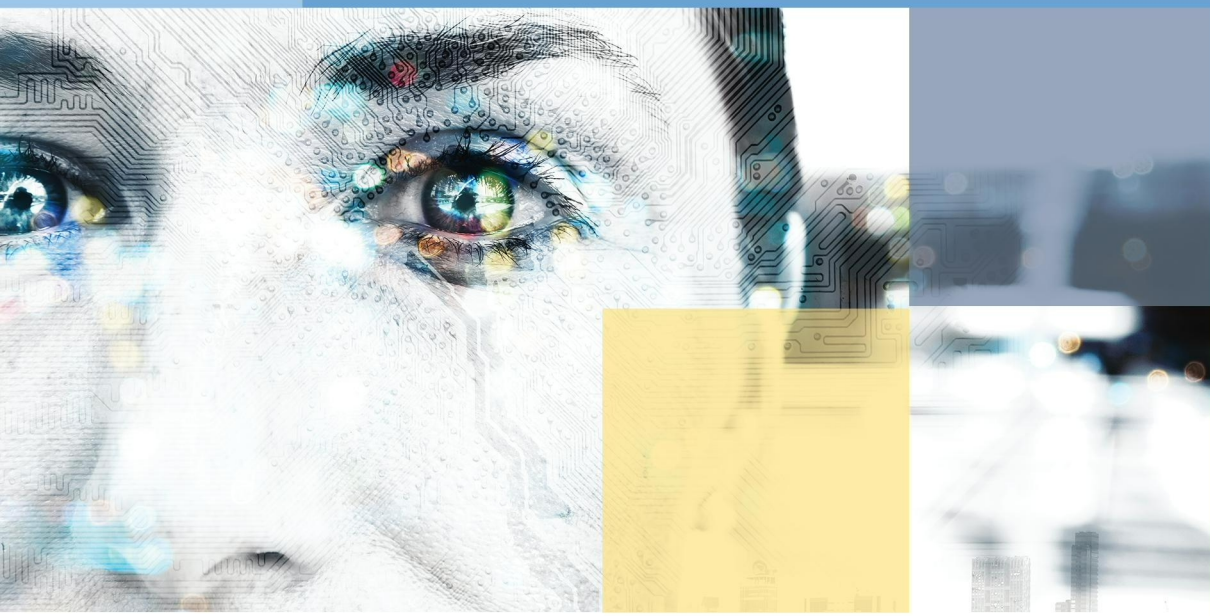
ЦИФРОВІ ТЕХНОЛОГІЇ У ВИБОРАХ

Питання, висновки та перспективи



COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

ЦИФРОВІ ТЕХНОЛОГІЇ У ВИБОРАХ

Питання, висновки та перспективи

Ардіта Дріза Маурер

Рада Європи

Це видання розроблено Управлінням з виборів і громадянського суспільства Ради Європи та перекладено українською мовою за сприяння та в рамках проєкту Ради Європи «Підтримка прозорості, інклюзивності та чесності виборчої практики в Україні».

Це видання містить раніше неопубліковані роботи. Висловлені у цьому виданні думки належать авторці та не обов'язково відображають офіційну позицію Ради Європи.

Обкладинка та дизайн:
Ганна Война

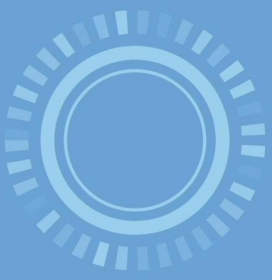
Фото на обкладинці: Shutterstock

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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

ELECLAB

Useful
Relevant
Sustainable
Owned


Розробка нормативно-правової бази щодо цифрових технологій, які використовуються у виборчому циклі*

* Це дослідження було проведено на запит Центральної виборчої комісії за підтримки проєкту Ради Європи «Підтримка прозорості, інклюзивності та чесності виборчої практики в Україні», що впроваджується в рамках Плану дій Ради Європи для України на 2018–2021 роки.

Зміст

ВСТУП

На різних етапах виборчого циклу цифрові рішення вже використовують органи управління виборчим процесом (ОУВП), виборці, політичні партії, органи виборчого правосуддя, засоби масової інформації тощо. Географічні інформаційні системи для визначення меж виборчих округів та встановлення виборчих дільниць, електронні реєстри виборців, пристрої для електронного голосування або інтернет-системи для голосування, оптичні сканери для підрахунку паперових бюлетенів, електронні рішення для передавання результатів голосування із виборчих дільниць до центральних органів влади, електронне підписання вимоги щодо ініціативи чи референдуму, електронне підписання списків затверджених кандидатів чи партій, системи збору та публікації результатів або їхня візуалізація за географічним розподілом, статистичні методи для оцінювання точності результатів та виявлення потенційного шахрайства – це деякі приклади цифрових рішень, які використовують у виборчому циклі. Вони базуються на оцифрованих даних. Інші цифрові технології, які вже використовують або планують використовувати, охоплюють біометрію, блокчейн, хмарні обчислення, штучний інтелект тощо.

Цифрові рішення для виборів мають узгоджуватися із принципами, які застосовуються для демократичних виборів. Однак практичне пристосування правових принципів до цифрових технологій – непросте завдання. Перша складність полягає в загальному характері правових принципів, сформульованих із використанням загальних та широких понять. Їхнє застосування в конкретному контексті потребує тлумачення з метою з'ясування точного значення та практичних наслідків, які випливають із принципів. Друга складність полягає в технічному характері цифрових рішень, внутрішнє налаштування та функціонування яких може зрозуміти лише невелика кількість фахівців, на відміну від пересічних осіб, які не зможуть обійтися без технічної допомоги. Втім, саме пересічні особи (виборець, адміністратор виборчого процесу, суддя, спостерігач тощо) мають використовувати і перевіряти цифрові рішення та їхні результати і, зрештою, довіряти їм.

Під регулюванням використання цифрових рішень розуміють, грубо кажучи, здійснення двох кроків. Спершу необхідно конкретизувати принципи демократичних виборів, тобто з'ясувати їхнє значення та врахувати вимоги, які застосовують у відповідному контексті. Другий крок – перетворення таких юридичних вимог у положення, які регулюють питання налаштування, використання та контролю цифрового рішення. Регулювання питання використання цифрових рішень має бути забезпечене на достатньому рівні для того, аби гарантувати дотримання принципів вищого рівня.

Регулювання важливе для тих, хто створює цифрові рішення, тих, хто вирішить їх упровадити, та тих, хто їх використовує, відстежує, контролює тощо. Це може бути працівник виборчої дільниці, виборець, спостерігач, центральний орган влади з питань опрацювання результатів голосування тощо. Тому важливо сформувати належну нормативно-правову базу, щоб права, обов'язки, повноваження і т. ін. всіх учасників були їм зрозумілі. Врешті, регулювання важливе для того, щоб вибори були вільними, чесними та демократичними.

Рада Європи та її держави-члени обговорюють використання цифрових технологій на виборах протягом останніх двадцяти років. У центрі уваги стоять питання електронного голосування та електронного підрахунку. Рада Європи ухвалила першу рекомендацію щодо електронного голосування у 2004 році та оновила її у 2017 році[1], розширивши визначення електронного голосування шляхом включення до нього електронного підрахунку бюлетенів. Однак інші цифрові рішення, які використовують під час виборчого циклу, як-от електронні реєстри, рішення для інформації про виборців, підрахунок голосів, передавання результатів тощо, не увійшли до Рекомендації CM/Rec(2017)5 щодо стандартів для електронного голосування.

У розділах, представлених нижче, подано огляд відповідних міжнародних правових інструментів, а також висвітлено деякі питання, які законодавець або регулятор має брати до уваги, зіштовхуючись з упровадженням цифрових рішень на виборах. Основну увагу акцентовано на керівних принципах, належних практиках та набутому досвіді.

Важливо зробити два попередні зауваження. По-перше, у кожній країні виборчі та політичні процеси відрізняються, на них впливають історичні, географічні, культурні та інші особливості. Це означає, що рішення, яке виявилося успішним в одному місці, може не бути реалізоване в такий самий спосіб та/або може не бути вдалим у інших місцях. Однак, незалежно від контексту, цифрові рішення також мають спільні технічні характеристики. Цей документ зосереджується саме на загальних рисах, а тому запропоновані тут загальні висновки мають бути дійсними повсюди.

По-друге, чинні керівні настанови щодо електронного голосування можна застосовувати й до інших цифрових рішень, які використовують на виборах, оскільки голосування – найскладніша та найчутливіша стадія виборчого процесу. Тому в цьому дослідженні часто траплятимуться посилання на досвід електронного голосування. Водночас у цьому документі міститься декілька новел порівняно з поточними документами щодо електронного голосування: він враховує всі цифрові рішення й не обмежується електронним голосуванням, а також пропонує зважати на деякі засвоєні уроки/висновки, отримані з нещодавнього досвіду використання електронного голосування,

1. Попередня Рекомендація Rec(2004)11 про юридичні, оперативні й технічні стандарти електронного голосування та пов'язані з нею Керівні принципи щодо сертифікації та прозорості. Була замінена Рекомендацією CM/Rec(2017)5 щодо стандартів для електронного голосування та пов'язаними з нею Керівними принципами щодо імплементації.

зокрема щодо прозорості й перевірки, які ще не знайшли відображення в запропонованих щодо електронного голосування керівних інструментах. Варто зауважити, що наразі Рада Європи працює над можливими керівними вказівками щодо використання цифрових технологій на виборах відповідно до загальноприйнятих принципів демократичних виборів[2].

2. Див. роботу Ради Європи/Європейського комітету із питань демократії та врядування Ради Європи (CDDG) щодо керівних настанов у використанні цифрових технологій упродовж виборчого циклу, за винятком фази голосування, що вже розглянуто в Рекомендації Комітету Міністрів Ради Європи CM/Rec(2017)5, а також виборчої агітації (соціальні медіа, інформація, дезінформація) та питань фінансування, які врегульовано у рамках інших ініціатив.

ПРАВОВІ СТАНДАРТИ

Це дослідження зосереджується на застосуванні принципів вільних та чесних демократичних виборів. До уваги також варто брати й інші принципи, пов'язані з виборами, як-от принципи щодо свободи поглядів і вираження думок, свободи мирних зібрань, свободи об'єднань, свободи пересування, свободи від дискримінації, право на ефективний правовий засіб захисту. Проте у цьому документі мова про них не йтиме.

Під час розгляду питання регулювання цифрових рішень, що використовуються на виборах, варто зважати як на міжнародні та національні інструменти, що регулюють питання виборів, так і на ті, що регулюють питання цифрових технологій.

1. Нормативно-правова база щодо виборів

a. Міжнародні інструменти

Міжнародно-правові зобов'язання охоплюють статтю 21 Загальної декларації прав людини 1948 року[3], статтю 25 Міжнародного пакту про громадянські та політичні права 1966 року (надалі – МПГПП) та статтю 3 додаткового (першого) Протоколу до Конвенції про захист прав людини й основоположних свобод Ради Європи (надалі – стаття 3 першого Протоколу до Європейської конвенції з прав людини), як її тлумачить Європейський суд з прав людини. Ці міжнародно-правові документи обов'язкові до виконання в тих країнах, які їх ратифікували[4]. Хартія основних прав Європейського Союзу містить схожі права та застосовується у країнах ЄС.

Офіційні тлумачення зазначених вище документів, інших політичних зобов'язань та принципів так званого європейського виборчого доробку є водночас частиною міжнародної правової бази щодо виборів. Зокрема, йдеться про Загальний коментар статті 25 МПГПП, практику Європейського суду з прав людини щодо статті 3 першого Протоколу до Європейської конвенції з прав людини, Копенгагенський документ Наради з безпеки та співробітництва в Європі (НБСЄ) 1990 року та інші зобов'язання, які стосуються виборів, Кодекс належної практики у виборчих справах 2002 року і Кодекс належної практики щодо референдумів 2007 року Європейської комісії «За демократію через право» (Венеційська комісія) Ради Європи.

3. Загальна декларація прав людини не є договором, однак її положення належать до загальновизнаних і розглядаються як звичаєве міжнародне право.

4. Усі держави-члени Ради Європи ратифікували Міжнародний пакт про громадянські та політичні права; деякі надали свої застереження (скажімо, Швейцарія – щодо таємниці голосування/стаття 25 МПГПП). 45 із 47 країн-членів Ради Європи ратифікували перший Протокол до Європейської конвенції з прав людини. Швейцарія та Монако підписали, але наразі не ратифікували його. Однак, за винятком відсутності таємного голосування на деяких виборах у Швейцарії (голосування здійснюється шляхом підняття рук), всі інші елементи закону Швейцарії суворіші та ширші порівняно зі статтею 3 першого Протоколу до Європейської конвенції з прав людини. Зазвичай така сама ситуація й в інших країнах. Міжнародні положення зазвичай пропонують мінімально необхідні стандарти, які дотримуються та є суворішими на рівні національного законодавства.

Авторитетні дослідження та оцінки проведених виборів і нормативно-правового регулювання для проведення виборів також містять рекомендації, при розгляді яких, звісно, варто брати до уваги особливості кожного окремого випадку, що аналізується, а також можливість застосування таких рекомендацій деінде. Наприклад, інтерес становлять звіти за результатами спостереження за виборами ОБСЄ/БДІПЛ (Бюро з демократичних інститутів і прав людини ОБСЄ), ПАРЄ (Парламентська Асамблея Ради Європи) тощо, а також спільні висновки ОБСЄ/БДІПЛ і Венеційської комісії Ради Європи щодо нормативно-правового регулювання у сфері виборів, зокрема й питань використання цифрових технологій у виборах. Інші дослідження, як-от Керівні принципи ОБСЄ/БДІПЛ щодо перегляду нормативно-правової бази для проведення виборів 2013 року та настанови ОБСЄ/БДІПЛ щодо спостереження й оцінювання цифрових рішень, які застосовують на виборах (зокрема й їхнє регулювання), також становлять неабиякий інтерес для регулятора. Ці документи містять цінні підказки, однак вони не дають вичерпних рекомендацій щодо врегулювання тих питань, які стосуються використання цифрових технологій на виборах.

Рада Європи стала першовідкривачем у питаннях врегулювання цифрових технологій, які використовують у процесах голосування та підрахунку. Першу рекомендацію було ухвалено 2004 року, яку згодом замінила Рекомендація CM/Rec(2017)5 щодо стандартів для електронного голосування. Це єдиний міжнародний інструмент, який дає рекомендації щодо втілення принципів європейського виборчого доробку щодо вимог до систем електронного голосування. Принципи передбачають загальне, рівне, вільне, пряме виборче право, таємне голосування, організацію виборів через регулярні проміжки часу, а також дотримання основних прав, рівнів регулювання і стабільності виборчого законодавства, процедурних гарантій. Рекомендація CM/Rec(2017)5 містить 49 стандартів, а саме детальні вимоги (Додаток 1), які застосовують до всіх видів електронного голосування та електронного підрахунку. Їх роз'яснено у Пояснювальній записці до Рекомендації. Вказівки щодо процедури впровадження містяться у відповідних керівних принципах імплементації Рекомендації CM/Rec(2017)5. Хоча ця Рекомендація стосується лише електронного голосування та електронного підрахунку, її норми можна враховувати у процесі планування інших цифрових рішень.

b. Національні інструменти

Регулювання виборчого процесу має національну прерогативу. Принципи вищого порядку, що регулюють виборчий процес, містяться в національній конституції та/або національному законодавстві про вибори. Такі принципи передбачають і розвивають міжнародні принципи. Детальні вимоги зазвичай містяться в регуляціях нижчого рівня. Вибори до Європейського Парламенту додатково врегульовує Європейський акт про вибори членів Європейського Парламенту, яким передбачено загальні та прямі вибори. У деяких країнах місцеві вибори можуть бути врегульовані на місцевому рівні. Втім, що стосується вільних і чесних демократичних виборів, усі нормативно-правові акти (наднаціональні, національні та місцеві) містять принаймні всі принципи вищого порядку, що закріплені у вищезгаданих міжнародних інструментах

(МПГПП та статті 3 першого Протоколу до Європейської конвенції з прав людини).

Принципи демократичних виборів вищого рівня запроваджувались поступово у національне законодавство та практику в XIX столітті, коли заснована на участі громадян демократія, яка відома нам сьогодні, почала свій розвиток після американської та французької революцій[5]. Технології (прості та високорозвинені) супроводжували цей розвиток. Запровадження таємниці голосування (австралійського голосування) в середині XIX століття стало результатом надання виборчих прав великій кількості виборців: відкрите голосування вже було неприйнятним, оскільки могло спричинити й спричиняло неналежний вплив[6]. Механічні пристрої для голосування запровадили ще в XIX столітті, а згодом запровадили й комп'ютери в 1960-х роках, електронні зчитувальні пристрої для голосування (DRE) у 1990-х роках та інтернет-голосування після 2000 року[7]. Спочатку механічна, а потім обчислювальна техніка супроводжували й підтримували проведення декількох правових реформ, а саме щодо: боротьби з фальсифікаціями[8], заохочення рівності виборців, надання права голосу, спроби полегшити процес голосування, спроби активізації участі у голосуванні.

На національному рівні регулювання технологій для використання їх на виборах переважно здійснювалося у дві хвилі. Спочатку було запроваджено регулювання використання простих технологій (паперових та механічних рішень), зокрема, в 1960–1970-х роках у Німеччині, Нідерландах та Франції. Пізніше таке регулювання було «оновлене» з огляду на цифрові рішення, і здебільшого воно стосувалося використання в 1990-х роках пристроїв для електронного голосування або електронного підрахунку. Країни, які обрали інтернет-голосування, розробили нові спеціальні регуляторні механізми, які, проте, було сформовано за аналогією до діючих «паперових» систем, а саме – голосування за допомогою поштового зв'язку (скажімо, у Швейцарії чи Естонії на початку 2000 року).

Незважаючи на достатньо детальний характер порівняно з регуляторними положеннями щодо паперового чи механічного голосування, регуляторні положення щодо пристроїв для голосування та підрахунку голосів у Німеччині, Нідерландах та Франції було визнано такими, що порушують конституційні

5. *Encyclopædia Britannica:* Існує прямий взаємозв'язок між кількістю виборців, формалізацією та стандартизацією практики голосування.

6. *Encyclopædia Britannica:* Австралійське голосування, яке також називають таємним голосуванням, – це система голосування, за якої виборці роблять свій вибір у приватному порядку на однакових роздрукованих та поширених урядом бюлетенях або віддають свій голос, використовуючи інші засоби, які забезпечують таємницю голосування. Цю систему запровадили спочатку в Австралії, потім поширили в Європі та США, аби задовольнити щораз вищі вимоги громадськості та парламенту щодо захисту виборців.

7. Така тенденція була і є нехарактерною для виборів. Із часів Промислової революції наприкінці XVIII – початку XIX століття технології сприяли зростанню та трансформуванню економік.

8. Шахрайство було досить поширеним, особливо в XIX та в першій половині XX століття, скажімо, в США, де корумповані юрисдикції чинили опір запровадженню пристроїв для голосування. Див.: Douglas W. Jones and Barbara Simon's, 2012, *Broken Ballots – Will Your Vote Count?* (Дуглас В. Джонс та Барбара Саймон, 2012 рік. *Зіпсовані бюлетені: чи врахують ваш голос?*).

принципи. Критерій відповідності (якому регулювання має відповідати) визначається законодавцем, суддею конституційного суду чи регулятором, й інколи він не є чітко визначеним. До того ж трапляються різні визначення. У деяких країнах критерій відповідності був таким, що регуляторні положення не можна було оновити, і тому використання пристроїв для голосування було призупинено (Німеччина, Нідерланди). В інших країнах кількість пристроїв для голосування була значно зменшена (Франція) внаслідок незадовільного рівня наявної регуляторної бази. Подекуди регуляторні оновлення запроваджували істотні зміни, дозволяючи подальше використання пристроїв для голосування (Бельгія, запровадження механізму контрольного відстеження результатів голосування з використанням бюлетенів (VVPAT)).

Нормативно-правове регулювання інтернет-голосування розвивалося ще швидше. В Австрії було визнано, що регулювання інтернет-голосування порушувало конституцію, оскільки не було достатньо деталізованим, щоб дозволити членам виборчих комісій виконувати свої завдання без технічної допомоги. Оскільки таке регулювання не було та не могло бути оновлене настільки, щоб задовольнити конституційні вимоги, запровадження інтернет-голосування в Австрії поки передбачити не можна. У Швейцарії аналіз тривалої експериментальної фази та нормативно-правового регулювання першого покоління, впровадженого у 2002 році, посприяв важливому оновленню нормативно-правової бази у 2013 році. Регулювання другого покоління запровадило новели, які відображали краще розуміння цифрових технологій: політика щодо ризиків, вимоги до перевірки, широкий контроль незалежними та експертними органами, більш жорсткий захист даних, вимоги щодо прозорості тощо. Рекомендації Ради Європи щодо електронного голосування розвивалися за схожим сценарієм; це також стосується і нормативно-правового регулювання в Естонії. Останній досвід застосування нових регуляторних положень (Швейцарія, Естонія) засвідчує потребу їхнього подальшого вдосконалення задля врегулювання питання перевірки чи прозорості. Така динаміка становить інтерес тоді, коли передбачено й регулювання інших цифрових рішень.

Судова практика вищих національних судів відіграла важливу роль у з'ясуванні практичного значення виборчих принципів у контексті їхнього застосування до цифрових рішень. Особливу увагу привертали рішення конституційних судів Німеччини (2009 року) та Австрії (2011 року). Судова практика продемонструвала важливість тлумачення принципів у частині їхньої трансформації у докладні вимоги до технологій та допомогла сформувати загальну згоду щодо необхідності детального регулювання цифрових технологій. Вона показала, що одні й ті самі принципи можна тлумачити в дуже різний спосіб, що зрештою призводить до різних результатів залежно від фактичних, історичних, культурних особливостей. Підготовку такого тлумачення необхідно покласти на законодавця/регулятора, а не на технічних працівників або постачальників технологій.

Якщо порівнювати з електронним голосуванням, то цифрові рішення на виборах досі залишаються не достатньо врегульованими. Однак зростає

усвідомлення того, що цю ситуацію потрібно змінювати з огляду на роль цифрових рішень у забезпеченні доброчесності виборів. Дослідження та звіти, у яких оцінюють налаштування й використання цифрових рішень на національному рівні, становлять інтерес для регулятора.

2. Нормативно-правова база щодо нових технологій

a. Міжнародні інструменти

Правові інструменти, що стосуються цифрових технологій, можуть мати важливе значення, навіть якщо вони не стосуються безпосередньо виборів. Скажімо, Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) слугує настановою для будь-якої країни, яка розробляє комплексне національне законодавство щодо кіберзлочинності, та є основою для міжнародного співробітництва між державами-учасницями цієї Конвенції. У керівній настанові щодо втручання у вибори пояснюється, як Конвенцію можна застосовувати для вирішення питань втручання у вибори за допомогою комп'ютерних систем. Конвенція криміналізує декілька видів поведінки, у нашому випадку – злочини, спрямовані проти виборів. Процесуальні повноваження та положення про взаємну правову допомогу, які містяться в цій Конвенції, мають важливе значення під час розслідувань та проваджень щодо втручання у вибори.

Інструменти щодо захисту даних, а саме Модернізована Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108+) та відповідний документ ЄС, Регламент (ЄС) 2016/679, Загальний регламент захисту даних (GDPR)[9], також мають важливе значення. Конвенцію 108+ та GDPR розробляли паралельно, а тому вони взаємно узгоджені. Керівний документ Європейської комісії пояснює застосування GDPR у виборчому контексті. Однак більшість даних, які використовують на виборах, – це перевірені дані, обробку яких можна дозволити лише тоді, коли в законі закріплено відповідні гарантії. Це означає, що захист виборчих даних потрібно врегульовувати у регуляторних актах щодо виборів, які є суворішими, ніж інструменти захисту даних.

Наднаціональне (на рівні ЄС) законодавство про кібербезпеку лише починає формуватися. Директива про безпеку мережевих та інформаційних систем (Директива NIS), ухвалена Європейським Парламентом у липні 2016 року, – перший законодавчий акт про кібербезпеку на всій території ЄС. Вона передбачає правові заходи для підвищення загального рівня кібербезпеки в ЄС, вимагаючи від держав-членів відповідного оснащення, створення групи співробітництва для підтримки й полегшення стратегічної співпраці щодо

9. Регламент (ЄС) 2016/679 Європейського Парламенту та Ради (Загальний регламент захисту даних), який 25 травня 2018 року став чинним на всій території ЄС. Єврокомісія зазначає, що він забезпечує ЄС інструментами, необхідними для вирішення питань незаконного використання персональних даних у виборчому контексті.

інцидентів у сфері кібербезпеки та обміну інформацією про ризики, а також сприяння культурі безпеки у сферах, які життєво важливі для економіки й суспільства. Після набуття чинності Директиви в 2019 році було ухвалено Акт про кібербезпеку ЄС, відповідно до якого уперше на всій території ЄС запроваджується система сертифікації кібербезпеки для продуктів, послуг та процесів інформаційно-комунікаційних технологій (ІКТ).

Останнім часом (а саме з 2016 року) особливу увагу приділено кібербезпеці цифрових рішень, які використовують на виборах, та на конкретному застосуванні до них міжнародних інструментів із захисту даних або із кібербезпеки. Європейська комісія розробила настанови щодо застосування нормативного акта ЄС про захист даних (GDPR) у виборчому контексті[10]. Робота на рівні ЄС із питань кібербезпеки виборчих технологій сприяла створенню Збірки з кібербезпеки виборчих технологій, яка спрямована на обмін досвідом та надання рекомендацій, а також огляду інструментів, методів та протоколів для виявлення кіберзагроз, їх запобіганню та пом'якшенню. Комітет із питань Конвенції про кіберзлочинність (T-CY) Ради Європи підготував рекомендації щодо застосування Будапештської конвенції до випадків втручання у вибори за допомогою комп'ютерних систем. У інших документах, які становлять інтерес, розглянуто ситуації щодо того, як різні країни вирішують питання такого характеру та визначають належну практику (зокрема, у дослідженні Міжнародного інституту демократії та сприяння виборам (IDEA) «Кібербезпека на виборах та моделі міжвідомчої співпраці» 2019 року).

b. Національні інструменти

До цифрових рішень, які використовують на виборах, так само застосовують і національні нормативно-правові акти про захист даних, прозорість, кібербезпеку, електронну ідентичність, управління реєстрами тощо, навіть якщо такі нормативно-правові акти не стосуються конкретно виборів. Але це у випадку, якщо немає спеціальних норм, що регулюють ці питання у виборчому законодавстві й відповідно мають пріоритет (*lex specialis*).

Національне регулювання щодо кібербезпеки або захисту від кіберзлочинності наразі приводиться у відповідність до міжнародних інструментів. Визначено належні практики щодо забезпечення кібербезпеки виборчих технологій (наприклад, згадана вище Збірка із кібербезпеки виборчих технологій, уперше опублікована у березні 2018 року); очікується, що такі практики сприятимуть подальшому наближенню національних практик у цих сферах.

10. Європейська комісія, вільні та чесні вибори – Керівний документ. Керівництво Єврокомісії щодо застосування нормативного акта ЄС про захист даних у виборчому контексті. *Заява Європейської комісії на зустрічі лідерів у Зальцбурзі, 19–20 вересня 2018 року* (COM(2018) 638 final).

3. Приклади регулювання з інших сфер

Диджиталізація впливає на всі сфери життя. Вона руйнує попередні способи поведінки, витісняючи їх та ставлячи під сумнів старі навички й підходи. Законодавство та інші сфери перебувають під тиском. Цікаво спостерігати за тим, як це питання регулюється в інших сферах (наприклад, у критично важливих системах, що мають спільні риси з виборами).

Можна спостерігати фрагментарність підходу застосування законодавства про інтернет у сфері дотримання захисту даних, кібербезпеки тощо[11]. Однак у сфері виборів визнають, що до всіх таких питань необхідно застосовувати більш жорсткі вимоги, а відповідні стандарти мають бути закріплені у спеціальному виборчому нормативно-правовому регулюванні. Отже, є імовірність того, що у випадку з виборчою сферою підхід буде менш фрагментарним.

Захист основоположних прав у цифровому контексті – це загальна потреба. Загальновизнаним фактом є те, що необхідно посилити застосування основоположних прав при використанні цифрових технологій для протидії руйнівним тенденціям. Немає необхідності в нових конституційних положеннях щодо використання цифрових технологій, проте є велика потреба в ефективному застосуванні чинних конституційних положень до цифрових технологій. Великим питанням є те, як це зробити. І це справді виклик для законодавця в контексті регулювання питання цифрових рішень на виборах.

Як приклад можна навести систему охорони здоров'я, яка взяла на озброєння та у використання багато цифрових рішень. Ця система є життєво важливою для суспільства. Досвід багатьох країн можна узагальнити так: «Ми бачимо, що останніми роками на ринку з'являється низка цифрових рішень у сфері охорони здоров'я. Деякі рішення були гарними, а деякі – не дуже. Але найбільшим викликом було визначення загального стандарту того, як має виглядати гарне рішення»[12]. Таке твердження буде актуальним й для виборчої сфери. Відповідь варто шукати в нормативно-правовій базі щодо цифрових рішень, які використовують у виборчому процесі.

11. Замість багатьох інших джерел див.: Udo di Fabio, *Grundrechtsgeltung in digitalen Systemen, 2016*.

12. UK National Health System, How we assess health apps and digital tools (Національна система охорони здоров'я Великої Британії. Як ми оцінюємо програми та цифрові інструменти у сфері здоров'я). https://digital.nhs.uk/services/nhs-apps-library/guidance-for-health-app-developers-commissioners-and-assessors/how-we-assess-health-apps-and-digital-tools#top

ЗАПИТАННЯ ВІД І ДО РЕГУЛЯТОРА

Коли законодавець ставить за мету замінити, доповнити або удосконалити поточні прості технологічні рішення, які використовують на виборах, на цифрові рішення, він[13] зіштовхується з питаннями на перетині виборчого законодавства та цифрових технологій, які потребують вирішення. Наведені нижче питання базуються на опрацьованих документах (див. посилання нижче).

1. Визначення проблеми

Найкраще, якщо запровадження цифрових інновацій стане вирішенням наявних проблем, а не просто самоціллю. Чітке визначення проблеми, яку необхідно вирішити, – це перший крок до пошуку відповідного рішення. «Проблема» – це різниця між поточною та бажаною ситуацією. Мова може йти про певне питання, яке потребує коригування, про потенційне підвищення ефективності або удосконалення процесу досягнення принципів вищого рівня.

Визначення «початкової» проблеми корисне для того, щоб відрізнити її від подальших проблем, які можуть виникнути внаслідок використання цифрової технології та оцінювання конкуруючих прав. Складова процесу ідентифікації «проблеми» полягає у виявленні тих, на кого така проблема впливає, або ж тих, хто зацікавлений у її вирішенні, та відповідно з'ясуванні їхніх очікувань. Це можуть бути певні категорії виборців (як-от експатріанти, люди зі слабким зором тощо), виборча адміністрація, політичні конкуренти тощо. Будь-яка інновація у виборчому циклі має враховувати наявні інтереси. Пропозиції щодо цифрових рішень мають спиратися на дослідження проблеми та на очікування користувачів.

Після визначення проблеми та перед вибором рішення необхідно оцінити ефективність поточних і можливих рішень для досягнення вільних, чесних та демократичних виборів. Важливо, щоб такі оцінки широко застосовувались.

2. Цілі та завдання

Наступний крок – визначення бажаної ситуації та встановлення завдань для досягнення цієї мети. Цілі (кількісні та якісні) будуть критеріями оцінювання рішення. Мета та завдання мають бути «нейтральними щодо рішення». Досвід показує, що під час визначення цілей та завдань варто уникати чіткого уявлення про рішення. До того ж цілі та завдання мають бути узгодженими.

13. У цьому документі ми використовуємо поняття «законодавець» (зазвичай парламент) або «регулятор» (зазвичай уряд чи його підрозділи) як синоніми.

З огляду на це, подальший крок полягає у визначенні можливих рішень. Усі можливі рішення необхідно розглядати з метою пошуку тих рішень, які найкраще сприятимуть зміцненню конституційних принципів. Досвід показує, що цифрові рішення не можуть бути найкращим варіантом для всіх випадків. Аналіз їхніх переваг та ризиків – наступний важливий крок. Наприклад, робоча група Міністерства юстиції Фінляндії дійшла висновку, що інтернет-голосування не варто запроваджувати на загальних виборах, оскільки у такому випадку ризиків більше, ніж переваг. Хоча технічно це було можливо, проте технологія вважалась такою, що «ще не на достатньо високому рівні задовольняє усі вимоги» у контексті вирішення питань, пов'язаних із перевіркою та таємницею голосування.

3. Переваги та недоліки

Для оцінювання можливості впровадження запланованого рішення законодавець має враховувати як його переваги, так і недоліки. Зазвичай законодавець отримує інформацію про ці аспекти через ініціатора регулювання, а також може консультуватися з іншими експертами.

Деякі переваги стосуються адміністрування виборів, інші можуть стосуватися виборців або загалом всієї системи. У контексті адміністрування виборів цифрові рішення можуть сприяти більш швидкому отриманню результатів, передбачати менший ризик помилок, полегшити взаємодію та обмін інформацією в режимі реального часу або покращити контроль над реєстрами, забезпечуючи ефективні механізми ідентифікації повторюваних записів. Можна підкреслити ефективність та економічну доцільність. Проте переваги у різних країнах сприймаються по-різному. Наприклад, мобільна технологія, яка дає змогу швидше оголосити результати виборів, може бути визнана дуже корисною в тих країнах, де це допомагає зменшити напругу під час виборчих перегонів із невеликим розривом між політичними суперниками. Натомість в інших країнах із менш конфліктною політичною культурою така технологія, вочевидь, не матиме такого великого значення.

Із точки зору виборців та перспектив для демократії цифрові рішення можуть запропонувати переваги у питаннях доступності (онлайн-реєстрація, дистанційне голосування), незалежності (скажімо, деякі варіанти електронного голосування можуть запропонувати людям з інвалідністю можливість таємного голосування, яке б вони за інакших обставин не мали), запобігання мимовільним помилкам під час заповнення бюлетенів тощо. Водночас запроваджувати технології задля того, аби виглядати сучасними перед електоратом, не рекомендовано.

Законодавець повинен мати можливість отримати обґрунтовану інформацію про реальні вигоди. Деякі з них можна оцінити ще до запровадження технології (скажімо, ефективність, швидкість, відсутність помилок, прозорість тощо). Інші ж вигоди більш гіпотетичні та складні для оцінювання аж до моменту ефективної реалізації запропонованого рішення (як-от підвищення рівня участі, підвищення довіри виборців). З огляду на це, законодавець може

розглянути механізми періодичного оцінювання переваг та недоліків після того, як рішення набуде чинності, а також періодичної повторної оцінки таких рішень.

До моменту прийняття рішення про впровадження цифрових технологій на виборах необхідно провести ґрунтовні дискусії. Основні виклики потрібно публічно обговорити. Серед питань для обговорень також мають бути питання сталості та економічної доцільності використання технології. У контексті аналізу досвіду деяких країн серед проблемних питань також постає питання порівняно високих витрат на обслуговування пристроїв та оновлення програмного забезпечення.

Окрім того, країни зіштовхуються із таким серйозним викликом, як кібербезпека. Важливо стежити за стійкістю цифрових систем до кіберзагроз, аби запобігти неправомірному втручанню чи шахрайству на виборах. Цифрові рішення необхідно регулярно оновлювати. Поруч має постійно бути навчений та досвідчений персонал. Можливі ситуації, коли для забезпечення конституційно прийнятного виборчого середовища необхідно виділяти дедалі більше фінансових та людських ресурсів, зокрема для цифрових рішень, доступних через інтернет, як-от дистанційне голосування. Витрати на регулярне тестування систем або на заходи, пов'язані зі зберіганням та оновленням обладнання чи необхідністю залучити кваліфікований персонал, – важливі складники, які необхідно враховувати.

Технологія може допомогти покращити виборчі процеси; однак ті, хто раніше почав застосовувати технології, також повідомляють про зростання складнощів унаслідок впровадження ІКТ. Так, спланувати виборчі цикли стає дедалі складніше. Зі зростанням витрат на організацію виборів збільшується й кількість укладених вартісних контрактів із приватними фірмами (і часто міжнародними). Можлива залежність від рішень приватного сектора є головним недоліком, який має обговорюватися законодавцем.

Вплив імовірних збоїв у цифрових рішеннях на доброчесність виборів – ще одне питання, яке викликає занепокоєння. Істотного негативного впливу на виборчий цикл фактично можна завдати за порівняно невеликих зусиль через зменшення вимог до цифрових рішень. Проте водночас можливо передбачити інноваційні рішення, які допомагатимуть протистояти таким ризикам. Законодавець має добре розуміти переваги, недоліки та суть відповідних рішень, аби мати можливість повноцінно все зважувати та ухвалювати обґрунтовані рішення.

Зазвичай для усунення недоліків важливо запастися терпінням на етапі впровадження цифрових рішень. Чіткі цілі, техніко-економічні обґрунтування, пілотні проєкти мають передувати та спрямовувати запровадження цифрових рішень у виборчому процесі. На нашу думку, існує необхідність у періодичному оцінюванні переваг та недоліків після впровадження рішення й у проведенні періодичної повторної оцінки таких рішень.

4. Підхід «Виборчий цикл»

Законодавець має мислити якомога ширше у питаннях використання цифрових рішень упродовж усього виборчого циклу. Як показує практика, одне з перших питань полягає у вивченні рівня автоматизації усього циклу. Мета полягає в розумінні та регулюванні питання про використання цифрових технологій упродовж циклу, а не лише в застосуванні окремих рішень. Рішення можуть швидко еволюціонувати, тоді як основні особливості ключового методу, ймовірно, зберігатимуться в довготерміновій перспективі й повинні бути врегульовані для усього циклу.

Необхідно дослідити інтеграцію цифрових рішень та їхню потенційну синергію з іншими низькотехнологічними рішеннями, які використовують у виборчому циклі. Тривалість експлуатації цифрових технологій – окрема проблема. Така тривалість може бути порівняно короткою, а тому необхідно зіставляти тривалість експлуатації різних технологій, які використовують упродовж виборчого циклу.

Ще один важливий аспект стосується потреби, аби законодавець чи регулятор критично переглянув усі процеси, у рамках яких розглядається цифровізація. Добре відомо, що технологія не поліпшить ключового процесу: якщо в ньому є проблеми, цифрова технологія на відміну від низькотехнологічних рішень може лише збільшити такі проблеми і завдати ще відчутнішої шкоди.

5. Міжгалузевий підхід

Законодавець має підходити до питання регулювання цифрових рішень не лише з точки зору юридичних аргументів та обґрунтувань, а й із добрим розумінням технічних питань. Така вимога передбачає міжгалузеву роботу. Дуже важливу роль відіграють визначення та тлумачення. Визначення важливі для покращення взаєморозуміння, і за останні роки було розроблено декілька глосаріїв, які пояснюють юридичні та технічні терміни для фахівців обох напрямів (приклади містяться у Додатку II до Рекомендації CM/Rec(2017)5, глосарії Венеційської комісії з виборчих та технічних термінів тощо). Такі визначення – необхідні та важливі, але недостатні.

Цифрові рішення базуються на математиці. Програмісти потребують формальних/чітких роз'яснень відповідних правових понять (скажімо, принципи вільних та чесних демократичних виборів), на основі яких вони формують моделі або рішення. Якщо ключові визначення змінюються, рішення також потребує вдосконалення. На практиці правові принципи мають дуже широкі визначення. Їхнє застосування в конкретних ситуаціях потребує роз'яснення. Роз'яснення допоможе розтлумачити поняття у кожній окремій ситуації. Роз'яснення також необхідне для оцінювання суперечливих понять та цінностей. Що стосується цифрових рішень, важливо, щоб такі роз'яснення давали компетентні органи, а не довіряли цю роботу лише постачальникам рішень або технічним працівникам.

Необхідно застосовувати міжгалузевий підхід. Такий підхід потребуватиме неодноразових обмінів даними між юридичними та технічними експертами. Законодавець має передбачити відповідні ресурси, структуру та час для проведення такого важливого діалогу.

6. Незалежне рішення

Прийнятність використання цифрових рішень на виборах залежить від того, чи відповідають вони принципам вищого рівня, зокрема й принципам вільних і чесних демократичних виборів. Таку відповідність спершу необхідно передбачити на регуляторному рівні.

Жоден міжнародний керівний документ не вимагає від країн (відповідно і законодавців) упроваджувати цифрові технології на виборах. Як зазначалося раніше, таке рішення залежить від багатьох чинників, деякі з них чітко зумовлені специфікою певної країни. Крім того, цифрові технології – це не завжди найкраще рішення. Підхід, застосований у міжнародних інструментах, полягає в тому, щоб закликати країни до усвідомлення необхідності забезпечення відповідності цифрових рішень конституційним положенням і надати керівні настанови щодо цього питання. Навіть коли впровадження цифрових інструментів заохочується, головною передумовою є дотримання їх відповідності принципам вільних та чесних виборів (наприклад, змінений Акт ЄС про вибори (не набув чинності), який надає державам-членам свободу пропонувати... електронне голосування або інтернет-голосування, якщо вони впевнені в дотриманні відповідних правил ЄС щодо захисту персональних даних, таємниці голосування та достовірності результатів)[14].

Іноді міжнародні рішення можуть побічно змушувати країни до диджиталізації виборчих процесів. Змінений Акт ЄС про вибори (ще не набув чинності) запроваджує нову статтю, яка покладає на кожну державу-члена зобов'язання призначати орган, відповідальний за обмін даними щодо виборців та кандидатів зі своїми колегами в інших державах-членах із метою уникнення дублювання записів у реєстрах і недопущення багаторазового голосування. Такі обміни інформацією фактично змушують оцифровувати реєстри, оскільки, вочевидь, буде неможливо змістовно порівняти дані й виявити подвійні записи, якщо таку роботу проводити вручну. Таке «вимушене оцифрування» варто ретельно обговорити, перш ніж воно стане обов'язковим.

14. Стаття 223 Договору про функціонування Європейського Союзу (ДФЄС) передбачає внесення змін до Акту про вибори задля забезпечення *«єдиної процедури у всіх державах-членах або відповідно до загальних для всіх держав-членів принципів»*. На додаток до гармонізації матеріально-правових норм (наприклад, щодо різного мінімального віку для можливості балотуватися на виборах або щодо загальних мінімально необхідних порогових меж) цей нормативний акт також має на меті *«заохотити участь виборців на виборах до Європейського Парламенту та повною мірою скористатися наданими можливостями, які пропонують технологічні розробки»*. У статті 4а зазначено, що *«держави-члени можуть передбачати можливості дострокового голосування, голосування за допомогою поштового зв'язку та електронного голосування й інтернет-голосування на виборах до Європейського Парламенту. Якщо вони це роблять, вони вживають заходів, достатніх для забезпечення, зокрема, надійності результату, таємниці голосування та захисту персональних даних відповідно до вимог чинного законодавства Союзу»*. Однак незрозуміло, на підставі яких свідчень автори акту дійшли висновку, що електронне голосування підвищить рівень участі.

Зрештою, рішення про впровадження цифрових рішень є національною прерогативою. Його має ухвалити національний законодавець, спираючись на національні інтереси. Як свідчить рішення конституційного суду Німеччини 2009 року, кожне суспільство має знайти власне рішення та врахувати наслідки кожної модернізації, зокрема й ціну таких наслідків. Кожне суспільство, тобто законодавець, має вирішити, чи готове таке суспільство до модернізації і чи здатне платити ту ціну, в основі якої лежить не лише фінансовий чинник, а й важливіші цінності. Законодавець також має вирішити, чи готова і здатна країна запровадити стабільну та корисну модернізацію. Гарним підходом є проведення тестування, що надасть важливу інформацію для ухвалення рішення.

7. Необхідність, форма та рівень регулювання

Регулювання – необхідна основа для відповідності цифрового рішення конституційним положенням. Досвід показує, що регулювання часто розглядають наприкінці процесу введення в дію після того, коли рішення майже фіналізоване. Такий підхід неправильний, зокрема з урахуванням попередніх розділів щодо виявлення проблеми, оцінювання цілей та завдань тощо. Передбачається, що регулювання має запропонувати вказівки для розроблення рішень. Це означає, що законодавець має зайняти проактивну позицію у регулюванні основних аспектів використання цифрових технологій на виборах у нейтральний спосіб щодо самого рішення.

Як показує досвід багатьох країн (США, Німеччина, Нідерланди, Франція та ін.), регуляції, успадковані від механічних чи інших низькотехнологічних рішень, незважаючи на оновлення, непридатні для регулювання цифрових рішень. Загалом проведення аналогій із традиційними процесами недостатньо. Як показує приклад Німеччини, недостатньо встановити в законі, що «пристрої можна використовувати за умови забезпечення таємності голосування» (стаття 35 Федерального закону про вибори). Детальне регулювання має чітко визначати, що під цим мається на увазі, й уможливити здійснення контролю дотримання таких вимог незалежними контрольними механізмами.

Інше питання полягає в тому, хто і що регламентує. У деяких країнах саме суди визначили, якої форми має бути регулювання, щоб забезпечити відповідність цифрових рішень встановленим вимогам. Конституційний суд Німеччини зазначив, що регулювання має бути детальним до тієї міри, щоб громадянин міг проконтролювати процедуру опрацювання його/її голосу за відсутності в нього/неї технічних знань чи підтримки. Це важливе визначення прозорості виборів. Звичайно, суд «розкрив» це визначення (спираючись на його розуміння відповідних конституційних положень) і нічого не вигадував. У інших країнах, як-от США чи Швейцарії, суди запропонували сформулювати такі визначення законодавцеві. В Індії вищий суд ухвалив рішення, що застосування пристроїв для голосування потребує механізму контрольного відстеження результатів голосування з використанням паперових бюлетенів задля забезпечення дотримання встановлених принципів, але виборчий орган вже очікував на

таке рішення. Спільним у всіх випадках є те, що визначення конкретної суті принципів вищого порядку в контексті, коли використовують цифрові рішення, впливає на саму суть принципів. Отже, рішення має ухвалювати компетентний орган, зазвичай це законодавець.

Делегування регуляторних повноважень уряду, Центральній виборчій комісії тощо має бути чітко окреслено. Наприклад, Венеційська комісія та ОБСЄ/БДІПЛ підкреслили, що використання цифрових рішень, які є основними питаннями у виборчих процедурах (як-от інтернет-голосування), необхідно чітко врегулювати в законодавстві.

Аспекти регулювання у федеральних державах більш складні. У такому разі впровадження нової технології має додатково узгоджуватися з децентралізованою системою управління виборами. В Аргентині провінції розширили регуляторні повноваження, і розходження у регулюванні електронного голосування в різних провінціях лише завдали шкоди. Аналогічно у Канаді відсутність федеральних чи провінційних стандартів дозволила багатьом муніципалітетам ухвалювати рішення переважно відокремлено від інших. В обох випадках розрахунок на постачальників, аби встановити вимоги для кібербезпеки та громадської відповідальності, викликав проблеми. У цьому контексті Швейцарія, ще одна федеральна країна, може слугувати гарним прикладом: на відміну від інших аспектів виборів інтернет-голосування насамперед та переважно регулюють на федеральному рівні, забезпечуючи застосування однакових стандартів на всій території країни. Однак це (наразі) не стосується інших цифрових рішень, які застосовують на виборах, як-от виключно електронний підрахунок: кантони чинили опір спробам гармонізувати/централізувати такі регуляції на федеральному рівні.

8. Зміст регулювання

a. Докладні вимоги

Докладне регулювання важливе в контексті введення в дію цифрових рішень для виборчого процесу, для процедур контролю та сертифікації, для визначення прав та обов'язків зацікавлених сторін, а також для інформування новаторів і постачальників цифрових рішень щодо вимог.

Венеційська комісія та ОБСЄ/БДІПЛ наголосили, що положення щодо використання технологій мають супроводжуватися ретельною підготовкою законодавчого регулювання питання використання технічних рішень та відповідних процедур, яких потрібно дотримуватися. Ці положення мають охоплювати, поміж іншим, аспекти, пов'язані з закупівлями, тестуванням, аудитом та доступом громадськості до технологій. Венеційська комісія та ОБСЄ/БДІПЛ підкреслюють, що заявляти про загальні принципи недостатньо в умовах врегулювання цифрових рішень для виборчого процесу, якщо немає гарантії того, що ці загальні принципи реалізовуватимуться разом із конкретними правилами, які є основоположними для дійсно демократичних

виборів. Тому необхідно, щоб регуляторні положення розробляли детально та відповідально.

При впровадженні нових технологій на різних етапах виборчого циклу, зокрема під час голосування та підрахунку голосів, виникає конфлікт між вимогами таємниці голосування та точності. Наприклад, виборець повинен мати можливість перевірити, що його/її голос був зареєстрований і підрахований відповідно до його/її волі (точність), але в той же час виборець не повинен мати змоги отримати докази, що дозволять йому/їй продати свій голос або довести третій особі, як він/вона проголосував/-ла (таємниця). Громадськість повинна мати можливість перевірити правильність результату (точність) без того, щоб дізнатися, як проголосували окремі виборці (таємниця). Криптографія пропонує рішення, які певною мірою відповідають таким вимогам. Однак не можна повністю і одночасно задовольнити всі вимоги, які можуть перебувати в колізії одна з одною. Криптографічні рішення засновані на припущеннях, що деякі учасники процесу, наприклад, чесні. Такі припущення безпосередньо впливають на реалізацію загальних принципів вищого рівня та повинні детально регламентуватися компетентним органом.

b. Права людини – у центрі уваги

Сьогодні загальновизнано, що інструменти участі з використанням ІКТ мають за своїм дизайном узгоджуватися з правами людини. У нашому випадку така вимога означає необхідність підготовки детального регуляторного положення, що вказувало б, як права людини (у нашому випадку йдеться про права на вільні, чесні та демократичні вибори) будуть забезпечуватися при використанні цифрових рішень на виборах. Таке регуляторне положення має передувати розробленню та впровадженню конкретного рішення. Розробники рішень повинні зосереджувати свою роботу на врахуванні таких регуляторних вимог. Вони мають заздалегідь знати, як запропонована технологія відповідатиме принципам вільних, чесних, демократичних виборів.

Знову ж таки цей підхід засвідчує, що законодавець має проявляти активність та мати всеохопне бачення використання цифрових рішень у виборчому циклі. Нижче наведено кілька складових елементів (перелік далеко не вичерпний) такого регулювання.

c. Практичність

Практичність – важливий аспект не лише для отримання зручних для користувача рішень. Це важливо і з точки зору безпеки. Щоб досягти бажаного результату, але при цьому мінімізувати помилки/зловживання, цифрові рішення необхідно належно розуміти та використовувати. Користувачі мають бути готові помічати та вирішувати можливі помилки. Важливо, щоб такі питання було вирішено на регуляторному рівні, щоб компетенції та обов'язки користувачів були чітко визначені. Це також підтверджує важливість освіти потенційних користувачів та інших зацікавлених сторін, а також необхідність регуляторних положень щодо інформації та освіти.

d. Захист даних

Під час регулювання питання електронного голосування необхідно враховувати інструменти захисту даних. Але, як уже згадувалося раніше, виборчі дані є особливими, а отже щодо їх захисту мають бути передбачені більш жорсткі вимоги у виборчому законодавстві.

Варто наголосити, що захист даних під час виборів означає захист певних даних із боку контролера даних (наприклад, виборчого органу). Таємниця голосування вимагає, щоб ні орган адміністрування виборів, ні будь-які інші суб'єкти не знали, як проголосував виборець. Водночас орган влади має контролювати доступ до певного рішення, оскільки такий доступ обмежений лише тими, хто має на це право. Це робить використання цифрових рішень щодо деяких виборчих аспектів, як-от голосування, особливо делікатною справою. Саме тому законодавець має ухвалити важливі рішення щодо цього. Наприклад, йому треба буде проаналізувати та зважити такі цінності, як безпека та прозорість чи свобода голосувати. Такі рішення мають передувати впровадженню цифрових технологій.

Поточне регулювання, здебільшого щодо електронного голосування, було удосконалене та потребує подальшої роботи над ним. Важливо забезпечити належний контроль за реалізацією захисту даних. Зважаючи на вибори до Європейського Парламенту 2019 року, Європейська комісія підготувала керівний документ щодо застосування нормативного акта про захист даних на території ЄС у виборчому контексті.

e. Прозорість

Роль прозорості полягає в тому, щоб забезпечити належну роботу всієї системи та конкретного цифрового рішення. Водночас регулятор повинен визначити, які частини системи мають бути прозорими, на які конкретні наслідки очікувати, хто бере участь у процесі забезпечення прозорості, як забезпечити необхідну прозорість та контролювати її, як карати за її недотримання, як поводитися з інформацією, яку розкривають на підставі принципу прозорості, тощо. Крім того, учасники мають бути поінформовані та мати змогу брати участь у процесі забезпечення прозорості, особливо якщо прозорість є частиною безпеки системи.

Прозорість має й інший вимір: у деяких випадках очікується, що цифрові рішення зроблять політику прозорішою, допоможуть побороти корупцію, покращити сферу державних послуг, істотно збільшити рівень залученості громадян до процесів розробки місцевої політики тощо. За умов належного регулювання та застосування у цій царині можна навіть досягти успіху.

Упродовж останніх років регулювання прозорості цифрових рішень зазнало істотного розвитку, починаючи від підходів маскування та системи «чорного ящика» і завершуючи частковою прозорістю (залучення політичних партій та акредитованих спостерігачів до процесу забезпечення прозорості), більш відкритим підходом, який передбачає публікацію вихідних кодів та іншої

відповідної документації, контроль із боку незалежних фахівців, етичний хакінг рішень тощо. Таку прозорість вважають частиною заходів безпеки.

f. Кібербезпека

За останні роки питання кібербезпеки виборів набуло надзвичайної актуальності. Країнам стало відомо, що використання цифрових рішень, особливо пов'язаних з інтернетом, може дозволити одному суб'єкту (зокрема й іноземному) контролювати вибори через відсутність надійних та очевидних доказів коректних результатів/даних. Нормативні положення мають охоплювати стратегії управління ризиками, заходи захисту, можливості перевірки, планування дій у разі надзвичайних ситуацій.

Що стосується стратегій управління ризиками, заходів захисту та планування дій у разі надзвичайних ситуацій, на регіональному рівні існують рекомендації, засновані на міжнародних правових інструментах, які стосуються кібербезпеки. Скажімо, Комітет із питань Конвенції про кіберзлочинність (Будапештська конвенція) оприлюднив Керівну настанову щодо виборів. У настанові йдеться про використання процедурних повноважень та положень про взаємну правову допомогу в конкретному кримінальному розслідуванні або провадженні, пов'язаному з втручанням у вибори, що передбачені Конвенцією. Конвенція криміналізує декілька видів поведінки (незаконний доступ, незаконне перехоплення, втручання в дані, втручання в роботу системи, неналежне використання пристроїв, фальсифікація з використанням комп'ютерних ресурсів). Якщо це робиться без отримання згоди фізичних і юридичних осіб або інших груп, в умовах виборчого процесу така поведінка порушує вільні, чесні та демократичні вибори. Втручання у вибори має часто міжнародний характер, а тому Конвенція пропонує настанови щодо співпраці країн у боротьбі з такими правопорушеннями. До того ж на рівні ЄС Група NIS зі співробітництва оприлюднила певні вказівки, присвячені кібербезпеці технологій, які використовують на виборах. Мета цієї збірки з кібербезпеки виборчих технологій 2018 року полягає в обміні досвідом та наданні настанов, а також огляді інструментів, методів і протоколів для виявлення таких загроз, їхньому запобіганню та пом'якшенню.

Що стосується можливостей верифікації, то основну частину зусиль докладають саме у сфері електронного голосування. Останній досвід показує, що контроль над створенням та реалізацією рішень має вирішальне значення, якщо такі рішення належно функціонують. Однак процес використання таких методів ще перебуває в зародковому стані, а їхнє розуміння з боку неспеціалістів досить обмежене. Потрібно мати більше міжгалузевого розуміння, якщо такі методи необхідно застосувати для гарантування безпеки цифрових рішень, які використовують на виборах.

g. Контроль, правозастосування, підзвітність

Досвід електронного голосування показує, що регулювання має передбачати мінімальні вимоги, зокрема й щодо контролю за рішенням та щодо незалежної

перевірки як рішення, так і його результатів (див. Рекомендацію CM/Rec(2017)5 щодо стандартів електронного голосування).

Такі вимоги можна застосовувати й поза електронним голосуванням. Вони мають певною мірою віддзеркалювати принципи вільних та чесних демократичних виборів й інші відповідні правові принципи. Цифрові рішення мають підлягати оцінюванню з боку незалежних та компетентних органів через відповідні проміжки часу та після запровадження важливих змін. Такі органи мають бути відкритими для аудиту та інформувати про потенційні проблеми й загрози.

Повну відповідальність за дотримання вимог навіть у разі збоїв й атак покладають на орган, відповідальний за виконання завдання в рамках цього цифрового рішення. Орган має здійснювати контроль, аби переконатися в тому, що рішення, усі пов'язані з ним матеріали та процедури є справжніми, належно функціонують, оновлюються, захищаються, експлуатуються у безпечний спосіб. Рішення повинно віддзеркалювати реальний стан, а це означає, що важливе значення має налагодження співпраці з науковими колами (незалежними та компетентними експертами). Досвід роботи з електронним голосуванням показує, що справа стосується складного завдання, а сучасність рішення з часом стає важко підтримувати на належному рівні.

Як зазначалося раніше, для критично важливих та пов'язаних з інтернетом рішень контролю (сертифікація, аудит тощо) може бути недостатньо. Необхідно забезпечити незалежну перевірку результатів. Залежно від рішення перевірка може набувати різних форм. Це може бути цифрова, паперова форма або комбінація цих форм. Що стосується цифрових інструментів верифікації, то досвід показує, що існує потреба нагляду за контролерами, тобто контролю за системою верифікації. Окрім цього, аби правильно виконувати свою функцію, рішення щодо перевірки мають бути зрозумілими та застосовними для користувачів, які можуть бути виборцями, виборчою адміністрацією, спостерігачами тощо. Тому необхідно мати кваліфікованих користувачів, які зможуть правильно використовувати рішення. Зокрема, деякі атаки на цифрові рішення можна виявити лише тоді, коли достатня кількість кінцевих користувачів проводить перевірку, розуміє проблему, виявлену під час перевірки, та скаржиться на цю проблему.

Понад десять років тому конституційний суд Німеччини заявив про недостатність сертифікації та потребу в перевірці з боку виборця. Суд відхилив аргумент, за яким робилося припущення, що розгорнуті системи можна вважати функціонально придатними, оскільки до моменту їхнього розгортання вони пройшли перевірку та відповідну сертифікацію за визначеною процедурою. Рекомендація Комітету Міністрів Ради Європи CM/Rec(2017)5 щодо стандартів електронного голосування передбачає проведення індивідуальної й універсальної перевірки голосування та загальних результатів (див., зокрема, стандарти 15–18) – два важливих результати системи електронного голосування. Це допомагає реалізувати право на вільне голосування.

Німецька чи австрійська модель верифікації потребує, щоб перевірка була зрозумілою та аби її проводила пересічна особа (виборець чи член виборчої комісії) без будь-яких технічних знань. Для цього необхідно забезпечити співіснування паперового методу, зрозумілого пересічній особі, та цифрового рішення. Інша модель верифікації – естонська чи швейцарська. Під методом верифікації розуміють можливість контролю та перевірки з боку експертів, які посилаються на методи, затверджені відповідною науковою спільнотою. Втім, як видається, важко застосувати такі методи до виборів та референдумів із коефіцієнтом один до одного.

h. Управління змінами, ресурси та співпраця з приватним сектором

Ще одна відмінність між традиційними та цифровими рішеннями – це еволюційний характер цифрового методу. Процес регулювання має зважати на цей аспект та відображати його. Тісна пов'язаність з еволюційним характером технології означає те, що цифрові рішення потребують кваліфікованих кадрових та фінансових ресурсів. Із часом потреба в ресурсах може змінюватися залежно від зусиль, необхідних для забезпечення конституційної відповідності рішення. Потребу в ресурсах і перспективу того, що така потреба може з часом еволюціонувати, необхідно належно передбачити у процесі регулювання. Органи управління виборчим процесом, які впроваджували цифрові рішення, зіштовхувалися з проблемою обслуговування та заміни програмного й апаратного забезпечення. Є певні сумніви щодо стабільності розвитку певних виборчих технологій. Можливо, доцільно розглядати такі питання уже на етапі регулювання та уникати застосування дуже складних технологій.

Важливим аспектом є необхідна співпраця з приватним сектором. Приватний сектор може відігравати кілька ролей, зокрема й як постачальник рішень, контролер, орган сертифікації, оператор тощо. З огляду на це законодавець має ретельно проаналізувати відносини між державним та приватним секторами. Докладні вимоги, що забезпечуватимуть дотримання принципів вищого рівня, необхідно передбачити вже на етапі підготовки тендерної документації. Остаточну відповідальність за проведення виборів покладено на державний орган, відповідальний за їх проведення. Регулювання має відповідати вимогам підзвітності та контролю і, як показує досвід, бути спроможним упоратися з наслідками можливих недоліків. Законодавець повинен ретельно розглянути залежність чутливих рішень, які критично впливають на весь виборчий цикл, від приватних постачальників та в ідеалі не допустити такої залежності. Крім того, такий орган влади повинен мати достатньо кваліфікованого персоналу й інвестувати в його навчання, аби гарантувати належне технічне обслуговування системи, сприяти впровадженню нових функцій та інших модифікацій, а також забезпечити належне його функціонування.

9. Довіра

Довіру часто згадують під час обговорення питання про використання цифрових рішень на виборах. Довіра має різні грані.

Довіру вважають передумовою впровадження цифрових рішень на виборах. Така позиція зрозуміла в контексті електронного голосування, але також вона стосується й інших цифрових рішень, зокрема біометричної технології. Впровадження технології не може усунути браку довіри до виборчої системи. У минулому застосовували й інші підходи. Ті, хто першим найзавзятіше обстоював використання цифрових технологій на виборах, належали до числа найбідніших країн часто без тривалої історії проведення демократичних виборів. У таких контекстах взяття на озброєння нових, а іноді й дорогих технологій мало на меті боротьбу зі зловживаннями та побудову довіри між сторонами, задіяними у виборчому процесі, й електоратом. Спочатку деяким країнам такі зміни вдавалися. Однак згодом стало зрозуміло, що самі лишень цифрові рішення не можуть сформувати довіри. Наявна довіра, особливо до органів влади, відповідальних за проведення виборів, є необхідною умовою впровадження цифрових рішень. Якщо громадськість чи політичні гравці не мають взаємної довіри або не довіряють цифровим рішенням, такі рішення не сприйматимуть, навіть якщо й удасться досягнути об'єктивних технічних результатів та продемонструвати їх переваги. Для успішного впровадження цифрових рішень необхідна довіра, а також громадські консультації та підтримка. Досвід показує, що консультації, тестування, апробація й т. ін. можуть допомогти встановити атмосферу довіри. Однак насамперед рішення має заслуговувати на довіру.

Дослідження звертають велику увагу на питання надійності цифрових технологій на виборах. Це стосується найсучасніших вимог, контролю, реалізації, рішень, затверджених на тому самому рівні, тощо. Проте у багатьох випадках технологію впроваджують без проведення належних досліджень, планування, апробації, навчання чи підготовки виборців, і це натомість знижує довіру до процесу та збільшує витрати. Подекуди запроваджено технології, які не заслуговують на довіру та загрожують доброчесності виборчого процесу, а такі випадки можуть призвести до зменшення довіри громадськості до виборчих процесів.

Довіра базується на прозорості. Відповідно до позиції конституційного суду Німеччини, недостатньо, щоб рішення заслуговували на довіру, а вибори були вільними, чесними та демократичними, важливо, щоб люди також були в цьому впевнені. Дотримання конституційних принципів вільних, чесних, таємних тощо виборів має супроводжуватися впевненістю людей у дійсному дотриманні цих принципів. У тому-таки суді Німеччини зауважують, що єдиний спосіб досягти цього – дозволити кожному перевіряти дотримання цих принципів.

ВИСНОВКИ

Нижче підсумовано основні моменти цього дослідження.

1. Цифрові рішення вже використовують у виборчому циклі. Вони мають відповідати всім належним **конституційним принципам**, точніше принципам вільних, чесних, демократичних виборів.

   - На відміну від регулювання низькотехнологічних рішень для регулювання цифрових рішень недостатньо лише повторно озвучити принципи. В основі регулювання мають лежати докладні положення, які трансформують принципи в докладні юридичні вимоги щодо управління цифровими технологіями.

   - Завдання для законодавця полягає в тому, аби забезпечити вже на регуляторному рівні дотримання конституційних прав.

2. **Міжнародні інструменти**, що регулюють питання виборів, є актуальними під час розробки регулювання цифрових рішень, які використовують на виборах. Сюди зараховують універсальні міжнародно-правові документи (Загальна декларація прав людини, Міжнародний пакт про громадянські та політичні права) та регіональні документи (Європейська конвенція з прав людини, Хартія основних прав ЄС), авторитетні тлумачення таких конвенцій, прецедентне право міжнародних судів, політичні зобов'язання, документи «м'якого права», дослідження та оцінювання поточних норм і використання цифрових рішень.

3. **Міжнародні інструменти**, що регулюють захист даних, кіберзлочинність чи кібербезпеку, також є актуальними.

   - Конвенція 108+ Ради Європи та Загальний регламент захисту даних ЄС (GDPR) – вельми актуальні документи, однак деякі виборчі дані належать до категорії конфіденційних: вони потребують більш жорсткого захисту, що необхідно враховувати в конкретних регуляторних положеннях, які стосуються виборів.

   - Ураховуючи положення GDPR, було розроблено Будапештську конвенцію Ради Європи щодо кіберзлочинності та правові інструменти ЄС щодо кібербезпеки, конкретні вказівки й збірки передового досвіду щодо виборів.

4. **Національні регуляторні положення щодо цифрових рішень**, які використовують на виборах, ще перебувають на початковому етапі свого розвитку, але продовжують постійно розвиватися.

   - Спеціальне нормативне регулювання стосується переважно електронного голосування. Здебільшого використовують два види регулювання. У деяких країнах з метою управління механізмами електронного голосування почали розвивати застарілі інструменти,

які регулювали застосування низькотехнологічних рішень. Однак використання більшості з них не узгоджувалося з конституцією, що призвело до припинення або різкого скорочення використання пристроїв електронного голосування. Нормативне регулювання щодо інтернет-голосування першого покоління також було визнано недостатнім. Подекуди його оновлювали задля кращого розуміння роботи цифрових технологій (політика управління ризиками, можливість перевірки, незалежний контроль, вимоги щодо прозорості), однак нещодавно отриманий досвід свідчить, що ці положення необхідно удосконалювати для кращого врегулювання таких питань, як забезпечення можливості перевірки чи прозорості.

- Інші цифрові рішення врегульовані недостатньо.

5 Чітка **ідентифікація проблеми**, яку необхідно вирішити, – це перший крок до пошуку відповідного рішення.

- Пропозиції щодо цифрових рішень мають спиратися на дослідження проблеми та на очікування користувачів.
- Такі висновки повинні мати широку підтримку.

6 Наступним кроком є визначення бажаної ситуації (**мети**) та встановлення **завдань** для досягнення цієї мети.

- Цілі та завдання мають бути «нейтральними щодо рішення».
- Визначивши їх, законодавець має розглянути всі можливі рішення з метою пошуку тих, які найкраще сприятимуть зміцненню конституційних принципів.

7 Для оцінювання можливості впровадження передбаченого рішення законодавець має взяти до уваги **як його переваги, так і недоліки**.

- Законодавець має добре розуміти переваги, недоліки та суть відповідних рішень, аби мати можливість повноцінно все зважувати та ухвалювати обґрунтовані рішення.
- Зазвичай для усунення недоліків важливо запастися терпінням на етапі впровадження цифрових рішень. Чіткі цілі, техніко-економічні обґрунтування та оцінки, пілотні проєкти мають передувати та спрямовувати запровадження цифрових рішень у виборчий процес.
- Ми вважаємо, що існує необхідність запровадити періодичне оцінювання переваг та недоліків після втілення рішення і періодичне переоцінювання таких рішень.

8 Законодавець має мислити якомога ширше з точки зору використання цифрових рішень упродовж **усього виборчого циклу**.

- Рішення можуть швидко еволюціонувати, тоді як основні особливості ключового методу, вочевидь, функціонуватимуть у довгостроковій перспективі. Ми пропонуємо, аби такі функції регулювали упродовж усього циклу. Мета полягає в розумінні та регулюванні питання про використання цифрових технологій упродовж циклу, а не лише в застосуванні окремих рішень.

- Ступінь автоматизації виборчого циклу, тривалість експлуатації різних використовуваних технологій та критичний перегляд процесів, оцифрування яких перебуває на розгляді, – дуже важливі аспекти.

9 Регулювання цифрових рішень потребує **міжгалузевого підходу**.

- Перші кроки було зроблено – за останні роки розроблено кілька глосаріїв юридичного та технічного напряму, у яких подано фахівцям відповідних галузей тлумачення використовуваних термінів. Такий захід необхідний і важливий, але недостатній.

- Оскільки цифрові рішення базуються на математиці, програмісти використовують формальні/чіткі визначення відповідних правових концепцій для побудови цифрових рішень. Утім, на практиці правові концепції мають дуже широке визначення, а тому потребують тлумачення. Не існує чіткого визначення правової концепції. Щодо цифрових рішень, то важливо, щоб тлумачення принципів для відповідної технології зрештою надавав компетентний орган (законодавець чи регулятор), а не постачальники рішень чи технічний персонал.

- Ми пропонуємо, щоб міжгалузева робота базувалася на постійному обміні інформацією між юридичними та технічними експертами. Законодавець має передбачити відповідні рамки, ресурси та час для проведення цього важливого діалогу, і така співпраця має стати нормою під час регулювання цифрових рішень для виборчого процесу.

10 Жоден міжнародний керівний документ не вимагає від країн (відповідно і законодавців) впроваджувати цифрові технології на виборах. Це рішення є **незалежним**. Кожне суспільство, зокрема законодавець, має вирішити для себе питання, чи готове та здатне воно запровадити таку модернізацію. Належною практикою є проведення тестування/апробації, які нададуть важливу інформацію для процесу ухвалення рішення.

11 **Необхідність**, **форма** та **рівень регулювання**

- Регулювання – необхідна основа для відповідності цифрового рішення конституційним вимогам. Воно має передбачати вказівки щодо розроблення рішень. Законодавець має проактивно регулювати основні аспекти використання цифрових технологій на виборах, у нейтральний спосіб, незалежно від рішення.

- Нормативне регулювання не повинно просто дублювати принципи або передбачати положення аналогічні для паперових рішень. Воно має чітко вказувати на практичні наслідки для принципів і дозволяти незалежним механізмам контролю забезпечувати дотримання докладно виписаних вимог.

- Визначення конкретного значення принципів вищого рівня у контексті використання цифрових рішень впливає на саму суть принципів. Отже, рішення має ухвалювати компетентний орган, зазвичай це законодавець.

- Делегування регуляторних повноважень уряду, Центральній виборчій комісії тощо має бути чітко структуроване.

- Аспекти нормативного регулювання більш складні у федеральних державах із децентралізованою системою управління виборами. Важливо переконатися, що однакові правові стандарти та рішення застосовують на всій території країни.

12 Важливо забезпечити **докладно виписані вимоги**. Заявляти про загальні принципи недостатньо у випадку регулювання цифрових рішень для виборчого процесу, якщо немає гарантії, що ці загальні принципи реалізовуватимуться разом із конкретними правилами, які є основоположними для дійсно демократичних виборів. Тому необхідно, щоб нормативне регулювання було розроблене детально та відповідально.

13 Інструменти участі **за своєю структурою мають забезпечувати дотримання прав людини**. Розробники рішень повинні зосереджуватися на дотриманні докладних регуляторних вимог до цифрових рішень. Вони мають заздалегідь знати про основний вплив запропонованої технології на дотримання принципів вільних, чесних, демократичних виборів. Детальні вимоги особливо важливі у випадку запровадження криптографічних рішень.

14 **Практичність** – важливий аспект із точки зору зручності використання та сприяння безпеці цифрового рішення.

15 Деякі виборчі дані мають конфіденційний характер.

- **Захист даних** у цьому випадку означає захист певних даних від контролера даних (наприклад, виборчого органу). Один і той самий орган має водночас контролювати доступ до певного рішення, оскільки такий доступ обмежений лише тими, хто має на це право. Це робить використання цифрових рішень щодо деяких виборчих аспектів, як-от голосування, особливо делікатною справою.

- Законодавець повинен проаналізувати та зважити протилежні цінності, як-от безпека та прозорість чи свобода голосування. Такі рішення повинні передувати впровадженню цифрового методу.

16 Регулювання **прозорості** цифрових рішень еволюціонувало до більш відкритого підходу.

- Він передбачає публікацію вихідних кодів та інших відповідних документів, контроль із боку незалежних фахівців, етичний хакінг рішень тощо. Таку прозорість вважають частиною заходів безпеки.
- Регулятор повинен визначити, які частини системи мають бути прозорими, на які конкретні наслідки очікувати, хто бере участь у процесі забезпечення прозорості, як забезпечити необхідну прозорість та контролювати її, як карати за її недотримання, як поводитися з інформацією, яку розкривають унаслідок дотримання принципу прозорості, тощо.

17 За останні роки питання **кібербезпеки** виборів стало надзвичайно актуальним. Нормативні положення, поміж іншим, мають охоплювати стратегії управління ризиками, заходи захисту, можливості перевірки, планування дій у разі надзвичайних ситуацій.

- Що стосується стратегій управління ризиками, заходів захисту та планування в разі надзвичайних ситуацій, на регіональному рівні існують рекомендації, засновані на міжнародних правових інструментах, які стосуються кібербезпеки.
- Що стосується можливостей верифікації, то основну частину зусиль докладають саме у сфері електронного голосування. Контроль над створенням та реалізацією рішень має вирішальне значення, якщо такі рішення належно функціонують. Існує необхідність у міжгалузевому підході та розумінні, якщо такі методи необхідно застосувати для гарантування безпеки цифрових рішень, які використовують на виборах.

18 **Контроль**, **правозастосування**, **підзвітність**

- Регулювання має передбачати мінімальні вимоги, зокрема й до контролю за рішенням та до незалежної перевірки як рішення, так і його результатів.
- Повна відповідальність за дотримання вимог навіть у разі збоїв й атак покладається на орган, відповідальний за виконання завдання в рамках цього цифрового рішення.
- Рішення повинно віддзеркалювати реальний стан, а це означає, що важливе значення має налагодження співпраці з науковими колами (незалежними та компетентними експертами). Досягнути такої мети із плином часу може бути складно.
- Для критично важливих та пов'язаних з інтернетом цифрових рішень контролю (сертифікація, аудит тощо) може бути недостатньо.

Необхідно забезпечити незалежну перевірку результатів. Перевірка (верифікація) може мати різні форми.

- Що стосується цифрових інструментів верифікації, то досвід показує, що існує потреба нагляду за контролерами, тобто контролю за системою верифікації.
- Рішення щодо перевірки мають бути зрозумілими та застосовними для кінцевих користувачів, які можуть бути виборцями, членами виборчих комісій, спостерігачами тощо. Зокрема, деякі атаки на цифрові рішення можна виявити лише тоді, коли достатня кількість кінцевих користувачів проводить перевірку, розуміє проблему, виявлену під час перевірки, та скаржиться щодо цієї проблеми.

19 Управління змінами

- Еволюційний характер цифрового методу повинен бути закладений у нормативне регулювання.
- Тісна пов'язаність з еволюційним характером технології означає те, що цифрові рішення потребують кваліфікованих кадрових та фінансових ресурсів. Потребу в ресурсах і перспективу того, що така потреба може з часом еволюціонувати, необхідно належно передбачити в процесі регулювання.
- Законодавець має ретельно проаналізувати відносини між державним та приватним секторами. Докладні вимоги, що забезпечуватимуть дотримання принципів вищого рівня, мають бути визначені завчасно в тендерній документації.
- Остаточну відповідальність за проведення виборів покладено на державний орган, відповідальний за проведення виборів. Нормативне регулювання має містити положення з вимогами щодо підзвітності та контролю і, як показує досвід, регулювати питання, пов'язані з наслідками можливих недоліків.
- Орган повинен мати достатньо кваліфікованого персоналу й інвестувати в його навчання.

20 Довіра

- Довіру вважають передумовою впровадження цифрових рішень на виборах.
- Рішення мають насамперед заслуговувати на довіру. Це стосується найсучасніших вимог, контролю, реалізації, рішень, затверджених на тому самому рівні тощо.
- Довіра ґрунтується на прозорості та можливостях перевірки.

СПИСОК ДЖЕРЕЛ

Міжнародно-правові тексти, керівні вказівки, оцінки, належні практики

Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms, (European Convention on Human Rights, ECHR) (in force, 1953) (Конвенція Ради Європи про захист прав людини та основоположних свобод (Європейська конвенція з права людини, ЄСПЛ) (чинна, 1953 р.)*

Council of Europe, *Convention for the protection of individuals with regard to the processing of personal data (Convention 108+), CETS № 223 (Protocol adopted in June 2018) (Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108+), CETS № 223 (Протокол, схвалений у червні 2018 р.)*

Council of Europe, Consultative Committee of the Convention 108+, *Report on Artificial Intelligence. Artificial intelligence and data protection: challenges and possible remedies (January 2019) (Консультативний комітет Ради Європи із питань Конвенції 108+. Звіт щодо штучного інтелекту. Штучний інтелект та захист даних: виклики та можливі засоби захисту (січень 2019 р.)*

Council of Europe, *Convention on Cybercrime (Budapest Convention), CETS № 185 (in force, 2004) (Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція), CETS № 185 (чинна, 2004 р.)*

Council of Europe, Cybercrime Convention Committee (T-CY), *Guidance note № 9, Aspects of election interference by means of computer systems covered by the Budapest Convention. Adopted by T-CY on 8 July 2019 (Комітет із питань кіберзлочинності (T-CY), Настанова № 9. Аспекти втручання у вибори за допомогою комп'ютерних систем, на які поширюється Будапештська конвенція. Підготовлено T-CY 8 липня 2019 р.)*

Council of Europe, European Court of Human Rights, *Guide on Article 3 of Protocol № 1 to the European Convention on Human Rights – Right to free elections (April 2019) (Рада Європи, Європейський суд з прав людини, Посібник зі статті 3 Протоколу № 1 до Європейської конвенції з прав людини. Право на вільні вибори (квітень 2019 р.))*

Council of Europe, Committee of Ministers, *Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting (Adopted by the Committee of Ministers on 14 June 2017 at the 1289th meeting of the Ministers' Deputies) (Рада Європи, Комітет Міністрів, Рекомендація CM/Rec(2017)5 Комітету Міністрів державам-членам щодо стандартів електронного голосування (Ухвалено Комітетом Міністрів 14 червня 2017 р. на 1289-му засіданні заступників міністрів))*

European Union, *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) № 526/2013 (Cybersecurity Act) (Регламент ЄС 2019/881 Європейського*

Парламенту та Ради від 17 квітня 2019 року про ENISA (Агентство Європейського Союзу з питань мережевої та інформаційної безпеки) і про сертифікацію у сфері інформаційних та комунікаційних технологій з урахуванням вимог кібербезпеки та про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку)

European Union, *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, (NIS Directive) (Європейський Союз, Директива (ЄС) 2016/1148 Європейського Парламенту та Ради від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу (Директива про NIS))*

European Union, NIS Cooperation Group, *Compendium on Cyber Security of Election Technology, CG Publication 03/2018 (Європейський Союз, Група співробітництва NIS, Збірка із кібербезпеки виборчих технологій, Публікація групи співробітництва (березень 2018 року))*

European Union, *Regulation (EU) 2016/679 General Data Protection Regulation, (GDPR) (Європейський Союз, Регламент (ЄС) 2016/679, Загальний регламент захисту даних (GDPR))*

European Commission, *Free and Fair Elections. Guidance Document (Європейська комісія. Вільні та чесні вибори. Керівний документ). Commission guidance on the application of Union data protection law in the electoral context (September 2018) (Керівництво Комісії щодо застосування нормативного акта ЄС про захист даних у виборчому контексті (вересень 2018 р.))*

European Union (Council of the), *Council Directive 94/80/EC of 19 December 1994 laying down detailed arrangements for the exercise of the right to vote and to stand as a candidate in municipal elections by citizens of the Union residing in a Member State of which they are not nationals (Європейський Союз (Рада), Директива Ради 94/80/ЕС від 19 грудня 1994 року про встановлення докладних механізмів реалізації права голосу та висування кандидатури на муніципальних виборах громадянами Союзу, які проживають у державах-членах, але не є їхніми громадянами)*

European Union, *Act concerning the election of the representatives of the Assembly by direct universal suffrage, OJ L 278, 8.10.1976, p. 5 as amended lastly by Council Decision 2002/772/EC, Euratom of 25 June and 23 September 2002 (Європейський Союз, Акт щодо обрання представників Асамблеї шляхом прямого загального голосування (ОВ L 278, 8.10.1976 р., с. 5, з останніми змінами Рішенням Ради 2002/772/ЕС, Євратом від 25 червня та 23 вересня 2002 р.))*

European Union (Council of the), *Council Decision 2018/994* [not in force] *amending the Act concerning the election of the members of the European Parliament by direct universal suffrage, annexed to Council Decision 76/787/ECSC, EEC, Euratom of 20 September 1976 (*Європейський Союз (Рада ЄС), *Рішення Ради 2018/994* [нечинне] *про внесення змін до Акта щодо виборів членів Європейського Парламенту шляхом прямого загального голосування, доповнення до Рішення Ради 76/787/ECSC, EEC, Євратом від 20 вересня 1976 р.)*

European Union, Estonian Presidency of the Council of the EU, *Tallinn Declaration on eGovernment (Oct. 2017)* (Європейський Союз, Головування Естонії в Раді ЄС, *Талліннська декларація про електронне урядування* (жовтень 2017 р.))

European Union, *Regulation № 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative (*Європейський Союз, *Регламент Європейського Парламенту та Ради № 211/2011 від 16 лютого 2011 р. щодо ініціативи громадян)*

European Commission for Democracy through Law (Venice Commission) et al., *Joint Report on Digital Technologies and Elections (June 2019)* (Європейська комісія «За демократію через право» (Венеційська комісія) та ін., *Спільна доповідь про цифрові технології та вибори* (червень 2019 р.))

European Commission for Democracy through Law (Venice Commission), *Compilation of Venice Commission opinions and reports concerning digital technologies in the electoral process, CDL-PI(2018)011 (2018) (*Європейська комісія «За демократію через право» (Венеційська комісія)*, Збірка висновків та доповідей Венеційської комісії щодо цифрових технологій у виборчому процесі, CDL-PI(2018)011 (2018))*

European Commission for Democracy through Law (Venice Commission), Grabenwarter, Ch. (Європейська комісія «За демократію через право» (Венеційська комісія), Грабенвартер Ч.) *Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe, 2004 (Звіт про сумісність дистанційного голосування та електронного голосування зі стандартами Ради Європи, 2004 рік)*

European Commission for Democracy through Law (Venice Commission), *Code of Good Practice on Electoral Matters – Guidelines and explanatory report* (2002) *(*Європейська комісія «За демократію через право» (Венеційська комісія), *Кодекс належної практики 2002 року у виборчих справах: керівні принципи та пояснювальний звіт (2002))*

IDEA*, Cybersecurity in Elections. Models of Interagency Collaboration, 2019 (*IDEA (Міжнародний інститут демократії та сприяння виборам), *Кібербезпека на виборах. Моделі міжвідомчої співпраці, 2019 р.)*

IDEA, RECEF, *The Use of New Technologies in Electoral Processes – Workshop report: Praia, Cabo Verde, 22–23 November 2017 (*IDEA (Міжнародний інститут демократії та сприяння виборам), RECEF, *Використання нових технологій у виборчих процесах. Доповідь на семінарі: Прая, Кабо-Верде, 22–23 листопада 2017 р.)*

IDEA, *Certification of ICTs in Elections, 2015 (*IDEA, *Сертифікація ІКТ на виборах, 2015 р.)*

IDEA, *Electoral Management Design, Revised Edition, 2014 (*IDEA, *Модель виборчого менеджменту, оновлена редакція, 2014 р.)*

IDEA*, International Obligations for Elections, Guidelines for Legal Frameworks, 2014 (*IDEA, *Міжнародні зобов'язання щодо виборів, Керівні принципи законодавчих рамок, 2014 р.)*

IFES, Goldsmith, B./Ruthrauff, H., *Implementing and overseeing Electronic Voting & Counting Technologies, 2013 (*IFES (Міжнародна фундація виборчих систем), Голдсміт Б./Рутрауфф Х., *Впровадження та моніторинг технологій електронного голосування та підрахунку, 2013 р.)*

OSCE/ODIHR, *Handbook for the observation of new voting technologies, 2013 (*ОБСЄ/БДІПЛ, *Посібник зі спостереження за новими технологіями голосування, 2013 р.)*

OSCE/ODIHR, *Guidelines for reviewing a legal framework for elections, 2013 (*ОБСЄ/БДІПЛ, *Настанови для перегляду законодавчої основи виборів, 2013 р.)*

OSCE/ODIHR, див.: «Needs Assessment Mission» and «Election Assessment Mission» Reports on elections held in countries of the Council of Europe region. (ОБСЄ/БДІПЛ, див.: Звіти щодо виборів, проведених у країнах регіону Ради Європи «Місія з оцінювання потреб» та «Місія з оцінювання виборів»). (див. розділи відповідних звітів, зокрема, «Нормативно-правова база», «Нові технології голосування» та «Рекомендації», доступні на вебсторінці: https://www.osce.org/elections)

UN Secretary General's High-level panel, *The age of digital interdependence, June 2019 (*Група високого рівня Генерального секретаря ООН, *Епоха цифрової взаємозалежності, червень 2019 р.)*

UN General Assembly, Human Rights Council, Report of the Office of the United Nations High Commissioner for Human Rights – *Draft guidelines for States on the effective implementation of the right to participate in public affairs (September 2018) (*Генеральна Асамблея ООН, Рада з прав людини, Доповідь Управління Верховного комісара ООН з прав людини *«Проєкт керівних принципів для держав щодо ефективного здійснення права на участь у публічних справах» (вересень 2018 р.))*

Відповідні дослідження з правових та регуляторних аспектів

Barrat, J. (Coord.) *El voto electronic y sus dimensiones jurídicas: entre la ingenua complacencia y el rechazo precipitado, Iustel (2016)*

Barrat, J. and Goldsmith, B., *Compliance with International Standards, Norwegian e-vote project (2012) (*Барат Дж. та Голдсміт Б. *Відповідність міжнародним стандартам, Норвезький проєкт електронного голосування (2012 р.))*

Benaloh, J., Rivest, R., Ryan, P. et al.*: End-to-end verifiability (2014)* (Бенало Дж., Рівест Р., Райан Р. та ін.: *Наскрізна можливість для здійснення перевірки (2014 р.)*)

Cardillo et al. *Online Voting in Ontario Municipal Elections: A Conflict of Legal Principles and Technology?, in R. Krimmer et al. (Eds.): E-Vote-ID 2019 (*Карділло та ін. *Інтернет-голосування на муніципальних виборах в Онтаріо: конфлікт правових принципів та технології? За ред. Р. Кріммер та ін.: E-Vote-ID 2019)*

Driza Maurer A.: *The Swiss Post/Scytl Transparency Exercise and its possible Impact on Internet Voting Regulation, in R. Krimmer et al. (Eds.): E-Vote-ID 2019 (*Дріза Маурер А.: *Вправа на прозорість швейцарської пошти/Scytl та її можливий вплив на регулювання інтернет-голосування. За ред. Р. Кріммер та ін.: E-Vote-ID 2019)*

Driza Maurer, A., Barrat, J. (Eds), *E-Voting Case Law: A Comparative Analysis, Routledge 2017. (*Дріза Маурер А., Барат Дж. (ред.). *Прецедентна практика електронного голосування: порівняльний аналіз, Рутледж, 2017 р.)*. Ця публікація містить розділи про правові рамки цифрових технологій, які використовують на

виборах у Німеччині, Австрії, Бразилії, Індії, Естонії, Франції, Аргентині, Фінляндії, Мексиці, Швейцарії, США, Австралії та Венесуелі.

Driza Maurer, A.: *Updated European Standards for E-voting (*Дріза Маурер А. *Оновлені європейські стандарти електронного голосування) Рекомендація Ради Європи Rec(2017)5 щодо стандартів електронного голосування. За ред. Р. Кріммер та ін.: E-Vote-ID 2017*

Driza Maurer, A. *Update of the Council of Europe Recommendation on Legal, Operational and Technical Standards for E-Voting – a Legal Perspective (*Дріза Маурер А. *Оновлення Рекомендації Ради Європи про юридичні, операційні та технічні стандарти електронного голосування – правова перспектива). У пр.: Tagungsband IRIS (Internationales Rechtsinformatik Symposion), 2016 р.*

Driza Maurer, A.: *Ten Years Council of Europe Rec(2004)11. Lessons learned and outlook. In: Krimmer, R., Volkamer, M. (eds) Proceedings of Electronic Voting 2014 (*Дріза Маурер А. *Десятиріччя рекомендації Ради Європи Rec(2004)11. Набутий досвід та перспектива. За ред. Кріммер Р., Волкамер М. Матеріали електронного голосування 2014 р.)*

Driza Maurer, A.: *Internet Voting and Federalism: The Swiss Case, In Barrat, J. (Coord.) (*Дріза Маурер А. *Інтернет-голосування та федералізм: справа Швейцарії, у співпраці з Баррат Дж.) El voto electronic y sus dimensiones jurídicas: entre la ingenua complacencia y el rechazo precipitado, Iustel (2016 р.)*

Gibson, P., Krimmer, R. et al. *A review of E-voting: the past, present and future, 2016 (*Гібсон П., Кріммер Р. та ін. *Огляд електронного голосування: минуле, сучасне та майбутнє, 2016 р.)*

Hill, R. *E-Voting and the Law. Issues, Solutions, and a Challenging Question. In Krimmer, R. et al. (eds.). Proceedings of E-VOTE-ID 2016 (*Хілл Р. *Електронне голосування та закон. Проблеми, рішення та найскладніше питання. У пр.: Кріммер Р. (ред.) та ін. Процедури E-VOTE-ID 2016)*

Krimmer et al. (Eds), See proceedings of E-Vote-ID Conferences, 2019, 2018, 2017, 2016 (За ред. Кріммер Р. та ін. Див. процедури засідань E-Vote-ID, 2019, 2018, 2017, 2016, 2016)

Loeber, L., *Legislating for e-enabled elections: dilemmas and concerns for the legislator (*Льобер Л. *Підготовка нормативних актів для запуску е-виборів: дилеми та проблеми для законодавця). In Krimmer, R. et al. (eds.) Proceedings of E-VOTE-ID 2016 (Кріммер Р. та ін. (ред.) Процедури E-VOTE-ID 2016)*

Loeber, L. *«E-Voting in the Netherlands; from General Acceptance to General Doubt in Two Years» in Krimmer, R. and Grimm, R. (Eds.) Electronic Voting 2008 (EVOTE08) (2008) (*Льобер Л. *«Електронне голосування в Нідерландах; від загального схвалення до загального сумніву за два роки». За ред. Кріммер Р. та Грімм Р. Електронне голосування 2008 (EVOTE08) (2008 р.))*

Madise, Ü. and Vinkel, P., *«Constitutionality of Remote Internet Voting: The Estonian Perspective», Juridica International, 2011 (*Мадіз Ю. та Вінкель П. *«Конституційність дистанційного інтернет-голосування: естонська перспектива», Juridica International, 2011 р.)*

Mohanty et al., *Auditing Indian Elections,* 2019 *(*Моханти та ін. *Аудит виборів в Індії, 2019 р.)*

Neumann, S., Volkamer, M.: *A Holistic Framework for the Evaluation of Internet Voting Systems In: Zissis, D., Lekkas, D. (eds.) Design, Development and Use of Secure Electronic voting Systems, IGI Global book series (2014) (*Нойман С., Волькаммер М.: *Цілісна структура оцінювання інтернет-систем голосування. За ред. Зіссіс Д., Леккас. Проєктування, розроблення та використання захищених електронних систем голосування, серія книг IGI Global (2014 р.))*

Neumann, S., *Evaluation and Improvement of Internet Voting Schemes Based on Legally-Founded Security Requirements, 2016 (*Нойман С. *Оцінювання та вдосконалення схем інтернет-голосування на основі законодавчо обґрунтованих вимог безпеки, 2016 р.)*

Puiggali, J., Rodriguez-Peréz, A.*: Designing a national framework for online voting and meeting its requirements: the Swiss experience. In Krimmer et al. (eds) E-Vote-ID 2018 Proceedings (*П'югаллі Дж., Родрігез-Перез А.: *Розроблення національної системи для онлайн-голосування та виконання її вимог: досвід Швейцарії. За ред. Кріммер та ін. Процедури E-Vote-ID 2018)*

Saltman Roy, *The History and Politics of Voting Technology. In Quest of Integrity and Public Confidence, 2008 (*Солтман Рой, *Історія та політика технологій голосування. У пошуках доброчесності та довіри громадськості, 2008 р.)*

Schwartz, B. and Grice, D. *Establishing a legal framework for e-voting in Canada, 2013 (*Шварц Б., та Гріс Д. *Створення нормативно-правової бази для електронного голосування в Канаді, 2013 р.)*

Solvak, M., Vassil, K., *E-voting in Estonia: Technological diffusion and other developments over ten years (2005–2015) (*Сольвак М., Василь К. *Електронне голосування в Естонії: технологічна дифузія та інші розробки упродовж десяти років (2005–2015 рр.))*

Spycher, O., Volkamer, M. and Koenig, R. *(2011) Transparency and technical measures to establish trust in Norwegian internet voting (*Спайхер, Волькамер М. та Кьоніг Р. *(2011) Прозорість та технічні заходи для побудови довіри до норвезької процедури інтернет-голосування)*

Taylor, G. *Constitutional restrictions on touch-screen voting computers in Germany, in Election Law Journal, Volume 9, Number 4, 2010 (*Тейлор Г. *Конституційні обмеження щодо комп'ютерів для голосуванням із сенсорним екраном у Німеччині, у пр.: Журнал виборчого права, том 9, номер 4, 2010 р.)*

Venice Commission/Permanent Electoral Authority of Romania, *Electoral Expert, Proceedings of the 1st Scientific Electoral Experts Debates «Electoral Law and New Technologies: Legal Challenges», Bucharest, 12–13 April 2016* (several experts' contributions) *(*Венеційська комісія/Постійний виборчий орган Румунії, *експерт із питань виборчих питань, Матеріали перших наукових дебатів експертів на тему «Виборче право та нові технології: юридичні виклики», Бухарест, 12–13 квітня 2016 р. (Внесок кількох експертів))*

Vinkel, P., *Remote Electronic Voting in Estonia: Legality, Impact and Confidence, TUT Press, 2015 (*Вінкель П. *Дистанційне електронне голосування в Естонії: законність, вплив та довіра, TUT Press, 2015 р.)*

Volkamer, M., Spycher, O. and Dubuis, *E. (2011) Measures to establish trust in internet voting (*Волькаммер М., Спайхер О. та Дюбуі Е. *(2011) Заходи щодо побудови довіри до інтернет-голосування)*

Volkamer, M., *Evaluation of Electronic Voting, Requirements and Evaluation Procedures to Support Responsible Election Authorities, Springer-Verlag Berlin Heidelberg 2009 (*Волькаммер М. *Оцінювання електронного голосування, вимог та процедур оцінювання для підтримки відповідальних виборчих органів, Springer-Verlag Berlin Heidelberg, 2009 р.)*

Відповідні документи у вибраних країнах

Austria, *Students' Union Act (Bundesgesetz über die Vertretung der Studierenden [Hochschülerinnen- und Hochschülerschaftsgesetz 1998 – HSG 1998]), Federal Law Gazette I 1999/22, last amendment Federal Law Gazette I 2013/79. У 2014 році Акт про учнівську спільноту 1998 року було замінено Актом про учнівську спільноту 2014 року, Federal Law Gazette I 45/2014*

Austria, Constitutional Court *(Verfassungsgerichtshof) Decision V 85-96/11-15, 13 December 2011 (*Австрія, Конституційний Суд *(Verfassungsgerichtshof), Рішення V 85-96/11-15, 13 грудня 2011 р.). Для отримання більш докладної інформації див. розділ про Австрію Меліни Освальд (Melina Oswald) «E-Voting in Austria: Legal Determination Matters» in Driza Maurer/Barrat (Eds), E-Voting Case Law: A Comparative Analysis, 2017 («Електронне голосування в Австрії: питання правового визначення». За ред. Дріза Маурер/Баррат, Прецедентне право щодо електронного голосування: порівняльний аналіз, 2017 р.)*

Belgium (Law on e-voting with paper audit trail) *(*Бельгія, *Закон про електронне голосування з паперовим журналом обліку) Loi du 7 fevrier 2014 organisant le vote électronique avec preuve papier (Moniteur belge du 14 février 2014)*

Finland, Ministry of Justice, *Working Group Report «Online voting in Finland – Feasibility study» 19.12.2017 (*Фінляндія, *Міністерство юстиції, Доповідь робочої групи «Онлайн-голосування у Фінляндії: дослідження можливостей реалізації», 19.12.2017 р.)*

France, Commission Nationale de l'Informatique et des Libertés (CNIL), *Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet*

France, *Rapport d'information n° 73 (2018–2019) de Mme Jacky Deromedi et M. Yves Détraigne, fait au nom de la commission des lois, déposé le 24 octobre 2018 «Réconcilier le vote et les nouvelles technologies»*

France, Sénat, Commission des lois, *Rapport d'information de MM. Alain Anziani et Antoine Lefevre, «Vote électronique: Préserver la confiance des électeurs», 2014*

Germany, *Ordinance on the Use of Vote Counting Devices in Elections to the German Bundestag (Verordnung über die Verwendung von Stimmenzählgeräten bei Wahlen zum Deutschen Bundestag) (BGBl. 1961 I 1618)*

Germany, Constitutional Court *(Bundesverfassungsgericht), Decision 2 BvC 3/07, 2 BvC 4/07, of 3 March 2009 (*Німеччина, Конституційний Суд *(Bundesverfassungsgericht), рішення 2 BvC 3/07, 2 BvC 4/07 від 3 березня 2009 р.). Для отримання більш докладної інформації див. розділ про Німеччину Себастьяна Зедорфа (Sebastian Seedorf), «Germany: The Public Nature of Elections and its Consequences for E-Voting» in Driza Maurer/Barrat (Eds), E-Voting Case Law: A Comparative Analysis, 2017 («Німеччина: публічний характер виборів та його наслідки для електронного голосування». За ред. Дріза Маурер/Баррат, Прецедентне право щодо електронного голосування: порівняльний аналіз, 2017 р.)*

Netherlands (The), Election Process Advisory Commission*, Report: Voting with confidence. Summary, Conclusions and Recommendations (2007) (*Нідерланди (Консультативна комісія з виборчих процесів), *Доповідь: Голосування з довірою. Підсумок, висновки та рекомендації (2007 р.))*

Swiss *Federal Chancellery Ordinance on Electronic Voting (VEleS), RS 161.116 (Постанова Федеральної канцелярії Швейцарії про електронне голосування (VEleS), RS 161.116)*

Федеральна рада Швейцарії (Перший урядовий звіт щодо можливості електронного голосування) *«Rapport sur le vote électronique. Chances, risques et faisabilité», 9 січня 2002 р., FF 2002 612 (2002 р.)*

Федеральна рада Швейцарії (Другий урядовий звіт щодо оцінювання пілотних проєктів) *«Rapport sur les projets pilotes en matière de vote électronique», 31 травня 2006 р., FF 2006 5205 (2006 р.)*

Федеральна рада Швейцарії (Третій урядовий звіт щодо оцінювання досвіду та основи для подальшого розгортання електронного голосування) *«Rapport du Conseil fédéral sur le vote électronique. Evaluation de la mise en place du vote électronique (2006–2012) et bases de développement», 14 червня 2013 року, FF 2013 4519 (2013 р.)*

Огляд цифрових технологій, які використовуються у виборчому циклі**

Зміст

** Це скорочена версія дослідження «Нові технології у виборчому циклі. Керівні настанови від Ради Європи», яку 28 січня 2020 року авторка презентувала на засіданні робочої групи з питань демократії та технологій Європейського комітету з питань демократії та врядування (CDDG) Ради Європи. Європейський комітет з питань демократії та врядування отримав завдання розробити стандарти використання нових технологій на різних етапах виборчого процесу. Цим завданням займається робоча група з питань демократії та технологій.

1. ПІДХІД І ВИЗНАЧЕННЯ

a. Вступ

У цьому дослідженні міститься огляд основних цифрових технологій, які використовуються або передбачені для використання під час виборчого циклу, а також перелік питань щодо відповідності використання таких технологій принципам демократичних виборів. Це скорочена версія дослідження «Нові технології у виборчому циклі. Керівні настанови від Ради Європи», яку 28 січня 2020 року було презентовано на засіданні робочої групи з питань демократії та технологій Європейського комітету з питань демократії та врядування (надалі – CDDG (European Committee on Democracy and Governance)) Ради Європи[1].

Основною місією Ради Європи як організації, що перебуває на сторожі цінностей, закріплених у Європейській конвенції про захист прав людини і основоположних свобод (надалі – Конвенція або Європейська конвенція з прав людини) та протоколах до неї, є контроль за дотриманням Конвенції, включаючи контроль за діяльністю, пов'язаною з виборами, у країнах регіону. Відповідно до статті 3 додаткового (першого) Протоколу до Конвенції[2] та практики Європейського суду з прав людини, орган управління виборчим процесом (тобто держава) має позитивне зобов'язання забезпечувати, щоб уся його діяльність у межах виборчого циклу, зокрема діяльність, що передбачає використання нових технологій, відповідала праву на вільні вибори. Це дослідження фокусується на дотриманні та імплементації статті 3 першого Протоколу до Конвенції новими технологіями, що використовуються у виборчому циклі. Більш детально фокус зосереджено на принципах загального, рівного, вільного виборчого права, таємного голосування і на деяких умовах, необхідних для імплементації цих принципів (наприклад, процедурних гарантіях неупередженості, прозорості, спостереження тощо)[3]. Інші дотичні до виборів принципи, такі як свобода поглядів та вираження, свобода мирних зібрань, свобода об'єднань, свобода рухів, свобода від дискримінації, право на ефективні засоби правового захисту, також мають бути досліджені. Однак у цій роботі вони не розглядаються.

---

1. Ознайомитися з роботою Ради Європи у сфері виборів та керівними настановами з питань використання цифрових технологій у виборчій сфері , зокрема з поточною роботою Європейського комітету з питань демократії та врядування (CDDG), Управління з виборчого сприяння та громадянського суспільства і Європейської комісії Ради Європи «За демократію через право» (Венеційська комісія), можна за посиланням www.coe.int.

2. 45 із 47 держав-членів Ради Європи ратифікували перший Протокол до Конвенції. Швейцарія та Монако підписали, але ще не ратифікували його. Однак, за винятком відсутності таємного голосування на (лише) деяких місцевих виборах, де вдаються до голосування шляхом підняття рук, виборчі принципи швейцарського законодавства зазвичай вважаються суворішими, ніж це закладено у статті 3 першого Протоколу до Конвенції.

3. Венеційська комісія, Кодекс належної практики у виборчих справах, висновок №190/2002, затверджений Венеційською комісією на 52-й сесії (Венеція, 18-19 жовтня 2002 року); CDL-AD (2002) 23 rev. Технології, що застосовуються у виборчому циклі, як здається, не впливають на застосування принципів прямого голосування та періодичність проведення виборів.

Цифрові рішення покращують та полегшують виборчі процеси, але вони також спричиняють появу викликів і ризиків. Вони здатні підвищити ефективність та швидкість, дозволяють уникнути помилок, яких можна припуститися під час ручної роботи, тощо, проте вони можуть також стати причиною вразливості, відкрити виборчу систему для нових загроз і уможливити нові атаки на неї. Регуляторний орган повинен приймати поінформовані рішення для того, щоб нові технології впроваджували та застосовували у безпечний спосіб. Їх безпечне використання передбачає, що цифрові рішення (як і будь-який аспект виборів) відповідають принципам демократичних виборів і відповідно гарантують, поміж іншим, загальне, рівне, вільне виборче право шляхом таємного голосування.

Усі країни регіону зобов'язалися дотримуватися мінімальних міжнародних стандартів щодо проведення демократичних виборів. Такі стандарти наведено в статті 25 Міжнародного пакту про громадянські і політичні права (МПГПП) 1966 року та в статті 3 першого Протоколу до Європейської конвенції з прав людини[4], які стосуються права на вільні вибори[5]. Згодом ці стандарти було розкрито в політичних зобов'язаннях (Копенгагенський документ Наради з безпеки і співробітництва в Європі 1990 року, що зобов'язує держави-учасниці гарантувати права людини та основоположні свободи включно з правами, що стосуються виборів), у практиці Європейського суду з прав людини та «м'якому праві» (Загальний коментар Управління Верховного комісара ООН з прав людини №25 1996 року, Кодекс належної практики у виборчих справах Венеційської комісії 2002 року і Кодекс належної практики щодо референдумів 2007 року).

У дослідженні міститься огляд деяких нових технологій, які було впроваджено або які передбачено використати у виборчому циклі, їхні основні особливості та питання відповідності міжнародним принципам, нормам та стандартам. Далі в документі проаналізовано різні стадії виборчого процесу та цифрові рішення, які використовують чи які планують використати, а також їхню відповідність міжнародним принципам, нормам та стандартам. Документ завершується висновком та деякими наскрізними питаннями, які стосуються всіх нових технологій і кожної зі стадій виборчого процесу.

Дослідження ґрунтується на попередньому документі Ради Європи у сфері електронного голосування (див. Рекомендацію CM/Rec(2017)5 щодо стандартів електронного голосування). Так само в пропонованій роботі взято до уваги документи Венеційської комісії, Управління з виборчого сприяння та громадянського суспільства, Конвенцію Ради Європи про кіберзлочинність

4. 45 із 47 держав-членів Ради Європи ратифікували цей протокол. Швейцарія та Монако підписали, але ще не ратифікували його. Однак, наприклад, у Швейцарії федеральні та кантональні виборчі принципи є фактично суворішими порівняно зі статтею 3 першого Протоколу до Європейської конвенції з прав людини. Єдиний виняток полягає у відсутності таємниці голосування на (лише) деяких місцевих виборах, де вдаються до голосування шляхом підняття рук, – таке волевиявлення визнає Верховний Суд із історичних та практичних підстав, незважаючи на критику з правової точки зору.

5. У статті 3 першого Протоколу до Європейської конвенції з прав людини зазначено: «Високі Договірні Сторони зобов'язуються проводити вільні вибори з розумною періодичністю шляхом таємного голосування в умовах, які забезпечуватимуть вільне вираження думки народу у виборі законодавчого органу».

(Будапештська конвенція) та Модернізовану Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108+), а також документи інших інституцій, таких як Бюро демократичних інститутів та прав людини Організації з безпеки та співробітництва в Європі, Міжнародний інститут демократії та сприяння виборам (IDEA) , ЄС тощо.

б. Виборчий цикл

Виборчий цикл охоплює всі кроки та процеси, необхідні для проведення виборів чи голосування[6]. Орган управління виборчим процесом (надалі – ОУВП) – орган, відповідальний за організацію виборів, який здійснює та/або контролює діяльність виборчого циклу. Поняття «циклу» також передбачає, що ці кроки повторюються з регулярними проміжками часу в кожному виборчому процесі[7]. Виборчий цикл складається з таких основних етапів:

1. **Нормативно-правова база,** включно з розробкою та підготовкою законопроєктів.
2. **Планування й підготовка** до здійснення виборчої діяльності, включно з підбором та навчанням виборчого персоналу, а також плануванням виборів.
3. **Навчання й освіта виборців**, регулювання поведінки спостерігачів.
4. **Реєстрація** виборців, політичних партій та спостерігачів на виборах; висування партій і кандидатів. Реєстрація та розгляд питань, що потенційно можуть бути винесені на референдум (народне голосування).
5. **Виборча агітація**, включно з офіційною інформацією, адресованою виборцям.

Джерело: IDEA

6. Мається на увазі виборчий цикл у розумінні, представленому IDEA у виданні *Electoral Management Design, 2014, pp. 12, 16. 75-77,* із незначними змінами та доповненнями.

7. Концепцію виборчого циклу було визначено Міжнародним інститутом демократії та сприяння виборам (IDEA) та Європейською комісією у 2005 році, щоб проілюструвати, що вибори – це не події, а процеси, а також забезпечити застосування таких знань на кожному з етапів планування та впровадження всіх проєктів виборчого сприяння з метою подовження фінансових та інших ресурсних зобов'язань, збереження орієнтації на сталість виборчих установ та загальну прихильність до демократичного розвитку країни, що виходить далеко за межі безпосередньої події, яку потрібно підтримати (https://www.idea.int/data-tools/tools/online-electoral-cycle).

6 **Організація голосування**, включно з проведенням голосування, підрахунком голосів та зведенням результатів.

7 Оголошення **результатів виборів**, включно з передачею та оприлюдненням результатів, вирішенням виборчих спорів, звітуванням, аудитом.

8 **Післявиборчі** обов'язки, включно зі знищенням та/або архівуванням матеріалів[8].

Проведення голосування з використанням принципу прямої демократії передбачає уживання аналогічних кроків і додаткових етапів, таких як формальне та/або фактичне затвердження пропозиції (ініціатива чи референдум), контроль форми збирання підписів прихильників, отримання й контроль дійсності підписів, підрахунок, підтвердження та публікація результатів і, зрештою, організація процесу голосування, якщо потрібну кількість справжніх підписів було успішно зібрано. Усі ці кроки входять до етапу реєстрації (пункт 4 у переліку вище). Після цього ОУВП інформує виборців, планує та проводить голосування тощо. У цьому дослідженні термін «виборчий цикл» стосується як виборів, так і голосувань із використанням принципу прямої демократії.

У роботі розглянуто використання нових технологій на різних етапах виборчого циклу за винятком питань формування думки й фінансування виборів, які проаналізовано в межах інших напрямів діяльності Ради Європи.

в. Нові технології

У цьому документі слова «новий» та «цифровий» використовуються як синоніми. Цифрові технології та рішення, які використовують, випробовують або планують впроваджувати у виборчому циклі, – це оцифрування (диджиталізація) документів і процедур, біометрія, блокчейн, хмарні обчислення. У роботі розглянуто використання штучного інтелекту, за винятком його застосування у сфері формування думки (передвиборна агітація).

Цифрові рішення зберігають та обробляють інформацію в цифровому вигляді, відповідно пересічна особа не може отримати до неї доступу та зрозуміти її. Більш складні технології, як-от штучний інтелект, можуть розвиватися так, що деталі їхнього функціонування перестануть бути зрозумілими навіть інженерам, які їх спроєктували. Отже, принциповою особливістю таких технологій є їхня складність. Окрім того, вони швидко розвиваються. Це робить їх якісно відмінними від «старих» паперових або механічних технологій і рішень.

8. Фактична хронологічна послідовність етапів може відрізнятися від наведеної вище.

2. ПЕРЕВІРКА НОВИХ ТЕХНОЛОГІЙ НА ЇХНЮ ВІДПОВІДНІСТЬ СТАТТІ 3 ПЕРШОГО ПРОТОКОЛУ ДО ЄВРОПЕЙСЬКОЇ КОНВЕНЦІЇ З ПРАВ ЛЮДИНИ

a. Перспектива з точки зору технологій

Диджиталізація (оцифровування)

Існування цифрових технологій та їх застосування майже у всіх сферах життя, включно з виборами, є фактом, який не ставлять під сумнів[9]. Диджиталізація – це перший рівень, який дозволяє обробити інформацію за допомогою комп'ютера. Це перетворення тексту, ілюстрацій, звуку в цифрову форму, яку може обробити комп'ютер.

Оцифрованими даними можуть бути списки виборців, реєстри кандидатів, результати, внесені в електронному форматі, тощо. Серед оцифрованих процесів варто згадати електронну реєстрацію, електронну ідентифікацію виборців, електронне голосування на машинах для голосування, що розташовані на виборчих дільницях, або за допомогою інтернету, електронний підрахунок голосів (тобто програмне забезпечення, яке використовують для реєстрації та підрахунку результатів, а також, можливо, і для розподілу мандатів), програмне забезпечення, яким послуговуються для статистики, електронна передача попередніх та/або остаточних результатів, наприклад, із виборчих дільниць до центрального органу тощо. Оцифровування процесів є складнішим при передаванні їх через інтернет у зв'язку з проблемами, що пов'язані з питаннями кібербезпеки. Оцифровані дані та процеси можуть бути об'єднані в системи інформації та управління виборчим процесом.

У наступні розділи ми включили інформацію із опитувальника, який було підготовлено та розповсюджено Європейським комітетом із питань демократії та врядування Ради Європи (CDDG) і на який у кінці 2019 року надало свої відповіді декілька країн. Опитувальник був коротким та зосереджувався на впровадженні Рекомендації CM/Rec(2017)5. Відповіді надавали різні установи, серед яких не обов'язково були ОУВП. Незважаючи на такі обмеження, відповіді дозволяють отримати актуальний, хоча й не вичерпний огляд цифрових технологій, які використовують у виборчих процесах.

Електронне голосування – приклад найбільш контрольованого використання нових технологій у виборчому циклі, адже воно охоплює найчутливіший процес виборчого циклу – власне голосування та підбиття підсумків виборів. Це також найсучасніший приклад використання нових технологій, оскільки зазвичай це не просто оцифрування процесів голосування та підрахунку

9. Європейська комісія Ради Європи «За демократію через право» (Венеційська комісія) та ін., 2019 р., «Спільна доповідь про цифрові технології та вибори».

голосів – при найкращій реалізації електронне голосування передбачає, що всі залучені документи й процеси оцифровують, щоб передавання даних могло відбуватися безперервно та за допомогою одного засобу передавання інформації.

Відповідно до Рекомендації CM/Rec(2017)5 електронне голосування охоплює електронне подання голосів та електронний підрахунок бюлетенів. Електронне подання голосів передбачає як голосування на електронних машинах для голосування (надалі – ЕМГ) на виборчих дільницях, так і голосування через інтернет із неконтрольованого середовища (надалі – інтернет-голосування). Електронне подання голосів передбачає їх електронний підрахунок. Існує також окремо електронний підрахунок паперових бюлетенів за допомогою оптичних сканерів, які оцифровують паперовий бюлетень, після чого здійснюється підрахунок.

Електронне голосування практикують у декількох країнах, про що свідчать відповіді на питання із опитувальника: *Бельгія* (ЕМГ для всіх видів виборів та референдумів); *Болгарія* (ЕМГ тільки для національних виборів та виборів до Європарламенту, а також виборів президента й віце-президента Республіки Болгарії, але не для референдумів); *Естонія* (інтернет-голосування на всіх національних виборах, але не для проведення місцевих референдумів, під час яких використовують інші технічні рішення); автономний регіон *Аландських островів* у *Фінляндії* (інтернет-голосування, нещодавно використання призупинено); *Франція* (ЕМГ у 66 комунах та інтернет-голосування для французьких експатів під час парламентських виборів і консульських виборів, на місцевому рівні для проведення виборів у муніципальні ради можуть використовувати інтернет-голосування); *Ісландія* та *Норвегія* (інтернет-голосування лише для місцевих референдумів); *Російська Федерація* (ЕМГ для національних і регіональних виборів); *Швейцарія* (інтернет-голосування під час проведення виборів та голосувань на федеральному рівні, а також на рівні кантонів і комун; наразі використання призупинено).

Відповіді на опитувальник CDDG свідчать про те, що виключно електронний підрахунок (технологію оптичного розпізнавання позначок) практикують в *Угорщині* (лише для попередніх результатів), *Латвії, на Мальті* (із травня 2019 року для виборів до Європейського Парламенту і місцевих рад), *Норвегії*, *Швейцарії* (деякі кантони здійснюють сканування та підрахунок паперових бюлетенів під час голосування на референдумах), *Російській Федерації*, а також у *Великобританії* (*Англія* використовує його з 2000 року на місцевих і національних виборах; *Шотландія* використовувала цю систему на місцевих та національних виборах 2007 року. Тоді ж було виявлено істотні помилки в оформленні бюлетенів. Електронний підрахунок знову використовували на місцевих виборах 2012 і 2017 років – успішно. Підрахунок виборчих бюлетенів [при системі єдиного перехідного голосу] скоротився з трьох/чотирьох днів до кількох годин).

Електронне голосування планують упровадити в *Азербайджані*, *Франції*[10], *Румунії*[11], *Сербії*[12], *Україні*[13] та у *Великобританії*[14]. Застосування цієї системи частково або повністю призупинили чи скасували в *Болгарії*[15], *Фінляндії*[16], *Франції*[17], *Німеччині*[18], *Ірландії*, *Нідерландах*[19], *Норвегії*[20], *Швейцарії*[21] та *Великобританії*[22].

Електронне голосування розглядали в контексті проведення виборів та референдумів, проте не запровадили в *Австрії*[23], *Чехії*, *Данії*, *Фінляндії*[24],

10. У доповіді Сенату Франції за 2018 рік (Deromedi, Detraigne) було рекомендовано використовувати інтернет-голосування на консульських виборах 2020 року та на парламентських виборах, що відбуватимуться у 2022 році. Нещодавно уряд Франції ухвалив рішення про використання інтернет-голосування на виборах, що відбудуться у 2020 році.

11. Постійний виборчий орган Румунії розглядає питання електронного голосування, проте, як зазначалося у наданій відповіді на опитувальник, упровадження може не розпочатися до кінця 2020 року, оскільки деякі політичні суб'єкти та адміністративні установи мають недовіру до цієї технології.

12. Можливий закон про референдум та народні ініціативи розглядає електронну ініціативу як перше випробування електронного голосування в Сербії.

13. Відповідно до наданої у відповідь на опитувальник інформації готується закон про національні та місцеві референдуми, який розглядатиме варіант запровадження електронного голосування.

14. Випробування, яке не мало правових наслідків, відбулося в травні 2019 року під час проведення місцевих виборів. Стверджується, що було використано безперервну надійну систему, яка передбачала використання комп'ютера із сенсорним екраном у кабіні для голосування, кодів, виданих виборцям, паперових квитанцій, які підтверджували особу виборця, оприлюднення зашифрованих голосів на сайті виборів, системи, що повідомляє про будь-яке неправомірне втручання в процес електронного голосування. Випробування здійснювали в контексті інших ініціатив, зокрема, коли уряди Уельсу та Шотландії запропонували проведення пілотного електронного голосування на місцевих виборах.

15. У 2019 році парламент Болгарії скасував застосування електронного голосування на місцевих виборах у зв'язку зі складністю проведення таких виборів та значними фінансовими витратами на здійснення електронного голосування.

16. Таке голосування відмінили після випробування, здійсненого під час виборів до муніципалітетів у 2008 році, а також виявлених на той момент проблем.

17. Починаючи з 2008 року, заборона припиняє будь-яке застосування ЕМГ у нових комунах. На останніх національних виборах інтернет-голосування було скасовано. Однак, як очікують, його застосують у 2020 та 2022 роках, як це було рекомендовано в доповіді Сенату за 2018 рік.

18. Рішення Федерального конституційного суду від 3 березня 2009 року (BVerfGE 123, 39) визнало Указ про федеральну машину для проведення голосування (*Bundeswahlgeräteverordnung від 3 вересня 1975 року, BGBl. 1975 I 2459, у редакції відповідно до статті 1 Указу від 20 квітня 1999 року, BGBl. 1999 I 749*) як такий, що є несумісним із принципом публічного характеру виборів, згідно з яким пересічна особа повинна мати можливість стежити за основними кроками виборчого процесу та розуміти їх без спеціальних технічних знань.

19. У 2006 році, після десятиліть застосування електронного голосування, використання ЕМГ у Нідерландах зазнало нищівної критики внаслідок відсутності безпеки та неможливості проведення аудиту. Із 2008 року голосування проводять за допомогою лише паперових бюлетенів.

20. Після проведення випробувань у 2011 та 2013 роках у 10 та 12 муніципалітетах відповідно уряд Норвегії припинив застосовувати інтернет-голосування через брак політичної волі для використання його як постійного методу голосування. Його використання можливе лише під час проведення місцевих референдумів.

21. Використання інтернет-голосування у Швейцарії було *фактично* припинене із середини 2019 року, оскільки жодна система інтернет-голосування не відповідала вимогам законодавства.

22. Після випробувань на місцевих виборах в Англії у період між 2002 та 2007 роками використання електронного голосування було припинене головним чином через проблеми зі складністю й питаннями прозорості; ризики було визнано більшими за переваги, а також не вистачало чіткого бачення, стратегії, ефективного планування, розуміння економічної ефективності та сертифікації системи.

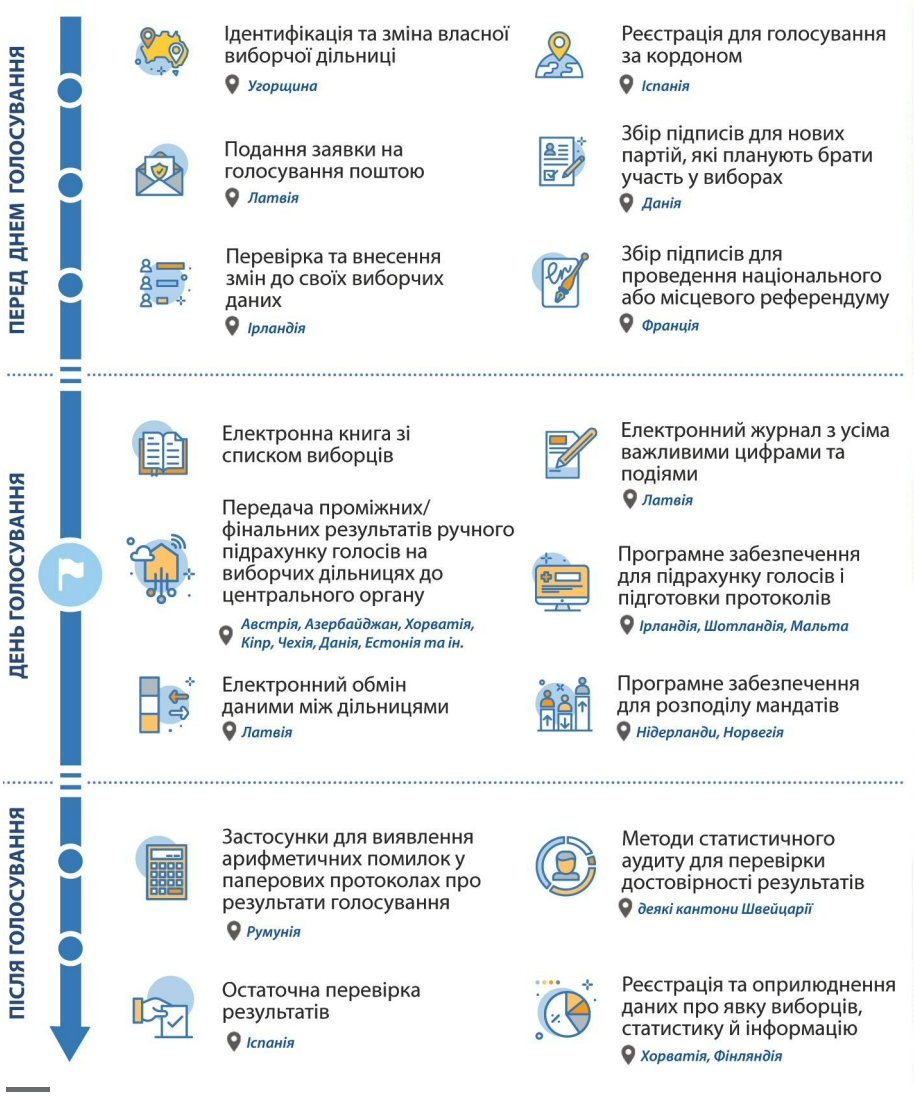
23. Рішенням конституційного суду в 2011 році було встановлено, що виборча комісія повинна розуміти всі кроки та процедури інтернет-голосування без допомоги технічних експертів, чого досягти на практиці неможливо.

24. У доповіді, оприлюдненій наприкінці 2017 року, зазначено, що ризики інтернет-голосування станом на той час перевищували переваги.

Латвії[25], *Іспанії*[26]. Основні аргументи проти запровадження електронного голосування стосуються питань безпеки, складності та великих витрат.

Однак оцифрування документів та процесів виборчого циклу є поширеним явищем. Нижче наведено огляд, що ґрунтується на відповідях на опитувальник CDDG, наданих наприкінці 2019 року.

Приклади цифрових процесів та послуг, що використовуються у виборчому циклі



25. Згідно з відповідями на опитувальник, деякі обговорення в парламенті свідчать про те, що питання про запровадження інтернет-голосування знову переглядають, хоча ця думка не знаходить великої кількості прихильників.

26. Інтернет-голосування обговорювали лише для іспанців, які проживають за кордоном.

Згідно з представленою інформацією основні дані та процеси оцифровують у *Фінляндії, Угорщині, Латвії* (скажімо, виборчі округи, муніципалітети, виборчі дільниці, виборчі органи, підготовка та оприлюднення списків кандидатів, підготовка макетів бюлетенів).

Оцифровані послуги або процеси, до яких вдаються перед днем голосування, охоплюють електронні послуги для виборців, які допомагають знайти та змінити свою виборчу дільницю (*Угорщина*), подати заявку на голосування поштою (*Латвія*), перевірити та внести зміни до своїх виборчих даних (*Ірландія*) або зареєструватися для голосування за кордоном (*Іспанія*); провести збір підписів для нових партій, які бажають балотуватися на вибори (*Данія*[27]); провести збір підписів для проведення національних або місцевих референдумів (*Франція*).

Серед оцифрованих послуг або процесів, доступних у день голосування і після нього (окрім будь-яких різновидів електронного голосування), трапляються: електронний *журнал* з усіма важливими цифрами та подіями (*Латвія*); електронна книга зі списком виборців; електронний обмін даними між виборчими дільницями, що забезпечує для виборців можливість голосувати на будь-якій дільниці упродовж днів проведення дострокового голосування (*Латвія*[28]); передача попередніх та/або остаточних результатів голосування після ручного підрахунку на виборчих дільницях до центральних структур, де такі результати об'єднують, підраховують та публікують залежно від обставин (*Австрія, Азербайджан, Хорватія, Кіпр, Чехія, Данія, Естонія, Фінляндія, Греція, Німеччина, Угорщина, Латвія, Норвегія, Румунія, Словаччина, Словенія, Іспанія, Нідерланди*); програмне забезпечення, що допомагає уповноваженим із виборів із підрахунком голосів і підготовкою протоколів відповідно до системи пропорційного представництва – єдиного перехідного голосу (PR-STV) (*Ірландія*, *Шотландія, Мальта*); програмне забезпечення для розподілу мандатів (*Нідерланди*, *Норвегія* та ін.).

Важливим типом оцифрованих документів, які використовують майже скрізь у регіоні, є реєстри: реєстри виборців та кандидатів, реєстри, які ведуть облік тих, хто вже проголосував під час виборів (скористалися своїми виборчими правами). Окрім країн з *електронним поданням голосу*, їх також використовують у *Фінляндії*, *Угорщині*, *Латвії*, *Норвегії*, *Сербії*, *Словенії*.

Оцифровані послуги або процеси, доступні після дня голосування, охоплюють рішення для *перевірки* результатів, включно з додатками, що ідентифікують арифметичні помилки щодо даних, записаних у паперових протоколах виборів (*Румунія*[29]); методи статистичного аудиту для перевірки достовірності

27. Після початкових випробувань та виявлених проблем парламент Данії вирішив у 2019 році замовити оновлену систему.

28. У Латвії пілотний проєкт відбувся на виборах до Європейського Парламенту у 2019 році.

29. Застосунок сигналізує про будь-яку невідповідність між результатами; як запобіжний захід, програмне забезпечення може не допускати негайної передачі даних тоді, коли цифри не збігаються, як це відбувається в Румунії.

результатів; остаточну перевірку результатів (*Іспанія*[30]); реєстрацію та оприлюднення даних про явку виборців, статистику й інформацію (зокрема у *Хорватії* чи *Фінляндії*).

Про плани розширити використання цифрових рішень у виборчому циклі повідомляють у кількох країнах, а саме в *Данії*, де очікують упровадження системи управління виборами у 2020 році; у *Франції*, де передбачено збирання електронних підписів для проведення референдумів; у *Фінляндії*, де заплановано запровадити виборчу інформаційну систему (EIS); в *Ірландії*, де триває модернізація виборчого реєстру та досліджується робота загальнонаціональної системи реєстрації в мережі; у *Латвії*, де є намір запровадити електронний список виборців для виборчих дільниць на наступних муніципальних і парламентських виборах, щоб дати можливість голосувати на будь-якій із них у день виборів. У цих випадках необхідним є запровадження правових змін.

Відповідність рішень щодо електронного голосування національним принципам демократичних виборів (національні норми спираються на міжнародні стандарти, встановлені у статті 25 МПГПП та статті 3 першого Протоколу до Європейської конвенції з прав людини) розглянули вищі суди, зокрема, таких країн, як *Німеччина*, *Австрія*, *Естонія*, *Швейцарія*, *Франція*[31]. Занепокоєння щодо іноземного втручання у вибори останнім часом спонукало до більш детального контролю безпеки (і відповідності міжнародним принципам, нормам та стандартам) інших цифрових рішень, ніж електронне голосування, що використовуються у виборчих процесах, зокрема щодо реєстрів виборців та процедури реєстрації чи систем передачі або підрахунку результатів – саме так було в *Німеччині* та *Нідерландах* у 2017 році.

Під час процесів оцифрування першочергове питання полягає в тому, як повинен виглядати оцифрований процес: чи має він імітувати традиційний паперовий процес, чи може впроваджувати нові революційні функції, які необхідні для відповідності принципам демократичних виборів та які стають можливими завдяки новій технології? Наразі імітація переважає. Так, із точки зору рівного волевиявлення метод електронного голосування не може запропонувати виборцям додаткових або інших можливостей, аніж традиційний метод (див. стандарт 5 Рекомендації CM/Rec(2017)5). Однак було й використано іншу логіку, орієнтовану на досягнення цілей, а не на досягнення формальної рівності між рішеннями, що ґрунтуються на різних технологіях, та й виглядає такий підхід більш доцільним. Основну увагу зосереджено на принципах, яких потрібно дотримуватися та які необхідно застосовувати, а також враховано особливості використовуваної технології. Наприклад, специфічні вразливості та загрози, пов'язані з електронним голосуванням,

30. Через три дні після виборів проводять остаточну перевірку голосів шляхом перерахунку паперових бюлетенів, які надсилає кожна дільниця, – у цьому випадку виборчим комісіям допомагають комп'ютерні застосунки, що полегшують роботу.

31. У контексті міжнародного порівняльного аналізу див.: Driza Maurer, Barrat (Eds.), *E-Voting Case Law – A Comparative Analysis*, Routledge, 2015, 2017. Окрім аналізу ситуації в згаданих європейських країнах, також розглянуто судову практику в Індії, Бразилії, Мексиці, США, Австралії, Аргентині та Венесуелі.

потребують запровадження індивідуальної й універсальної перевірки з метою забезпечення дотримання принципу вільного волевиявлення (див. стандарт 15 і наступні стандарти Рекомендації CM/Rec(2017)5). Так, індивідуальна перевірка електронного голосування надає можливість виборцю перевірити власний голос, що є абсолютно новою рисою, відсутньою при голосуванні з використанням паперових бюлетенів. Також багаторазове голосування дозволене спеціально для інтернет-виборців (у деяких країнах) із метою протидії ризику сімейного голосування, який існує в разі застосування будь-яких віддалених голосувань, включно з голосуванням через інтернет. Іншим прикладом є специфічна структура системи електронного голосування, яка дозволяє, наскільки це можливо, людям з інвалідністю та особливими потребами голосувати самостійно. Ще одна вимога – система електронного голосування повинна сповістити виборця в тому випадку, якщо він/вона подає недійсний голос (стандарт 14 Рекомендації CM/Rec(2017)5). Знову ж таки ця можливість відсутня при паперовому голосуванні: у цьому випадку електронне голосування має перевагу, яка дозволяє краще забезпечити право на вільне волевиявлення.

Врешті, оцифрування документів та процесів відіграє важливу роль у підтримці виборів у багатьох країнах Ради Європи, забезпечуючи прискорену та єдину обробку даних. Кожен етап виборчого циклу стає легшим унаслідок застосування цифрових інструментів. Їхнє впровадження та розширення є безперервним і може стати підґрунтям для подальшого впровадження інших нових технологій.

Біометрія

Біометрія надає можливість фіксувати та зберігати в електронному форматі деякі фізичні характеристики (райдужна оболонка, відбитки пальців, зображення обличчя тощо), які повинні забезпечувати унікальну ідентифікацію людини. Традиційно унікальна ідентифікація забезпечується процедурними правилами та ґрунтується на реєстрі виборців. Виборчі списки поповнюються біометричними даними виборців задля забезпечення унікальної ідентифікації виборців та запобіганню багаторазовому голосуванню. У день виборів біометричні характеристики виборців фіксують та порівнюють із біометричною інформацією, яка зберігається в базах даних. Біометрію на виборах застосовують здебільшого в країнах Південної Америки чи Африки. Окрім незначних винятків, країни Ради Європи не використовують біометрію під час виборів. Захист даних, таємниця голосування, а також позбавлення виборців права на голосування внаслідок помилок у біометричній ідентифікації (помилкове прийняття та помилкова відмова) є одними з основних причин того, що біометрію досі не використовують на виборах у Європі. У доповіді Сенату Франції 2018 року запропоновано розглянути можливість здійснення унікальної ідентифікації виборців шляхом використання біометрії.

Використання біометрії на виборах викликає питання дотримання статті 3 першого Протоколу до Європейської конвенції з прав людини. Наскільки

унікальними та незмінними є біометричні дані для забезпечення виборчого права з часом? Чи легко та швидко збирати біометричну інформацію та засвідчувати аутентифікацію виборця під час голосування? Чи прийнятні для виборців збирання та використання таких даних? Необхідно гарантувати безпечне зберігання даних (захист секретності) та безпеку системи.

Блокчейн

Блокчейн – це незмінний ланцюг записів даних, що має певну часову позначку та розподіляється і керується кластером комп'ютерів. Основними його характеристиками є децентралізація, прозорість та незмінність[32]. Операції записують на багатьох комп'ютерах, а тому будь-який відповідний запис не можна змінювати заднім числом без зміни всіх подальших блоків.

На місцевому рівні було проведено декілька голосувань із застосуванням блокчейну[33]. Блокчейн-голосування «заявляє» багато переваг порівняно з традиційними централізованими паперовими системами голосування. Однак більшість його властивостей (як-от електронна ідентифікація, цифрові підписи для гарантії цілісності даних, сильна криптографія, перевірка виборців, можливість багаторазового голосування) не виняткові для блокчейну і наявні також у «традиційному» електронному голосуванні, яке можна перевірити. Блокчейн-голосування запроваджує щонайменше одну специфічну особливість: будь-яка інформація, яку обробляють за допомогою обчислювальної техніки або зберігання даних, розподіляється між кількома вузлами (децентралізація). У децентралізованій системі голосування результат голосування кожної особи надсилається певній кількості суб'єктів, і всі вони мають отримати однакові дані – лише за цієї умови голос буде записано. Це означає, що немає жодного утворення, яке контролює процес: мова йде не лише про організатора голосування, ОУВП, який затверджує голос, але й про інші різні акредитовані установи (такі як Рада Європи, політичні партії чи місцеві ради). Така особливість надає перевагу захисту від внутрішньої загрози: як стверджується, навіть корумпований уряд не зможе підробити голоси. Після того як голос записано, його не можна видалити або змінити, оскільки блокчейн-ланцюги непорушні. Якщо вузлів (у кластері) достатньо, стверджується, що система захищена від зламу. Особистість виборця анонімізована, голосування нібито таємне. Таке твердження викликає сумніви, оскільки ідентифікація особи можлива через відстеження та використання інформації про публічну адресу та IP-адреси. Інші питання стосуються сумісності, витрат тощо.

Блокчейн усе частіше використовують для процесів, коли потрібні незмінні, постійні та пошукові записи чи транзакції, контракти й офіційні документи. Адміністрації, які впроваджують блокчейн, послуговуються ним для офіційних

32. Blockchain / Wikipedia (https://en.wikipedia.org/wiki/Blockchain).

33. Наприклад, місто Цуг у Швейцарії упродовж 25 червня – 1 липня 2018 року провело пробне інтернет-голосування із застосуванням блокчейну. Див. оцінювання: http://www.stadtzug.ch/dl.php/de/5c00ff8dbd830/eVoting_Final_Report_ENG.pdf.

земельних реєстрів, для проведення офіційних транзакцій тощо. Можна передбачити, що адміністрації можуть спокуситися використовувати його й у виборчому циклі, скажімо, для ведення реєстрів виборців, партій тощо. Отже, якщо цивільний реєстр ґрунтується на блокчейні, то «витягнутий» із нього виборчий реєстр, імовірно, потрібно буде вести так само. Запровадження блокчейну для обробки одного елемента виборчого циклу може вплинути на весь виборчий цикл.

У зв'язку з блокчейном постає декілька питань щодо відповідності статті 3 першого Протоколу до Європейської конвенції з прав людини, зокрема, щодо таємниці голосування (оскільки дані, розміщені в блокчейні, залишаються в ньому), неприйнятності оприлюднення проміжних результатів (оскільки кількість голосів за кожного кандидата відома до моменту завершення голосування), щодо безпеки, зручності у користуванні (оскільки для завершення транзакції або голосування потребується певний час), дотримання принципу «один виборець – один голос» (оскільки обчислювальна потужність важлива для прийняття рішень у блокчейні) тощо.

Хмарні обчислення

Хмарні обчислення – це забезпечення доступу на вимогу до ресурсів комп'ютерної системи, зокрема, для зберігання даних та використання обчислювальної потужності, без безпосереднього активного управління з боку користувача. Термін зазвичай використовують для опису центрів обробки даних (дата-центрів), доступних багатьом користувачам мережі Інтернет[34]. Існують як публічні, так і приватні хмари.

34. Cloud computing / Wikipedia (https://en.wikipedia.org/wiki/Cloud_computing).

Організації, як і бізнес, планують перенести або вже перенесли свої IT-служби в хмару, оскільки існує переконання, що це дешевше і безпечніше, ніж підтримка власних потужностей. Це складно, якщо йдеться про такі критичні системи, як вибори, де органи влади повинні здійснювати управління, а також бажано – відповідно до сьогоднішнього уявлення про ці процеси – володіти IT-навичками й власними IT-рішеннями.

Хмара може стати причиною появи нових вразливостей у виборчій системі; скажімо, це стосується безпеки конфіденційних документів та процесів, секретності й конфіденційності, підзвітності чи сумісності (тобто можливості забрати дані з хмари або перенести їх в іншу хмару), а також багатьох загроз атак, у той час як розслідування порушень та проведення криміналістичних експертиз стають складнішими. Використання хмарних обчислень для документів та процесів виборчого циклу раніше не ставало об'єктом детальної уваги. Їхнє фактичне використання та супутні питання щодо відповідності (секретність, безпека, сумісність тощо) потребують подальшого дослідження.

Штучний інтелект

Штучний інтелект (ШІ) стосується широкого спектра методів – як існуючих, так і абстрактно теоретичних[35]. Ідеться про системи, які демонструють інтелектуальну поведінку, аналізуючи своє оточення та вчиняючи дії – із певним ступенем самостійності – для досягнення конкретних цілей[36]. Сфера ШІ спирається на багато інших сфер. Традиційні цілі дослідження ШІ охоплюють обґрунтування та прийняття рішень (представлення знань, планування, створення графіка, пошук, оптимізація), навчання (машинне навчання, нейронні мережі, глибоке навчання, дерева рішень тощо) та робототехніку (вбудований ШІ, здатність рухатись і взаємодіяти із фізичним світом). На сьогодні рішення ШІ специфічні для кожної окремої сфери.

Штучний інтелект може мати вплив на нові технологічні рішення, які застосовують у виборах. Наприклад, потенційно його використовуватимуть для проведення кібератак, адже передбачити його буде ще складніше й важче, ніж зараз, враховуючи його «окрім іншого, більшу спроможність переслідувати цілі, які з високою точністю підлаштовані під користувача, та адаптуватись у режимі реального часу»[37]. ОУВП повинні серйозно на це зважати. Водночас також очікується, що ШІ навчатимуть та використовуватимуть для кіберзахисту. Використання ШІ також можна передбачити в навчанні та освіті або в питаннях вирішення спорів. Це може бути цікаво в контексті добування та пошуку інформації.

---

35. Європейська парламентська служба досліджень (2019) «Як працює штучний інтелект», «Чому штучний інтелект важливий». Див. також: Artificial intelligence / Wikipedia (https://en.wikipedia.org/wiki/Artificial_intelligence).

36. Європейська комісія, незалежна Експертна група високого рівня з питань штучного інтелекту, «Визначення штучного інтелекту: основні можливості та напрями», 8 квітня 2019 року.

37. Доповідь групи експертів високого рівня ООН, *Епоха цифрової взаємозалежності*, червень 2019 року.

До основних питань, пов'язаних зі штучним інтелектом, належать питання даних та можливість пояснення. Системам ШІ потрібно обробити багато даних, щоб вони були ефективними й такої самої якості, як і дані, які їм надають. Якщо дані, за якими буде здійснюватися навчання ШІ, будуть упередженими (наприклад, недостатньо інклюзивними), то й ШІ навчатиметься з відповідним упередженням, а його рішення будуть несправедливими. Однак є одне важливе застереження: принцип відкритих даних не поширюється на всі види даних, які збирають на виборах, що ускладнює розробку рішень ШІ для виборів. Насправді все якраз навпаки, адже, наприклад, детальна інформація про участь та зміст голосування захищаються вимогою таємниці голосування. Можливість пояснення стосується непрозорого характеру деяких систем ШІ: навіть інженери, які створюють ці системи, не можуть зрозуміти, як вони приймають рішення. Зростає національне та міжнародне розуміння того, що системи ШІ потрібно розробляти так, аби їхні рішення можна було пояснити, а люди залишались відповідальними[38].

б. Перспектива з точки зору виборчого циклу

I. Нормативно-правова база

Ця частина виборчого циклу охоплює розробку та підготовку законодавства і регулювання виборів на всіх рівнях влади за допомогою усіх типів актів/документів, включно з процесуальним та матеріальним правом і навіть кодексами належної поведінки та іншими інструментами, які можуть мати безпосередній чи опосередкований вплив на вибори. Не всі ці елементи ініціюють або розробляють ОУВП, тому також важливо, аби ОУВП мали належне розуміння та оцінку всіх регуляторних елементів, які варто враховувати у виборчому циклі. Тут можуть допомогти нові технології, якщо, наприклад, потрібно підготувати, організувати та віднайти інформацію.

Інший аспект цього питання полягає в тому, що законодавство має регулювати використання нових технологій у виборчому циклі. Сьогодні, як виявилося, складно писати положення, які відповідають принципам вищого рівня, про що свідчать рішення конституційних судів Німеччини та Австрії щодо такої відповідності правил електронного голосування. Незрозуміло, як можна застосувати правові принципи до нових технологій і яким повинен бути зміст відповідного регулювання. Такі принципи, як законність чи правова визначеність виборчого закону, постають перед викликом через складність нових технологій та їхній швидкий розвиток.

Одна зі складностей стосується концепцій, зміст, обсяг та застосування яких у цифровому світі можуть відрізнятися порівняно з аналоговим. Так, в аналоговому світі виборча безпека та контроль розглядається досить

38. Рекомендація 3С Доповіді групи експертів високого рівня ООН, *Епоха цифрової взаємозалежності*, червень 2019 року; *закон США про алгоритмічну відповідальність від 2019 року*; Урядова стратегія Німеччини Künstliche Intelligenz der Bundesregierung, листопад 2018 року; доповідь Седріка Віллані (Франція) *За змістовний штучний інтелект. Назустріч французькій та європейській стратегії*, березень 2018 року.

статично – як чітко визначені продукти та процеси, тоді як у цифровому контексті вони повинні розвиватися щодня, аби реагувати на вразливості та загрози, що постійно оновлюються, і мати змогу протистояти новим ризикам. Деякі порівнюють такий процес із гонкою озброєнь. Цей аспект потрібно відображати в регулюванні, але як? Для прикладу, в аналоговому світі ОУВП відповідають за безпеку, крім настання виняткових випадків, таких як форс-мажор. Як визначити їхню відповідальність у цифровому контексті? У низькотехнологічних контекстах встановити форс-мажор нескладно. Чи прийнятними є ризики в програмному забезпеченні (з посиланням на ШІ)? Зважаючи на те, що нові технології розвиваються шляхом спроб та помилок, що саме повинен забезпечувати ОУВП, тобто які позитивні зобов'язання постають у контексті завдання ОУВП забезпечувати відповідність виборчого процесу статті 3 першого Протоколу до Європейської конвенції з прав людини упродовж виборчого циклу?

Відповіді на ці запитання зовсім не прості та буденні. Конституційні суди (як-от у Німеччині та Австрії), парламенти, урядові та наглядові організації (наприклад у Нідерландах, Норвегії чи Франції) визнали недоліки наявних норм щодо, скажімо, електронного голосування. Розроблені в 70-х, 80-х та 90-х роках минулого століття норми повинні розвиватися для того, щоб враховувати новітні технології. У кількох випадках регулятор оновив їх або запровадив нові (Бельгія, Естонія, Швейцарія). Їхню відповідність міжнародним принципам, нормам та стандартам перевіряють на практиці, й виявляється, що такі норми повинні продовжувати розвиватися (наприклад, перевірка прозорості під час інтернет-голосування в 2019 році у Швейцарії та відповідні висновки/засвоєні уроки щодо можливості перевірки, прозорості й сертифікації)[39]. Рекомендація Комітету Міністрів Ради Європи CM/Rec(2017)5 була важливою для країн у їхніх регуляторних зусиллях щодо електронного голосування. Питання, які виникли нещодавно, ще не були детально обговорені, зокрема, такі як: контроль механізмів перевірки голосів; оцінка припущень щодо довіри, що обов'язково присутні при електронному голосуванні, яке можна перевірити; подальші заходи щодо забезпечення прозорості (наприклад, що відбувається після оприлюднення вихідного коду) тощо.

З усіх нових технологій, які використовують у виборчому циклі, електронне голосування було об'єктом найбільшої уваги з регуляторної точки зору. Інші цифрові рішення, які використовують у виборчому циклі, регулюються – у кращому разі – лише з точки зору управління інформаційними технологіями. Спроби ОУВП запровадити/вдосконалити такі норми часто наражаються на спротив[40]. Однак усе змінюється – зокрема, після популяризації теми втручання

39. Driza Maurer, Ardita (2019), *The Swiss Post/Scytl Transparency Exercise and Its Possible Impact on Internet Voting Regulation*, in R. Krimmer et al. (Eds.): E-Vote-ID 2019, LNCS 11759, с. 83-99, 2019 (*Дріза Маурер А.*: Вправа на прозорість швейцарської пошти/Scytl та її можливий вплив на регулювання інтернет-голосування. За ред. Р. Кріммер та ін.: E-Vote-ID 2019)

40. Прикладом може слугувати дискусія про федеральне регулювання рішень електронного підрахунку голосів у Швейцарії та початкову стриманість, зокрема кантонів, які відповідають за впровадження, управління та моніторинг цих рішень.

іноземних країн у президентські вибори у США 2016 року та підозри щодо зламу деяких технічних рішень, що базувалися на використанні цифрових технологій. Останні приклади виборів 2017 року в Нідерландах (програмне забезпечення для підрахунку та зведення результатів) і Німеччині (програмне забезпечення для передачі результатів) свідчать про те, що життєво важливі для результатів виборів процеси зіштовхуються з викликами, подібними до тих, які постають під час електронного голосування, і їх варто краще регулювати. Потрібно якісніше дослідити їхню відповідність статті 3 першого Протоколу до Європейської конвенції з прав людини та національним виборчим принципам.

Відповідність статті 3 першого Протоколу до Європейської конвенції з прав людини передбачає, що цифрові рішення також потрібно впроваджувати/використовувати за дотримання певних умов, серед яких, зокрема: поступове впровадження нових технологій, підзвітність (сертифікація, аудит), розподіл відповідальності, прозорість та можливість спостереження, надійність, безпека та сумісність. Відповіді на опитувальник CDDG засвідчують, що країни підтримують рекомендації Ради Європи. Так, Рекомендацію CM/Rec(2017)5 щодо електронного голосування вважають важливою для країн, зокрема й тих, які дозволяють проводити електронне подання голосу (Бельгія, Естонія та Швейцарія), та тих, хто практикує виключно електронний підрахунок голосів (Чехія, Данія чи Угорщина). У відповідях країн зроблено акцент на необхідності подальшого обговорення на регіональному рівні питань кібербезпеки виборів, верифікації голосу, цифрової ідентичності, процедур на випадок надзвичайних ситуацій у разі переривання зв'язку, а також підкреслено, що таким питанням належить приділяти більше уваги на регуляторному рівні.

II. Планування та підготовка

ОУВП здійснює нагляд за детальними етапами виборчого циклу: календар виборів, підбір та навчання персоналу, логістика та безпека, національна або регіональна виборча політика, виборчі служби, закупівлі для аутсорсингових послуг, набір та підготовка працівників на виборах тощо. Для цього використовують IT-підтримку, адаптовану до таких потреб.

Основне питання тут полягає в тому, наскільки ці рішення є стійкими до зламу (безпека), наскільки від них залежать процеси виборчого циклу та чи передбачено резервні рішення.

III. Навчання та освіта

ОУВП зазвичай проводить просвітницькі та освітні заходи для виборців та громадян. Цей орган підтримує доступ для всіх, сприяє політиці та практиці рівності й справедливості, може надавати засоби для проведення виборчих досліджень. Окрім підтримки виборців, він наймає та тренує тимчасових працівників для проведення виборів. ОУВП забезпечує акредитацію спостерігачів та регламентує їхню діяльність. Орган здійснює підготовку спостерігачів політичних партій та кандидатів. Діяльність ОУВП охоплює і роботу з засобами масової інформації: ОУВП забезпечує доступ ЗМІ, регулює

поведінку засобів масової інформації під час виборів, регулює опитування громадської думки.

Для підтримки вищезазначеної діяльності використовують ІТ. Ті самі питання, які було визначено для етапу планування та підготовки, застосовуються і тут.

IV. Реєстрація

У підпункті про диджиталізацію було згадано про те, що зазвичай існує два типи реєстрів: виборчі, або реєстри виборців, та реєстри партій. Під час голосування також реєструються використання виборчого права (факт того, що людина проголосувала). Усі ці реєстри оцифровані, ймовірно, в усіх країнах Ради Європи.

Реєстри виборців включають виборців, які проживають у країні, виборців, які проживають за кордоном та мають право голосу, а в деяких випадках й іноземці, які перебувають у країні на законних підставах. ОУВП також реєструє політичні сили (партії, рухи тощо). Перед кожними виборами він отримує заявки та затверджує висунення кандидатів. Окрім того, він може контролювати попередній відбір або праймериз у політичних партіях.

У контексті дотримання статті 3 першого Протоколу до Європейської конвенції з прав людини постає питання, яке стосується усіх реєстрів, – унікальна ідентифікація осіб, тобто виборців та кандидатів. Мета унікальної ідентифікації полягає в забезпеченні рівного волевиявлення (одна людина – один голос), а також у дотриманні виборчих правил щодо можливості висунення. В аналогових паперових системах осіб визначають вручну: процедура громіздка й передбачає високу ймовірність помилок під час перевірки. У цифровому світі рішення, що базуються на використанні цифрових технологій, пропонують такі переваги, як швидка перевірка даних та ефективне запобігання багаторазовому голосуванню чи багаторазовому висуванню на виборах. Рішенням, що обговорюється, є унікальна електронна ідентифікація. Естонія використовує електронні посвідчення особи для аутентифікації виборців. У деяких країнах, де не використовуються електронні посвідчення особи, намагаються використовувати альтернативні унікальні ідентифікатори, такі як номери соціального страхування, наприклад, для ідентифікації кандидатів. Спочатку таким ініціативам жорстоко чинили опір наглядові організації у сфері захисту даних. Турбота про захист даних переважала над повагою до виборчих принципів (правила щодо висування або «одна людина – один голос»). Зовсім нещодавно наглядові організації у сфері захисту даних почали приймати таке використання даних. Водночас електронні посвідчення особи стають усе більш поширеними. Очевидно, вони полегшують різні операції у всіх сферах життя. Питання таємниці голосування та участі у голосуванні лишається важливим, і його потрібно уважно розглядати, оскільки використання електронних посвідчень особи та інших засобів електронної ідентифікації стає буденною практикою.

V. Виборча агітація

Використання нових технологій у виборчій агітації стосується переважно формування думки. Як уже було згадано раніше, використання нових технологій із метою формування думки виходить за межі окресленого в цьому дослідженні кола питань.

VI. Операції з голосуванням

Цей етап стосується виборчого процесу – від відкриття до закриття голосування та подальшого підрахунку, перевірки й оприлюднення результатів. Під час цього етапу можна використовувати декілька цифрових рішень, включно з електронною ідентифікацією виборців, електронним голосуванням, електронним підрахунком, електронною передачею результатів. Питання відповідності було обговорено вище (див. «Диджиталізація (оцифровування)»).

VII. Результати виборів

Окрім збирання, підрахунку та оприлюднення результатів (див. вище), ОУВП використовують цифрові рішення і для проведення аудиту та перевірки правильності результатів. Існують інструменти, які перевіряють достовірність результатів, тобто виявляють виборчі невідповідності за допомогою статистичних методів[41]. Статистичні методи оцінюють вірогідність правильності результатів, ґрунтуючись на даних попередніх виборів. Для послугування такими методами потрібно мати дані з поточних та попередніх виборів. Що стосується ШІ, то якість та кількість таких даних мають вирішальне значення для оптимального функціонування цих методів.

ОУВП можуть також діяти як органи вирішення спорів. Цифрові рішення можна використовувати для отримання та обробки інформації. Тут не йдеться про прогнозоване правосуддя, проте такі інструменти можуть бути цікавими та допомагати ОУВП приймати правильні та швидкі рішення. Їх також можна використати для того, щоб допомогти виборцям краще розуміти свої права та знати, як їх захистити, що врешті покращить доступ до правосуддя для учасників процесу, що мають скарги (виборців, партій тощо). У всіх цих випадках важливо звернути увагу на відповідність рішення вільному та таємному волевиявленню і праву на ефективну систему оскарження.

VIII. Післявиборчі обов'язки

Такі обов'язки передбачають видалення або архівування даних про вибори, роботу над оновленням інформації та інструментів, перегляд та оцінку належності виборчої нормативно-правової бази та ефективності діяльності ОУВП, а також консультування уряду й органів законодавчої влади з питань виборчої реформи. Ті самі зауваження, які пов'язані з плануванням та підготовкою, стосуються і цифрових інструментів, якими послуговуються тут. Окрім того, потрібно дотримуватися таємниці голосування та участі у голосуванні.

41. Європейська комісія Ради Європи «За демократію через право» (Венеційська комісія), 2018 рік, «Доповідь про виявлення виборчих порушень за допомогою використання статистичних методів», CDL-AD(2018)009.

3. ПІДСУМКИ ТА НАСКРІЗНІ ПИТАННЯ

Цей короткий огляд свідчить про те, що найбільш поширеною і необхідною технологією є диджиталізація. Вона становить основу для будь-якої іншої нової технології, наприклад, біометрії, блокчейну, хмарних обчислень або штучного інтелекту.

Важливо, щоб цифрові рішення, які використовують у виборчому циклі, відповідали принципам та умовам демократичних виборів. Питання щодо електронного голосування було розглянуто досить глибоко. Відповідність міжнародним принципам, нормам та стандартам інших ніж електронне голосування цифрових рішень, які застосовують у виборчому циклі, наразі лишається без достатньої уваги. Останні результати свідчать про те, що використання таких рішень повинно бути ретельно сплановане та регламентоване. Вимоги щодо конфіденційних документів та процесів можуть бути узгоджені з вимогами Рекомендації CM/Rec(2017)5 щодо електронного голосування.

Деякі питання є наскрізними: вони стосуються всіх цифрових технологій та всіх етапів виборчого циклу. Такі питання пов'язані з кібербезпекою, захистом даних, процедурами щодо надзвичайних ситуацій або випадками державно-приватного співробітництва. Наявні інструменти Ради Європи вже регулюють ці питання. Однак вибори – окремий випадок, до якого можна застосовувати більш жорсткі вимоги, наприклад, щодо захисту даних або кібербезпеки. Відповіді країн на опитувальник CDDG свідчать про те, що робота на регіональному рівні необхідна – особливо у питаннях кібербезпеки, верифікації голосу, цифрової ідентичності та процедур надзвичайних ситуацій у разі переривання зв'язку.

Захист даних – це дійсно наскрізне питання. Захист даних регулюється Модернізованою Конвенцією Ради Європи про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108+). На рівні ЄС основним правовим інструментом є Регламент (ЄС) 2016/679 – Загальний регламент про захист даних (GDPR). Конвенцію 108+ та GDPR розробляли паралельно, і вони узгоджені між собою. GDPR посилює деякі принципи Конвенції 108+. Дані, які використовують на виборах або які пов'язані з політичною думкою, є перевіреними даними, обробку яких потрібно дозволяти лише тоді, коли відповідні гарантії передбачено на законодавчому рівні (стаття 6 Конвенції 108+). Однак органам, що відповідають за вибори, не зовсім зрозуміло, як саме повинні виглядати відповідні гарантії/запобіжні заходи. Варто враховувати взаємозв'язок між різними інструментами та специфікою виборчого процесу. У цьому випадку необхідні сукупні експертні знання: наприклад, використання криптографії може бути важливим заходом для захисту деяких із цих даних.

Ще одним наскрізним питанням є кібербезпека. Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) регулює важливий аспект кібербезпеки, а саме співпрацю між країнами в контексті переслідування правопорушень, спрямованих проти вільних, чесних виборів без порушень. Інші аспекти регулюються на національному рівні, наприклад, положеннями про кібербезпеку об'єктів критичної інфраструктури. Вибори кваліфікують як критично важливу інфраструктуру. Їх безпека – особливо важлива. Аналогічно важливим є планування протидії атакам (викривлення даних, переривання обслуговування тощо). Приклади органів влади, роботу яких було порушено, наприклад, через вірус-вимагач (Балтимор, травень 2018 року), демонструють, що щось може піти не так на виборах і критично важливі процеси можуть стати мішенню політичних чи фінансово мотивованих хакерів тощо.

Державно-приватне співробітництво – ще одне важливе наскрізне питання, оскільки цифрові рішення та їх контроль здебільшого забезпечує приватний сектор. Умови закупівлі повинні відображати вимоги, важливі у контексті відповідності технологічного рішення статті 3 першого Протоколу до Європейської конвенції з прав людини. Важливо уточнити обов'язки. Політичну відповідальність за використання цифрових рішень на виборах потрібно покладати на ОУВП. На першопочатках співпраці між ОУВП та приватними постачальниками має бути зрозуміло, як вирішуватимуться питання невідповідності виборчим принципам, нормам та стандартам.

4. ВИБРАНІ ДЖЕРЕЛА

Рада Європи, Комітет експертів (MSI-AUT), *Проєкт Рекомендації Комітету Міністрів державам-членам про вплив алгоритмічних систем на права людини,* 26 червня 2019 року.

Рада Європи*, Конвенція 108+, Модернізована Конвенція про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних*, червень 2018 року.

Рада Європи, Консультативний комітет Конвенції про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних, *Доповідь про штучний інтелект. Штучний інтелект та захист даних: виклики й можливі засоби захисту*, 25 січня 2019 року.

Ради Європи, Комітет з питань кіберзлочинності (T-CY), *Настанова № 9, Аспекти втручання у вибори за допомогою комп'ютерних систем, на які поширюється дія Будапештської конвенції,* 8 липня 2019 року.

Рада Європи*, Декларація Комітету Міністрів про маніпулятивні можливості алгоритмічних процесів,* 13 лютого 2019 року.

Рада Європи*, Рекомендація Комітету Міністрів державам-членам щодо стандартів електронного голосування, CM/Rec(2017)5*.

Європейська комісія*, Вільні та чесні вибори. Керівний документ. Посібник Комісії щодо застосування права Європейського Союзу про захист даних у виборчому контексті*. Внесок Європейської комісії у зустріч лідерів у Зальцбурзі 19-20 вересня 2018 року.

Європейська комісія, Експертна група високого рівня з питань штучного інтелекту, *Визначення ШІ: основні можливості та напрями*, 8 квітня 2019 року.

Європейська комісія Ради Європи «За демократію через право» (Венеційська комісія) *та ін.*, *Спільна доповідь щодо цифрових технологій та виборів*, 21–22 червня 2019 року.

IDEA*, Кібербезпека на виборах. Моделі міжвідомчої співпраці,* 2019 рік.

IDEA*, Розробка управління виборчим процесом,* оновлена редакція, 2014 рік.

ОБСЄ/БДІПЛ*, Посібник із питань спостереження за новими технологіями голосування,* 2013 рік.

Група експертів високого рівня Генерального секретаря ООН, *Епоха цифрової взаємозалежності*, червень 2019 року.

Цифрові рішення все частіше використовуються на виборах. Останні роки особлива увага приділяється питанню безпеки таких цифрових рішень, оскільки це впливає на чесність виборів. На законодавця покладається тягар ухвалити нормативно-правове регулювання, яке гарантує, що на виборах зможуть бути використані лише ті цифрові рішення, які відповідають конституційним принципам. Це непросто, оскільки сфера використання цифрових рішень у виборах все ще досить експериментальна. Два дослідження, які увійшли до цього видання, порушують правові питання, містять висновки з урахуванням минулого досвіду деяких країн та пропонують можливі підходи використання цифрових рішень у виборчому процесі. Це видання буде цікавим для законодавців та органів виконавчої влади, а саме органів управління виборчим процесом, яким пропонується ухвалити рішення щодо використання цифрових рішень на виборах.

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