УДК 141.7:004.9:342.7
DOI https://doi.org/10.24195/spj1561-1264.2026.2.10

Філімонов Володимир Володимирович
аспірант кафедри філософських, політичних і психологічних студій
Черкаського державного технологічного університету
бульв. Шевченка, 460, Черкаси, Україна
orcid.org/0009-0000-7934-4057

ЦИФРОВА СВОБОДА ТА ЗАХИСНИЙ ПРОФАЙЛІНГ: ВЕРИФІКАЦІЯ ВІКУ ЯК ДИСПОЗИТИВ НАГЛЯДУ

Актуальність проблеми: *концепції захисного профайлінгу у вимірі подвійного диспозитиву потребують доповнення крізь оптики алгоритмічного контролю. Контролю над даними потребує поглиблення через розгляд захисного профайлінгу як онтополітичного акту на основі ідей М. Фуко, Ж. Дельоза та Ш. Зубофф. У цьому контексті актуальним стає уточнення поняття цифрових свобод через виявлення внутрішнього парадоксу: розширення захисту дітей пов'язане зі звуженням приватності у цифровому середовищі, зменшенню ролі автономії та автентичності всіх користувачів.*

Мета дослідження: *обґрунтувати концепцію захисного профайлінгу як подвійного диспозитиву, в якому збір і обробка персональних даних, легітимовані цілями захисту дітей, структурно відтворюють логіку капіталізму нагляду та формують нормативний прецедент для ширшого регулювання цифрової активності.*

Методи та результати дослідження: *основу становлять концепція диспозитиву М. Фуко, психополітика Б.-Ч. Хана, теорія капіталізму нагляду Ш. Зубофф і поняття дивідуума Ж. Дельоза; емпірично дослідження спирається на компаративний аналіз законодавчих режимів вікової верифікації у трьох юрисдикціях. Застосовано концептуальний аналіз, критичну теорію та порівняльно-правовий підхід включно з бібліографічним аналізом.*

Показано, що вікова верифікація є не технічним, а онтополітичним актом, який конституює фізичного субє'кта через його відображення – цифрового суб'єкта через зовнішнє знання та переносить індивідуальний цифровий суверенітет до двох акторів – бізнесу і держави лишаючи громадянське суспільство поза межами впливу. Відтак, перед громадянським суспільством постають ризики набуття рис пасивного реципієнта зануреного у стан перманентного зовнішнього контролю. Виявлено спільну логіку нормативного дрейфу від цільового захисту до потенційного масового контролю, де захист чи контроль делегується суспільством до державних та комерційних акторів. Виявлено також внутрішній парадокс захисного профайлінгу: розширення захисту дітей у цифровому середовищі структурно пов'язане зі звуженням цифрової свободи всіх користувачів у трьох її вимірах – приватності, автономії та автентичності.

Ключові слова*: цифрова свобода, верифікація віку, профайлінг, капіталізм нагляду, алгоритмічний контроль.*

Вступ. У цифрову епоху свобода людини щораз частіше визначається не лише правовими гарантіями, а й архітектурою інфраструктур даних. Вони неекспліцитно структурують можливості дії, видимості й анонімності користувачів цих інфраструктур. Одним із найпоказовіших прикладів такої інфраструктурної трансформації є запровадження обов'язкової верифікації віку, що позиціонується як інструмент захисту дітей, але водночас створює умови для систематичного збору, агрегування та аналізу персональних даних. У цьому контексті цифрова свобода

набуває додаткових аспектів балансування між обіцянкою безпеки та розширенням механізмів нагляду, де кожен акт «захисту» потенційно вбудовує нові канали контролю.

Стаття розглядає верифікацію віку не як нейтральний технічний інструмент, а як диспозитив нагляду, в якому логіка захисту поєднується з логікою профайлінгу та алгоритмічного контролю. Спираючись на концепції М. Фуко, Ш. Зубофф, Ж. Дельоза та Б.-Ч. Хана, ми аналізуємо, як практики захисного профайлінгу конституюють статус цифрового суб'єкта, перетворюючи його на «дивідуума», чия свобода визначається параметрами вбудованих систем оцінювання та допуску. Особливу увагу приділено тому, як у правових моделях верифікації віку у демократичних державах – зокрема у Великій Британії, Бразилії та Каліфорнії – захисні норми формують інфраструктурні передумови розширення капіталізму нагляду та зумовлюють нову конфігурацію цифрових прав і свобод.

Профайлінг як онтополітичний акт

Від суб'єкта до дивідуума

Щоб зрозуміти, чому профайлінг є філософською, а не лише технічною проблемою, необхідно звернутися до питання про суб'єкт. Класична філософська традиція розуміє суб'єкт як цілісну, автономну особу – *in-dividuum*, неподільний. Дельоз, аналізуючи суспільства контролю, що прийшли на зміну дисциплінарним суспільствам Фуко, запропонував поняття дивідуума: «Individuals have become "dividuals", and masses, samples, data, markets, or "banks"» [14, с. 5] . Дивідуум – суб'єкт, що може бути розкладений на набір атрибутів, поведінкових патернів і числових параметрів; саме числовий код, а не ім'я чи підпис, стає ключем доступу в суспільстві контролю.

Цифровий профіль є матеріалізацією дивідуума. Коли система зустрічає користувача, вона зустрічає не людину, а сукупність даних: вік, місцезнаходження, пристрій, час активності, пошукові запити, патерни взаємодії з контентом. Профіль репрезентує людину для системи – але ця репрезентація завжди є редукцією: вона відбирає певні виміри існування і залишає інші поза увагою.

Цей процес має онтологічний вимір: людина переводиться в іншу систему буття, де вона набуває нових властивостей і нових вразливостей. Кулдрі та Мехіас визначають цей процес як датафікацію – кількісне вираження людського буття через цифрову інформацію, яке дуже часто має на меті отримання економічної вартості [10]. Датафікація є не просто технічним процесом збору інформації, а фундаментальною зміною онтологічного статусу суб'єкта.

Влада-знання і конституювання суб'єкта

Для Фуко влада й знання утворюють єдиний контур: не можна здійснювати владу без знання, так само як неможливо, щоб знання не породжувало владні ефекти. [15, с. 51–52]. Клінічна медицина, психіатрія, кримінологія – кожна з цих дисциплін конституювала своїх суб'єктів через систематичне знання про них: «хворий», «божевільний», «злочинець» – це не просто описові категорії, а нормативні конструкти, що визначають, що є нормою, а що підлягає корекції.

У цифровому контексті цей механізм відтворюється з новою ефективністю. Алгоритмічні системи збирають безпрецедентно детальне знання про користувачів і на основі цього знання здійснюють владні акти: визначають, яку інформацію показати, який контент рекомендувати, до якого типу доступу надати. Верифікаційна система не просто описує вік користувача – вона конструює категорію «неповнолітній» як юридично та технічно значущу, а отже – підпорядковану. Сахакян та співавтори підкреслюють, що на відміну від дисциплінарних суспільств Фуко, де нормування відбувалося після вчинку, цифровий контроль є передбачувальним: він діє до нього, формуючи поведінкові можливості ще до моменту вибору [9].

Профіль як «зовнішнє Я»: проблема автентичності

Лейєнбергер вказує на ще один вимір профайлінгу – його вплив на самопізнання та автентичність: алгоритмічний профайлінг формує концепції та норми, що визначають суб'єкта [8]. Цифровий профіль починає впливати зворотно на суб'єкта: людина поступово підлаштовується під свій цифровий образ – чи принаймні той образ, який пропонує їй система.

Тут виникає зв'язок із тим як Поль Рікер розрізнює *idem-identity* (тотожність – хто я є незмінно) та *ipse-identity* (самість – ким я стаю у відношенні до Іншого) [16, с. 2, 116]. Цифровий

профіль претендує на *idem* – фіксує і «заморожує» суб'єкта як певний тип. Але насправді він здійснює примусову *ipse*: нав'язує суб'єкту образ себе, сформований зовнішнім актором і зовнішніми цілями. Автентичне самовизначення стає проблематичним у ситуації, коли алгоритм вже «знає», ким ти є, і відповідно формує твоє інформаційне середовище.

На підставі розглянутих концепцій профайлінг можна розглядати як онтополітичний акт – процес конституювання суб'єкта через зовнішнє знання про нього, при якому влада над цим знанням визначає владу над суб'єктом. Профайлінг не лише описує – він виробляє певний тип суб'єктності.

Диспозитив верифікації: порівняльний аналіз законодавства

Поняття диспозитиву і його застосування

Для аналізу законодавства про верифікацію віку продуктивним є поняття диспозитиву за Фуко, як «гетерогенного ансамблю, що охоплює дискурси, інститути, архітектурні форми, регуляторні рішення, закони, адміністративні заходи, наукові висловлювання, філософські та філантропічні пропозиції» (переклад наш) [15, с. 194–196] . Ключовою ознакою диспозитиву є його стратегічна функція: він є відповіддю на певну термінову суспільну потребу, проте не вичерпується нею – функція диспозитиву може трансформуватися і розширюватися незалежно від початкових намірів.

Застосовуючи це поняття до верифікації віку, ми можемо описати її як диспозитив, що включає: юридичні норми (закони про верифікацію), технічні засоби (системи ідентифікації), інституційних акторів (платформи, регулятори, батьківство), дискурсивні формації (захист дітей, цифрова безпека) та потенційно – практики розширеного нагляду. Принципово важливо, що диспозитив верифікації не є нейтральним інструментом: він несе в собі певну стратегічну логіку з структурним потенціалом до трансформації.

Велика Британія: Online Safety Act 2023

У 2023 році парламент Великобританії ратифікував Online Safety Act – закон, спрямований на захист неповнолітніх від шкідливого контенту в мережі [2]. Основний механізм – верифікація віку для обмеження доступу до забороненого для дітей контенту: реклами алкоголю, тютюну, азартних ігор, а також певних категорій сексуального контенту. Відповідальність за верифікацію покладається на виробників і постачальників контенту.

Філософськи значуща ознака британського підходу – розмитість технічних вимог при чіткості правових наслідків. Закон зобов'язує платформи «вжити розумних заходів» для верифікації віку, не визначаючи конкретного технічного методу. Це відкриває простір для конкурентних рішень – від верифікації через кредитні картки до біометричних методів – кожне з яких має різні наслідки для приватності. Важливо, що закон не забороняє комерційного використання зібраних вікових даних, залишаючи відкритим питання про те, чи не стане верифікаційна система основою для побудови детальних цифрових профілів.

Бразилія: «Цифровий статут для дітей та підлітків» 2025

У жовтні 2025 року Міністерство прав людини і громадянства Бразилії затвердило «Цифровий статут для дітей та підлітків» – документ, що зобов'язує розкривати вікові дані для доступу до широкого кола IT-продуктів: додатків, програм, ігор з інтернет-з'єднанням [3].

Бразильський документ вирізняється спробою встановити баланс: комерційний профайлінг неповнолітніх прямо заборонено [3, с. 26, 30]. Проте заборона є вужчою, ніж може здатися: дозволеними залишаються передача, зберігання та інші форми обробки даних, прив'язаних до персональних акаунтів і акаунтів батьківського контролю. Таким чином, хоча пряме комерційне використання вікових даних заборонено, інфраструктура для їх збору і зберігання залишається легальною. Механізм батьківського контролю піднімає окреме питання: цифрова ідентичність дитини конструюється через призму іншого суб'єкта, що фактично підриває декларований суверенітет дитини над власними даними.

Каліфорнія: Assembly Bill 1043 (2026)

Найбільш радикальним кроком у напрямку системної верифікації є Assembly Bill 1043, що набув чинності у Каліфорнії у березні 2026 року. Закон запроваджує обов'язковий збір вікової

інформації на рівні операційної системи: ОС запитує вікову групу користувача та передає ці дані сервісам за запитом [4].

Значення цього кроку важко переоцінити. Попередні підходи передбачали верифікацію на рівні окремих платформ. Каліфорнійський закон переносить верифікацію на рівень базової цифрової інфраструктури: вік стає постійним атрибутом цифрової ідентичності, вбудованим у саму архітектуру взаємодії з пристроєм. Це структурно нагадує те, що вже відбувається в екосистемах великих технологічних компаній: маємо прецедент інтегрування користувача в екосистему з автоматичною передачею поведінкових даних на рівні операційної системи [5]. Каліфорнійський закон юридично легітимізує цю архітектуру.

Логіка нормативного дрейфу

Порівняльний аналіз трьох юрисдикцій дозволяє виявити спільну траєкторію нормативного дрейфу. Усі три випадки об'єднує вектор руху: від захисту конкретного суб'єкта (неповнолітнього) – до збору даних про всіх користувачів; від верифікації у конкретному контексті взаємодії – до верифікації як постійного атрибута цифрової ідентичності; від заборони певного контенту – до контролю над архітектурою доступу взагалі.

Цей дрейф є структурним наслідком самої логіки захисного механізму: для того, щоб захистити неповнолітнього від певного контенту, система повинна знати або визначити хто є неповнолітнім. Але в мережі неможливо визначити вік без збору даних, чи аналізу поведінки, а значить, захист автоматично передбачає профайлінг. Захисна мета і наглядові засоби нерозривно пов'язані.

Захисний профайлінг як диспозитив

Визначення поняття

На основі проведеного аналізу можна сформулювати поняття захисного профайлінгу як, процесу систематичного збору, обробки та зберігання персональних даних, що здійснюється в рамках законодавства, спрямованого на захист прав певної уразливої групи, але структурно відтворює механізми нагляду, застосовувані у комерційному та державному контролі.

Поняття «захисний» стосовно профайлінгу справді реалізує захисну функцію стосовно неповнолітніх. Але ця захисна функція є лише однією складовою диспозитиву – і, як показує аналіз Фуко, первісна функція диспозитиву не вичерпує його стратегічний потенціал. Диспозитив є «відповіддю на термінову потребу», але за своєю природою здатний до розширення і трансформації.

Парадокс захисту через нагляд

Центральним філософським питанням є парадокс: як захист свободи одних суб'єктів стає загрозою свободи всіх?

Масьєро описує цей парадокс у контексті систем цифрової ідентичності: вони ставлять користувача перед бінарним вибором – або реєструйся й потрапляй під профайлінг, або відмовляйся від базових послуг [11]. У контексті верифікації віку цей вибір набуває особливого характеру: неповнолітній опиняється в ситуації, де захист від небажаного контенту є умовою включення до цифрового суспільства – але ціна цього включення є якраз те, від чого намагаються захистити: видимість, відстежуваність, вразливість до маніпуляції.

Проте парадокс виходить за межі становища неповнолітнього. Для верифікації неповнолітніх система повинна верифікувати всіх, або аналізувати всіх – адже не можна відрізнити неповнолітнього від повнолітнього без перевірки обох. На нашу думку, захист конкретної групи технічно передбачає нагляд за всіма. Захист свободи дітей здійснюється через обмеження анонімності дорослих.

Передача цифрового суверенітету

Характерно, що громадянське суспільство яке виступало рушійною силою прийняття захисного законодавства і є його формальним бенефіціаром – залишається поза структурою операційного контролю над даними. Виняток становлять окремі елементи бразильського законодавства: вимога пов'язувати акаунти неповнолітніх до 16 років з акаунтами батьків або опікунів та обов'язок платформ надавати батьківські інструменти контролю [3, с. 24]. Проте цей

батьківський контроль є мікрорівневим і індивідуалізованим: він дозволяє конкретному батьку наглядати за конкретною дитиною, але не надає громадянському суспільству як колективному актору жодних важелів впливу на те, як платформи збирають, зберігають і передають вікові дані сукупності користувачів.

Відтак, у диспозитиві нагляду здійснюється боротьба двох акторів. Перший актор – держава. Через законодавчу функцію визначає, які дані підлягають збору і в яких умовах, а через виконавчу отримує правові підстави для доступу до верифікаційних даних у встановлених законом випадках. Другий актор – бізнес (платформи і верифікаційні провайдери). Здійснює технічну обробку і зберігання даних, отримуючи від цього як регуляторну легітимність, так і потенційний комерційний ресурс. Таким чином, роль громадянського суспільства обмежена у фазі дискурсивної легітимації: воно надає моральний мандат диспозитиву («захист дітей»), але не отримує натомість інституційного контролю над ним – ані на рівні регулятора, ані на рівні колективного нагляду за архітектурою даних. Таким чином, цифровий суверенітет, який у публічному дискурсі приписується громадянському суспільству як бенефіціару захисного законодавства, фактично концентрується в руках держави та бізнесу.

Прецедентна логіка та майбутні ризики

Нинішні закони про верифікацію віку самі по собі ще не є інструментом масового контролю, тому що їх дія поки що має спрямованість на конкретну категорію користувачів.

Прецедент включає кілька рівнів. На правовому рівні – легітимізацію принципу обов'язкової ідентифікації в інтернеті: якщо суспільство погодилося з тим, що для доступу до певного контенту необхідно пред'являти посвідчення особи, наступний крок – розширення категорій «небезпечного» контенту – стає технічно і нормативно підготовленим. На технічному рівні – формування інфраструктури верифікації, яку можна використовувати для інших цілей. На суспільному рівні – нормалізацію практики ідентифікації як умови доступу: те, що здавалося виключенням, стає нормою.

Водночас, чим точніший індивідуальний профайлінг, тим менше індивід відчуває що за ним слідкують [17]. На нашу думку, це свідчить про структурні зміни у відчутті стеження та реальним обсягом стеження. Такі зміни ще знаходяться у динамічному положенні, проте демонструють тренди синергії бізнес-держава стосовно цифрового профайлінгу.

Онтополітичні наслідки для цифрової свободи

Три виміри звуження цифрової свободи

Ланюк, аналізуючи свободу в умовах капіталізму нагляду крізь призму Зубофф, виокремлює три виміри, в яких вона підривається: приватність, автономія та автентичність [7]. Застосовуючи цю схему до захисного профайлінгу, можна виявити специфічний спосіб, у який верифікаційне законодавство діє на кожен із цих вимірів.

Приватність підривається найбільш очевидно: верифікація за визначенням вимагає розкриття персональних даних. Навіть якщо закон обмежує комерційне використання цих даних (як у бразильському прикладі), сам факт їх існування у зовнішніх системах є структурним підривом приватності.

Автономія підривається через асиметрію вибору: суб'єкт може «відмовитися» від верифікації, але ціна відмови – виключення з певних сфер цифрового простору – зростає разом із розширенням верифікаційних вимог. В умовах, де операційна система запитує вік (каліфорнійський закон), відмова від верифікації стає практично неможливою без відмови від базової цифрової інфраструктури.

Автентичність підривається через опосередкований вплив: коли алгоритм «знає» вік суб'єкта і відповідно формує його інформаційне середовище, суб'єкт взаємодіє не з відкритим цифровим простором, а з його персоналізованою (і відфільтрованою) версією. Параметри фільтрації залишаються для суб'єкта прихованими.

Онтополітика верифікації та питання «третього шляху»

Верифікація віку є онтополітичним актом у тому сенсі, що вона виробляє цифрові суб'єктності: «повнолітній» і «неповнолітній». Вони постають не просто правовими

категоріями, а вбудованими у цифрову архітектуру атрибутами буття. Конституюючись через зовнішнє знання – через дані, зібрані і класифіковані системою – суб'єкт набуває цифрової ідентичності, яку він сам не визначав і над якою має обмежений контроль.

Констатація проблеми захисного профайлінгу не є аргументом проти захисту неповнолітніх. Питання не в тому, чи потрібен захист, а в тому, чи є профайлінг єдиним або найкращим способом реалізації захисту. Технологічно існують альтернативні підходи, що мінімізують обсяг зібраних даних. Зокрема, атестація з нульовим розголошенням (zero-knowledge proof), що дозволяє підтвердити факт (наприклад, «користувач є повнолітнім»), не розкриваючи вихідних персональних даних [12]. Або-ж Ці технології залишаються поза мейнстримом законодавчих рішень, що свідчить: вибір верифікаційного підходу відображає певне бачення відносин між суб'єктом, даними і владою, а не лише технічну доцільність.

У дослідженнях оптимізаційних систем запропоновано поняття захисних технологій оптимізації (Protective Optimization Technologies, POTs), які можна розуміти як технічні стратегії «контр-гри» проти небажаних ефектів алгоритмів [18]. На відміну від підходів, що чекають, поки самі платформи «виправлять» свої моделі, POTs зосереджуються на діях ззовні: зміні правил гри, середовища та доступних даних так, щоб алгоритм почав поводитися інакше й завдавати менше шкоди уразливим групам. У контексті верифікації віку це відкриває можливість мислити не лише про черговий рівень профайлінгу, а про контрдиспозитиви, у яких громадянське суспільство й користувачі свідомо обмежують видимість своїх даних, запроваджують посередницькі сервіси та колективні технічні практики, що мінімізують наглядовий потенціал вікових перевірок, не скасовуючи при цьому їхньої захисної функції. Наприклад, шкільна бібліотека або освітній портал можуть виступати таким «захисним посередником»: учні заходять до ресурсів через шкільний шлюз, де вік підтверджується локально, а зовнішнім платформам передається лише мінімальний маркер на кшталт «користувач перевірений як неповнолітній/повнолітній», без передачі біометрії чи повного набору персональних даних.

Можливість «третього шляху» – верифікації без профайлінгу, захисту без нагляду – є не лише технічним, але й нормативним і філософським завданням: вона вимагає ревізії базових уявлень про те, що таке ідентичність у цифровому просторі і яке знання системи мають право мати про суб'єкта-користувача.

Результати дослідження. Показано що профайлінг є онтополітичним актом: він конституює суб'єкта через зовнішнє знання про нього, редукуючи цілісну особу до керованої цифрової категорії – дивідуума у дельозівському сенсі. Це фундаментальна зміна онтологічного статусу суб'єкта, а не технічна процедура збору даних.

Висвітлено у прикладах що верифікація віку є прикладом подвійного диспозитиву: захисна функція щодо неповнолітніх і наглядова функція щодо всіх користувачів є двома аспектами одного і того самого механізму. Порівняльний аналіз законодавства Великої Британії, Бразилії та Каліфорнії виявляє спільну логіку нормативного дрейфу від цільового захисту до системної верифікації.

Показано як захисний профайлінг здійснює системний трансфер цифрового суверенітету від індивіда до акторів – бізнесу і держави. Це залишає громадянське суспільство на рівні дискурсивної легітимації, але не реального контролю над даними, їх обробкою та розповсюдженням.

Доведено що верифікаційне законодавство структурно підриває всі три виміри цифрової свободи за Зубофф – Ланюком: приватність (через обов'язкове розкриття даних), автономію (через асиметрію вибору між верифікацією і виключенням) та автентичність (через алгоритмічну фільтрацію інформаційного середовища).

Перспективи подальших досліджень охоплюють: нормативну філософію цифрової ідентичності та критерії правомірного знання системи про суб'єкта; порівняльний аналіз захисних і репресивних диспозитивів у цифровому регулюванні в різних правових культурах; філософське обґрунтування альтернативних верифікаційних архітектур (зокрема, на основі zero-knowledge proof), що мінімізують наглядовий потенціал захисного законодавства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Airapetov M. Digital human rights and freedoms. reality without proper regulation. *National technical university of Ukraine journal. Political science. Sociology. Law*. 2025. No. 1(65). P. 130–137. URL: https://doi.org/10.20535/2308-5053.2025.1(65).332569 (date of access: 20.04.2026).

2. Online Safety Act 2023 : UK Public General Act of 26.10.2023 no. 2023 c. 50. URL: https://www.legislation.gov.uk/ukpga/2023/50 (date of access: 05.04.2026).

3. Digital Statute for Children and Adolescent : ECA Digital of 17.09.2025 no. 15,211/2025. URL: https://www.gov.br/mdh/pt-br/assuntos/noticias/2025/novembro/brasil-apresenta-avancos-em-seguranca-digital-da-infancia-e-lanca-eca-digital-em-ingles-durante-cupula-social-do-g20-na-africa-do-sul/eca-digital-ing-v2.pdf (date of access: 05.04.2026).

4. Age verification signals: software applications and online services : Assembly Bill of 13.10.2025 no. AB-1043. URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB1043 (date of access: 05.04.2026).

5. Data collection summary for Windows. *Microsoft*. URL: https://www.microsoft.com/en-us/privacy/data-collection-windows (date of access: 09.04.2026).

6. Zuboff Sh. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019. 704 p.

7. Laniuk Y. Freedom in the Age of surveillance capitalism: Lessons from Shoshana Zuboff. *Ethics & bioethics*. 2021. Vol. 11, no. 1-2. P. 67–81. URL: https://doi.org/10.2478/ebce-2021-0004 (date of access: 19.04.2026).

8. Leuenberger M. Track thyself? The value and ethics of self-knowledge through technology. *Philosophy & technology*. 2024. Vol. 37, no. 1. URL: https://doi.org/10.1007/s13347-024-00704-4 (date of access: 21.04.2026).

9. Sahakyan H., Gevorgyan A., Malkjyan A. From disciplinary societies to algorithmic control: rethinking foucault's human subject in the digital age. *Philosophies*. 2025. Vol. 10, no. 4. P. 73. URL: https://doi.org/10.3390/philosophies10040073 (date of access: 21.04.2026).

10. Couldry N., Mejías U. Datafication. *Internet Policy Review*. 2019. Vol. 8, no. 4. URL: (date of access: 21.04.2026).

11. Masiero S. Digital identity as platform-mediated surveillance. *Big data & society*. 2023. Vol. 10, no. 1. P. 205395172211351. URL: https://doi.org/10.1177/20539517221135176 (date of access: 21.04.2026).

12. Koziuberda D. O., Yesina M. V., Golikov Y. L. Digital identity and ZKP: anonymous data and secure authentication. *Radiotekhnika*. 2025. No. 221. P. 39–45. URL: https://doi.org/10.30837/rt.2025.2.221.05 (date of access: 21.04.2026).

13. Han B.-Ch. Psychopolitics: Neoliberalism and New Technologies of Power. London: Verso, 2017. 96 p.

14. Deleuze G. Postscript on the societies of control*. *Surveillance, crime and social control*. 2017. P. 35–39. URL: https://doi.org/10.4324/9781315242002-3 (date of access: 21.04.2026).

15. Foucault M. Power/knowledge: selected interviews and other writings, 1972-1977. Brighton [Eng.] : Harvester Press, 1980. 270 p.

16. Ricoeur P. Oneself as Another. Chicago: University of Chicago Press, 1992. 363 p.

17. Google knows me too well! Coping with perceived surveillance in an algorithmic profiling context / D. Zhang et al. *Computers in human behavior*. 2024. P. 108536. URL: https://doi.org/10.1016/j.chb.2024.108536 (date of access: 21.04.2026).

18. Kulynych B., Overdorf R., Troncoso C., Gürses S. POTs: Protective Optimization Technologies. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT* '20)*, 2020. p. 177–188. URL: https://doi.org/10.1145/3351095.3372853 (date of access: 21.04.2026).

REFERENCES

1. Airapetov, M. (2025). Digital human rights and freedoms: Reality without proper regulation. *National Technical University of Ukraine Journal: Political Science. Sociology. Law*, 1(65), 130–137. https://doi.org/10.20535/2308-5053.2025.1(65).332569

2. Assembly Bill No. 1043, Age verification signals: Software applications and online services, California Legislature (2025, October 13). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB1043

3. Couldry, N., & Mejías, U. (2019). Datafication. *Internet Policy Review*, 8(4). https://doi.org/10.14763/2019.4.1428

4. Deleuze, G. (2017). Postscript on the societies of control. In *Surveillance, crime and social control* (pp. 35–39). https://doi.org/10.4324/9781315242002-3

5. Digital Statute for Children and Adolescents (ECA Digital), No. 15,211/2025 (2025, September 17). Ministério dos Direitos Humanos e da Cidadania. https://www.gov.br/mdh/pt-br/assuntos/noticias/2025/novembro/brasil-apresenta-avancos-em-seguranca-digital-da-infancia-e-lanca-eca-digital-em-ingles-durante-cupula-social-do-g20-na-africa-do-sul/eca-digital-ing-v2.pdf

6. Foucault, M. (1980). *Power/knowledge: Selected interviews and other writings, 1972–1977*. Harvester Press.

7. Han, B.-Ch. (2017). *Psychopolitics: Neoliberalism and new technologies of power*. Verso.

8. Koziuberda, D. O., Yesina, M. V., & Golikov, Y. L. (2025). Digital identity and ZKP: Anonymous data and secure authentication. *Radiotekhnika*, (221), 39–45. https://doi.org/10.30837/rt.2025.2.221.05

9. Kulynych, B., Overdorf, R., Troncoso, C., & Gürses, S. (2020). POTs: Protective optimization technologies. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT* '20)* (pp. 177–188). https://doi.org/10.1145/3351095.3372853

10. Laniuk, Y. (2021). Freedom in the age of surveillance capitalism: Lessons from Shoshana Zuboff. *Ethics & Bioethics*, 11(1–2), 67–81. https://doi.org/10.2478/ebce-2021-0004

11. Leuenberger, M. (2024). Track thyself? The value and ethics of self-knowledge through technology. *Philosophy & Technology*, 37(1). https://doi.org/10.1007/s13347-024-00704-4

12. Masiero, S. (2023). Digital identity as platform-mediated surveillance. *Big Data & Society*, 10(1), 205395172211351. https://doi.org/10.1177/20539517221135176

13. Microsoft. (n.d.). *Data collection summary for Windows*. https://www.microsoft.com/en-us/privacy/data-collection-windows

14. Online Safety Act 2023, c. 50. (2023, October 26). UK Public General Acts. https://www.legislation.gov.uk/ukpga/2023/50

15. Ricoeur, P. (1992). *Oneself as another*. University of Chicago Press.

16. Sahakyan, H., Gevorgyan, A., & Malkjyan, A. (2025). From disciplinary societies to algorithmic control: Rethinking Foucault's human subject in the digital age. *Philosophies*, 10(4), 73. https://doi.org/10.3390/philosophies10040073

17. Zhang, D., Strycharz, J., Boerman, S. C., Araujo, T., & Voorveld, H. (2024). Google knows me too well! Coping with perceived surveillance in an algorithmic profiling context. *Computers in Human Behavior*, 165, 108536. https://doi.org/10.1016/j.chb.2024.108536

18. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

Filimonov Volodymyr Volodymyrovych
Postgraduate Student at the Department of Philosophical, Political and Psychological Studies
Cherkasy State Technological University
460 Shevchenko Blvd., Cherkasy, Ukraine
orcid.org/0009-0000-7934-4057

DIGITAL FREEDOM AND PROTECTIVE PROFILING: AGE VERIFICATION AS A DISPOSITIF OF SURVEILLANCE

Problem: *Existing concepts of protective profiling, understood as a dual dispositif, require further development through the lens of algorithmic control. Control over data to be deepened by viewing protective profiling as an ontopolitical act grounded in the ideas of M. Foucault, G. Deleuze, and S. Zuboff. In this context, it becomes essential to refine the notion of digital freedoms by revealing an internal paradox: the expansion of child protection is linked to the narrowing of privacy in the digital environment and to the diminishing role of autonomy and authenticity for all users.*

Purpose: *To substantiate the concept of protective profiling as a dual dispositif in which the collection and processing of personal data, legitimized by the objectives of child protection, structurally reproduce the logic of surveillance capitalism and create a normative precedent for broader regulation of digital activity.*

Methods and results: *The study is based on M. Foucault's concept of the dispositif, B.-Ch. Han's psychopolitics, S. Zuboff's theory of surveillance capitalism, and G. Deleuze's notion of the dividual; empirically, it relies on a comparative analysis of age verification legal regimes in three jurisdictions.*

Conceptual analysis, critical theory, and a comparative-legal approach, including bibliographic analysis, are employed. It is shown that age verification is not a technical but an ontopolitical act that constitutes the physical subject through its reflection – the digital subject – via external knowledge and transfers individual digital sovereignty to two actors – business and the state. As a result, civil society faces the risk of acquiring the traits of a passive recipient immersed in a state of permanent external control. Shared logic of normative drift is revealed: from targeted protection toward potential mass control, in which protection or control is delegated by society to state and commercial actors. An internal paradox of protective profiling is also identified: the expansion of child protection in the digital environment is structurally linked to the narrowing of digital freedom for all users in its three dimensions – privacy, autonomy, and authenticity.

Key words: *digital freedom, age verification, profiling, surveillance capitalism, algorithmic control.*

Дата першого надходження статті до видання: 23.04.2026
Дата прийняття статті до друку після рецензування: 18.05.2026
Дата публікації (оприлюднення) статті: 30.05.2026