Переклад[1]
Спільної заяви про цифрове відстеження контактів

Голови Комітету «Конвенція 108»[2] Алессандри П'єруччі і
Комісара Ради Європи з захисту даних
Жана-Філіпа Вальтера

Страсбург, 28 квітня 2020 р.

Минув місяць після нашої першої Спільної заяви про право на захист даних в умовах пандемії COVID-19. Країни і народи усього світу продовжують невтомно вживати всіх зусиль для запобігання подальшому поширенню цього вірусу.

З самого початку пандемії і до цього часу уряди і зацікавлені сторони, що беруть участь у боротьбі з вірусом, у тому числі, науково-дослідна спільнота, спираються у протидії цій новітній загрозі на аналітику даних і цифрові технології.

Нагадуємо, що стандарти захисту даних, закріплені в "Конвенції 108" і в її модернізованій версії - "Конвенції 108+", повною мірою сумісні та узгоджуються з іншими основоположними правами та відповідними суспільними інтересами, як-от охорона громадського здоров'я, і відповідно, наразі вкрай важливим є забезпечення реалізації необхідних гарантій захисту даних під час вжиття надзвичайних заходів щодо охорони громадського здоров'я.

У сфері застосування даних і технологій мобільного зв'язку в боротьбі з COVID-19 вживаються або іншим чином пропонуються конкретні заходи, зокрема застосування даних про місцезнаходження мобільних пристроїв для аналізу пересування населення або забезпечення дотримання заходів з ізоляції, застосування пристроїв як цифрового доказу наявності імунітету, для виявлення симптомів, самотестування або, нарешті, цифрового відстеження контактів інфікованих осіб.

Усі ці більшою чи меншою мірою інноваційні інструменти залежать від людей,

[1] Переклад Спільної Заяви здійснено в рамках проєкту «Європейський Союз та Рада Європи працюють разом задля посилення операційної спроможності Омбудсмана у захисті прав людини»
[2] Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних

які володіють відповідними мобільними пристроями і мають їх при собі. Наприклад, подібні підходи не розповсюджуватимуться на людей, в яких немає придатних для цього мобільних пристроїв. Крім того, ці інструменти, робота яких базується на обробці персональних даних, впливають на приватність і захист даних, інші основоположні права і свободи людини. Отже, вкрай важливо забезпечити, щоб ці заходи і пов'язана з ними обробка даних були необхідними та пропорційними відносно легітимної мети, щоб вони на всіх етапах відображали справедливий баланс усіх відповідних інтересів, а також прав і свобод, які піддаються ризику, як це передбачено Конвенцією про захист прав людини і основоположних свобод (стаття 8) та "Конвенцією 108+" (статті 5 і 11).

Зокрема, говорячи про відстеження контактів (і попередження), слід, насамперед, пам'ятати, що процес моніторингу завжди використовувався – у ручному режимі – в епідемічному спостереженні з метою скорочення масштабів захворювань, встановлення осіб, які могли вступити в контакт із зараженою особою, для попередження їх, за потреби, та надання їм можливості отримати необхідну допомогу та самоізолюватися для запобігання подальшому розповсюдженню захворювання.

Багато хто наразі розглядає мобільні застосунки як додатковий засіб реагування на потребу в швидкому здійсненні такого моніторингу контактів. Дійсно, мобільні рішення, які надають можливість автоматичного виявлення контактів, заощадять цінні години роботи співробітників органів охорони здоров'я, які відслідковують ланцюг інфікування, вони здатні заповнювати вагомі прогалини, на що не здатна людська пам'ять, і можуть робити це з оперативністю, співставною зі швидкістю розповсюдження вірусу. І хоча технологічні інструменти можуть відіграти важливу роль у подоланні теперішнього виклику, проте, перед тим, як системно і некритично довіритися технологіям, не проаналізувавши їхню ефективність і співмірність, ми повинні задати собі найперше і ключове питання: чи є ці застосунки дійсно вирішенням проблеми? Чи варто, зважаючи на відсутність доказів їхньої ефективності, наражатися заради обіцянок на передбачувані суспільні і правові ризики? А там, де уряди вирішують вдатися у боротьбі з пандемією COVID-19 до цифрового відстеження контактів, якими повинні бути правові і технічні гарантії для пом'якшення наявних ризиків?

I. Ефективність

Як це вже було відзначено у першій спільній заяві, "широкомасштабну обробку персональних даних можна здійснювати лише у разі, якщо, відповідно до наукових доказів, потенційна користь для охорони громадського здоров'я від подібного цифрового епідемічного спостереження, зокрема, відстеження контактів, а також його точність, перевищують користь від альтернативних і тих, що передбачають менше втручання, рішень".

Ефективність цифрового відстеження контактів залежить від багатьох

пов'язаних між собою чинників:

- комплексної національної епідеміологічної стратегії, яка поєднує дієву підтримку системи охорони громадського здоров'я, відстеженням контактів в ручному режимі та особливу увагу масштабного тестування;

- обраної моделі (застосована технологія, обрана архітектура, визначення "близькості" пристроїв у термінах як відстані, так і часу тощо), а також

- широкого доступу до мобільних пристроїв і мобільного зв'язку (що може також потребувати окремих технічних функцій, наприклад, Bluetooth з низьким енергоспоживанням). Водночас, слід із жалем визнати, що значна кількість населення не має змоги придбати їх або користуватися ними, зокрема групи високого ризику, як-от особи похилого віку.

Там, де органи влади приймають рішення задіяти цифрове відстеження контактів, наступні розділи мають слугувати настановою для розробки і застосування таких систем[3] разом з ухваленням відповідної нормативно-правової бази, яка б регулювала ці системи.

II. Довіра і добровільність

Прийнятність системи цифрового відстеження контактів чітко залежить від того, якою мірою та чи інша система викликає і забезпечує довіру до себе. Оскільки суспільна довіра є істотним чинником впровадження тієї чи іншої системи, важливо наголосити на тому, що таку довіру можна значно посилити шляхом інтеграції функцій, що підвищують конфіденційність, а також прозорого інформування користувачів, зокрема, про функціонування системи, її мету, а також інформацію, що обробляється.

Отже, впровадження системи, яка викликає довіру і яку не нав'язують людям, а натомість застосовують на добровільній основі, полегшить її широке сприйняття. Це також означає, що неприєднання до цієї системи не матиме негативних наслідків.

Добровільність не означає, що правовою основою обробки персональних даних має обов'язково бути особиста згода. "Конвенція 108+" дозволяє обробку даних, виходячи із суспільного інтересу, у тому числі, й інтересів охорони громадського здоров'я, що передбачено законодавством. Тому

3 "Керівні принципи з геолокації та інших інструментів відстеження в умовах спалаху COVID-19", ухвалені Європейською радою із захисту даних Європейського Союзу 21 квітня 2020 р., надають так само важливі настанови з цих питань. Докладніша інформація міститься за веб-адресою: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

національне законодавство, що заохочує справжню добровільну згоду на застосування таких систем, може становити належну правову основу для подібної обробки даних, за умови наявності необхідних гарантій.

III. Аналіз впливу і захист даних за призначенням

З урахуванням імовірного впливу систем цифрового відстеження контактів на права й основоположні свободи осіб, розробка таких систем повинна ґрунтуватися на попередньому аналізі цього ймовірного впливу до їх впровадження.

Ці системи повинні розроблятися таким чином, щоб запобігти або мінімізувати ризики втручання у права й основоположні свободи осіб, насамперед забезпечити, щоб дані про місцезнаходження осіб не використовувались, не було можливості прямої ідентифікації та деанонімізації.

IV. Конкретизація мети

Метою системи цифрового відстеження контактів з COVID-19 є визначення осіб, які мають потенційний ризик зараження вірусом. Це суворо виключає подальшу обробку даних у будь-яких не пов'язаних із тим цілях, наприклад, комерційних або правоохоронних.

Подальша обробка даних в цілях епідеміологічних досліджень або в статистичних цілях обов'язково вимагатиме чіткої згоди особи.

V. Дані: чутливість, якість, мінімізація

Дані, що стосуються здоров'я, є спеціальною категорією даних, які можуть оброблятися лише за наявності відповідних гарантій, закріплених у статті 6 "Конвенції 108+", які доповнюють решту вимог до захисту даних.

З урахуванням особливого характеру даних про місцезнаходження, а також того факту, що близькість осіб може бути встановлена без фіксації їхнього місцезнаходження, цифрове відстеження контактів має здійснюватися на основі записів про зв'язок між пристроями, а не на основі даних про місцезнаходження (наприклад, даних, згенерованих GPS).

Вкрай важливо забезпечити якість і точність даних, оскільки особи, ідентифіковані як потенційні контакти інфікованої особи, можуть мати від того серйозні наслідки (самоізоляція, тестування).

Дані, що обробляються в цілях цифрового відстеження контактів, мають бути зведені до мінімуму. Не можуть збиратися дані, що не пов’язані і непотрібні для цілей відстеження.

VI. Автоматизоване прийняття рішень

Навіть за поточної ситуації люди зберігають право не бути залежними від рішень, які їх суттєво зачіпають і при цьому ґрунтуються виключно на автоматичній обробці даних, без урахування їхньої думки. Зрозуміло, що наслідки у вигляді самоізоляції та тестування можуть суттєво зачіпати людей.

Тому користувачі цифрових систем відстеження не повинні зазнавати наслідків, не маючи чітких засобів оскарження таких наслідків, особливо з урахуванням неточностей та викривлень, які можливі у таких системах.

VII. Знеособлення

Не повинно бути прямої ідентифікації користувачів цифрової системи відстеження даних. Такі системи повинні використовувати унікальні і псевдонімізовані ідентифікатори, які генеруються системою і є притаманними виключно їй. Ці ідентифікатори повинні постійно оновлюватися і бути криптографічно стійкими.

VIII. Безпека

Системи цифрового відстеження даних повинні включати найновітніші технології шифрування, безпеку комунікацій, практики безпечної розробки та автентифікацію користувача для попередження таких ризиків як доступ до даних системи цифрового відстеження контактів, їх модифікація або розголошення.

IX. Архітектура

Системи цифрового відстеження контактів мають базуватися на архітектурі, що максимально спирається на обробку і збереження даних на пристроях індивідуальних користувачів.

Існує кілька моделей централізованих, частково централізованих або децентралізованих архітектур, але жодна з них не запобігає повною мірою вразливостям і ризику деанонімізації.

X. Сумісність

Оскільки пандемія COVID-19 не зважає на кордони, задля міжнародного обміну наявною інформацією потрібно забезпечити сумісність систем, що стає можливим, за умови наявності необхідних гарантій, включаючи належні підстави для передачі даних, суворі заходи безпеки, а також засоби забезпечення точності вхідних та вихідних даних.

XI. Прозорість

У зв'язку з інтрузивним характером систем цифрового відстеження контактів, наполегливо рекомендується забезпечити повну прозорість шляхом

застосування програмного забезпечення з відкритим початковим кодом, що дасть можливість будь-якій зацікавленій особі переглядати код (та, можливо, покращувати його).
Інформація для користувачів має викладатися чіткою та простою мовою.

Особи мають право на одержання інформації про причини обробки даних у випадках, коли до них застосовуються її результати, як-от у разі цифрового відстеження контактів. Інформація про загальні принципи, за якими працює та чи інша система цифрового відстеження контактів, має бути повністю оприлюднена перед початком і протягом її застосування.

XII. Тимчасовість

Дані, що використовуються для цифрового відстеження контактів, повинні зберігатися лише протягом періоду боротьби з пандемією COVID-19. Мають бути визначені часові обмеження для зберігання даних з урахуванням їх епідеміологічної значущості (наприклад, інкубаційного періоду вірусу).

Після закінчення цього попередньо визначеного періоду усі персональні дані мають бути знищені і забезпечено підтримку технічних заходів, що уможливлюють автоматичну деактивацію застосунку і знищення даних.

XIII. Нагляд і перевірка

Системи цифрового відстеження контактів мають підлягати незалежному та ефективному контролю і перевіркам з метою забезпечення дотримання права на недоторканність приватного життя і захист персональних даних. Органи влади у сфері захисту персональних даних мають із самого початку залучатися до розробки таких систем, застосовувати повноваження щодо втручання і розслідування задля забезпечення дотримання вимог захисту персональних даних.

Пандемія COVID-19 породжує безпрецедентні спільні виклики, які вимагають від нас як найбільшої рішучості, так і обережності. Наше майбутнє залежить від політичного вибору, суспільної підтримки і нашої особистої рішучості. Попри свою невідкладність, цифрове відстеження контактів ставить перед нами нові запитання, якими не можна нехтувати перед прийняттям рішень про реалізацію подібних заходів, що охоплюють усе населення. Окрім міркувань про недоторканність приватного життя і захист персональних даних, підходи до цифрового відстеження контактів породжують питання нерівності і дискримінації, які теж мають бути розглянуті.

Алессандра П'єруччі і Жан-Філіп Вальтер