованими Конвенцією про кіберзлочинність. Комітет Т-СУ підкреслює, що наведене нижче є лише прикладами; тобто, оскільки втручання вибори – це феномен, що розвивається, він може виявлятися у багатьох формах, відмінних від перелічених нижче. Однак експерти комітету Т-СУ очікують, що Конвенція про кіберзлочинність достатньо гнучка, щоб стосуватися і їх.

Відповідні статті	Приклади
Стаття 2. Протиправний доступ	До комп'ютерної системи може здійснюватися протиправний доступ задля отримання чутливої чи конфіденційної інформації, що стосується кандидатів, кампаній, політичних партій або виборців.
Стаття 3. Протиправне перехоплення	Непублічне передання комп'ютерних даних до, від чи в межах комп'ютерної системи може бути протиправно перехопленим задля отримання чутливої чи конфіденційної інформації, що стосується кандидатів, кампаній, політичних партій або виборців.

Відповідні статті	Приклади
Стаття 4. Втручання у дані	Комп'ютерні дані можуть пошкоджуватися, знищуватися, псуватися, змінюватися або приховуватися задля зміни сайтів, внесення змін до баз даних виборців або маніпулювання результатами голосування, наприклад, через втручання в роботу машин для голосування.
Стаття 5. Втручання у систему	Функціонуванню комп'ютерних систем, що використовуються у виборах або кампаніях, можуть створювати перешкоди, щоб втрутитися в агітаційні повідомлення, завадити реєстрації виборців, унеможливити подання голосів або не допустити підрахунку голосів за допомогою атак типу «відмова в обслуговуванні», шкідливих програм або іншими засобами.
Стаття 6. Зловживання пристроями	Продаж, надання у використання, імпорт, розповсюдження чи інші дії, що уможливлюють отримання комп'ютерних паролів, кодів доступу чи аналогічних даних, за допомогою яких можна здійснити доступ до комп'ютерних систем, здатні сприяти втручанню у вибори, зокрема крадіжці чутливих даних у політичних кандидатів, партій чи кампаній.
Стаття 7. Підробка, пов'язана з комп'ютерами	Комп'ютерні дані (наприклад, відомості, що використовуються в базах даних виборців) можуть вводитися, змінюватися, знищуватися або приховуватися, внаслідок чого до уваги беруть неавтентичні дані або на їх підставі діють із законними цілями, начебто такі дані автентичні. Наприклад, у деяких країнах від виборчих кампаній вимагають оприлюднення їхніх фінансових джерел. Підробка комп'ютерних даних може створювати враження, нібито були оприлюднені неправильні відомості, або приховувати сумнівні джерела фінансування кампанії.
Стаття 11. Незавершені злочини, сприяння та співучасть	Злочини, визначені в договорі, спрямовані на втручання у вибори, можуть бути незавершеними; їх вчинення може здійснюватися у формі сприяння чи співучасті.
Стаття 12. Корпоративна відповідальність	Злочини, передбачені статтями 2-11 Конвенції, здійснені на вчинення втручання у вибори, можуть бути вчинені юридичними особами, які повинні нести відповідальність відповідно до статті 12.

Відповідні статті	Приклади
Стаття 13. Санкції	Злочини, передбачені Конвенцією, можуть становити загрозу для фізичних осіб і для суспільства, особливо якщо злочини спрямовані проти таких засад політичного життя, як вибори. Злочинні дії та їхні наслідки можуть бути різними в різних країнах, однак втручання у вибори здатне підірвати довіру до демократичних процесів, змінити результати виборів, спричиняти видатки і потрясіння у зв'язку з повторними виборами або призводити до фізичного насильства між прихильниками зацікавлених учасників виборів та їх спільнотами. Сторона може передбачати у своєму внутрішньому законодавстві надмірно м'яке покарання за пов'язані з виборами дії, що передбачені статтями 2-11, а також може не дозволяти розгляду обтяжувальних обставин або спроб, допомоги чи співучасті. Це може означати, що Сторони повинні будуть розглянути зміни до свого внутрішнього законодавства. Відповідно до статті 13 Сторони повинні забезпечити, аби кримінальні правопорушення, пов'язані з такими діями, «каралися ефективними, пропорційними і переконливими санкціями, включаючи позбавлення волі». Сторони можуть також розглядати обтяжувальні обставини, наприклад, якщо такі дії суттєво впливають на вибори, або спричинюють смерть чи тілесні пошкодження, або значну матеріальну шкоду.

3. ЗАЯВА Т-CY

Т-CY погоджується з тим, що матеріальними злочинами у сенсі Конвенції можуть також бути дії із втручання у вибори, як це визначено чинним законодавством, тобто злочини проти вільних, чесних і чистих виборів.

Передбачені Конвенцією матеріальні злочини можуть бути вчинені задля сприяння, участі чи підготовки дій із втручання у вибори.

Процесуальні засоби та інструменти взаємної правової допомоги, надані Конвенцією, можуть використовуватися під час розслідування випадків втручання у вибори, сприяння такому втручанню, участі у ньому або підготовчих дій.

CDL-AD(2019)016

Спільна доповідь Венеційської комісії та Директорату з питань інформаційного суспільства та протидії злочинності Генерального Директорату з прав людини і верховенства права (DGI) про цифрові технології та вибори[1]

Схвалено Радою з демократичних виборів
на її 65-му засіданні (Венеція, 20 червня 2019 року)

Схвалено Венеційською комісією на її 119-ій Пленарній сесії
(Венеція, 21-22 червня 2019 року)

Підготовлено на основі коментарів експертів:
пана Річарда БАРРЕТА (член Комісії, Ірландія)
пані Гердіс КЄРУЛЬФ ТОРҐЕЙРСДОТТІР (членкиня Комісії, Ісландія)
пана Рафаеля РУБІО НУНЬЄСА (заступник члена Комісії, Іспанія)
пана Хосе Луїса ВАРҐАСА ВАЛЬДЕСА (тимчасовий член, Мексика)
пані Крістіни РОЗҐОНІ (експертка DGI, Департамент управління медіа та мережею Інтернет)
пані Невени РУЖИЧ (експертка DGI, Департамент захисту даних)

I. ВСТУП

1. На своєму 59 засіданні (15 червня 2017 року) Рада з демократичних виборів за ініціативою пана Хосе Луїса Варґаса Вальдеса, а також на основі його документа «Дослідження про роль соціальних медіа та Інтернету в демократичному розвитку» (CDL-LA(2018)001) вирішила провести дослідження щодо використання цифрових технологій під час виборчих процесів спільно з Департаментом інформаційного суспільства Ради Європи.

2. Окрім пана Варґаса Вальдеса, доповідачами були пані Гердіс Кєрульф Торґейрсдоттір, пан Річард Баррет і пан Рафаель Рубіо Нуньєс. Пані Крістіна Розґоні та пані Невена Ружич виступили експертами від імені Директорату інформаційного суспільства та протидії злочинності – Департаменту управління медіа та мережею Інтернет та Департаменту захисту даних відповідно. Пан Александр Сеґер, керівник Департаменту кіберзлочинності, також зробив свій внесок до відповідних частин цієї спільної доповіді.

3. Ця спільна доповідь була підготована на основі авторського дослідження пана Варґаса Вальдеса та коментарів, поданих доповідачами й експерта-

1. Оригінал тексту доступний на веб-сторінці за посиланням: venice.coe.int.

ми, зазначеними вище; доповідь було розглянуто на засіданні Підкомісії з питань Латинської Америки 30 листопада 2018 року, прийнято Радою з демократичних виборів на її 65 засіданні (Венеція, 20 червня 2019 року) та згодом прийнято Венеційською комісією на її 119 Пленарній сесії (Венеція, 21-22 червня 2019 року).

II. ЗАГАЛЬНІ ЗАУВАЖЕННЯ

4. Цифрові (або «нові») технології та соціальні медіа (останні варто розуміти як «інтернет-платформи, що дозволяють здійснювати двосторонню взаємодію через контент, створений користувачами»[2]) здійснили революцію у способах, якими люди взаємодіють та здійснюють свою свободу вираження поглядів й інформації, а також інші пов'язані з цими – а іноді й конфліктні з ними – основні права[3]. Люди, залучені до соціальних медіа, можуть використовувати інтернет для того, щоб створювати та вимагати кращі послуги, більшу прозорість й осмислену участь на політичній арені[4]. Індивіди в усьому світі тепер здатні формувати глобальне сприйняття, виявляти власну позицію у своєму національному порядку денному і сприяти політичній активності[5]. Така цифрова трансформація змінює відносини між державами та громадянами.

5. Відповідно до доповіді ***Global Digital*** за 2018 рік, більше ніж половина світового веб-трафіку тепер припадає на мобільні телефони. Із загальної кількості 7,6 мільярда мешканців світу приблизно 4 мільярди – це користувачі інтернету (що становить 53% від загальної кількості населення), а 3,2 мільярда – активні користувачі соціальних медіа (що становить 42% від загальної кількості населення).

6. Протягом 2017 та 2018 років кількість користувачів інтернету зросла на 7%, а активних користувачів соціальних медіа стало більше на 13%. Середньостатистичний користувач інтернету проводить в інтернеті близько 6 годин щодня. Значну частину цього часу витрачають на такі соціальні платформи, як ***Facebook*** (2 167 мільйонів користувачів), ***Youtube*** (1 500 мільйонів), ***Instagram*** (800 мільйонів) або ***Twitter*** (330 мільйонів).

2. У цьому дослідженні соціальні медіа визначено як «веб-платформи або платформи для мобільних пристроїв, що дозволяють здійснювати двосторонні взаємодії через контент, створений користувачами (*user-generated content*, UGC) та спілкування. Тому соціальні медіа не є такими засобами масової інформації, які походять лише з одного джерела або транслюються зі статичного сайту. Радше вони є медіа на певних платформах, розроблених для того, щоб користувачі мали можливість створювати («генерувати») контент та взаємодіяти з інформацією і її джерелом (International IDEA 2014: 11). Хоча соціальні медіа спираються на інтернет як на посередника, важливо зазначити, що не всі сайти чи платформи відповідають визна-ченню соціальних медіа. Деякі сайти не передбачають можливості інтерактивно спілкуватися з аудиторією, тоді як інші дозволяють користувачам лише виставляти коментарі як реакцію на певний опублікований контент у вигляді публікацій для обговорень (або «тем»), які модерують та контролюють» (International IDEA 2014: 11).

3. Парламентська Асамблея Ради Європи, Резолюція 1987 (2014) про право на доступ до інтернету.

4. Santiso, 2018.

5. Існують яскраві приклади цього: від єгипетських підлітків, які використовували *Facebook*, щоб згуртувати протестувальників на площі Тахрір, до впливу дезінформації на результат виборів президента Кенії та до чилійців, які агітували в інтернеті, щоб зробити голосування за кордоном ключовим виборчим питанням із *«Haz tu voto volar»* або проєктом перевірки фактів *«Verificado2018»* у Мексиці.

7. Сьогодні приблизно два мільярди користувачів інтернету користуються соціальними мережами[6] щодня, а соціальні медіа стали невід'ємною частиною сучасної політичної агітації, їхній вплив на громадськість залежить від багатьох чинників, таких як зміна каналів (наприклад, ***Twitter*** проти ***Instagram***), специфічні характеристики аудиторії та її схильності, мотивація користувачів і загальний контекст політичної агітації[7].

8. Хоча виглядає, що практично кожен використовує інтернет та соціальні медіа, різні вікові групи використовують їх для різних цілей. Відповідно до доповіді ***Reuters Institute Digital News Report 2017***, соціальні медіа, зазвичай, є основним джерелом новин для людей віком від 18 до 34 років, тоді як телебачення більш важливе для людей віком понад 55 років.

9. За даними того ж таки дослідження ***Reuters Institute***, більше ніж половина респондентів (54%) віддає перевагу джерелам, які використовують алгоритми для вибору повідомлень (пошукові системи, соціальні медіа та багато агрегаторів) на противагу вибору з боку редакторів чи журналістів (44%). Це означає, що молоді громадяни можуть приймати політичні рішення, ґрунтуючись на інформації, відфільтрованій за алгоритмами таких цифрових середовищ, а не поданій відповідно до строгих журналістських стандартів. Водночас треба зауважити, що відповідно до недавніх досліджень[8] персоналізовані рекомендації шляхом алгоритмічного вибору можуть надавати такі самі різноманітні новинні пропозиції, як і редакційний вибір, здійснений людиною.

10. Відповідно до доповіді ***Reuters Institute Digital News Report 2018***, використання соціальних медіа для доступу до новин у 2017 році знизилося. Здається, люди менше почали довіряти джерелам соціальних медіа. Також було зауважено, що «інтернет швидко відійшов від платформи, яку використовують здебільшого для доступу до інформації, і став учасницьким середовищем, що тісно мімікрує під традиційну у фізичному світі демократичну участь»[9]. Внаслідок цього масове використання інтернету та соціальних медіаплатформ в усьому світі змінює багато аспектів нашого соціального й політичного життя. Соціальні механізми формування знань та поглядів стають усе більш взаємно узгодженими й саморегульованими (наприклад, ***Wikipedia, Facebook***), а політична активність знайшла нові ефективні способи організації та вираження[10].

11. На початку свого існування інтернет вітали як обіцянку рівності та свободи. Його розглядали як потенційну ***нову публічну сферу***, платформу для демократичної публічної дискусії, що розширює можливість індивідам

6. Статистика: Найбільш популярні соціальні мережі світу станом на жовтень 2018 року. Доступно за посиланням: www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users.

7. Dimitrova & Matthes, 2018.

8. Див.: www.tandfonline.com/doi/abs/10.1080/1369118X.2018.1444076 та www.thatseemsimportant.com/content/blame-the-algorithm.

9. Laidlaw 2015, p. 7.

10. Castells 2011; Cohen et al. 2012.

бути активними учасниками публічного дискурсу, а отже, сприяти більш ефективній політичній демократії з освіченою громадськістю завдяки активному дискурсу в соціальних мережах. Публічна сфера була ієрархічно організованою за допомогою визначених і встановлених функцій різних гравців, як держава, засоби масової інформації, церква або навчальні заклади, які всі сьогодні втратили контроль над горизонтальним обміном новинами та поглядами користувачів. Соціальні медіа обіцяють надати голос кожному. На противагу традиційним засобам масової інформації інтернет має відкриту багатосторонню архітектуру, а витрати на доступ до нього відносно низькі. Ці риси роблять інтернет особливо ефективним засобом масової інформації для пересічного громадянина, здатного стати активним спікером замість просто отримувача інформації, і створили «мережеву публічну сферу», де індивіди можуть «контролювати та блокувати використання засобів масової інформації» завдяки миттєвому доступу до декількох джерел інформації і розповсюдження даних.

12. У минулому журналісти зі своєю редакційною практикою та етичними зобов'язаннями виконували роль вартового у процесі комунікації, не лише вирішуючи, що підходить для друку чи публікації, а й дотримуючись встановлених законодавством вимог, таких як справедливе та збалансоване висвітлення у суспільних засобах інформації, дотримання періодів тиші, коли це передбачено, та/або надання кандидатам та політичним партіям права на відповідь і рівнозначні засоби захисту. Тепер цю функцію вартового щораз більше беруть на себе нові посередники. До таких компаній належать інтернет-провайдери ***(internet service providers, ISP)***, пошукові системи та платформи соціальних медіа. Інтернет-посередники[11] – це організації (передусім прибуткові компанії), які «поєднують або полегшують транзакції між третіми сторонами в інтернеті. Вони надають доступ до контенту, продуктів і послуг, які створюють треті особи в інтернеті, розміщують такий контент, підтримують, передають та індексують їх, або надають інтернет-послуги третім особам». Отже, вони отримали контроль над потоком, наявністю, можливостями пошуку та доступністю інформації та іншого контенту онлайн[12].

13. Великою обіцянкою інтернету було те, що він діятиме за межами компетенції наявних комунікаційних монополій, але насправді великі транс-

11. Термін «інтернет-посередники» позначає операторів онлайн-медіаплатформ, пошукових систем, соціальних мереж та магазинів-застосунків (van der Noll, Helberger, & Kleinen-von Königslöw, 2015). Відповідно до Рекомендації Ради Європи CM/Rec (2018) 2 про ролі та обов'язки інтернет-посередників, ці суб'єкти сприяють взаємодії в інтернеті між фізичними і юридичними особами, пропонуючи та виконуючи різноманітні функції і послуги. Деякі з них підключають користувачів до інтернету, дозволяють обробку інформації та даних або розміщення веб-сервісів, зокрема для створеного користувачем контенту. Інші збирають та узагальнюють інформацію та дозволяють здійснювати пошук; вони надають доступ до контенту та сервісів, розроблених та/або керованих третіми сторонами, зберігають та індексують такий контент та сервіси. Деякі з них сприяють продажу товарів та послуг, включно з аудіовізуальними послугами, і дозволяють проводити інші комерційні операції, включно з платежами.

12. www-cdn.law.stanford.edu/wp-content/uploads/2017/04/07_28.2_Persily-web.pdf.

національні корпорації[13] зберігають глобальний контроль над потоком інформації, а тому можуть формувати політичний дискурс і погляди. Тут працюють ті самі сили, що і в традиційному ландшафті засобів масової інформації, але тепер їхні голоси підсилено соціальними медіа, і вони здатні сягнути всіх куточків світу та видозмінити суспільство й життя людей. Уявлення, що інтернет повинен забезпечити хоча б мінімально конкурентний ландшафт для нових учасників, уже не виглядає актуальним. Декілька приватних суб'єктів, які володіють інформаційними магістралями, є потужними й нерегульованими достатньою мірою, щоб диктувати умови щодо соціальних, індивідуальних та політичних свобод, відповідно з'являючись як ще один актор на демократичній арені; а виробництво контенту стало настільки «демократичним» та анонімним, що вкрай важко визначити достовірну інформацію і знайти відповідального за протиправну поведінку онлайн.

14. Соціальні медіа, як ***Facebook***, не менше, ніж традиційні засоби масової інформації, контрольовані ринковими силами. Ціна акцій ***Facebook***, як і будь-яких великих медіакорпорацій, залежить від його доходів від реклами; мета корпорації – фінансове зростання та підтримка власної ринкової вартості. Реклама у ***Facebook*** працює через визначення інтересів його користувачів на підставі даних, які вона збирає під час їхнього перегляду, вподобань і т. ін. шляхом високотехнологічних операцій. Сайти заробляють гроші за кліки, і за допомогою алгоритмічного регулювання створюють ехо-камери та фільтри-бульбашки, де індивіди отримують ту інформацію, яку попередньо вони обирали або, більш зловісно, яку, як уже вирахували алгоритми, вони хочуть почути. Це дозволяє політичній рекламі бути все більше індивідуалізованою та таргетованою. Замість того, щоб бути публічним простором, у якому присутні багато голосів, постає простір, у якому люди стають усе більш ізольованими та відірваними від усього спектру суспільства.

15. «Демократизація» створення контенту та централізація каналів розповсюдження в інтернеті призвела до непередбачуваних наслідків поширення фальшивої інформації, використання тактик приватної і публічної дезінформації. Поява кожного засобу комунікації (1) розширює розповсюдження інформації та доступ до неї (свобода спілкування); (2) має наслідком ризик зловживань (зловмисний контент); (3) відкриває шлях до цензури та (4) до маніпуляцій із боку потужних державних і приватних суб'єктів.

16. Розвиток інтернету та соціальних медіа вивів масову комунікацію, процес надання та отримання повідомлень до масштабів, які були невідомі з часів створення друкованої преси. Поширення фальшивої інформації, тактики приватної та публічної дезінформації стали за останні декілька років

13. Див., наприклад: www.forbes.com/sites/steveandriole/2018/09/26/apple-google-microsoft-amazon-and-facebook-own-huge-market-shares-technology-oligarchy/#372d73d92318.

набагато більш поширеними й технічно витонченими – боти, виробники пропаганди, розповсюджувачі дезінформації, що використовують соціальні медіа та алгоритми пошуку, які забезпечують високу видимість і бездоганну інтеграцію у контент, якому довіряють, чим вводять в оману велику аудиторію споживачів новин і, що ще більш важливо, виборців. Хоча дезінформація завжди була стратегією дискредитації опонентів та схилення політичної підтримки в той чи інший бік, цифрові технології збільшили загрози фальшивої інформації для демократії з різних причин: швидкість поширення (фальшивої) інформації через інтернет[14]; той факт, що дезінформації фактично сприяє сучасна архітектура пошукових систем і соціальних медіа; відсутність інструментів (як правових, так і соціальних чи технічних) для ідентифікації фальшивої інформації та припинення її поширення; складність розслідування й покарання такої поведінки в інтернеті.

17. Протягом останніх років іноземне втручання у вибори шляхом використання соціальних медіа також стало проблемою для демократій. Технологічні ресурси, такі як дешеві цифрові шпигунські кампанії, мережі платних користувачів та ботів, вибіркове розкриття інформації або продукування фальшивої інформації змінили правила гри під час виборчих кампаній. Як побічний ефект, це розмиває довіру до демократичних урядів.

18. У світовому масштабі згадані вище практики, яким сприяють цифрові технології, можуть становити загрозу демократії та ставити під сумнів ідею інтернету як технологічного засобу для більш демократичного врядування.

19. Існування цифрових технологій та їхнє застосування майже у всіх сферах життя, включно з виборами, є фактом, який не можна поставити під сумнів. Це дослідження не має наміру оцінювати їхні позитивні та негативні аспекти, а спрямоване на те, щоб відповісти на виклики, які цифрові технології породжують у сфері виборів. Тому це дослідження передусім зосереджене на проблемах, що є наслідками інновації, та можливому їх вирішенні, аніж на перевагах інновацій.

20. Ця доповідь не прагне пропонувати конкретні та універсальні рішення усіх проблем, які можуть постати в усіх виборчих процесах внаслідок використання інтернету й соціальних мереж. Особливості кожної нації та кожної демократії зробили б таке завдання неможливим[15]. Натомість мета цієї доповіді полягає в тому, щоб визначити найбільш важливі правові

14. Тепер існують також докази того, що люди більш схильні ділитися фальшивими новинами. Навіть більше, за даними найбільшого з коли-небудь проведених досліджень цього явища в цифрових медіа, проведеного *MIT (Massachusetts Institute of Technology.* – Прим. ред.), поширення фальшивої інформації цифровими засобами є більш ймовірним. Окрім того, виглядає, що для досягнення користувачів правдивими повідомленнями потрібно приблизно в шість разів більше часу, ніж для фальшивих (Vosoughi, Roy and Aral, 2018). Відповідно до *Edelman Trust Barometer 2018 Global Report*, близько 70% світових користувачів інтернету стурбовані тим фактом, що «фейкові новини» використовуються як зброя.

15. Див. документ CDL-AD(2019)016 щодо прикладів різних критеріїв для вирішення подібних проблем.

проблеми, спричинені використанням цих технологій, описати їхню логіку та параметри їх можливого вирішення, вказати на їхні недоліки, виявлені на цей час, і запропонувати загальний набір принципів і настанов, які могли б допомогти пристосувати демократію та її закони до нових технологічних реалій. У цьому сенсі висновок такого документа швидше нагадує дорожню карту принципів наявного та майбутнього регулювання і співробітництва, а не посібник для вирішення всіх проблем.

21. Це дослідження варто розглядати як доповнення до попередніх документів Ради Європи на цю тему, а саме, Доповіді Ради Європи «Інформаційний безлад»[16] 2017 року ***(2017 Council of Europe report on «Information Disorder»***; надалі – Доповідь РЄ про інформаційний безлад 2017 року) та «Дослідження щодо використання інтернету під час виборчих кампаній» ("the Study on the use of internet in electoral campaigns"; надалі – Виборче дослідження Ради Європи 2017 року)[17].

III. НОВІ ТЕХНОЛОГІЇ ТА ІНФОРМАЦІЯ

22. В онлайн-суспільстві інформація є основним товаром не тільки економічного виробництва, а й соціальної взаємодії та управління. Вплив інтернету на реальність є універсальним, і він впливає навіть на тих, хто ніколи не користувався цією технологію. Інтернет безпосередньо впливає на громадську думку, де б люди не перебували, та вже змінив спосіб мислення та поведінки людей у світі, який їх оточує. Він надає голос усім і кожному зацікавленому та створює їм можливості зробити внесок у публічний дискурс, як негативний, так і позитивний. Це відкриває шлях для того, щоб «PR-війська» кинулися на форум, де багато що поставлено на карту, намагаючись вплинути на перебіг подій. Часом у цю взаємодію віртуального та фізичного втручається вигадка[18]. Публічні діячі можуть виявити, що їхні вигадані персонажі є навіть більш впливовими «акторами», ніж їхні фізичні сутності[19]. Гумор часом має подібний ефект: користувачі інтернету можуть формувати різні сприйняття, створюючи, наприклад, фейкові сатиричні акаунти для публічних діячів, що безпосередньо впливають на імідж людини, яку прагнуть копіювати, та часом дезорієнтують громадськість і засоби масової інформації[20].

16. Council of Europe Report, DGI (2017) 09.

17. Council of Europe Report, DGI (2017) 11.

18. Виразний приклад руйнування межі між вигадкою та реальністю можна спостерігати в комунікаційній стратегії ІДІЛ. Свідомо наслідуючи відеоігри та блокбастери, вони генерують увагу, створюючи гуманізований образ терориста й знеособлений образ жертв (Lesaca, Javier. Armas de seducción masiva. Peninsula, Atalaya, 2017). Навпаки, традиційні засоби масової інформації не відображають наслідків їх варварства у всій його суворості.

19. Підтримка Кевіна Спейсі або його втілення президента Сполучених Штатів Америки в серіалі «Картковий будинок» (House of Cards) породила багато суперечок. Справа борця Ґалка Ґоґана (Hulk Hogan) потрапила до північноамериканських судів, і врешті-решт у ній було винесено позитивний вирок, який ґрунтувався на розрізненні дій вигаданого персонажа на рингу й поза ним та особи, яка виконувала цю роль.

20. На різних платформах соціальних медіа фейкові акаунти виглядають як справжні, і незалежно від того, чи попереджають вони про свою пародійну природу, такі акаунти формують стереотип тієї дійової особи, яку копіюють, використовуючи гумор. Деякі з них виходять за межі дійсного акаунту особи, яку вони пародіюють. В іспанській політиці помітні приклади включають @EspeonzaAguirre та @NanianoRajoy.

23. Інформація передається здебільшого через зображення, які, на відміну від слів, обробляються автоматично: людина ризикує перетворитися на пасивного рецепієнта, зануреного в кольори, форми, послідовності та фонові шуми і нездатного, за відсутності писемної культури та вербальної мови, трансформувати інформацію в знання, а зображення – у судження та ідеї. Цей ризик призводить до прогресивного розмивання спроможності абстрагування. ***Homo sapiens*** щораз більше перетворюється на ***homo videns***[21] – істоту, яка дивиться, але не думає; істоту, яка бачить, але не розуміє. Зображення обрамлено написаними позитивними або негативними текстами, які також перетворюються на зображення і, як і інша інформація, обробляються негайно замість того, щоб спонукати до осмислення[22].

24. Коли інформація зводиться до простих подразників, які впливають на реципієнта[23], люди більше реагують на сприйняття та менше – на інформацію. Наголос на зображенні також призводить до труднощів у поясненні складних понять, які потребують певного рівня абстрагування. Подразники, на які люди реагують, є майже винятково аудіовізуальними, з презумпцією правдивості, і люди реагують лише на зображення, які здатні викликати таку реакцію. Емоційний зміст у чутках стає важливішим за фактичний і відповідно провокує емоційні реакції – зазвичай, ненависть чи наклеп. Цим щораз більше користаються PR-агенції, яким платять політичні актори з метою створення простору на ґрунті ненависті та наклепу.

25. Явище під назвою «фейкові новини»[24] привернуло широку увагу на хвилі президентських виборів у США в 2016 році. Термін «фейкові новини» описує різноманітні окремі явища. Зазвичай вони поєднують елементи традиційних новин із рисами, що є невластивими для професійної журналістики[25]. «Фейкові новини» є ознакою краху традиційних новин (тоді як дезінформація, помилкова інформація чи сенсаціоналізм не є новими явищами) та панівного хаосу у комунікації в соціальних медіа. Це нова версія старої боротьби за визначення правди, яку ведуть політичні та фінансові кола довкола війни пропаганди, де «фейкові новини» є основною зброєю.

26. Масове розповсюдження зображень вирішальним чином сприяло успіху «фейкових новин» шляхом надання інформації вигляду безпомилковості. Комунікація закінчується, перетворюючись на виставу, заохочуючи прості поняття, оманливі заголовки, будь-що, що привертає увагу читача (наживка), хоча зрештою це все може виявитися досить спрощеним.

---

21. Sartori, Giovanni. Homovidens, Taurus, 1989.

22. У зв'язку з цим важливо ще раз обдумати відому фразу E.M. Фостера, який сказав: *«Книги – це факти, які варто читати (що дратує, оскільки це займає тривалий час); це єдиний спосіб дізнатися, що в них написано. Деякі дикі племена їдять їх, але на Заході читання є єдиною відомою технікою».*

23. Schwartz, Tony. La respuesta emocional. Ed. Liderazgo democrático 2. Quito, 2001, p. 37.

24. Доповідь Ради Європи про інформаційний безлад за 2017 рік *(2017 Council of Europe Information Disorder report)* свідомо утримується від використання терміну «фейкові новини» на тій підставі, що він неадекватно охоплює складність інформаційного забруднення і стає щораз більше політизованим.

25. Mourao, R.R. and Robertson, C.T.: Fake News as Discursive Integration: An Analysis of Sites that Publish False, Misleading, Hyperpartisan and Sensational Information, published online: 13 Januar 2019.

Форма панує над змістом, а зображення – над ідеями; іде пошук простих відповідей, які поділяють світ на чорне і біле, так і ні, і в якому немає нюансів. Стислість, важливість зображення та простота поширення контенту, типові для соціальних мереж, – усе це сприяє поширенню методів, які спотворюють реальність.

27. Сьогоднішнє очікування постійних оновлень та навіть передбачень[26] призводить до того, що інформація розповсюджується одразу після створення, без перевірки або обмірковування. Така динаміка віддає перевагу швидкості перед якістю, створюючи інформативні цикли, які часто тривають менше ніж двадцять чотири години, виснажуючи інформацію, перш ніж її встигнуть опублікувати в друкованій пресі наступного дня. Необмеженість ємності пам'яті та її доступність означає, що заяви можуть бути відкликані за лічені секунди з відповідних сайтів через місяці або навіть роки після цього. Такі суперечності також зазнають масового розповсюдження, а іноді, якщо їх розглядати поза контекстом, вони можуть стати предметом «фейкових новин».

28. Тисячі аналізів, оцінок і даних про кожну з подій хаотично накопичуються в соціальних мережах і поширюються завдяки майже безмежній «капілярності» через різні термінали, до яких підключені громадяни. Перевантаження інформацією перешкоджає комунікації, оскільки певні події можуть так і залишитися поза увагою, тоді як перевагу отримують простіші аспекти інших подій, що впадають в око. Процес демонстрації фактів з метою виправлення помилок в інформації є недостатнім засобом виправлення цих помилок.

29. Індивіди створюють власну інформаційну екосистему чи особистий світ, який складається з фрагментів інформації, що посилаються самі на себе і не потребують будь-якого типу узгодженості ані з попередніми текстами, ані з дійсністю. Результатом є дуже упереджене сприйняття тих, хто не входить до тієї самої інформаційної екосистеми. Нові та різноманітні джерела інформації дозволяють висвітлити індивідуальні ідеї, а відповідно посилити підтверджену упередженість, у якій увага й довіра надається тій інформації, яка підживлює власні переконання. Алгоритми, що використовуються у засобах приватного спілкування та інших соціальних мережах, виявляють уподобання користувачів, відображаючи їх частіше і тим самим ще більше підсилюючи знання та підтримку суміжних тем. Отже, незважаючи на масу доступної інформації, до її більшої частини або не звертаються, або звертаються лише ті, хто вже впевнений у її обмеженій достовірності. Небажані або неприємні факти можна ігнорувати на користь персоналізованих наративів. Інформацію та виправлення підбирають вибірково, щоб довести, що певна думка є правильною і що альтер-

26. В Іспанії, особливо у Вікіпедії, поточні тенденції включають навіювання, що люди вже померли, коли насправді вони перебувають у доброму здоров'ї. Наприклад, медсестра, яка захворіла на Еболу, була кремована, а потім дивом знову повернулася до життя.

нативні думки є хибними[27]. Це може статися навіть із перевіреною інформацією, оскільки вона розповсюджується набагато краще, коли підкріплена попередніми ідеями, ніж коли її ставлять під сумнів[28].

30. Соціальне середовище також визначає, як інформація отримується, зокрема тоді, коли така інформація дозволяє людині ототожнити себе з групою та приховати те, що може їй зашкодити або не збігатися з позицією групи. Наприклад, ефект натовпу ґрунтується на потребі належати до чогось та на тому, що соромно бути інакшим. Отже, люди довіряють поглядам більшості, створюючи ехокамеру, де погляди взаємно підкріплюються.

31. Підтверджене упередження викликає спускову фрагментацію між інформаційними бульбашками[29] паралельних інформаційних світів, що породжує труднощі для існування спільних просторів для дискусій. На цей час загальна публічна сфера зводиться до невеликих високомобілізованих блоків, ізольованих один від одного. Можливість спілкуватися та бути інформованими вибірковим, майже персоналізованим способом, що принципово полегшується за допомогою технологій та соціальних мереж, створює самореферентійні мікроспільноти, у межах яких можливість пізнання та здатність поставити себе на місце іншого заохочують до більш радикальних позицій і браку діалогу, що заважає емпатії[30]. Разом ці два елементи сприяють поляризації та дозволяють створити єдину систему цінностей, принаймні в межах закритих груп, які зрештою глушать голоси інакодумців та витісняють їх. Під час взаємодії різних інформаційних екосистем вони стикаються, що само по собі живить цю поляризацію, оскільки довіра до кожної радикальної позиції зменшується відповідно до поглядів її опонентів, своєю чергою підживлюючи радикальний дискурс іншої сторони[31].

32. Технологія не просто впливає на спосіб розповсюдження інформації, вона впливає на весь комунікативний процес збирання, зберігання, організації та розповсюдження інформації. Громадяни не є просто отримувачами інформації, вони стають основними учасниками комунікативного процесу. Вони створюють власні джерела інформації за відсутності традиційних вартових та регуляторів. Внаслідок цієї численності та різноманітності інформації засоби масової інформації втрачають власну референційну суть і авторитет. Навіть більше, помилки, допущені традиційними медійними джерелами внаслідок згаданої вище швидкоплин-

27. Sunstein, C., Scala, A., Quattrocioccchi, W. Echo Chambers on Facebook. 2016. Доступно за посиланням: ssrn.com/abstract=2795110 (звернення 25.01.2018 р.).
28. Shin, Jieun, Thorson, Kjerstin. Partisan Selective Sharing: The Biased Diffusion of Fact-Checking Messages on Social Media. Journal of Communication. Vol 67, 2017. Доступно за посиланням: onlinelibrary.wiley.com/doi/10.1111/jcom.12284/full (звернення 25.01.2018 р.).
29. Parisier, Eli. The filter bubble. The Penguin Press. New York. 2011.
30. Sunstein, C. R. The law of group polarization. Journal of political philosophy 10, 175–195 (2002).
31. Див.: www.buzzfeed.com/charliewarzel/2017-year-the-internet-destroyed-shared-reality (звернення 25.01.2018 р.).

ності інформаційного процесу в поєднанні зі змішуванням джерел, сприяли зниженню довіри до засобів масової інформації[32]. Отже, індивіди приєднуються до засобів масової інформації, і часто на рівних умовах. Формуються персональні інформаційні простори, у яких громадяни знаходять притулок; зустрівшись із потоками контенту, вони тікають у зменшений та керований, надійний та безпечний інформаційний всесвіт, у якому панують стосунки з тими, хто їм найближчий у їх особистому та професійному житті та за ідеологічними поглядами.

33. Під час обміну інформацією громадяни стають основними дійовими особами комунікації, ставлячи під сумнів цінність засобів масової інформації[33]. Громадяни все частіше використовують інтернет як джерело інформації, і коли вони роблять це, то не розрізняють справжніх, більш достовірних джерел інформації та решти контенту, що надходить від сім'ї і друзів[34]. По суті, 79% розглядають останній контент як достовірне джерело інформації, після якого йдуть міркування наукових експертів (72%), працівників підприємств (60%) та підприємств, послугами яких вони користуються (59%). Інформація від журналістів (48%), керівників вищої ланки (43%), відомих онлайн-діячів (42%) та знаменитостей (29%) перебуває у нижній частині списку[35].

34. Вага, якої набуває міжособистісна комунікація через соціальні мережі, призвела до масового продукування ботів, анонімних, автоматизованих та інколи фейкових облікових записів, які виступають у ролі індивідів в інтернеті й збільшують масове поширення специфічної інформації, спрямованої на штучне створення потоків громадської думки або ж прийняття чи відмову від людей або ідей[36]. Через створення враження, що вони мають широку підтримку, такі явища формують ефект натовпу, а інші сприймають ідеї, які поділяє ця начебто більшість. Це породжує стадну поведінку, завдяки якій індивіди нехтують особистою відповідальністю і підпорядковуються волі колективу; вони імітують один одного та заперечують розбіжність. Надмірність неправдивої інформації, особливо коли її знаходять у засобах масової інформації, стає «переконанням», беззаперечною основою, відмова від якої наражає на ризик бути дискваліфікованим (як член спільноти. – *Прим. ред.*).

---

32. Президент Трамп використав деякі з цих реальних або очевидних невдач, щоб присудити призи за «фейкові новини»: www.elconfidencial.com/mundo/2018-01-18/trump-fake-news-awards-noticias-falsas-premios_1508101 (звернення 25.01.2018 р.).

    З іншим прикладом можна ознайомитись за посиланням: theintercept.com/2017/12/09/the-u-s-media-yesterday-suffered-its-most-humiliating-debacle-in-ages-now-refuses-all-transparency-over-what-happened (звернення 25.01.2018 р.).

33. 46% громадян Європейського Союзу стежили за новинами в соціальних мережах у 2016 році: Reuters Institute Digital News Report 2016; доступно за посиланням: reutersinstitute.politics.ox.ac.uk/sites/default/files/research/files/Digital%2520News%2520Report%25202016.pdf (звернення 25.01.2018 р.).

34. Відповідно до доповіді «Я бачив новини у Facebook» ("I saw the news on Facebook"), підготованої Reuters Institute for the Study of Journalism at the University of Oxford, у 2017 році більше половини британців отримувала інформацію із соціальних мереж. З цієї половини понад 50% не пам'ятають справжнього джерела інформації.

35. Edelman Trust Barometer 2016.

36. agendapublica.elperiodico.com/desde-rusia-bots.

IV. ВПЛИВ СОЦІАЛЬНИХ МЕДІА ТА ІНТЕРНЕТУ НА ДЕМОКРАТІЮ І ВИБОРЧІ ПРОЦЕСИ

35. Інтернет надав людям безпрецедентний доступ до інформації про вибори та можливість висловлювати свої погляди, взаємодіяти з кандидатами та бути активно залученими до виборчих кампаній[37]. Соціальні медіа, зокрема, є платформою, де переважно відбуваються політичні дебати, та відповідно є джерелами політичної інформації. Дослідження свідчать, що чимраз більший потік інформації[38], підсилений соціальними медіа, посилює критичну спроможність громадян щодо своїх урядів[39], і що існує сильна позитивна кореляція (0,71) між використанням інтернету та соціальних медіа, з одного боку, і підтримкою демократії як бажаної форми правління – з другого[40]. Навіть більше, багато авторів стверджують, що узагальнене використання інтернету та соціальних медіа забезпечує більш точне знання інтересів громадян і сприяє організації широкомасштабних соціальних рухів[41].

36. Проте, навіть якщо «інтернет має силу, щоб бути інструментом демократії..., його потенціал у цьому відношенні несе ризики..., [тому що] та сама технологія, яка полегшує дискурс, створює можливості для цензури інформації, моніторингу онлайн-практики та тонкого формування поведінки й маніпулювання нею»[42], відповідно загрожуючи автентичності голосування, справедливості виборчої конкуренції та, зрештою, спроможності перетворити волю народу в інституційне представництво та урядові рішення[43]. Потрібно зазначити, що будь-який протиправний вплив на автентичність та свободу голосування може позначитися не лише на перетворенні волі народу на конкретні дії, але й також на захисті меншин, на рівновазі між основоположними правами людини та на можливості утримувати підзвітними політичні партії та виборних посадовців. Навіть хоча такі загрози вже існували в минулому, вони посилилися завдяки створенню більш досконалих методів, яким сприяли цифрові технології.

37. Постійний та одночасний потік інформації в режимі реального часу через численні платформи становить величезну проблему для нагляду за поведінкою і ресурсами під час політичних кампаній. Навіть більше, розсіяне й анонімне створення контенту істотно перешкоджає виявленню та покладанню відповідальності за незаконну поведінку онлайн. Розширення масштабів використання ботів і тролів для встановлення порядку денного в соціальних медіа, як і масове розповсюдження фальшивої інформації, серйозно шкодять справедливості у виборчій конкуренції та

37. CoE Election Study 2017, p. 7.
38. Democracy Reporting International 2017.
39. Gainous et al. 2016.
40. Basco 2018.
41. Castells 2011; Metaxas and Mustafaraj 2012; Cohen et al. 2012; European Union 2015.
42. Laidlaw 2015, p. 1.
43. Пор.: CoE Election Study 2017, p. 7-9. Див. також: Tambini 2018, p. 265-293.

дозволяють зовнішнім суб'єктам маніпулювати дискурсом і преференціями виборців[44]. Крім того, алгоритми, які керують пошуковими системами та соціальними медіа, можуть сприяти неповному, а іноді й ілюзорному розумінню політики та демократії[45].

38. Вплив цифрового середовища на вибори було висвітлено в спорах після референдуму щодо Брекзиту в Сполученому Королівстві та президентських виборів у США 2016 року. Дотримання правил та регулювання щодо платної реклами було обмеженим; особисті дані виборців збиралися та оброблялися для цілей виборчого процесу без згоди самих виборців та за відсутності законних повноважень; політична комунікація була спрямована через нерегульовані платформи соціальних медіа без належного забезпечення справедливого висвітлення у медіа. Ці наслідки кинули виклик усталеним інституціям та принципам регулювання виборчих комунікацій, таким як свобода об'єднання, обмеження витрат і регулювання політичної реклами[46], та підірвали здатність існуючих режимів регулювання підтримувати рівні умови для виборчих комунікацій. Вони становили загрозу виборам і створили потенціал для виникнення корупційних дій.

39. Трансформовані комунікативні сфери в інтернеті та змінений спосіб передання політичних повідомлень виборцям надають можливість фальшивій та/або шкідливій інформації «поширюватися серед потенційних виборців у безпрецедентних масштабах, без будь-якого нагляду чи спростування»[47]. Це призвело до певного рівня ***інформаційного безладу,*** який може набувати трьох різних форм:

    - Помилкове інформування, тобто обмін фальшивою інформацією, але без наміру заподіяти шкоду.

    - Дезінформація, яка означає свідомий обмін фальшивою інформацією з наміром заподіяти шкоду.

    - Зловмисне інформування, що означає розповсюдження справжньої інформації з наміром заподіяти шкоду, часто шляхом розголошення інформації з приватної сфери у публічній сфері[48].

40. У деяких випадках неправдиву інформацію ***стратегічно*** поширювали з наміром ***впливати на результати виборів***. Було задокументовано, що ***кібервійська*** в інтернеті часто є ***урядовими, військовими чи політичними партійними командами, завдання яких полягає в тому, щоб маніпулювати громадською думкою*** через соціальні медіа. Організовані ***маніпуляції із***

44. Quintana 2016; Fidler 2017.
45. Van Dijck 2013; McChesney 2013.
46. CoE Election Study 2017, p. 13.
47. CoE Election Study 2017, p. 15.
48. CoE Information Disorder Report 2017.

соціальними медіа вперше виникли у 2010 році, а до кінця 2017 року про такі випадки відомо у 28 країнах[49].

41. Не лише соціальні медіа, а й провайдери пошукових систем можуть маніпулювати інформацією з наміром або без наміру спотворити результати виборів на користь певної політичної опції. Недавні дослідження показують, що маніпулювання результатами пошуку такими провайдерами може призвести до так званого ***ефекту маніпулювання пошуковою системою***, який може змістити преференції тих виборців, які ще не визначилися, на 20% чи навіть більше в деяких демократичних групах[50].

42. Існують випадки, коли державні органи використовували армії «формувачів поглядів» для поширення позиції уряду та протидії критикам у соціальних мережах; чи такі, як справа «***Cambridge Analytica***» – компанії, яку звинувачують у втручанні у вибори президента США у 2016 році* та в референдум щодо Брекзиту шляхом доступу та використання приватних даних 50 мільйонів користувачів ***Facebook***[51]. На відміну від інших прямих методів цензури, таких як блокування сайтів чи арешт за інтернет-діяльність, маніпуляції з контентом онлайн важко виявити, а ще складніше їх подолати, враховуючи їх розсіяну природу і велику кількість людей та ботів, залучених для цієї мети.

43. Оскільки цільові повідомлення доходять не до всієї громадськості, а лише до вибраних груп чи індивідів і не підлягають жодному нагляду чи журналістському перегляду, політичні кандидати та партії можуть давати різні обіцянки різним людям, розсіюючи свої політичні цілі окремими меседжами, які не обов'язково узгоджуються між собою. Дійсно, деякі дослідження вказують на посилення цифрової агітації щодо так званих наріжних питань, які розділяють суспільство, але мають здатність мобілізувати виборців (імміграційна політика, добробут, одностатеві шлюби і т. ін.). Нарешті, таргетування меседжів має за мету оптимізацію ресурсів передвиборчої агітації, відповідно зосереджуючи зусилля на хитких або невизначених виборцях. Ті, на кого не спрямовані меседжі політичних партій, позбавлені цілого спектра політичних позицій, що, своєю чергою, створює нерівності щодо наявної інформації, на підставі якої виборці роблять свій політичний вибір.

44. Нарешті, держави та приватні суб'єкти в усьому світі можуть використовувати цифрові технології для порушення прав людини або навіть як військовий інструмент для нападу на країни і їхні інституції шляхом ви-

49. Bradshaw & Howard, 2017. Див. також *Freedom House 2017 report*, відповідно до якого тактика маніпуляцій та дезінформації відігравала важливу роль на виборах принаймні в 17 інших країнах протягом року. За даними *Communications Security Establishment* (CSE) уряду Канади, лише в 2017 році в 13% країн, де проводилися федеральні вибори, на їхній демократичний процес були націлені хактивісти, кіберзлочинці і навіть публічні чи приватні політичні актори, і всі вони мали намір маніпулювати інформацією, розхитувати громадську думку чи навіть дестабілізувати демократичні інститути.

50. Epstein & Robertson, 2015.

* В оригіналі – «2017», що варто визнати опискою. – *Прим. ред.*

51. Mccausland, P. та Schecter, A., 2018, BBC, 2018.

користання шкідливого програмного забезпечення, програм для вимагання коштів, шпигунських програм та інших витончених програм[52]. Такі дії відомі під назвою «***кібервійна***»; до них і раніше успішно вдавалися для підриву державних проєктів і систем, наприклад, атака ***Stuxnet*** на атомну станцію Натанз в Ірані[53].

45. Окрім своєї доступності, витонченості та публічної привабливості, кібернетичні інструменти вбудовані в середовище без меж. Те, що було легально створено в рамках національного законодавства, тепер може бути незаконно розміщеним в іншій юрисдикції, і навпаки. Навіть більше, зі зростанням рівня використання ***хмарних технологій*** інформація в інтернеті стала ще більш фрагментарною, завдяки чому вкрай складно визначити її походження чи авторство. Кіберзлочинність та кіберзагрози діють поза рамками будь-якої національної юрисдикції. Така ситуація становить труднощі для кримінального розслідування і притягнення до відповідальності; отже, існує потреба вивчення цього явища з транснаціональної точки зору[54].

46. Підсумовуючи, сьогодні ми спостерігаємо паралельне поширення інформації та її забруднення в глобальному масштабі. Інтернет-сервіси збагатили та урізноманітнили джерела новин, спростивши індивідам доступ до інформації та прийняття рішень щодо найбільш важливих питань демократії, зокрема щодо вибору їхнього законодавчого органу. Проте водночас нова ера інформаційного безладу спотворила комунікаційну екосистему настільки, що виборцям може бути істотно ускладнено здійснення власного вибору через введення в оману, маніпулятивну та фальшиву інформацію, метою якої є вплив на їхні голоси. Таке середовище потенційно підриває реалізацію права на вільні вибори та створює значні ризики для функціонування демократичної системи.

47. Цифрові технології змінили способи, якими суспільства перетворюють волю народу у голоси та представництво, і вони значною мірою змінили політичну агітацію. Навіть хоча інтернет посилює деякі аспекти демократичної конкуренції, він водночас і перешкоджає їм. Всесвітня розповсюдженість цифрових технологій перенесла арену демократичних дебатів у віртуальний світ, поставивши багато питань щодо їхнього впливу на участь виборців та необхідність нагляду та регулювання соціальної поведінки онлайн. Навіть більше, необхідно забезпечити належний захист від кібервійни.

V. ВІДПОВІДНІ ЄВРОПЕЙСЬКІ ТА МІЖНАРОДНІ СТАНДАРТИ Й ДОКУМЕНТИ

48. Зазначені вище явища загрожують низці основоположних прав, захищених на європейському та всесвітньому рівнях кількома міжнародними деклараціями й конвенціями, такими як Загальна декларація прав людини,

52. Quintana 2016.

53. Quintana 2016; Mecinas Montiel 2016, c. 404, 418-419.

54. Davara 2003; Salt 2017 c. 520-521.

Міжнародний пакт про громадянські та політичні права, Американська декларація прав і обов'язків людини, Американська конвенція про права людини, Хартія основних прав Європейського Союзу та Європейська конвенція з прав людини (надалі – ЄКПЛ).

A. ПРАВО НА ВІЛЬНІ ВИБОРИ ТА СВОБОДУ ВИРАЖЕННЯ ПОГЛЯДІВ

1. Основні принципи

49. Відповідно до ЄКПЛ у трактуванні Європейського Суду з прав людини (надалі – ЄСПЛ), держави-члени Ради Європи зобов'язані забезпечити права та свободи кожного, хто перебуває під їхньою юрисдикцією. Право на вільні вибори, передбачене статтею 3 Першого протоколу до ЄКПЛ, є не лише об'єктивним та істотним принципом у будь-якому демократичному суспільстві, а й основоположним індивідуальним правом, на яке може покластися кожен громадянин, тим, що найбільш ефективно сприяє «справжній демократії»[55].

50. Право на вільні вибори охоплює право голосу та право балотуватися на виборах[56]. Навіть більше, воно також має наслідком позитивне зобов'язання держав-членів забезпечувати умови, в яких люди можуть вільно формувати та висловлювати свої погляди та обирати своїх представників. Цей обов'язок має вкрай важливе значення щодо (не)зруйнованого комунікативного контексту виборів. Право на вільні вибори передбачає, що держави-члени «зобов'язуються проводити вільні вибори з розумною періодичністю шляхом таємного голосування в умовах, які забезпечать вільне вираження думки народу у виборі законодавчого органу», що вказує на те, що право на свободу вираження поглядів та право на вільні вибори є необхідними умовами одне для одного[57]. Таке розуміння підтверджене ЄСПЛ, який ствердив, що «вільні вибори та свобода вираження поглядів, зокрема, свобода політичних дебатів, разом є основою будь-якої демократичної системи»[58].

51. ЄСПЛ також ствердив, що обидва права взаємопов'язані та діють на зміцнення одне одного, а свобода вираження поглядів є однією з умов, необхідних для забезпечення вільних виборів. Для забезпечення прав, гарантованих статтею 3 Першого протоколу, захист таких прав поширюється на передвиборчу агітацію. З цієї причини особливо важливо, щоб впродовж передвиборчого періоду було дозволено вільний обіг погля-

55. Thorgeirsdóttir, Herdis (2005), Journalism Worthy of the Name: the Affirmative Side of Article 10 of the ECHR, Kluwer Law International. Lécuyer, 2014. Див. *«Матьє-Моен і Клерфет проти Бельгії» (Mathieu-Mohin and Clerfayt v. Belgium)*, заява № 9267/81 (ЄСПЛ, 2 березня 1987 року); *«Жданока проти Латвії» (Ždanoka v. Latvia)*, заява № 58278/00 (ЄСПЛ, 16 березня 2006 року). Див. також: ЄСПЛ, 2018 рік, "Guide on Article 3 of Protocol No. 1 to the European Convention on Human Rights – Right to free elections"; доступно за посиланням: www.echr.coe.int/Documents/Guide_Art_3_Protocol_1_ENG.pdf.

56. *«Матьє-Моен і Клерфет проти Бельгії» (Mathieu-Mohin and Clerfayt v. Belgium); «Жданока проти Латвії» (Ždanoka v. Latvia).*

57. Plaizier, 2018.

58. *«Боуман проти Сполученого Королівства» (Bowman v the United Kingdom)*, заява № 24839/94 (ЄСПЛ, 19 лютого 1998 року), параграф 42.

дів та інформації усіх видів[59]. Відповідно до ЄСПЛ, держави-члени мають позитивне зобов'язання забезпечити ефективність свободи вираження поглядів: від них вимагається створити сприятливе середовище для участі в публічних дебатах усіх зацікавлених осіб, надаючи їм можливість висловлювати свої погляди та ідеї без остраху. Держава повинна не просто утримуватися від будь-якого втручання у свободу вираження поглядів, але має позитивне зобов'язання захищати право на свободу вираження поглядів від нападів, зокрема й із боку приватних осіб[60].

52. Проте ЄСПЛ визнав, що за певних обставин права, передбачені статтею 10 ЄКПЛ та статтею 3 Першого протоколу, можуть конфліктувати між собою, внаслідок чого може виникнути потреба встановити перед виборами і під час них певні обмеження свободи вираження поглядів такого типу, який у звичайних умовах є неприйнятним, для того, щоб забезпечити «вільне вираження думки народу у виборі законодавчого органу»[61]. Суд визнав, що для досягнення балансу між цими двома правами держави-члени мають таке саме поле розсуду, яке вони мають, взагалі кажучи, щодо визначення своїх виборчих систем. Водночас Суд наголосив на тому, що будь-які обмеження свободи вираження поглядів повинні бути пропорційними законній меті, яку перед собою ставлять, та бути необхідними в демократичному суспільстві. Суд вказав, наприклад, що стаття 10 ЄКПЛ як така не забороняє обговорення або розповсюдження отриманої інформації, навіть якщо є значні підозри щодо того, що ця інформація може бути неправдивою[62]. З другого боку, варто звернути увагу на рішення Суду щодо права неурядової організації (НУО) здійснювати політичну рекламу на радіо та телебаченні, у якому він збалансував право НУО-заявника передавати інформацію та ідеї, які становлять загальний інтерес і які громадськість має право отримувати, з бажанням влади захистити демократичну дискусію і процес від спотворення шляхом використання потужних фінансових груп із переважним доступом до впливових засобів масової інформації[63]. Суд визнав, що такі групи можуть отримати конкурентні переваги у сфері платної реклами і тим самим обмежити вільну та плюралістичну дискусію, у якій держава залишається єдиним гарантом. Як результат, для підтримання вільної та плюралістичної дискусії необхідно враховувати ризик дисбалансу між політичними силами у їх конкуренції.

59. *«Боуман проти Сполученого Королівства» (Bowman v the United Kingdom)*, заява № 24839/94 (ЄСПЛ, 19 лютого 1998 року); *«Орловська Іскра проти Росії» (Orlovskaya Iskra v. Russia)*, заява № 42911/08 (ЄСПЛ, 21 лютого 2017 року). Під час європейських виборів 2019 року Facebook дозволив загальноєвропейську політичну рекламу для [виборів до] Європейського Парламенту: www.politico.eu/article/facebook-allows-eu-wide-political-ads-for-european-parliament; techcrunch.com/2019/04/26/facebook-says-its-open-to-advertising-u-turn-for-the-eu-elections-enabling-cross-border-campaigns/?renderMode=ie11.

60. *«Дінк проти Туреччини» (Dink v. Turkey)*, заяви № 2668/07, 6102/08, 30079/08, 7072/09 та 7124/09 (ЄСПЛ, 14 вересня 2010 року).

61. *«Боуман проти Сполученого Королівства» (Bowman v the United Kingdom)*, заява № 24839/94 (ЄСПЛ, 19 лютого 1998 року); *«Орловська Іскра проти Росії» (Orlovskaya Iskra v. Russia)*, заява № 42911/08 (ЄСПЛ, 21 лютого 2017 року).

62. *«Салов проти України» (Salov v. Ukraine)*, заява № 65511 8/01 (ЄСПЛ, 6 вересня 2005 року).

63. *«Енімал Дефендерз Інтернешнл проти Сполученого Королівства» (Animal Defenders International v. the United Kingdom)*, заява № 48876/08 (ЄСПЛ, 2013 рік).

53. Права, передбачені статтею 3 Першого протоколу, не є абсолютними: щодо них можуть існувати «неявні обмеження»[64], і в цій сфері державам-членам має бути надано широке поле розсуду. При дослідженні дотримання статті 3 Першого протоколу Суд здебільшого зосередив увагу на двох критеріях: чи не було сваволі або недостатньої пропорційності та чи перешкоджало обмеження вільному вираженню думки народу[65].

54. ЄСПЛ визнав право індивідів на доступ до інтернету, оскільки у своєму рішенні проти широкого блокування онлайн-контенту він ствердив, що «інтернет тепер став одним із головних засобів реалізації права на свободу вираження поглядів та інформації, забезпечуючи важливі інструменти для участі в заходах і дискусіях, що стосуються політичних питань і питань, що становлять загальний інтерес»[66]. Суд ствердив, що стаття 10 ЄСПЛ гарантує свободу висловлювати, отримувати та передавати інформацію й ідеї незалежно від кордонів. Блокування доступу до сайтів хостів та третіх сторін на додаток до сайтів, які стосувалися справи, робить багато інформації недоступною, тим самим обмежуючи права користувачів інтернету. Суд далі роз'яснив, що обмеження доступу до джерела інформації є сумісним з Конвенцією лише тоді, коли наявні чіткі законодавчі рамки, які забезпечують гарантію судового перегляду для запобігання можливим зловживанням.

55. Навіть більше, ЄСПЛ визнав, що, «враховуючи важливу роль, яку відіграє інтернет у розширенні доступу суспільства до новин та спрощенні процесу розповсюдження інформації (див. «Делфі АС проти Естонії» (Delfi AS v. Estonia) [ВП], § 133, ЄСПЛ, 2015 рік), функції блоґерів і користувачів соціальних медіа можна прирівняти до ролі «публічного вартового» в контексті захисту статті 10»[67]. Цей захист може поширюватися на доступ до (публічно розміщеної) інформації, якщо вона сприяє здійсненню права на свободу вираження поглядів: інформація, до якої шукають доступу, повинна відповідати тесту на публічний інтерес. Проте, як було згадано вище, стаття 10 не гарантує необмеженої свободи вираження поглядів; обмеження можуть бути дозволені, наприклад, із метою захисту права на приватне життя (стаття 8 ЄКПЛ), якщо використовувані засоби пропорційні поставленій меті.

64. Стаття 3 не обмежена певним переліком «законних цілей», таких, які перелічено в статтях 8-11 ЄКПЛ, і ЄСПЛ не застосовує традиційних тестів «необхідності» або «нагальної соціальної потреби», які використовуються у контексті статей 8-11 ЄКПЛ.

65. *«Матьє-Моен і Клерфет проти Бельгії» (Mathieu-Mohin and Clerfayt v. Belgium); «Жданока проти Латвії» (Ždanoka v. Latvia).*

66. *«Ахмет Їлдірім проти Туреччини» (Ahmet Yildirim v. Turkey)*, заява № 3111/10 (ЄСПЛ, 18 грудня 2012 року). Див. також: *«Ченґіз та інші проти Туреччини» (Cengiz and Others v. Turkey)*, заяви № 48226/10 та 14027/11 (ЄСПЛ, 1 грудня 2015 року).

67. *«Мадьяр Гельсінкі Бізоттшаґ проти Угорщини» (Magyar Helsinki Bizottság v. Hungary)*, заява № 18030/11 (ЄСПЛ, 8 листопада 2016 року). Див. також *«Енімал Дефендерз Інтернешнл проти Сполученого Королівства» (Animal Defenders International v. the United Kingdom)*», заява № 48876/08 (ЄСПЛ, 2013 рік).

56. Крім того, основні принципи, що стосуються виборів, викладено в Кодексі належної практики у виборчих справах, прийнятому Венеційською комісією у 2002 році[68]. Вони включають, ***inter alia***:

- рівність можливостей партій та кандидатів;
- нейтральне ставлення органів державної влади до передвиборчої агітації, до висвітлення в засобах масової інформації та до державного фінансування партій і кампаній;
- рівність можливостей може бути пропорційною, а не строгою, що стосується, зокрема, «ефірного часу на радіо й телебаченні»;
- відповідно до свободи вираження поглядів повинні бути вжиті правові заходи з метою забезпечити, щоб усім учасникам виборів надавався мінімальний доступ до приватних аудіовізуальних засобів масової інформації для проведення передвиборчої агітації та реклами;
- фінансування кампаній має бути прозорим;
- рівність можливостей може призвести до обмеження витрат політичних партій, особливо на рекламу.

57. Основні принципи, що стосуються виборів, зазнають особливих викликів, коли використовуються електронні методи голосування. Рада Європи продовжує залишатися єдиною організацією, яка встановила міжурядові стандарти у сфері е-голосування. Рекомендація Комітету Міністрів Rec(2004)11, яку застосовують у національній юриспруденції навіть держави, що не є членами Ради Європи, а також інші відповідні міжнародні суб'єкти, нещодавно була оновлена: нова рекомендація, яка складається з власне Рекомендації CM/Rec(2017)5 щодо стандартів е-голосування, Керівних принципів імплементації положень Рекомендації з конкретними вимогами та Пояснювальної записки (меморандуму), була розроблена як посилення рекомендації Rec(2004)11, і вона стосується найбільш критичної частини виборчої технології, а саме е-голосування, що означає використання електронних засобів для подання та підрахунку голосів. До цієї категорії належать такі системи, як електронні пристрої для голосування з прямим записом ***(Direct Recording Electronic (DRE) voting machines)***, сканери бюлетенів, цифрові ручки та системи голосування через інтернет. Рекомендація спрямована на забезпечення того, щоб е-голосування гарантувало загальне, рівне виборче право, вільні вибори й таємне голосування, і вона містить положення щодо організаційних вимог, підзвітності, надійності та безпеки системи[69].

68. CDL-AD(2002)023rev-cor. Див. також: Joint Guidelines for Preventing and Responding to the Misuse of Administrative Resources during Electoral Processes (CDL-AD(2016)004), які підтверджують принципи нейтральності та рівності можливостей щодо доступу до засобів масової інформації, що перебувають у публічній власності.

69. Кодекс належної практики у виборчих справах, CDL-AD (2002) 023rev-cor, пункт I.3.2.iv; див. також параграфи 42-44 Пояснювальної доповіді. Див. також: the Venice Commission Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe, CDL-AD(2004)12.

58. У зв'язку з цим доцільно звернути увагу на відповідні документи Венеційської комісії. Кодекс належної практики у виборчих справах чітко вказує, що «електронне голосування може бути застосоване лише в тому випадку, якщо воно безпечне й надійне; зокрема, виборці повинні мати можливість отримати підтвердження своїх голосів і виправити їх за потреби з дотриманням таємниці голосування; система має бути прозорою».

2. Фінансування виборчих кампаній

59. Існує низка загальноприйнятих стандартів проти корупції при фінансуванні політичних партій та виборчих кампаній (які рекомендується застосовувати також до суб'єктів, пов'язаних із політичними партіями, скажімо, до політичних фондів). Вони були встановлені Рекомендацією Парламентської Асамблеї 1516(2001) щодо фінансування політичних партій та продовжені Рекомендацією Комітету Міністрів Rec(2003) 4 про загальні правила боротьби з корупцією при фінансуванні політичних партій та виборчих кампаній. Стандарти, які належить застосовувати, включають: (a) ***вимоги щодо розумного балансу*** між публічним та приватним фінансуванням політичних партій; (b) застосування ***справедливих критеріїв*** розподілу державних внесків партіям; (c) встановлення чітких правил щодо приватних пожертв, зокрема й ***заборону чи обмеження внесків*** іноземних донорів, релігійних організацій та обмеження для корпорацій та анонімних пожертв; (d) ***обмеження витрат партій***, пов'язаних із виборчими кампаніями; (e) положення щодо прозорості пожертв і витрат політичних партій; та (f) заснування ***незалежного органу влади*** [для цілей аудиту. – *Прим. ред.*] та запровадження серйозних ***санкцій*** для тих, хто порушує відповідні правила.

60. Подібно в Керівних принципах щодо регулювання політичних партій[70] Венеційська комісія та ОБСЄ/БДІПЛ зазначають, що положення про виборчі кампанії повинні

- не допускати неналежного впливу (та забезпечувати незалежність партій) на політичні рішення шляхом фінансових пожертв;
- забезпечити прозорість витрат політичних партій;
- забезпечити, щоб усі політичні партії мали можливість конкурувати відповідно до принципу рівних можливостей.

61. Для досягнення цих цілей «основним шляхом регулювання агітаційної комунікації є виборче законодавство, що включає обмеження витрат та контроль за фінансуванням передвиборчої агітації; субсидії для агітаційних комунікацій; дні тиші перед голосуванням; регулювання засобів масової інформації, зокрема ліцензування мовлення; правила щодо політичної реклами, зокрема й неупередженість, субсидії та безоплатний ефірний час; а також саморегуляція і журналістська етика»[71].

70. CDL-AD(2010)024, p. 35, para. 159.
71. CoE Election Study 2017, p. 9.

62. Стандарти, що мають застосовуватися, було встановлено для того, щоб «захистити доброчесність виборів та забезпечити, щоб вони були вільними і чесними, а не були опановані вузьким колом інтересів»[72]. Проте законодавчі кроки, вжиті державами-членами, та запроваджені ними норми були зосереджені на офлайн-контексті[73]. Тому їхня ***застосовність й ефективність у часи цифрової політичної реклами*** виявилися ***надзвичайно обмеженими***. Як зазначалося вище, за останні роки політикам, урядам та так само громадянському суспільству довелося зустрітися з реаліями існування меж ***правозастосування чинних норм до інтернету***, зокрема й щодо застосовності чинного регулювання передвиборчої агітації.

63. А саме, законодавчі обмеження щодо фінансування агітації зустрілися з викликом нових форм цифрової реклами, що за своєю суттю є менш прозорими, аніж їхні аналогічні попередники, що тим самим підриває чинні визначення та обмеження, які ґрунтуються на конкретних типах засобів масової інформації. Запобіжники проти корупції, засновані на методах обчислення витрат та категоріях звітності про витрати на традиційних медіаканалах, втратили своє значення, коли політична агітація переміститилася в інтернет. У підсумку, абсолютні обмеження витрат, які застосовують щодо мовлення, також стають менш значущими, тоді як норми щодо прозорості, які забезпечують обізнаність громадян щодо фінансування агітації та витрат, важко, якщо не неможливо, запровадити через кордони у цифровому середовищі[74].

3. Політичні промови та висвітлення засобами масової інформації виборчих кампаній

64. Хоча «свобода вираження поглядів забезпечує життєздатність демократії», тепер усі правові системи мають норми та обмеження щодо фінансування кампаній та зобов'язання щодо прозорості. У приватній сфері вираження поглядів може заслуговувати на захист незалежно від змісту, але це не може стосуватися агітації. Переважна більшість, якщо не вся сукупність конституційних систем, передбачає обмеження свободи вираження поглядів під час виборчого процесу: наприклад, період тиші, санітарний кордон навколо виборчих дільниць, правила фінансування виборчих кампаній та зобов'язання щодо прозорості. Усі обмеження передвиборчої кампанії, навіть ті, що сприяють прозорості, належить розглядати насамперед як втручання, яке повинно бути виправданим у європейських системах у контексті перевірки на необхідність та пропорційність. Регулювання публікації політичної реклами виглядає правомірно припустимим у принципі щодо: a) унормування прозорості, а не змісту; b) регулювання політичної агітації; c) регулювання, або спрямованого на вибори чи опитування, або пов'язаного з механізмами фінансування, або яке спрямоване на встановлення походження поза політичною спіль-

72. CoE Election Study 2017, p. 9.

73. У цьому контексті проведення краудфандингових кампаній, переважно через інтернет, стає щораз більш важливим для зміни сфери фінансування виборчих кампаній.

74. CoE Election Study 2017, p. 20-21.

нотою. Хоча тут існують концепції, складні для закріплення, цілком можливо розробити схему для реклами в традиційній пресі, мовленні або на плакатах. Але якщо йдеться про цифрову сферу, то чим тут є публікація і хто є її видавцем? Коли повідомлення є «рекламним», а не індивідуальним висловленням думки, яка «стає вірусною»?

65. ЄСПЛ чітко вказав на відповідальність держави у запобіганні нерівності онлайн та офлайн медіависвітленні виборів[75], проте із істотними відмінностями щодо ***впливу*** між традиційними й новими медіа[76]. Тепер на карту поставлено питання, як чітко визначити ці відмінності: ***чи вони вже досягли «достатньо серйозного зрушення у відповідному впливі»***[77]. Найважливішим елементом моменту цього «зрушення» є визначення, чи повинна позитивна відповідальність держави за забезпечення рівного висвітлення політичних партій та кандидатів застосовуватися до нових інформаційних посередників і як саме.

66. Стандарти Ради Європи та інші документи у цій сфері спрямовані на ***забезпечення комунікаційного контексту, який уможливить реалізацію права на вільні вибори.*** Вони відображають позитивні зобов'язання держави забезпечити громадянам отримання необхідної та правдивої інформації про політичні партії для того, щоб підтримати їхній демократичний вибір із метою обрання своїх представників.

67. Рекомендація CM/Rec (2007) 15[78] стосується широкого кола засобів масової інформації безвідносно до тих засобів та технологій, які використовуються для розповсюдження їх контенту, надаючи керівні принципи щодо віль-ного та незалежного висвітлення засобами масової інформації політич-них кампаній, при цьому передбачаючи вищі стандарти для суспільних мовників. Рекомендація охоплює низку керівних принципів, спрямованих на забезпечення відповідального, точного та чесного висвітлення виборчих кампаній; однак суспільні мовники несуть особливе зобов'язання висвітлювати вибори «чесно, збалансовано та неупереджено, без дискримінації конкретної політичної партії чи кандидата». Що ж стосується загальних можливостей політичних партій та кандидатів звертатися до електорату, то Рекомендація залишає питання дозволу платної політичної реклами на розсуд окремих країн-членів. Проте якщо партії мають можливість придбати рекламний простір для цілей передвиборчої агітації, вони повинні мати змогу робити це за рівних умов та тарифів.

68. Навіть більше, Рекомендація встановлює декілька загальних вимог щодо забезпечення чесних та прозорих кампаній; наприклад, ***право на відпо-***

75. «Комуністична партія Росії та інші проти Росії» (Communist Party of Russia and Others v. Russia)», заява № 29400/05 (ЄСПЛ, 19 червня 2012 року).

76. «Енімал Дефендерз Інтернешнл проти Сполученого Королівства» (Animal Defenders International v. the United Kingdom), заява № 48876/08 (ЄСПЛ, 22 квітня 2013 року).

77. Там само, п. 119

78. Рекомендація CM/Rec(2007)15 Комітету Міністрів державам-членам щодо заходів стосовно медіависвітлення виборчих кампаній.

відь або еквівалентні засоби захисту, які повинні бути доступними кандидатам та/або політичним партіям так, щоб вони мали можливість ефективно реагувати на будь-які заяви, які можуть спричинити упереджене ставлення до них упродовж відносно короткої тривалості виборчих кампаній. Окрім того, ***способи та умови поширення результатів соціологічних опитувань*** повинні надавати громадськості достатню інформацію для розуміння значення опитувань, тоді як потенційний вплив виборчих повідомлень безпосередньо перед голосуванням пом'якшується положенням, яке дозволяє державам-членам розглянути можливість заборони поширення таких результатів у день, що передує голосуванню (так званий «день роздумів»). Крім того, Рекомендація чітко визначає ***вимоги щодо прозорості платного рекламного контенту та вимоги щодо власності на засоби масової інформації*** разом з ***власністю*** на носія (ці вимоги детально описано в Рекомендації CM/Rec(2018)1)[79]. Зазначені вище керівні принципи спрямовані передусім на лінійних (приватних та публічних) мовників з поширенням на нелінійні аудіовізуальні послуги суспільних мовників. Однак разом із переходом політичної агітації в онлайн протягом останнього десятиліття ефективність такої агітації у соціальних медіа, як виявилося, знизилась.

69. Такий перехід агітації з офлайн- в онлайн-простір відображено в Рекомендації CM/Rec (2018) 1, у якій чітко вказано на потенційно тривожний вплив, якого може зазнати ***медіаплюралізм*** внаслідок контролю з боку онлайн-платформи над потоком, наявністю, простотою пошуку та доступністю інформації. Вибіркове висвітлення медіаконтенту, що призводить до потенційної фрагментації суспільства, ідентифікується як одна з основних проблем, особливо під час виборів. Тому Рекомендація закликає держави виконати своє позитивне зобов'язання та виступити головним гарантом медіаплюралізму, ***забезпечивши плюралізм у всій мультимедійній екосистемі.***

70. Таке тлумачення підсилюється Рекомендацією CM/Rec(2018)2[80], яка розглядає ролі та відповідальність інтернет-посередників щодо своїх користувачів і держав-членів, приділяючи належну увагу зростанню їх влади над комунікацією та розповсюдженням інформації. У цьому контексті потрібно пам'ятати про потенційну співвідповідальність посередників за контент, який вони зберігають, у тому разі, якщо вони не діють оперативно, щоб обмежити доступ до контенту чи послуг невідкладно після отримання інформації про їхню протиправність (відповідно до принципів законності, необхідності та пропорційності). Тим часом для посередників не потрібно встановлювати загального зобов'язання контролювати контент, до якого вони просто надають доступ або який вони передають чи зберігають. У зв'язку з цим варто також звернути увагу на Рекомендацію CM/Rec(2016)1, яка закликає держави-члени забезпечити принцип нейтральності мережі під час розробки національної нормативно-пра-

79. Recommendation CM/Rec (2018) 1 on media pluralism and transparency of media ownership.
80. Recommendation CM/Rec (2018) 2 on the roles and responsibilities of internet intermediaries.

вової бази, щоб забезпечити захист права на свободу вираження поглядів та на доступ до інформації, а також право на приватність[81].

71. У своїй Декларації Decl(13/02/2019)1 від 13 лютого 2019 року[82] про маніпулятивні можливості алгоритмічних процесів Комітет Міністрів наголосив на «необхідності оцінки нормативної бази, пов'язаної з політичною комунікацією та виборчими процесами, щоб захистити справедливість і доброчесність виборів як у режимі офлайн, так і в режимі онлайн, відповідно до встановлених принципів. Зокрема, необхідно забезпечити, щоб виборці мали доступ до інформації щодо усього політичного спектру, яку можна порівнювати, щоб виборці усвідомлювали небезпеку політичної практики «червоних ліній», яка виникає, коли політична агітація обмежується тими, хто найбільше піддається впливу, а також гарантувати, що виборці ефективно захищені від недобросовісної практики та маніпуляцій.

72. Парламентська Асамблея у своїй Резолюції 2254 (2019) про свободу засобів масової інформації як умову демократичних виборів[83] закликала держави-члени впроваджувати ефективні стратегії захисту виборчого процесу від маніпуляцій інформацією та протиправної пропаганди через соціальні медіа. Вона пропонує такі заходи, як розробка специфічних нормативних рамок для інтернет-контенту в період виборів та встановлення чіткої правової відповідальності для компаній-власників соціальних медіа, які публікують незаконний контент, який шкодить кандидатам, з уникненням особливих заходів, як блокування сайтів у цілому. Парламентська Асамблея також закликала організації в медіасекторі розробити рамки саморегулювання з професійними та етичними стандартами висвітлення виборчих кампаній, а інтернет-посередників – до співпраці з громадянським суспільством та організаціями всіх політичних спрямувань, що спеціалізуються на верифікації контенту задля забезпечення того, що всю інформацію буде підтверджувати авторитетне стороннє джерело.

B. ПРАВО НА ПРИВАТНІСТЬ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

73. Стаття 8 ЄКПЛ передбачає захист права на приватне життя. На цій основі ЄСПЛ розвинув широку практику щодо захисту персональних даних[84].

74. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних ETS № 108 1981 року встановлює принципи

81. Рекомендація CM/Rec(2016)1 щодо захисту та просування права на свободу вираження поглядів та права на приватне життя у мережі.

82. Декларація Decl(13/02/2019)1 щодо маніпулятивних можливостей алгоритмічних процесів, search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b.

83. Резолюція 2254(2019) про медіа свободу як умову для демократичних виборів, assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=25409&lang=en.

84. Практика Європейського суду з прав людини у справах щодо захисту персональних даних; доступно за посиланням: rm.coe.int/case-law-on-data-protection/1680766992. Див. також: ECtHR, 2018, "Європейський суд з прав людини, 2018, «Посібник щодо Статті 8 Європейської конвенції з прав людини – Право на повагу до приватного та сімейного життя», доступно за посиланням: www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

та правила обробки персональних даних, а також права індивідів. Додатковий протокол до Конвенції 2011 року визначає стандарти для створення наглядових органів щодо захисту даних. Особлива цінність цієї нормативно-правової бази порівняно із Загальним регламентом щодо захисту даних ***(General Data Protection Regulation)*** Європейського Союзу полягає в тому, що, будучи відкритою для підписання будь-якою країною світу, вона надає можливість різним правовим системам «перебувати під однією парасолькою», гармонізуючи так різні правові режими[85].

75. 10 жовтня 2018 року новий протокол, що оновлює положення Конвенції, підписала 21 держава-учасниця Конвенції (надалі – Модернізована Конвенція). Стаття 5 Модернізованої Конвенції посилює принципи захисту даних, вимагаючи, щоб дані обробляли чесно та прозоро, щоб їх збирали для явних, визначених і легітимних цілей і не обробляли їх способом, несумісним із цими цілями, тоді як будь-яка подальша обробка з метою архівування в суспільних інтересах, з метою наукових чи історичних досліджень або для статистичних цілей підлягає відповідним запобіжникам, сумісним із цими цілями. Навіть більше, Модернізована Конвенція передбачає додаткові принципи та вимоги, такі як конфіденційність із вбудованим у систему захистом, оцінка впливу персональних даних та конфіденційність за замовчуванням, а також обов'язкове повідомлення про порушення щодо захисту даних принаймні до органів захисту даних. Вона запроваджує додаткові запобіжники з огляду, зокрема, на повсюдну присутність інформаційних технологій в обробці даних, а також визнає нові категорії даних як такі, що мають чутливу природу. Додаткові запобіжники особливо стосуються обробки чутливих даних, таких як політичні погляди. Модернізована Конвенція передбачає більш детальні положення щодо транскордонних потоків даних, додаткові вимоги до володільців даних та механізму подальшого контролю.

76. Крім того, існує значна кількість правових актів Ради Європи, що стосуються захисту персональних даних у межах функціонування соціальних мереж.

77. Рекомендація Комітету Міністрів від 1999 року № R(99)5 щодо захисту приватності в інтернеті містить Керівні принципи щодо захисту індивідів у процесі збирання та обробки персональних даних на інформаційних магістралях. Рекомендація CM/Rec(2010)13 про захист індивідів щодо автоматичної обробки персональних даних у контексті профілювання передбачає умови такої обробки та встановлює детальний перелік інформації, яку необхідно надавати суб'єктам даних. Вона відзначає, що відсутність прозорості чи навіть «невидимість» профілювання та брак точності, що може бути наслідком автоматичного застосування встановлених правил припущення, здатні спричинити значні ризики для прав і свобод індивіда. Хоча спочатку профілювання сприймали як техніку, яку використовують у бізнесі та маркетинговому контексті, останні події демонструють, що профілювання також застосовують і у виборчих процесах.

85. Це стосується як неєвропейських країн (Кабо-Верде, Маврикій, Мексика, Сенегал, Туніс та Уругвай), так і європейських країн (наприклад, Албанія, Росія, Сербія, Туреччина, Україна).

78. Резолюція № 3 Міністрів юстиції 2010 року про захист даних та приватність у III тисячолітті, MJU-30 (2010) RESOL, відзначає ймовірні наслідки широкого використання інформаційно-комунікаційних технологій (ІКТ), що дозволяє спостерігати, зберігати та аналізувати більшу частину повсякденної діяльності людини, тим самим потенційно створюючи ефект страху, пов'язаний із відчуттям нагляду, що може погіршити вільне користування правами людини та основними свободами, якщо надійні стандарти захисту даних належним чином не будуть ефективно дотримуватися в усьому світі. Резолюція Парламентської Асамблеї 2011 року 1843 (2011) про захист приватності та персональних даних в інтернеті та в онлайн-медіа підкреслює, що захист права на захищеність [персональних] даних є необхідною складовою людського життя та гуманного функціонування демократичного суспільства і що порушення такого права впливає на гідність, свободу й безпеку особи.

79. Рекомендація Комітету Міністрів CM/Rec(2012)3 2012 року щодо захисту прав людини щодо пошукових систем визнає виклик, спричинений тим, що історія пошуку індивіда містить слід, який може розкрити вірування, інтереси, стосунки чи наміри особи, а також встановити, ***inter alia***, політичні погляди, релігійні чи інші переконання. Вона закликає вжити заходів щодо посиленого дотримання принципів захисту даних, зокрема обмеження цілей, мінімізації даних та обмеженого зберігання даних, тоді як суб'єкти даних повинні бути обізнані з обробкою й отри-мувати всю відповідну інформацію.

80. Рекомендація CM/Rec(2012)4 щодо захисту прав людини стосовно сервісів соціальних мереж вказує на все більш помітну роль таких та інших сервісів соціальних медіа, які пропонують великі можливості для посилення потенціалу участі індивідів у політичному, суспільному та культурному житті. Вона рекомендує дії, спрямовані на забезпечення середовища для користувачів соціальних мереж, що дозволяє їм надалі користуватися своїми правами та свободами, піднімати рівень усвідомлення користувачами можливих викликів їхнім правам людини і негативного впливу на права інших людей при використанні цих сервісів, а також підвищити прозорість щодо обробки даних та заборонити протиправну обробку персональних даних. Ці заходи можуть бути вжиті шляхом залучення провайдерів соціальних мереж. Рекомендація також підкреслює, що користувачі мають бути поінформовані про те, де використовуються їхні персональні дані в контексті профілювання.

81. Декларація Комітету Міністрів від 2013 року про ризики для основних прав, що випливають із цифрового відстеження та інших технологій спостереження, підкреслює, що держави-члени мають не лише негативне зобов'язання утримуватися від втручання в права людини, а й позитивне повноваження активно захищати ці права, що включає захист індивідів від дії недержавних суб'єктів. Розповсюджене використання різних пристроїв та інформації, зібраної за допомогою цих пристроїв, робить можливим

відстеження і спостереження за людьми, а відтак дозволяє виявляти делікатну та/або чутливу персональну інформацію, зокрема й політичні чи релігійні вподобання, що може бути зібрано для формування їх детальних та ретельних профілів.

82. Рекомендація Комітету Міністрів CM/Rec(2014)6 2014 року надає Посібник з прав людини для інтернет-користувачів, а в 2017 році Комітет Конвенції ETS 108 прийняв Керівні принципи щодо захисту осіб у зв'язку з обробкою персональних даних у світі великих даних. У своїй Декларації Decl (13/02/2019) 1 від 13 лютого 2019 року про маніпулятивні можливості алгоритмічних процесів Комітет Міністрів закликав держави-члени «розглянути потребу додаткових захисних рамок, пов'язаних із даними, що виходять за межі сучасних уявлень про захист персональних даних і приватність, та більш широко розглянути питання важливості подолання значного впливу цілеспрямованого використання даних на суспільство і на реалізацію прав людини».

83. Насамкінець, Рада Європи розробила або замовила різні доповіді та дослідження у цій сфері, зокрема й доповідь про «використання інтернету та пов'язаних із ним сервісів, приватне життя та захист даних: тенденції і технології, загрози та наслідки»[86]. Ця доповідь містить заклик щодо підтвердження та захисту права на анонімність в інтернеті, регулювання та суворого обмеження створення й використання профілів у різних контекстах всіх видів, а також до прийняття Радою Європи керівних принципів щодо обмежень, які потрібно застосовувати до технологій спостереження, включно з міжнародною торгівлею такими технологіями.

C. ЗАХИСТ ВІД КІБЕРЗЛОЧИННОСТІ

84. Конвенція Ради Європи про кіберзлочинність ETS185 2001 року (Будапештська конвенція) стосується двох типів загроз для виборчої демократії[87]. По-перше, це атаки на конфіденційність, цілісність і доступність виборчих комп'ютерів та даних, що є такими формами кіберзлочинності, як протиправний доступ до комп'ютерних систем (стаття 2), протиправне перехоплення (стаття 3), втручання в дані та систему (статті 4 та 5) та інші. По-друге, це дезінформаційні операції, коли порушуються норми щодо захисту персональних даних, політичного фінансування, висвітлення виборів у засобах масової інформації чи в мовленні, тобто норм, які забезпечують вільні, чесні та чисті вибори.

85. Хоча другий тип поведінки сам по собі не є кіберзлочинністю, докази того, що такі норми порушуються, часто мають форму електронних доказів. Тому істотно, щоб держави надавали своїм органам кримінальної юстиції

86. Korff, 2013, доступно за посиланням: rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168067f7f4.

87. Подальша інформація ґрунтується на доповіді Александра Сеґера (Виконавчий секретар Комітету з питань кіберзлочинності Ради Європи) на 15-й Європейській конференції органів адміністрування виборів, Осло, Норвегія, 19-20 квітня 2018 року.

необхідні повноваження, щоб забезпечити отримання таких доказів. Від держав-учасниць Будапештської конвенції вимагається діяти так відповідно до статей 16-21, які охоплюють повноваження, що встановлюються процесуальним законодавством, такі як прискорене збереження даних, пошук та вилучення комп`ютерних систем і даних, судові накази про надання інформації тощо.

86. Основна проблема полягає в тому, що дані – а відповідно і електронні докази – є нестабільними і часто утримуються постачальниками послуг у закордонних юрисдикціях або зберігаються у багатьох, змінних або невідомих юрисдикціях, тобто «десь на серверах у хмарі»[88]. Визначити суб'єкта атаки або просто встановити користувача адреси інтернет-протоколу (IP) чи власника соціального медіа або облікового запису електронної пошти часто неможливо в межах розумних зусиль. Це одна з причин, чому кіберзлочинність та інші кіберзагрози виборчій демократії переслідуються дуже рідко.

87. Ефективне міжнародне співробітництво та співпраця з постачальниками послуг гарантується. Будапештська конвенція в її поточній формі містить детальні положення про міжнародне співробітництво, поєднуючи прискорені тимчасові заходи щодо захисту даних (наприклад, стаття 29 про прискорене збереження та стаття 35 про контактні пункти 24/7) з положеннями про взаємну правову допомогу. Ці положення постійно використовуються для розслідування кіберзлочинів.

88. Проте вони недостатньо вирішують проблему хмарних обчислень та пов'язані з ними проблеми юрисдикції, а також той факт, що постачальники послуг в одній державі пропонують свої послуги у багатьох інших без юридичної чи фізичної присутності чи підзвітності в таких державах.

89. З цієї причини держави-учасниці Будапештської конвенції розпочали переговори щодо Другого додаткового протоколу, щоб уможливити додаткові варіанти посилення міжнародного співробітництва та доступу до даних у хмарі. Запропоновані рішення передбачають пряму співпрацю з постачальниками послуг в інших державах-учасницях, розширення пошуків на комп'ютерах в інших юрисдикціях за обмежених обставин, а також екстрену взаємодопомогу. Очікується, що переговори триватимуть до кінця 2019 року[89].

VI. ІНШІ МІЖНАРОДНО-ПРАВОВІ НОРМИ ТА НАЦІОНАЛЬНЕ ЗАКОНОДАВСТВО, ПРЕЦЕДЕНТНЕ ПРАВО ТА ІНІЦІАТИВИ[90]

A. МІЖНАРОДНИЙ РІВЕНЬ

90. На рівні Організації Об'єднаних Націй у Спільній декларації про свободу слова та інтернету ***(Joint Declaration on Freedom of Speech and Internet)*** від

88. Детальну довідкову інформацію див. у доповідях, підготованих Групою з питань хмарних доказів Комітету з питань кіберзлочинності: www.coe.int/en/web/cybercrime/ceg (звернення 30 вересня 2018 року).

89. Див.: www.coe.int/en/web/cybercrime/t-cy-drafting-group.

90. Ця доповідь не містить вичерпного опису національних матеріалів. Див. також: CDL-AD(2019)016.

1 червня 2011 року[91] було зазначено, що підходи до регулювання, розроблені для інших засобів комунікації, таких як телефонні послуги чи мовлення, дуже відрізняються від підходів, необхідних для інтернету, і такі методи повинні бути розроблені спеціально для нього. Нещодавня Спільна декларація від 3 березня 2017 року тепер включає «фейкові новини», дезінформацію і пропаганду та підкреслює необхідність надання пріоритету свободі слова, стверджуючи, що заборони на розповсюдження інформації, базованої на сумнівних і неоднозначних ідеях, зокрема й «фейкових новин» або «необ'єктивної інформації», є несумісними із міжнародними стандартами щодо обмеження свободи вираження поглядів, як вони встановлені в пункті 1(a)[92], і повинні бути скасовані.

91. Зростаюче усвідомлення необхідності запобігати неправдивим новинам та обмежити їх розповсюдження, зокрема під час виборчих періодів, сфокусувало увагу різних досліджень, освіти та співпраці на саморегуляторних та регуляторних рішеннях, зокрема й на міжнародному рівні. У НАТО створено центр передового досвіду (Stratcom Centre of Excellence), аналітичний центр, який зосереджується на питаннях впливу інформаційного домінування в інтернеті та кіберзахисту. У результаті співпраці між ЄС та НАТО щодо гібридних загроз у 2017 році було започатковано Європейський центр передового досвіду з протидії гібридним загрозам (European Centre of Excellence for Countering Hybrid Threats)[93].

92. Існує декілька мереж людей, які працюють разом для перевірки фактів в онлайн-інформації, наприклад, Міжнародна мережа перевірки фактів (International Fact-Checking Network, IFCN) працює як підрозділ Інституту Пойнтера (the Poynter Institute), її діяльність присвячена об'єднанню осіб, які займаються перевірками фактів у всьому світі. IFCN була створена у 2015 році для підтримки та вивчення роботи 64 організацій з усього світу, що перевіряють факти.

B. ЄВРОПЕЙСЬКИЙ СОЮЗ

93. У січні 2018 року Європейська Комісія створила групу високого рівня експертів (HLEG) для консультування щодо ініціатив з розробки політики для протидії «фейковим новинам» та дезінформації, що поширюються

91. Декларація підписана 1 червня 2011 року Спеціальним доповідачем із питань свободи думки і вираження поглядів ООН, Представником ОБСЄ із питань свободи медіа, Спеціальним доповідачем із питань свободи вираження поглядів Організації Американських Держав (OAS) та Спеціальним доповідачем із питань свободи вираження поглядів і доступу до інформації Африканської комісії з питань прав людини і народів *(ACHPR)*.

92. Держави можуть встановлювати обмеження права на свободу вираження поглядів лише відповідно до тесту щодо таких обмежень, передбаченого міжнародним правом, а саме: обмеження мають бути встановлені законом, служити одному з законних інтересів, визнаних міжнародним правом, і бути необхідними та пропорційними для захисту цього інтересу.

93. Див. також практичний посібник із використання соціальних медіа під час виборчого процесу, розроблений Міжнародним інститутом демократії та сприяння виборам *(International IDEA)* для органів адміністрування виборів: Seema Shah, «Guidelines for the Development of a Social Media Code of Conduct for Elections», International IDEA, 2015. Посібник доступний за посиланням: www.idea.int/sites/default/files/publications/social-media-guide-for-electoral-management-bodies.pdf.

онлайн. У своїй Підсумковій доповіді [94] HLEG рекомендувала запровадити багатовимірний підхід, який ґрунтуватиметься на п'яти опорах, призначених для того, щоб:

i) підвищити прозорість новин у мережі;

ii) сприяти медіа- та інформаційній грамотності для протидії дезінформації;

iii) розробити інструменти для розширення можливостей користувачів і журналістів для подолання дезінформації;

iv) захищати різноманітність та сталість екосистеми європейських новинних засобів масової інформації;

v) сприяти продовженню досліджень впливу дезінформації в Європі.

94. Спираючись на результати діяльності HLEG, Європейська Комісія у квітні 2018 року опублікувала Комюніке, у якому окреслено стратегію Комісії щодо вирішення проблеми онлайн-дезінформації [95]. Така стратегія не передбачає регуляторного втручання і має такі основні напрями дій: i) розробка амбітного саморегуляторного Кодексу практики (Code of Practice) провідних суб'єктів ринку (включно із соціальними мережами, рекламодавцями та іншими суб'єктами рекламної індустрії); ii) посилення перевірки фактів та здатності контролю дезінформації; iii) використання нових технологій (наприклад, штучного інтелекту) для подолання дезінформації; iv) зміцнення виборчих процесів; v) посилення розвитку освіти та медіаграмотності.

95. Кодекс практики щодо дезінформації (the Code of Practice on Disinformation) було прийнято у вересні 2018 року [96] з метою захисту майбутніх виборів у ЄС. Кодекс спрямований на:

- забезпечення прозорості щодо спонсорованого контенту, зокрема політичної реклами, а також обмеження опцій таргетування політичної реклами і зменшення доходів постачальників дезінформації;
  надання більшої чіткості щодо функціонування алгоритмів та уможливлення верифікації з боку третіх сторін;
- спрощення для користувачів відкриття та доступу до різних джерел новин, що надають альтернативні точки зору;
- запровадження заходів для ідентифікації та закриття фейкових акаунтів і вирішення проблеми автоматичних ботів;

94. Див.: ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

95. Заява Комісії до Європейського Парламенту, Ради, Європейського Комітету з економічних та соціальних питань та Комітету з питань регіонів щодо «Вирішення питання онлайн-дезінформації: європейський підхід», COM(2018)236final. Доступно за посиланням: eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0236&from=EN.

96. Доступно за посиланням: ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

- надання можливості фахівцям з перевірки фактів, дослідникам та органам державної влади здійснювати постійний моніторинг онлайн-дезінформації.

96. Європейська комісія завдяки Рамковій програмі «Горизонт 2020» (Framework Programme Horizon 2020) досліджень та інновацій підтримала також декілька інноваційних заходів із метою розробки нових інструментів і сервісів для допомоги фахівцям та громадянам у перевірці онлайн-контенту (тексту, зображення та відео). Навіть більше, вона створить незалежну Європейську мережу фахівців з перевірки фактів (European network of fact-checkers), яких відбиратимуть із європейських членів Міжнародної мережі перевірки фактів (International Fact-Checking Network, IFCN). Мережа розвиватиме методи роботи та встановлюватиме найкращі практики, щоб здійснити якомога більше фактологічних виправлень. Для того, щоб допомогти їй досягти своєї мети, Комісія надасть мережі необхідні онлайн-інструменти та безпечну європейську онлайн-платформу з питань дезінформації. Завдяки механізму Connect Europe Facility (CEF) Комісія також підтримає розгортання Європейської платформи щодо дезінформації для того, щоб збільшити здатність виявлення та аналізу дезінформаційних кампаній у всій Європі.

97. У вересні 2018 року Європейська Комісія надала конкретні рекомендації з метою захисту демократичних процесів Європи від маніпуляцій із боку третіх країн чи приватних інтересів та запропонувала нові правила щодо мереж співпраці з виборчих питань, онлайн-прозорості, захисту у разі інцидентів з кібербезпекою та кроків, спрямованих на протидію кампаніям дезінформації у контексті європейських виборів [97]. У грудні 2018 року було прийнято План дій проти дезінформації [98], спрямований на розбудову спроможностей та зміцнення співробітництва між країнами-членами й інституціями ЄС із метою протистояння загрозам, породженим дезінформацією. Також увагу приділено висновку Європейського органу з нагляду за захистом даних [99] (European Data Protection Supervisor), виданого у березні 2018 року, щодо онлайн-маніпуляцій та персональних даних, який рекомендує, щоб правила захисту даних були доповнені та поси лені, щоб регулятори намагалися здійснювати колективну діагностику проблеми та співпрацювати в міжсекторному контексті, щоб заохочувалися саморегулювання та кодекси поведінки, а також щоб індивіди були спроможними реалізовувати свої права, включаючи вчинення колективних дій.

98. Серед уже наявних нормативних актів ЄС у цьому контексті особливо актуальними є такі:

97. Заява Комісії до Європейського Парламенту, Ради, Європейського Комітету з економічних та соціальних питань та Комітету з питань регіонів щодо «Забезпечення вільних та чесних європейських виборів», COM(2018)637final. Доступно за посиланням: eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:637:FIN.

98. Див.: ec.europa.eu/digital-single-market/en/news/europe-protects-eu-steps-action-against-disinformation.

99. Доступно за посиланням: edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

- Загальний регламент захисту даних (General Data Protection Regulation, GDPR)[100], який безпосередньо застосовують у ЄС із 25 травня 2018 року. Його положення є обов'язковими і надають індивідам численні права, зокрема й права на прозорі комунікації, стирання (право бути забутим) та право переносити дані (тобто передавати від одного володільця даних до другого). Регламент передбачає загальну заборону обробки персональних даних, «що розкривають расове чи етнічне походження, політичні погляди, релігійні чи філософські вірування, членство в професійних спілках, і опрацьовують генетичні дані, біометричні дані з метою однозначної ідентифікації фізичної особи, дані щодо стану здоров'я чи дані про статеве життя фізичної особи або її сексуальну орієнтацію», за деякими винятками, особливо коли «обробка є необхідною з підстав істотного суспільного інтересу, на основі законодавства Союзу або держави-члена, що має бути пропорційним до поставленої мети, поважати сутність права на захист даних і передбачати належні та конкретні заходи для захисту основоположних прав та інтересів суб'єкта даних». Права, встановлені GDPR, можуть здійснюватися та забезпечуватися не лише індивідами, але й організаціями, які діють від імені індивідів. Щоб заповнити прогалину захисту від неналежної обробки персональних даних за межами ЄС, GDPR поширює правовий захист на обробку персональних даних суб'єктів даних ЄС, «безвідносно до того, де проводиться діяльність з обробки». Це робить його застосовним також до організацій, створених за межами ЄС, якщо вони пропонують товари чи послуги індивідам у Союзі або якщо вони здійснюють моніторинг їхньої онлайн-поведінки. Регламент передбачає жорсткі норми щодо передання даних за межі Союзу; суб'єкти обробки даних повинні вести записи усіх дій з обробки. Вони несуть відповідальність за вжиття всіх необхідних заходів, щоб гаран-тувати, що обробка персональних даних здійснюється правомірно, чесно та прозоро. Отже, GDPR має потенціал запобігти несанкціонованій обробці персональних даних для виборчих цілей, як це було у випадку з Cambridge Analytica[101].

- Регламент (EU) 2015/2120, що встановлює заходи щодо відкритого доступу до інтернету [102] і є чинним від 30 квітня 2016 року, створює індивідуальне та захищене право для кінцевих користувачів у ЄС на доступ та розповсюдження інтернет-контенту й сервісів на свій вибір, а також закріплює принцип недискримінаційного управління трафіком. Застосування норм відкритого інтернету в межах ЄС є завданням національних регуляторних органів, які повинні дотримуватися настанов, прийнятих бюро Європейських регуляторів електронних комунікацій (the body of European Regulators for Electronic Communications,

100. Доступно за посиланням: ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

101. Щодо інформації про імплементацію *GDPR* у різних європейських країнах див.: www.gdprtoday.org/gdpr-loopholes-facilitate-data-exploitation-by-political-parties.

102. Доступно за посиланням: eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R2120.

BEREC) у 2016 році. Відповідно до них, завдання судити про успіх чи невдачу розповсюджених сервісів та контенту не покладається на постачальників інтернет-сервісів. Ці норми закріплюють принцип нейтральності мережі у праві ЄС і прагнуть не допустити блокування, припинення чи дискримінації онлайн-контенту, додатків та сервісів[103].

- Директива 2000/31/ЕС Європейського Парламенту та Ради[104] містить винятки з відповідальності, що надаються певним провайдерам онлайн-сервісів, зокрема й провайдерам послуг «хостингу» за умови, що вони оперативно діють, видаляючи або унеможливлюючи доступ до протиправної інформації, яку вони зберігають, ***при отриманні фактичного повідомлення про наявність такої інформації***. У зв'язку з цим потрібно зазначити, що Європейська Комісія в декількох останніх комюніке наголошувала на потребі того, щоб онлайн-платформи діяли більш відповідально й активізували зусилля щодо саморегулювання в усьому ЄС для видалення протиправного контенту; 1 березня 2018 року Комісія прийняла Рекомендацію щодо заходів ефективного подолання незаконного онлайн-контенту (Recommendation on measures to effec-tively tackle illegal online content)[105], яка спрямована на країни-члени та провайдерів послуг хостингу і яка має за мету підвищити прозорість та точність механізмів сповіщення та дій.

C. ПРИКЛАДИ НА НАЦІОНАЛЬНОМУ РІВНІ

99. Нещодавно декілька держав прийняли – або планують прийняти – законодавство для регулювання онлайн-контенту та протидії політичній дезінформації з політичним навантаженням під час виборів. Німеччина діяла першою[106], зобов'язуючи інтернет-посередників (таких як Facebook, Instagram, Twitter або YouTube) негайно видаляти на підставі скарги будь-який незаконний контент, який визначено як такий у Кримінальному кодексі; очевидно незаконний контент повинен бути заблокованим або видаленим протягом 24 годин. Шкала злочинів охоплює від промов, що пропагують ненависть, та певних дифамаційних злочинів до контенту, що становить загрозу конституційному ладу чи національній безпеці і т. ін., який може чинити безпосередній вплив на обговорення та погляди в суспільстві, особливо під час виборів (цей закон є загальним, він не регулює безпосередньо виборчі кампанії). Закон про правозастосування в мережі (Network Enforcement Act), який набрав чинності на початку 2018 року, передбачає штрафи до 50 мільйонів євро, які можуть бути застосовані навіть тоді, коли правопорушення не було вчинено в Німеччині.

103. Див.: ec.europa.eu/digital-single-market/en/open-internet-net-neutrality.
104. Доступно за посиланням: eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031.
105. Доступно за посиланням: ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online.
106. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz NetzDG) – Закон про правозастосування в мережі *(Network Enforcement Act)*, germanlawarchive.iuscomp.org/?p=1245.

100. У листопаді 2018 року парламент Франції прийняв закон про боротьбу з маніпулюванням інформацією[107] під час виборчих періодів, який спрямовано на виявлення та блокування умисних тверджень про фальшивий чи оманливий факт на онлайн-платформі протягом тримісячного періоду перед виборами. Відповідно до нового законодавства, платформи підлягають обов'язку щодо прозорості: вони повинні надавати чітку, правильну та прозору інформацію про власну ідентичність і якість або про третю сторону, для якої платформи спонсорують контент; вони також повинні оприлюднити суму коштів, отриманих в обмін на спонсорство контенту. Прокурор чи будь-яка особа, яка має законний інтерес для внесення справи до суду на підставі невідкладності, а також партія чи кандидати можуть подати скаргу щодо відомостей, які начебто фальшиві чи неправдиві, які свідомо, штучно та масово розповсюджуються онлайн; власне поняття штучного і широкого розповсюдження вказує на неправдивість інформації. Суддя зобов'я-заний розглянути справу такого типу протягом 48 годин і має право заблокувати публікацію та змусити платформу припинити цю кампанію. Технічні посередники, які є особами, що пропонують доступ до послуг зв'язку, повинні негайно видаляти будь-який незаконний контент, про який їм стало відомо, та впроваджувати легкодоступний і видимий механізм, який дозволить особам повідомляти про будь-які фальшиві новини. Навіть більше, французький орган регулювання мовлення має право відмовити у підписанні конвенції з іноземною країною, якщо діяльність останньої може серйозно дестабілізувати життя нації шляхом поширення фальшивих новин або порушеного плюралізму напрямів думок[108].

101. Росія[109], Сінгапур[110] та Філіппіни безпосередньо цитують німецький закон як позитивний приклад, оскільки вони планують запровадити або вже запровадили законодавство щодо видалення «незаконного» онлайн-контенту[111].

---

107. Loi n° 2018 1202 relative à la lutte contre la manipulation de l'information, www.legifrance.gouv.fr/affichTexte.do;jsessionid=EDB587F21F791D8941E5E11E82A0320A.tplgfr22s_1? cidTexte=JORFTEXT000037847559&categorieLien=id.

108. Цей французький закон свого часу став об'єктом значної критики, див.: www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law. Щодо Німеччини див., наприклад, www.dw.com/en/germany-implements-new-internet-hate-speech-crackdown/a-41991590 та www.economist.com/europe/2018/01/13/germany-is-silencing-hate-speech-but-cannot-define-it.

109. Федеральний закон «Про інформацію, інформаційні технології та захист інформації» (від 27 липня 2006 року № 149-ФЗ) було прийнято 18 березня 2019 року. Він передбачає покарання за розповсюдження «ненадійної соціально важливої інформації», яка може наражати на небезпеку життя та здоров'я населення, підвищувати загрозу масового порушення громадської безпеки тощо. Цей закон дозволяє блокувати веб-сторінку, що містить таку інформацію. Того самого дня було прийнято Федеральний закон № 30-ФЗ («Закон про неповагу») шляхом доповнення статтею 15-1-1 Федерального закону «Про інформацію, інформаційні технології та захист інформації» (від 27 липня 2006 року № 149-ФЗ). Ця стаття встановлює покарання за висловлювання, які «демонструють неповагу до суспільства, держави, офіційних державних символів... та органів державної влади» і які виражено в «нецензурному вигляді». До Кодексу про адміністративні правопорушення було внесено зміни у вигляді запровадження штрафів за публікації, що містять «нецензурну неповагу» та «фейкові новини».

110. Див.: techcrunch.com/2019/05/09/singapore-fake-news-law/?renderMode=ie11&guccounter=1&guce_referrer_us=aHR0cHM6Ly90ZWNoY3J1bmNoLmNvbS8yMDE5LzA1LzA5L3NpbmdhcG9yZS1mYWtlLW5ld3MtbGF3Lw&guce_referrer_cs=oKT9smcHtaNhdWGcU8VGvg; https://mediawrites.law/fake-news-law-passed-in-singapore-protection-from-online-falsehoods-and-manipulation-act.

111. Див.: www.hrw.org/news/2018/02/14/germany-flawed-social-media-law.

102. Британська виборча комісія закликала збільшити прозорість цифрових виборчих кампаній для виборців. Вона надала рекомендації щодо відповідальності цифрових кампаній, витрат на цифрові кампанії, прозорості платежів за цифрові кампанії та виконання цих правил[112].

103. У США двопартійний Закон про чесну рекламу (Honest Ads Act), внесений у жовтні 2017 року до Конгресу США[113], передбачає правила розкриття інформації та відмови від відповідальності щодо політичної реклами онлайн. Хоча від телебачення та радіомовлення давно вимагається розголошувати покупців та контент щодо усіх, хто купує рекламу на їхніх станціях, від інтернет-компаній цього досі не вимагалося. Закон про чесну рекламу передбачає зобов'язати інтернет-компанії розкривати ідентичність та зміст реклами, пов'язаної з виборами чи кампаніями. Зокрема, це передбачається зробити внесенням змін до прийнятого кілька десятиліть тому закону про фінансування кампаній 1971 року через доповнення переліку форм медіа, на які поширюється дія цього закону, фразою «платний інтернет або платний цифровий зв'язок». Він також вимагатиме від будь-якого сайту, що має щонайменше 50 мільйонів відвідувачів щомісяця, зокрема й Facebook, Google та Twitter, вести публічний список усіх організацій чи осіб, які витрачають щонайменше 500 доларів на рекламні матеріали, пов'язані з виборами. Виняток зроблено для «новин, коментарів чи редакційних матеріалів», щоб гарантувати, що ці вимоги не застосовуються до справжніх новинних сюжетів чи коментарів.

104. У деяких країнах створені або створюються спеціалізовані підрозділи для боротьби з інформаційним безладом, наприклад:

- a) У Сполученому Королівстві планується сформувати підрозділ з національної безпеки зв'язку для боротьби з дезінформацією «фейковими новинами».

- b) У Чеській Республіці Центр проти тероризму та гібридних загроз, складова Міністерства внутрішніх справ, є спеціалізованим аналітичним і комунікаційним підрозділом, який здійснює моніторинг загроз, безпосередньо пов'язаних із внутрішньою безпекою, що передбачає широкий спектр загроз та потенційних інцидентів, пов'язаних з тероризмом, атак, спрямованих на програмне забезпечення, безпекових аспектів міграції, екстремізму, публічних зібрань, порушення громадського порядку та різних злочинів, але й також дезінформаційних кампаній, пов'язаних із внутрішньою безпекою. Центр також розробляє пропозиції щодо рішень по суті та рішень на законодавчому рівні, які також і застосовує там, де це можливо, і поширює інформацію про ці проблеми та їх усвідомлення серед широкого загалу й фахівців.

112. Див.: www.electoralcommission.org.uk/__data/assets/pdf_file/0010/244594/Digital-campaigning-improving-transparency-for-voters.pdf.

113. Див.: www.congress.gov/search?q=%7B%22source%22%3A%22legislation%22%2C%22search%22%3A%22Honest%20Ads%20act%22%7D&searchResultViewType=expanded.

105. У Бразилії підтримується співпраця між органами адміністрування виборів, науковцями та практиками з метою оцінки справжнього впливу й ефективності вжитих заходів через Консультативну раду з питань інтернету та виборів (Advisory Council for Internet and Elections), яка консультує Виборчий трибунал (Election Tribunal). Панама та Мексика[114] є прикладами країн, у яких оператори та платформи співпрацюють із органами адміністрування виборів для того, щоб виявляти загрози та поширювати офіційну інформацію.

106. Перевірка фактів (фактчекінг)[115] розвинулася у багатьох країнах[116], а в деяких із них створено цілі мережі таких фахівців з перевірки фактів (фактчекерів); цікавим прикладом є «#Verificado2018», група журналістів та їх партнерів з громадянського суспільства та академічних кіл, які мали на меті спростовувати вірусну дезінформацію, перевіряти факти у заявах політиків і боротися з «фейковими новинами» під час федерального виборчого процесу в Мексиці. Іспанія також створила спеціальний підрозділ перевірки фактів під час останніх виборів[117].

VII. Е-ВИКЛИКИ ДЕМОКРАТІЇ ТА ПРАВАМ ЛЮДИНИ

107. Проведення демократичних виборів, а отже, і саме існування демократії є неможливими без поваги до прав людини, зокрема свободи вираження поглядів, преси, свободи зібрань та об'єднань у політичних цілях, зокрема й створення політичних партій. Повага цих свобод є особливо життєво важливою під час виборчих кампаній. Обмеження цих основоположних прав має узгоджуватися з Європейською конвенцією з прав людини та, більш загально, з вимогою, що таке обмеження повинно мати законну підставу, становити загальний інтерес та дотримуватися принципу пропорційності. Чіткі критерії балансування конкурентних прав повинні бути визначені законодавчо та ефективно застосовуватися через механізми виборчого та звичайного правосуддя.

108. На деякі специфічні поняття демократії впливає використання цифрових технологій. По-перше, нові інформаційні технології – наприклад, електронне голосування, формування та актуалізація централізованих реєстрів виборців – здійснюють вплив на ***електоральну демократію***, яку розуміють як інституційну діяльність та інфраструктуру, що роблять вибори можливими, і яка в контексті інтернету широко відома під назвою «е-уряд». По-друге, інтернет та нові інформаційні технології мають потенціал забезпечити більшу прозорість і підзвітність, а також більш ши-

114. *INE (Instituto Nacional Electoral)* Мексики під час підготовки виборів 2018 року уклав угоди про співпрацю з *Facebook, Twitter* та *Google*; див.: INE, Democracia en riesgo, Elecciones en tiempos de desinformación, Estrategia y acciones implementadas para enfrentar la desinformación deliberada en las elecciones mexicanas de 2018.

115. Див.: Lazer *et al.*, 2018.

116. Див., наприклад, Додаток до Доповіді Ради Європи 2017 року про інформаційний безлад, у якому наведено список європейських ініціатив щодо перевірки фактів та спростувань. Див. також: reporterslab.org/fact-checking.

117. Див.: elpais.com/politica/2019/03/10/actualidad/1552243571_703630.html.

рокі та ефективні форми політичної участі, розширюючи «публічну сферу»; у цьому сенсі вони впливають на ***деліберативну демократію***, яка передбачає участь окремих людей у відкритих дискусіях, базуючись на вірі в те, що це приведе до кращих рішень у питаннях, що становлять спільний інтерес[118]. Нарешті, там, де ці технології полегшують процес, завдяки якому великі дезорганізовані групи людей організуються та діють разом для вирішення конкретних соціальних, економічних чи політичних питань, ці технології можна вважати такими, що впливають на так звану «***моніторингову демократію***», визначену як «публічна підзвітність та громадський контроль тих, хто приймає рішення, незалежно від того, чи діють вони у сфері державних або міждержавних установ, чи в межах так званих неурядових організацій або організацій громадянського суспільства, таких як підприємництво, профспілки, спортивні асоціації та благодійні організації»[119]. Можна вважати, що змінні моніторингової демократії вбудовані у категорію деліберативної демократії у тій мірі, наскільки здатність громадян здійснювати нагляд та самоорганізовуватися для політичних цілей залежить як від інформації, доступ до якої вони можуть отримати, так і від їхніх можливостей обдумати й погодити спільний порядок денний.

A. ВИКЛИКИ ПЕРЕД ЕЛЕКТОРАЛЬНОЮ ДЕМОКРАТІЄЮ

109. Як вже було згадано вище, поняття «***електоральна демократія***» стосується інституційної діяльності та інфраструктури, які роблять вибори можливими. Від організації самих виборів до створення та ведення реєстрів виборців або запровадження електронних бюлетенів та інтернет-голосування виборчий аспект демократії встановлює матеріальні та інституційні умови, необхідні для перетворення народного голосування у процес призначення представників або затвердження законів і публічної політики. Наприклад, належне ведення реєстрів виборців має вирішальне значення для реалізації принципу загального виборчого права; чітке дотримання процедур голосування та підрахунку є визначальним для реалізації принципу вільних виборів.

110. Якщо, з одного боку, використання цифрових технологій може зробити демократичні процеси більш доступними для всіх громадян, то, з другого боку, воно також може створити перепони для здійснення і розвитку електоральної демократії, наслідком чого стане виникнення нових форм протиправного втручання у право голосу та право балотуватися на виборах (стаття 3 Першого протоколу до ЄКПЛ), у право на свободу вираження поглядів (стаття 10 ЄКПЛ) та в право на повагу до приватного життя (стаття 8 ЄКПЛ).

118. Laidlaw 2015, p. 10-11.

119. John Keane, The Life and Death of Democracy, 2009. Визначення «моніторингової демократії» викладено у: thelifeanddeathofdemocracy.org/glossary/monitorydemocracy.

111. За даними Установи з питань безпеки комунікацій (Communication Security Establishment, CSE) уряду Канади, «опоненти в усьому світі використовують кіберспроможності... проти виборів... для зниження рівня участі виборців, підробки результатів виборів та крадіжки інформації про виборців... проти політичних партій і політиків... для здійснення кібершпигунства задля цілей примусу та маніпуляцій і публічної дискредитації індивідів… [та] проти як традиційних, так і соціальних медіа… задля поширення дезінформації та пропаганди й формування думки виборців»[120]. Навіть більше, CSE вважає, що «існує велика ймовірність того, що загрозлива кібердіяльність, спрямована проти демократичним процесів у всьому світі, буде зростати кількісно і за своєю витонченістю» протягом наступних років через такі причини[121]:

- *Багато ефективних кіберможливостей є загальнодоступними, дешевими та простими в користуванні.*
- *Швидке зростання соціальних медіа разом із занепадом давніх авторитетних джерел інформації полегшує опонентам використання кіберспроможностей та інших методів для введення дезінформації і пропаганди в медіа і впливу на виборців.*
- *Виборчі органи все частіше використовують інтернет для покращення послуг для виборців. Чим частіше ці послуги переносяться до мережі, тим більше вони стають вразливими до кіберзагроз.*

120. CSE 2017. Ми бачили декілька прикладів таких втручань у всьому світі:
   - «У червні 2016 року американський штат Арізона зупинив свою систему реєстрації виборців майже на тиждень після того, як опоненти намагалися отримати доступ до системи. Наступного місяця в Іллінойсі виборче агентство штату на два тижні вимкнуло власний сайт після виявлення підозри щодо того, що десятки тисяч записів виборців (наприклад, імена, адреси та номери посвідчень водія) потрапили до рук опонентів» (CSE із посиланням на Nakashima).
   - «Реагуючи на можливі вразливості програмного забезпечення у своїх машинах підрахунку голосів, а також на попередження про те, що вибори можуть стати об'єктом атак із боку Росії, на останніх виборах Нідерланди внесли зміни до процедур голосування. Щоб уникнути можливостей опонентів втручатися у вибори, усі голоси було підраховано вручну» (CSE із посиланням на Escritt).
   - «У грудні 2016 року опоненти отримали доступ до сайту Центральної виборчої комісії Гани під час загальних виборів у момент підрахунку голосів. Невідомий опонент виклав у Twitter фейкові результати, відповідно до яких кандидат, який на час виборів обіймав посаду, програв. Потім виборча комісія оприлюднила власні повідомлення у Twitter, стверджуючи, що ці результати були фальшивими. Хоча результат виборів не було змінено, цей інцидент посіяв розгубленість у свідомості багатьох виборців» (CSE із посиланням на BBC News).
   - «На останніх президентських виборах в США обидві основні політичні партії зазнали атак з елементами спроб кібершпигунства з боку Росії. Російські оперативники використовували кіберможливості, щоб отримати доступ до електронних пошт ключових працівників політичних штабів, які розробляли кампанію Демократичної партії. Після цього електронні листи були «злиті» для того, щоб дискредитувати кандидата від Демократичної партії» (CSE з посиланням на ODNI).
   - «За повідомленнями засобів масової інформації, французька розвідка вважає, що соціальні ботнети використовувалися для впливу на президентські вибори. Деякі акаунти в соціальних медіа – ті самі, які були активними під час минулорічних виборів у США, – просували фальшиву та наклепницьку інформацію щодо провідного кандидата. В останні дні виборів одна партія також стала жертвою несанкціонованого оприлюднення тисяч електронних листів, пов'язаних з агітацією» (CSE з посиланням на Auchard).
   - «Кібервійна, колись здебільшого гіпотетична загроза, стала добре задокументованою реальністю, а напади іноземних держав тепер є серйозною загрозою для національної системи онлайн-голосування. Нещодавно, у травні 2014 року, зловмисники, пов'язані з Росією, атакували виборчу інфраструктуру в Україні та ненадовго затримали підрахунок голосів» (Springall et al., 2014).
121. CSE 2017.

- *Стримування загрозливої кіберактивності є складним завданням, тому що часто такі загрози важко вчасно виявити, визначити та відреагувати на них. Як результат, терези витрат/вигод переважують на користь тих, хто використовує кіберможливості, а не тих, хто захищається від їхнього використання.*

- *Нарешті, можемо спостерігати динаміку успіху, яка спонукає опонентів знову й знову вдаватися до своїх дій та надихати на копіювання таких дій інших».*

112. Конвенція Ради Європи про кіберзлочинність ETS185 2001 року (Будапештська конвенція) та поточна робота над Другим додатковим протоколом до цього договору свідчать, що багато держав зрозуміли ризики[122].

113. Із точки зору кіберзлочинності загрози електоральній демократії можуть включати принаймні два типи втручання. Один тип – це атаки проти конфіденційності, цілісності й доступності виборчих комп'ютерів та даних, серед яких:

- компрометація баз даних або систем реєстрації виборців, наприклад, шляхом зламу комп'ютерних систем чи видалення, зміни або додавання даних;

- злам машин для голосування з метою маніпулювання результатами;

- втручання у роботу систем (наприклад, розподілена атака шляхом відмови сервісу в день виборів);

- протиправний доступ до комп'ютерів для крадіжки, зміни або розповсюдження чутливих даних, як, наприклад, крадіжка даних із комп'ютерів передвиборчої агітації для використання в інформаційних операціях.

114. Такі атаки, безумовно, є формами кіберзлочинності, визначеними Будапештською конвенцією про кіберзлочинність, як протиправний доступ до комп'ютерних систем (стаття 2), протиправне перехоплення (стаття 3), втручання в систему та дані (статті 4 та 5) та інші. На цей час понад шістдесят держав-учасниць цього договору перенесли такі положення до свого внутрішнього законодавства.

115. Як вже зазначалося вище, ці напади є втручанням у декілька основоположних прав, гарантованих ЄКПЛ та іншими міжнародними документами з прав людини. Їх можуть здійснювати уряди, політичні партії/кандидати, іноземні органи влади та приватні суб'єкти. У цьому відношенні необхідно підкреслити, що відповідно до ЄКПЛ держави мають позитивний обов'язок забезпечити вільні й безпечні вибори та гарантувати права людини, такі як право на приватне життя та свободу вираження поглядів.

122. «Кіберзлочинність у виборчому процесі: роль Будапештської конвенції», www.venice.coe.int/files/15EMB/Alexander_Seger.pptx.

116. Другий тип атаки містить (дез)інформаційні операції, які не належать до кіберзлочинності, але які порушують норми щодо захисту персональних даних, політичних фінансів, висвітлення виборів у засобах масової інформації чи в мовленні, тобто норм, які забезпечують вільні, чесні та чисті вибори. Докази того, що такі норми порушені, часто мають форму електронних доказів, тобто це докази, знайдені в комп'ютерних системах. Тому важливо, щоб держави наділяли свої органи кримінальної юстиції необхідними повноваженнями для забезпечення таких доказів. Від держав-учасниць Будапештської конвенції вимагається робити це відповідно до статей 16-21.

117. Міжнародні стандарти дійсно вказують на відповідальність держав за те, щоб запобігти нерівності у висвітленні виборчих кампаній у засобах масової інформації та забезпечити інформування громадян про політичні партії, щоб вони могли робити вільний політичний вибір своїх представників. Окрім своїх зобов'язань не втручатися протиправно у здійснення основоположних прав, держави також мають позитивні зобов'язання запобігати порушенням, які вчиняють треті сторони. Необхідно забезпечити справедливий баланс між конкурентними правами. Стандартними сценаріями такої конкуренції є неналежне використання даних реєстру виборців для виборчих цілей або надмірне розкриття особистої інформації про кандидата в розпал політичної кампанії. Більшість демократій вважали б перший сценарій явним порушенням права на приватність та виборчої справедливості, навіть якщо політичні партії мають право на доступ до такої інформації. Проте можна стверджувати, що природа демократичних дебатів дозволила б розширену припустимість переваги політичного права на вираження поглядів перед правом кандидата на приватне життя за умови, що такі вислови явно не становлять наклепу або брехні. Сучасні демократії звикли до цих сценаріїв і створили досить багатий набір правил та національного законодавства щодо цього питання.

118. Протягом принаймні двох десятиліть декілька країн проводили експерименти із застосуванням інтернет-голосування задля зміцнення політичних прав. Наприклад, у 2000 році Швейцарія запустила проєкт ***«vote électronique»***, щоб випробувати його надійність. Відтоді ця країна провела понад 150 спроб на федеральному рівні, а деякі кантони зробили е-голосування доступним для своїх громадян. У 2008 році Норвегія також розпочала тестування інтернет-голосування та здійснила деякі спроби під час муніципальних виборів 2011 року та парламентських виборів 2013 року. У Канаді інтернет-голосування доступне в деяких провінціях (Онтаріо та Нова Шотландія) із 2003 року. Мабуть, найбільш успішний експеримент провела Естонія, де дискусії щодо інтернет-голосування розпочалися в 2001 році, а з 2005 року таке голосування розглядають як додаткову та юридично зобов'язальну форму голосування[123].

123. ACE Project 2018.

119. Незважаючи на успіх деяких спроб, використання інтернету для подання голосів спричинило виникнення деяких проблем безпеки. «Естонія була першою у світі країною, яка використовує інтернет-голосування на національному рівні, і станом на сьогодні понад 30% усіх голосів подається онлайн», але дослідники Мічиганського університету та Групи відкритих прав (Open Rights Group) дійшли висновку, що «[естонська] система е-голосування має серйозні архітектурні обмеження та процедурні прогалини, які потенційно загрожують цілісності виборів» настільки, що «зловмисники можуть атакувати виборчі сервери або клієнти виборців, щоб змінити результати виборів або підірвати легітимність системи». Їх сумніви були настільки серйозними, що вони дійшли висновку, що «колись, у разі фундаментального прориву в комп'ютерній безпеці, профіль ризику може стати більш сприятливим для інтернет-голосування, але ми не віримо, що сьогодні система інтернет-голосування може бути зроблена безпечною»[124].

120. У цьому контексті варто підкреслити: можливо, поширення неправдивої інформації та широке цифрове втручання у політичний дискурс спрямовані не на дискредитацію механізму власне виборів, а радше на те, щоб підірвати публічну довіру до самого процесу та до політичної системи. Відкритість ліберальної демократії є силою, але також і вразливістю. Не можна дозволити цифровим технологіям зруйнувати довіру громадськості до виборчого процесу, отже, існує необхідність переконати громадськість у безпеці таких технологій. Із цією метою цифрові технології повинні впроваджуватися поступово і можуть поєднуватися з традиційними методами. Інновації не можна запроваджувати коштом правових вимог, зокрема й безпеки.

121. З цими викликами треба вести справу з позиції взаємозалежності, що означає, що (1) проблема має транснаціональний характер та (2) повинна бути визнана істотна роль, яку відіграють вартові інформаційних магістралей (тобто сервіс-провайдери інтернету) у розслідуванні та притягненні до відповідальності за кіберзлочини. Необхідно посилити міжнародну нормативно-правову базу, щоб встановити більш ефективні механізми транснаціональної співпраці між націями та приватними суб'єктами, а також, якщо це можливо, забезпечити більшу уніфікованість національних законодавств. Нарешті, виглядає, що вирішенням може бути «пристосування конституційних рамок сучасних демократій» до нового електронного середовища, у якому процвітає кіберзлочинність та водночас у якому уряди, корпорації і громадяни взаємодіють і роблять демократію можливою[125].

B. ВИКЛИКИ ПЕРЕД ДЕЛІБЕРАТИВНОЮ ДЕМОКРАТІЄЮ

122. Принцип вільних виборів ґрунтується на свободі виборців формувати свою думку. Ця свобода, яка частково перетинається з рівністю виборчих

124. Springall et al. 2014.
125. Mecinas Montiel 2016, p. 427.

можливостей, взагалі кажучи, вимагає від держави та органів публічної влади дотримуватися свого обов'язку безсторонності, зокрема там, де це стосується використання засобів масової інформації, розміщення плакатів, права оприлюднювати детальні розцінки і фінансування партій та кандидатів[126]. Свобода формування думки охоплює право бути належно поінформованим перед прийняттям рішення, право приватного перегляду в інтернеті та право здійснювати конфіденційне спілкування в інтернеті. Моніторинг онлайн-активності людей без їхньої згоди та з метою розуміння й використання їх способів поведінки порушує ці права.

123. Технологія змінює спосіб ведення виборчих кампаній. Інтернет є потужною платформою для того, щоб політичні партії представляли свої програми електорату та мобілізували більшу базу підтримки власних тез. Вартість спілкування з виборцями може бути значно нижчою через цього посередника, аніж через мовників, з огляду на наявність безплатних платформ для обміну блогами та відео і соціальних медіа. Зокрема, невеликі політичні партії з обмеженими ресурсами та незалежні кандидати можуть скористатися таким типом спілкування.

124. Проте зміни у виробництві та споживанні контенту, пов'язаного з виборами, породжують виклики для усталених інститутів і принципів регулювання виборчих комунікацій, таких як свобода об'єднання, обмеження витрат та регулювання політичної реклами. Вони підривають здатність чинного регулювання підтримувати рівні умови для виборчих комунікацій між новими й усталеними, багатими й бідними, корпоративними й громадськими кампаніями. Нові посередники та платформи тепер займають важливі позиції вартових, які колись займали журналісти, проте вони ще не сприйняли етичних зобов'язань засобів масової інформації. Це становить загрозу для виборів та потенціал для корупційних практик. Дослідження Ради Європи щодо виборів 2017 року визначає низку проблем щодо чесності та легітимності виборчих процесів, як брак прозорості агітації, витрат, повідомлень й алгоритмів, які використовуються у цифровій рекламі, масштабні вторгнення в приватне життя, відсутність фільтрів у журналістиці для перевірки фактів, що містяться у політичних повідомленнях, збільшення кількості дезінформації, а також прогалини у регулюванні передвиборчої агітації (наприклад, неможливість змусити дотримуватися періоду тиші), які дозволяють зробити висновок, що «поточної нормативно-правової бази вже недостатньо, щоб підтримувати рівні умови для політичної конкуренції та обмежувати роль грошей у виборах»[127].

126. Венеційська комісія, Кодекс належної практики у виборчих справах, Пояснювальна доповідь, Вільні вибори.

127. Дослідження Ради Європи щодо виборів 2017 року (Council of Europe Election Study 2017); див. також: Дослідження 2018 року «Дезінформація та виборчі кампанії» (Doublet, 2018, CDDG(2018)11), де Раді Європи пропонується підготувати широку Програму дій у цій сфері. Рекомендується, наприклад, визначити тривалість виборчих кампаній, щоб уникнути ризику проведення серйозних цифрових кампаній до періоду виборчої кампанії; вимагати роздруку цифрового матеріалу, щоб знати, хто стоїть за онлайн-платформами; отримувати відкрито дані про витрати на діяльність з цифрових виборчих кампаній на онлайн-платформах; забороняти фінансування цифрових виборчих витрат іноземними фізичними чи юридичними особами.

125. Традиційній виборчій агітації кидають виклик нові форми каналів комунікації, які не лише допомагають поширювати повідомлення за низьку вартість, а й використовують специфічні маркетингові техніки, які найкраще пристосовані до конкретних прошарків електорату. Віднедавна на виборчій арені застосовуються такі механізми, як використання персоналізованих оголошень та звернень, застосовних у будь-якій сфері цифрового маркетингу, що забезпечує деяким суб'єктам, які мають доступ до цих механізмів, непрозорі переваги. Отже, виборчі повідомлення стають щораз більше персоналізованими. Тим, хто розробляє кампанії, не потрібно думати про більшість електорату, яка вже вирішила, як проголосувати. По суті, вони можуть сконцентруватися на малих групах виборців, які ще не визначилися. Нові агітаційні технології надають можливість робити націлені виборчі звернення, дещо замасковані під загальні, політично нейтральні повідомлення. Здійснення такого прихованого впливу полегшується використанням соціальних платформ не лише через алгоритми обробки даних, а загалом через те, що вони надають можливість прямо націлюватися на конкретні групи профілів із персоналізованими зверненнями та повідомленнями, тоді як цільові користувачі не помічають такої персоналізації. За допомогою технології методи ведення агітації перейшли до еволюційної концепції «один до одного» або «багато до багатьох»: саме це Джозеф Пайн (Joseph Pine) називає «масовим підлаштуванням»[128]. На відміну від традиційних засобів масової інформації, які у принципі мають задекларованe політичне забарвлення, відоме читачеві, інтернет-провайдери не мають задекларованої політичної лінії, так що за відсутності чітких вказівок на те, що надана ними інформація насправді є упередженою політичною рекламою, користувачі можуть перебувати під враженням, що така інформація є політично нейтральною.

126. Маніпуляції з виборчими перевагами вивчав Роб Епстейн (Rob Epstein), зокрема, предметом його уваги був вплив рейтингів пошукових систем (особливо Google у зв'язку з його домінуванням) на преференції виборців, відомий під назвою «ефект маніпуляції через пошукові системи» (Search Engine Manipulation Effect, SEME)[129]. Відповідно до дослідження 2015 року вищі в рейтингу позиції, пов'язані з веб-сторінками, що віддають перевагу одному кандидату, впливають на думку виборців, які ще не визначилися[130]. Докази, отримані з п'яти експериментів у двох країнах, свідчать про те, що «(i) упереджені пошукові рейтинги можуть змінити виборчі преференції виборців, які ще не визначилися, на 20% або й більше, (ii) розрив може бути набагато вищим у деяких демографічних групах, і (iii) такі рейтинги можуть бути замасковані, так що люди не усвідомлюють маніпуляції». Автори дослідження роблять висновок: «якщо Google віддає перевагу одному кандидатові на виборах, вплив системи на невиз-

128. Pine, B.J., II. (1993). Mass Customization: The New Frontier in Business Competition. Harvard Business School Press, Boston.

129. Epstein 2016.

130. Epstein and Robertson 2015.

начених виборців може легко вирішити результат виборів». Хоча може існувати потреба підтвердження таких результатів подальшими дослідженнями, можна погодитись із висновком авторів, відповідно до якого «ще більше турбує» те, що «пошуковий бізнес є зовсім нерегульованим».

127. У цьому контексті потрібно враховувати, що ранжування пошукових систем – це продукт складних алгоритмів, і воно не обов'язково проєктується як маніпулятивне, однак спрямоване на забезпечення найбільш провідних, актуальних та нових результатів; однак алгоритмами можуть маніпулювати різні сайти, намагаючись отримати кращі рейтинги. У дійсності ми бачимо, що це відбувається, і Google постійно вдосконалює алгоритм пошуку для запобігання таким втручанням. У будь-якому випадку, незалежно від того, чи така маніпуляція є навмисною, чи ні, SEME має два важливі наслідки для демократії: силу маніпулювати преференціями можуть використати приватні чи державні суб'єкти для впливу на рівність у виборах; той факт, що користувачі пошукових систем не знають про критерії (кодування) механізмів ранжування, перешкоджає їхній здатності приймати повністю інформовані рішення, а отже, і здійснювати свою свободу вираження поглядів.

128. SEME не є єдиною проблемою для пошукових систем у мережі. Платформи соціальних медіа також керуються базовою архітектурою кодування, яка не є неупередженою. Такі компанії, як Facebook, Twitter або Instagram, на відміну від традиційних засобів масової інформації, не мають політичної орієнтації; вони насамперед мотивовані комерційними інтересами й розробляють свою структуру кодування відповідно до цих інтересів. У цьому сенсі алгоритми, що керують соціальними медіа, сприяють частковому, а іноді ілюзорному розумінню політики та демократії, оскільки вони надають необ'єктивну інформацію, яка відображає часткові інтереси та поведінку їхніх користувачів[131].

129. Дійсно, соціальні медіа та компанії пошукових систем можуть формувати онлайн соціальні взаємодії не тільки тому, що вони мають владу кодувати середовища таких взаємодій, а й завдяки здатності створювати профілі («профілювання») та передбачати характеристики та поведінку своїх користувачів. Ці компанії можуть легко отримати доступ до «цифрових записів поведінки, оскільки вподобання «лайки» у Facebook, історії перегляду, пошукові запити чи історії закупівель можуть бути використані для автоматичного й точного передбачення низки особливо чутливих особистих характеристик, серед яких: сексуальна орієнтація, етнічна належність, релігійні та політичні переконання, риси особистості, інтелект, рівень щастя, вживання речовин, що викликають залежність, розлучення батьків, вік та стать»[132]. Окрім того, ці комплекси здатні обробляти таку інформацію, щоб створити високоточні профілі своїх користувачів, передбачити їхні уподобання та навіть спрямувати на них індивідуа-

131. Van Dijck 2013; McChesney 2013.

132. Graepel *et al.* 2013.

лізовану інформацію й рекламу з метою заохочування до певних форм поведінки або відмови від них[133].

130. З одного боку, такі компанії, як Facebook або Google, перетворюють інформацію про своїх користувачів на товар і продають її на ринку. Покупці, з другого боку, використовують цю інформацію з мінімальною відповідальністю або зовсім без неї, щоб упливати на споживачів і часом на виборців за допомогою «спеціальних реклам, заснованих на особистих даних»[134]. Саме це й було зроблено у випадку з «Cambridge Analytica». Поточна бізнес-модель багатьох сайтів пропонує контент в обмін на персональні дані. Той факт, що люди пропонують свою особисту інформацію в обмін на безплатні сервіси, дає можливість широко розповсюджувати дані на сайтах, що може призводити до як належного, так і неналежного використання цих даних різними суб'єктами.

131. Навіть якщо це правда, що користувачі соціальних медіа повинні явно прийняти загальні умови конфіденційності, встановлені компаніями, що володіють соціальними медіа, вони мають незначний контроль або й зовсім його не мають щодо того, хто має право «купувати» їхню особисту інформацію, або щодо того, як ця інформація буде використовуватися. Така ситуація підриває основоположне право на приватне життя та захист персональних даних, оскільки обмежує спроможність користувача накладати обмеження на використання своєї персональної інформації[135]. У рішенні 292/2000 Конституційний трибунал Іспанії встановив, що «основоположне право на захист персональних даних... надає відповідальній особі набір повноважень накладати на третіх осіб зобов'язання виконувати або утримуватися від певної поведінки, які надають індивідам повноваження приймати рішення щодо власних даних... [такі повноваження є марними], якщо відповідальна особа не знає, яка інформація перебуває в руках третіх осіб, ким ці треті особи є та з якою метою таку інформацію буде використано»[136].

132. Використання персональних даних та зловживання ними для виборчих цілей, замасковані під свободу підприємництва, можуть становити серйозну загрозу для вільних виборів і виборчої рівності щонай-

133. Наприклад, відповідно до запису Роберта Епстейна (Robert Epstein, 2016):
«… Дослідження Роберта М. Бонда (Robert M Bond), який на цей час є професором політології Університету штату Огайо, та інших, опубліковане у «Nature» *в 2012 році, описало етично сумнівний експеримент, під час якого у день виборів 2010 року* Facebook *надіслав нагадування «Іди та голосуй» понад 60 мільйонам своїх користувачів. Нагадування спричинило те, що проголосувало близько 340 тисяч людей, які інакше не зробили б цього. У статті у* «New Republic» *у 2014 році Джонатан Зіттрейн (Jonatan Zittrain), професор міжнародного права Гарвардського університету, зазначив, що з огляду на величезну кількість інформації, зібраної про своїх користувачів,* Facebook *міг легко надсилати такі повідомлення лише тим людям, які підтримують одну конкретну партію або кандидата, і такими діями міг би легко «зробити» вибори з невеликим розривом між лідерами, – і ніхто б не знав, що це сталося. А через те, що реклама, як і рейтинги пошуку, є ефемерною, таке маніпулювання виборами не матиме жодного документального підтвердження».*

134. Christopher Wylie, як цитує Guimón 2018.

135. Davara 2003, с. 43-44.

136. Як зазначає Davara 2003. Переклад [англійською. – *Прим. ред.*] авторів.

менше у трьох аспектах: по-перше, приватні суб'єкти можуть використовувати таку інформацію для безпосереднього нав'язування неналежного впливу на виборчу конкуренцію; по-друге, компанії, які забезпечують інтернет і соціальні мережі, з посиланням на свободу підприємництва можуть обмежувати доступ до такої інформації відповідно до своїх політичних преференцій, надаючи таким способом непрозору перевагу деяким партіям чи кандидатам перед іншими; і по-третє, перетворення персональних даних у товар становить виклик для нагляду за фінансуванням у політичних кампаніях.

133. Ризик порушити право на приватне життя, вільні вибори/виборчу рівність і свободу вираження поглядів та переконань – і, як стверджують деякі експерти, навіть свободу думки, – наводить на думку про необхідність врегулювати комерційні права інтернет-компаній та компаній, які володіють соціальними медіа. Взагалі кажучи, повна заборона «комодитизації інформації» також перешкоджала б розвитку інтернету та, як наслідок, доступу до очевидно необмеженого джерела політичної інформації і демократичних дій. Поки суспільства не знайдуть нових форм фінансування інтернету, накладення надмірних обмежень на комодитизацію персональної інформації може обмежити основні політичні права, такі як свобода вираження поглядів та свобода організації політичної акції. Парадокс полягає в тому, що ті самі технології, що розширюють можливості вираження, є тими, які обмежують такі можливості [137].

134. З одного боку, право доступу до інтернету є необхідною умовою повної реалізації свободи вираження поглядів, що є необхідною умовою існування демократичного суспільства[138]. З другого боку, інтернет сам по

137. Як висловився Laidlaw (2015, p. xi-xii), *«Технології комунікації, які надають або позбавляють можливості участі в онлайн-дискурсі, є приватною власністю... Отже, ми неминуче покладаємось на ці компанії при реалізації права на свободу вираження поглядів онлайн, і вони відповідно стають вартовими нашої онлайн-діяльності...*

Те, що ми покладаємося на цих вартових при здійсненні права на свободу слова, має два наслідки. По-перше, такі вартові все частіше стають об'єктом правових заходів, призначених для того, щоб отримати перевагу від спроможності цих структур регулювати поведінку третіх сторін… По-друге,… регулювання висловлювань у кіберпросторі значною мірою залишалося справою саморегулювання; здебільшого через те саме регулювання інтернету загалом є майже поверховим... Результатом є система приватного управління, яка працює паралельно із законом, без жодних запобіжних заходів щодо прав людини, яких загалом очікують від керованих державою систем, як принципи підзвітності, передбачуваності, доступності, прозорості та пропорційності».

138. *«Лінґенс проти Австрії» (Lingens v. Austria)*, заява № 9815/82 (ЄСПЛ, 8 липня 1986 року): «Свобода вираження поглядів, закріплена в частині першій статті 10 (ст. 10-1), становить одну з важливих основ демократичного суспільства». Далі, у справі *«Ахмет Їлдирим проти Туреччини» (Ahmet Yıldırım v. Turkey)* (заява № 3111/10, 18 грудня 2012 року) ЄСПЛ постановив, що блокування інтернету може «безпосередньо суперечити чинному формулюванню частини першої статті 10 Конвенції, відповідно до якого права, викладені в цій статті, забезпечуються «незалежно від кордонів».

Див. також: Laidlaw (2015, p. 19-21): *«Демократія завжди втілена в практиці спілкування, а свободу вираження поглядів суди повсякчас визначали як центральну в демократії. У справі «Лінґенс проти Австрії» Європейський Суд з прав людини (ЄСПЛ) чудово прокоментував, що свобода вираження поглядів «є однією з важливих основ демократичного суспільства»...*

Багато держав, як-от Естонія, Фінляндія, Франція, Греція та Іспанія, законодавчо визнали доступ до інтернету основоположним правом. У 2003 році Комітет Міністрів Ради Європи прийняв Декларацію, що підтверджує важливість свободи вираження поглядів в інтернеті. З 2010 року ми спостерігаємо зсув парадигми на міжнародному рівні в бік визнання прав людини в кіберпросторі. Доступ до інтернету як основоположне право отримав підтримку Організації Об'єднаних Націй (ООН) у доповіді Франка Ля Рю (Frank La Rue), Спеціального доповідача щодо підтримки та захисту права на свободу переконань і вираження поглядів… Далі цю тезу висловила у 2012 році Рада ООН з прав людини, яка провела резолюцію, що визнає свободу користування інтернетом як основоположне право людини, зокрема як складову права на свободу вираження поглядів».

собі створює різноманітні загрози для демократії. Оскільки соціальні медіа та інтернет не є (і не повинні бути) простором, який перебуває поза правовими параметрами[139], існує невідкладна потреба пошуку таких рішень цих конфліктів прав, які б дозволили забезпечити розумний захист приватності, політичних та підприємницьких прав.

135. Брак або недостатність регулювання інтернету та соціальних медіа залишили користувачів без будь-яких правових засобів захисту своїх даних і більш за все власної свободи вираження поглядів та демократичних прав. З одного боку, існує проблема, коли приватні технологічні компанії цензурують контент, який вони вважають «шкідливим», без власної підзвітності та прозорості їхніх заходів.

136. З другого боку, позитивне зобов'язання держави запобігати протиправному втручанню третіх сторін не повинно призводити до протиправного втручання самої держави шляхом надмірного або неналежного регулювання, наслідком якого може бути порушення саме тих прав, які воно мало б захищати. Невиправданий державний нагляд за приватними комунікаціями та різними способами використання онлайн-платформ може бути використаний так, що – навмисне чи випадково – впливатиме на потік інформації, безпосередньо обмежуватиме свободу вираження поглядів, перешкоджатиме демократичному діалогу та порушуватиме принципи інституційної нейтральності та виборчої рівності. Хоча з контексту, описаного вище, можна зрозуміти, що на цей час багато держав мають на порядку денному завдання вирішити питання «фейкових новин» через законодавство, це може становити загрозу основоположному праву на свободу вираження поглядів та інформації з огляду на те, що на гіперболізовані розповсюджується захист відповідно до міжнародних стандартів прав людини, зокрема статті 10 ЄКПЛ. Якщо дозволити органам влади втручатися у публічний дикурс, це може призвести до зловживання владою, коли дисидентів примушуватимуть мовчати та перешкоджатимуть дискусії, яка б ставила під сумнів панівну думку, з метою обмеження критичних настроїв у суспільстві. Як підкреслила Венеційська комісія, «засоби масової інформації – це не єдина категорія, яка повинна мати право на високий рівень свободи вираження поглядів. Отже, особам, які передають інформацію та ідеї щодо питань суспільного інтересу і сприяють публічній дискусії щодо таких питань, зокрема й членам агітаційних груп та виборним представникам, потрібно надати високий рівень свободи вираження поглядів, зокрема й до певної міри перебільшення та навіть провокації, якщо вони діють добросовісно й виявляють належну ретельність із метою надання точної та достовірної інформації»[140].

137. Фільтрація, блокування й видалення протиправного контенту в інтернеті для того, щоб, зокрема, боротися зі злочинами на ґрунті ненависті та

139. Electoral Tribunal of Mexico, g.

140. CDL-AD (2013) 024, Opinion on the legislation pertaining to the protection against defamation of the Republic of Azerbaijan, para. 37.

проти національної безпеки, а також із метою захисту інтелектуальної власності й приватності або прав, пов'язаних із захистом честі і гідності, є необхідним, проте дуже делікатним завданням, яке може призвести до зловживань і цензури, а також незаконного примусу політичних опонентів до мовчання. Будь-які подібні заходи повинні відбуватися відповідно до закону, що включає чітке та вузьке визначення відповідних правопорушень[141], і повинні переслідувати одну з законних цілей, наведених у статті 10 ЄКПЛ. Завжди повинні бути дотримані критерії необхідності в демократичному суспільстві та пропорційності[142]. Повинен бути гарантований ефективний судовий розгляд незалежним і безстороннім судом.

138. Що стосується «фейкових новин», які здебільшого не підпадають під жодну категорію, яка б дозволила притягнути винних до відповідальності, потрібно застосовувати альтернативні засоби, такі як перевірка фактів (яка, хоч і не є панацеєю, але стає все більш розвиненою та ефективною), програми з медіаграмотності, спрямовані на підвищення чутливості щодо цієї проблеми та розпізнання фальшивого контенту, а також інвестиції в якісну журналістику[143]. У цьому починанні державним органам буде потрібна співпраця як із громадянським суспільством, так і з інтернет-корпораціями.

139. Водночас потрібно підкреслити, що будь-які заходи щодо інформаційного безладу повинні бути розроблені дуже обережно, щоб не порушити принципу «нейтральності мережі». Це базовий принцип інтернету, згідно з яким інтернет-провайдери зобов'язані поводитися з усіма онлайн-даними на рівних засадах та забезпечувати умови для безперебійного доступу користувачів без дискримінації, заснованої на контенті або його джерелі. Захист демократичної функції інтернету від монополізації приватними корпоративними силами вимагає однакового поводження з усіма даними, які надсилаються та отримуються, без різниці в оплаті та якості послуг[144]. Скасування політики «нейтралітету мережі», як це зробила Федеральна комісія США з питань зв'язку (United States Federal Communication Commission) у грудні 2017 року[145], дозволяє провайдерам блокувати чи заглушувати (уповільнювати) сайти і стягувати плату за більшу швидкість завантаження на сервер та з нього. За таких обставин онлайн-сервісам, додаткам та сайтам може надаватися пільговий режим через будь-які причини, комерційні чи ідеологічні, зокрема й у менш демокра-

141. Див., наприклад: Venice Commission, Opinion on the Federal law on combating extremist activity of the Russian Federation, CDL-AD (2012) 016.

142. Див., наприклад: Venice Commission, Opinion on the law no. 5651 on regulation of publications on the internet and combating crimes committed by means of such publications ("the internet law") of Turkey, CDL-AD (2016) 011.

143. Див.: the CoE Information Disorder Report 2017, де запропоновано понад 30 рекомендацій для різних зацікавлених сторін.

144. З точки зору як конституційного права, так і міжнародного права прав людини, вирішально важливо враховувати реальність впливових суб'єктів поза межами виборних органів, які перешкоджають реалізації основоположних прав. Див.: Thorgeirsdóttir, Herdis (2005), *Journalism Worthy of the Name: the Affirmative Side of Article 10 of the ECHR*, Kluwer Law International.

145. Положення щодо нейтральності мережі, запроваджені у 2015 році з метою припинення надання інтернет-провайдерам преференційного ставлення до сайтів та сервісів, які платили їм за прискорення своїх даних, офіційно втратили чинність у червні 2018 року.

тичних країнах, де інтернет-провайдери перебувають у державній власності та цензуровані і де влада може спокуситись надати більш швидкі магістралі доступу проурядовим виробникам.

140. Зрештою, хоча надмірне чи неналежне регулювання інтернету може бути контрпродуктивним та перешкоджати доступності й розвитку інтернету і, як наслідок, свободі вираження поглядів та демократичному діалогу як такому, проблему дезінформаційного безладу не можна залишати без уваги. Ризик порушити право на приватність шляхом протиправного використання особистої інформації та загроз свободі вираження поглядів і виборчої рівності, що створюються архітектурою інтернету (тобто *SEME*, пізнавальні бульбашки, ехокамери та «фейкові новини»), разом із браком регулювання, що залишає громадян без ефективного правового ресурсу для захисту їхніх особистих і політичних прав, є ситуаціями, які вимагають невідкладних дій.

141. Такі дії повинні залучати потужних приватних акторів, які, будучи мотивовані насамперед комерційними інтересами, мають усі можливості, щоб зашкодити правам людини, підтримуючи важливу платформу демократії, і повинні визнавати таку відповідальність.

VIII. ВИСНОВКИ

142. Проведення демократичних виборів, а отже, і саме існування демократії є неможливим без поваги до прав людини, зокрема, свободи вираження поглядів, преси, а також свободи зібрань та об'єднань у політичних цілях включно зі створенням політичних партій. Повага цих свобод є життєво важливою, зокрема, під час виборчих кампаній. Обмеження цих основоположних прав має узгоджуватися з Європейською конвенцією з прав людини та, більш загально, з вимогою, відповідно до якої таке обмеження повинно мати законну підставу, становити загальний інтерес та дотримуватися принципу пропорційності. Чіткі критерії балансування конкурентних прав повинні бути встановлені на законодавчому рівні та ефективно впроваджуватися за допомогою механізмів виборчого й звичайного правосуддя.

143. Співвідношення між демократією та цифровими технологіями є досить складним. З одного боку, інтернет та соціальні медіа стали панівною платформою політичної взаємодії в деяких демократіях, використання цих інструментів посилило критичне ставлення громадян до своїх урядів, а їхнє широке застосування сприяє організації масштабних соціальних рухів і більш тісній взаємодії між громадянами та політичними партіями. З другого боку, нові віртуальні інструменти можуть бути використані, а часом і дійсно використовуються проти виборів для зниження рівня участі виборців, підробки результатів виборів та крадіжки інформації про виборців, проти політичних партій та політиків за допомогою кібершпигунства з метою тиску та маніпуляцій, для публічної дискредитації індивідів, а також проти традиційних і соціальних медіа з метою поши-

рення дезінформації та пропаганди і формування думки виборців. Нова цифрова сфера дозволяє створювати нові форми злочинності та комерціалізації даних, що становить серйозну загрозу правам приватності, та зменшує соціальну взаємодію шляхом вибіркового (а іноді і стратегічного) подання або приховування конкретної інформації для своїх користувачів, сприяючи так частковому розумінню реальності та створенню перепон для свободи вираження поглядів.

144. Інтернет-сервіси збагатили та урізноманітнили джерела новин, полегшуючи доступ індивідів до інформації та прийняття їхніх рішень щодо найважливіших питань демократії, зокрема, щодо вибору їхнього законодавчого органу. Проте водночас інформаційний безлад – помилкова інформація, дезінформація, зловмисна інформація – може спотворити екосистему комунікації настільки, що виборці можуть мати істотні труднощі при прийнятті власних рішень внаслідок введення в оману, маніпулятивної та фальшивої інформації, призначеної чинити вплив на їхні голоси. Таке середовище потенційно підриває реалізацію права на вільні вибори та створює значні ризики для функціонування демократичної системи.

145. Невелика кількість дуже потужних приватних суб'єктів, які буквально володіють інформаційними магістралями, мають власні комерційні інтереси та права, які мають тенденцію вступати у протиріччя як з громадянськими і політичними правами, так і з виборчими принципами. Ці інтернет-провайдери перебрали на себе роль вартових, яка спочатку належала традиційним засобам масової інформації, проте вони не взяли на себе етичних зобов'язань цих засобів масової інформації. Отже, приватні технологічні компанії цензурують контент, який вони вважають «шкідливим», без власної підзвітності і прозорості своїх заходів. Правда, нещодавно соціальні платформи запровадили низку заходів щодо запобігання фальшивим новинам та обмеження їх поширення, зокрема, під час виборчих періодів. Існує концепція корпоративної соціальної відповідальності, певний різновид саморегулювання для бізнесу, з первинною метою «не нашкодити» та дотримуватися принципів верховенства права та прав людини, зокрема й права на захист своїх користувачів, і нести відповідальність за власні продукти (відповідно до господарського права, конкурентного права, екологічного права тощо)[146]. Проте це зроблено на добровільній та неврегульованій основі, без визнаних рамок, заснованих на принципі верховенства права.

146. Хоча держави несуть позитивну відповідальність за запобігання протиправному втручанню в громадянські та політичні права третіми особами, протиправне втручання самої держави через надмірне або неналежне регулювання може мати наслідком порушення саме тих прав, які

146. *Facebook, Google* та *Twitter* є підписантами Кодексу практики проти дезінформації *(Code of Practice against disinformation)*, вони зобов'язалися щомісячно звітувати про заходи, вжиті перед виборами до Європейського Парламенту у травні 2019 року: див. April reports on the implementation of the Code of Practice, ec.europa.eu/digital-single-market/news-redirect/651264.

передбачалося захищати. Невиправданий державний нагляд за приватними комунікаціями та за різними способами, якими можуть використовуватися онлайн-платформи так, щоб – навмисне чи випадково – впливати на потік інформації, безпосередньо обмежує свободу вираження поглядів, перешкоджає демократичному діалогу та посягає на принципи інституціональної нейтральності та виборчої рівності. Якщо дозволити органам влади втручатися у публічний дикурс, це може призвести до зловживання владою, коли дисидентів примушуватимуть мовчати та перешкоджатимуть дискусії, яка б ставила під сумнів панівну думку, з метою обмеження критичних настроїв у суспільстві. Зокрема, фільтрація, блокування й видалення протиправного контенту в інтернеті з метою боротьби, зокрема, зі злочинами на ґрунті ненависті та захисту національної безпеки, а також із метою захисту інтелектуальної власності й приватності або прав, пов'язаних із захистом честі і гідності, повинні відповідати законодавству, яке встановлює чітке та вузьке визначення відповідних правопорушень; такі дії мають переслідувати одну з законних цілей, наведених у статті 10 ЄКПЛ. Повинні завжди бути дотримані критерії необхідності в демократичному суспільстві та пропорційності. Повинен бути гарантований ефективний судовий розгляд незалежним і безстороннім судом.

147. Щодо «фейкових новин» потрібно застосовувати альтернативні засоби, такі як перевірка фактів (fact-checking), програми з медіаграмотності, спрямовані на підвищення чутливості щодо цієї проблеми та розпізнавання фальшивого контенту, а також інвестиції в якісну журналістику.

148. Водночас потрібно підкреслити, що будь-які заходи, спрямовані на інформаційний безлад, повинні розроблятися дуже обережно, щоб не порушити принципу «нейтральності мережі». Інтернет повинен залишатися відкритою платформою.

149. Щоб вирішити ці проблеми, з перспективи взаємозалежності і глобальної точки зору необхідно забезпечити декілька заходів, зокрема, Щодо виборчої демократії:

- A. Криміналізувати кібератаки проти приватності, цілісності й доступності виборчих комп'ютерів та даних відповідно до Будапештської конвенції про кіберзлочинність.

- B. Надати органам кримінальної юстиції необхідні повноваження забезпечувати електронні докази щодо порушень норм захисту персональних даних, політичних фінансів, висвітлення засобами масової інформації або мовлення під час виборів.

- C. Підготувати національні органи адміністрування виборів (Election Management Bodies, EMB) до надзвичайних ситуацій та створити кризову організацію; EMB потрібно забезпечити відповідними ресурсами й навчанням для впровадження цифрових технологій та готовності до

пов'язаних із цим ризиків для кібербезпеки. Щодо деліберативної демократії:

- D. Визнати (1) транснаціональний характер проблеми та (2) важливу роль, яку відіграють інтернет-посередники (тобто постачальники послуг інтернету, а також компанії, що володіють пошуковими системами та соціальними медіа).

- E. Посилити міжнародні нормативно-правові рамки, (1) щоб встановити більш ефективні механізми транснаціональної співпраці між націями та приватними акторами, а також, якщо можливо, (2) забезпечити більшу уніфікованість національних законодавств.

- F. Працювати над нормативно-правовою та правозастосовчою моделлю, заснованою на співвідповідальності приватних та публічних акторів, а також на різноманітних підходах до регулювання й вирішення конфліктів. Така модель могла б включати принаймні чотири стратегії, які здатні постійно пристосовуватися до завжди мінливого середовища інтернету та комунікаційних технологій:

  - Сприяти подальшому дослідженню та співпраці між виборчими органами, науковцями та практиками з метою оцінки реального впливу цифрових технологій на виборчі процеси й ефективності вжитих заходів.

  - Посилювати освіту для зміцнення правової та демократичної культури громадян.

  - Сприяти саморегулюванню, як-от обов'язковому прийняттю етичних норм та корпоративних кодексів соціальної відповідальності серед постачальників послуг інтернету й компаній, що володіють пошуковими системами та соціальними медіа.

  - Забезпечити механізми захисту на рівні права, політики та альтернативних механізмів вирішення конфліктів.

150. На рівні Ради Європи вже зроблено багато для вирішення зазначених вище проблем. Зокрема, Будапештська конвенція надала низку інструментів для запобігання кіберзлочинності, зокрема й під час виборчого процесу, та для міжнародного співробітництва, спрямованого на отримання електронних доказів; важливо, що поточна робота над Другим додатковим протоколом до Конвенції надасть додаткові можливості для розширеного міжнародного співробітництва та доступу до даних у хмарі. Навіть більше, існує набір правових стандартів для захисту приватності та персональних даних у контексті соціальних медіа. Зокрема, Модернізована Конвенція про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних, яка відкрита для підписання будь-

якою країною світу і встановлює міжнародні стандарти, має слугувати загальним договором щодо захисту даних. Нарешті, було розроблено низку правових документів для забезпечення вільних виборів, зокрема, шляхом регламентування фінансування виборчих кампаній та заходів, спрямованих на запобігання нерівності в контексті висвітлення засобами масової інформації під час виборів як онлайн, так і офлайн.

151. Водночас декілька документів Ради Європи засвідчують можливість подальшого вдосконалення. Зокрема, Доповідь РЄ про інформаційний безлад за 2017 рік містила низку рекомендацій для урядів, міністерств освіти, медіаорганізацій, технологічних компаній та громадянського суспільства, спрямованих на вирішення проблем, які виникають у зв'язку з щораз більшою кількістю недостовірної інформації, дезінформації чи зловмисної інформації та їх впливом на демократичні процеси; а у Дослідженні РЄ щодо виборів за 2017 рік зроблено висновок, що поточна нормативно-правова база не є більше достатньою для підтримки рівних умов політичної конкуренції та обмеження ролі грошей на виборах, і запропоновано низку заходів для вирішення цієї проблеми.

152. З огляду на основні результати зазначених документів та цього дослідження, нещодавні зміни щодо впливу каналів виборчих комунікацій в інтернеті змушують вдатися до заходів у таких сферах:

- A. Перегляд норм і положень щодо політичної реклами у сенсі доступу до медіа (оновлення квот та лімітів мовлення і категорії звітності, запровадження нових заходів, що охоплюють інтернет-медіа, платформи та інші сервіси, подолання наслідків мікротаргетування) та в сенсі витрат (розширення сфери комунікаційних каналів, охоплених відповідним законодавством, визначення моніторингових спроможностей національних органів влади).

- B. Підзвітність інтернет-посередників у сенсі прозорості та доступу до даних із підвищенням прозорості витрат, особливо на політичну рекламу. Зокрема, інтернет-посередники повинні забезпечити доступ до даних про платну політичну рекламу, щоб уникнути сприяння протиправному (іноземному) втручанню у вибори, та визначити категорії цільової аудиторії.

- C. Якісна журналістика: зростання точності та надійності новин, посилення взаємодії з аудиторією, зміцнення суспільних і місцевих засобів масової інформації, посилення саморегулювання з додатковим зверненням уваги на прозорість онлайн-новин та їх обіг.

- D. Розширення можливостей виборців критично оцінювати цілеспрямовану (таргетовану) дію виборчих повідомлень для запобігання впливу фальшивої, оманливої та шкідливої інформації (із належним обміркуванням щодо меж для ініціатив із перевірки фактів); зусилля, спря-

мовані на медіаграмотність (включно з грамотністю щодо соціальних мереж) через освіту й адвокацію.

- E. Відкритий інтернет: забезпечення нейтральності мережі, розгляд законодавчого зміцнення прав користувачів на відкритий інтернет, забезпечення того, що будь-які обмеження доступу до інтернет-контенту засновані на чіткій та передбачуваній нормативно-правовій базі, яка регулює застосування будь-яких таких обмежень, а також забезпечення судового нагляду для запобігання можливим зловживанням.

- F. Захист даних: підтвердження та захист права на анонімність в інтернеті, регулювання та суворе обмеження щодо створення й використання профілів у всіх видах різних контекстів. Окрім того, Рада Європи могла б розглянути можливість прийняття керівних принципів щодо обмежень, які будуть застосовуватися до технологій нагляду, зокрема й до міжнародної торгівлі такими технологіями; просування Конвенції 108+ як «золотого світового стандарту» і можлива розробка спеціального правового документа, який би враховував великий ризик, що постає у сфері захисту персональних даних у зв'язку з використанням цифрових технологій у політичних кампаніях та рекламі.

153. Як було підкреслено вище, природа інтернету та приватна власність на інформаційні магістралі роблять сучасні виклики перед демократією та виборчими процесами особливо складними. Тому міжнародне співробітництво та залучення відповідних приватних акторів є незамінним для вирішення таких викликів і забезпечення права на вільні вибори та функціонування демократії в майбутньому.

ДЛЯ НОТАТОК

Держави-члени Ради Європи взяли на себе зобов'язання «*проводити вільні вибори з розумною періодичністю шляхом таємного голосування в умовах, які забезпечують вільне вираження думки народу у виборі законодавчого органу*».

Протокол 1 до Європейської конвенції про захист прав і основоположних свобод,
Стаття 3: Право на вільні вибори

«Штучний інтелект породжує важливі та невідкладні питання. Штучний інтелект вже серед нас – змінює інформацію, яку ми отримуємо, вибір, який ми робимо, та спосіб, у який функціонують наші суспільства. У найближчі роки штучний інтелект відіграватиме ще більшу роль у діяльності урядів та державних інституцій, а також у взаємодії громадян та їх участі у демократичних процесах».

Марія Пейчинович Бурич
Генеральний секретар Ради Європи

У цю збірку входять різні документи Ради Європи, які визначають стандарти та дають рекомендації державам-членам щодо того, як забезпечити право на вільні вибори, передбачене Європейською конвенцією з прав людини, в епоху цифрових технологій та штучного інтелекту. Ця збірка буде регулярно оновлюватися відповідними документами Ради Європи, щойно вони будуть розроблені та схвалені.

www.coe.int

Рада Європи є провідною організацією у сфері прав людини на континенті. Вона налічує 47 держав-членів, серед яких усі держави-члени Європейського Союзу. Кожна держава-член Ради Європи стала учасницею Європейської конвенції з прав людини – угоди, метою якої є захист прав людини, демократії та верховенства права. Дотримання Конвенції в державах-членах контролює Європейський суд з прав людини.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE