УДОСКОНАЛЕННЯ ЕЛЕКТРОННОГО УРЯДУВАННЯ В КОНТЕКСТІ ЕФЕКТИВНОЇ СИСТЕМИ ЦИФРОВОЇ ІДЕНТИЧНОСТІ

РОМАНЧУК Ольга Захарівна - здобувач кафедри конституційного права та порівняльного правознавства ДВНЗ «Ужгородський національний університет»

DOI:10.32782/LAW.2020.1.3
УДК 342.727

Стаття присвячена аналізу правових аспекти удосконалення електронного урядування в контексті ефективної системи цифрової ідентичності.

Доведено, що конституційне право первинно імплементує ідеї трансформації публічно-правового життя. Доктрина конституціоналізму передбачає принцип участі громадян у здійсненні публічної влади, комунікацію з громадськістю, а основне прийняття державних рішень з врахуванням думки громадян. Отож електронне врядування первинно націлене на ефективну реалізацію вказаних принципів. Його слід вважати засобом демократизації державної влади та конституційного – правових норм. Електронне управління виокремлює таку важливу функцію як забезпечення участі громадськості у формі звернення громадян.

Петиція - це офіційний запит, адресований владі та підписаний численними особами. За допомогою петицій громадяни мають змогу висловити підтримку чи невдоволення урядовими ініціативами та надати відгуки урядовим установам.

Петеційна форма звернень в Україні потребує удосконалення в аспекті ідентифікації особи. Запозичивши позитивний досвід нормативно на національному рівні слід визначити ряд вимог, для можливості функціонального забезпечення петеційної форми участі громадян та збереження конфіденційності інформації.

Ключові слова: електронний уряд, цифрова ідентичність, електронна петиція, доступність влади.

Постановка проблеми

Однією з найбільш затребуваних реформ сучасної конституційно-правової реальності є широке застосування інформаційно-комунікаційних технологій на публічній службі. Швидкі події в цій галузі та величезні перспективи, які вони мають у різних сферах, не тільки посилили очікування громадськості для управління, орієнтованої на громадян, вони також поставили значні виклики перед публічною владою та правовою системою для задовольнити зростаючі очікування громадян шляхом пропонуючи покращені послуги та інноваційні рішення проблем публічного управління. Вказане є досить важливим в сучасній конституційній реформі, оскільки «формування громадянського суспільства та заохочення громадської активності визнано пріоритетним завданням суспільнополітичного розвитку» [1, с.242].

Стан дослідження

Проблемою відкритості та доступності органів публічної влади займалися представники як теоретичної юриспруденції, так і конституційного і адміністративного права, зокрема О. Дніпров, О. Зарічний, І. Жаровська, В. Ковальчук, Ю. Бисага, Д. Бєлов, О. Скрипнюк та інші. Проте активне впровадження системи електронного урядування потребує додаткового аналізу проблемних питань в цій сфері.

Метою статті є правові аспекти удосконалення електронного урядування в контексті ефективної системи цифрової ідентичності.

Виклад основних положень

Конституційне право первинно імплементує ідеї трансформації публічно-правового життя. Доктрина конституціоналізму передбачає принцип участі громадян у здійсненні публічної влади, комунікацію з громадськістю, а основне прийняття державних рішень з врахуванням думки громадян. Отож електронне врядування первинно націлене на ефективну реалізацію вказаних принципів. Його слід вважати засобом демократизації державної влади та конституційного – правових норм.

Така первинна ідея демократизації передбачає активне впровадження інформаційно-комунікативних технологій в усіх цивілізованих державах, влада по всьому світу розпочали програми та проекти, які прагнуть кардинально покращити надання державних послуг шляхом прийняття ІКТ у державному секторі. Насправді відомий як електронний уряд, цифровий уряд, електронне управління та уряд в Інтернеті стати провідною ознакою реформи державного сектору як в розвинених, так і в країнах, що розвиваються. Фактично електронний уряд позиціонується як засіб подолати обмеження традиційних бюрократій та тим більше покращити надання державних послуг.

Історично ініціативи електронного уряду були спрямовані на покращення внутрішніх процесів та ефективності роботи державних агентств, тепер все більше проектів електронного уряду використовуються для спроби надання інтегрованих послуг громадянам, бізнесу та іншим зацікавленим сторонам. Згодом система електронного врядування розширилася і включає в собі надання послуг у різних сферах, зокрема прийнято виділяти:

- електронне управління, зосереджене на внутрішньодержавному процесі управління (G2G);
- електронні послуги, орієнтовані на надання державних послуг громадянам та бізнесу (G2C / G2B);
- та електронне громадянство, орієнтоване на вклад громадян та бізнесу в управління (C2G, B2G) [2, с.1916].

Електронне управління виокремлює таку важливу функцію як забезпечення участі громадськості у формі звернення громадян.

Петиція - це офіційний запит, адресований владі та підписаний численними особами. За допомогою петицій громадяни мають змогу висловити підтримку чи невдоволення урядовими ініціативами та надати відгуки урядовим установам. У світі підписанти петиції зазвичай надають унікальний ідентифікатор (наприклад, національний ідентифікаційний номер) разом із власноручним підписом, щоб не допустити фальшивості або дублювання підписів. Враховуючи високу вартість збору та перевірки підписів петицій вручну, не дивно, що петиції все більше доступні в Інтернеті. Електронні петиції представляють суттєві переваги щодо фізичної петицій: набагато простіше охопити велику кількість людей, які потенційно зацікавлені у їх підписанні, і процес перевірки підписів може бути автоматизований.

Петиційна форма звернень в Україні потребує удосконалення в аспекті ідентифікації особи. Зокрема, стаття 23^{-1} Закону України «Про звернення громадян» визначає загальні положення про сутність електронної петиції, порядок її подання та розгляду. Так «відповідні органи державної влади, органи місцевого самоврядування та громадські об'єднання під час збору підписів на підтримку електронної петиції зобов'язані забезпечити серед іншого і «електронну реєстрацію громадян для підписання петиції; недопущення автоматичного введення інформації, у тому числі підписання електронної петиції, без участі громадянина; фіксацію дати і часу оприлюднення електронної петиції та підписання її громадянином»[3]. Вказаний акт тільки в загальному встановлює основні принципи ідентифікації.

Підзаконний нормативний акт, який дещо ширше тлумачить цю дію полягає в наступному. Постановою Кабінету Міністрів України від 22 липня 2016 р. № 457 затверджено Порядок розгляду електронної петиції, адресованої Кабінету Міністрів України. Там не міститься інформації про ідентифікацію підписантів, виключно розширено ведеться мова про ініціатора петиції. Зокрема «громадянин, який бажає представити свою позицію щодо петиції, заповнює спеціальну форму, яка розміщена на Урядовому порталі або веб-сайті громадського об'єднання. Громадя-

нин, який бажає представити свою позицію щодо петиції, повинен ідентифікуватися на Урядовому порталі або веб-сайті громадського об'єднання за допомогою засобів електронної ідентифікації, що підпадають під схему електронної ідентифікації, затверджену Кабінетом Міністрів України» [4]

Відповідно існує Положення про інтегровану систему електронної ідентифікації, яке було затверджено постановою Кабінету Міністрів України від 19 червня 2019 р. № 546. Воно подає наступне тлумачення «інтегрована система електронної ідентифікації - інформаційно-телекомунікаційна система, яка призначена для технологічного забезпечення зручної, доступної та безпечної електронної ідентифікації та автентифікації користувачів системи, сумісності та інтеграції схем електронної ідентифікації, їх взаємодії з офіційними веб-сайтами (веб-порталами), інформаційними системами органів державної влади, органів місцевого самоврядування, юридичних осіб і фізичних осіб - підприємців, забезпечення захисту інформації та персональних даних з використанням єдиних вимог, форматів, протоколів та класифікаторів, а також задоволення інших потреб, визначених актами законодавства» [5]

Отож, зробити ці дії можливо наступним чином.

1. Шляхом отримання електронного цифрового підпису, що вимагає комплексу попередніх дій та необхідності відвідання компетентних уповноважених органів, наприклад представництво АЦСК органів юстиції України, які доступні тільки в обласних центрах.

2. Ідентифікація через ID-картки можлива тільки для власників нового, пластикового паспорта з реквізитами безпеки доступу до чипа персональних даних. Якщо особа є власником паспорта громадянина у формі ID-картки без відповідного чипа та/або паспорта у форматі книжечки, пройти процедуру ідентифікації за їх допомогою неможливо.

3. Через BankID – це спосіб електронної автентифікації громадян за допомогою їхніх даних у банку, де вони обслуговуються. Цей сервіс дозволяє онлайн, без необхідності особистого візиту, підтвердити особистість людини. Проте має суттєві перестороги, в електронному порядку необхідно вводити свої дані, необхідним є введення логіна, пароля, номера картки тощо. Отож користувачі повинні бути впевнені у безпечності передачі такої інформації, оскільки при цьому використовуються дані людини, що зберігаються в банку, де вона обслуговується, – ПІБ, паспорт, ІНН, адреса, електронна пошта та інші.

4. Використовуючи послугу MobileID. Проблема в тому, що звичайна SIM-карта не дає змоги записати на неї електронний підпис, тому необхідним є відвідування центру обслуговування клієнтів оператора [на підставі аналізу даних 6].

На сайті офіційного інтернет представництва Президента України така ідентифікація не є доступною, як до речі й ідентифікація через Ідентифікація через ID-картки [7].

Поряд з цим, безпечна і надійна система цифрової ідентичності визнається важливою складовою розвитку електронного уряду. З одного боку, і для раціональності та ефективності важливо запропонувати користувачеві унікальний ідентифікатор під час взаємодії з різними державними структурами. З іншого боку, за певних обставин видається необхідним зберегти анонімність користувача, щоб не гальмувати активність користувачів. Таке обмеження суперечить принципам систем Web 2.0, що передбачає взаємодію та комунікацію.

Наприклад, якщо мова йде про надання особистого висновку громадянина про рівень якості надання публічної послуги, користувач може дійсно бажати залишатись анонімним. За відсутності унікального ідентифікатора та неможливості взаємодії анонімним способом громадянин отримує дві можливості, або утворювати декілька ідентифікаторами для доступу до різних сервісів, або створити вигадані ідентичності для збереження анонімності. Така ситуація за твердженням фахівців «створює складність та когнітивні витрати та збільшує ризик шахрайства та надмірності даних» [8].

З технічної точки зору цілком можливо, що унікальний ідентифікатор може бути сертифікований державним органом, щоб дозволити доступ до всіх публічних онлайн-сервісів. Наприклад, платформи Facebook та Google дали можливість використовувати

свої відповідні ідентифікатори для підключення до сайтів за допомогою API Facebook Connect та API відкритого соціального ідентифікації Google (інтерфейси програмування програм). Тому для державних систем унікальна ідентифікація викликає фундаментальне питання щодо централізації ідентифікації даних стосовно набору державних органів, які можуть створити і управляти ідентифікаторами. Тобто необхідною є система, подібніа до Facebook та Google, де усі сервіси підключалися б до єдиної системи, яка управляє даними про з'єднання та надає дозволи на доступ. Встановлення такої структури залежить від того, чи є унікальний ідентифікатор, концептуально (тобто, яка інформація) та адміністративно (тобто як вона обробляється), визначений для кожного громадянина в управлінських відносинах країни.

Якщо такий ідентифікатор ключа існує (як це має місце в деяких європейських країнах), централізована система аутентифікації буде прозорою для користувача. Якщо такого унікального ідентифікатора не існує (як це відбувається наприклад у Франції), реалізація є більш складною, оскільки вимагає поступової заміни декількох входів одним логіном. У Франції портал service-public.fr розробляється з метою доступу до всіх державних служб (наприклад, соціальне забезпечення, декларація про доходи) за допомогою єдиного входу. З етичних міркувань та для запобігання перетину даних і, таким чином, захисту конфіденційності громадян було прийнято рішення створити окремий конкретний ідентифікатор для цього порталу [9].

Технічні досліджень продемонстрували небажання громадян приймати унікальні системи ідентифікації. Прийняття користувачів часто затримується занепокоєнням щодо контролю та / або використання даних для злочинних дій.

Багато доступних на сьогодні електронних петицій просто збирають ім'я та національний ідентифікаційний номер підписників. Зважаючи на те, що ця інформація не є секретною, неможливо перевірити, чи справді підписант петиції надає свої власні дані. Іншими словами, виявити обман не вдається, що зменшує надійність списку підписів петиції. Щоб запобігти цьому, деякі сервери електронних петицій перевіряють IP-адресу підписанта та дозволяють лише один підпис на IP-адресу. Але це обмежує права користувачів на свободу висловлення думки, саме тих які використовують IP-адресу умісно з іншими людьми (наприклад, що в деяких організаціях тисячі користувачів поділяють ту саму IP-адресу).

Для того, щоб електронний підпис під петицією був унікальним та законним, необхідно використовувати криптографічні засоби, такі як цифрові підписи, як зокрема пропонується нині в Україні. Якщо припустити, що громадяни мають електронні картки електронного посвідчення, очевидним способом реалізації електронних петицій є те, щоб громадяни підписували їх за допомогою ключів, наявних на їх електронній картці. Однак таке рішення проблематично з точки зору конфіденційності. Сертифікат відкритого ключа електронного ідентифікатора (необхідний для підтвердження цифрового підпису) містить багато інформації про власника картки, наприклад, ім'я, номер національного реєстру та дату народження. Розкриття всієї цієї інформації для підписання петиції, безумовно, буде суперечити принципу мінімізації даних, що ґрунтується на юридичній доктрині захисту персональних даних. Мінімізація даних означає, що певна кількість персональних даних може оброблятися, але лише така їх частина, яка є вкрай необхідно для законних цілей. Іншими словами, додаткові питання захисту даних виникають, коли петиції дозволяють отримувати конфіденційну інформацію про користувача, обробка якої взагалі заборонена законодавством про захист даних. Зокрема, така інформація може стосуватися (серед інших категорій даних) політичної думки, релігійних чи особистих переконань, всі вони розглядаються як «чутливі персональні дані» відповідно до Директиви 95/46/ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних»[10].

Унікальною технічною можливістю є апробована бельгійська система. При розробці електронних петицій використовують бельгійський електронний ідентифікатор для початкової автентифікації, а потім до-

зволяє користувачеві отримати анонімні, які використовуються для електронного підпису петицій на сервері. Для надання первинної автентифікації використовується існуюча електронна картка електронного посвідчення на основі чого в подальшому особа отримує один анонімний обліковий запис для петиції. Використання анонімних даних для підписання електронних петицій забезпечує максимальний захист конфіденційності завдяки мінімізації даних. Використовуючи анонімні дані, узгоджуються дві, здавалося б, суперечливі вимоги: анонімне підписання петиції, в той час як встановлює обмеження щодо того, хто має право підписувати, і гарантує, що кожен громадянин може підписати певну петицію лише один раз. Комп'ютерні системи виявляють багаторазове підписання петиції з тим самим анонімним обліковим записом, щоб усунути повторне підписання [11].

Висновок

Таке удосконалення є первинно необхідне для національної правової системи. Отож запозичивши позитивний досвід нормативно на національному рівні слід визначити ряд вимог, для можливості функціонального забезпечення петеційної форми участі громадян та збереження конфіденційності інформації.

· Захищена автентифікація - сервери електронного урядування повинні чітко аутентифікувати себе перед користувачем, щоб запобігти дублюванню нелегітимних серверів, особливо з метою запобігання отримання від громадян облікових даних та забезпечення того, що запит надходить від законного користувача.

· Авторизація, тобто тільки громадяни, які мають право підписати петицію, повинні це зробити. Наприклад, в деяких випадках петиції можуть підписувати лише громадяни, які мають повноліття, або ті, хто проживає на певній території. Наприклад створення спеціальних верефікаторів, зокрема програма не дізнається точний вік користувача, але може перевірити мінімальний / максимальний вік засвідчений емітентом у облікових даних.

· Цілісність даних, тобто жодна організація не повинна мати змогу змінювати дані, що обмінюються між громадянином та серверами електронного уряду.

· Конфіденційність, що вимагає, щоб усі обміни даними між громадянином та серверами електронного уряду повинні зберігатися в таємниці від інших організацій. Крім того, необхідний захист аналізу трафіку, щоб зовнішні спостерігачі не змогли визначити, що громадянин отримує доступ до сервера електронних петицій (або певної петиції на сервері).

· Анонімність підписанта - сервер електронних петицій (навіть у змові з емітентом облікових даних) не повинен ідентифікувати громадян, які підписали петиції.

· Профілактика декількох підписів, тобто заявка на електронну петицію повинна бути розроблена таким чином, щоб вона могла належним чином виявляти та виправляти спроби громадян підписати одну електронну петицію кілька разів.

· Наявність громадської перевірки, тому що важливою вимогою до прозорості підписання електронної петиції є надання доказів справедливого підрахунку підписів під петицією.

Література

1. Жаровська І. М. Генезис ідеї відкритості влади Форум права. 2009. № 3. С. 242-246.

2. Khanh N. T.V., Danh M. T., Gim G. E-Government in Vietnam: Situation, Prospects, Trends, and Challenges *Open Government: Concepts, Methodologies, Tools, and Applications*. 2020. P. 1915-1931

3. Про звернення громадян: закон України від 02.10.1996№ 393/96-ВР *Відомості Верховної Ради*. України. 1996. № 47. ст.256.

4. Порядок розгляду електронної петиції, адресованої Кабінету Міністрів України: затв. постановою Кабінету Міністрів України від 22 липня 2016 р. № 457 URL: https://zakon.rada.gov.ua/laws/show/457-2016-%D0%BF

5. Положення про інтегровану систему електронної ідентифікації: затверджено постановою Кабінету Міністрів України від 19 червня 2019 р. № 546 URL: https://zakon.rada.gov.ua/laws/show/546-2019-%D0%BF

6. Інтегрована система електронної ідентифікації URL: https://id.gov.ua/

7. Електронні петиції. Офіційне інтернет представництво президента України. URL:https://petition.president.gov.ua/

8. Fioravanti, E. Nardelli Identity Management for e-Government Services. H. Chen, L. Brandt, V. Gregg, R. Traunmüller, S. Dawes, E. Hovy, A. Macintosh, C. A. Larson. *Digital Government*. 2008. Boston, MA: Springer US. P. 331-352.

9. Mattatia F. L'impact sociétal de l'identification électronique. S. Assar, I. Boughzala. *Administration électronique: constats et perspectives*. Editions Hermès Lavoisier. 2006.

10. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних: Директива 95/46/ЄС Європейського Парламенту і Ради від 24 жовтня 1995 року 24.10.1995 URL: https://zakon.rada.gov.ua/laws/show/994_242

11. Diaz C., Kosta E., Dekeyser H., Kohlweiss M., Nigusse G. Privacy preserving electronic petitions. Identity in the Information Society. 2009. vol. 1, no. 1. P. 203-219.

IMPROVEMENT OF ELECTRONIC GOVERNMENT IN THE CONTEXT OF AN EFFECTIVE DIGITAL IDENTITY SYSTEM

The article focuses on analyzing the legal aspects of improving e-government in the context of an effective digital identity system.

It is proved that constitutional law primary implements the ideas of transformation of public-legal life. The doctrine of constitutionalism envisages the principle of citizen participation in the exercise of public authority, communication with the public, and the basic decision-making of the state, taking into account the opinion of citizens. Therefore, e-government is primarily aimed at effectively implementing these principles. It should be considered as a mean of democratization of state power and constitutional - legal norms. E-government highlights such an important function as ensuring public participation in the form of citizen appeals.

The petition is an official request addressed to the authorities and signed by numerous persons. Petitions allow citizens to express their support or dissatisfaction with government initiatives and provide feedback to government agencies.

The petition form of appeals in Ukraine needs improvement in the aspect of person identification.

It is summarized that, having borrowed positive experience, a number of requirements should be defined at the national level in order to be able to provide a functional form of petition for citizen participation and to preserve the confidentiality of information.

1. Secure Authentication - e-government servers should clearly authenticate themselves to the user to prevent illegitimate servers' duplication, especially to prevent obtaining from citizens credentials and ensuring that the request is received from a legitimate user.

2. Authorization, i.e. only citizens who have the right to sign the petition, must do so. For example, in some cases petitions can only be signed by citizens who are of legal age or who live in a certain territory.

3. Data integrity, i.e. no organization should be able to modify the data exchanged between the citizen and the e-government servers.

4. Confidentiality, which requires that all communications between the citizen and e-government servers should be kept secret from other organizations. In addition, traffic analysis protection is required to prevent external observers from determining that a citizen is accessing the e-petition server (or a specific petition on the server).

5. Subscriber's anonymity - the e-petitions server (even in collusion with the issuer of credentials) should not identify the citizens who have signed the petitions.

6. Prevention of multiple signatures, i.e. an e-petition application must be designed in such a way that it can properly identify and correct citizens' attempts to sign one e-petition several times.

7. The availability of public scrutiny, as an important requirement for transparency in the signing of an electronic petition is to provide evidence of a fair counting of the petition signatures.

Keywords: e-government, digital identity, e-petition, availability of authority.