Тихомирова Є.Б.*

КОМУНІКАТИВНА ПОЛІТИКА ЄС: ІНФОРМАЦІЙНА БЕЗПЕКА VS ТРАНСПАРЕНТНІСТЬ

Проаналізовано комунікаційну політику Європейського Союзу в контексті встановлення балансу між транспарентністю та інформаційною безпекою ЄС. Визначається її спрямованість на формування транспарентності інституцій ЄС та застосування заходів щодо інформаційною безпекою європейського суспільства. Характеризуються основні завдання структур ЄС у забезпеченні транспарентності інформаційної безпеки і безпеки транспарентності.

Ключові слова: комунікаційна політика ЄС, інформаційна безпека, Європейський Союз, Інтернет, транспарентність.

Проанализирована коммуникационная политика Европейского Союза в контексте обеспечения баланса между транспарентностью и информационной безопасностью ЕС. Определяется ее направленность на формирование транспарентности учреждений ЕС, проведение мероприятий по информационной безопасностью европейского общества. Характеризуются основные задачи структур ЕС в обеспечении транспарентности информационной безопасности и безопасности транспарентности.

Ключевые слова: коммуникационная политика ЕС, информационная безопасность, Европейский Союз, Интернет, транспарентность.

The communication policy of the European Union in the context of ensuring a balance between transparency and information security of the EU is analyzed. By its focus on the formation of transparency of EU institutions and activities in information security of European society is defined. By the main tasks of the EU structures to ensure transparency of information security and transparency are characterized.

Keywords: EU communication policy, information security, European Union, Internet access, and transparency.

Постановка наукової проблеми та її значення. Європейська інтеграція стала не тільки політичним, але і комунікаційним викликом. Щоб подолати проблеми взаємодії між громадянами Європи та ЄС, Європейська Комісія значно посилила свою увагу до проблем комунікації, а комунікаційна діяльність стала важливою складовою функціонування всіх європейських організацій і держав ЄС. Сьогодні Європейський Союз серйозно зацікавлений у покращенні свого іміджу та комунікаційного потенціалу як на загальносоюзному, так і на національному рівні.

* доктор політичних наук, професор, завідувач кафедри міжнародної інформації Волинського національного університету ім. Лесі Українки

Комунікація, як зазначають європейські дослідники, не може зробити Європейський Союз (ЄС) краще та вирішити його економічні, соціальні, політичні та екологічні проблеми. Тим не менш, вона допомагає підвищенню обізнаності та мобілізації людей. Вона може стати провідним інструментом для зміцнення ідентичності, інтеграції, поваги і демократії. Комунікація може допомогти краще зрозуміти своїх громадян, і через це розуміння ЄС буде в змозі поліпшити свої інститути і політики.

Аналіз останніх досліджень з цієї проблеми свідчить, що вона є предметом дослідження зарубіжних науковців. Важливість встановлення балансу між транспарентністю та інформаційною безпекою ЄС та інтерес до ініціатив з покращення їх співвідношення стимулювали широкі наукові дебати з цього питання.

Численні публікації європейських вчених висвітлюють різні аспекти комунікаційної політики ЄС загалом і, зокрема, звертають увагу на роль і значення в її реалізації принципів транспарентності і безпеки. Це дослідження директора Інституту комунікативних досліджень Університету Лідса (Великобританія) Дж. Лодге [1], іспанських науковців К. Капелли, Х. Кунья, Б. Гонсалес, Х. С. Сампайо Прадо Лейте [2], американського менеджера проектів Д.Л. Пеллса [3] та ін.

В українській науці цей аспект проблеми залишився поза увагою. Тому предметом нашого дослідження став аналіз комунікаційної політики ЄС у контексті збалансування її прозорості і інформаційної безпеки.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження. Комунікаційна політика ЄС сприяє тенденціям відкритості і прозорості, що діють у сучасному світі. Транспарентність стає, з одного боку, важливим чинником національних і демократичних перетворень світу. З іншого – міжнародне співробітництво не здатне успішно розвиватися без взаємної довіри та взаєморозуміння, які вимагають прозорості та відкритості взаємин. Як зазначалося у «Стратегії інформації і комунікації для Європейського Союзу», так само, як держави–члени, ЄС стоїть перед проблемою втрати громадськістю довіри до його політики. У зв'язку з розширенням ЄС та обговоренням його майбутнього, у контексті недовіри до глобалізації виникає потреба зробити Європейські проекти більш зрозумілими і транспарентними [4].

Проте, транспарентність, будучи передумовою демократичних трансформацій суспільства, глобальним імперативом гармонізації міжнародних відносин, не лише забезпечує подолання надмірної закритості влади і пов'язаного з нею відчуження від суспільства, але і породжує певні проблеми. Серед негативних наслідків впровадження транспарентності в життя суспільства ми бачимо проблему інформаційної безпеки, яка актуалізується в умовах поширення транспарентності на різні сфери життя. Саме тому, коли ми говоримо про відкритість суспільства, транспарентність влади або соціального інституту або організації, на наш погляд, не слід забувати про їхню безпеку.

Проблема транспарентності і інформаційної безпеки органічно пов'язані між собою і взаємозалежні. В умовах, коли світ став більш єдиним завдяки глобальним комунікаціям і глобальній мережі Інтернет, ризики небезпеки, пов'язані з ними, значно збільшилися. Вирішення проблем інформаційної безпеки потребує захисту громадян і суспільства: захищеності від тероризму у локальному і глобальному масштабі, захисту активів організацій від конкурентів, злочинців, хакерів чи диверсантів, від кіберризиків тощо.

Не випадково, логічним продовженням реалізації комунікаційної політики ЄС, викладеної у Білій книзі з комунікації, стало формування та реалізація політики транспарентності. У промові у Ноттингемському університеті 3.03.2005 р. [5], С. Каллас, комісар з адміністративних питань і боротьби з шахрайством, висунув ідею транспарентності, зо-

рієнтовану на три ключові області: збільшення фінансової звітності ЄС; зміцнення особистої недоторканності і незалежності інститутів ЄС; введення більше суворого контролю на лобіювання. Застосування політики транспарентності, на його думку, збільшило би відкритість і доступність установ ЄС, підвищило поінформованість про бюджетні витрати й загалом зробило ЄС більш підзвітною громадськості. Ці ідеї були відображені у Зеленій книзі «Європейська ініціатива прозорості» – «European Transparency Initiative» (2006р.) [6], а потім і в інших документах [7; 8; 9; 10]. Основною метою Ініціативи транспарентності стало зробити роботу інститутів ЄС більш прозорою і доступною. Одним з практичних заходів для досягнення цієї мети став намір Комісії оприлюднити на своєму сайті «Європа» імена тих, хто отримує фінансування ЄС. З 10 жовтня 2006 р. тут можна отримати доступ до інформації про гранти ЄС і контракти.

На основі Зеленої книги з європейської ініціативи прозорості було розпочато консультації. Учасникам було запропоновано висловити свою думку щодо прозорості та представлення інтересів в ЄС (лобіюванням); мінімальних стандартів для консультацій із зацікавленими сторонами (застосування стандартів щодо зворотного зв'язку); оприлюднення імен одержувачів фінансування ЄС (грошей з різних фондів ЄС). Ініціативи із забезпечення прозорості були продовжені ЄК не лише в контексті оприлюднення розподілених коштів і становлення фінансової прозорості, яка дозволяє громадянам побачити, як і ким їхні податки витрачаються. Мало місце і підвищення прозорості інститутів ЄС з допомогою упорядкування лобізму в ЄС, розпочате дещо раніше [11]. Станом на 20.12.10 в ЄС було зареєстровано 3389 лобістів [12].

Оскільки транспарентність та інформаційна безпека є компліментарними[1] поняттями і характеризують одне явище – стан поінформованості соціальних суб'єктів, було б логічно співвіднести ці категорії, порівнюючи концептуальні підходи ЄС до транспарентності та інформаційної безпеки. Чи забезпечений у комунікативній стратегії ЄС належний баланс між транспарентністю і необхідністю забезпечення інформації безпеки?

Як зазначає Дж. Лодге, близько 17% всіх законодавчих пропозицій ЄК ставляться до свободи, безпеки і правосуддя. При цьому вона підкреслює, що відкритість і секретність не обов'язково суперечать один одному, оскільки більша відкритість означає меншу неясність. Проте передачу інформації, особливо важливої інформації, в контексті безпеки дослідниця вважає досить складним завданням. Стратегічні, тактичні й оперативні вимоги мають бути ретельно зважені, щоб не поставити під загрозу діяльність ЄС [1]. Створенню ж більш ефективних правил прозорості, у свою чергу, сприяє високий рівень конфіденційності і безпеки.

У програмі «Е–Європа 2005»т констатується, що забезпечення інформаційної безпеки не є чисто технологічною проблемою, вона стосується значною мірою людської поведінки, знання та передбачення погроз і засобів захисту. Проблеми інформаційної безпеки охоплюють недоторканність приватного життя, економічної політики, міжнародної торгівлі, прав громадян, правопорядку, оборони, і багато чого іншого, тому цілісний підхід до цієї проблеми, як на європейському, так і глобальному рівнях, має важливіше значення.

ЄС уже розробив правила для безпечного обміну електронними повідомленнями («Конфіденційність в інформаційному суспільстві»). Деякі інші засоби розглядаються в рамках мережної безпеки (поліпшення надійності мереж і інформаційних систем щодо нещасних випадків і злочинних зазіхань). Про безпечні комунікації електронного уряду

[1] Компліментарність (complementarity) ми трактуємо як взаємну відповідність, здатність елементів певної структури взаємно доповнювати, замінювати одне одного.

йдеться в контексті розробки безпечної транс'європейської мережі зв'язку, через яку можна буде використовувати секретну інформацію.

Особливу увагу ЄС приділяє безпеці персональних даних. Ще у 1995 р. була прийнята директива про захист даних персональних даних у Європейському Союзі. Вона закріплювала два основних права: право на захист персональних даних і на їхнє вільне поширення. У 2002 р. була прийнята директива про недоторканність приватного життя й електронних [13].

Проте, швидкі технологічні зміни і глобалізація докорінно змінили світ навколо нас, і принесли нові виклики. Зараз технологія дозволяє особисту інформацію поширювати в усьому світі у безпрецедентних масштабах. Соціальні мережі, із сотнями мільйонів членів, поширені по усьому світі. Дослідження підтверджують, що зростає зближення позицій щодо захисту даних органів влади, бізнес–асоціацій і організацій споживачів, пов'язаних з онлайн–активністю. Органи державної влади, зокрема, використовують усе більше і більше персональних даних для різних цілей, такі, як відстеження осіб у випадку спалаху інфекційних захворювань, для запобігання боротьби з тероризмом і злочинністю, для адміністрування соціального забезпечення схем або для цілей оподатковування, у рамках своїх додатків електронного уряду.

Підвищення прозорості є основною умовою здійснення контролю і забезпечення ефективного захисту особистих даних. Тому дуже важливо, щоб особи були добре і чітко поінформовані на транспарентній основі про ці дані, що збираються і обробляються, з яких причин, на який термін. Вони мають знати про їхні права, якщо вони хочуть отримати доступ, виправити або видалити свої дані.

Основним елементом прозорості має бути легкість і доступність інформації для розуміння, що забезпечується чіткістю і простою мови, яка використовується. Це особливо актуально в он–лайн середовищі. Для цього Комісія пропонує введення загального принципу прозорості у правовій базі, прийняття конкретних зобов'язань про умови надання інформації, складання стандартних форм, які можуть використовуватися. У документі ЄС передбачені і ситуації, якщо дані будуть втрачені або виникне ризик витоку даних [14].

На європейському рівні застосовуються організаційні заходи для підтримки політики інформаційної безпеки. Створений, зокрема Центр європейський мережевої і інформаційної безпеки (ENISA), розширює співробітництво й обмін інформацією між різними зацікавленими структурами держав–членів ЄС, робить внесок у підвищення рівню інформаційної безпеки у внутрішньому інформаційно–комунікативному просторі. Ним реалізуються програми – безпечного Інтернету, досліджень і розробок у рамках Шостої рамкової програми з наукових дослідженнях у таких областях, як електронна аутентифікація (смарт–карти, біометрія); застосування нових стандартів безпеки мереж і інформації; розвитку транс–європейської мережі для телекомунікацій, якою може бути забезпечена залежно від довіри й упевненості в послугах активна участь бізнесу і громадян в інформаційному суспільстві [15].

Важливе значення для забезпечення необхідного балансу транспарентності та інформаційної безпеки має впровадження в ЄС транспарентних принципів безпеки. ЄК, довівши здатність активно застосовувати ІКТ та створивши великомасштабні інформаційні системи, має не лише гарантувати їх якість і доступність, але і безпеку. Це завдання може розглядатися як стратегічний напрям комунікаційної політики ЄС.

Досвід європейських країн свідчить про те, що в них давно законодавчо визначаються обмеження щодо запровадження принципу транспарентності на окремі категорії інформації. Ці обмеження стосуються інформації про захист національної безпеки і міжнародних відносин, захисту приватного життя, комерційної конфіденційності, правоохоронної

діяльності і забезпечення громадського порядку, а також інформації, отриманої конфіденційно. У багатьох парламентарних системах доступ до документів, представленим на розгляд Кабінету для прийняття рішень, і матеріалам засідань Кабінету, закритий протягом певного часу (в Ірландії цей строк, наприклад, становить десять років) [16].

Подібна практика впроваджена і на рівні ЄС, коли визначаються види інформації, які повинні і які не повинні розкриватися. Для цього сформульовані кілька основних принципів відкриття інформації: діяльність у рамках спільної інформаційної політики безпеки і практики; розкриття інформації при наявності відповідного мандата, коли розкриття необхідно у зв'язку з правовими або нормативними вимогами; формування адекватної архітектури безпеки, коли повинні бути розкриті деталі безпеки, які можуть або сприяти або перешкоджати забезпечення безпеки; управління.

Також сформульовані принципи, при яких розкриття не рекомендується: не посилювати ризики, не розкривати нічого, що може створити ризик для центрів обробки даних або цілісності даних, що зберігаються в центрі обробки даних; не нашкодь: слід уникати розкриття інформації, якщо це може створити потенційну шкоду для клієнтів або партнера; управління відповідальністю, що вимагає уникнення розкриття інформації у випадку створення невиправданої відповідальності; утримання від розкриття інформації при наявності відповідного мандата (якщо розкриття призвело б до порушення юридичних чи нормативних вимог, його слід уникати) [17].

Важливим аспектом транспарентизації інформаційної безпеки є підвищення поінформованості та розуміння проблеми безпеки, а також базових знань у цій області, що може бути пов'язано з процесом масового просвітництва та формуванням культури транспарентності та інформаційної безпеки. Аналітики RAND Corporation зазначають, що баланс між свободою, конфіденційністю і безпекою фактично поляризується навколо проблеми громадянських свобод та громадської безпеки. Вони дослідили, що люди можуть зробити, коли зіткнулися у реальному житті з вибором відносно приватного життя, свободи і безпеки, отримавши кількісні характеристики думку та уподобань громадян як користувачів інфраструктури безпеки. Було виявлено, зокрема, що люди готові відмовитися від деяких свободу і недоторканність приватного життя, і навіть доплачувати за певні переваги безпеки, але з застереженнями. У деяких випадках уряди повинні субсидіювати людей прийняти вторгнень на їх особисте життя [18].

Висновки. Напруга між транспарентністю і доступом до інформації, з одного боку, і можливістю гарантувати суспільну безпеку, а також навпаки, – проблема, що не знайшла в ЄС однозначного вирішення. На жаль, прозорість і безпека до сих пір фактично розглядаються як діаметрально протилежні і тому їхні вимоги дуже важко задовольняються одночасно. Існування напруженості у відносинах між прозорістю та доступом до публічної інформації може бути послаблена за рахунок збільшення можливостей держави у забезпеченні громадської і національної безпеки.

Саме тому варто вирішувати проблему, виходячи з такого постулату: інформаційна безпека має стати більш транспарентною, а транспарентність – безпечною. Механізм забезпечення цього принципу може стати предметом подальших наукових пошуків.

Література

1. Juliet Lodge. Transparency and EU governance: Balancing Openness with Security [Електронний ресурс] – Режим доступу : http://www.iccr–international.org/europub/docs/ws1–lodge.pdf; Communicating (in)Security: A Failure of Public Diplomacy? [Електронний ресурс] – Режим доступу : http://www.ceps.eu/ceps/download/1231.

2. Claudia Cappelli. Herbet Cunha, Bruno Gonzalez–Baixauli, Julio Cesar Sampaio do Prado Leite. Transparency versus security: early analysis of antagonistic requirements [Електронний ресурс] – Режим доступу : http://portal.acm.org/ft_gateway.cfm?id=1774151&type=pdf.
3. David L. Pells. Transparency vs. Security! A growing Dilemma for Project Managers & Organization. [Електронний ресурс] – Режим доступу : http://www.pmforum.org/library/editorials/2007/PDFs/Pells–5–07.pdf.
4. On an information and communication strategy for the European Union. – Brussels: Commission of the European Communities, 2002. – 44c. [Електронний ресурс] – Режим доступу : http://eur–lex.europa.eu/LexUriServ/site/en/com/2002/com2002_0350en02.pdf.
5. Kallas S. The Need for a European Transparency Initiative (Speech/05/130): The European Foundation for Management, Nottingham Business School, Nottingham, 3 March [Електронний ресурс] – Режим доступу : http://europa.eu.int/rapid/pressReleasesAction.do?reference=SPEECH/05/130&format=HTML&aged=0&language=EN&guiLanguage=en.
7. Green Paper European Transparency Initiativa Com(2006) 194 final [Електронний ресурс] – Режим доступу : http://europa.eu/documents/comm/green_papers/pdf/com2006_194_en.pdf.
9. Follow–up to the Green Paper «European Transparency Initiative». Brussels, 21.3.2007Com(2007) 127 final [Електронний ресурс] – Режим доступу : http://ec.europa.eu/transparency/eti/docs/com_2007_127_final_en.pdf.
10. Report on the development of the framework for the activities of interest representatives (lobbyists) in the European institutions [Електронний ресурс] – Режим доступу : http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A6–2008–0105&language=EN&mo.
12. European Transparency Initiative. A framework for relations with interest representatives (Register and Code of Conduct). Brussels, 27.5.2008. Com(2008) 323 final [Електронний ресурс] – Режим доступу : http://ec.europa.eu/transparency/docs/323_en.pdf.
13. European Transparency Initiative: the Register of Interest Representatives, one year after. Brussels, 28.10.2009 Com(2009) 612 final [Електронний ресурс] – Режим доступу : http://ec.europa.eu/transparency/docs/communication_2009_en.pdf.
14. Lobbying in the European Union: current rules and practices. Constitutional Affairs Series. European Communities, 2003 [Електронний ресурс] – Режим доступу: http://ec.europa.eu/civil_society/interest_groups/docs/workingdocparl.pdf.
15. Statistics for register [Електронний ресурс] – Режим доступу: https://webgate.ec.europa.eu/transparency/regrin/consultation/statistics.do.
16. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [Електронний ресурс] – Режим доступу: http://eurolex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF
17. A comprehensive strategy on data protection in the European Union [Електронний ресурс] – Режим доступу: http://epic.org/privacy/intl/eu_data_protection_ directive.html.

18. Europe 2005 Security Policies in Brief [Електронний ресурс] – Режим доступу : http://ec.europa.eu/information_society/eeurope/2005/all_about/security/index_en.htm.
19. Банисар Дэвид. Свобода информации и доступ к правительственным документам. Обзор законодательства по доступу к информации в мире. – М.: Де Ново, 2006. – 217с.
20. What is Transparent Security [Електронний ресурс] – Режим доступу : http://www.save9.com/wp–ontent/uploads/2010/01/BUILDING_CUSTOMER_TRUST_Cloud_Computing_White–Paper_Nov_2009.pdf.
22. Understanding the Security, Privacy and Trust Challenges. [Електронний ресурс] – Режим доступу: http://www.rand.org/randeurope/research/innovation _policy/ict.html.