

THE IMPACT OF INFORMATION TECHNOLOGY ON ENSURING HUMAN RIGHTS AND FREEDOMS IN AN OPEN SOCIETY

Bochkoviy O.,

Ph.D., Senior Researcher. Head of Educational and Scientific Laboratory Research preventive action of Dnipropetrovsk State University of Internal Affairs, Dnipro, Ukraine

ORCID: <https://orcid.org/0000-0001-7262-3416>

bochkin.0583@gmail.com

Khankevich A.,

Ph.D., associate professor. Professor of the department of operative investigative activity and crimes investigation of the Kharkiv National University of Internal Affairs, Kharkiv, Ukraine

ORCID ID: <https://orcid.org/0000-0002-6897-347X>

a.n.khankevich@gmail.com

Abstract. The article is devoted to the influence of developing technologies on society, human rights and freedoms, which causes a revision of the existing attitude to the outside world. The intensity of the emergence of new forms of organizing social relations (social networks, virtual reality, robotics, blockchain, etc.) complicates the adaptation of existing social institutions to them. This situation leads to many contradictions both in the regulatory sphere and among the population. It has been determined that the danger of the latest technologies is that the rules of conduct have not been formed and, therefore, the institution of responsibility for their violation has not been formed. The article provides an analysis of this problem and possible ways to solve it in order to increase the efficiency of protecting the rights of citizens.

Keywords: information technology, open society, citizen rights, protection, security, security, big data

Останніми роками «великі дані» (Big Date) є загальноновизнаним трендом економічного та технологічного розвитку, який формують одночасно багато факторів: 1) проникнення Інтернету в повсякденне життя; 2) розвиток електронної комерції; 3) поява та розвиток пошукових сервісів, які мають у своїй основі рекламну бізнес-модель, котра передбачає збирання великих масивів інформації про поведінку індивідів у мережі Інтернет; 4) поява соціальних мереж, які агрегують дані не тільки про індивіди, але й про відношення між ними; 5) розповсюдження смартфонів та планшетів, котрі дозволяють постійно (он-лайн) відслідковувати маршрут пересування своїх користувачів, а також обмінюватись миттєвими повідомленнями. Як наслідок, ключові процеси життєдіяльності людини перетекли в Інтернет та будь-яка дія індивіда залишає цифровий слід, що в сукупності викликало появу величезних об'ємів цифрової інформації. При цьому, за прогнозами компанії IDC, яка спеціалізується на аналітиці в сфері інформаційних технологій, більша частина даних буде генерована не людьми, а різного роду пристроями в ході їх взаємодії між собою та мережами даних (наприклад, смартфонами, пристроями радіочастотної ідентифікації (RFID), супутниковими системами навігації типу (GPS).

Такий стрімкий розвиток технологій провокує перегляд існуючого відношення до навколишнього світу, у тому числі й до суспільства. Сфери застосування комп'ютерних програм різноманітні: космос, оборона, промисловість, освіта тощо. Наприклад, спеціальні програми навіть здійснюють діагностику захворювань в медицині і за твердженнями самих медиків точність у встановленні діагнозу підвищилась до 90% [1]. Під час порівнювальних тестів було показано, що за рахунок інтелектуальних програмних алгоритмів досягається підвищення ефективності при скороченні часу постановки діагнозу до 70%. Це дає можливість значно знизити кількість помилкових діагнозів, що грає ключову роль для здоров'я пацієнта. Крім того, відбувається скорочення часу на окупність діагностичного обладнання, зменшується потреба в повторних обстеженнях, знижується ризик юридичних наслідків, які можуть виникати при помилковому призначенні неправильного лікування [2].

У судочинстві основними цифровими технологіями можуть стати:

- великі дані (Big Date);
- нейротехнології та штучний інтелект (наприклад, «бот-юрист» вже сьогодні здатен скласти позовні заяви до фізичних осіб, штучний інтелект навчений передбачати судові рішення у справах про порушення прав людини в Страсбурзькому суді (ЄСПЧ) з ймовірністю 79%);
- системи розподіленого реєстру (на прикладі використання технології блокчейн мова піде далі);

- квантові технології (в якості однієї з можливостей комп'ютерів на основі (в якості однієї з можливостей комп'ютерів на основі квантових технологій є можливість забезпечення кібербезпеки та надбезпечний обмін даними на довгих відстанях);

- компоненти робототехніки та сенсоріка;

- технології бездротового зв'язку (оперативне використання різних банків даних, обліків, проведення он-лайн процесуальних дій тощо);

- технології віртуальної та доповненої реальності (подання доказів у суді, моделювання в судовому процесі подій) тощо.

Активно з'являються нові форми організації суспільних відносин (соціальні мережі, віртуальна реальність, робототехніка, блокчейн тощо), а інтенсивність, з якою вони з'являються ускладнюють пристосування до них вже існуючих суспільних інститутів, не говорячи про форми державного контролю. Адже чим більше персональних даних про особу агрегується та піддається обробці, тим вищий ступінь можливого впливу на життя такої особи результатів автоматизованої обробки та, відповідно, розмір ризику, пов'язаний з порушенням її прав.

Така ситуація призводить до виникнення різноманітних протиріч як у нормативному полі, так і серед населення. Адже природно, що невідоме викликає занепокоєння та страх. Катастрофічні прогнози та теорії щодо запровадження штучного інтелекту стали ідеями для багатьох художніх фільмів-катастроф.

Недостатнє розуміння можливостей та ролі сучасних інформаційних технологій у житті суспільства призвело до виникнення трьохаспектної проблеми:

1) держава не виробила дієвих механізмів впливу та контролю в сфері нових суспільних відносин, які виникли на фоні стрімкого розвитку інформаційних технологій;

2) вказаним упущенням зі сторони держави скористались окремі особи, які почали використовувати сучасні інформаційні здобутки у злочинних цілях, залишаючись при цьому безкарними;

3) вищевказані факти сформували у населення занепокоєння та загрозу своїм правам та свободам.

Реакція суспільства цілком виправдана та передбачувана. Адже будь-кого занепокоїть перспектива стати жертвою злочину або об'єктом іншого порушення особистих прав та свобод. Не дивлячись на відносну ефективність положень чинного законодавства про персональні дані стосовно сталих методів обробки масивів даних, ізольованих рамками окремих організацій, технології «Великих даних» несумісні з низкою базових принципів, які складають основу законодавства про персональні дані, що зумовлює необхідність його реформування.

Небезпека з новітніми технологіями у тому, що не сформовано правил поведінки, а тому й не сформовано й інституту відповідальності за їх порушення. Зокрема, проблематично притягнути особу до відповідальності за незаконні операції з криптовалютою в державі, яка не визнає останню платіжним засобом.

Звісно, будь-яке суспільство не може існувати без норм поведінки, які створюються тільки тоді, коли допускається можливість їх порушення. Закон описує не факти, а орієнтири для нашої поведінки. Якщо цей закон має сенс і значення, то він може бути порушений, а якщо його неможливо порушити, то він поверхневий і не має сенсу [3, с. 187]. Складно не погодитись з К. Поппером, але що робити, коли законодавець ігнорує суспільні відносини, які вже існують?

Ігноруючи вказані суспільні відносини держава створює небезпеку порушення прав та свобод громадян, адже позбавляє можливості захистити їх відповідними правоохоронними органами, які діють виключно в рамках правового поля, в яке не заведені нові суспільні відносини.

Зазначена тематика є новою для правової науки в Україні, утім, деякі науковці (Розовський Б. Г. [4, с. 280–292], Карчевський М. В. [5, с. 17], Конашевич О. І. [6] та інші) вже сьогодні звертають увагу на необхідність відповідного реагування державними органами на новітні загрози, на недопущення ігнорування суспільних процесів та інформаційно-технічного прогресу, що ми спостерігаємо сьогодні.

Для кращого розуміння сутності проблеми, а отже й для пошуку шляхів її вирішення потрібно усвідомити два аспекти.

По-перше, рівень розвитку та можливості сучасних інформаційних технологій дозволяють стверджувати, що ми прямуємо до формування відкритого суспільства. При цьому, у даному випадку, ми маємо на увазі не концепцію Карла Поппера [3], а відкрите суспільство як об'єктивну реальність. Практично кожен громадянин сьогодні знаходиться у віртуальній мережі. Це відбувається незалежно від того, хочемо ми цього чи ні. Залишитися сьогодні поза віртуальною мережею практично неможливо, адже знаходячись ще в утробі матері, інформація про майбутню людину вноситься до різноманітних інформаційних обліків та комп'ютерних систем. Можемо з упевненістю сказати, що у сучасному цивілізованому світі у практично кожній реальній особі є свій віртуальний двійник.

Якщо припустити, що усі системи та мережі об'єднані, то застосування технологій розпізнавання обличчя у поєднанні з активним розповсюдженням відеоспостереження дозволить спостерігати за життям

будь-якого громадянина у режимі реального часу як у фільмі. Такий громадянин стає дійсно відкритий для структур, які контролюють таку систему.

Разом з тим, потрібно уточнити, що зважаючи на вищевказане, називаючи суспільство відкритим ми не ототожнюємо його з суспільством інформаційним, що часто вживається як синоніми. Сам термін «інформаційне суспільство» приписується професору Токійського технологічного інституту Ю. Хаяши [7, с. 62]. Надалі цей термін почали широко застосовувати інші вчені у різних сферах знань.

Деякі вчені визначають інформаційне суспільство у цілому як суспільство, в якому [8, с. 11–12]:

- кожен член суспільства має можливість своєчасно і оперативно отримувати за допомогою глобальних інформаційних мереж повну і достовірну інформацію будь-якого виду і призначення, при знаходженні практично в будь-якій частині географічного простору;

- реалізується можливість оперативної, практично миттєвої комунікації не тільки кожного члена суспільства, а й певних груп населення з державними і громадськими структурами незалежно від місця проживання;

- трансформується діяльність ЗМІ за формою створення і поширення інформації, розвивається і інтегрується в інформаційні мережі телебачення;

- зникають географічні та геополітичні кордони держав в рамках інформаційних мереж, відбувається об'єднання інформаційного законодавства країн.

Розглянуті питання не були залишені без уваги міжнародним співтовариством і знайшли своє відображення в ряді міжнародно-правових актів. Так, наприклад, в Декларації принципів «Побудова інформаційного суспільства – глобальне завдання в новому тисячолітті», прийнятої ООН в Женеві 12 грудня 2003 року, заявлено про наміри держав учасниць побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство [9].

У Хартії глобального інформаційного суспільства [10] вказується, що в інформаційному суспільстві кардинальні зміни відбуваються не тільки в економіці, але і в інших сферах діяльності. Наукове знання, сучасні інформаційні технології, засоби телекомунікації і зв'язку все активніше входять в повсякденне життя людини, істотно змінюючи його. Інформаційне суспільство дозволяє людям ширше використовувати свій потенціал і реалізувати свої наміри, надає нові можливості для пошуку, зберігання, обробки і поширення інформації.

Також, інформаційним суспільством слід вважати [11]:

- суспільство нового типу, яке формується в результаті глобальної соціальної революції і породжується розвитком інформаційних і комунікаційних технологій;

- суспільство знання, тобто суспільство, в якому головною умовою благополуччя кожної людини і кожної держави стає знання, здобуте завдяки вільному доступу до інформації та вмінню працювати з нею;

- глобальне суспільство, в якому обмін інформацією не буде мати ні часових, ні просторових, ні політичних кордонів; яке, з одного боку, сприяє взаємопроникненню культур, а з іншого – відкриває кожному співтовариству нові можливості для самоідентифікації.

Поєднуючи існуючі положення та позиції, окремі науковці, надаючи визначення вказують на взаємозв'язок понять інформаційного та відкритого суспільства. Так, Пастухов П. С. зазначає, що інформаційне суспільство – це відкрите, громадянське суспільство, засноване на вільному доступі до інформації, свободи думок, право прямого голосу, відкритості, толерантності, конкурентності думок і оцінок [12].

Загалом погоджуючись з позиціями науковців зазначимо, що поняття інформаційне та відкрите суспільство відносяться одне до одного як частка й ціле. Тобто відкрите суспільство не може існувати без відповідної інформаційної складової у її сучасному розумінні, з сукупністю систем, програм, та мереж. Разом з тим, інформаційне суспільство стає відкритим тільки тоді, коли формується відкрита громадянська позиція, коли безпека кожного індивіда у суспільстві визнається найвищою цінністю й підтримується усіма. Відкрите суспільство – це ментальна готовність активної поведінки за для суспільної безпеки, у тому числі й застосовуючи сучасні інформаційно-технічні досягнення.

Звісно, завжди існують загрози некоректного чи незаконного використання інформації, отриманої з відповідних систем чи мереж. Але не потрібно забувати й про те, що так само відкриті й злочинці, незаконна діяльність яких буде помітна для правоохоронних органів.

Аналіз останніх публікацій та практики показали, що більша частина цивілізованого світу давно усвідомила важливість та невідворотність впровадження сучасних інструментів аналізу в правоохоронній сфері. *Так, в англійському журналі «Police» опублікована стаття про використання сучасних інформаційних технологій у роботі фінансових слідчих. На початку XXI століття практично кожна особа залишає за собою електронний слід інформації (наприклад, у Великобританії загальна кількість баз даних, де громадяни можуть залишити електронний слід, становить близько трьохсот). Перед слідчими постає завдання зібрати дані з цих баз відносно конкретної особи, потім відфільтрувати з цих відомостей такі, що відповідають параметрам розслідування, тобто, інакше кажучи, перевірити*

отриману інформацію стосовно більш широкого контексту розслідування для того, щоб звести воєдино всі відомості і провести аналіз, згідно з яким необхідно діяти надалі [13, с. 22].

Постійно зростаюча кібернетизація інформаційних потоків зажадала зміни існуючої структури кадрів оперативних працівників. У Скотланд-Ярді (Велика Британія) кількість оперативних працівників-аналітиків перевищує кількість інших («класичних») оперативних працівників у 2,8 разу, а у Федеральному бюро розслідувань (США) – у 4,7 разу. У спецслужбах (Центральне розвідувальне управління, США) цей показник сягає дев'яти.

І це зрозуміло. Проблемаю сьогодення є те, що інформації надто багато: будь-який сучасний сенсор може транслювати мільйони терабайт даних та 5 тис. годин відео високої чіткості за добу. Ця інформація збирається гігапіксельними камерами та сотнями сенсорів. Правильно організований аналіз та візуалізація цих даних дозволять оптимізувати процес інформаційно-аналітичного забезпечення кримінального провадження.

Але щоб отримати користь у всіх цих «горах» терабайтів, потрібні науковці, які спеціалізуються на аналізі даних, за яких поліцейським приходится вступати в конкуренцію з «цивільними» індустріями.

Сьогодні вже існують технології, котрі допомагають автоматично аналізувати величезні масиви текстів, причому проводити не структурний аналіз та пошук ключових слів, а семантичний. Система фактично розуміє зміст текстів. У перспективі цей самий підхід може використовуватись для аналізу відео-та статичного зображення, а також звуку.

Зазначені факти дозволяють стверджувати, що в Україні *розвиток аналітичної розвідки потребує виведення організації й тактики правоохоронної діяльності на якісно новий рівень.*

Для здійснення комп'ютерної розвідки останнім часом застосовують спеціалізовані *розвідувальні комп'ютерні програми*. Завдяки своїм специфічним функціям розвідувальні програми, порівняно з іншими програмами пошуково-аналітичного призначення, дозволяють розширити зону пошуку, зменшити пошуковий термін, виявити латентні зв'язки, підвищити цінність отримуваної інформації. Розвідувальні комп'ютерні програми є найбільш універсальним і тому найбільш застосовуваним інструментом аналітичної розвідки. С.С. Овчинський наголошує на винятково важливій ролі сучасних методів обробки різноманітної інформації для становлення аналітичної розвідки як «самостійного виду діяльності» [14, с. 319].

Як пише О.В. Дем'янчук, комп'ютерні мережі, насамперед Інтернет, усе більш активно використовуються зловмисниками для створення нелегальних ринків збуту зброї, наркотиків, людських органів, порнографічної продукції, вибухових пристроїв, пропозицій щодо надання кілерських «послуг», а також є способом розповсюдження інформації щодо виготовлення саморобних вибухових пристроїв, пропаганди національної ворожнечі й закликів до розв'язання війни [15].

Правоохоронні органи зарубіжних країн широко використовують автоматизовані інформаційно-пошукові системи, які дозволяють значно оптимізувати розкриття та розслідування злочинів, учинених членами організованих угруповань [16]. Але сучасні темпи обміну інформацією та загальний ритм життя, у тому числі й злочинний, змушує постійно удосконалювати методи та способи роботи з постійно зростаючими масивами даних. У цьому процесі незамінними помічниками є інформаційно-аналітичні системи, основною перевагою яких є аналіз та прогнозування.

Більше того, новітні технології дають змогу активно та продуктивно протидіяти транснаціональній злочинності за рахунок відсутності кордонів у глобальній мережі. Значно полегшується взаємодія та обмін даними між правоохоронними органами різних країн. Приміром, розшукуваний злочинець може бути встановлений шляхом застосування однієї з програм ідентифікації особи по фото чи відео зображенню. Такий досвід вже практикується окремими закордонними державними та приватними відомствами [17].

Більше перспектив у використанні новітніх технологій дає космічна галузь. Адже ще в далекому 1962 році М.С. Хрущов, після успішних випробувань в СРСР засобів протиракетної оборони сказав: «Ми можемо поцілити у муху в космосі» [18].

Сьогодні ж, в США розробляється система космічного контролю, яка здатна спостерігати за наземними процесами навіть через хмарність [19]. На орбіту Землі на сьогодні виведено 12 тисяч штучних супутників [20].

В той же час, не відомо жодного факту використання можливостей космічних супутників в цілях правоохоронної сфери. Перш за все це пояснюється технічними можливостями, та фінансовою доцільністю. Але робота у цьому напрямі активно ведеться і вже є перші успіхи у передаванні супутникового зображення у режимі реального часу [21]. За сучасного темпу науково-технічного прогресу, досить швидко з'являться технічні можливості космічного моніторингу в правоохоронних цілях.

По-друге, застаріла система державного управління, так само як і її нормативно-правова база не здатні адаптуватись до стрімкого розвитку інформаційних технологій та суспільства в цілому, що створює значні протиріччя, які не сприяють захисту прав та свобод громадян.

В реальному світі, для задоволення своїх потреб є величезна кількість обмежень та заборон, які відсутні у світі віртуальному. Зокрема, у віртуальній мережі відсутні кордони, нівельовані відстані, мережа позбавлена надмірного правового регулювання тощо.

Чого мережа не позбавлена, так це контролю, який здійснюється відповідним адміністратором, а рівень контрольованості залежить від самого адміністратора, адже він встановлює правила, які будуть діяти у мережі. Таким чином, кожна мережу можна, умовно, порівняти з формою організації суспільства (спілька, громада, держава і т.ін.), як і керівництво нею.

Таким чином, з розвитком мережі, її поширеністю, ускладнюються і форми її регулювання, що з часом може призводити до наслідків, з якими стикаються деякі держави. Вже сьогодні ми є свідками розширення штату юридичних консультантів законодавців, адже постійно множаться правові норми, які потребують свого узгодження з вже існуючими. І чим далі, тим цей процес більше ускладняється. Надмірна зарегульованість веде до неузгодженості законодавства, що, у свою чергу, призводить до порушення прав фізичних та юридичних осіб та до певного хаосу. Надалі, спроби кожного з суб'єктів суспільства захистити лише свої права та свободи, міра для яких у кожного своя, провокують запровадження репресивних засобів зі сторони держави для врегулювання ситуації. Результати таких дій можуть бути різними, від зміни влади чи запровадження авторитарного правління до розпаду держави як такої.

Сучасне інформаційне суспільство, представниками якого ми є, вочевидь потребує такої форми його організації, яка змогла б поєднати як реальну так і віртуальну його сторони. Одним з виходів може бути запровадження технології блокчейн – однорівневої мережі, в якій немає одного виділеного центру і в якій валідність транзакцій гарантується криптоалгоритмом і, відповідно, усіма учасниками мережі.

Блокчейн (англ. blockchain або block chain) – це розподілена база даних, у якій пристрої зберігання даних не підключені до загального серверу. Ця база даних зберігає список упорядкованих записів, що називаються блоками, який постійно зростає. Кожен блок містить мітку часу та посилання на попередній блок. Найчастіше копії ланцюжків блоків зберігаються на незалежно один від іншого обробляються на різних комп'ютерах. Основним принципом функціонування нової технології є прозорість здійснюваних операцій з неможливістю їх зміни особами, які не мають до неї санкціонованого доступу.

Блокчейн-технологія використовує криптографію та цифрові підписи для посвідчення особи: транзакції відслідковуються аж до криптографічних ідентифікаційних даних, які теоретично є анонімними, але можуть бути прикріплені до реальних ідентифікаційних даних після деякого інженерного аналізу.

З зазначеного можна зробити висновок про те, що функція блокчейн технології полягає в реєстрації кожної транзакції з крипто валютою. Будь-яка передача криптовалюти підтверджується в мережі внесенням транзакційного блоку. Блок додається до довгого ланцюжку, котрий дозволяє будь-кому відстежити в мережі зміну власників кожної криптовалюти від моменту створення. Технічно це досягається за допомогою послідовного шифрування даних про кожну чергову транзакцію. Будь-якій угоді, що заноситься в блок присвоюється криптографічний ідентифікатор (хеш), котрий додається в заголовок запису про наступну транзакцію, та це повторюється знов і знов, так що хеш транзакції на вершині ланцюжка містить зашифровані дані про всі попередні транзакції, записані в блоці. Втрутитися та змінити вже записану транзакцію неможна, адже це скомпрометує весь ланцюжок.

Сам факт, що блоки коректно вбудовуються в ланцюг, свідчить про те, що угода пройшла належним чином. Так що блок являє собою одночасно й підтвердження транзакції (з електронним підписом та відміткою про час вчинення), й частину загальної (в масштабах всієї мережі) історії транзакцій. Для ідентифікації в реєстрі володільців криптовалют можливо використання шифрування з відкритим ключем, котрий записується в базу даних. Тільки утримувач закритого ключа вправі далі проводити операції з цими криптовалютами. Так, шифрування забезпечує необхідну конфіденційність, притому, що ухвалити транзакцію може лише володільць закритої половини пари ключів. Таким чином, у користувача є тільки один ключ, й при його незнанні неможливий доступ до первинної інформації.

Розглядувана технологія передачі та зберігання даних стала об'єктом уваги осіб, які вчиняють злочини. В зоні їх особливої уваги опинилась й криптовалюта, котра, по суті, не є засобом платежу в буквальному сенсі, але фактично вже стала сурогатом емітованих платіжним засобів.

Дії, що здійснюються з криптовалютою, не мають конкретного законодавчого регулювання, й ідентифікувати їх злочинні неможна. Марко Стренг характеризує криптовалюти наступним чином:

- неінфляційність;
- подільність;
- тривалість;
- доступність;
- глобальність та, як правило, анонімність;
- відкритий вихідний код;
- одно ранговість;

– децентралізованість.

Однак при вчиненні злочинів в інтернет-просторі криптовалюта виступає засобом вчинення злочину, та використовується в якості платіжного засобу для покупки зброї, наркотичних засобів та інших заборонених предметів, або з метою легалізації злочинних доходів.

Один з найпопулярніших способів обігу криптовалюти в злочинних цілях здійснюється через криптовалютні біржі. Список усіх бірж криптовалют та обмінників біткоїн, Litecoin та їх форків на початок червня 2016 р. містив наступні дані про їх місцезнаходження: США – 25; Німеччина – 8; Росія – 6; Китай – 3; Польща, Велика Британія, Франція, Тайвань – по 2; Казахстан, Британські Віргінські острови, Україна, Канада, Швейцарія, Болгарія, Індія, Нова Зеландія, Австралія, Бельгія – по 1.

Коли мова заходить про правове регулювання біткоїнів та інших криптовалют в Україні (PPCoin або Peercoin), передусім згадують роз'яснення НБУ в Листі від 08.12.2014 № 29-208/72889, який визначає Bitcoin як «грошовий сурогат», що не має забезпечення реальною вартістю й не може використовуватися фізичними та юридичними особами на території України як засіб платежу, оскільки це, на його думку, суперечить нормам українського законодавства.

Якщо ж розглядати Закон України «Про платіжні системи та переказ коштів в Україні» від 18.09.2012 № 2921-14, електронні гроші – це одиниці вартості, що зберігаються на електронному пристрої, приймаються як засіб платіжними іншими особами, аніж тим, хто їх випускає, і є грошовим зобов'язанням у готівковій або безготівковій формах. Випуск електронних грошей може здійснювати виключно банк, на якого покладаються обов'язки з їх погашення.

Через свої технології Bitcoin і не потрапляє під українське визначення поняття «електронні гроші», оскільки не містить зобов'язання емітента з його погашення, не має єдиного емісійного центру, не прив'язаний до жодних готівкових чи безготівкових коштів. У свою чергу, «безготівкові кошти», за українським законодавством, можуть існувати виключно у формі записів на банківських рахунках. Банки не беруть участі у процесі емісії та обігу криптовалют, тому Bitcoin не може вважатися «коштами». Не потрапляє Bitcoin і під визначення «платіжна система», оскільки основною та обов'язковою функцією платіжної системи є проведення переказу коштів, тоді як через електронний гаманець здійснюється переказ виключно Bitcoin, який, коштами не є.

Для з'ясування правової природи Bitcoin важливо звернути увагу на те, що в Законі України «Про Національний банк України» від 20.05.1999 № 679-14 визначено, що грошовий сурогат – це будь-які документи у вигляді грошових знаків, що відрізняються від грошової одиниці України, випущені в обіг не НБУ й виготовлені з метою здійснення платежів у господарському обігу. Водночас ознаки криптовалюти не підпадають під поняття «електронний документ», оскільки під останнім розуміється документ, інформація в якому зафіксована у вигляді електронних даних, ураховуючи обов'язкові реквізити документа.

Таким чином, слід погодитись з думкою науковців, що поняття криптовалюти не визнається грошовим сурогатом, а діяльність із приводу використання Bitcoin під час оплати послуг в Україні є інноваційною, відповідне законодавче врегулювання та чітке визначення статусу криптовалюти як такої повністю відсутнє.

Разом з тим, технологія, за час існування з 2009 року, жодного разу не стала жертвою взлому чи іншого несанкціонованого впливу [22].

Якщо ж зберігати інформацію у блокчейн, то інформація стає невразливою до зовнішнього втручання. Крім того, відпадає потреба у посередництві, яка є основою державного впливу.

Вказана технологія активно впроваджується у розвинених країнах світу. Так, сучасна Швейцарія – це рідкісний приклад країни з інструментами прямої демократії. Безпосередньо громадяни можуть пропонувати зміни до будь-якого закону чи навіть Конституції [23].

Ми згодні, що в цивілізованій правовій державі особистість, її інтереси, права та свободи мають бути найвищою цінністю. Проте, як би ми не звеличували особистість, вона була, є й залишиться часткою суспільства. А отже, інтереси особистості не можуть протиставлятися інтересам суспільства, що ми спостерігаємо сьогодні.

У сучасних реаліях неприпустима невинуватена конкуренція демократії і безпеки особи, суспільства. Як відзначають дослідники, «безпека – складне соціальне явище, що суперечливим чином відображає відносини різних соціальних суб'єктів. Часто, одні з них прагнуть забезпечити свою безпеку за рахунок інших або у своїй діяльності не беруть до уваги інтереси інших соціальних груп і їх потребу в безпеці. Мову в такому разі слід вести про своєрідний «соціальний егоїзм», який якщо й був відносно терпимий у попередні епохи, то в епоху наростаючої глобалізації сам починає ставати серйозною загрозою»... Протиставлення безпеки особи і безпеки соціальної безпеки взагалі, як правило, виникає в історично конкретних обставинах, пов'язаних, як не дивно, з відносно стабільними і безпечними періодами розвитку того чи іншого суспільства. Події 11 вересня 2001 року чудово це підтверджують, оскільки до цього дня США достатньо довго не знали серйозних проблем у забезпеченні безпеки, через що в громадській думці

цінність безпеки, що сприймається як даність, відсунулася на другий план. Закономірно, що в певний момент уявлення, що безпека перешкоджає свободі особи, змінилося уявленням про безпеку як про необхідну умову свободи» [24, с. 102–105]. Крім того, вузьконаправлена оцінка громадянином своїх прав і свобод, при безперечному їх пріоритеті, але поза інтересами суспільства, неприпустима [25, с. 350-355].

Щоб проілюструвати принцип роботи технології блокчейн можна привести наглядний приклад. Уявімо, що у великому залі (відповідній мережі) присутні багато людей, які одночасно спостерігають за тим, як дві особи обговорюють умови договору між собою і підписують контракт. Усі бачать, як учасники переговорів досягають згоди і поміщають підписаний контракт до скляного блоку, який закривається та опломбовується підписами усіх присутніх. Після закриття блок неможливо відчинити, проте можна з нього читати. Будь-які дії у кімнаті відразу видні усім учасникам, а невиконання умов відразу стає відомим усім учасникам мережі. При цьому, будь-які дії з запакованим контрактом фіксуються в автоматичному режимі і так само поміщуються у блок, поверх того, який вже є і так само підтверджується усіма учасниками, у жодного з яких немає адмініструючих прав.

А тепер цей примітивний приклад помножте на можливості комп'ютерних систем та програм з обробки даних та отримаєте приблизне уявлення про принцип роботи технології блокчейн, який, разом з тим, є надзвичайно важливим для розвитку відкритого інформаційного суспільства.

Сьогодні ми є свідками монополізації та локалізації певних інформаційних ресурсів. Більшість баз даних належить державі, яка встановила монополію на їх використання, аргументуючи це необхідністю їх захисту та надаючи, нібито, гарантії такого захисту.

В той же час, будь-яку базу даних можна зламати та добути конфіденційну інформацію або спотворити її. Системи захисту створюються людьми, а тому й люди можуть їх зламати. Так, нещодавно інформаційні системи усього світу стали об'єктом нападу вірусу Petya.A, найбільше від якого постраждали інформаційні системи України. Паралізувалась робота багатьох державних органів та установ, так само як і більшості державних банків. На цьому фоні курс біткойна тільки виріс, а сама технологія, за час існування з 2009 року, жодного разу не стала жертвою злому чи іншого несанкціонованого впливу [22]. Можна навести й інші приклади витоку конфіденційної інформації, зокрема в Індії:

- Reliance Jio (2017) – виток даних 120 мільйонів клієнтів;
- Aadhaar (2017) – 210 урядових сайтів зробили конфіденційну інформацію загальнодоступною.

Якщо ж зберігати інформацію у блокчейн, то інформація стає невразливою до зовнішнього втручання. Крім того, відпадає потреба у посередництві, яка є основою державного впливу. Адже, у разі покупки транспортного засобу договір потребує нотаріального посвідчення, а факт підтвердження володіння потребує реєстрації у сервісному центрі МВС. У разі ж фіксування інформації за допомогою блокчейн у формі токена (цифрового вираження будь-якого матеріального чи нематеріального об'єкта) посередники не потрібні.

У невеликих суспільних групах така система діє постійно і не викликає жодних запитань. У сім'ї діти не вимагають від батьків щоразу показувати їм документи, щоб підтвердити своє батьківство, або учні в класі не змушені щотижня підтверджувати, що вони саме з цього класу.

Якщо ж група збільшується, наприклад, до величини міста чи області, то навіть такі елементарні питання як підтвердження статусу породжують складнощі. Для зарахування на роботу потрібно надати документи про освіту, підтвердити родинні зв'язки, судимість чи її відсутність і т. ін.

Технологія блокчейн, разом з всеохоплюючою інформатизацією та автоматизацією суспільства робить його з однієї сторони максимально відкритим, з другої – надзвичайно захищеним.

У разі, коли все відкрите, то його надзвичайно складно вкрати. Як непомітно взяти щось зі столу, коли цей стіл посеред кімнати й усі навкруги на нього дивляться? Це неможливо.

Запровадження принципу технології блокчейн на загальнодержавному рівні, безумовно має беззаперечні переваги. Але чи готове суспільство до таких змін ментально? Гадаємо що ні.

Сучасний рівень корупційності та олігархізації державного апарату не дозволить запровадити подібну технологію. Адже, навіть заповнення елементарних електронних декларацій державними службовцями не можуть забезпечити вже протягом року. В Україні не існує єдиного інформаційного центру, який би дав змогу відстежувати фінансові потоки громадян, щоб контролювати рівень незаконного збагачення чиновників. Навіть елементарні бази даних правоохоронних органів не мають єдиного скоординованого центру. Що вже говорити про зміну технології накопичення та обробки інформації.

Але існує надія на більш розвинені держави. Успішне запровадження технології блокчейн на державному рівні хоча б деякими країнами буде мотивувати інших.

Зокрема, шлях яким розвивається Швейцарія дуже надихає. Так, сучасна Швейцарія – це рідкісний приклад країни з інструментами прямої демократії. Безпосередньо громадяни можуть пропонувати зміни до будь-якого закону чи навіть Конституції. З 521 референдумів, в 216 випадках предметом голосування була ревізія Конституції і, в 148 - предметом були закони. випадках прийняття законопроекту або

схвалення будь-якого договору. Народ теж не пасе задніх, дві сотні референдумів ініціював саме звичайний швейцарець. Для народної ініціативи, за швейцарською Конституцією, необхідно 100 000 підписів громадян. Предметом може бути, зокрема, перегляд Основного закону. Додатково, швейцарці можуть використовувати право на факультативний референдум. Він стосується міжнародних угод, рішень федерального рівня, вступ до союзів та міжнародних організацій. Для цього треба підтримка ініціативи з боку 50000 чоловік або 8 кантонів [23].

Більше того, саме Швейцарія є країною, яка намагається йти у ногу з часом і свої інструменти прямої демократії перевести у цифровий формат, що має назву електронної прямої демократії (ЕПД) або прямої цифрової демократії (ПЦД)[26]. Електронну пряму демократія іноді називають такими термінами, як управління відкритого коду чи спільне управління [27].

Поки що це експериментальна система і повністю ще не реалізована, у більшості випадків застосовується як інноваційні грантові проекти[28], але цей процес набирає обертів, а технологія блокчейн значно розширює горизонти для застосування такої системи.

Крім Швейцарії й інші країни стали на шлях цифрової демократії: Австралія, Швеція, Великобританія, Індія. Зокрема, першою основною партією прямої демократії, яка була зареєстрована у виборчій комісії якоїсь країни є британська партія Народна Адміністрація Прямой Демократії (*People's Administration Direct Democracy Party*) [29]. Ця партія розробила і опублікувала повну схему законодавчого впровадження реформи ЕПД. Заснована музикантами і політичними активістами, Народна Адміністрація виступає за використання Інтернету та телефонії для забезпечення більшості виборців можливостями створювати, пропонувати і голосувати з усіх політичних питань. Проект Народної Адміністрації публікувався в різних формах починаючи з 1998 року. Народна Адміністрація – є першою у світі партією прямої демократії, зареєстрованою у форматі, що дозволяє голосувати.

Є перші невеликі кроки й в Україні. Першим напрямом використання технології блокчейн є електронні аукціони eAuction 3.0, які сьогодні тестуються у Білій Церкві, Одесі та Херсоні[30]. Зокрема, мер Білої Церкви Геннадій Дикий зареєстрував проект рішення щодо запровадження eAuction [31].

Більше того, розпочались обговорення застосування технології на платформі блокчейн (e-Vox) для організації та проведення виборів [32].

Отже, нагальною потребою є комплексне рішення, котрі для застосування правил використовує технології без втручання людини та забезпечує:

- захист від внутрішніх зловмисників, які умисно спотворюють дані;
- захист від несанкціонованого зовнішнього втручання;
- механізм отримання згоди людей на кожне використання їх персональних даних.

Висновки. Проте, будучи реалістами, змушені констатувати, що запровадження нових технологій у вітчизняних державних структурах є на вкрай низькому рівні. Навіть давно використовувані у інших країнах прийоми та способи застосування інформаційних технологій не застосовуються в правоохоронних цілях. Основна проблема, яка сьогодні не дозволяє застосувати технологію блокчейн та розроблені на її основі програми у державному управлінні – це відсутність нормативно-правової бази [33].

Надія тільки на те, що стрімкий розвиток інших держав не дозволить в Україні ігнорувати новітні технології, і ми будемо розвиватися, хоч з певним запізненням.

References:

1. Zhmudyak L.M., Zhmudyak A.L. Programma diagnostiki zabolevaniy. URL: <http://www.swsys.ru/index.php?page=article&id=2341>. (accessed 19.07.2020). (In Russian).
2. Obzor: IT v zdravookhraneniі 2014. URL: http://www.cnews.ru/reviews/publichealth2014/articles/po_pomogaet_povysit_kachestvo_meditinskoy_diagnostiki (accessed 15.12.2019). (In Russian).
3. Popper K. Otkrytoye obshchestvo i yego vragi. T. 1: Chary Platona. Per. s angl., pod red. V. N. Sadovskogo. M.: Feniks, Mezhdunarodnyy fond «Kul'turnaya initsiativa», 1992. 448 p. (In Russian).
4. Rozovskyy B.H. Pravo kak kletka v zveryntse. Visnyk Luhans'koho derzhavnoho universytetu vnutrishnikh sprav imeni E.O. Didorenka. 2017. № 1. P. 280-292. (In Ukrainian).
5. Karchevs'kyi M.V. «Klasychni» ta novitni problemy kryminal'no-pravoho rehulyuvannya u sferi informatyzatsiyi. Aktual'ni pytannya kryminal'noho prava, protsesu i kryminalistyky, udoskonalennya diyal'nosti sudovoyi i pravookhoronnoyi system : mater. Vseukr. nauk.-prakt. konf. (m. Syevyerodonets'k, 19 travn. 2017 r.). Syevyerodonets'k : Luhan. derzh. un-t vnutr. sprav im. E.O. Didorenka, 2017. P. 11–19. (In Ukrainian)
6. Konashevych O.I. Pravovi pidstavy dlya realizatsiyi posluh ta tovariv za bitcoiny URL: http://jurliga.ligazakon.ua/blogs_article/725.htm (accessed 25.02.2020). (In Ukrainian).
7. Izmaylova Ye.V. Informatsiya v kommercheskikh otnosheniyakh. Vestnik Moskovskogo universiteta. Ser. 11: Pravo. 2005. № 1. P. 62–79. (In Russian).

8. Kristal'nyy B. Informatsionnoye obshchestvo, informatsionnaya politika, pravovaya informatsionnaya zashchita. Informatsionnoye obshchestvo. 1997. № 1. P. 9-12. (In Russian).
9. Deklaratsiya printsipov «Postroyeniye informatsionnogo obshchestva – global'naya zadacha v novom tysyacheletii» ot 12 dekabrya 2003 goda. URL: http://zakon4.rada.gov.ua/laws/show/995_c57 (accessed 14.03.2020). (In Ukrainian).
10. Okinavskaya Khartiya global'nogo informatsionnogo obshchestva ot 22 iyulya 2000 goda URL: http://www.conventions.ru/view_base.php?id=13180 (accessed 29.05.2020). (In Russian).
11. White Paper on growth, competitiveness and employment – the challenge and ways forward into 21st century // European Commission. Belgium, 1993. 54 p. (In Russian).
12. Pastukhov P.S. Modernizatsiya ugovovno-protsessual'nogo dokazyvaniya v usloviyakh informatsionnogo obshchestva. Spetsial'nost: 12.00.09: avtoref. dis. na soisk. uchenoy stepeni d.yu.n. M., 2015. 65 p. (In Russian).
13. Police. 2001. September. P. 24–27. Vyyavleniye prestupnikov s pomoshch'yu informatsionnykh tekhnologiy. Bor'ba s prestupnost'yu za rubezhom. Informbyulleten'. M.: VINITI, 2003. № 6. C. 19–23. (In Russian).
14. Ovchinskiy S.S. Operativno-rozysknaya informatsiya. Teoreticheskiye osnovy informatsionno-prognosticheskogo obespecheniya operativno-rozysknoy i profilakticheskoy deyatelnosti organov vnutrennikh del po bor'be s organizovannoy prestupnost'yu. M.: INFRA-M, 2000. 367 p. (In Russian).
15. Dem'yanchuk E.V. Monitorynh sety Ynternet kak meropryyatye, provodymoe s tsel'yu poluchenyya operativno znachymoy ynformatsyy. Spetsial'na tekhnika u pravookhoronniy diyal'nosti: materialy II mizhnarodnoyi naukovo-praktychnoyi konferentsiyi. K.: Kyiv's'kyy nats. un-t vnutrishnikh sprav, 2006. C. 171–178. (In Ukrainian).
16. Khirsin A.B. Udoskonalennya avtomatyzovanykh informatsiyno-poshukovykh system, yaki vykorystovuyut'sya u borot'bi z orhanizovanoyu zlochynnistyuu. Pravo Ukrayiny. № 6. 2004. P.55–60. (In Ukrainian).
17. Poisk cheloveka po fotografi – eto real'nost'. URL: <http://softopirat.com/main/399-poisk-cheloveka-po-fotografii-yeto-realnost.html>. (accessed 15.03.2020). (In Russian).
18. The New York Times, July 17, 1962. (In English).
19. Armiya SSHA polnost'yu zavisit ot sputnikov. URL: <http://www.dsnews.ua/future/kak-pentagon-gotovitsya-k-novoy-kosmicheskoy-voyne-11052016224400> (accessed 24.04.2020). (In Ukrainian).
20. 12 tysyach kosmicheskikh sputnikov pod kontrolem. Rossii ne strashny zvezdnyye voyny. URL: <http://tvzvezda.ru/news/forces/content/201503051818-pdbu.htm>. (accessed 15.03.2020). (In Russian).
21. Planeta Zemlya v real'nom vremeni. URL: <http://www.infokart.ru/planeta-zemlya-v-realnom-vremeni> (accessed 15.03.2020). (In Russian).
22. Podobriy O. V bitkoinakh yest' odin negativnyy moment – uchenyy iz Italii. URL: <https://www.obozrevatel.com/finance/business-and-finance/19048-bitkoinyi.htm> (accessed 15.03.2020). (In Ukrainian).
23. Ivanov V. U Shveytsariyi za 150 rokiv provedeno bil'she 500 referendumiv: bloh Vladymyra Yvanova. URL: http://blogs.lb.ua/vladimir_ivanov/159889_shveytsarii_150_rokiv_shveytsarii.html (accessed 29.03.2020). (In Ukrainian).
24. Mozdakov A.YU. Sotsial'naya bezopasnost' i bezopasnost' lichnosti. Gosudarstvo i pravo. 2008. № 6. P. 102–105. (In Russian).
25. Rozovskyy B.H. Protyvoprestupnoe pravo: popytka synerhyi mer pravovoho rehulyrovannya. Kryminal'nyy kodeks Ukrayiny: 10 rokiv ochikuvan': Tezy dopovidey ta povidomlen' uchasnykiv Mizhnarodnoho sympoziumu 23-24 veresnya 2011 r. L'viv: L'viv's'kyy derzhavnyy universytet vnutrishnikh sprav, 2011. P. 350–355. (In Ukrainian).
26. Jan A.G.M. van Dijk. Digital Democracy: Vision and Reality. / Jan A.G.M. van Dijk, // I. Snellen & W. van de Donk 'Public Administration in the Information Age: Revisited', IOS- Press, 2013. p. 49–63. (In English).
27. Open Governance and the Definition of e-Democracy. URL: <http://www.gov2u.org/index.php/blog/128-open-governance-and-the-definition-of-edemocracy> (accessed 23.05.2020). (In English).
28. Electronic Voting in Switzerland URL: http://web.archive.org/web/20070212194901/www.swissworld.org/dvd_rom/eng/direct_democracy_2004/content/votes/e_voting.html (accessed 14.04.2020). (In English).
29. Direct Democracy URL: <http://www.paparty.co.uk>. (accessed 22.03.2020). (In English).
30. V Kiyeye podpisan istoricheskij Memorandum o zapuske blokcheyn-platformy e-Auction 3.0. URL: <http://forklog.com/v-kieve-podpisan-istoricheskij-memorandum-o-zapuske-blokcheyn-platformy-e-auction-3-0/> (accessed 14.04.20). (In Ukrainian).
31. V Beloy Tserkvi sostoyalis' torgi na e-Auction 3.0 URL: <https://bitcoinconf.com.ua/ru/news/v-beloy-tserkvi-sostoyalis-torgi-na-eauction-3-0-52509> (accessed 14.04.20). (In Ukrainian).
32. Blokcheyn-servis elektronnykh petitsiy e-Vox otobran dlya uchastiya v inkubatore EGAP. URL: <http://forklog.com/blokcheyn-servis-elektronnyh-petitsiy-e-vox-otobran-dlya-uchastiya-v-inkubatore-egap/> (accessed 14.04.20). (In Russian).
33. Bitcoin protiv byurokratii: kak Ukraina perekhodit na blokcheyn URL: <https://ain.ua/2016/09/14/bitcoin-protiv-byurokratii-kak-ukraina-perexodit-na-blokcheyn> ((accessed 14.04.20). (In Ukrainian).

Влияние информационных технологий на обеспечение прав и свобод человека в условиях открытого общества

Бочковой Алексей Васильевич, e-mail: bochkin.0583@gmail.com

Днепропетровский государственный университет внутренних дел, г. Днепр, Украина

Ханькевич Андрей Николаевич, e-mail: a.n.khankevich@gmail.com

Харьковский национальный университет внутренних дел, г. Харьков, Украина

Аннотация: Статья посвящена влиянию развивающихся технологий на общество, права и свободы человека, что вызывает пересмотр существующего отношения к внешнему миру. Интенсивность появления новых форм организации социальных отношений (социальные сети, виртуальная реальность, робототехника, блокчейн и т.д.) усложняет адаптацию к ним существующих социальных институтов. Такая ситуация приводит к множеству противоречий как в нормативной сфере, так и среди населения. Определено, что опасность новейших технологий состоит в том, что не сформированы правила поведения и, следовательно, не сформирован институт ответственности за их нарушение. В статье дан анализ указанной проблемы и возможные пути ее решения с целью повышения эффективности защиты прав граждан.

Ключевые слова: информационные технологии, открытое общество, права граждан, защита, безопасность, большие данные.