15 листопада 2019 року T-PD(2019)06FIN

КОНСУЛЬТАТИВНИЙ КОМІТЕТ КОНВЕНЦІЇ ПРО ЗАХИСТ ОСІБ У ЗВ'ЯЗКУ З АВТОМАТИЗОВАНОЮ ОБРОБКОЮ ПЕРСОНАЛЬНИХ ДАНИХ

Конвенція №108

Захист даних дітей в системах освіти. Виклики та можливі засоби їх вирішення

Доповідь Джен Перссон, директорки «DefendDigitalMe»

Генеральний директорат з прав людини та верховенства права

Зміст

I Контекст

I.1. Вступ

Не варто недооцінювати конфіденційність цифрових даних учнів та студентів. (Робочий документ Міжнародної робочої групи з питань захисту даних в галузі телекомунікації щодо платформ електронного навчання (квітень 2017 року)).

> *«Деякі з цих платформ електронного навчання, а також аналітика навчальних даних, якій сприяють такі платформи, мають величезний потенціал для стимулювання розробки інноваційних та ефективних методів навчання. У кращому випадку вони можуть посилити та доповнити взаємодію студентів, батьків і педагогів в освітньому середовищі та допомогти їм реалізувати свій відповідний потенціал. Однак платформи електронного навчання можуть створювати загрози для приватного життя, пов'язані зі збором, використанням, повторним використанням, розголошенням та зберіганням персональних даних цих осіб*». (Резолюція щодо платформ електронного навчання, Міжнародна конференція уповноважених з питань захисту даних і недоторканості приватного життя (ICDPPC), 2018 рік).

Потенційна шкода від неналежного використання звичайних цифрових освітніх записів може здатися незначною в порівнянні зі складнішими технологіями, які вже використовуються в освіті. Але якщо оцінити масштаби учнівських баз даних, що містять сотні одиниць персональних даних про поіменно названих осіб у мільйонах різних записів на національному рівні, то ризики для людей, а також інституційні та репутаційні ризики втрати навіть найпростіших даних можуть стати більш очевидними.

Вкрай важливо також визнати, що, попри відмінності в освітній ситуації в різних географічних регіонах, загальноприйнятою практикою є використання дітей в освіті як випробувальний полігон для нових технологій, як з боку компаній для розробки своїх продуктів, так і з боку державних структур, а вже після таких випробувань приймається рішення про випуск технології в маси.

Існують малодосліджені, але важливі питання здоров'я та безпеки людини, а також питання етики й управління, пов'язані з впровадженням нових технологій в навчальних класах, як-от відчуття нудоти при русі у віртуальній реальності із повним зануренням. Розвиток нейротехнологій та постцифрової науки вимагають одночасної уваги з боку дослідників в галузі освіти (Вільямсон (Williamson), 2019 р.), а також з боку регуляторних і законодавчих органів.

Хоча наглядові органи із захисту даних займаються питаннями захисту даних і недоторканості приватного життя в різних секторах, спільна увага і системні дії досі обмежувалися лише захистом прав дітей у сфері освіти й, як правило, спрямовувалися на поточну ситуацію, а не на дослідження перспектив.

У 2009 році робоча група з питань реалізації статті 29 опублікувала висновок (2/2009) щодо захисту персональних даних дітей («Загальні рекомендації та окремий випадок шкіл»). Автори визнали, що

> *«зі статичної точки зору дитина — це особа, яка ще не досягла фізичної та психологічної зрілості. З динамічної точки зору дитина перебуває в процесі фізичного і розумового розвитку на шляху до дорослого життя. Права дитини та здійснення цих прав — в тому числі й захист даних — слід викладати у такий спосіб, аби відобразити обидві ці точки зору».*

Згідно з цими точками зору, діти в різних системах освіти, кожна з яких має свій особистий досвід культурних, соціальних, економічних і політичних змін, можливо, не зазнали значних змін за ці десять років, але в їхніх навчальних класах спостерігається швидке зростання доступних технологій.

Школи відкривають свої двері та бази даних особистої конфіденційної інформації школярів все більшій кількості комерційних структур. Упродовж занять до дітей вже можуть застосовуватися інструменти сканування мозку, 360-градусні камери з функцією запису голосу, стеження за допомогою технологій радіочастотної ідентифікації (RFID), вони також можуть користуватися в класі шоломами доповненої реальності. Компанії та їхні спонсори прагнуть використовувати освіту як новий ринок, в якому країни перейшли від менш контрольованих державою до більш комерційно орієнтованих моделей освіти. Аналогічним чином, успішні компанії на нинішніх ринках, як-от ринок камер безпеки, розширюють свою діяльність в секторі освіти. В результаті вплив на дітей широкого спектра технологій обробки даних значною мірою залишається непоміченим.

Права дітей згідно із законодавством про захист даних залишалися практично незмінними протягом десятиліття. Але чи будуть цих прав дотримуватися, залежить від компаній, що діють за лаштунками, та механізмів правозастосування з боку регуляторних органів, оскільки контроль і гарантії на рівні школи можуть.

Як відзначили Луптон (Lupton) і Вільямсон (Williamson) 2017 року,

«*Діти стають об'єктами безлічі пристроїв для моніторингу, які генерують докладні дані про них, а дослідники критичних даних і захисники недоторканності приватного життя лише починають звертати увагу на таку практику*».

I.1.1 Нинішній підхід означає, що права зазнають утисків

Існує міф про те, що діти не переймаються питаннями недоторканності приватного життя. Це просто неправда. Є безліч доказів на підтвердження очікувань дітей. Самі діти та молодь можуть виявитися більш уважними до ризиків, ніж це уявляє більшість дорослих (Патерсон Л. (Paterson, L.) та Грант Л. (Grant, L.), ред., 2010 р.), а молодь стурбована конфіденційністю й тим, що особисті дані можуть потрапити «не туди».

Уповноважений у справах дітей в Англії вважає, що ми, дорослі, не виконуємо свого засадничого обов'язку — надати дітям інструменти, які дозволять їм стати провідниками свого власного життя. (Уповноважений у справах дітей, 2017 р.).

На національному рівні державним органам, можливо, доведеться переглянути свій підхід до використання загальнонаціональних наборів освітніх даних для вторинних цілей, таких як профілювання ризиків для оперативних заходів або дослідження державної політики, що виходить далеко за рамки цілей, для яких ці дані були зібрані.

Використання державою освітніх даних в адміністративних цілях може дедалі більше ставитися під сумнів в разі визнання, що «великі дані (Big Data) позбавили актуальності нинішній підхід до захисту приватного життя і громадянських свобод». (Мунді (Mundie), 2014 р.).

Підвищення обізнаності щодо того, що дані використовуються не за призначенням, збільшить випадки бойкотування збору даних, (коаліція «Against Borders for Children» (Великобританія), 2016–2018 рр.), що надовго зашкодить як суспільним, так і комерційним інтересам (Батьківська коаліція за недоторканність приватного життя студентів, (США) InBloom, 2012–14 рр.) і потенційно поставить під загрозу позитивні зрушення, які служать інтересам дитини.

Комерційне впровадження продуктів і підходів вимагає більш ретельної перевірки та консультацій. Коли програма онлайн-навчання «Summit Learning» ввела до системи державної освіти комерційні технологічні моделі, спостерігався запеклий опір з боку батьків («Summit Schools», Канзас, 2019 р.).

Довіра є крихкою, і деякі практики ставлять під загрозу сприйняття суспільством повсякденних технологій у дедалі більш розповсюдженому інтернеті речей, що також проник вже в навчальні класи. Використання даних з ігноруванням цього збільшує колективний ризик для інших компаній, що використовують персональні дані. Як було запропоновано в доповіді Ради із захисту прав споживачів Норвегії #Toyfail 2016 року,

> *«Якщо громадськість не лякає думка про те, що таємниці їхнього сексуального життя та пристрої можна "хакнути", можливо, загальна довіра до під'єднаних пристроїв буде знищена, коли вони побачать, як незнайомці розмовляють з їхніми дітьми через радіоняню або іграшку».*

Питання про те, наскільки сталими є поточні моделі збору даних з точки зору рівня довіри та терпимості суспільства, перевіряється новітніми технологіями в навчальних класах,

такими як технології розпізнавання обличчя. (CNIL (Національна комісія з питань інформаційних прав і свобод), 2019 р.)

Регуляторні органи відіграють життєво важливу роль у забезпеченні правовладдя, яке має слугувати надійною та сталою базою для забезпечення того, щоб на шляху у доросле життя кожну дитину супроводжував якомога менший цифровий слід.

Крім того, попри дедалі більше розповсюдження інститутів етики та матеріалів, в яких йдеться про етику і цифровий слід, ще не приділяється належна увага питанню про комплексний вплив цих технологій на життя дитини наразі і в майбутньому, або оцінити їхній вплив на «вуглецевий відбиток» кожної дитини, а також чи можемо ми створити більш сталі моделі апаратного забезпечення, щоб не надмірно завантажувати їхній майбутній з огляду на взаємодію цих моделей в сьогоднішньому цифровому середовищі.

Все більша кількість застарілих ІКТ у деяких школах, перетворює їх на шафу, повну непридатних до використання пристроїв, які вони не можуть дозволити собі замінити, та які побудовані з використанням операційних систем, що більше не підтримуються компаніями.

Будь-яка повна етична оцінка впливу новітніх технологій повинна також охоплювати питання їхнього впливу на навколишнє середовище і зобов'язання компаній вживати необхідних заходів для мінімізації споживання ними природних ресурсів і енергії.

Ризики, властиві застарілим системам, наражають їх на безпекові загрози, зокрема від програм-вимагачів.[1]

1.1.2 Обсяг і різноманітність суб'єктів даних в освітній галузі

Обсяг даних, створених і зібраних в шкільних системах задля управління і навчання, має приголомшливі наслідки для «датифікованої дитини» (Луптон (Lupton), Вільямсон (Williamson), 2016 р.).

Типи суб'єктів на території освітніх установ, які беруть участь в обробці персональних даних дітей зі шкіл, можуть бути розділені на тих, що мають прямі відносини з дитиною (вчителі, адміністратори шкіл), та тих, які не контактують з дитиною (регіональні адміністратори, що обробляють дані з метою аналізу результатів роботи вчителів і показників успішності учнів).

Але переважна більшість суб'єктів, залучених до повсякденної обробки даних кожного дня, року і протягом всього життя дитини (їх дуже важко візуалізувати через великий обсяг), знаходяться не на території школи, а за її межами, в сотнях компаній, що обробляють дані на основі хмарних технологій.

Типи зібраних даних можна загалом розділити на адміністративні та навчальні дані.

Цілі обробки даних в галузі освіти можуть охоплювати контроль відвідуваності, перевірку та відстеження навчальних успіхів, спостереження за поведінкою, комунікацію та залученість батьків, управління класними кімнатами та схеми розсадки, здійснення безготівкових платежів, забезпечення захисту і протидія насильницькому екстремізму, відстеження активів і підзвітність персоналу, а також управління якістю роботи та зіставлення контрольних показників. Перш за все, дані обробляються для оцінки

[1] Районні відділи освіти є особливо легкою мішенню для операторів програм-вимагачів через їхній малий бюджет на інформаційні технології та обмежені ресурси в царині безпеки (ArsTechnica, 2019 р.) https://arstechnica.com/information-technology/2019/08/rash-of-ransomware-continues-with-13-new-victims-most-of-them-schools/

інтелекту, підтримки навчання, виконання домашніх завдань або для проведення досліджень. Технології використовуються для викладання, відстеження успішності учнів і тестування.

Без достатньої кількості перевірок, у зв'язку з великою кількістю різних окремих провайдерів, які залучені до навчального процесу дитини, збір і повторне використання даних дітей упродовж шкільних років може сягнути таких масштабів, що навіть самі школи та законні опікуни не знатимуть про це.

1.1.3 Добування і використання даних

З різних причин на світовому ринку освітніх технологій edTech спостерігається швидке зростання комерційних учасників і новітніх технологій, які розповсюджуються не лише завдяки інвесторам та акселераторам на англомовному ринку США і Великобританії, але і по всьому світу. Оцінки ринкової вартості та інвестицій варіюються в широкому діапазоні, від 8 млрд дол. до цифр, зазначених у дослідженні Metaari «The 2018 Global Learning Technology Investment Patterns: The Rise of the Edtech Unicorns» (Глобальні інвестиційні моделі навчальних технологій 2018 року: Повстання єдинорогів Edtech), згідно з яким китайські компанії освітніх технологій були основними одержувачами глобальних інвестицій на ринку Edtech у 2018 році та отримали 44,1% від загальних ринкових витрат в розмірі 16,34 млрд дол.

Водночас в умовах глобального тиску, пов'язаного з необхідністю забезпечення недорогого державного навчання і маркетизації, інфраструктура, що використовується для надання державної освіти, і діти в ній зазнають впливу комерційного «вільно поширюваного» програмного забезпечення, яке компанії пропонують на безоплатній основі, часто в рамках прихованого обміну даними.[2]

Недостатня підготовка та невміле управління змінами часто супроводжують впровадження нових технологій, разом з браком навчальних матеріалів і низькою кваліфікацією викладачів. (Сабатес Р. (Sabates, R.), 2010 р.)

1.1.4 Приховане прогнозування

В експерименті, проведеному в місті Еспоо, Фінляндія, у співпраці з компанією «Tieto» штучний інтелект був застосований для аналізу даних про охорону здоров'я та соціальне забезпечення, пов'язаних з навчанням дітей молодшого віку з 2002 по 2016 роки. (Automating Society: Taking Stock of Automated Decision- Making in the EU (Автоматизація суспільства: підбивання підсумків автоматизованого прийняття рішень в ЄС), AlgorithmWatch, 2019 р.).

В Англії рада графства Ессекс використовує прогностичну аналітику для виявлення дітей, які не будуть «готові до школи» коли їм виповниться п'ять років, а міська рада Бристоля експериментує з новими алгоритмічними можливостями, щоночі отримуючи дані школярів[3] для врахування у своїй прогностичній аналітиці щодо забезпечення соціальних потреб дітей. (Пегг (Pegg, McIntyre), Макінтайр (McIntyre), 2018 р.)

[2] Наприклад, NetDragon Websoft Group у 2019 році «займалася монетизацією своєї користувальницької бази» від онлайн-спільноти Edmodo. (стор. 4 (6/84) http://file.download.99.com/down/ir_e_20191011f.pdf)

[3] http://specification.sifassociation.org/Implementation/UK/2.0/html/

Прогностичний характер обробки таких даних, що застосовується для втручань на ранній стадії, може мати значний вплив, і будь-які небажані наслідки цього можуть тривати все життя, починаючи з раннього віку.

Програмне забезпечення, пропоноване на ринку як таке, що використовує штучний інтелект, також використовується для прогнозування поведінкових ризиків в продуктах інтернет-моніторингу, в персоналізованих навчальних платформах і навіть для прийняття рішень на низькому рівні, на рівні шкільних класів, наприклад для визначення планів розміщення в класі на основі даних про поведінку дітей, що містяться у комп'ютерних застосунках, які аналізуються у непрозорий спосіб для визначення компонування кімнат, оптимізованого з точки зору поведінки дітей.

Результати досліджень, проведених Ріган (Regan) і Стівз (Steeves) (2019 р.), дозволяють припустити таке:

> *«суперечливі дискурси щодо персоналізованого навчання обертаються навколо спірних визначень того, який тип знань необхідний для навчання в XXI столітті, як має виглядати самонаправлене навчання, чи стосується навчання процесу або змісту, а також доказів, які необхідні для встановлення, чи призводить персоналізоване навчання до кращих результатів для учнів».*

Потенційні глобальні наслідки для безпеки та стабільності освітніх інфраструктур державного сектора і взаємодії з іншими державними секторами, де дані про дітей використовуються для втручання в їхнє життя, особиста шкода для дітей з точки зору недоторканності приватного життя, а також наслідки нормалізації автоматизованого прийняття рішень, можуть продовжуватися і за межами життя цього датифікованого покоління.

1.1.5 Формування життєвого середовища, в якому поважають права

Стурбованість з приводу технології та її впливу на стосунки та роль людини в суспільстві не є новою. Анаіс Нін (Anaïs Nin) у своєму щоденнику за 1946 рік зазначила про

> *«небезпечний час, коли механічні голоси, радіо, телефони приходять на зміну людським інтимним стосункам, а концепція спілкування з мільйонами людей призводить до все більшої убогості в інтимних відносинах і людському баченні».* (Щоденник Анаіс Нін (The Diary of Anais Nin), том 4: 1944-1947 рр.).

Але масштаби, швидкість і простота передачі даних стрімко зростають з моменту створення інтернету і всесвітньої павутини, а вартість зберігання даних знизилася. Перешкоди на шляху доступу до даних, їхнє копіювання та розповсюдження зменшилися завдяки кращій доступності, заразом зникли ті заходи захисту, які пропонувалися суб'єктам даних з практичної точки зору, а компанії та установи припинили їх дотримуватися.

У пункті 8 свого зауваження загального характеру № 1 про цілі освіти Комітет Конвенції ООН про права дитини заявив у 2001 році про таке:

> «*Діти не втрачають своїх прав людини після того, як увійшли до шкільних дверей. Отже, наприклад, освіта, повинна надаватися таким чином, щоб шанувалася природна гідність дитини і щоб дитина могла вільно висловлювати свої погляди відповідно до пункту 1 статті 12 і брати участь у шкільному житті».*

Як зазначено в Рекомендації CM/Rec (2018)7 Комітету міністрів Ради Європи, держави-члени зобов'язані поважати, захищати та реалізувати права дитини в цифровому середовищі. Якщо постачальники технологій не поважають ці права, їхня продукція не повинна використовуватися.

Дані, що використовуються в дитинстві для профілювання і, зокрема, прогностичного аналізу, можуть мати неясні наслідки протягом усього життя. І в багатьох наукових спільнотах з ентузіазмом пропонується починати таку датифікацію для стратифікації ризиків та вжиття відповідних заходів ще до народження дитини. Інтелект — здатність вчитися, розмірковувати та розв'язувати проблеми — перебуває в авангарді поведінкових генетичних досліджень. (Пломін (Plomin), Штум (Stumm), 2018 р.)

Прогнози, засновані на машинному аналізі великих наборів персональних даних, автоматизовані рішення, які вносять зміни в життєвий досвід дитини на екрані та за його межами лише за допомогою легкого натискання на клавіші, і персоналізовані дії, що вживаються в результаті дорослими, — все це вже є можливим на таких рівнях інвазивності і таким шляхом, що є прихованим або непрозорим, які більшість сімей і працівників шкіл самі і не помітять. Питання чому не виконуються зобов'язання щодо забезпечення прозорості і як це можна виправити вимагають іншого системного підходу, щоб діти та сім'ї розуміли, що їхні власні дані обробляються іншими людьми.

Деякі види застосування технологій, що ґрунтуються на зборі, фіксації та тлумаченні даних дітей, повинні бути визнані занадто інвазивними й такими, що занадто заважають повному і вільному розвитку дитини, адже неприпустимо, аби діти зазнавали такого впливу в системі освіти. Регулювання повинно мати випереджувальний характер, вимагаючи співпраці між законодавством про безпеку споживачів і органами із захисту даних у тих випадках, коли товари й послуги впроваджуються в навчальне середовище або використовуються для роботи з дітьми. Однак це не означає нав'язування випробувань і тестувань продукту в реальних умовах на дітях в навчальному класі в рамках системи обов'язкової державної освіти, здебільшого в інтересах виробників продукції.

1.1.6 Норми повинні забезпечувати суворе дотримання основних принципів.

Всі права людини, закріплені в Конвенції ООН про права дитини (КПД ООН), Конвенції про захист прав людини і основоположних свобод (ETS № 5) та протоколах до неї, повинні повною мірою дотримуватися, захищатися і реалізовуватися у сфері освіти.

Основоположні принципи обмеження цілей використання даних, мінімізації даних і прозорості часто є недієвими на практиці без рішучого і стримувального виконання.

Крім того, дорослі повинні забезпечити, щоб заходи захисту, які надаються дітям, були не лише належними протягом їхнього дитинства, а й сприяли тому, щоб діти могли безперешкодно досягти дорослого життя та могли повністю і вільно розвиватися, повною мірою розкривати свій потенціал і людські здібності.

Принципи необхідності, пропорційності та практичного застосування строків зберігання даних повинні бути посилені з тим, щоб передбачити в шкільних записах дітей положення про встановлене законом обмеження термінів зберігання даних індивідуального рівня, що дозволяють ідентифікацію.

Принцип мінімізації даних є основою того, що необхідно дітям, аби захист даних чинив істотний вплив на їхню особистість і людську гідність, а не лише дозволяв безпечно,

справедливо і законно обробляти їхні дані. Обмеження щодо того, наскільки підхід, запропонований Експертною робочою групою високого рівня з питань штучного інтелекту (HLEG-AI) в документі від квітня 2019 року «Рекомендації щодо політики та інвестицій в галузі надійного штучного інтелекту», повинен застосовуватися для кращого захисту в освітньому середовищі, не повинні залежати від державних органів або комерційних продуктів, а натомість від потреб та інтересів дитини, щоб забезпечити її повний і вільний розвиток на шляху до дорослого життя.

> *«Дітям має бути забезпечено вільний та неконтрольований простір для розвитку, і після досягнення дорослого віку їм треба надавати «чистий лист» у будь-яких державних чи приватних сховищах даних».* (HLEG-AI, 2019 р.)

2. Освітнє середовище і перспективи розвитку технологій

У процесі законотворення і закупівель на всіх рівнях державного врядування необхідно дотримуватися прийнятого Комітетом з прав дитини КПД ООН Зауваження загального характеру №16 (2013 р.) про зобов'язання держави щодо впливу підприємницького сектора на права дітей.

> *«Держава не повинна брати участь в порушеннях прав дітей, підтримувати або потурати таким порушенням, коли вона сама виконує підприємницьку роль або веде бізнес із приватними підприємствами. Як приклад, держави повинні вживати заходів для забезпечення того, щоб контракти на державні закупівлі призначалися тим учасникам торгів, які зобов'язуються дотримуватися права дітей. Державні установи та інституції, включно із силами безпеки, не повинні співпрацювати з третіми сторонами, які порушують права дитини, або потурати їм. Держави не повинні інвестувати бюджетні фінанси та інші ресурси в комерційну діяльність, що порушує права дітей».*

Зміни в розумінні того, що є допустимим, що є можливим і що прийнятним у галузі освіти, є теоретичним питання для багатьох науковців і осіб, відповідальних за розробку політики. Три роки на випробування та виведення продукту на ринок, або на виявлення, що певний інструмент освітніх технологій є неефективним або непедагогічним , може бути коротким терміном для розробників, проте це може становити понад чверть життя дитини в системі обов'язкової освіти.

Сподівання та ентузіазм 2012 року, року Масових відкритих онлайн-курсів (MOOC) (New York Times, 2012 р.), дещо згасли, а разом з ними й думка про те, що безоплатні онлайн-курси можуть принести найкращу освіту до найвіддаленіших куточків світу, без зусиль навчати людей новим професіям, і «розширювати інтелектуальні та особисті мережі».

Дехто досі має певні підозри щодо бізнес-моделі MOOC, що заохочує лекторів брати участь у викладенні MOOC, питаючи, чи отримують студенти та викладачі інтелектуальний прибуток, доки інвестори накопичують гроші. (Девідсон, С. (Davidson, C.), 2017 р.)

Однак, хоча деякі навчальні платформи розширилися, можливо, не так добре, як прогнозувалося, зростає число нових платформ, які часто обіцяють те, що сприймається як новітні технології, ШІ та функціональні можливості, підтримувані машинним навчанням. Галузь освіти рясніє новими адміністративними інструментами, які часто обіцяють зменшити робоче навантаження і підвищити ефективність роботи персоналу, а також поліпшити результати навчання дітей. Разом з тим, принаймні у Великій Британії,

управління цією галуззю все більше здійснюється за принципами бізнесу та маркетингу, що веде до зменшення викладацького складу у державній освіті та витрат на освіту

Цей короткий виклад ситуації з використанням персональних даних дає уявлення про деякі типи технологій, які існують, використовуються, і змушують нас порушити питання про адекватність наявних норм захисту даних і механізмів їхнього застосування, які спираються на індивідуальні скарги при розв'язанні питань, пов'язаних з правами дитини в освітньому середовищі.

3. Сфера застосування доповіді

Для цілей цієї доповіді використовуються ті самі визначення, що і для цілей Конвенції. Отже, суб'єкт даних – це дитина, і відповідно до Конвенції ООН про права дитини (КПД ООН) (пункт 1) дитиною є кожна людська істота до досягнення 18-річного віку, якщо за законом, застосовуваним до даної особи, вона не досягає повноліття раніше. У використаних джерелах можуть зустрічатися терміни «учень» і «студент» на взаємозамінній основі в залежності від країни походження.

У джерелах щодо обробки даних в галузі освіти не проводиться розмежування між моделями освіти, пропонованими в усьому світі, а також між обов'язковою освітою, фінансованою приватним сектором чи державою. Натомість автор розглядає певні аспекти надання освіти, які можуть передбачати обробку даних дітей органами влади та комерційними третіми сторонами і вже широко застосовуються та виходять за межі національних кордонів.

Діти у США можуть не зазнавати тих самих обмежень мобільності, з якими стикаються діти при доступі до навчальних закладів у країнах Африки на південь від Сахари, в Гані, Малаві або Південній Африці (Портер (Porter), проте вони так само наражаються на стеження за собою внаслідок використання цифрових інструментів на мобільному телефоні або портативному планшеті.

Наприклад, Bridge International стверджує, що їхній «застосунок для смартфона дозволяє менеджерам Академії безперешкодно синхронізувати планшети своєї академії, відвідуваність учнів та вчителів, оплату за навчання, моніторинг навчальних занять і багато іншого».

В інших країнах лунає критика на адресу «технологічного солюціонізму», стандартизованої високотехнологічної педагогічної програми, розробленої в їхній штаб-квартирі в США, і її використання у сфері комерційної освіти. (ESCR-Net — Міжнародна мережа з питань економічних, соціальних і культурних прав, 2018 р.) У березні 2018 року вісімдесят вісім організацій громадянського суспільства приєдналися до колективного листа, що закликає провідних фінансових інвесторів припинити підтримку «Bridge International Academies» (BIA), багатонаціональної комерційної корпоративної мережі, що управляє більш ніж 500 школами в Кенії, Ліберії, Нігерії, Уганді та Індії.

Коли Марк Цукерберг спробував застосувати рішення в стилі Кремнієвої долини до фінансованої Facebook освітньої моделі «Summit Schools» в Канзасі, штаті США на Середньому Заході, він наштовхнувся на сильні заперечення навіть з боку самих дітей (Боулз (Bowles), 2019 р.).

Найбільший комерційний внесок у зміну освітньої інфраструктури вносять ті, хто формує світ бізнесу: Google, Microsoft і Apple. Крім того, деякі з найбільших у світі видавництв також беруть участь в наданні онлайнових освітніх інструментів. Наприклад, компанії Pearson, Wiley і NewsCorp., які відстежують наукові публікації та їхній зміст, також створюють теги онлайн-контенту, що дозволяє здійснювати контроль за використанням

цього контенту в таких масштабах, яких в нецифровому вигляді неможливо досягти. За словами тодішнього генерального директора освітньої компанії «Knewton» Хосе Феррейра (Jose Ferreira) у 2012 році,

«людство стоїть на порозі існування, повністю заснованого на добувані даних...освіта сьогодні є сферою, в якій дані добуваються найбільше в світі».

З цього випливає подальше питання: хто володіє великими даними? (Рупперт (Ruppert), 2015 р.) Оскільки цифрові дані використовуються все більш потужними технічними організаціями для виробництва інформації і стимулювання прийняття рішень (Вільямсон (Williamson), 2017 р.), а знання, добуті з даних в галузі освіти, все частіше використовуються для впливу на поведінку дитини в класі та за його межами й для її прогнозування, баланс сил в житті дитини змінюється у такий спосіб, який дитина не усвідомлює.

Отже, захист даних в контексті захисту дитини в освітньому середовищі виконує багато важливих функцій, але переходячи від слів до дій, такий захист повинен меншою мірою зосереджуватися на забезпеченні відповідності правилам законної обробки даних, а більшою мірою — на захисті й здійсненні прав дитини. Захист даних про дитину — це захист самої дитини з метою забезпечення її вільного розвитку і гідності, і він повинен створювати систему стримувань і противаг щодо використання влади та впливу, яких зазнає дитина. Недоторканість приватного життя також є чинником, що сприяє здійсненню подальших прав.

Діти повинні бути забезпечені інформацією та навичками, необхідними для того, щоб користуватися приватністю, захищати свою репутацію і мати свободу вираження поглядів в мережі (Ніст (Nyst), 2018 р.) відповідно до розвитку здібностей дитини.

У системі освіти роль права на приватне життя і захист даних не часто демонструється як право, що посилює інші права, підкреслюючи зв’язок між пунктом 1 статті 29 і системною боротьбою із расовою дискримінацією, ксенофобією і пов’язаною з ними нетерпимістю.

Усі цілі, викладені в п’яти підпунктах пункту 1 статті 29 КПД ООН, безпосередньо пов’язані з реалізацією людської гідності та прав дитини з урахуванням особливих потреб дитини у розвитку різноманітних здібностей, що постійно прогресують.

Оскільки освіта і цифрові інструменти нерівномірно розподілені по всьому світу, проблеми, пов’язані з деякими інструментами цифрової освіти, є новими для певних груп населення. Агенції розвитку відзначають, що біженці активно уникають деяких таборів біженців, щоб уникнути здачі біометричних даних. Аналогічні демотивувальні наслідки спостереження за даними можна виявити у галузі освіти.

Універсальність принципів КПД ООН має бути основою правозахисного підходу до захисту даних кожної дитини.

(Стаття 3) «В усіх діях щодо дітей, незалежно від того, здійснюються вони державними чи приватними установами, що займаються питаннями соціального забезпечення, судами, адміністративними чи законодавчими органами, першочергова увага приділяється якнайкращому забезпеченню інтересів дитини».

(Стаття 16), «1. Жодна дитина не може бути об’єктом свавільного або незаконного втручання в здійснення її права на особисте і сімейне життя, недоторканність житла, таємницю кореспонденції або незаконного зазіхання на її честь і гідність. 2. Дитина має право на захист закону від такого втручання або зазіхання».

Визнаючи, що персональні дані можуть оброблятися для здійснення необхідного адміністрування освіти та в інтересах дітей, закон про захист даних згідно з п. «a» ч. 4 статті 5 оновленої Конвенції №108 та п. «a» ч. 1 статті 5 Загального регламенту про захист даних (GDPR) вимагає, щоб обробка даних здійснювалася у сумлінний і прозорий спосіб щодо суб'єкта даних. Що стосується інтернет-послуг, особливості обробки даних повинні дозволяти суб'єктам даних дійсно розуміти, що відбувається з їхньою персональною інформацією. Принцип сумлінності виходить за рамки прозорості та пов'язаний з обробкою в етичний спосіб відповідно до обґрунтованих очікувань особи.

У тих випадках, коли ми дійсно розглядаємо конкретні питання захисту даних і недоторканості приватного життя в зв'язку з окремими технологіями, ми виключаємо розгляд ширших наслідків, які виходять за рамки сфери освіти та компетенції Ради. Наприклад, ми не зачіпаємо майбутні наслідки для національної безпеки, пов'язані з широким впровадженням біометричних даних в школах, включаючи збір голосових даних і відбитків пальців.

Ця доповідь покликана допомогти відповідним зацікавленим сторонам у здійсненні прав, закріплених в міжнародних і європейських конвенціях і стандартах щодо прав людини, з особливим наголосом на оновленій Конвенції №108.

II. Виклики

II.1. Проблема надання згоди

Наразі вже існує багато різнопланових законів про захист даних, то навіщо ж для освіти потрібно щось додаткове?

II.1.1 Згода повинна бути інформованою і вільно наданою

Можливо, найбільші проблеми, пов'язані з правами та свободами дитини в освітньому середовищі, також є точкою відліку для того, щоб зрозуміти, чому ця галузь заслуговує на більш пильну увагу порівняно з наявними стандартами загального захисту даних.

1. Освіта є обов'язковою для дітей та молоді.

2. Згода як основний чинник розширення прав і можливостей особи є вкрай недосконалою та майже ніколи не надається вільно у відносинах між дитиною і дорослим, між родиною і навчальним закладом.

Будьте як всі, інакше ви не отримаєте місця в цій школі. (Тейлор (Taylor), 2015 р.) За своєю суттю обов'язкова шкільна освіта може суперечити статті 12 КПД ООН, відповідно до якої поглядам дитини повинна приділятися належна увага згідно з її віком і рівнем зрілості. Цей дисбаланс може бути, а може і не бути, бажаним навчальним середовищем з огляду на культурні норми, політику і законодавство держав-членів, але такий розгляд виходить за рамки цієї доповіді.

Насправді дисбаланс влади означає, що права дитини рідко захищаються на основі принципів, які відстоюють права особистості відповідно до Конвенції №108+ і Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних, GDPR). Повсякденна практика освітніх установ часто може вимагати позбавлення прав і можливостей за замовчуванням.

> *«Як можна бачити, стеження у сфері державної освіти передбачає значно більше, ніж лише нагляд за учнями і їхньою дисципліною. Стеження є домінантою в організаційній логіці сучасних установ, яка визначає всю їхню діяльність (Ліон (Lyon), 2007 р.). [..} Ми визначаємо стеження як нагляд, моніторинг, відстеження або аналіз даних з метою контролю. Стеження як форма вироблення знань спирається на нормативні категорії зовнішніх ознак і поведінки й тим самим надає їм форми та змісту. Стеження являє собою владне діяння. Як уже давно відзначав Мішель Фоко (Michael Focault, 1980 р.), влада — це не лише контроль однієї людини над іншою, а цілий апарат матеріальних, соціальних і символічних відносин, всередині якого опиняються людські суб'єкти».* (Монахан (Monahan) і Торрес (Torres), 2009 р.)

В освіті згода не є нормою, попри те, що її часто запитують і отримують у вигляді позначки в обов'язковому для заповнення ріядочку, що не є процесом отримання згоди, а скоріше визнанням процесу обробки, про яку школа повідомила родині, з більш-менш докладним поясненням термінів і умов. Освіта з точки зору дитини загалом є обов'язковою, навіть якщо це не передбачено законом. Чи завдяки рішенню батьків, чи черезз застосування правил працівниками шкіл, дитина в системі освіти, незалежно від віку, не має владних повноважень.

Шведське управління із захисту даних визнало цей факт у своїй постанові в серпні 2019 року щодо комуни Шеллефтео, в якій зазначено, що введення системи розпізнавання

обличчя для цілей фіксації відвідуваності є незаконним, і наказало шкільним органами влади виплатити стримувальний грошовий штраф в розмірі 200 000 шведських крон (20 700 дол. США) за порушення закону про недоторканість приватного життя і захист даних. Згода на збір конфіденційних даних не могла надаватися вільно, адже не було проведено попередніх консультацій з наглядовим органом, а оцінка впливу ризиків, пов'язаних із захистом даних, була неналежною.

Важливо, що це рішення було направлене на захист прав дітей, а не допускало неналежного використання штучної «згоди».

II.1.2 Ненадання згоди не може завдавати шкоди та вважатися вільно наданою

Альтернативний підхід до отримання «згоди» полягає в тому, щоб запропонувати процес заперечення. Однак при цьому виникають ті самі проблеми, що і при отриманні активної згоди, в сесні дисбалансу влади. Сім'ї та діти не можуть легко заперечити проти надання згоди або відмовити в її наданні, не відчуваючи певного дискомфорту або стигматизації через те, що вони є іншими або «важкими» батьками. Навіть у тих випадках, коли як альтернатива пропонується «відмова» від надання згоди, або заперечення проти обробки даних, така альтернатива може означати «залишення поза грою» і відчуття того, що дітям, які ставлять на перше місце своє особисте життя, а не використання комерційних продуктів в класі або залучення батьків, буде надано нижчий рівень підтримки або навчання. Тому провайдери освіти зобов'язані застосувати такі альтернативи із дотриманням прав людини, тобто забезпечивши надійний процес, заснований на передовій практиці, який не залишає сімей без практичних можливостей здійснення всього спектру прав щодо даних (доступ до особистого файлу, обмеження і заперечення проти обробки даних або автоматизованого профілювання) і не залишає їм ніякої іншої альтернативи, крім як заперечувати проти використання повсякденних технологій в навчальному класі з тим, щоб забезпечити захист прав їхньої дитини на недоторканність приватного життя.

Базовий рівень очікуваних стандартів обробки даних з використанням постачальників технологій повинен бути підвищений при збереженні однакового рівня прийнятного альтернативного стандарту освіти (тобто заперечення проти використання провайдера не повинно призводити до зниження рівня освіти дитини).

- Згода не може бути вільно наданою і є належною для обробки даних дітей у сфері освіти лише для дуже вузького кола цілей, коли відмова від надання згоди не завдає шкоди освіті дитини. (Скажімо, фотографії шкільних заходів, які використовуються пресою).
- Дані часто збираються про дитину, проте не в самої дитини.
- Дані про дитину можуть бути створені працівниками шкіл, яких дитина і його сім'я ніколи не бачили.
- Часто вторинна обробка даних прямо передбачається законом.

За таких обставин пункт 3 статті 8 Конвенції стосовно прозорості обробки обмежує права суб'єктів даних щодо поінформованості про те, у який спосіб обробляються їхні дані, за умови, що такі випадки мають винятковий характер і що згода є статус-кво:

> В разі, якщо персональні дані не відбираються у суб'єктів даних, контролер не зобов'язаний надавати таку інформацію, якщо така обробка чітко передбачена

законом, або якщо це виявляється неможливим, або передбачає докладання непропорційно значних зусиль.

Проте, в галузі освіти згода на обробку даних не є статус-кво, навіть якщо її можуть вимагати у законних опікунів і дітей як частину угод про домашнє навчання або політики прийнятного використання комп'ютерів.

В інших умовах взаємозв'язок між батьками та дитиною може забезпечити додатковий рівень захисту та очікувань щодо нагляду між продавцем і дитиною, наприклад, при покупці застосунків для дому, для особистого використання. Очікується, що з часом ця роль зміниться, і право дитини бути почутою буде збільшуватися з віком.

«Той факт, що поглядам дитини приділяється все більше уваги, не означає однак, що власні погляди батьків на питання, що зачіпають їхніх дітей, можуть просто ігноруватися як неактуальні або що їх всеосяжна відповідальність може бути замінена або проігнорована в тих випадках, коли це зручно. Передбачається, що цей процес натомість буде поступовою зміною балансу сил і відповідальності батьків за своїх дітей в міру появи досвіду, досягання зрілості та підвищення здатності кожної дитини розуміти наслідки дій і рішень». (Андерсон (Anderson) та ін., 2009 р.)

У шкільному середовищі ці взаємозв'язки, як і раніше, грають важливу роль, однак вони не забезпечують такого ж рівня захисту за участі установ, і натомість сім'ї можуть зіткнутися з тим, що їхні власні преференції суперечать політиці школи.

II.1.3 Згода не може бути повністю інформованою відповідно до чинної практики

Впровадження технологій в це середовище ще більше позбавляє дітей прав та можливостей, оскільки вводить нових суб'єктів, які мають більше контролю і влади над тим, як дитина взаємодіє із застосунком або платформою, ніж дитина, її сім'я і нерідко її вчитель.

Багато компаній і розробників, які займаються певним продуктом, є прихованими, зокрема, у разі, коли персональні дані підлягають обробці не лише для безпосередніх шкільних цілей застосунку, як-от, скажімо, домашні завдання, відстеження поведінки, спілкування між домом та школою, або обробка безготівкових платежів; але для численних організацій-партнерів, дочірніх компаній та сторонніх обробників даних, які можуть передбачати у своїх положеннях та умовах певні повноваження щодо персональних даних як активів у разі продажу, злиття або поглинання компанії.

Крім безпосередньої обробки даних третіми особами, може існувати ще один рівень обробки персональних даних, запроваджений розробниками, які запозичують код з бібліотек коду, копіюють його з чужого коду і впроваджують його у свої власні творіння. Це може привести до такої поведінки застосунків і обробки персональних даних, які навіть розробник в точці продажу або розповсюдження не зможе повністю зрозуміти або контролювати, і може мати непередбачені наслідки.

Таким чином, школа не може отримати юридично дійсної згоди на обробку персональних даних від імені своїх постачальників.

Діти та законні опікуни просто не можуть зрозуміти, на що вони дають згоду.

Але саме обсяг навіть очевидних взаємодій з третіми сторонами змушує школи

говорити, що вони не можуть керувати згодою.

Це може частково пояснити, чому зараз отримання згоди розглядається школами як важке завдання, і компанії можуть стверджувати, що це створює «бар'єр для інновацій». Школи можуть ігнорувати згоду, оскільки керування згодою є занадто складним для шкіл або компаній, а школи часто дають «згоду за дорученням».

Це дійсно дозволяє розкривати інформацію в надзвичайних ситуаціях, які за своєю природою специфічні, стосуючись безпосереднього піклування про дитину та її життєво важливих інтересів, і обмежені в часі. Таким неправильним чином школи отримують можливість залишати поза увагою права сімей і дітей при виконанні повсякденних завдань з обробки даних.

II.1.4 Приклад припущення згоди

Інтелектуальний центр «Nesta» в Англії розпочав випробувальну програму спільно з Міністерством освіти для тестування продуктів освітніх технологій edTech в середині 2019 року. Що стосується обробки персональних даних, то вони припускають, що нема потреби запитувати згоду, об'єднуючи комерційну обробку даних третьою стороною з обробкою даних шкілами в рамках свого суспільного завдання, а також не враховують додаткові вимоги щодо даних особливої категорії (конфіденційних).

> *«Оскільки цей проєкт дозволяє отримати фактичні дані про продукти, що сприяє досягненню цілей сьогоднішніх шкіл і коледжів, і відповідає суспільним інтересам, нема потреби в отриманні індивідуальної згоди*». (Nesta, Випробувальний полігон інновацій «EdTech Innovation Testbed», 2019 р.)

Економічний стимул для розробки освітніх технологій на експорт очевидний. Як уникнути при цьому експлуатації дитячого населення держави буде залежати від стану правовладдя і здатності громадян покладатися на його застосування, коли практика визначається рішеннями, що ґрунтуються на неналежній етичній позиції політиків, або політичними цілями.

Таким чином, проблема має подвійний характер:

- Як забезпечити захист даних і приватного життя дитини, коли згода не є законною підставою для обробки даних і сприймається школою як відсутність вимоги діяти за обопільною згодою.
- Як належним чином отримати згоду, якщо вона є законною підставою для обробки даних і є обов'язковою, беручи до уваги роль батьків/сім'ї та роль дитини, а також їхні взаємини між собою і стосунки з навчальним закладом.

II.1.5 Згода та умови договору можуть підлягати перегляду в контексті шкіл

Патріархальна модель влади більшості західних навчальних закладів і систем та притаманний їй дисбаланс влади вимагають іншої моделі надання прав і можливостей дітям і сім'ям, кращої, ніж це передбачено чинним законодавством щодо захисту даних. Сучасні моделі відстоюють індивідуальну автономність і згоду як потужну гарантію контролю над даними.

Думки дітей повинні бути почуті відповідно до їх віку та здібностей. Законодавчі рамки варіюються в залежності від юрисдикції, наприклад, у Великобританії вік, з якого починається кримінальна відповідальність, становить 10 років. Коли йдеться про школу, інтереси дітей зазвичай представляють їхні законні опікуни або установа.

Така інституційна модель може бути чи не бути бажаною з точки зору автономії та особистих прав, але якщо школи не готові до значного скорочення числа суб'єктів, що беруть участь в обробці даних, то іншої реально керованої моделі може і не бути.

Це, однак, означає, що необхідна міцна законодавча база, для того, щоб потоки даних, які проходять через установу, входять і виходять з неї, жорстко контролювалися з чіткою підзвітністю.

Наприклад, відповідно до законодавства США про освіту, Закон про права сім'ї на доступ до інформації, пов'язаної з освітою, і її захист (FERPA) вимагає, щоб установи, що фінансуються з федерального бюджету, в рамках програм, підвідомчих Міністерству освіти США, дотримувалися певних процедур щодо розкриття та ведення обліку освітніх даних.

Це є ще однією з потенційних моделей керування комунікаціями узгоджених компаній і третіх осіб, з якими школа має намір ділитися персональними даними протягом навчального року дитини.

Захист даних, що надається цією американською моделлю, передбачає достатні очікування щодо поведінки компанії. Умови контракту узгоджуються на рівні регіональних штатів. Стандарт, затверджений FERPA, може бути досягнутий лише компаніями, які готові дотримуватися і підтримувати загальні попередньо узгоджені умови протягом усього періоду їхньої дії.

Насправді має бути винятком, щоб комерційна третя сторона була контролером даних, а не обробником персональних даних школярів, зібраних під час їхнього навчання.

Тягар проведення перевірки зменшується для сімей на індивідуальному рівні внаслідок наявності в шкільній системі належним чином підготовленого персоналу на регіональному рівні, який може приймати рішення про закупівлю відповідно до результатів ретельної оцінки захисту даних і етичного впливу, а потім укладати контракти з компаніями, даючи школам, по суті, зелене світло для укладення контрактів з такими компаніями на місцевому рівні.

Окремі особи та сім'ї можуть отримати доступ до інформації про оцінку захисту даних і етичні питання в режимі онлайн або за запитом школи, і, отже, можуть ставити питання і бути докладно поінформованими, якщо вони того бажають. При цьому створюються рівні умови для всіх, щоб забезпечити однаковий рівень довіри до стандартів виконання норм що, як очікується, дозволить компанії взагалі взаємодіяти з державною системою освіти.

FERPA класифікує захищену інформацію за трьома категоріями: освітня інформація, інформація, що дозволяє встановити особу, і довідкова інформація. Обмеження, що накладаються FERPA, варіюються в залежності від кожної категорії.

Однак американська модель недостатньо захищає приватність, та і всі персональні дані, які можуть перебувати в будь-якій з цих категорій, оскільки неможливо розділити персональні дані на окремі та чіткі категорії, адже природа персональних даних залежить не лише від самої інформації, а й від її контексту, а також від того, чи може контролер володіти або отримати у володіння інші персональні дані, які перетворять перший набір даних у такі, що ідентифікують особу.

З метою захисту прав школи зобов'язані запропонувати можливість заперечити проти

використання стороннього провайдера, а також школи зобов'язані підтримувати належний рівень альтернативного надання освіти в разі, якщо сім'я або дитина заперечує проти певного продукту.

Для того, щоб зрозуміти межі того, що дозволено і вимагається на підставі згоди, а не на інших законних підставах, працівники шкіл потребують набагато більшої ясності та чіткіших вказівок. Практичні міркування вимагають уваги до того, як школи ефективно спілкуються з дітьми та сім'ями, а не тільки як вони виконують свої законні зобов'язання.

II.2. Свобода вибору дітей

Використання інтернету може становити особливі проблеми для дітей, які часто не розуміють комерційну природу використовуваних ними цифрових послуг, або як ці послуги використовують їхні дані. Втім, якщо дітям важко зрозуміти, як збираються, обробляються, передаються і монетизуються їхні персональні дані онлайн, коли вони самостійно підключаються до певних послуг, то їм практично неможливо зрозуміти це, коли працівники школи приймають таке рішення від імені дітей. Навіть якби діти були належним чином освічені та поінформовані про те, як керувати своєю конфіденційністю, вони не можуть цього зробити, якщо школи самостійно від імені дітей приймають рішення про те, які програми й платформи вони використовуватимуть.

Питання, чого хочуть діти, постає дуже рідко. (Стоілова (Stoilova), Лівінгстон (Livingstone) і Нандагірі (Nandagiri), 2019 р.)

Комерційним інтернет-провайдерам можна відправляти персональні дані дітей, що містяться у шкільній системі управління інформацією, без попереднього інформування сімей або дітей. Найбільшою проблемою щодо ролі шкіл в управлінні освітніми даними може бути необхідність їм усвідомити, що їхнє суспільне завдання із надання освіти, яке вимагає певної обробки персональних даних, не повинне за замовчуванням означати, що ті ж самі персональні дані можуть передаватися комерційним постачальникам застосунків і платформ, які не мають законодавчо встановлених зобов'язань щодо надання освіти, і що компанії, які обробляють дані для своїх власних цілей, як-от розробки нових продуктів, не виконують такого суспільного завдання.

Діти мають мало можливостей для автономії в сфері освіти або для контролю над розповсюдженням своїх персональних даних. Але все частіше школи також втрачають контроль над ними. Існують загальні «ланцюжки» даних, що передаються від одного контролера до іншого, які беруть свій початок від збору або створення даних в освітньому середовищі.

II.2.1 Школи та універсальні «click-wrap» угоди

Школи укладають багато контрактів із третіми сторонами, часто приймаючи стандартний набір умов, які вимагають, щоб користувач натиснув кнопку прийняття угоди, щоб при першому використанні отримати доступ до послуги або застосунку. Такі типи угод зазвичай мають назву «click-wrap» угоди. Ці угоди можуть передбачати отримання великих обсягів даних про учнів із масштабованих шкільних систем управління інформацією на умовах компанії та без можливості школи обмежити пакети даних, що відправляються до компанії, лише мінімально необхідним обсягом. (Міністерство освіти США (Центр технічної допомоги з питань конфіденційності), 2015 р.) Наприклад, системи громадського харчування із безготівковою формою оплати можуть мати доступ до даних про релігію або етнічне походження.

Ба більше, зміни до цих умов неможливо відхилити без припинення послуги. Вони можуть бути надіслані електронною поштою адміністратору шкільної системи, такими

компаніями, як «Google for Education», і будь-які нові умови або зміни у вимогах компанії до обробки рідко будуть доведені до відома законних опікунів або дітей.

II.2.2 Видобування даних державними органами накладає зобов'язання на школи

Окрім нерівних стосунків в угодах між компаніями та школами, які хочуть отримати послуги, існує значний дисбаланс влади в стосунках між школами та державними органами на національному та місцевому рівнях. Школи, що залежать від державного фінансування, не володіють достатньою адміністративною здатністю відхиляти національні запити про надання даних або необхідними технічними засобами приховувати дані від автоматизованих систем вилучення даних або збору даних під час перепису населення, де обов'язкові для заповнення поля визначені державою. У шкіл може не бути вибору щодо подання даних в тих випадках, якщо законодавство зобов'язує школу подавати дані, якими вона володіє.

Держава мала б змушувати надавати конфіденційні персональні дані тільки у вузьких і чітко визначених цілях, і майже у всіх випадках конфіденційні дані повинні зберігатися в місцевих, а не в загальнодержавних системах. (Андерсон (Anderson) та ін., 2009 р.)

> «Державна політика та діяльність дітей онлайн порушує всілякі запитання щодо конфіденційності та цілісності даних, і життєво важливе питання про те, хто може або повинен давати згоду на збір, зберігання та поширення конфіденційної інформації про дітей, виходить на перший план». (Дауті (Dowty), 2009 р.)

II.2.3 Учні та законні опікуни практично не мають права голосу на своїх власних умовах

Як свідчить Управління комісара з питань інформації Великої Британії, державним органам, роботодавцям та іншим організаціям, які мають певну владу, може виявитися складнішим довести правомірність вільно висловленої згоди. Відповідно, не варто вважати це звичайною підставою для щоденної обробки базових даних.

Учні та сім'ї все частіше заперечують проти нав'язування технологічних рішень у сфері освіти, які стверджують, що повертають дітям втрачену свободу вибору. У той час як учасники програми «Summit» та її спонсори, включаючи Білла Гейтса, Марка Цукерберга та Ініціативу Чан-Цукерберга, стверджують, що студенти програми «Summit» можуть продемонструвати «більшу відповідальність за свою навчальну діяльність», студенти з міста Макферсон, Канзас, насправді беруть на себе контроль над своєю освітою, залишаючи школу і беручи участь в сидячих страйках на знак протесту проти її впровадження. (Батьківська коаліція за недоторканність приватного життя студентів, 2019 р.) Після закінчення школи діти зазвичай більше не мають постійних відносин з навчальним закладом, проте такі заклади можуть продовжувати обробляти дані дитини або підтримувати відносини з третіми сторонами, які здійснюють таку обробку. Інформація про збережені дані та їхню обробку повинна передаватися сім'ї та дитині, доки їхні дані продовжують оброблятися, можливо, на щорічній основі.

II.3 Постійний єдиний запис

11.3.1 Важливість «чистого аркуша»

У 2009 році Робоча група з питань реалізації статті 29 визнала, що, «оскільки діти розвиваються, дані, що їх стосуються, змінюються і можуть швидко застарівати та втрачати актуальність для первісної мети зборіання даних. Коли це відбувається, дані не повинні більше зберігатися».

Десять років по тому, в червні 2019 року, Експертна робоча група високого рівня з питань штучного інтелекту (HLEG-AI) у своєму документі «Рекомендації щодо політики та інвестицій в галузі надійного штучного інтелекту» виступила з пропозицією:

> «Дітям має бути забезпечено вільний та неконтрольований простір для розвитку, і після досягнення дорослого віку їм варто надавати «чистий лист» у будь-яких державних чи приватних сховищах даних».

Ці рекомендації та чинні положення про зберігання даних найчастіше не беруться до уваги у сфері освіти на підставі суб'єктивних тверджень про винятки, пов'язані з дослідницькою роботою, поєднання видалення ідентифікаційних даних зі знеособленням, а також безризикової політики управління записами, що не розглядає надлишок даних як проблемний актив. Для забезпечення дотримання положень про зберігання даних необхідні відповідні правозастосовні заходи.

Розвиток технологій дозволив зберігати необмежені обсяги особистої інформації про кожну дитину в школі, цілій країні або навіть в усьому світі в потенційно постійних записах.

11.3.2 Дитина не може контролювати надмірне збереження даних, що може привести до зловживань

Ці записи можуть бути швидко поширені на інші комп'ютери в хмарних службах і скопійовані необмежену кількість разів невизначеними особами, безкінечно. Вся освітня історія дитини може бути передана одним натисканням миші. Інформація, яка колись знаходилася в локальних журналах і займала велику кімнату, повну шаф для зберігання документів, може бути розміщена на портативному пристрої, а ціла база даних, що складається з мільйонів записів, може бути швидко скопійована і завантажена. Записи, які постійно зберігаються в державних установах щодо етнічної належності, національності або релігії, використовувалися упродовж всієї історії для знущань над цілими громадами.

Неналежне використання загальнодержавних записів з учнівськими даними Міністерством внутрішніх справ Сполученого Королівства з метою забезпечення дотримання імміграційного законодавства було виявлено 2016 року, коли Міністерство освіти додало інформацію про національність до шкільного перепису. (defenddigitalme, 2016 р.) Ризики, пов'язані з неналежним використанням даних державними установами у не пов'язаних з навчанням цілях, занадто великі та свідчать про те, що загальнодержавні записи не повинні зберігатися на індивідуальному рівні, що передбачає можливість ідентифікації.

У 2002 році в Англії вперше були зібрані комплексні дані шкільного перепису дітей у віці від 2 до 19 років, включно з прізвищами учнів. Парламентаріїв запевнили стосовно змін, внесених тодішнім державним міністром освіти та професійної підготовки до «Центральної бази даних про учнів», що «Міністерство не зацікавлене у встановленні особи окремих учнів як таких і буде використовувати цю базу даних виключно в статистичних цілях, а доступ до даних з прізвищами учнів матиме тільки технічний персонал, що безпосередньо бере участь у процесі збору даних».

Тринадцять років по тому за іншого уряду дані про прізвища дітей, дату народження, стать та адресу почали таємно зіставляти з записами, які Міністерство внутрішніх справ щомісяця запитувало з метою забезпечення дотримання імміграційного законодавства.

11.3.3 Діти мають право на свою репутацію

Довгострокові наслідки постійних записів і рішень, що приймаються на їхній основі, можуть супроводжувати дітей навіть у дорослому житті в результаті державних та комерційних дій. Такі дані можуть бути використані згодом, а їхня ціль може бути легко змінена без відома людини.

Репутація дітей все частіше формується дедалі більшим обсягом інформації про них в інтернеті. Це не лише впливає на міжособистісні стосунки дітей, але також може вплинути на їхню здатність отримати доступ до послуг і працевлаштування, коли вони розпочнуть доросле життя. (ЮНІСЕФ, Приватність та свобода вираження поглядів дітей в інтернеті, Матеріали для обговорення та галузевий інструментарій, 2018 р.).

Життєвий цикл даних повинен розглядатися з особливою увагою, коли йдеться про дітей. Діти повинні мати право обмежувати розкриття інформації приватним компаніям для забезпечення свого всебічного розвитку та успішного початку дорослого життя, зокрема в тому, що стосується конфіденційних даних, які не завжди відповідають критеріям даних особливої категорії. Наприклад, варто передбачити можливість припинення розповсюдження шкільних записів з історією поведінки без згоди дитини, якщо мета виходить за рамки безпосереднього піклування про неї; записів, які стосуються насильства, протиправних дій сексуального характеру або наркотиків, якщо кримінальність можна не розголошувати; проте як показники поведінки та некримінальні записи вони можуть передаватися на довічне зберігання третім особам без відома дитини (або вже дорослої людини) і можуть відправлятися за межі школи або до інших юрисдикцій.

При оцінці випадків обробки таких даних існує значна нерівність між керівництвом школи та дитиною, і обговорення цього питання з сім'ями має бути проведено до передачі даних третій стороні. Відмова від обробки даних є недостатньо надійним механізмом захисту, зокрема через те, що так багато даних може бути отримано від шкіл автоматизованим шляхом.

Коли уповноважені люди не можуть здійснювати ефективний нагляд за рішеннями ШІ, виникає ширше питання про те, чи слід взагалі використовувати ці системи замість методів з участю людей, зокрема, для обробки даних особливих категорій. (Мантелеро (Mantelero), 2018 р.)

11.3.4 Комерційні вимоги щодо надмірного збереження даних або маркетингових цілей необхідно відхиляти

Комерційні постачальники освітніх продуктів (edTech), забезпечуючи портативність даних і передачу їх школам через того ж самого комерційного постачальника, не повинні зберігати унікальні та ідентифікаційні записи дітей поза межами обсягів, необхідних для їхньої освіти. Подальше необхідне зберігання для цілей аудиту має забезпечуватись місцевим навчальним закладом, а не постачальниками. Результати екзаменів містяться в табелі успішності і мають бути доступними, доки особа бажає на них посилатися, або доки роботодавці та інші особи можуть запитувати підтвердження результатів. Однак комерційні провайдери не повинні зберігати детальні записи про поведінку в класі, хвороби та відвідуваність, а також про використання застосунків.

Зазвичай комерційні онлайнові освітні сервіси не дозволяють працівникам шкіл видаляти віртуальні класи, облікові записи або онлайновий контент (включно з інформацією про учня), а компанії замість цього архівують їх на термін від одного до двох років або більше. (Уповноважений з питань захисту інформації та недоторканності приватного життя в Онтаріо (IPC Ontario), Глобальна правоохоронна мережа захисту приватної таємниці (GPEN), Звіт щодо перевірки конфіденційності освітніх онлайн-сервісів, 2017 р.).

Деякі застосунки пропонують обмежене період часу, протягом якого школа може просити видалення даних про учня, після чого компанія зберігає їх довічно.

11.3.5 Практичні приклади застосування постійних записів

Математичний застосунок «mathletics», що використовується дітьми у всьому світі, донедавна пропонував граничний проміжок часу в один рік, коли вчителі повинні звернутись із проханням про видалення даних облікового запису дітей, в іншому випадку компанія зберігає псевдонімізовані дані необмежений час. Крім того, компанія «3P learning» вважає, що IP-адреса, всупереч рішенню Суду ЄС у справі Брейера, не є персональною інформацією, і замість цього вимагає її безстрокового зберігання разом з даними про поведінкову діяльність.

> «Погоджуючись з умовами, реєстранти надають нам право використовувати цю анонімну інформацію для власних цілей, як-от підготовка статистичних звітів або поліпшення і зміна контенту наших продуктів».

Платформа відстеження поведінки «Class Dojo», навпаки, заявила, що вони не створюють **не** постійних записів.

> *«Дані профілю, які не збережені батьками або учнем, втрачають силу і видаляються через рік».*
>
> І вони зобов'язуються не використовувати персональні дані,
>
> *«Ми не продаємо, не надаємо в оренду і не передаємо вашу особисту інформацію (або інформацію дітей) третім особам в рекламних або маркетингових цілях».*

Проте, бізнес-модель цих компаній є такою, яку деякі сім'ї можуть вважати нерозумною або неетичною. Компанії покладаються на використання електронної пошти законних опікунів, пов'язаної з обліковим записом дитини. Обробка персональних даних, наданих школою, отриманих для безпосередніх цілей навчання дитини в школі, що є суспільним завданням, не повинна використовуватися для подальшого збуту продукції сім'ям, для комерційних цілей компанії, які виходять за рамки суспільного завдання і, отже, може розглядатися як така, що не відповідає законній підставі для обробки даних у вигляді виконання суспільного завдання.

«Ми плануємо заробляти гроші коштом преміальних функцій, які ми розробляємо і за які можуть платити школи та батьки». (ClassDojo: У чому помилялась The New York Times)

II.4 Управління ідентифікаційною інформацією

Як молодь формує відчуття власного «я»? Процеси буття і становлення через соціальну та інституційну взаємодію є важливими для дітей. З віком діти розвиватимуться та опановуватимуть різні особистості.

Необхідність збереження анонімності дітей молодшого віку онлайн зазвичай пов'язана з навчанням безпечної поведінки в інтернеті і захистом персональних даних від сторонніх. Особиста інформація про дітей здебільшого пов'язана з їхньою сімейною

інформацією в шкільних записах та є необхідною для реєстрації облікових записів в освітніх застосунках. Таким чином, втрата конфіденційних і персональних даних може колективно впливати на сім'ю або спільноту, а не лише на особу, коли йдтьсяе про освітні продукти та системи.

Часто вважається, що діти до 11 років занадто малі для того, аби взагалі розуміти наслідки конфіденційності в мережі. Дослідники з Оксфорда виявили, що діти можуть добре виявляти та формулювати певні ризики щодо приватності, як-от надмірний обмін інформацією або розкриття реальних персональних даних в мережі. (Чжао (Zhao) та інші, 2019 р.) Сім'ї, однак, рідко розуміють нерівність між компаніями та дітьми в цифрову епоху, а отже діти особливо вразливі до експлуатації даних, частково через те, що у них слабке уявлення про ризики, пов'язані з накопиченням персональних даних з плином часу, а також через те, що вони можуть стати першим поколінням, життя якого зберігається в даних компаній від самого народження.

Нещодавні дослідження довели, що хоча підлітки, як правило, стурбовані тим, що їхні особисті дані можуть бути ідентифіковані невідомими користувачами, і дбають про свою репутацію, вони не усвідомлюють потенційної загрози повторної ідентифікації через окремі фрагменти інформації, якими вони діляться, скажімо, зображення або геолокація, які не вважаються ідентифікаційними, і, зокрема, їм важко зрозуміти концепцію динамічних даних тривалого спостереження. (Чжао (Zhao) і ін., 2019 р.)

На відміну від змін в характері дитини з плином часу, в шкільній системі може створюватись незмінний центральний запис, обсяг якого зростатиме і зберігатиметься.

Оцифрований запис про учня можна також копіювати необмежену кількість разів. А контекст збору даних, будь-які зроблені висновки і якість запису можуть бути втрачені при кожному копіюванні та спільному використанні.

Наратив персоналізації, що пронизує багато навчальних технологій, зосереджений на індивідуумі. Індивідуалізація полягає в перетворенні людської «ідентичності» із «наданого» стану буття в «завдання» становлення. (Лівінгстон (Livingstone), 2016 р.)

Право на вільний вибір, вільний від втручання, є основоположним для автономії та повного і вільного розвитку особистості.

Стрижнем основоположного права на недоторканність приватного життя як громадянина є свобода від незаконного втручання з боку держави. Це є передумовою свободи розвитку своєї ідентичності в демократичному суспільстві. (Хільдебрандт (Hildebrandt), 2015 р.)

Постійний шкільний запис і надання його іншим збільшує ризик втрати персональних даних, контролю над приватними рішеннями через вплив і рішення, що приймаються іншими щодо втручання у ваше життя, а також дискримінацію через те, ким система вважає нас, як в дитинстві, так і в дорослому житті.

Резолюція Мсіжнародної конференції ICDPPC щодо платформ електронного навчання, яка може бути більш широко застосована до будь-яких персональних даних в навчальному середовищі, рекомендує наступне:

«Відповідно до принципу мінімізації даних і в максимально можливій мірі повинна бути мінімізована або виключена можливість ідентифікувати особистість індивідуумів та їхні персональні дані, оброблювані за допомогою платформи електронного навчання».

II.4.1 Перевірка віку та ідентифікаційних даних

Наразі поширюються заклики до обов'язкового використання реальних особистих даних та впровадження механізмів перевірки віку дітей. Однак і те, й інше загрожує конфіденційності дітей і призводить до втрати безпечного простору, який надає анонімність.

Перевірка віку є певною формою «посвідчення особи», коли необхідно визначити лише один атрибут (вік). Метод, за допомогою якого це робиться, не нав'язується, проте було б неправильно, якби бажання забезпечити конфіденційність і захист призводило б до появи більшої кількості нових баз даних і більшого ризику. (Бут, П. (Booth, P.), 2017 р.)

У 2008 році Центр інтернету та суспільства ім. Беркмана Гарвардського університету опублікував доповідь щодо дітей в інтернеті і дійшов висновку, що перевірка віку є недоцільною.

> «Перевірка/автентифікація віку/особистості не є рішенням, оскільки такі заходи належать сфері соціальних онлайн мереж або будь-яким іншим онлайновим системам, де неповнолітні взаємодіють з дорослими. Вже довгий час ми вважаємо, що ризики є значними, а переваг немає». (Заява «Symantec», 2018 р.)

Безпечні застосунки та платформи, дозволені до використання в школі та підтверджені відповідними процедурами закупівлі та ретельними перевірками, а також відповідна фільтрація і блокування контенту повинні створювати середовище, що не потребує додаткового захисту, пов'язаного з віком.

Однак педагоги також передають управління ідентифікаційними даними на аутсорсинг широкому колу компаній, включно з брокерами даних, не тільки для перевірки віку, але і для соціальних медіаплатформ, багато з яких дозволяють здійснювати перевірку облікових даних для входу в інші застосунки та платформи, що використовуються для виконання домашніх завдань і проведення занять в класі.

11.4.2 Дані для входу в соціальні медіа як засіб перевірки ідентифікаційних даних

В резолюції ICDPPC (2018 рік) школам рекомендується:

> «*Уникати використання даних для входу до соціальних мереж, оскільки це може призвести до надмірного збору і розкриття докладної інформації про профіль та іншої ідентифікаційної інформації між сайтом соціальної мережі та платформою електронного навчання і може обмежити можливості учнів запобігати відстеженню їхньої мережевої діяльності в інтернеті*».

Facebook, як приклад, зазвичай використовується як інструмент групового адміністрування в деяких школах, зокрема, для дітей старшого віку, а також у технічних коледжах і коледжах підвищення кваліфікації, але компанія все частіше зазнає критики з боку американських і європейських регуляторних органів через те, як вона поводиться з інформацією користувачів і не користувачів шляхом відстеження та аналізу вебсайту. Її політика реєстрації та використання реальних прізвищ означає, що персональні дані використовуються компанією, але можуть бути об'єднані зі шкільними обліковими записами, якщо це вимагається персоналом.

Працівники шкіл повинні дуже ретельно враховувати свої зобов'язання щодо захисту даних про учнів та школу, якщо вони вимагають використання таких платформ, і ретельно оцінювати їх правову підставу. Приховане використання персональних даних, а також приховане маніпулювання з боку Facebook новинними стрічками користувачів з

метою викликати емоційну реакцію, як видається, робить їх цінності несумісними із зобов'язанням педагогів поважати права і свободи дитини. (Форбс (Forbes), 2014 р.)

Однак це не зупиняє пропагандистів технології від закликів використовувати її в класі. («Education Foundation», 2013 р.) У 2013 році вони заявили, шо, «вона вже широко використовується в коледжах і університетах в усій Великій Британії та в усьому світі, але потенційно вона може змінити життя вчителів, шкіл і класних кімнат». Це «швейцарський армійський ніж» серед інструментів, що відкриває молоді можливості навчання як в класі, так і за його межами».

Діти та підлітки мало розуміють, що може зробити компанія з обраними ними шляхами нібито управління своїми настройками конфіденційності, використовуючи персональні дані, надані для цілей реєстрації користувачів. Такого використання слід уникати в сфері освіти.

Школи та застосунки edTech не повинні використовувати соціальні мережі та інші персональні дані про дітей або членів сім'ї, отримані з відкритих джерел, для дотримання принципу мети.

II.4.3 Біометричні дані для перевірки ідентифікації

Управління ідентифікаційними даними може здійснюватися в школі різними способами, але часто така перевірка відбувається шляхом взаємодії між школою і сторонніми постачальниками технологій або на місці, або через служби, підключені до інтернету. Біометричні дані забезпечують високу, хоча і все ще недосконалу ступінь впевненості в ідентифікації. Проте обговоренню досі підлягає питання, чи слід використовувати такі високорівневі методи перевірки особистості для операцій низького рівня, як це робиться сьогодні в школах, скажімо, для ідентифікації дитини, яка бере книги в бібліотеці, або для оплати їжі та напоїв в шкільній їдальні за допомогою систем безготівкових розрахунків.

Технології виявлення і розпізнавання обличчя вже деякий час застосовуються в системі освіти як засіб перевірки особистості учнів і відвідувачів шкіл. Однак технологія стає все складнішою, тож способи її застосування можуть також ускладнюватись.

Зараз така технологія використовується для зчитування виразів і відстеження осіб, щодо яких відсутня ідентифікаційна інформація, з камер у торгових центрах з наміром з'ясувати стать, вік і «настрій» окремих покупців (Енском (Anscombe), 2017 р.). Показово, що ці застосунки починають переходити з технології виявлення до технології ідентифікації, оскільки комерційні точки продажу прагнуть зв'язати дані камер з інформацією про покупку. Коли системи розпізнавання обличчя отримають широке поширення, застосунки з виявлення (як-от задля з'ясування «настрою») також впроваджуватимуться в таких цілях, як маркетинг і безпека. Наприклад, Міністерство національної безпеки США розробляє системи для виявлення «злого наміру» (наміру завдати шкоди) за допомогою візуальних і біометричних сигналів (Акерман (Ackerman), 2017 р.). (Андреєвич (Andrejevic) і Селвін (Selwyn), 2019 р.).

В інших, менш звичайних обставинах діти можуть підлягати розпізнаванню за обличчям для перевірки їхньої особистості протягом певного проміжку часу. Наприклад, при тестуванні та проходженні екзаменів біометричні ідентифікаційні системи, що використовують розпізнавання обличчя, все частіше використовуються для перевірки особистості кандидата не лише при вході, а й протягом усього періоду проходження тесту, шляхом постійного повторного зняття біометричних характеристик кандидата.

У серпні 2019 року регуляторний орган Швеції ухвалив, що впровадження системи розпізнавання обличчя з метою ідентифікації учнів в рамках реєстрації відвідуваності занять є незаконним (див.: II. 6.2 Біометричні дані), а аналогічні впровадження з боку компанії «Aurora Computer Services» вже потрапили до новин 2010 року в Англії.

Інші біометричні портативні пристрої та системи розпізнавання обличчя розробляються з метою збору даних про емоції учнів, їхню залученість і уважність в шкільному середовищі, як спосіб отримання вчителями зворотних даних про соціальні та емоційні навички й характеристики учнів (IEEE, 2018 р.), а також для «персоналізації» методів навчання. Більш детально це питання розглядається в частині II.10.8 «Біометричні дані».

Всесвітній економічний форум виступив за розширене використання «сприяння соціальному та емоційному навчанню за допомогою технологій» у 2016 році.

Малоймовірно, що сьогоднішнє законодавство про захист даних є достатнім для захисту дітей від все більш агресивного використання особистої інформації про їхні фізичні характеристики, включно з аналізом ходи та емоцій, які збираються не в цілях перевірки особистості окремої людини, відповідно до статті 6 та особливих категорій даних в рамках Конвенції, а для того, щоб зробити висновок про їхні емоції та наміри.

II.5 Джерела даних і непрозора обробка даних

Не всі дані є рівними, і, зокрема, слід визнати, що великий обсяг даних про дітей в галузі освіти є лише думкою або припущенням. В сфері освіти існують великі відмінності між джерелами даних:

- Наданих сім'єю
- Наданих дитиною
- Створених вчителями
- Створених шкільними адміністративними системами
- Створених органами державної влади
- Створених компаніями освітні інструменти та платформи, які знайомі дітям і сім'ям,
- Створених компаніями інструменти, яких ніколи навіть не бачили школи, діти та сім'ї.
- Створені третьою стороною, що не має відношення до системи освіти, як-от брокерами даних або компаніями соціальних мереж, які можуть бути пов'язані з навчальними записами.

II.5.1 Приховані дані

До прихованих даних належать записи, засновані на даних та/або метаданих, які використовуються компаніями для створення профілів користувачів стосовно використання застосунків, наприклад, з метою включення учнів або їхніх батьків до цільової аудиторії для реклами та маркетингу. Про такі дані невідомо вчителям, законним опікунам або дітям, і вони можуть порушувати закони про електронну конфіденційність та захист прав користувачів, а також про захист даних.

Наприклад, ГО «Privacy International» провела у Великій Британії дослідження дедалі більш розповсюдженої тенденції використання в класі застосунків щодо психічного здоров'я і добробуту, деякі з яких, безсумнівно, зазнають тих самих недоліків, що і застосунки щодо психічного здоров'я, призначені для дорослих.

«Privacy International» опублікувала дослідження 136 популярних вебсторінок, пов'язаних з психічним здоров'ям у Франції, Німеччині та Великобританії, згідно з яким вебсайти обмінюються персональними даними користувачів з рекламодавцями, брокерами даних і великими технічними компаніями, як-от Google, Facebook і Amazon.

Деякі вебсайти, присвячені тестуванню на наявність депресії, також передають відповіді на питання і результати тестування третім сторонам. Отримані результати свідчать, що деякі вебсайти, присвячені психічному здоров'ю, розглядають персональні дані відвідувачів як товар, не виконуючи при цьому своїх зобов'язань за європейськими законами про захист даних і недоторканність приватного життя. («Privacy International», 2019 р.)

Приховані дані включають також нову інформацію або висновки, здобуті завдяки зв'язуванню та вторинному використанню даних, зібраних для освітніх цілей, але які використовуються місцевими органами влади для інших суспільних оцінок, таких як прогнозна оцінка соціальних ризиків.

Такі способи використання перенаціlених даних не мають нічого спільного з тим, на що багато людей можуть розраховувати, коли відправляють свою дитину в школу, і мають далекосяжні наслідки для приватного і сімейного життя.

II.5.2 На практиці перенаціленню треба запобігати

Може здатися ефективним, коли дані збираються лише раз, а використовуються багаторазово, але така ситуація може призвести до необачного і неналежного використання даних, коли цілі не є сумісними або прозорими для дитини або сім'ї.

В системах освіти може чинитися тиск щодо повторного використання даних, зібраних для безпосередніх цілей в школі, місцевими та національними органами влади для непрямих цілей порівняльного аналізу даних, щодо об'єднання даних про учнів в озера даних для використання третіми сторонами, а також щодо пов'язування учнівських даних шкіл з даними студентів вищих навчальних закладів та з динамічними наборами даних тривалого спостереження інших державних відомств (дані про результати випускних іспитів LEO, Міністерства освіти Великобританії, дані про соціальний стан і оподаткування).

Зростає зв'язок освітніх даних з іншими адміністративними даними про дитину або сім'ю для оцінки ступеню ризику і прогнозних втручань у виявлення випадків жорстокого поводження з дітьми, домашнього насильства та скорочення числа виключень зі школи (Кардіфська лабораторія інформаційної справедливості (Cardiff Data Justice Lab), 2018 р.). Ці дані ніколи не формувалися і не збиралися для таких цілей. Значний ризик виникає тоді, коли рішення ґрунтуються на зібраних поглядах, а не на фактах.

Багато компаній вважають, що обробка персональних даних учнів з метою створення знеособлених даних для інших цілей є прийнятною практикою без інформування сімей або шкіл, оскільки закон про захист даних не захищає анонімні дані. Але це не так, принаймні через те, що процес анонімного надання даних сам собою є обробкою персональних даних. Та і важко зробити дані анонімними і зберегти при цьому ідентифікатори шкіл або місця знаходження, навіть якщо такі дані не розглядаються як персональні, оскільки вони також можуть значно збільшити ризик повторної ідентифікації.
Наразі не існує методу інформування дітей і сімей про перенаціlювання даних доти, поки це не відбудеться. Таке порушення принципів захисту даних має припинятися шляхом рішучого правозастосування.

II.6 Роль участі батьків у зборі даних про дітей в школах

Контролери даних ставляться до прав дітей недбало і регулярно ігнорують їх у навчальному середовищі, де, як стверджують треті сторони, школи можуть «давати згоду» від імені своїх дітей, перебуваючи у ролі опікунів. Однак іноді вони можуть приймати рішення не в найкращих інтересах дитини, а в найбільш практичних або зручних інтересах школи.

Хоча досвід роботи в класі значно відрізняється в різних точках світу, поява недорогих пристроїв з підключенням до інтернету, кишенькових пристроїв, ШІ та технічних засобів з підтримкою голосових функцій, які легко принести до класної кімнати без батьківського відома, дозволу або контролю, загрожує правам дітей в безпрецедентному глобальному масштабі, в тому числі загрожує недоторканності їхнього приватного життя, а також автономії й здатності контролювати свій цифровий слід.

II.6.1 Профілактика неналежного використання в школі — неможлива батьківська задача

Чи є різниця між інформуванням законних опікунів про запровадження певного продукту до повсякденної класної роботи і разовим дослідницьким тестуванням? Якими мають бути очікувані стандарти для затвердження комітетом з етики пілотного запуску продукту в школі? У який спосіб може бути досягнута висока планка надання згоди на обробку даних особливої категорії, якщо діти не можуть дати свою згоду через вік, і в будь-якому випадку дисбаланс влади означає, що дитина і, по суті, батьки будь-якого віку можуть зіткнутися з неможливістю дати дійсно вільну та інформовану згоду на обробку даних в шкільному середовищі, без того, щоб такий вибір не нашкодив дитині?

Права дітей повинні захищатися в далекоглядний спосіб, заснований на принципах Конвенції №108 як основи для їхнього повноцінного розвитку без втручання ззовні, а також для того, щоб сприяти їхньому всебічному добробуту.

Школи не повинні перебирати на себе відповідальність батьків щодо цифрового сліду дитини або створювати такий слід, який в іншому випадку вони б не створили, і який не можна контролювати або ліквідувати після закінчення освітнього процесу. При цьому права законних опікунів обмежуються і втрачають свою силу.

II.6.2 Батьківське розуміння

Щоб полегшити батьківське розуміння, навчальні записи повинні бути доступними для законних опікунів. Наразі це неможливе завдання, оскільки, за деякими оцінками, понад тридцять зовнішніх обробників даних можуть обробляти дані дитини в будь-який момент часу.

Крім того, може постати питання про те, чи отримують діти достатню підтримку від своїх батьків щодо ризиків, пов'язаних з конфіденційністю в інтернеті, та хто підтримує самих батьків. (Чжао Дж. (Zhao J.), 2018 р.)

Чжао стверджує, що:

> «Батьки дітей у віці від 6 до 11 років часто вважають, що діти ще надто малі для того, аби мати справу з проблемами конфіденційності в інтернеті або розуміти їх, і часто використовують захисний підхід для обмеження або моніторингу того, до чого діти можуть отримати доступ онлайн (вдома), замість того, щоб обговорити з дітьми питання конфіденційності. Батьки докладають зусиль для захисту безпеки

своїх дітей в інтернеті. Проте, мало відомо, наскільки обізнані батьки з ризиками, пов'язаними з неявним збором персональних даних основними або сторонніми компаніями, що стоять за мобільними застосунками, які використовують їхні діти, і, отже, наскільки добре батьки можуть захистити своїх дітей від таких ризиків».

Знання сімей про інструменти та пов'язані з ними ризики в шкільному середовищі, є ще меншим, як і нагляд батьків. Сьогодні навчальні заклади, мабуть, недооцінюють рівень ризиків і побоювань, пов'язаних з обробкою даних в школах, і, можливо, через непоінформованість батьків вони не встигають за масштабами обробки даних. Чи буде школа тримати законних опікунів навмисно «в невіданні» або припускатиме відсутність заперечень, оскільки механізми їхнього дотримання відсутні, ще треба досліджувати.

Існує необхідність в інструментах та процесах, що дозволяють школам виконувати свої зобов'язання щодо забезпечення прозорості, будучи відкритими стосовно обробки даних до того, як така обробка станеться, і демонструвати свою підзвітність після того, як ця обробка відбудеться. З метою забезпечення виконання школами цих зобов'язань можуть знадобитися відповідне законодавство і незалежний нагляд.

II.6.3 Приклади поглядів батьків в Англії

У 2018 році компанія «defenddigitalme» замовила опитування поглядів батьків. Опитування про стан даних 2018 року було проведено в режимі онлайн. Агенція «Survation» опитала 1004 батьків щодо збору даних про дітей і використання повсякденних технологій в державній освіті Англії. Респондентами були батьки дітей у віці від 5 до 18 років, які отримують державну освіту в Англії. Їм було запропоновано детальні питання про те, які персональні дані їхньої дитини зберігаються в школі, як вони розуміють, які саме технології використовуються, а також питання про їхнє ставлення до використання персональних конфіденційних даних дітей на національному рівні третіми особами.

Кожен четвертий з батьків (24%) сказав, що не знає, чи була їхня дитина зареєстрована в системах, що використовують персональні дані. Більшість з них не знають про те, що персональні дані про кожну дитину у віці від 2 до 18 років подаються до Департаменту освіти в процесі перепису в школах, або про те, як використовуються персональні дані дитини з Національної бази даних про учнів. 69% батьків заявили, що вони не були поінформовані про те, що Національний департамент освіти може видавати дані з Національної бази даних про учнів третім особам.

З усіх відповідей випливає, що батьки, судячи з усього, вважають, що дані дітей про особливі освітні потреби заслуговують додаткового розгляду, перш ніж школа передасть цю конфіденційну інформацію до Міністерства освіти (МО) для повторного використання. Ці дані не розглядаються як дані про здоров'я або як такі, що відповідають вимогам стандартів особливої категорії, попри те, що вони містять характеристики соціальних, емоційних потреб, а також в інформацію про психічне здоров'я, фізичні вади, розлад аутистичного спектра, порушення слуху і зору. (Міністерство освіти, SEND, 2019 р.).

- 81% батьків погодилися з тим, що передачі даних про особливі навчальні потреби дитини має передувати згода батьків.
- 60% батьків погодилися з тим, що до того, як школи передадуть дані до Національної бази даних про учнів МО, необхідно отримати згоду батьків.
- 65% погодилися з тим, що Міністерство освіти повинно мати батьківську згоду, щоб передавати персональні дані дітей комерційним компаніям, які займаються аналізом даних.

- Понад три чверті (79%), якби їм була надана можливість переглянути записи про свою дитину в Національній базі даних про учнів, вважали за краще б переглядати їх, використовуючи Запит про наявність інформації щодо суб'єкта персональних даних.

Для реалізації намірів і цілей захисту, передбачених Конвенцією, батьки повинні мати право заперечувати проти вторинних непрямих цілей обробки даних та таких цілей, щодо яких батьки не очікують, що дані їхньої дитини будуть оброблені в процесі навчання.

II.6.4 Батьки очікують, що школи захищатимуть права дитини та дотримуватимуться їх.

Відповідно до Рекомендації CM/Rec (2018)7 про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі,

> «Державам та іншим зацікавленим сторонам слід впевнитися, що діти знають як реалізовувати своє право на приватне життя та захист даних з урахуванням їхнього віку та зрілості, а також, де це доречно, під керівництвом та з порадами їхніх батьків, опікунів, законних піклувальників або інших осіб, які несуть відповідальність за дитину у такий спосіб, що відповідає розвитку здібностей дитини».

Крім того,

> «Персональні дані дітей і молоді заслуговують особливого захисту та повинні оброблятися тільки на достатній правовій підставі. Діти й підлітки мають право на захист приватного життя і повинні мати можливість здійснювати свої права на захист даних за підтримки батьків або опікунів. Батьки повинні мати можливість надавати допомогу своїм дітям і активно брати участь в здійсненні цих прав». (ICDPPC, Резолюція щодо платформ електронного навчання, 2018 р.).

Однак свідоцтва недостатньої обізнаності та інформації, що передається зі школи законним опікунам, означають, що сім'ї позбавлені прав і не можуть діяти заради захисту прав своєї дитини в школі. Якщо законодавство не дозволяє законним опікунам накласти вето на використання персональних даних дитини, що вже зберігаються в школі, то не існує механізму заперечення проти обробки без самої інформованої обробки. Школи можуть дотримуватись мантри про те, що «дані збираються лише раз, а використовуються багато разів», і при цьому не інформувати законних опікунів про додаткову обробку після того, як персональні дані вже були зібрані вперше, без чіткої та вузької цілі, відмінної від цілі вступу дитини до школи. Таким чином, недостатньо захистити основоположні права і свободи дитини, якщо такий обов'язок покладається лише на батьків.

II.6.4 Права законних опікунів щодо персональних даних

Законні опікуни також можуть виявити, що їхні персональні дані передані комерційним освітнім компаніям через шкільну систему та пов'язані із записом їхньої дитини без їх відома.

Особливо маніпулятивні недоброчесні бізнес-моделі «замани і підміни» повинні бути незаконними в галузі освіти. Вони заохочують школи підписуватися на безкоштовні продукти, за які потім стягують платню зі школи за продовження передплати чи розширення послуг, або ціллю яких потім стають вчителі та законні опікуни шляхом

прямого маркетингу через електронну пошту або із використанням додаткового комерційного контенту в застосунках реклами та маркетингу.

Персональні дані законних опікунів також можуть розглядатися школами та освітніми установами як джерела даних, які можна добути. Британська освітня інспекція (Ofsted — Комітет зі стандартів у сфері освіти), у 2017 році проводила переговори з Міністерством освіти в рамках «проєкту з питань аналізу та обробки даних» з метою «вивчення можливості використання даних та інформації з соціальних мереж та інших джерел в режимі, близькому до реального часу, для прогнозування і запобігання зниженню успішності у школах». Запланований перегляд сторінок учнів і законних опікунів в соціальних мережах для моніторингу того, чи не знижуються шкільні стандарти, наразився на критику з боку вчительських спілок і груп із захисту громадянських свобод, стурбованих ненадійністю даних, серед яких можуть виявитися помилкові заяви та плітки, а також збитком, який інституційне спостереження може заподіяти громадській довірі. (i- news, 2017 р.)

II.7 Роль вчителів і працівників шкіл

В Англії дослідники з Лондонської школи економіки у 2019 році виявили, що «вчителі не знають, що відбувається з даними про дітей, та існує загальне нерозуміння того, який обсяг даних виходить за межі школи». (Стоілова (Stoilova), Лівінгстон (Livingstone) і Нандагірі (Nandagiri), 2019 р.).

Вони також виявили, що вчителі визнають «численні проблеми, які їм необхідно вирішити у зв'язку з навчальною програмою з цифрової грамотності — від формату викладання і впровадження технологій в процес навчання до більш захопливого контенту, зосередженого на можливостях і позитивних вістках».

З огляду на обсяг обробки даних, яка відбувається у звичайний день в житті дитини в школі: спілкування між школою та домівкою, реєстрація та відвідуваність, управління приміщеннями та обладнанням, навчальні платформи і застосунки, класні інструменти, управління поведінкою і безпекою, застосунки для виконання домашніх завдань, а також приховане використання персональних даних учнів для порівняльного аналізу та виміру ефективності роботи школи й вчителів, — може здатися дивним, що вчителі настільки погано оснащені державною системою для роботи з даними, а вимоги до них такі значні.

II.7.1 Вчителі довіряють системі та провайдерам, не маючи відповідної підготовки

Вчителі можуть обговорювати шкільну практику щодо відповідності Загальному регламенту про захист даних, а також просто «вірити в те, що шкільна система працює і належним чином регулюється». (Стоілова (Stoilova), Лівінгстон (Livingstone) і Нандагірі (Nandagiri), 2019 р.).

Базова підготовка вчителів і вимоги до підвищення кваліфікації можуть не містити жодних базових відомостей про захист даних або прав дітей. Зовнішні компанії можуть надавати технологію в руки вчителів, які не навчені і, як очікується, будуть просто «вчитися на практиці».

Підготовка в сфері захисту даних розглядається як доповнення, а не як невід'ємна частина підготовки вчителів у державному секторі, що означає, що при впровадженні будь-якої технології вони не в змозі оцінити її законність і провести перевірку на відповідність основним правам.

Належна обачність при впровадженні та подальшій перевірці повинна бути частиною циклу оцінки ризику протягом усього освітнього шляху дитини та обробки її даних, а не статичним процесом, здійснюваним на місці збору даних.

Коли вчителі просять дітей користуватися застосунками, жодна зі сторін не може мати у своєму розпорядженні достатньо інформації для розуміння того, чи є умови й положення справедливими, або як вони можуть обробляти персональні дані дитини протягом усього її життя.

Фахівець із захисту даних є необхідною одиницею в школі, хоча він може і не бути окремо призначеним співробітником. Відповідно до додаткових зобов'язань Конвенції (стаття 10(1)), варто роз'яснювати, що такий фахівець необхідний для установ, що обробляють дані про дітей у сфері освіти, і повинен мати достатні засоби, а також вміння для виконання своїх обов'язків.

У 2009 році Дауті (Dowty) та Корфф (Korff) встановили, що стандарти підготовки в сфері інформаційної безпеки, яка надається практичним працівникам, сильно розрізняються, і що в деяких місцевих органах влади Сполученого Королівства неточність консультацій з питань безпеки та неналежність процедур забезпечення безпеки викликає занепокоєння.

Зараз часто законні підстави для використання персональних даних дітей в галузі освіти невірно тлумачаться як частина обов'язків, передбачених законом, або як суспільне завдання. Проте, у третіх сторін немає суспільного завдання, яке вони повинні виконувати, і, наприклад, умови більшості застосунків передбачають обробку даних на основі згоди. Підготовка викладачів та персоналу є необхідною, і школи повинні перевіряти, як це робиться.

II.8 Тягар проведення перевірок

Хоча свобода вибору дітей є життєво важливою, і вони повинні бути краще поінформованими про те, як збираються їхні персональні дані та зберігається їхній цифровий слід, всі погоджуються, що від дітей не можна і не слід очікувати, що вони будуть орієнтуватися в дуже складному онлайн середовищі. (Лівінгстон (Livingstone), 2019)

Тягар проведення перевірок в школах є наразі дуже значним, щоб мати можливість зрозуміти деякі продукти, провести належну оцінку ризику, отримати інформацію, необхідну для надання суб'єктам даних, а також мати можливість зустрічатися з користувачами та відстоювати їхні права. Отже, багато чого з вказаного не відбувається, і персонал часто погоджується використовувати певний продукт без належних знань, що шкодить дітям.

II.8.1 Після закінчення обов'язкової освіти неможливо відстежити цифровий слід дитини

У зв'язку зі зміною умов контрактів з плином часу, поширенням необроблених даних, передачею даних з-за кордону, використанням компаніями edTech багатьох підрядних обробників, а також продажем бізнесу і зміною власників, навіть найпоінформованіші батьки і дитина на момент збору даних можуть наприкінці обов'язкової освіти вже не мати необхідного механізму, щоб зрозуміти обсяг і ступінь поширення свого цифрового сліду, який розпочала школа.

Оскільки діти не отримують достатньої підтримки з боку своїх законних опікунів щодо ризиків, пов'язаних з недоторканністю приватного життя в інтернеті, обов'язок щодо забезпечення повідомлення про зберігання будь-яких даних і їхню подальшу обробку,

коли дитина залишає навчальний заклад, лягає на школи та на їхні контактні треті сторони.

Підприємці також зобов'язані дотримуватися прав у своїй діяльності:

«Забезпечення прозорості роботи механізму для ширшого кола зацікавлених сторін за допомогою статистичних даних, практичних прикладів або більш докладної інформації про розгляд певних справ може мати важливе значення для демонстрації його легітимності та збереження широкої довіри». (Керівні принципи ООН з питань підприємницької діяльності в аспекті прав людини, 2011 р.).

В ході перевірки конфіденційності GPEN 2017 року було відзначено, що «посилання на політику конфіденційності та умови обслуговування часто були відсутні або їх було важко знайти після створення облікового запису». Це означає, що викладачу або учню не легко повернутися до правил та умов користування, як тільки він натисне кнопку «Я згоден».

II.9 Допомога, представництво і засоби правового захисту для суб'єктів даних

Відповідно до статей 9 і 12 (оновленої) Конвенції Ради Європи №108, кожна людина повинна мати можливість реалізувати свої права на компенсацію шкоди у зв'язку з обробкою персональних даних, що стосуються її. Для дітей судова система є недоступною, незрозумілою і лячною. (Керівні принципи здійснення правосуддя з урахуванням інтересів дітей, прийняті Комітетом міністрів Ради Європи (2010 р.)).

Тому без підтримки дитина не може мати можливість оскаржити в судовому порядку те чи інше рішення або підхід. Надання допомоги суб'єктам даних за статтею 18 не має чітких посилань на дітей. Таке питання може бути ширше розкрито в керівних принципах.

У Стратегії Ради Європи з прав дитини на 2016–2021 роки чітко вказано, що всі права дітей вважаються рівними, і те саме стосується їхніх поглядів до досягнення 18-річного віку. «Діти мають право бути почутими та брати участь в ухваленні рішень, які стосуються їхніх інтересів, як особистості і як група. Кожна людина має право на свободу вираження поглядів, гарантоване відповідно до статті 10 Європейської конвенції з прав людини. Конвенція ООН про права дитини надає дитині право вільно висловлювати свої погляди з усіх питань, які стосуються її інтересів, а також на те, щоб її думкам приділялась належна увага відповідно до віку і зрілості такої дитини».

> «Згідно з Конвенцією ООН про права дитини, дітям повинна надаватись можливість бути вислуханими в ході будь-якого судового чи адміністративного розгляду, який їх стосується, та мати доступ до компетентних, незалежних і неупереджених механізмів оскарження у випадку порушення їхніх прав. Крім того, держави-учасниці Конвенції ООН про права дитини визнають право кожної дитини, яка перебуває у конфлікті із законом, на таке ставлення, яке забезпечує дотримання почуття власної гідності дитини, беручи до уваги вік дитини та мету її реінтеграції в суспільство. В усіх діях щодо дітей, незалежно від того, здійснюються вони державними чи приватними установами соціального забезпечення, судами, адміністративними чи законодавчими органами, найкращі інтереси дитини повинні бути головним питанням». (Стратегія Ради Європи з прав дитини на 2016–2021 роки, пункти 37 і 52)

У зауваженні загального порядку ООН №16 (2013 р.) про зобов'язання держави щодо впливу підприємницького сектора на права дітей, підкреслюються проблеми, зокрема, щодо отримання дітьми засобів правового захисту для розв'язання проблем онлайн.

> «Існують особливі труднощі в отриманні засобів правового захисту від зловживань, які відбуваються в контексті глобальної діяльності бізнесу». (Пункт 67) «Державам, які ще не передбачили можливість подачі колективних скарг, як-от групові позови та судові провадження на захист громадських інтересів, слід запровадити їх як засіб розширення доступу до судів для багатьох дітей, які аналогічним чином зазнають впливу з боку підприємницької діяльності. Державам, можливо, доведеться надавати спеціальну допомогу дітям, які стикаються з перешкодами в доступі до правосуддя, наприклад, через мовні обмеження або інвалідність, або через те, що вони зовсім маленькі». (Пункт 68)

Діти не можуть легко забезпечити дотримання своїх прав, не залучаючи до цього інших. Той, хто подає до суду на державний орган або глобальну корпорацію, може отримати непідйомний рахунок на адвоката та судові витрати.

II.10 Технології, випробування і нові питання

Висновок доповіді Ровруа «Про дані та людей: Засадничі права і свободи у світі великих даних» (*Of data and men: Fundamental rights and freedoms in a world of Big Data*) застосовується рівною мірою як в освіті, так і щодо використання великомасштабної обробки даних в цілому.

> «Відповідно, ця “цифрова революція” вимагає постійної пильності та постійно оновлюваного вивчення актуальності та застосовності правових інструментів для захисту наших засадничих прав і свобод».

II.10.1 Проблема масштабованості даних в галузі освіти, як і в інших секторах

У цьому звіті не робиться спроба скласти вичерпний перелік всіх нинішніх і майбутніх проблем, які постають через масштабовану обробку даних в галузі освіти, що іноді називається «великими даними». У кращому випадку в цьому звіті можна навести кілька прикладів, які висвітлюють деякі актуальні питання щодо захисту даних і, в більш загальному плані, захисту засадничих прав і свобод дитини.

Можливо, найбільші проблеми в області захисту прав дитини, її гідності та повного і вільного розвитку без втручання, із підтримкою розквіту її людського потенціалу на шляху до дорослого життя пов’язані з обіцянками застосування машинного навчання і прогнозування з використанням великого обсягу даних, зібраних в школі, переданих через освітні установи та проаналізованих для вжиття заходів на випередження. Припущення про те, що це є можливим і бажаним, поширюється і на студентське життя.

> *«Алгоритми штучного інтелекту можуть бути використані для виявлення проблем на основі аналізу повсякденної інформації — утримання студентів стало однією з основних проблем для університетів, і нині навчальні заклади аналізують дані, щоб точно визначити, коли й чому студенти ризикують кинути навчання, в тому числі як часто студенти користуються системою управління студентським життям, відвідують бібліотеку або подають виконані завдання. Пошук причин для занепокоєння дозволяє університетам активно взаємодіяти з проблемними студентами та пропонувати підтримку і допомогу в найкоротші терміни.*
>
> *Крім підвищення показників утримання студентів, це допомагає університетам підвищити добробут студентів, виявляючи проблеми та пропонуючи допомогу на більш ранніх стадіях, замість того, щоб змушувати*

студентів звертатися по допомогу. Це також дозволяє навчальним закладам надавати на ранніх стадіях підтримку студентам, які мають проблеми з фізичним або психічним здоров'ям».

Однак головною безпосередньою проблемою, пов'язаною з новими та новітніми технологіями для дітей різного віку, є бажання як продавців, так і вчених розробити та протестувати продукцію.

II.10.2 Чи може участь у випробуваннях продуктів забезпечити безпечне виховання дітей?

Саутгейт (Southgate) та інші стверджують у своїй доповіді 2019 року «Штучний інтелект і новітні технології в школах», підготовленій на замовлення уряду Австралії:

«Штучний інтелект і новітні технології в школах необхідно ретельно "інкубувати" контрольованим шляхом в різних шкільних середовищах, зокрема в сільських районах і в школах з низьким рівнем доходів, з метою виявлення практичних, етичних і технічних проблем, а також проблем, пов'язаних з безпекою. Ця "інкубація" повинна супроводжуватися надійним, теоретично обґрунтованим дослідженням їхнього педагогічного потенціалу і впливу технологій на учнів і процес навчання».

Однак ця «інкубація» і, по суті, пілотні запуски та випробування в реальних умовах можуть прямо суперечити підходам, які керуються принципами обережності, про що свідчать висновки Шведського управління із захисту даних, зроблені в серпні 2019 року стосовно випробувань з використанням розпізнавання обличчя.

Життєво важливо визначити «практичні, етичні та технічні проблеми, а також проблеми, пов'язані з безпекою», перш ніж застосовувати ту чи іншу технологію до дітей, у яких немає іншого вибору, окрім як перебувати в класі.

Діти, від яких вимагається участь у випробуваннях, не можуть вільно давати згоду, і, як вже було сказано, концепція законної згоди в шкільному середовищі є принципово проблематичною. Ненадання згоди ніколи не повинно призводити до того, щоб основні послуги стали недоступними, проте і згода не може бути анульованою, а продукти — протестовані як частина суспільного завдання, якщо в школах існують менш інвазивні методи виконання рутинних завдань в сфері освіти.

Розробка алгоритмічних систем не повинна означати, що тестування або розгортання пов'язано з ризиками або витратами для окремих осіб, сімей або громад, і це вимагає законодавчої підтримки.

II.10.3 Чи можуть державні системи освіти бути безпечно сформовані в умовах комерційного захоплення?

Існують також значні всесвітні гравці, що формують наявні технології та забезпечують їхнє широке впровадження. Вони не завжди дотримуються законної або етичної практики. Німеччина наказала компанії Google, яка є глобальною платформою, змінити обробку даних користувачів, яка за рішенням Управління із захисту даних (DPA) порушувала закони країни як у 2015 році щодо профілювання, так і нещодавно, у 2019 році, з метою забезпечення того, щоб персональні дані не оброблялися за межами території Німеччини.

Культура і цілі освіти формуються глобальними компаніями в міру того, як такі компанії поступово беруть під контроль інфраструктуру управління даними великої частини освітнього сектора.

Google навіть розробив свою власну мову і терміни в галузі освіти, так само як і назва компанії вживається взаємозамінно з дієсловом «шукати в Інтернеті»; риторика компанії Google про інновації полягає також у створенні певних предметів, починаючи з прийняття цінностей платформи Google, які викладаються працівникам шкіл за допомогою безоплатного навчання.

> *«Презентацію для інвесторів платформи GE (Google Expeditions) також присвячено залученню пересічних людей до добровільного безоплатного розширення всесвіту Google. 70 мільйонів користувачів GFE (Google for Education) і GE також працюють на Google в обмін на обіцянку освітнього та особистого збагачення. У цьому полягає суть стратегії розширення GFE, яка перегукується з іншими стратегіями, що описані в наявній літературі, присвяченій м'якій владі Google, капіталізму платформ та стеження, а також колоніалізму даних (Срнічек (Srnicek), 2016 р.; Зубофф (Zuboff), 2019 р., Калдрі (Couldry) та Мейджас (Meijas), 2018 р.; Сандовал (Sandoval), 2014 р.; Фухс (Fuchs), 2014 р.; Хілліс (Hillis) та ін., 2013 р.). Таким чином, GE є чудовим прикладом того, як компанія Google може створювати, просувати й визначати умови участі в освітньому процесі, а також утверджувати свою роль щодо перспектив освітньої галузі.*
>
> *Хоча це є цінним внеском в освіту і технологічні дослідження, необхідно порушити ще багато питань, зокрема питання про те, що насправді поставлено на карту в цьому балансі між збагаченням і колоніалізмом? Що отримує Google зі шкіл, куди компанія рухається і як отримує прибуток (економічний або стратегічний) від цієї роботи? І найголовніше, які реальні наслідки розширення ролі Google в житті молоді, а також у громадській інфраструктурі та соціальних установах?* (Суджон, З. (Sujon, Z.), 2019 р.)

На момент написання цієї доповіді проблеми, пов'язані з його домінуванням на ринку, почали виникати в США, Швейцарії та з боку законних опікунів в Іспанії. («Ars Technica», 2019 р.) Генеральний прокурор штату Нью-Мексико подав у лютому 2020 року позов проти компанії «Google LLC», стверджуючи, що використання платформи Google Education та інших продуктів Google «немало коштує, що Google намірено приховує». (справа «Балдерас, Нью-Мексико, проти "Google LLC"» (Balderas, New Mexico, vs GoogleLLC), 2020 р.). Норвезьке управління із захисту даних також оголосило про те, що воно вивчає питання законності використання Google в школах. («Aftenposten», лютий 2020 р.) Органи влади та батьки починають чинити опір компанії, яка, на перший погляд, є бажаним безоплатним подарунком для шкільної інфраструктури за часів жорсткої економії. («Republik», 2019 р.)

II.10.4 Чи можна виміряти цінність освіти дитини не тільки на основі даних?

У міру того, як аналіз даних стає все більш потужною силою в питаннях підзвітності та оцінки роботи вчителів на основі даних про дітей, питання про те, як ми продовжуємо оцінювати те, що не можна виміряти за допомогою машин в галузі освіти (С. Сміт (Smith, S)., 2016 р.), вимагає цілеспрямованих заходів для визначення, якими суспільство бачить цінності освіти в мйбутьому.

Бездіяльність означатиме, що компанії будуть приймати рішення за нас, а їхні цінності стануть основою майбутніх суспільств і громадян, сформованих за допомогою наших систем освіти.

Комітет ООН з прав дитини в зауваженні загального порядку № 1 щодо цілей освіти (стаття 29) (2001 р.) настійно закликає міжнародні органи, що займаються питаннями освітньої політики та правозахисної освіти, прагнути до поліпшення координації, аби підвищити ефективність реалізації статті 29(1).

Законодавство про захист даних і недоторканність приватного життя може встановлювати параметри того, що є допустимим з-проміж того, що є можливим. Вкрай важливо, щоб цінності тих, хто формує наших дітей через освіту, ґрунтувалися на універсальних правах людини, пріоритетом яких є люди і розквіт їхніх особистостей .

Це включає визнання того, що створені в державному секторі дані, якщо вони використовуються для загального суспільного блага, повинні бути спрямовані на сприяння повноцінній участі в житті вільного суспільства, а не на отримання прибутку приватним сектором.

II.10.5 Штучний інтелект (ШІ) і освіта

Рекомендації повинні спиратися на наявні стандарти Ради Європи та відповідну практику Європейського суду з прав людини, а також на правозахисні аспекти методів автоматизованої обробки даних, що вже наявні або ще розробляються, зокрема алгоритми, можливі стандарти та нормативні наслідки.

> *«Наразі немає узгодженого визначення поняття "штучний інтелект". Однак для цілей цієї рекомендації ШІ використовується як збірний термін для загального позначення комплексу наук, теорій і методів, спрямованих на підвищення здатності машин робити дії, які потребують інтелекту. Система штучного інтелекту — це комп'ютерна система, яка надає рекомендації, робить передбачення або приймає рішення для певного набору цілей».* (Рада Європи, травень 2019 р.)

Починаючи з персоналізованих навчальних платформ і до автоматичного виявлення дислексії у дітей («AlgorithmWatch», 2019) ШІ зараз займає значне місце в обговореннях і фінансуванні серед наукових кіл, політиків і в промисловості.

> *«Компанії активно займаються переосмисленням можливостей, навичок і диспозицій, необхідних молоді, а також професійним викладачам-практикам, в період значних технологічних і економічних змін. В кінці 2016 року IBM і «Pearson» об'єднали свої зусилля у новому глобальному партнерстві».* (Вільямсон (Williamson), 2017 р., «Великі дані в освіті» (Big Data in Education)).

В опублікованому в травні 2019 року документі ЮНЕСКО «Пекінський консенсус щодо штучного інтелекту та освіти» містяться вказівки й рекомендації щодо того, як найкращим чином використовувати технології штучного інтелекту для досягнення ЦСР 4. Однак в ході такої інформаційно-роз'яснювальної роботи рідко постає питання про те, чи забезпечує персоналізація якісніший освітній досвід або кращі результати, як саме і чому. На сьогодні від постачальників продукції або від їхніх інкубаторів надходить обмежена кількість доказів цього.

При пошуку рекомендацій, в першу чергу, можна використовувати взагалі не слово «штучний інтелект», з його розпливчастими але обмеженими визначеннями, а слово

«автономна інтелектуальна система» або «алгоритмічне прийняття рішень», оскільки правове визначення відсутнє. Друга рекомендація полягає в тому, щоб розглядати обробку даних з використанням цих інструментів за таких самих високих очікувань, що й стосовно інших методів обробки даних для прийняття рішень.

II.10.6 Упередженість і дискримінація в даних є універсальними питаннями

З правозахисної позиції щодо ШІ в галузі освіти Консенсус дійшов висновку, що:

> «розвиток і використання ШІ в освіті не повинно поглиблювати цифровий розрив і не має демонструвати упередженості щодо будь-якої меншини або вразливих груп».

Питання про те, чи усувають «монетизовані» індивідуалізовані рішення причини нерівності та чи здатні вони краще їх усувати, лише починає оцінюватися незалежними третіми сторонами. (Девіс, Х. (Davies, H.), готується до публікації).

Нові технології, яким властиві широкі можливості для обробки даних і непрозора практика або можливості для прийняття рішень, мають значні наслідки для освіти в державному секторі та, зокрема, на робочому місці, як-от в царині набору персоналу, аналізу даних чи прогнозуванні та вжитті заходів.

Щодо застосунків, які вимагають великих обсягів даних, таких як ШІ, який збирає дані про взаємодію користувачів кожні дві секунди, то роль комітетів з етики привертає все більшу увагу в колах ШІ, хоча не існує єдиної думки щодо їхнього характеру, незалежності або функцій. Теоретичні дослідження, політичні документи й корпоративні ініціативи — всі вони пропонують різні та іноді суперечливі рішення щодо цього.

II.10.7 Права дітей можуть бути порушені на стадії розробки продукту

Конфлікту між конфіденційністю та інноваціями не повинно виникати, однак розробка деяких продуктів в нових сферах, включно з машинним навчанням, штучним інтелектом, біометрією й технологією розпізнавання обличчя, може швидко обмежувати права в широких масштабах. Захист даних і приватного життя за своїм задумом передбачає обережний підхід, який особливо важливий для обробки даних при роботі з дітьми.

Саутгейт (Southgate) та інші наголошують у своїй доповіді 2019 року «Штучний інтелект і новітні технології в школах», підготовленій на замовлення уряду Австралії, що:

> “Лакін (Luckin) і колеги (2016 р.) також вказують на потенційні можливості використання навчальних помічників ШІ для несправедливого або прихованого спостереження за роботою викладачів (з використанням даних про учнів), що було підтримано Камполо (Campolo) та іншими (2018 р.), які рекомендують “проводити більше досліджень і розробляти політику в галузі використання систем ШІ в процесі управління і моніторингу на робочому місці” (стор. 1). До числа інших питань, що викликають занепокоєння, входять питання про те, у який спосіб ШІ прагне змінити поведінку в процесі навчання шляхом вироблення рекомендацій, переконання і забезпечення зворотного зв’язку, що в кінцевому підсумку може не відповідати найкращим інтересам учня. Деякі з них вважають, що навчальні помічники ШІ, призначені для підтримки учнів на їхньому освітньому шляху протягом усього життя, “можуть призвести до постійної фіксації невдач учня на шкоду майбутньому прогресу” (Лакін (Luckin) та інші, стор. 39)».

«Спостереження Бойда (Boyd) і Крофорда (Crawford) (2012 р.) щодо великих даних особливо актуальні в контексті ШІ: “Багато (людей) не знають про безліч агентів і алгоритмів, які наразі збирають і зберігають їхні дані для використання в майбутньому”. (стор. 673). Це вказує на третю область обізнаності — учні, батьки та вчителі повинні бути повністю обізнані щодо збору даних ШІ, процедури їхнього зберігання та обміну ними за наявності інформованої згоди батьків і дозволу з боку учнів. Така думка підтверджується рекомендаціями IEEE (2017 р.)».

17 жовтня 2017 року Робоча група з питань реалізації статті 29 (надалі — «Робоча група»), опублікувала керівні принципи щодо автоматизованого індивідуального прийняття рішень і профілювання для цілей Регламенту 2016/679 (GDPR). Робоча група не вважає пункт 71 преамбули абсолютною забороною на виключно автоматизоване прийняття рішень, що стосуються дітей, але зазначає, що він повинен застосовуватися лише за певних вузьких обставин (скажімо, для захисту життєво важливих інтересів дитини).

Однак регулювання цих інструментів, можливо, призведе до того, що ми зможемо погодитися на використання технології у такий спосіб, що необхідність в ній буде поставлена під сумнів, причому більш рішуче.

«Коротше кажучи, захопленість вузькими обчислювальними головоломками відвертає нас від набагато більш важливої проблеми колосальної асиметрії між суспільними витратами та особистою вигодою при розгортанні автоматизованих систем. Це також позбавляє нас можливості ставити питання: чи повинні ми взагалі будувати ці системи?»

«Штучний інтелект приводить до міфічної, об’єктивної всемогутності, але він підкріплений реальними силами грошей, влади та даних. Користуючись цими силами, ми створюємо потужні історії, які призводять до повсюдної залежності від регресивних, заснованих на спостереженні систем класифікації, які залучають всіх нас до безпрецедентного соціального експерименту, з якого важко вибратися. Зараз, більш ніж коли-небудь, ми потребуємо надійної, сміливої, творчої відповіді». (Паулс (Powles), 2018 р.)

Обізнаність і освіта є життєво важливими, але не є панацею. Деякі технології та обробка даних обмежуватимуть права навіть в тих випадках, коли обробка даних є прозорою, оскільки всі ризики, в тому числі зміщені в часі, можуть і не бути такими. Держави повинні визнати необхідність надавати дітям освіту щодо їхніх власних даних і того, як вони використовуються, аби дати їм можливість адекватно розуміти вплив їхньої цифрової історії на своє майбутнє, в освіті та на робочому місці, а також дати їм можливість оскаржувати автоматизовані рішення в тих випадках, коли вони здаються несправедливими згідно зі статтею 9(1)(a) Конвенції, можливість розвиватися повною мірою, щоб реалізувати свій потенціал.

II.10.8 Біометричні дані

Використання біометричних даних є більш втручальним шляхом доступу до шкільних служб, ніж використання PIN-коду або безконтактної карти. У школах використовується безліч різних типів біометричних технологій. Найчастіше такою біометричною технологією є відбиток пальця, який використовується в британських школах з 1999 року. (Кінг П. (King, P.), 2019 р.)

Ці технології вже існують певний час. Школа Марі-Жозе в Льєжі (Бельгія) була обладнана такою технологією попри серйозну критику навіть у 2007 році.

Біометричні вимірювання вже використовуються у всьому світі в галузі освіти для управління системами безготівкових розрахунків, користування шафками для одягу та обладнанням для друку, зокрема, для автентифікації особи учнів, забезпечення академічної доброчесності та безпеки.

За деякими оцінками, понад 2 мільйони дітей були змушені надати на обробку відбитки своїх пальців в британських школах і комерційних їдальнях до 2012 року, коли в Англії й Уельсі був введений в дію Закон про захист свобод 2012 року, а саме розділ 2 «Захист біометричної інформації дітей в школах тощо», з метою отримання згоди, необхідної при обробці в школах біометричних даних дітей. Школи повинні отримати письмову згоду батьків, якщо вони хочуть зберігати/обробляти біометричні дані дитини з 1 вересня 2013 року. Однак у 2019 році дослідження, проведене на замовлення «defenddigitalme», довело, що з 1000 батьків, чиї діти використовують біометричні дані в школах, у 38% не запитували дозволу. Таким чином, залишається відкритим питання про те, чи слід взагалі використовувати в школах для порівняно тривіальних процесів дозвільне законодавство щодо вагомих даних особливої категорії, які можуть мати життєво важливе значення для верифікації щодо значних операцій в дорослому житті.

II.10.9 Чи варто цінувати або нормалізувати біометричні дані?

Дослідження за участю дітей, проведені Сандрою Літон Грей (Sandra Leaton Gray) і Енді Фіппен (Andy Phippen) та задокументовані в їхній книзі «Invisibly Blighted» (Невидимо загублені, видавництво «UCL IOE Press», 2017 р.), виявили докази такої нормалізації біометричного нагляду, а також того, що школи вільно збирають біометричні дані, не піклуючись при цьому про право дітей на недоторканність приватного життя:

> «Хоча з технічної точки зору цінність біометричних даних для адміністраторів є очевидною, більш важливо те, що до уваги не береться цінність цієї порівняно важливої біометричної інформації для окремої людини. Дійсно, здається, що її недооцінюють, асоціюючи її з чимось банальним і повсякденним, як шкільна столова або бібліотека. Це особливо важливо з урахуванням віку відповідних осіб і того факту, що їхня соціальна ідентичність все ще знаходиться під сильним впливом закладу, в якому вони перебувають, а саме школи».

Однак біометричні технології, як-от сканери відбитків пальців і райдужної оболонки ока, все ширше застосовуються в школах і університетах, зокрема для автентифікації особи учнів, забезпечення академічної доброчесності та безпеки. (Пол (Paul), 2017 р.)

Сканування райдужної оболонки та моніторинг рухів очей часто використовуються в поєднанні з навчальними платформами та автоматизованими рішеннями для онлайн нагляду за студентами. З їхньою допомогою буде зроблена спроба автентифікації та повторної автентифікації особистості учнів в інтернеті з використанням розпізнавання обличчя за допомогою вебкамер і частого збору даних під час іспиту.

II.10.10 Виявлення та розпізнавання обличчя

Технології виявлення і розпізнавання обличчя вже давно застосовуються в системі освіти Китаю (Грін (Greene), 2018 р.) і починають застосовуватися в ширших колах шкільних установ різними способами.

До цього часу ці технології в основному розглядалися як звичайний додаток до шкільних систем з уже розвиненою культурою моніторингу та спостереження. У зв'язку з цим

виникає ряд соціальних проблем і занепокоєнь, які заслуговують особливої уваги. До них належить ймовірність того, що технологія розпізнавання обличчя змінить характер шкіл та шкільного навчання з точки зору розбіжностей в суспільстві, авторитарних проблем і обмеження прав. (Андреєвич (Andrejevic) та Селвін (Selwyn), 2019 р.)

Дедалі більша громадська стурбованість починає відбиватися в регулятивних заходах. Шведське управління із захисту даних (SDPA) у своїй постанові щодо комуни Шеллефтео, ухваленій в серпні 2019 року, зазначило, що введення системи розпізнавання обличчя для цілей фіксації відвідуваності є незаконним і наказало шкільним органами влади виплатити стримувальний грошовий штраф в розмірі 200 000 шведських крон (16 800 фунтів стерлінгів, 20 700 дол. США) за порушення закону про недоторканість приватного життя і захист даних. Згода на збір конфіденційних даних не була надана вільно, адже не проводилися попередні консультації з наглядовим органом, а оцінка впливу ризиків, пов'язаних із захистом даних, була неналежною.

Важливо, що це рішення було направлене на захист прав дітей і не допускало неналежного використання штучної «згоди». Інфраструктура для повсюдного впровадження систем виявлення і розпізнавання обличчя в школах і загалом в суспільстві глибоко турбує групи, що захищають громадянські свободи, а також деяких осіб в академічній спільноті, та попри обізнаність щодо її впровадження в школах, така інфраструктура все ще має низький рівень підтримки серед законних опікунів.

У лютому 2020 року французькі суди підтримали наглядове рішення CNIL про те, що розпізнавання обличчя в школах є незаконним.

> У школах, як правило, вже є база даних зображень кожної зарахованої дитини, і багато з них використовують камери відеоспостереження для нагляду за об'єктами, часто в рамках заходів безпеки. Це дозволяє легко впроваджувати системи розпізнавання обличчя. Як зазначає Селвін в проєкті «Data Smart Schools», в якому беруть участь дослідники з Університету Монаша й Університету Дікіна,
>
> *«Ще одним фактором, який пришвидшує впровадження систем розпізнавання обличчя в школах, є розповсюдженість відеомоніторингу та інфраструктури замкнутого відеоспостереження....систем камер відеоспостереження, розміщених всюди — від ігрових майданчиків до туалетних кімнат для учнів. Шкільний ентузіазм щодо технологій спостереження також призвів до того, що в школах як експеримент стали застосовувати натільні камери на вчителях, брати відбитки пальців і маркувати учнів за допомогою радіоміток». (Селвін (Selwyn), проєкт «Data Smart Schools», 2019 р.).*
> *«Використання радіоміток вже стало звичайною справою в таких країнах, як Бразилія, де на загальному соціально-культурному тлі вітаються додаткові спостереження за дітьми заради їхнього захисту від потенційних загроз». (Тейлор (Taylor), 2017 р.)*

Лише саме відеоспостереження несе з собою ризики для прав дітей на недоторканність приватного життя і захист даних. Значна кількість доказів щодо власних поглядів дітей на системи відеоспостереження свідчить, що ці системи втручаються у приватне життя в туалетних кімнатах, породжують недовіру, а робота у сфері технологічного спостереження призводить до наслідків і впливу, що не були очікувані. Використання системи відеоспостереження в школах продовжує розгортатись швидкими темпами, як ніколи раніше, коли йдеться про її використання не з метою боротьби зі злочинністю, а

інакодумці та особи, які їх критикують, рідко мають можливість висловити свою точку зору. (Тейлор (Taylor), Руні (Rooney), 2017 р.).

Існує припущення, що шкільні системи відеоспостереження призначені лише для профілактики злочинів, але насправді документально підтверджені випадки їхнього використання в Сполученому Королівстві охоплюють спостереження за іспитами, нагляд за роботою вчителів, а також здійснення стримувального впливу на поведінку учнів.

З аналізу світових новин про впровадження технологій стає зрозумлим, що між країнами та всередині країн існують очевидні відмінності в культурних нормах і очікуваннях щодо недоторканності приватного життя дітей і батьків, а також що права дитини не визнаються рівною мірою.

У липні 2019 року повідомлялося, що органи влади Делі планують встановити камери відеоспостереження в усіх державних школах до листопада. Проте, дані не залишаться в межах школи, а будуть зберігатися в хмарі з метою дозволити законним опікунам переглядати відеоканали систем відеоспостереження в реальному часі з тим, щоб стежити за поведінкою своєї дитини в школі, «протягом обмеженого проміжку часу, за допомогою мобільного застосунку “DSG live”». (Вацаля (Vatsalya), «Youth Ki Awaaz», 2019 р.).

Такі системи часто впроваджуються в школах з обмеженими технічними можливостями. Помилки можуть приводити до порушення роботи систем, як, наприклад, було виявлено в лютому 2018 року, коли з’ясувалося, що зображення з камер відеоспостереження британських шкіл транслюються в прямому ефірі на американському вебсайті через канали даних з незахищених камер, які, як повідомляється, «зображують сотні учнів протягом усього їхнього дня». В цьому випадку камери відеоспостереження не отримували зображення з приватних кабінок у туалетах. Але це може виявитися звичайною справою.

Натільні відеокамери спостереження і камери, що вдягаються на голову, також стають все більш поширеними, якщо школи вважають за краще використовувати їх для спостереження за поведінкою.

Активацією вебкамер також можна управляти дистанційно. У 2010 році у справі «Роббінс проти шкільного округу Ловер-Меріон» (Robbins v. Lower Merion School District) з’ясувалося, що школи можуть таємно фотографувати дітей за допомогою вебкамер, поки вони знаходяться на самоті вдома, використовуючи програмне забезпечення, встановлене на ноутбуці дитини. Такі вкрай втручальні методи відтоді набули широкого поширення, і часто вони передбачають політику використання власних пристроїв, при цьому практично без проведення обговорень і здійснення контролю, в рамках програм із боротьби з насильницьким екстремізмом в Австралії, США і Великобританії.

II.11 Забезпечення захисту і протидія насильницькому екстремізму

У 2009 році Робоча група з питань реалізації статті 29 висловила думку про те, що «*в*

жодному разі не можна допускати, щоб з міркувань безпеки діти стикалися з надмірним наглядом, який обмежував би їхню самостійність. У цьому контексті необхідно знайти баланс між захистом особистого і приватного життя дітей та їхньою безпекою». (Висновок 2/2009 про захист персональних даних дітей)

Але сьогодні, для порівняння, Джефф Паттерсон (Jeff Patterson), генеральний директор компанії «Gaggle», що спеціалізується на програмному забезпеченні для захисту шкіл, визнає, що деякі програми для захисту, які використовуються в школах, є надто втручальними. *«Конфіденційність вийшла з-під контролю за останні п'ять років. На благо суспільства, для захисту дітей».* («Education Week», травень 2019 р.)

Через відсутність практичного застосування в минулому десятилітті недоторканність приватного життя дітей була знецінена постачальниками послуг в галузі освіти, і тепер вона розглядається не як право, а як товар, ціна, яку необхідно заплатити компаніям, які стверджують, що натомість пропонують безпеку.

У документі, підготовленому Карлі Ніст (Carly Nyst), «Принципи забезпечення конфіденційності та свободи вираження думок дітей в Інтернеті» (Дитячий фонд Організації Об'єднаних Націй (ЮНІСЕФ), 2018 р.) та галузевому посібнику до нього наводяться деякі ризики, пов'язані з програмними інструментами, що використовуються для забезпечення онлайн безпеки в школах.

> *«недоторканність приватного життя дітей в інтернеті зазнає серйозного ризику з боку тих, хто намагається їх експлуатувати та глумитися над ними, використовуючи інтернет як засіб для встановлення контакту з дітьми та улещування їх з метою наруги або поширення матеріалів щодо сексуального насильства над дітьми. Втім, недоторканність приватного життя дітей також знаходиться під загрозою через ті самі заходи, які були прийняті для їхнього захисту від цих загроз. Закони, спрямовані на запобігання та розкриття злочинів проти дітей онлайн, часто вимагають моніторингу та спостереження в інтернеті, зобов'язують посередників створювати та зберігати особисту інформацію, а також надають державним органам доступ до даних, що знаходяться в приватному володінні. Між тим, в домашніх умовах популярні механізми батьківського контролю з моніторингу та обмеження доступу до інтернету обіцяють розкрити кожну деталь діяльності дітей в інтернеті».*

Оцінка ключових постачальників такого програмного забезпечення у Великій Британії й США, проведена «defenddigitalme» у 2018–2019 роках, показала, що персональні дані обробляються за межами домашньої території, а законним опікунам або дітям часто взагалі не надавалася інформація про те, як працюють системи, або які профілі ці системи генерують.

Існують суперечливі історії про можливість працівників редагувати записи та видаляти помилки. Пошукові запити дітей, в яких фігурували скелі та чорні носороги, позначалися прапорцями як потенційний ризик самогубства і членство в банді, відповідно. Таке сортування є просто неправильним, але працівники можуть не мати можливості або бажання видаляти такі прапорці, а натомість «*коли спрацьовує ключове слово, яке школа вважає помилковим збігом, може додаватися примітка, що дозволяє рецензенту надати пояснення*». Отже, існує вірогідність запису неточної інформації щодо дитини, а дитина, зі свого боку, не може побачити цей запис або виправити його.

Дослідження також довело, що 50% шкіл застосовують політику використання власних пристроїв, яка являє собою непрозорий рівень спостереження за особистим майном, що активується при підключенні до шкільної мережі, а іноді постійно, незалежно від мережевого підключення.

Вплив такої політики на поведінку дітей при використанні інтернету є недостатньо дослідженим, проте якісні дані свідчать про її стримувальний ефект на пошукові запити стосовно питань сексуальності, здоров'я і підліткового розвитку.

II.11.1 Це може підвищити, а не знизити ризики для дітей

Що стосується фільтрації, то в доповіді Спеціального доповідача ООН з питань прав дітей і свободи вираження поглядів за 2014 рік[4] йдеться про таке:

> «Використання розпливчастих і широких визначень поняття шкідливої інформації при встановленні, наприклад, захисних інтернет-фільтрів може позбавити дітей можливості доступу до важливої інформації, яка могла б допомогти їм зробити усвідомлений вибір. Це стосується, зокрема, доступу до правдивої та об'єктивної інформації, що відповідає їхньому віку, з таких питань, як важливість охорони сексуального здоров'я і небезпека вживання наркотиків. Тому заборона на таку інформацію може лише підвищити, а не знизити їхню вразливість до ризиків».

Оскільки з 2001 року посилюється занепокоєння держав з приводу того, як протистояти насильницькому екстремізму, те, що вважається істотним в цьому програмному забезпеченні, перейшло від явного наміру до дій, класифікованих як тероризм, до більш розпливчастих і широких визначень екстремізму і радикалізації. Те, що системи можуть позначити як підозрілу дію або «ризик», наразі замість деякої оцінки наміру і можливості вчинення дій передбачає перехоплення і втручання щодо потенційно незначних імовірних припущень про схильність до таких ідей.

Результати збору цих даних включають створення профілів дітей, які отримали позначку «тероризм і екстремізм», «заподіяння собі шкоди» і «проблеми психічного здоров'я».

Проведений професором Енді Фіппеном (Andy Phippen) аналіз даних, отриманих з 4507 із 6950 шкіл в Англії, які проводили заходи самоконтролю з питань електронної безпеки, доводить, що працівники шкіл не здатні впоратися з наслідками застосування цих технологій або подолати їх.

II.11.2 Пов'язування даних під егідою захисту дітей створює систему кругового нагляду

Ще один крок від застосування систем відеоспостереження в шкільних приміщеннях і вебмоніторингу до спостереження за особистою діяльністю дітей онлайн полягає в тому, щоб об'єднати все це в систему кругового нагляду, де залучені органи влади, правоохоронні органи і приватні комунікації дитини.

Технології розпізнавання обличчя розробляються для освітніх установ з метою розв'язання аналогічних проблем («Guardian», 2019 р.), при цьому для виявлення випадків насильства в школі пропонуються технології «виявлення емоцій».

У червні 2018 року в рамках заходів з запобігання перестрілок в школах законодавці штату Флорида (США) санкціонували створення централізованої бази даних, яка буде об'єднувати індивідуальні дані про учнів , що надходять від правоохоронних органів і соціальних служб штату, з інформацією, що береться з особистих облікових записів учнів в соціальних мережах. (Герольд (Herold), «Education Week»)

4 Доповідь Спеціального доповідача щодо заохочення і захисту права на свободу думок і їх вільне вираження https://documents-dds- ny.un.org/doc/UNDOC/GEN/N14/512/72/PDF/N1451272.pdf

«випадок Флориди дає нам уявлення про потенційно величезні масштаби перепрофілювання, рециркуляції та рекомбінації шкільних даних. Він також вказує на необхідність проявляти обережність, перш ніж генерувати будь-який єдиний елемент даних про учня або вчителя, які можуть бути ідентифіковані, і, отже, може бути пов'язаний з іншими особистими записами».

«Багато політиків і батьків з Флориди з цілком зрозумілих причин розглядають плани штату як обґрунтоване використання даних учнів в ім'я "безпеки в школі". Йдеться про емоційну область, в якій мало ефективних заходів реагування в країні, яка, схоже, не бажає впроваджувати ефективний контроль над зброєю. В таких умовах збільшення цифрового спостереження пропонує переконливу альтернативу для політиків і шкільної адміністрації, які хочуть, щоб їх вважали тими, хто "щось робить"».

Дослідження, проведені з батьками і підлітками, показали, що наявні інструменти часто працюють всупереч цінностям батьків і дітей, пов'язаних з недоторканністю приватного життя, і вони вважали за краще б, щоб інструменти сприяли посередництву батьків у використанні технологій дітьми, а не забезпечували можливості спостереження. (Чжао (Zhao), 2019 р.)

II.12 Дослідження перспектив: когнітивна наука, емоційне і поведінкове стимулювання

В освітньому середовищі все частіше використовуються онлайнові технології, спрямовані на ідентифікацію учнів і управління ними за допомогою емоційної складової. Ці форми моніторингу можна розуміти як методику встановлення контакту з учнями через призму позитивної психології. (Неморін (Nemorin), 2018 р.)

У 2017 році журнал «Wired» повідомив, що «Nudge Unit» або Підрозділ з аналізу поведінки (Behavioural Insights Unit) уряду Великобританії експериментував з використанням алгоритмів машинного навчання, аби оцінити, наскільки добре працюють школи, і такі експерименти були непрозорі за своїм задумом:

«Дані про етнічну і релігійну належність учнів були навмисно виключені з набору даних в спробі запобігти алгоритмічній упередженості. Попри те, що деякі чинники впливатимуть на рішення алгоритму більшою мірою, ніж інші, Сандерс (Sanders) відмовився сказати, які саме це чинники. За його словами, причиною для цього почасти є те, що він не хоче, аби школи знали, як алгоритм приймає свої рішення, а частково — те, що важко точно визначити, як працюють ці алгоритми. «Такий процес трохи схожий на чорний ящик. Ось у чому його суть», — говорить він.

Регулювання однієї конкретної технології часто виявляється неефективним, оскільки невелика зміна в конструктивному рішенні може вивести її за рамки передбачених засобів захисту. Однак протягом найближчого десятиліття збір даних про учнів може здійснюватися за допомогою все сучасніших технологій, які стають все більш інвазивними з фізичної та психометричної точки зору, як-от технології, здатні виявляти індивідуальні психологічні характеристики, фізичні риси, нейронну активність мозку і геномну інформацію, що отримується з ДНК. Якщо держави вирішать використовувати їх в широких масштабах, скажімо, для прихованої оцінки своїх установ або окремих осіб, або якщо вони не розуміють точно, як працює ця технологія, люди потребуватимуть значного захисту від прихованої шкоди.

І найбільше - діти, які досі розвиваються фізично і розумово в процесі формування.

II.12.1 Які засоби захисту мають наші діти в школі від впливу на мозок і формування поведінки, та від технологій занурення?

Дослідники в Австралії нещодавно дійшли такого висновку:

> *«Існують етичні питання і питання безпеки, пов'язані з віртуальною реальністю (VR) з повним зануренням. Деякі з них передбачають імовірність того, що маленькі діти матимуть несправжні спогади та кіберхворобу (яка схожа на нудоту при пересуванні транспортом). Існують етичні та правові проблеми, пов'язані з недоторканністю приватного життя, інтелектуальною власністю та авторським правом, особливо щодо створення учнями та викладачами контенту VR і обміну їм».*

Щодо доповненої реальності (AR) вони виявили те ж саме,

> *«Існують етичні та правові проблеми, пов'язані з недоторканністю приватного життя, інтелектуальною власністю та авторським правом, особливо щодо створення учнями та викладачами контенту AR і обміну їм».*

Бен Вільямсон (Ben Williamson) з Единбурзького університету зробив важливий внесок у розв'язання деяких актуальних питань, пов'язаних з технологіями, що використовуються в освіті, і з тим, як діти можуть здійснювати своє право вибору.

> *«У галузі психології "цифрова психометрія" і "цифрове фенотипування" з'явилися як способи побудови докладних психологічних профілів людей на підставі їхньої діяльності в інтернеті, хоча вони були затьмарені асоціюванням з мікроцільовою політичною рекламою. (Матс С. (Mats, S.), «Wired», 2017 р.)*
>
> *Втім, аспекти цифрової психометрії починають з'являтися в освіті. Наприклад, в рамках дослідження ОЕСР щодо соціальних та емоційних навичок використовуватиметься інструмент онлайн-дослідження для оцінки молоді відповідно до моделі особистості «Велика п'ятірка» або OCEAN. (ОЕСР, 2018 р.) OCEAN — це та сама модель особистості, яка передбачає п'ять факторів та використовується цифровими психометриками Кембридзького університету в тесті «myPersonality», проведеному через Facebook. Інші організації, що беруть участь в цьому русі для оцінки соціального та емоційного навчання і навичок, також вивчають інноваційні технології для проведення цифрової психометрії в галузі освіти. (МакКоун (McKown), 2017 р.)*
>
> *Біометричні технології, як-от мобільні датчики, що розміщуються на шкірі, та розпізнавання обличчя, швидко стають цікавими як освітні застосунки. (Хенд (Hand), 2019 р.) Портативні біометричні пристрої, мабуть, найбільш наочно проявляються в фізичному вихованні, де використовується низка приладів для збору фізіологічних даних студентів. (Плюм (Pluim), 2016 р.)*
>
> *"Нейротехнології", як-от інтерфейси мозок-комп'ютер і нейростимулятори, вже розробляються і випробуються для збору даних про нейронну активність учнів під час освітньої діяльності. (Вільямсон Б. (Williamson, B.), 2019 р.) Наприклад, «BrainCo» розробила наголів'я, яке повідомляє в реальному часі дані мозкових хвиль на приладову панель вчителя, щоб показати рівні уваги та залученості, а також надати інформацію програмі тренування мозку, заснованій на зворотному нейро-зв'язку, для поліпшення концентрації учнів. (Цзин М. (Jing, M.)., 2019 р.)*

Аналогічним чином, дослідники з Кембриджського університету розробили портативні «когнітивні біометричні» пристрої, які відстежують «діафрагматичні нейро-дихальні сигнали» як провідники стану концентрації та збудження. Компанія «FOCI» використовує машинне навчання для аналізу і візуалізації результатів, а також «тренер штучного інтелекту, що підвищує концентрацію уваги» (AI Mind Coach), заснований на когнітивній підготовці, позитивному підкріпленні та методах отримання зворотного нейрозв'язку, щоб забезпечити надання «порад в реальному часі для оптимізації концентрації уваги». Інші розробки в сфері нейростимуляції передбачають більш активне втручання в стан мозку учнів. (FOCIAI, 2019 р.)

Методи нейростимуляції, як-от транскраніальна електрична стимуляція (TEC), досліджуються для з'ясовування їхнього потенціалу як когнітивних підсилювачів молоді.

За даними огляду досліджень нейростимуляції стосовно освіти, використання методів TEC пов'язується з поліпшеннями в низці когнітивних областей, зокрема, щодо пам'яті, уваги, мови, математики та прийняття рішень, деякі з яких були визнані довгостроковими. (Шуйєр Дж. (Schuijer, J.), 2017 р.).

Освітні нейродослідники все більше цікавляться потенціалом нейростимуляції, (Університетський коледж Лондона, Центр освітньої нейрології, 2019 р.), яка також стимулює галузь у питаннях технологій поліпшення когнітивних функцій, що продаються безпосередньо споживачам.

Біоінформатика є обчислювальним дослідженням людської ДНК. Останнім часом біоінформатичні дослідження почали з'являтися в царині освіти з використанням методу, що зветься «полігенна оцінка», спрямованого на прогнозування шкільної успішності, досягнень та інтелекту учнів, виходячи з їхніх генетичних даних. (Вільямсон Б. (Williamson, B.), 2018 р.). Ці дослідження в галузі біоінформатики, засновані на «великих даних», відкривають можливість все ширшого використання генетичних даних для «персоналізації» освіти відповідно до спадкових генетичних схильностей і поведінкових характеристик учнів. Інші компанії можуть вбачати ринковий потенціал освітньої геноміки, скажімо, стартап-виробники дешевих наборів ДНК для генетичного тестування IQ в школах, «інтелектуальні застосунки» або інші генетичні продукти освітніх технологій». (Циммер (Zimmer), 2018 р.)

II.12.2 Як має виглядати обличчя освіти?

Той факт, що Міністерство освіти та парламентський комітет Сполученого Королівства розглядали роль генетики в низькій успішності хлопчиків походженням з робітничого класу, повинен дати привід для роздумів. («Низька успішність у галузі освіти» (Underachievement in Education) (2014 р.), Комітет Палати громад з питань освіти)

Чи повинна взагалі полігенна оцінка грати роль в освіті? Якщо генетичне прогнозування буде застосовуватись для прогнозу майбутніх можливостей дитини в галузі освіти, то можуть з'явитися нові підходи до штучного відбору майбутніх поколінь (Конлі (Conley), Флетчер (Fletcher), 2017 р.) або до цілеспрямованого втручання, передбачаючи тим самим «євгеніку 2.0» для відбору «більш розумних» дітей (Регаладо (Regalado), 2017 р.) чи іншого ставлення до дітей, не на підставі індивідуального уявлення і потреб, очевидних для викладацького складу, а на основі їхніх даних.

«Компанії можуть вбачати ринковий потенціал освітньої геноміки, скажімо, стартап-виробники дешевих наборів ДНК для тестування IQ в школах, "інтелектуальні застосунки" або інші генетичні продукти освітніх технологій.

«Споживчі компанії, як-от "23andMe", досліджували розшифровування геному людини для запуску послуг генетичного тестування як комерційних продуктів, наводячи приклад рухів в біомедичній області, щоб віддати персональні дані під корпоративний контроль (Стівенс (Stevens), 2016 р.). Того самого тижня було опубліковано дослідження SSGAC (Консорціум генетичних асоціацій соціальних наук), а "23andMe" також домовилася про угоду на 300 мільйонів доларів з великою фармацевтичною компанією "GlaxoSmithKline" щодо застосування машинного навчання і штучного інтелекту для аналізу даних своїх 5 мільйонів клієнтів для здійснення медичних відкриттів і фармацевтичних інновацій, позиціонуючи себе як частину інфраструктури та біоекономіки генної фармацевтики, а також освіти». (Циммер (Zimmer), 2018 р.)

Критики стверджували, що речі, які ми асоціюємо з інтелектом, занадто складні та неоднозначні, щоб так спрощено їх зображати. Тим часом євгеністи використовували новітню концепцію інтелекту у своїй кампанії з перебудови суспільства. (Циммер (Zimmer), 2018 р.)

Пропонується, щоб засоби регулювання забезпечували дітям можливість досягти повноліття в якомога більш незмінному стані, без втручання в їхнє тіло за допомогою зміненої реальності чи поведінкових підштовхувань, заснованих на нейротехнології або непрозорому використанні даних, щоб вони могли зберегти свою автономію, входячи до світу, який все активніше створює невидимі стимули для прихованого впливу на поведінку й емоційні стани, щоб вони могли приймати свої власні рішення.

II.13 Інструменти забезпечення конфіденційності в освітніх установах

II.13.1 Оцінка ризику конфіденційності

З урахуванням досягнень щодо обсягу і швидкості збору і передачі даних, а також у зв'язку з переходом на наступний рівень технологій, який передбачає доступ до дітей в класах при проведенні випробувань, виникає гостра потреба в регулюванні з метою забезпечення практичної та суттєвої підтримки прав.

Оцінка ризику при обробці даних охоплює не лише одноразовий ризик на початку збору даних, а поширюється на весь життєвий цикл обробки даних. Дійсно, деякі з найбільш значних ризиків можуть бути перенесені на майбутнє доросле населення. Саме це варто відобразити в оцінці, що проводиться, а також в інформації, що надається дітям та сім'ям за її результатами, на початку, під час і в кінці обробки їхніх персональних даних. Таким чином підвищується рівень інформованості про обробку і ступінь обізнаності контролерів щодо їхньої відповідальності і ризики.

Дехто вважає, що оцінка впливу на захист даних стосовно дітей повинна бути адаптована до них. (Данський інститут з прав людини, 2016 р.), а також що необхідно належним чином пояснити пасивний збір даних і відповідний ризик. Невидима інформація про дитину, що перебуває в школі (радіомітки, маячки, віртуальні помічники в класі та пристрої, підключені до інтернету), може створити великий цифровий слід, який ані сім'я, ані дитина чи навіть вчитель не могли створити власноруч.

Ймовірно, оцінка ризику повинна бути ґрунтовною, а технічні документи з коротким поясненням функціональності й ризиків можуть бути викладені доступною мовою. Оцінки впливу на дані повинні регулярно інтегруватися в процеси закупівель.

Належна оцінка впливу на захист даних, конфіденційність та етичність повинна стати невід'ємною частиною процесу впровадження будь-якої технології та вимагати відповідного рівня знань і підготовки. Спільно використовувані послуги, ймовірно, забезпечать більш високий рівень надійної компетентності й можуть посилити довіру шкіл до впровадження нових технологій, а також знизити вимоги до робочого навантаження на місцевому рівні, які повинні стосуватися належної обачності на необхідному рівні. Це особливо корисно, коли застосовується модель регіональних контрактів з визнаними мінімальними стандартами в рамках передбачених законом правил належної практики.

У процесі законотворення і закупівель на всіх рівнях державного врядування необхідно дотримуватися зауваження загального характеру ООН №16 (2013 р.) про зобов'язання держави щодо впливу підприємницького сектора на права дітей.

Оцінки впливу на дані повинні публікуватися в державному секторі, особливо у галузі освіти та у випадках, коли здійснюється обробка даних про дітей, що дає громадянському суспільству і сім'ям можливість ретельно вивчити діяльність третіх сторін з обробки даних.

II.13.2 Мінімізація даних

Принципу мінімізації даних при захисті даних необхідно дотримуватися на етапі їх збору, коли у дітей ще є можливість звести до мінімуму свій цифровий слід, що створюється в процесі отримання освіти. Обробка персональних даних повинна бути належною, актуальною і не надмірною з точки зору цілей, для яких вони обробляються, однак в освіті відбувається поєднання цілей численними користувачами даних всередині освітніх систем і поза ними. Мінімальний допустимий обсяг даних повинен збиратися у вузьких цілях.

Все частіше персональні дані, що обробляються в контексті освіти, зберігаються не тільки в адміністратора школи, а й спрямовуються до зовнішніх сховищ, оскільки «навчальні заклади покладаються на зовнішніх провайдерів, що працюють на основі "хмарних" технологій, для зберігання та обробки даних про учнів». (Робочий документ Міжнародної робочої групи з питань захисту даних в галузі телекомунікації щодо платформ електронного навчання (квітень 2017 року)).

Імпорт та експорт даних здійснюється швидко та у великих масштабах. Різні компанії виступають як інтегратори даних, пропонуючи послуги посередництва для контрольованої передачі даних. Однак у міру зниження витрат на зберігання даних збільшується обсяг зібраних даних і з'являється можливість збільшення обсягу профілювання динамічних даних тривалого спостереження і зв'язування даних.

Як було запропоновано Мантелеро (Mantelero) в «Керівництві щодо великих даних» (Big Data Guidelines, 2017 р.), визнається, що мінімізація даних створює проблеми для навчання продуктів ШІ. Проте, як видається, сектор технологій часто задовольняється тим, що як плату за розв'язання проблеми ШІ він приймає умови приватного життя дітей, замість того, щоб шукати рішення, які більшою мірою зберігають конфіденційність. Заклик до надання більшого обсягу даних для систем ШІ часто буває гучним, але регулятори не повинні плутати бажання з необхідністю. Існує також низка методів

збереження конфіденційності, які можуть бути використані для зведення до мінімуму обробку даних на етапі навчання.

Біннс Р. (Binns, R., 2019 р.), дослідник в області штучного інтелекту (ШІ), і Галло В. (Gallo, V.), радник з технологічної політики, обговорюють деякі з методів, які організації можуть використовувати для дотримання вимог щодо мінімізації даних при впровадженні систем ШІ, у нещодавній статті щодо механізму аудиту штучного інтелекту ICO (ICO AI Auditing Framework):

> *«Деякі з цих методів включають модифікацію навчальних даних для зниження можливості пов'язати їх з конкретними людьми, зберігаючи при цьому їх корисність для цілей навчання ефективних моделей. Така модифікація може передбачати довільну зміну значень елементів даних, що належать окремим особам (відоме як "збурення" або додавання до даних "шуму"), у такий спосіб, за якого зберігаються деякі статистичні властивості цих елементів (див., скажімо, алгоритм RAPPORT)[5].*
>
> *Ці типи методів збереження конфіденційності можуть бути застосовані до навчальних даних після того, як вони вже були зібрані. Однак за можливості вони повинні застосовуватися до збору будь-яких персональних даних, щоб взагалі уникнути створення великих наборів персональних даних.*
>
> *Відповідний метод збереження конфіденційності іменується федеративним навчанням. Він дозволяє декільком різним учасникам навчати моделі на основі своїх власних даних ("локальні" моделі), а потім об'єднувати деякі з виявлених в цих моделях закономірностей (відомі як "градієнти") в єдину, більш точну "глобальну" модель, без необхідності обміну один з одним будь-якими навчальними даними. Федеративне навчання є відносно новим, але має кілька великомасштабних застосувань. Вони охоплюють автоматичну корекцію і моделі інтелектуального введення тексту на смартфонах, а також передбачають застосування для медичних досліджень, пов'язаних з аналізом за декількома базами даних пацієнтів.*
>
> *Хоча обмін градієнтом, отриманим за допомогою локально навченої моделі, являє собою менший ризик для конфіденційності, ніж обмін самими навчальними даними, градієнт все ж може розкрити деяку особисту інформацію, що стосується суб'єктів даних, від яких він був отриманий, особливо якщо модель є складною з великою кількістю детальних змінних. Тому контролерам даних все одно доведеться оцінювати ризик повторної ідентифікації. У разі федеративного навчання організації, що беруть участь, швидше за все, будуть вважатися спільними контролерами, навіть якщо вони не мають доступу до даних один одного».*

Наглядові органи повинні заохочувати організації та державні органи до просування механізму дотримання прав і цінностей, які дозволяють уникнути моделей обробки даних, що передбачають плату за конфіденційність, а отже по суті ставлять дітей в невигідне становище з фінансової точки зору і підвищують рівень непропорційної експлуатації більш маргіналізованих дітей, молоді та сімей, що живуть в бідності.

II.13.3 Механізми аудиту

[5] http://www.chromium.org/developers/design-documents/rappor

Школи повинні запровадити механізми аудиту, щоб дати дітям і сім'ям можливість зрозуміти, «хто та що знає про мене». (Уповноважений у справах дітей, (2017 р.) Великобританія) Такі механізми могли б включати щорічні звіти шкіл і їхніх фахівців з інтеграції даних, аби полегшити розуміння, які треті сторони мають доступ до даних, для яких цілей і для використання скількома фізичними особами. Недостатньо, щоб сім'я могла зрозуміти із загальної політики обробки даних, загальної для всіх, опублікованої на вебсайті школи, що було зроблено з особистими даними її дитини.

II.13.4 Доступ суб'єктів персональних даних та звіти про використання даних

На довіру до використання конфіденційних даних впливає розуміння безпеки даних, анонімізація, наявність автономії й контролю, знання того, хто буде мати доступ, наскільки точними є записи, як людей інформують про зміни, хто підтримує і регулює базу даних, і як люди будуть захищені від упереджень і дискримінації при використанні їхніх даних.

Повідомлення про плани збереження і знищення даних також повинні вводитися в практику, коли дитина залишає навчальний заклад і завершує кожен етап обов'язкової освіти (дитячий садок, початкову, середню, спеціальну, вищу освіту).

Освітні установи повинні публікувати щорічний 12-місячний аудиторський звіт про захист даних на рівні школи, включно з реєстром поширення персональних даних третьої сторони, оцінкою впливу на захист даних, наданням повідомлень про конфіденційність і будь-які значні зміни, а також повідомляти про будь-які порушення та оприлюднювати звіти про будь-які аудиторські перевірки, проведені постачальниками або користувачами даних про учнів.

II.14 Роль розробників та галузі

II.14.1 Несумісні наслідки

У керівних вказівках має бути роз'яснено, що створення умов для здійснення всіх прав, передбачених статтею 9 Конвенції, є вимогою щодо захисту даних за замовчуванням, а не факультативною можливістю, і що таке рішення, яке спричиняє несумісні наслідки *за замовчуванням* для здійснення школярами своїх прав, повинно розглядатися як несправедливе і протизаконне. Зараз ми зустрічаємося з продуктами та контролерами даних, які стверджують, що їхня база даних суб'єктів занадто велика, аби мати можливість підтримувати зв'язок, що було підкреслено в справі, де вперше накладено штраф польським Управлінням із захисту даних (DPA) згідно з GDPR і польським Законом про захист персональних даних від 10 травня 2018 року, який надає чинності GDPR. Це рішення надає деякі обмежені уявлення про тлумачення терміну «несумісні наслідки» в значенні статті 14(5)(b) GDPR. Ми рекомендуємо, щоб цей термін сам собою розглядався як недотримання статті 25, а не використовувався як привід для позбавлення суб'єктів даних їхніх прав. Отже, саме обробка даних повинна бути визнана незаконною, а не підтримка ідеї про те, що позбавлення можливості здійснювати права є прийнятним.

Екамбаранатан (Ekambaranathan) і Чжао (Zhao) (2019 р.) встановили, що багато розробників технологій, спрямованих на сім'ю, вважають неетичною практикою збір і продаж даних про дітей як товару (5/5 респондентів і 71/81 респондентів опитування). Деякі розробники також відмовляють третім особам в платному доступі до даних своїх в

силу моральних причин і зобов'язань. Разом з тим в цих технологіях, призначених для дітей, як і раніше часто виявляється недостатнє забезпечення конфіденційності даних.

II.14.2 Бібліотеки сторонніх розробників

При розробці програмного забезпечення повторне використання наявних бібліотек кодів, створених іншими розробниками, вважається загальною практикою, що дозволяє спільнотам розробників знизити накладні витрати на розробку і більш ефективно використовувати наявні ресурси (як-от хмарні обчислення). Однак використання цих бібліотек кодів часто означає, що розробник не бачить або не розуміє повною мірою вплив цих бібліотек кодів і їхню взаємодію зі своїми власними. Це може відбуватися з безневинних причин, наприклад, бібліотеки кодів часто створюються розробниками в країнах, які не мають систем захисту даних, і тому вони не знають про нормативні бази РЄ або ЄС; або такі причини можуть бути менш безневинними, наприклад, коли бібліотеки кодів створені розробниками, що фінансуються галуззю рекламних технологій (adTech). З цього випливає, що програмне забезпечення може поширювати дані користувачів третім особам, про яких розробник може повністю і не знати.

«Бібліотеки третіх осіб все частіше використовуються в сучасних застосунках. Провідним чинником для цього є те, що розробники покладаються на цільову рекламу для отримання доходу, яка своєю чергою використовує сторонні бібліотеки для збору цільових даних. Крім того, вони також спрощують розробку, забезпечують підвищену функціональність і можуть бути більш безпечними, ніж власноруч розроблені програмні модулі. Втім, ці бібліотеки мають дозволи на збір конфіденційних даних та, як було доведено, часто отримують доступ до дозволів на розташування, відстежують журнали викликів, історію браузера і контактну інформацію для цільової реклами, навіть якщо це не було заплановано функціоналом». (Чжао (Zhao) та інші, очікується у 2019 р.)

Як приклад, розглянемо Комплект розробника програмного забезпечення Facebook (Software Developer Kit) щодо того, як застосунки на платформі Android обмінюються даними з Facebook (навіть якщо у вас немає облікового запису на Facebook). («Privacy International», 2019 р.)

«Розробники застосунків обмінюються даними з Facebook через Комплект Facebook для розробки програмного забезпечення (SDK — Software Development Kit), який є набором інструментів для розробки програмного забезпечення та застосунків (Apps) для конкретної операційної системи. Комплект Facebook SDK для Android дозволяє розробникам застосунків інтегрувати свої застосунки із платформою Facebook і містить низку основних компонентів: Analytics (Аналітика), Ads (Реклама), Login (Логування), Account Kit (Управління обліковим записом), Share (Обмін даними), Graph API (Графічний API), App Events (Події застосунку) та App Links (Посилання застосунку). Наприклад: Використання Комплекту SDK Facebook дозволяє підтримувати автентифікацію на основі функції «Вхід через Facebook», яка дозволяє користувачам входити в систему, використовуючи телефонний номер або адресу електронної пошти з паролем Facebook. Комплект SDK Facebook також пропонує аналітику (Analytics) (дані, тренди й сукупну інформацію про аудиторію, а саме людей, що взаємодіють із застосунком), а також рекламу (Ads), читання і запис в графічний API Facebook».

Умови користування продуктом часто передбачають, що згода є необхідною підставою для обробки даних, і не через цілі, для яких школа використовуватиме особисті дані дитини, а через те, як продукт і його постачальники будуть використовувати ці дані. Однак, якщо погодитися з тим, що згода на обробку даних є законною підставою, вона не може бути вільно наданою і, отже, не може бути законною в шкільному середовищі

для виконання повсякденних завдань через дисбаланс сил у відносинах між дітьми, сім'ями та працівниками школи, і тим паче у непрямих відносинах між дитиною і власниками продукту. Це означає, що очікування третіх осіб щодо того, що їм дозволено робити, повинні змінитися.

II.14.3 Законна підстава для обробки

В керівних принципах Європейської ради із захисту даних 2/2019 з обробки персональних даних відповідно до статті 6(1)(b) GDPR в контексті надання онлайн послуг суб'єктам даних (жовтень 2019 року) зазначено, що в більшості випадків користувач укладає договір на використання наявної послуги. Хоча що можливість удосконалення та зміни послуги може бути включена в умови договору, така обробка зазвичай не може розглядатися як об'єктивно необхідна для виконання договору з користувачем, і це, зокрема, стосується шкільного середовища, в якому не існує прямих відносин між дитиною і компанією.

Що стосується обробки особливих категорій конфіденційних персональних даних, то в керівних принципах щодо надання згоди Робоча група з питань реалізації статті 29 також зазначила, що стаття 9(2) GDPR не визнає «необхідне для виконання договору» винятком із загальної заборони на обробку особливих категорій даних. З цього випливає, що «необхідне для роботи продукту» не є істотною підставою для виключення із закону про захист даних. Іншими словами, школи, компанії та розробники продукту не повинні чекати звільнення від примусових заходів лише тому, що продукт працює без дотримання прав.

Якщо більшість послуг і інструментів з обробки даних, доступних сьогодні школам, не відповідають високим стандартам закону, а також етичним очікуванням щодо того, що слід робити з персональними даними дітей, то виникає необхідність нового підходу.

Навіть США, які традиційно виступають проти законодавства про недоторканність приватного життя, змінюють свій підхід. На момент написання доповіді Федеральна торгова комісія США проводить відкриту консультацію щодо реалізації положення про захист приватного життя дітей онлайн (COPPA). У ньому постає питання про те, чи є вимога про згоду ефективною з точки зору захисту приватного життя та безпеки дітей в інтернеті. З огляду на те, який обсяг даних про дітей в Європі збирається або обробляється американськими компаніями, за консультацією COPPA треба уважно стежити.

II.14.4 Необхідні керівні вказівки для розробників в контексті EdTech

Очікуваний стандарт обробки даних про дітей в сфері освіти повинен встановлювати високу планку за замовчуванням, щоб відповідати прийнятним рівням якості та законності. Це повинно підкріплюватися поєднанням галузевих керівних принципів, законодавчо закріплених кодексів практики та більш конкретними секторальними заходами щодо забезпечення їх дотримання регуляційними органами.

Такі стандарти можуть бути викладені в кодексах практики, і при їх розробці необхідна широка співпраця з розробниками, галуззю, фахівцями-практиками в сфері освіти, академічними колами, організаціями, що представляють викладачів, сім'ями та громадянським суспільством.

На закінчення: Хто формуватиме майбутнє?

Розробникам політики не слід боятися запитувати про те, якою мірою швидке зростання націлених на школярів технологій і автоматизація шкільної адміністрації відповідають найкращим інтересам дитини.

> *«Взяті разом, кореляційні та експериментальні дані не дають переконливих доказів загального впливу цифрових технологій на результати навчання. З цього не випливає, що не варто інвестувати в використання технологій для поліпшення успішності. Але це повинно заохочувати нас до обережності при застосуванні технологічних рішень в освітніх питаннях. Потрібно ретельно подумати, перш ніж використовувати технології, аби забезпечити максимальну ефективність*». (Хіггінс С. (Higgins, S.), Сяо З. (Xiao, Z.) і Каціпатакі М. (Katsipataki, M.), 2012 р.).

Так само слід проявляти обережність відносно заяв компаній, що звучать під час маркетингу всіх новітніх технологій.

> *«Те, що мається на увазі, коли організації застосовують "штучний інтелект" до певної проблеми, часто не відрізняються від застосування обчислень, статистики або навіть доказів. Використання цієї фрази стало настільки сміховинно двозначним і буденним, що її можна порівняти з висловлюванням про те, що для розв'язання проблеми міської інфраструктури необхідно "застосовувати електроінструменти"...*
>
> *Бен Грін (Ben Green) розглядає ці питання у своїй нещодавній книзі "Досить розумне місто" (The Smart Enough City), наголошуючи на необхідності розглядати технологію як один з інструментів в наборі: лише один з багатьох засобів, які потенційно можуть бути використані для досягнення складної та погодженої з суспільством мети. Основну увагу слід приділити зніманню "технічних окулярів" для з'ясування проблем, викликів і потреб, а також не боятися виявити, що інші альтернативні стратегічні варіанти є кращими за інвестиції в технології*». (Веале М. (Veale, M.), 2019 р.)

Метою цієї Конвенції є забезпечення на території кожної Сторони для кожної особи, незалежно від її громадянства або місця проживання, поваги до її прав і засадничих свобод, і зокрема її права на недоторканність приватного життя, з огляду на автоматичну обробку персональних даних, що її стосуються («захист даних»). Повага до «до свого приватного і сімейного життя, до свого житла і кореспонденції» з деякими обмеженнями, які накладаються «згідно із законом» і є «необхідними у демократичному суспільстві», означає право на відсутність втручання.

Ця доповідь має сприяти розумінню відповідальних за розробку політики осіб необхідності переходу від культури дотримання правил до культури поваги прав при обробці даних в галузі освіти. Рекомендації повинні визнавати професійну автономію, а також забезпечувати додаткове запровадження очікуваних високих стандартів.

Якщо ми будемо і далі йти нинішнім шляхом в цьому напрямку стосовно обробки даних в освіті, баланс сил назавжди залишиться на користь корпоративних гігантів. Саме вони визначатимуть пропозицію, безпеку та інституційну пам'ять державних освітніх систем, а також вплив, який ці системи щодня здійснюють на мільйони дітей.

Державна і корпоративна база знань про життя окремих людей, що зберігається в шкільних інформаційних системах управління, тисячах застосунків і платформних

системах, буде безперешкодно супроводжувати дитину на кожному етапі її навчання та в процесі трудової діяльності. Величезні обсяги даних з минулого будуть використовуватися працівниками школи, які все більше боятимуться, що їхні людські судження вартуватимуть менше, ніж рішення, прийняті під керівництвом машини. Прогнози будуть визначати навчальні плани дітей і їхній життєвий вибір, починаючи з дедалі більш раннього віку.

Генетичні відмінності між дітьми використовуватимуться для їхньої стратифікації за ризиками з народження, а також для іншого застосування чи відмови від освітніх заходів. Вибір місця дитини в школі, яке формує більшу частину його життя сьогодні, може перейти до вибору в утробі матері, на основі якого когнітивні характеристики будуть розглядатися як бажані і як аномалії, або ж дитина з додатковими потребами взагалі не матиме свого місце у світі.

Або ж відповідальні за розробку політики особи можуть в пріоритетному порядку визначити шляхи практичного здійснення і реалізації прав людини та цінностей, що лежать в основі Конвенції.

Якщо це покоління не має уповільнюватися через тягар своїх минулих даних, але натомість мати свободу, що необхідна для його формування, то діти повинні мати можливість здійснювати своє право на освіту у такий спосіб, щоб це не завдавало шкоди їх власному і колективному майбутньому. Баланс сил між організаціями та установами в порівнянні з балансом сил між дитиною і сім'єю повинен бути змінений в терміновому порядку,

«На вас дивляться всі майбутні покоління. І якщо ви нас зрадите, ми ніколи не пробачимо вам». (Ґрета Тунберг, Саміт ООН щодо зміни клімату, вересень 2019 року)

Визначення

1. Для цілей цієї доповіді

a. «Персональні дані» означають будь-яку інформацію, що стосується ідентифікованої або такої, що піддається ідентифікації, особи («суб'єкт даних»).

b. «Чутливі дані» означають персональні дані, щодо яких особа може мати певну довіру, скажімо, маркери поведінки, що вказують на акти насильства, але які не були розглянуті в суді, а отже технічно не є «кримінальним засудженням», чи сімейний дохід, але які можуть не підпадати під визначення даних особливої категорії, передбачених в законі про захист даних.

c. «Дані особливої категорії» мають те саме значення, що й у статті 6 оновленої конвенції №108+. «Обробка: генетичних даних; персональних даних, що стосуються правопорушень, кримінальних проваджень та судимості, а також пов'язаних із цим заходів безпеки; біометричних даних, які однозначно ідентифікують особу; персональних даних, що містять інформацію про расову або етнічну належність, політичні переконання, членство в профспілках, релігійні чи інші переконання, про здоров'я або сексуальне життя, дозволяється лише в тому випадку, коли закон закріплює відповідні гарантії, які доповнюють ті, що передбачені цієї Конвенцією. Такі гарантії повинні захищати від ризиків, які може становити обробка конфіденційних даних щодо інтересів, прав та основоположних свобод суб'єкта даних, зокрема, від ризику дискримінації».

d. «Обробка» означає будь-яку операцію або комплекс операцій, що здійснюються частково або повністю за допомогою автоматизованих процесів і застосовуються до персональних даних, як-от зберігання, консервація, адаптація або зміна, вилучення, консультування, використання, повідомлення, зіставлення або об'єднання, а також видалення або знищення.

e. «Профіль» (n) означає набір даних, що характеризують категорію осіб або поведінку, які призначені для застосування до окремої особи або групи осіб.

f. «Профілювання» означає метод автоматичної обробки даних, який полягає в обробці даних з метою застосування моделі «профілю» до окремої особи, віднесення особи до певної категорії або зіставлення атрибутів з моделлю, зокрема, для прийняття рішень, що стосуються суб'єкта, або для вжиття заходів втручання, або для аналізу чи прогнозування її особистих переваг, поведінки та ставлення. Такі профілі можуть бути створені з даних, які надають інші суб'єкти, або які є непрозорими для них, наприклад, дані взаємодії з використанням платформи, які відправляються з пристрою до компанії, але користувачі їх не бачать.

g. «Послуга інформаційного суспільства» означає будь-яку послугу, що зазвичай надається за винагороду, на певній відстані, за допомогою електронних засобів та відповідно до того самого визначення, яке надане в статті 1(1)(b) Директиви (ЄС) 2015/1535.

h. «Контролер» означає фізичну або юридичну особу, державний орган, установу або будь-який інший орган, який самостійно або у співпраці з іншими визначає цілі та засоби, що використовуються при зборі та обробці персональних даних.

i. «Обробник» означає фізичну або юридичну особу, орган державної влади, установу або будь-який інший орган, який обробляє персональні дані від імені контролера.

j. «Click-wrap угоди» означає угоди про умови, які компанія або постачальник продукту не дозволяє змінювати школі або користувачеві. Вони надаються у вигляді пакету, який школа може лише прийняти або від якого відмовитися, і відмова означатиме, що вони більше не зможуть використовувати продукт або платформу.

k. «Послідовний ланцюжок» (daisy-chain) розповсюдження означає серію операцій, які об'єднані разом, що дозволяє багатьом третім сторонам видобувати або отримувати дані від попередньої сторони в ланцюжку. Зображення являє собою зв'язаний віночок квітів, які діти зазвичай можуть сплітати разом.

Подяки

Авторка хотіла б висловити свою вдячність дуже багатьом особам з різних країн світу, які поділилися своїми власними роботами й міркуваннями на підтримку цієї роботи. Зокрема, подякувати тим, хто зробив безпосередній і значний внесок в роботу за своєю тематикою, зокрема, доктору Бену Вільямсону (Ben Williamson), науковому співробітнику Центру досліджень в галузі цифрової освіти та Единбурзького університету майбутнього; а також доктору Цзюнь Чжао, старшому науковому співробітнику факультету обчислювальної техніки Оксфордського університету, які поділилися своїми міркуваннями щодо розробників.

Список використаних джерел

«Aftenposten» (2020 р.) *Datatilsynet undersøker om det er lovlig å bruke Google i skolen*. Норвезьке управління із захисту даних оголосило про те, що воно вивчає питання законності використання Google в школах. (дата перегляду – 21 лютого 2020 року) https://www.aftenposten. no/norge/i/pLvba6/datatilsynet-undersoeker-om-det-er-lovlig-aa-bruke-google-I -skolen

Робоча група з питань реалізації статті 29, Висновок 2/2009 щодо захисту персональних даних дітей (Загальні керівні принципи та особливий випадок шкіл) https://ec.europa.eu/justice/article-29/ documentation/ opinion- recommendation/files/2009/wp160_en.pdf

Коаліція «Against Borders for Children» (2016 р.) https://www.schoolsabc.net/2016/09/letter-justine-greening/ (дата перегляду – серпень 2019 року)

Алім Ф. (Alim, F.), та інші (2017 р.). (Фонд електронних рубежів, Electronic Frontier Foundation) «Шпигунство за учнями: пристрої, видані школою, і конфіденційність учнів» (Spying on Students: School-Issued Devices and Student Privacy, https://www.eff.org/files/ 2017/04/13/student-privacy-report.pdf

Андреєвич М. (Andrejevic, M.) і Селвін Н. (Selwyn, N.) (2019 р.) «Технологія розпізнавання обличчя в школах: критичні питання та проблеми» (Facial recognition technology in schools: critical questions and concerns), журнал «Learning, Media and Technology», ідентифікатор DOI: 10.1080/17439884.2020.1686014

Андерсон Р. (Anderson, R.), Браун І. (Brown, I.), Клейтон Р. (Clayton, R.), Дауті Т. (Dowty, T.), Корфф Д. (Korff, D.) та Мунро Е. (Munro, E.), (2009 р.), «Бази даних про дітей. Безпека та конфіденційність» (Children's Databases - Safety and Privacy). Доповідь для Уповноваженого з питань інформації (Велика Британія). (дата перегляду – жовтень 2019 року) https://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf

«Ars Technica», Кокс К. (Cox, K.) (2019 р.) «50 штатів і територій розпочинають масштабне спільне розслідування відносно Google» (50 states and territories launch massive joint probe into Google) https:// arstechnica.com/tech-policy/2019/09/50-states-and-territories-launch-massive-joint-probe-into-google/

«Автоматизація суспільства: підбивання підсумків автоматизованого прийняття рішень в ЄС» (Automating Society: Taking Stock of Automated Decision-Making in the EU). «AlgorithmWatch» (2019 р.) https://algorithmwatch.org/wp-content/uploads/2019/01/Automating_Society_Report_2019.pdf

Справа «Балдерас, Нью-Мексико, проти “Google LLC”» (Balderas, New Mexico, vs GoogleLLC), 2020 р. https://cdn.vox- cdn.com/uploads/chorus_asset/file/19734145/document_50_.pdf (дата перегляду – 24 лютого 2020 року)

Центр інтернету та суспільства ім. Беркмана Гарвардського університету (2008 р.), Доповідь «Підвищення безпеки дітей і онлайн-технології» (Enhancing Child Safety and Online Technologies Report). h t t p s : / / c y b e r. h a r v a r d . e d u / s i t e s / c y b e r. l a w. h a r v a r d . e d u / fi l e s / ISTTF _ Final_ Report.pdf (дата перегляду – листопад 2017 року)

Біннс (Binns) та інші (2018 р.), «Вимірювання потужності сторонніх трекерів в інтернеті та на мобільних пристроях» (Measuring third party tracker power across web and mobile). WebSci’18. https:// ora.ox.ac.uk/objects/uuid:86310ed1−762e−4037−a4d2−80568c5ee7c4 (дата перегляду – вересень 2019 року)

Біннс (Binns) та інші (2018 р.), «Стороннє відстеження в мобільній екосистемі» (Third Party Tracking in the Mobile Ecosystem). TOIT. https://arxiv.org/abs/1804.03603 (дата перегляду – вересень 2019 року)

«Big Brother Watch» (2014 р.), доповідь: «Біометрика в школах» (Biometrics in Schools) https://www.bigbrotherwatch.org.uk/files/reports/Biometrics_final.pdf (дата перегляду – 12 листопада 2017 року) та «Моніторинг в у класі; Ще одна цеглина в стіні» (Classroom Monitoring; Another Brick in the Wall) (2016 р.) https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/11/Classroom-Management-Software-Another-Brick-in-the-Wall.pdf (дата перегляду – 12 листопада 2017 року)

Біннс (Binns) та інші (2018 р.), «Це зводить людську істоту до відсотка» (It’s Reducing a Human Being to a Percentage); Сприйняття справедливості в алгоритмічних рішеннях (Perceptions of Justice in Algorithmic Decisions). ArXiv:1801.10408 (Cs), 1–14. https://doi.org/10.1145/3173574 .3173951.

Бут Р. (Booth, P.) (2017 р.), «Перевірка віку як новий закон про cookie?» (Age Verification as the new cookie law?) http://www.infiniteideasmachine.com/ 2017/08/age-verification-as-the-new-cookie-law/

Боулз Н. (Bowles, N.), (2019 р.) New York Times. «Кремнієва долина дійшла до шкіл Канзасу. Це спричинило повстання. (Silicon Valley Came to Kansas Schools. That Started a Rebellion.) https://www.nytimes.com/2019/04/21/technology/silicon-valley-kansas-schools.html

Бойд Д. (Boyd, D.) і Кроуфорд К. (Crawford, K.) (2012 р.). «Критичні питання для великих даних: провокації для культурного, технологічного і наукового феномену» (Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon). 15(5), журнал «Information, Communication, & Society», 662–679

Справа «Брейер проти Німеччини» (Breyer vs Germany), http://curia.europa.eu/juris/document /document.jsf? docid=184668&doclang=EN (дата перегляду – 1 листопада 2017 року)

«Bridge International» (дата перегляду – вересень 2019 року) https://www.bridgeinternationalacademies.com/ supporting/teacher-tools/

Кардіффська лабораторія інформаційної справедливості (Cardiff Data Justice Lab), «Оцінки даних як звіт про врядування» (Data Scores as Governance Report) (2018 р.) https://datajusticelab.org/data-scores-as-governance/

Кампанія за вільне від комерції дитинство (Campaign for a Commercial Free Childhood) (2015 р.) https://commercialfreechildhood.org/3-million- teachers-mcdonalds-were-not-lovin-it/

Картер П. (Carter, P.), Лорі Г. (Laurie, G.), Діксон-Вудс М. (Dixon-Woods, M.) (2015 р.), «Соціальна ліцензія на дослідження: чому у care.data виникли проблеми» (The social licence for research: why care.data ran into trouble), J Med Ethics 2015;41:404-409 doi:10.1136/medethics-2014-102374

Уповноважений у справах дітей, (2017 р.) (Великобританія) «Цифровий розвиток» (Growing Up Digital) https://www.childrenscommissioner.gov.uk/publication/growing-up-digital/

Проєкти Chromium: Rappor (Рандомізовані агреговані орядкові відповіді, що зберігають конфіденційність) The Chromium (Projects: Rappor (Randomized Aggregatable Privacy Preserving Ordinal Responses)) http://www.chromium.org/developers/design-documents/rappor

«Class Dojo» (блог компанії) «У чому помилялась The New York Times» (What The New York Times Got Wrong). https://web.archive.org/web/20191113122736/ https://www.classdojo.com/en-gb/nyt/

Рішення щодо розпізнавання обличчя, CNIL (Національна комісія з питань інформаційних прав і свобод) (lycée les Eucalyptus à Nice et lycée Ampère à Marseille) (2019) Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position https:// www.cnil.fr/fr /experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-positi on

Конлі Д. (Conley, D.) і Флетчер (Fletcher), (2017 р.), «Фактор геному — що революція в соціальній геноміці відкриває про нас самих, нашу історію та майбутнє» (The Genome Factor - What the Social Genomics Revolution Reveals about Ourselves, Our History, and the Future), ISBN : 9780691164748, Princeton University Press

Стратегія Ради Європи з прав дитини на 2016–2021 роки, https://rm.coe.int/168066cff8 (дата перегляду – 1 листопада 2017 року), пункт 30, CM/Rec (2013) 2. 1.2. Протидія дискримінації

Рада Європи (2017 р.), Керівні принципи щодо захисту фізичних осіб при обробці персональних даних у світі великих даних. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTM Content?documentId=090 00016806ebe7a

Рада Європи, Комітет експертів з правозахисних аспектів автоматизованої обробки даних і різних форм штучного інтелекту (MSI-AUT) (робота готується) https://www.coe.int/en/web/ freedom-expression/msi-aut

Рада Європи, Дослідження iDGI(2019)05 щодо відповідальності та ШІ (Доповідач: Єнг (Yeung), 2019 р.). Підготовлено Комітетом експертів з правозахисних аспектів автоматизованої обробки даних і різних форм штучного інтелекту (MSI-AUT) https://rm.coe.int/responsability-and-ai-en/168097d9c5

Рада Європи (2017 р.), Розпакування штучного інтелекту. Десять кроків для захисту прав людини (Unboxing Artificial Intelligence, Ten Steps to Protect Human Rights) https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64

Рекомендація Комітету міністрів державам-членам CM/Rec (2018)7 про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі (Ухвалено Комітетом Міністрів 4 липня 2018 року на 1321-му засіданні заступників міністрів) https://search.coe.int/cm /Pages/result_details.aspx?ObjectID=09000016808 b79f7

Девідсон К. (Davidson, C.) (2017 р.) «Нова освіта: як провести революцію в університеті, щоб підготувати студентів до мінливого світу» (The New Education: how to revolutionise the university to prepare students for a world in flux) (Basic Books)

Міністерство освіти, (Великобританія) (2019 р.), «Спеціальні освітні потреби: аналіз та резюме джерел даних» (Special educational needs: an analysis and summary of data sources) https:// assets. publishing. service. gov. uk/ government/ uploads/ system/ uploads/ attachment_data /file/804374/Special_educational_ needs _May _19.pdf

Данський інститут з прав людини (2016 р.), Керівництво та інструментарій з оцінки впливу на права людини (Human rights impact assessment guidance and toolbox) (The Danish Institute for Human Rights) https://www.humanrights.dk/business/tools/human- rights- impact-assessment-guidance-and-toolbox

defenddigitalme, (2016 р.) «Хронологія використання шкільного перепису в імміграційних цілях» (Timeline of school census use for immigration enforcement purposes) https:// defenddigitalme.com/timeline-school-census/ and https://en.wikipedia.org/wiki/ England_school _cen sus

defenddigitalme (2016 р.) «Надання національних записів про учнів комерційним компаніям, благодійним організаціям, аналітичним центрам та пресі» (Distribution of national pupil records to commercial companies, charities, think tanks and the press) https://defenddigitalme.com/faqs/ на підставі https://www.gov.uk/government/publications/dfe-external-data-shares

Денхем Е. (Denham, E.), Уповноважений з питань інформації, ICO, (2017 р.) «Щодо “інновацій”, висновки на Google DeepMind та Royal Free» https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/ royal-free- google-deepmind-trial-failed-to-comply-with-data-protection-law/

Дауті Т. (Dowty, T.), Корфф Д. (Korff, D.) (2009 р.), «Захист віртуальної дитини: закон та згода дітей на обмін персональними даними» (Protecting the Virtual Child: the law and children’s consent to sharing personal data) https://www.nuffieldfoundation.org/sharing-childrens-personal-data

Дуркін Е. (Durkin, E.) (2019 р.) The Guardian, «Система розпізнавання обличь у шкільному окрузі Нью-Йорка викликає побоювання з приводу конфіденційності» (New York school district’s facial recognition system sparks privacy fears) https://www.theguardian.com/technology/2019/may/31/facial-recognition-school-new-york- privacy- fears

Випробувальний полігон інновацій «EdTech Innovation Testbed», Nesta (2019 р.) https://www.nesta.org.uk/project/edtech-innovation-testbed/ frequently-asked-questions/ permanent record at https://web.archive.org/web/20191015162357/https://www.nesta.org.uk/project/edtech-innovation testbed/frequently-asked-questions/

«Education Foundation» (2013 р.), Керівництво Facebook для освітян (Facebook Guide for Educators).https://www.ednfoundation.org/wp-content/uploads/Facebookguideforeducators.pdf Критикується громадянським суспільством в Англії як рекламний захід

The Economist (2012), «Здобуття нових знань» (Learning new Lessons) www.economist.com/news /international/ 21568738- online-courses-are-transforming-higher-education-creating-new-opportuniti es-best (дата перегляду – листопад 2017 року)

Елліот М. (Elliot, M.), Пурдам К. (Purdam, K.), Маккі Е. (Mackey, E.), (2013 р.), «Горизонти даних: нові форми даних для соціальних досліджень» (Data Horizons: New forms of Data for Social Research) Факультет соціальних наук Манчестерського університету http://hummedia.manchester .ac.uk/institutes/ cmist/archive-publications/reports/2013-05-Data_Horizons_Report.pdf (дата пере-г гляду – 11 листопада 2017 року)

ESCR-Net (2018 р.) «Громадянське суспільство засуджує некомерційну мережу шкіл ICT4D» (Civil society denounces for-profit ICT4D network of schools) (дата перегляду – серпень 2019 року) https://www.escr-net.org/news/2018/civil-society-denounces-profit-ict4d-network-schools and their list of Bridge International Academies Investors http://globalinitiative-escr.org/wp-content/uploads/ 2018/02/List-of-BIA-investors.pdf

Агентство Європейського Союзу з фундаментальних прав людини (2019 р.), Агентство зібрало інформацію про політичні ініціативи, пов’язані з ШІ, у країнах-членах ЄС у період 2016-2019 років. Колекція наразі налічує близько 180 ініціатив. https://fra.europa.eu/en/project/2018/artificial-intelligence-big-data-and-fundamental- rights/ai-policy-initiatives

Керівні принципи Європейської ради із захисту даних 2/2019 з обробки персональних даних відповідно до статті 6(1)(b) GDPR в контексті надання онлайн послуг суб’єктам даних https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public _consultation_en.pdf

«Evening Standard» (2012 р.) «Відеоспостереження в шкільному туалеті вашої дитини: Понад 200 шкіл зізнаються, що використовують камери в туалетах та роздягальнях» (The CCTV in your child’s school toilet: More than 200 admit using cameras in loos and changing rooms), https://www.standard.co.uk/news/education/the-cctv-in-your-childs-school-toilet-more-than-200-admit -using-cameras-in-loos-and-changing-rooms-8129753.html

Фічтер А. (Fichter, A.), Der Republik (2019) «Шпигун в класній кімнаті» (Der Spion im Schulzimmer) https://www.republik.ch/2019/07/02/der- spion-im-schulzimmer

Ферейра Х. (Ferreira, J.), генеральний директор освітньої компанії «Knewton» (2012 р.) https://www.youtube.com/watch?v=Lr7Z7ysDluQ Джерело: канал YouTube Управління освітніх технологій Міністерства освіти США.

FOCIAI https://fociai.com/

Forbes (2014 р.), «Facebook маніпулював новинними стрічками користувачів для створення емоційних відгуків» (Facebook Manipulated User News Feeds To Create Emotional Responses) (дата перегляду – вересень 2019 року) https://www.forbes.com/sites/gregorymcneal/2014/06/28/facebook-manipulated- user- news-feeds-to-create-emotional-contagion/

Застосунок «Google Family Link» https://families.google.com/familylink та посилання на блог: «Google Family Link для дітей віком до 13 років: друг або брехун з точки зору конфіденційності дітей?» (Google Family Link for Under 13s: children's privacy friend or faux?) Перссон Дж. (Persson, J.) (2017 р.) http://jenpersson.com/google- family- link/

Gazette, The (2018 р.) «Батьки заспокоїлися після того, як на сайті в США була розміщена пряма трансляція з камер відеоспостереження в школах Блекпула» (Parents reassured after live footage from Blackpool schools' CCTV cameras was 'hosted on US website) https://www.blackpoolgazette.co.uk/education/parents-reassured-after- live- footage-from-blackpool-schools-cctv-cameras-was-hosted-on-us-website-1-9036288

Грін Т. (Greene, T.) (2018 р.) «Китайський ШІ розпізнавання обличчя має нову ціль: студенти» (China's facial recognition AI has a new target: Students) https://thenextweb.com/ artificial-intelligence/2018/05/18/chinas-orwellian-surveillance-state-turns-its-ai-powered-gaze-on- students/

Керівні принципи здійснення правосуддя з урахуванням інтересів дітей, прийняті Комітетом міністрів Ради Європи 17 листопада 2010 року. Дата перегляду – вересень 2019 року, https://rm.coe.int/16804b2cf3 (Див. також Резолюцію 2010 (2014) Парламентської асамблеї «Ювенальна юстиція, доброзичлива до дітей: від риторики до реальності», а також рекомендації Європейського комітету із правового співробітництва (CDCJ(2014)15) щодо просування та підтримки впровадження Керівних принципів здійснення правосуддя з урахуванням інтересів дітей.)

Хенд Б. (Hand, B) (2019 р.) «Біометрія в школах: 4 способи використання біометричних даних для підвищення рівня навчання» (Biometrics In Schools: 4 Ways Biometric Data Can Be Used To Enhance Learning) https://elearningindustry.com/biometrics-in-schools-data-enhance-learning-4-ways

Герольд Б. (Herold, B.) (2018 р.) Education Week, «Щоб зупинити стрілянину в школах, штат Флорида об'єднає державні дані та повідомлення в соціальних мережах» (To Stop School Shootings, Fla. Will Merge Government Data, Social Media Posts), https://www.edweek.org/ew/articles/2018/07/26/to-stop-school-shootings-fla-will- merge.html

Хіггінс С. (Higgins, S.), Сяо З. (Xiao, Z.) та Каціпатакі М. (Katsipataki, M.) (2012 р.) «Вплив цифрових технологій на навчання: резюме для фонду Education Endowment Foundation» (The Impact of Digital Technology on Learning: A Summary for the Education Endowment Foundation). Педагогічна школа Даремського університету

Хільдебрандт М. (Hildebrandt, M.) (2016 р.) «Розумні технології та ціль (цілі) закону: нові суперечності між законом і технологіями» (Smart Technologies and the End(s) of Law : Novel Entanglements of Law and Technology) (Edward Elgar Publishing).(Глава 9)

HLEG-AI, Рекомендації щодо політики та інвестицій в галузі надійного штучного інтелекту (дата перегляду – 1 липня 2019 року) (опубліковано 26 червня 2019 року) https://ec.europa.eu/digital-single-market/en/news/policy- and- investment-recommendations-trustworthy-artificial-intelligence (permanent copy: https:// d e f e n d d i g i t a l m e . c o m / w p - c o n t e n t / u p l o a d s / 2 0 1 9 / 0 7 /AIHLEG Policy andInvestmentRecommendationspdf.pdf)

(Після відкритого процесу відбору Комісія призначила 52 експерти до Експертної робочої групи високого рівня з питань штучного інтелекту, до якої увійшли представники академічних кіл, громадянського суспільства, а також індустрії.)

IB Times, (2017 р.) «77 мільйонів акаунтів — студентів, вчителів, батьків — вкрадені» (77 Million Accounts, Students, Teachers, Parents Stolen), А.Дж. Деллінгер (AJ Dellinger), http:// www.ibtimes.com/edmodo-hacked-77-million-accounts-students-teachers-parents-stolen-education-social-2540073 (дата перегляду – 1 листопада 2017 року)

Резолюція ICDPPC щодо платформ електронного навчання, (2018 р.) (40-ва Міжнародна конференція уповноважених з питань захисту даних і недоторканості приватного життя) https://edps.europa.eu/sites/edp/files/publication/ icdppc-40th_dewg- resolution_adopted_en_0.pdf

Глобальна ініціатива IEEE з етичних міркувань у галузі штучного інтелекту та автономних систем. (2016 р.). «Етично узгоджений дизайн: бачення пріоритету добробуту за допомогою штучного інтелекту та автономних систем, версія 1.» (Ethically Aligned Design: A Vision For Prioritizing Wellbeing With Artificial Intelligence And Autonomous Systems, Version 1). IEEE, 2016 p. http://standards.ieee.org/develop/indconn/ec/ autonomous_systems.html.IEEE

IEEE, (2019 р.) «Машинний зір для аналізу відвідуваності і емоцій в школі» (Computer Vision for Attendance and Emotion Analysis in School Settings) https:// ieeexplore.ieee.org/document/8666488

India Today, (2019 р.), «Школа в Делі стала першою, яка надала батькам пряму трансляцію з системи відеоспостереження» (Delhi school becomes first ever to provide live CCTV video feed to parents) https://www.indiatoday.in/education-today/news/story/delhi-school-becomes-first-to-provide-live-cctv- video-feed-to-parents-cm-arvind-kejriwal-1564401-2019-07-08

Робочий документ Міжнародної робочої групи з питань захисту даних в галузі телекомунікації щодо платформ електронного навчання (2017 р.) https://epic.org/IWG/workingpapers/e-learning-platforms.pdf

i-news (2017 р.) «Ofsted планує «шпигувати» за батьками й учнями в соціальних мережах". (Ofsted to 'snoop 'on parents 'and pupils 'social media) https://inews.co.uk/news/ education/teachers-given-less-days-training-safeguarding/

Уповноважений з питань захисту інформації та недоторканності приватного життя в Онтаріо (IPC Ontario), Глобальна правоохоронна мережа захисту приватної таємниці (GPEN), Звіт щодо перевірки конфіденційності освітніх онлайн-сервісів (IPC Ontario GPEN Sweep Report) (2017 р.) https://www.ipc.on.ca/wp-content/uploads/2017/10/gpen- sweep-rpt.pdf (дата перегляду – серпень 2019 року)

Цзин М. (Jing, M.) (2019 р.) «Генеральний директор BrainCo каже, що його технологія «читання думок» призначена для поліпшення концентрації, а не для спостереження» (BrainCo CEO says his 'mind-reading 'tech is here to improve concentration, not surveillance) https://www.scmp.com/tech/innovation/article/3008439/brainco-ceo-says-his-mind-reading-tech-here-improve-concentration

Рішення Верховного Суду (2016 р.) UKSC51 https://www.supremecourt.uk/cases/docs/ uksc- 2015-0216-judgment.pdf

Рішення Суду Європейського Союзу у справі Бара (C-201/14) http://curia.europa .eu/jcms/upload/docs/application/pdf/2015-10/cp150110en.pdf (жовтень 2015 року)

Кінг П. (King, P.) «Біометрія в школах» (Biometrics in Schools) https://pippaking.blogspot.com/

Юридична спілка, (Великобританія) «Звіт про подію: Штучний інтелект, великі дані та верховенство права» (Event Report: Artificial Intelligence, Big Data and the Rule of Law), (дата перегляду – 12 листопада 2017 року) https://www.biicl.org/documents/1798_ai_event_-_final _report _ 15_11_2017_002.pdf

Стаття «Аналітика навчальних даних» (Learning Analytics) про громадянське навчання, підготовлена віцепрезидентом студентської спільноти (NSU) з комунікацій (серпень 2017 року), Університет Нортумбрії https://www.mynsu.co.uk/blogs/blog/tallykerr/ 2017/08/02/Learning-Analytics/ (дата перегляду – 11 листопада 2017 року)

Лівінгстон С. (Livingstone, S.) (2016 р.) «GDPR: Використання доказів для викриття наслідків для дітей онлайн» (The GDPR: Using evidence to unpack the implications for children online), блог проєкту з медіаполітики «LSE Media Policy Project», Лондонська школа економіки, http://blogs.lse.ac.uk/mediapolicyproject/ 2016/12/12/the-gdpr-using-evidence-to-unpack-the-implications-for-children-online/ (дата перегляду – 1 листопада 2017 року)

Лівінгстон С. (Livingstone, S.) (2017 р.) «Інтернет-виклики щодо конфіденційності, захисту та участі дітей: чого ми можемо очікувати від GDPR?» (Online challenges to children's privacy, protection and participation: what can we expect from the GDPR?), блог проєкту з медіаполітики «LSE Media Policy Project», Лондонська школа економіки, http:// blogs.lse.ac.uk/mediapolicyproject/2017/02/09/online-challenges-to-childrens-privacy-protection-and- participation-what-can-we-expect-from-the-gdpr/ (дата перегляду – 1 листопада 2017 року)

Лівенс Е. (Lievens, E.) (2016 р.) «Розшукується: доказова база на підтримку реалізації GDPR з урахуванням прав дітей» (Wanted: evidence base to underpin a children's rights-based implementation of the GDPR) блог проєкту з медіаполітики «LSE Media Policy Project», Лондонська школа економіки, http://blogs.lse.ac.uk/ mediapolicyproject/2016/11/10/wanted-evidence-base-to-underpin-a-childrens-rights-based- implementation-of-the-gdpr/ (дата перегляду – 1 листопада 2017 року)

Луптон Д. (Lupton, D.) та Вільямсон Б. (Williamson, B.) (2017 р.) «Датифікована дитина: датастереження за дітьми та наслідки для їхніх прав» (The datafied child: The dataveillance of children and implications for their rights). Журнал «New Media & Society» том 19, Випуск 5, 780–794;

Мантелеро А. (Mantelero A.) (2018 р.). «Штучний інтелект і великі дані: План оцінки впливу на права людини, соціальні та етичні аспекти» (AI and Big Data: A blueprint for a human rights, social and ethical impact assessment). Оцінка. Журнал «Computer Law & Security Review» (2018 р.), https://doi.org/10.1016/j.clsr. 2018.05.017.

Мантелеро А. (Mantelero A.) (2017 р.). «Регулювання великих даних. Керівні принципи Ради Європи в контексті Європейської системи захисту даних» (Regulating Big Data. The guidelines of the Council of Europe in the Context of the European Data Protection Framework), (2017) 33(5), журнал «Computer Law & Sec. Rev.» 584-602.

Матс С. (Mats, S.) (2018 р.) WIRED, «Психологічний мікротаргетінг дійсно може врятувати політику» (Psychological microtargeting could actually save politics) https:// www.wired.co.uk/article/psychological-microtargeting-cambridge-analytica-facebook

МакКоун (McKown) та інші (2017 р.) «Ключові принципи розробки прямої оцінки SEL: уроки, отримані після перших проблем в процесі розробки» (Key Design Principles for Direct Assessments of SEL: Lessons Learned from the First Design Challenge) (SEL – соціальне та емоційне навчання) https://measuringsel.casel.org/wp-content/uploads/2017/09/AWG-Design-Challenge-Direct-Assessments-of-SEL.pdf

Монахан Т. (Monahan, T.) і Торрес Р. (Torres, R) (2009 р.) «Школи під наглядом: Культура контролю в державній освіті (Критичні проблеми злочинності і суспільства)» (Schools Under Surveillance: Cultures of Control in Public Education (Critical Issues in Crime and Society)), Rutgers University Press, ISBN: 081354680X

Мунді К. (Mundie, C.) (2014 р.) «Прагматизм щодо конфіденційності. Акцент на використанні даних, а не на їх збиранні» (Privacy Pragmatism, Focus on Data Use not Collection), Foreign Affairs, березень/квітень (2014 р.), Том 93

Неморін С. (Nemorin, S.) (2017 р.) Університетський коледж Лондона, «Фіксація емоційних станів в цифровому шкільному просторі та модуляція суб'єктності учнів» (Affective capture in digital school spaces and the modulation of student subjectivities). Журнал «Emotion, Space and Society», ISSN 1755-458 http://eprints.lse.ac.uk/83298/

Неморін С. (Nemorin, S.), Селвін Н. (Selwyn, N.) (2018 р.) «Щоденне навчання в епоху цифрових технологій: середня школа або високі технології?» (Everyday Schooling in the Digital Age: High School, High tech?) https:// www.routledge.com/Everyday-Schooling-in-the-Digital-Age-High-School-High-Tech-1st-Edition/ Selwyn-Nemorin-Bulfin-Johnson/p/book/9781138069374

Доповідь Ради із захисту прав споживачів Норвегії #WatchOut (2017 р.) https://www.forbrukerradet.no/side/ significant-security-flaws-in-smartwatches-for-children та #ToyFail https://www.forbrukerradet.no/ siste-nytt/connected-toys-violate-consumer-laws/ (дата перегляду – 1 листопада 2017 року)

Норвезьке управління із захисту даних (2018 р.). Звіт про штучний інтелект і конфіденційність. https:// www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf.

Ніст К. (Nyst, C.) (ЮНІСЕФ) (2018), Принципи забезпечення конфіденційності та свободи вираження думок дітей в Інтернеті, Галузевий посібник (Principles for Children's Online Privacy and Free Expression Industry Toolkit) h t t p s : / / w w w . u n i c e f . o r g / c s r / fi l e s / UNICEF_Childrens_ Online_Privacy_and_Freedom _of _ Expression (1).pdf

ОЕСР (2018 р.), Дослідження ОЕСР щодо соціальних та емоційних навичок (діти 10-15 років) http:// www.oecd.org/education/ceri/thestudyonsocialandemotionalskills.html

Паппано Л. (Pappano, L.) (2012 р.) New York Times, Рік Масових відкритих онлайн-курсів (МООС) http://www.nytimes.com/2012/11/04/education/edlife/massive-open-online-courses-are-multiplying-at-a-rapid-pace.html

Патерсон Л. (Paterson, L.) та Грант Л. (Grant, L.) (2010 р.) Королівська інженерна академія, «Конфіденційність та упередженість: погляди молодих людей на електронні карти пацієнтів» (Privacy and Prejudice: Young people's views on Electronic Patient Records), довічний запис http://http://jenpersson.com/wp- content/uploads/2016/08/Privacy_and_Prejudice.pdf (page 40)

Паттерсон Дж. (Patterson. J.) (2019 р.), генеральний директор компанії «Gaggle», портал «Education Week», https://www.edweek.org/ew/articles/2019/05/30/ schools-are-deploying-massive-digital-surveillance-systems.html (дата перегляду – вересень 2019)

Батьківська коаліція за недоторканність приватного життя студентів (Parent Coalition for Student Privacy), Починаючи з 2012 року і до 2014 року відбувалося масове повстання проти планів штатів і округів розкрити персональні дані студентів в корпорації inBloom Inc., що фінансується Фондом Гейтса. https://www.studentprivacymatters.org/ background-of-inbloom/ (дата перегляду – листопад 2017 року)

Батьківська коаліція за недоторканність приватного життя студентів, «Студенти з міста Макферсон, Канзас, приєднуються до повстання проти програми "Summit" і знеособленого навчання, та отримують право відмовитися від участі» (McPherson KS students join the rebellion vs Summit and de-personalized learning and win the right to opt out) (2019 р.) https://www.studentprivacymatters.org/ kansas- students-join-the-rebellion-vs-summit-and-depersonalized-learning/

Пол Дж. (Paul, J.) (2017 р.) «Розквіт біометрії в освіті» (The Rise of Biometrics in Education) https://www.d2l.com/en-eu/blog/rise-biometrics- education/

Пегг, Макінтайр (Pegg, McIntyre) (2018 р.) The Guardian, https://www.theguardian.com/ society/2018/sep/16/child-abuse-algorithms-from-science-fiction-to-cost-cutting-reality

(дата перегляду – лютий 2020 року)

Пломін Р. (Plomin, R.), Штумм С. (Stumm, S.) (2018 р.) «Нова генетика інтелекту» (The new genetics of intelligence) https://www.nature.com/articles/nrg. 2017.104

Плюм К. (Pluim, C.) та Ґард М. (Gard, M.) (2016 р.) «Грандіозна конвергенція фізичного виховання: Fitnessgram®, великі дані та цифрова комерція здоров'я дітей» (Physical education's grand convergence: Fitnessgram®, big-data and the digital commerce of children's health) https:// www. tandfonline. com/ doi/ abs/ 10.1080/17508487.2016.1194303

Перше рішення Польського Управління із захисту даних та перший штраф згідно із Загальним регламентом про захист даних https://uodo.gov.pl/en/553/1009 на підставі відсутності чесної обробки для суб'єктів даних, посилаючись на несумісні наслідки, а також незаконну обробку персональних даних, зібраних із загальнодоступних джерел, у великих обсягах.

Портер Г. (Porter, G.) (2010 р.) «Мобільність, спостереження і контроль над дітьми та молоддю в повсякденному житті: перспективи країн Африки на південь від Сахари» (Mobility, surveillance and control of children and young people in the everyday:perspectives from sub-Saharan Africa) https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/sub-saharan and https:// www. theimpactinitiative .net/project/impact-mobile-phones- young-peoples-lives-and-life-chances-sub-saharan-africa-three-country

Паулс Дж. (Powles, J.) (2018 р.) Університет Західної Австралії, «Спокуслива диверсія "вирішення" упередженості в штучному інтелекті» (The Seductive Diversion of 'Solving 'Bias in Artificial Intelligence), https://medium.com/s/story/the-seductive-diversion-of-solving-bias-in-artificial-intellige nce-890df5e5ef53

«Privacy International» (2019 р.), Звіт: «Продається ваше психічне здоров'я» (Your Mental Health for Sale) https://privacyinternational.org/ campaigns/your-mental-health-sale

«Privacy International», Звіт — «Як застосунки на Android обмінюються даними з Facebook (навіть якщо у вас немає облікового запису Facebook)» (How Apps on Android Share Data with Facebook (even if you don't have a Facebook account)). (2018 р.) https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf

Закон про захист свобод 2012 року (Англія та Уельс) Захист біометричних даних дітей у школах (глава 2) http://www.legislation.gov.uk/ukpga/2012/9/part/1/chapter/2/enacted

Реган П. (Regan, P) та Стівз В. (Steeves, V.) (2019 р.) «Освіта, конфіденційність і алгоритми великих даних: виключення людей із персоналізованого навчання» (Education, privacy, and big data algorithms: Taking the persons out of personalized learning) https://doi.org/10.5210/fm.v24i11.10094

Рувруа F. (Rouvroy, A.) (2016 р.). «Про дані та людей: Основоположні права і свободи у світі великих даних» (Of Data and Men: Fundamental Rights and Liberties in a World of Big Data) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a6020.

Сабатес Р. (Sabates, R.) та інші (2010 р.) «Кидання школи: шаблони, причини, зміни та політика) «School Drop out: Patterns, Causes, Changes and Policies» https:// unesdoc.unesco.org/ark:/48223/pf0000190771

Савірімуту Дж. (Savirimuthu, J.), (2016 р.) «Загальний регламент ЄС про захист даних Стаття 8: Чи хтось консультувався з дітьми?» (EU General Data Protection Regulation Article 8: Has Anyone Consulted the Kids?) Блог проєкту з медіаполітики «LSE Media Policy Project», Лондонська школа економіки http://blogs.lse.ac.uk/ mediapolicyproject/2016/03/01/eu-general-data-protection-regulation-article-8-has-anyone-consulted- the-kids/ (дата перегляду – серпень 2019 року)

Шуйєр Дж. (Schuijer, J.), (2017 р.) «Транскраніальна електрична стимуляція для поліпшення когнітивних функцій здорових неповнолітніх: складне завдання уряду» (Transcranial Electrical Stimulation to Enhance Cognitive Performance of Healthy Minors: A Complex Governance Challenge) https://www.frontiersin.org/articles/10.3389/fnhum. 2017.00142/full

Селвін Н. (Selwyn, N.), (2019 р.) Університет Монаша, Австралія, «Які допустимі межі шкільних даних? Справа щодо бази даних для шкільної безпеки у Флориді» (What are the acceptable limits of school data? The case of the Florida 'school safety 'database) https://data-smart-schools.net/2019/06/05/what-are-the- acceptable-limits-of-school-data-the-case-of-the-florida-school-safety-database/

Селвін Н. (Selwyn, N.) (2015 р.). «Введення даних: до критичного вивчення цифрових даних і освіти» (Data entry: towards the critical study of digital data and education). Журнал «Learning, Media and Technology», 40(1), 64-82.

Селвін Н. (Selwyn, N.) (2016 р.) «Чи корисні технології для освіти?» (Is Technology Good For Education?) (Polity). Глава 4 «Підвищення рівня обчислюваності освіти» (Making Education More Calculable) (обговорюється «поворот даних» в освіті) / Глава 5 «Підвищення рівня комерційності освіти» (Making Education more Commercial) (обговорюються «Великі технології»).

Сміт С. (Smith. S), (2016 р.) «Тінь розумної машини: чи закінчиться машинне навчання?» (Shadow of the smart machine: Will machine learning end?) https://www.nesta.org.uk/ blog/shadow-smart-machine-will-machine-learning-end (дата перегляду – вересень 2019 року)

Саутгейт (Southgate) та інші, (2019 р.) «Штучний інтелект і новітні технології в школах» (Artificial Intelligence and Emerging Technologies in Schools), на замовлення уряду Австралії https://docs-edu.govcms.gov.au /system/files/doc/other/aiet_final_report_august_2019.pdf

Опитування щодо поглядів батьків на технології та дані у школах Великобританії. Survation (2018 р.) Великобританія https://survation.com/wp-content/uploads/2018/03/Defend-Digital-Me-Final-Tables-1.pdf

Стівз В. (Steeves, V.), Доцент кафедри кримінології факультету соціальних наук. Міждисциплінарна дослідницька лабораторія з прав дитини (IRLRC – The Interdisciplinary Research Laboratory on the Rights of the Child), «Канадська молодь у дротовому світі, Фаза III: Життя онлайн» (Young Canadians in a Wired World, Phase III: Life Online) https://mediasmarts.ca/ycww/life-online

Стоілова М. (Stoilova, M.), Лівінгстон С. (Livingstone, S.) і Нандагірі Р. (Nandagiri, R.), (2019 р.) «Дані і конфіденційність дітей в інтернеті: дорослішання в епоху цифрових технологій» (Children's data and privacy online: Growing up in a digital age), http://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy- online-report-for-web.pdf And what do children ask for? http://www.lse.ac.uk/my-privacy-uk/what-do- children-ask-for

Суджон, З. (Sujon, Z.) (2019 р.) «Підривна гра або платформний колоніалізм? Суперечлива динаміка Google Expeditions і освітньої віртуальної реальності» (Disruptive Play or Platform Colonialism? The Contradictory Dynamics of Google Expeditions and Educational Virtual Reality). Digital Culture and Education, 11 (1). ISSN 1836-8301

Постанова Шведського управління із захисту даних щодо системи розпізнавання обличчя для цілей фіксації відвідуваності в школах, BBC https://www.bbc.co.uk/news/technology-49489154 оригінальна постанова «Викладання як наука про дизайн» (Teaching as a Design Science), Дайана Лорілард (Diana Laurillard), Routledge, 2012 р., стор. 4. (Англійський переклад очікується від DPA)

Тейлор Е. (Taylor, E.) (2015 р.) Обговорення відповідності https://www.youtube .com/watch?v=QHLh485SJXc на конференції CPDP, «Бентам йде до школи: спостереження та конфіденційність учнів у класі» (Bentham goes to school: surveillance and student privacy in the classroom).

Тейлор Е. (Taylor, E.) та Руні Т. (Rooney, T.) (2017 р.) «Майбутнє спостереження: соціальні та етичні наслідки нових технологій для дітей та молоді» (Surveillance Futures: Social and ethical implications of new technologies for children and young people), https://www.taylorfrancis .com/books/e/9781315611402

Такер В. (Tucker, W) та Венс А. (Vance, A.) (2016 р.) «Спостереження в школі: наслідки для рівноправ'я та конфіденційності» (School Surveillance: The Consequences for Equity and Privacy). Звіт лідерів освіти (4), Національна асоціація державних рад з питань освіти (National Association of State Boards of Education), http:// www.nasbe.org/wp-content/uploads/Tucker_Vance-Surveillance-Final.pdf (постійна копія https:// defenddigitalme.com/wp-content/uploads/2019/09/Tucker_Vance-Surveillance-Final.pdf)

Керівні принципи ООН з питань підприємницької діяльності в аспекті прав людини (2011 р.) https://www.ohchr.org/Documents/ Publications/GuidingPrinciplesBusinessHR_EN.p

Університетський коледж Лондона, Центр освітньої неврології (2019 р.) «Майбутнє освіти - це стимулювання мозку» (The future of education is brain stimulation) http:// www.educationalneuroscience.org.uk/resources/neuromyth-or-neurofact/the-future-of-education-is-brain-stimulation/)

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, у присутності «Facebook Ireland Ltd» (Справа C-210/16). http://curia.europa.eu/juris/document/document.jsf?docid=195902&doclang=EN

Комітет з прав дитини КПД ООН, Зауваження загального характеру №16 (2013 р.) про зобов'язання держави щодо впливу підприємницького сектора на права дітей. https://www.unicef.org/csr/css/ CRC_General _Comment_ENGLISH_26112013.pdf

Комітет з прав дитини КПД ООН, Gауваження загального характеру № 1 (2001 р.) про цілі освіти (Стаття 29) https://www.ohchr.org/EN/Issues/Education/Training/Compilation/Pages/a)General Comment No1 The Aims of Education (article29)(2001).aspx

«Низька успішність у галузі освіти» (Underachievement in Education) (2014 р.), Комітет Палати громад з питань освіти http:// defenddigitalme.com/wp-content/uploads/2016/08/Plomin_-December-2013_142.pdf

Міністерство освіти США (Центр технічної допомоги з питань конфіденційності) (2015 р.) «Захист конфіденційності студентів під час користування освітніми послугами в Інтернеті: типові умови надання послуг» (Protecting Student Privacy While Using Online Educational Services: Model Terms of Service), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TOS_Guidance _ Jan%202015_0%20%281%29.pdf

Вацаля (Vatsalya), «Youth Ki Awaaz», (2019 р.), «Відеоспостереження у школах Делі» (CCTV in Delhi schools) https://www.youthkiawaaz.com/2019/08/ cctv- surveillance-in-schools-boon-or-bane/

Веале М. (Veale, M.), Біннс Р. (Binns R.) (2017 р.). «Більш справедливе машинне навчання в реальному світі: зниження дискримінації без збору конфіденційних даних» (Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data). Big Data & Society, 4(2):2053951717743530, https://doi.org/ 10.1177/2053951717743530.

Веале М. (Veale, M.) (2019 р.). «Критичний погляд на політичні рекомендації»Експертної робочої групи високого рівня ЄС з питань штучного інтелекту. (A Critical Take on the Policy Recommendations of the EU High-Level Expert Group on Artificial Intelligence.) https://doi.org/ 10.31228/osf.io/dvx4f

«Хто та що знає про мене» (Who Knows What About Me) (2017 р.) Уповноважений у справах дітей, Велика Британія https://www.childrenscommissioner.gov.uk/publication/who-knows-what-about-me/

Вільямсон Б. (Williamson, B.) (2017 р.) Единбурзький університет, Центр досліджень в області цифрової освіти, та Единбурзький інститут майбутнього, «Великі дані в освіті: цифрове майбутнє навчання, політика та практика» (Big Data in Education, the digital future of learning, policy and practice) (Sage)

Вільямсон Б. (Williamson, B.) (2018 р.) «Дані мозку: сканування, скобління та ліплення пластичного мозку, що навчається, за допомогою нейротехнологій» (Brain Data: Scanning, Scraping and Sculpting the Plastic Learning Brain Through Neurotechnology) https://link.springer.com/article /10.100 7%2Fs42438-018-0008-5

Вільямсон Б. (Williamson, B.) (2018 р.) «Постгеномна наука, великі дані та біосоціальна освіта» (Postgenomic science, big data, and biosocial education) (on_education) https:// www.oneducation.net/no-02-september-2018/postgenomic-science/

Світовий економічний форум (WEF) (2016 р.) «Нове бачення освіти: сприяння соціальному та емоційному навчанню за допомогою технологій» (New Vision for Education: Fostering Social and Emotional Learning through Technology) http://www3.weforum.org/docs/WEF_New_Vision_for_ Education.pdf

Зейде Е. (Zeide, E.) (2014 р.) «Загальновідомий довічний запис» (The Proverbial Permanent Record), Інститут інформаційного права Нью-Йоркського університету http://papers.ssrn.com/sol3 /papers.cfm? abstract_ id = 2507326 https://defenddigitalme.com/wp- content/uploads /2019/09/SSRN -id2507326.pdf

Чжао (Zhao) та інші (2019 р.) «Я вигадав дурне ім'я»: розуміння того, як діти сприймають ризики конфіденційності в інтернеті». ('I make up a silly name': Understanding Children's Perception of Privacy Risks Online.) CHI'2019. https://arxiv.org/abs/1901.10245 (дата перегляду – вересень 2019 року)

Чжао Дж. (Zhao J.) (2018 р.) «Чи отримують діти достатню підтримку від своїх батьків щодо ризиків, пов'язаних з конфіденційністю онлайн, та хто підтримує самих батьків?» (Are Children Well−Supported by Their Parents Concerning Online Privacy Risks, and Who Supports the Parents?). https://arxiv.org/abs/1809.10944 (дата перегляду – вересень 2019 року)

Циммер К. (Zimmer, C.) (2018 р.) The Atlantic, «Тести на генетичний інтелект майже не приносять користі» (Genetic Intelligence Tests Are Next to Worthless) https://www.theatlantic.com/science /archive/2018/05/genetic-intelligence-tests-are-next-to-worthless/561392/