ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ І 5G - ЧИ МОЖЛИВЕ СПІВІСНУВАННЯ

Андрій Ніколаєв

експерт із захисту персональних даних та приватності, засновник юридичної компанії Privacy Advisers

грудень 2021

Зміст

Коротке резюме 2
Вступне слово 4
Принципи захисту персональних даних 7
Загальний огляд еволюції технологій мобільного зв'язку 11
П'яте покоління мобільного зв'язку (5G) та його особливості 12
Ризики приватності та захисту персональних 15
Висновки та шляхи мінімізації ризиків 18

Коротке резюме

Метою даного дослідження є аналіз ризиків, які несе для захисту персональних даних впровадження п'ятого покоління мобільного зв'язку, відомого як 5G, а також технології та сервісів, які на ньому побудовані. Ризики розглядаються в контексті дотримання принципів захисту персональних даних під час використання цієї технології.

П'яте покоління мобільного зв'язку несе більше інновацій ніж усі попередні разом узяті. І це стосується не лише технічних характеристик, але й самої побудови системи зв'язку.

Найбільш істотними відмінностями та інноваціями 5G є:

- значно більша швидкість передачі інформації;
- дуже мала затримка передачі інформації;
- велика пропускна спроможність мережі;
- значно менший радіус покриття базових станцій та низька здатність високочастотних хвиль 5G оминати перешкоди та проникати через стіни будівель;
- віртуалізація мережевих функцій (NFV) - мережеві функції реалізуються завдяки програмному забезпеченню, а не апаратно;
- програмно-визначена мережа (SDN) - керування мережею здійснюється програмними засобами;
- Network Slicing (NS) - технологія, яка дозволяє мобільним операторам розгортати логічно ізольовані мережі, кожна з яких може бути виділена під певні потреби;
- Device-to-device (D2D) - технологія, яка дозволяє пристроям, що знаходяться недалеко один від одного, безпосередньо обмінюватися даними. Процес обміну здійснюватиметься без участі мережі оператора зв'язку.
- Технологічні особливості п'ятого покоління мобільного зв'язку можуть породжувати нові ризики для приватності та захисту персональних даних.

Серед таких ризиків можна назвати наступні:

- Підвищена точність визначення місцезнаходження абонента (до 1 метра);
- Зростаючі можливості для профілювання та застосування автоматизованих рішень;

- Розмивання відповідальності за безпеку персональних даних між зростаючою кількість різних учасників мережі;
- Зменшення рівня прозорості обробки персональних даних та ускладнення реалізації права на інформацію щодо такої обробки;
- Втрата користувачем контролю над своїми даними;
- Збільшення поверхні кібератак (cyber-attacks surface).

З метою мінімізації ризиків та належного реагування на нововиявлені ризики, слід сконцентрувати зусилля на розвитку таких напрямків:

- Сертифікація обладнання та програмного забезпечення і стандартизація електрозв'язку;
- Оновлення законодавства про захист персональних даних, як один із способів забезпечити, щоб технології залишалися безпечними та дружніми для людини. (*Важливим кроком для нашої держави є прийняття нової редакції Закону України "Про захист персональних даних", яка становить вимоги до рівня захисту персональних даних не нижчі ніж це передбачено у GDPR*).
- Державний контроль за дотриманням вимог стандартів електрозв'язку усіма гравцями ринку. Проте, при здійснені заходів контролю критично важливо забезпечити технологічну нейтральність та конкурентне середовище.
- Підвищення правової культури як надавачів послуг (контролерів і операторів персональних даних) так і користувачів послуг (суб'єктів персональних даних.

Вступне слово

Метою даного дослідження є аналіз ризиків, які несе для захисту персональних даних впровадження п'ятого покоління мобільного зв'язку, відомого як 5G, а також технології та сервісів, які на ньому побудовані. Ризики розглядаються в контексті дотримання принципів захисту персональних даних під час використання цієї технології.

Перш ніж перейти до аналізу захисту персональних даних, потрібно чітко окреслити саме поняття "персональних даних", які персональні дані можуть оброблятися з використанням технології зв'язку 5G, та що таке "обробка персональних даних".

Відповідно до визначення, яке міститься в Законі України "Про захист персональних даних"[1], а також у Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних[2] (далі - Конвенція 108), персональні дані - це відомості або сукупність відомостей про фізичну особу, яка ідентифікована, або може бути ідентифікована.

Проаналізувавши таке визначення персональних даних в рамках зазначеної сфери дослідження, можна дійти наступних висновків.

Перш за все, персональні дані - це інформація.

По-друге, персональні дані - це інформація / відомості про фізичних осіб.

В контексті використанням технології зв'язку 5G **це можуть бути відомості про**:

- абонентів телекомунікаційних мереж;
- користувачів сервісів, які підключені до телекомунікаційної мережі або побудовані з використанням технології 5G;
- інших осіб, які не є ні користувачами комунікаційної мережі, ні користувачами сервісів, але відомості про яких передаються телекомунікаційною мережею сервісами тощо.

По-третє, персональні дані - це можуть бути відомості про фізичних осіб, яких уже ідентифіковано. Тобто, **суб'єкти, які володіють або розпоряджаються персональними даними**[3] (володільці або розпорядники / контролери або оператори), ідентифікували фізичних осіб раніше за допомогою додаткової інформації та/або засобів і знають, саме кого

[1] https://zakon.rada.gov.ua/laws/show/2297-17#Text
[2] https://zakon.rada.gov.ua/laws/show/994_326#Text
[3] У чинному Законі України "Про захист персональних даних" вживаються терміни "володілець" та "розпорядник". Водночас, у GDPR це "контролер" та "процессор". А у проєкті нової редакції Закону України "Про захист персональних даних" запропоновано терміни "контролер" та "оператор".

стосується ця інформація (наприклад, відомості про контрактних абонентів мобільного зв'язку тощо).

По-четверте, персональні дані - це можуть бути відомості про фізичних осіб, які можуть бути ідентифіковані. Тобто в певний конкретний момент, фізичних осіб, яких стосується інформація ще не ідентифікували, проте існує об'єктивна можливість ідентифікації таких фізичних осіб у майбутньому.

Наприклад, це можуть бути певні відомості про абонента передплаченого зв'язку, яких на даний момент часу ще не можна ідентифікувати, проте, через певний час користування послугами про такого абонента, накопичується додаткова інформація, яка дасть змогу його ідентифікувати.

Важливо пам'ятати, що в контексті використання послуг зв'язку (зокрема доступу до мережі Інтернет), для ідентифікації особи не важливо знати її прізвище, ім'я, по-батькові, отримати номери чи копії її документів тощо. Для ідентифікації такої особи буде достатньо мати можливість, за тими чи іншими ознаками, відрізнити (відокремити) її серед інших осіб. *Наприклад, можливість відрізнити одного абонента від іншого, одного користувача сервісу від іншого.*

Визначення обробки персональних даних можна знайти у статті 2 Закону України "Про захист персональних даних", **обробка персональних даних - будь-яка дія або сукупність дій**, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем.

Більш ґрунтовне та структуроване визначення терміну обробка персональних даних можна знайти у Регламенті Європейського парламенту та 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[4] (далі - Загальний регламент ЄС про захист даних або GDPR), який, на сьогодні, вважається "золотим стандартом" захисту персональних даних. Відповідно до статті 4 GDPR, **обробка - це будь-яка дія (операція) або сукупність дій (операцій), що**

[4] Офіційний переклад: https://zakon.rada.gov.ua/laws/show/984_008-16#Text; Оригінал, англійською мовою: https://eur-lex.europa.eu/eli/reg/2016/679/oj

здійснюються з персональними даними з використанням засобів автоматизації або без використання таких засобів, включаючи збір, запис, організацію, структурування, накопичення, зберігання, адаптацію або зміну, завантаження, перегляд, використання, розкриття через передачу, розповсюдження або інший вид надання доступу, зіставлення або комбінування, скорочення, видалення або знищення.

Узагальнюючи наведені вище визначення можна дійти висновків, що:

- **обробка персональних даних - це будь-яка дія (операція) або сукупність дій (операцій), що здійснюються з персональними даними**;
- **перелік дій (операцій) та їх різновидів не є виключним.**

Принципи захисту персональних даних

Цілком природно, що зі змінами технологій виникають нові ризики. В тому числі ризики, пов'язані із конфіденційністю і захистом персональних даних.

Для того, щоб мати можливість оцінити вплив будь-якої технології на захист персональних даних - доцільно ознайомитися з принципами захисту персональних даних, які є наріжним комнем інституту захисту персональних даних.

В Україні ці принципи частково відображені у статті 6 Закону України "Про захист персональних даних". У Європейському Союзі ці принципи встановлені статтею 5 GDPR. Спроба у повній мірі імплементувати європейські принципи в законодавство України зроблена у проєкті нової редакції Закону України "Про захист персональних даних", зареєстрованому у Верховній Раді України за номером 5628 у липні 2021 року.

Загально прийнято виділяти 7 таких принципів:

Принцип перший: "lawfulness, fairness and transparency".

Персональні дані повинні оброблятися у законний, правомірний і прозорий спосіб відносно до суб'єкта даних[5] (***"законність, правомірність і прозорість"***).

Будь-яка обробка персональних даних має бути законною та справедливою. До фізичної особи має бути прозоро донесено те, що її персональні дані збираються, використовуються, переглядаються або іншим чином обробляються, а також те, в якому обсязі персональні дані обробляються або та будуть оброблятися.

Принцип прозорості вимагає, щоб будь-яка інформація та повідомлення щодо обробки персональних даних були легкодоступними і зрозумілими, викладені з використанням чітких і простих формулювань.

Цей принцип, зокрема, передбачає необхідність інформування суб'єктів персональних даних про особу контролера, про цілі (мету) обробки персональних даних, та додаткове інформування для забезпечення справедливої та прозорої обробки в частині, що стосується відповідних фізичних осіб та їхнього права на отримання підтвердження, та відомостей про ті персональні дані, які їх стосуються та обробляються.

[5] Субєкт персональних даних - фізична особа (людина) чиї персональні дані обробляються.

Фізичні особи повинні бути обізнані про ризики, правила, засоби захисту та права щодо обробки персональних даних, про те, як реалізувати свої права у зв'язку з такою обробкою.

Принцип другий: "purpose limitation".

Персональні дані можуть збиратися лише для конкретних, чітких і законних цілей, і не повинні оброблятися в подальшому у спосіб, що є несумісним із визначеними цілями (***"обмеження обробки метою"***);

Це означає:

- що мета обробки обов'язково має бути чітко визначеною до початку обробки;
- необхідно переконатися, що дії, які планується здійснювати з персональними даними є цілком законними;
- мета має бути задокументована, тобто прописана у відповідних документах, які регламентують обробку (порядок обробки, політика конфіденційності тощо).

Персональні дані повинні оброблятися лише з тією метою, з якою вони були зібрані.

Можна обробляти персональні дані з іншою метою тільки якщо:

- така мета сумісна з початковою метою або
- отримано згоду суб'єкта на обробку з новою метою або
- обробка необхідна для виконання зобов'язання встановленого законом або
- обробка здійснюється для реалізації повноважень встановлених законом.

Тобто, для обробки з новою метою повинна бути окрема підстава обробки.

Принцип третій: "data minimisation".

Персональні дані повинні бути адекватними, відповідними та ненадмірними, та обмежуватися тим, що є необхідним для цілей, з якими вони обробляються (***"мінімізація персональних даних"***).

- Дані є адекватними, якщо вони є достатніми для досягнення мети обробки.
- Дані є відповідними, якщо вони мають раціональний зв'язок із метою обробки та сприяють її досягненню.
- Дані є ненадмірними, якщо їх обсяг не більший, ніж це необхідно для досягнення мети обробки. Не можна збирати дані "про всяк випадок".

Тобто, дозволяється збирати та обробляти мінімальну кількість та обсяг персональних даних, які є достатніми для досягнення мети.

Якщо можна досягти цілей без обробки персональних даних - слід утриматися від обробки.

Принцип четвертий: "accuracy".

Персональні дані мають бути точними, достовірними та оновлюватися, якщо це необхідно для мети їх обробки ("***точність"***).

Необхідно вживати всіх раціональних заходів для того, щоб забезпечити точність персональних даних, які обробляються, а також усіх відповідних заходів для того, щоб неточні персональні дані було негайно видалено або виправлено.

Принцип п'ятий: "storage limitation"

Персональні дані не повинні зберігатися довше ніж вони потрібні для цілей, для яких ці дані обробляються (***"обмеження строків зберігання"***).

Після того, як мета була досягнута, персональні дані повинні бути знищені, або знеособлені. Знеособлені персональні дані - це дані, зі складу яких вилучили усі відомості, та які вже не дають змогу будь-яким чином ідентифікувати конкретну особу-суб'єкта персональних даних.

Персональні дані можуть зберігатися протягом більш тривалого часу винятково для досягнення цілей суспільних інтересів, наукового чи історичного дослідження або статистичних цілей за умов вжиття відповідних технічних і організаційних заходів, передбачених законодавством, для гарантування прав і свобод суб'єкта даних.

Щоб гарантувати, що персональні дані не зберігатимуться довше, ніж це необхідно, контролер повинен встановити терміни, після яких персональні видаляються або переглядаються.

Принцип шостий: "integrity and confidentiality"

Персональні дані повинні оброблятися таким чином, щоб забезпечити їх безпеку ("цілісність та конфіденційність").

Цей принцип включає захист від несанкціонованої або незаконної обробки (в тому числі захист від витоку даних), від випадкових або зловмисних втрат даних, їх знищення або пошкодження.

Персональні дані повинні оброблятися таким чином, щоб забезпечити належний рівень безпеки та конфіденційності цих персональних даних, у тому числі для запобігання несанкціонованому доступу до персональних даних або несанкціонованого використання персональних даних та обладнання, що використовується для обробки.

Володільці та розпорядники зобов'язані вживати технічні та організаційні заходи безпеки, на рівні, що відповідає законодавчим вимогам.

Принцип сьомий: "accountability".

Володілець (контролер) несе відповідальність за дотримання принципів обробки персональних даних та має бути здатним це довести (***"підзвітність"***).

Обов'язок доведення дотримання цих принципів покладається на володільця. Володілець зобов'язаний вжити заходів, які забезпечують можливість підтвердження дотримання ним принципів обробки персональних даних.

Наведені вище принципи становлять фундаментальну структуру захисту персональних даних, на якій базуються всі інші вимоги.

Загальний огляд еволюції технологій мобільного зв'язку

Технологію мобільного зв'язку прийнято поділяти на покоління. Кожне покоління відкривало нові можливості та новий функціонал. Проте, нові можливості можуть нести й нові ризики.

Перше покоління 1G (стандарти AMPS, TACS, ETACS, NMT, швидкість 1,9 кБіт/с) - з'явилося у 1980-х роках та передбачало аналогову передачу інформації. Головною функцією була можливість здійснювати дзвінки (голосові виклики).

Друге покоління 2G (стандарти GSM, TDMA, CDMA, швидкість до 14,4 кБіт/с) - з'явилося на початку 1990-х та, на відміну від попереднього покоління, передача інформації здійснювалася у цифровому вигляді. Зросла швидкість передачі даних, покращилася якість голосових викликів та з'явилася можливість відправки текстових повідомлень (SMS). З'явилося шифрування даних при їх передачі, що позитивно вплинуло на право користувачів на таємницю телефонних розмов та на реалізацію права на приватність.

Перехідне покоління 2,5G (стандарти GPRS, EDGE, швидкість до 384 кБіт/с) - на цьому етапі у користувачів мобільного зв'язку, вперше, з'явилася можливість постійного підключення до мережі Інтернет.

Третє покоління 3G (стандарти WCDMA, CDMA2000, UMTS, швидкість до 3,6 Мбіт/с) - з'явилося на початку 2000-х. З'явилася можливість влаштовувати відеоконференції, переглядати відео та мультимедіа контент. Також покращився захист від обривів зв'язку підчас переміщення абонента. Коли абонент віддалявся від однієї базової станції та наближався до іншої, наступна базова станція “підхоплювала” підключення, через базову станцію, що віддалялася, потік трафіку поступово зменшувався, а через базову станцію, що наближалася - поступово збільшувався. Водночас, така технологія покращила й можливість більш точно визначати місцезнаходження абонента, що має вплив на приватність.

Четверте покоління 4G (стандарти LTE и WiMAX, швидкість до 100 Мбіт/с - для рухомих абонентів та до 1 Гбіт/с - для стаціонарних абонентів) - з'явилося на початку 2010-х. Основна відмінність четвертого покоління полягає у тому, що воно повністю побудоване на протоколах пакетної передачі даних.

З кожним новим поколінням мобільного зв'язку, розширенням можливостей та функціоналу зростала й кількість користувачів, що призводило до збільшення масштабів можливих загроз.

П'яте покоління мобільного зв'язку (5G) та його особливості

П'яте покоління мобільного зв'язку несе більше інновацій ніж усі попередні разом узяті. І це стосується не лише технічних характеристик але й самої побудови системи зв'язку.

Найбільш очевидними відмінностями 5G є:

- швидкість передачі інформації;
- затримка передачі інформації;
- пропускна здатність мережі;
- радіус покриття базових станцій.

Швидкість

Найчастіше, для користувачів саме параметр швидкості є головною відмінністю між поколіннями мобільного зв'язку. Проте, п'яте покоління неоднорідне. Виділяють:

Низькочастотний 5G, який використовує частоти 600-850 МГц. Тобто, діапазон частот наближений до 4G і, як наслідок, практично ідентичний радіус розповсюдження сигналу. Швидкість передачі даних складає близько 50-250 Мбіт/с.

Середньо частотний 5G, використовує частоти в діапазоні 2.5-3.7 ГГц і забезпечує можливість передачі даних на швидкості 100-900 Мбіт/с.

Високочастотний 5G, який найбільш відповідає очікуванням від п'ятого покоління, використовує частоти в діапазоні 25-39 ГГц та забезпечує можливість передачі інформації на гігабітних швидкостях.

Затримка передачі інформації

Затримка – це проміжок часу, необхідний для переміщення пакету інформації між двома точками (пристроями). Затримка присутня під час будь-якої передачі даних. Затримка в мережах 4G становить близько 50 мілі секунд (мс), а в мережах 5G очікується скорочення цього показника до 1 мс.

Зменшення затримки має вирішальне значення для цілого ряду сервісів, наприклад хмарних обчислень чи віддаленого проведення медичних операцій, управління дорожнім рухом та самокерованими автомобілями. Очікується, що такі автомобілі зможуть управлятися хмарним штучним інтелектом, який завдяки мережі 5G зможе в режимі реального часу отримувати відомості про зміни дорожньої обстановки та приймати навігаційні рішення щодо керування автомобілем. **Якщо більшість автомобілів на дорозі будуть керовані одним хмарним штучним інтелектом чи принаймні оперативно обмінювати**

навігаційною інформацією - це дозволить звести ДТП до мінімума та забути про затори.

Пропускна здатність

Пропускна здатність характеризує яку кількість інформації може бути передано за допомогою бездротової технології в мережі.

Очікується, що мережі 5G також матимуть значно більшу пропускну здатність або ємність, ніж мережі 4G. Частково це пов'язано з тим, що технологія 5G дозволить ефективніше використовувати доступний частотний спектр. 4G використовує вузьку частину доступного спектру від 600 МГц до 2,5 ГГц, при цьому спектр частот, що використовуються для 5G, розділений на три різні діапазони. Кожен діапазон має власну смугу частот і швидкість, тому різнитимуться й варіанти їх використання додатками, споживачами, підприємствами і галузями промисловості. Це означає, що пропускна здатність мереж 5G значно вища за пропускну здатність мереж 4G.

Завдяки цьому, 5G може підтримувати підключення набагато більшої кількості пристроїв одночасно.

Радіус покриття базових станцій

Чим вища частота сигналу - тим менший радіус охоплення базової станції. Радіус охоплення базових станцій високочастотного 5G, який працює в частотному діапазоні 25-39 ГГц, не перевищує декількох сотень метрів. Крім того, такі високі частоти погано проникають через перешкоди: дерева, стіни будівель. У зв'язку з чим, виникає необхідність щільного розміщення базових станцій, з меншими відстанями між ними, а також їх розміщення всередині будівель. Така щільність мережі призведе до можливості більш точного визначення місцезнаходження користувацького обладнання, орієнтовно до 1 метра. Для порівняння, точність визначення місцезнаходження з використанням технології GPS - до 20 метрів.

Очікувано, що значне збільшення точності гелокації призведе до появи нових сервісів, заснованих на ній.

Одна із найбільших інновацій 5G полягає у тому, що більше не буде використовуватися спеціалізоване телекомунікаційне обладнання - зв'язок буде забезпечуватися звичайним обладнанням, яке використовується для розгортання мережі Інтернет.

Ці зміни мають значний вплив на розвиток та побудову мережі.

Серед інновацій, які стосуються побудови самої мережі варто виділити наступні:

- віртуалізація мережевих функцій (NFV);
- програмно-визначена мережа (SDN);
- Network Slicing (NS);
- D2D (Device-to-device).

Віртуалізація мережевих функцій (Network Functions Virtualization / NFV)

Передбачає новий спосіб створення, розгортання та управління мережевими службами за допомогою віртуалізації кожної функції, що надається мережею. Якщо в існуючих мережах для реалізації кожної мережевої функції необхідно окреме обладнання, то завдяки віртуалізації нові функції можна розгортати на уже наявному обладнанні, завдяки програмному забезпеченню. Це дозволяє значно швидше додавати нові мережеві функції та реалізувати потреби користувачів.

Програмно-визначена мережа (Software-Defined Networks / SDN)

Основна перевага технології полягає в тому, що керування мережею здійснюється програмно, в тому числі з можливостями використання хмарних технологій та штучного інтелекту.

На сьогодні мережа управляється апаратно, за допомогою спеціального телекомунікаційного обладнання. У разі необхідності впровадження додаткових функцій та сервісів, зміни важливих параметрів системи - необхідно провести заміну обладнання, що вимагає значних витрат ресурсів та грошей. Водночас, програмно-визначена мережа дозволяє впровадити такі зміни на рівні програмного забезпечення.

Network Slicing (NS)

Ця технологія дозволяє мобільним операторам розгортати логічно ізольовані мережі, кожна з яких буде виділена під певні потреби. При цьому, відокремленими мережами можуть керувати різні суб'єкти - віртуальні оператори мережі (зв'язку). Ізольовані мережі можуть передаватися в оренду чи іншим чином в управління стороннім особам, які не мають прямого відношення до оператора зв'язку.

D2D (Device-to-device)

Дана технологія дозволяє пристроям, що знаходяться недалеко один від одного, безпосередньо обмінюватися даними. Процес обміну здійснюватиметься без участі мережі оператора зв'язку.

Ризики приватності та захисту персональних

Аналіз технічних та технологічних особливостей технології 5G, з точки зору принципів захисту персональних даних, дозволяє виділити ряд ризиків, які з великою ймовірністю будуть виникати в процесі широкомасштабного впровадження новітнього покоління мобільного зв'язку та низки сервісів, що базуються на ньому.

Значно зростає точність визначення місцезнаходження користувача (абонента)

5G передбачає використання більш високих частот, які мають значно меншу довжину хвилі. Менша довжина хвилі призводить до меншого радіусу розповсюдження радіосигналу, що у свою чергу призводить до необхідності використовувати набагато більше базових станцій з меншою відстанню між ними. Це призводить до більш точного визначення місцезнаходження абонентського пристрою (телефона чи іншого обладнання).

Більше того, враховуючи те, що 5G передбачає використання вищих частот, сигнал гірше проникає через перешкоди, у тому числі через стіни будівель. Що призводить до необхідності розміщення окремих базових станцій усередині приміщень або на дахах будівель, а це призведе до ще більш точного визначення розташування пристрою. Якщо раніше місце розташування визначалося як точка на площині карти, то тепер з'являється можливість встановити в якому саме приміщення знаходиться користувач, включаючи поверх будівлі (тривимірна геолокація).

Профілювання та автоматизовані рішення

Підвищена точність геолокації, збільшення кількості та категорій даних, що збираються та передаються у мережі, поєднане із зростаючою кількістю пристроїв, які кожен користувач підключатиме через 5G (зокрема використовуючи технологію IoT - інтернету речей), створить можливості до точного профілювання (розподілення користувачів на групи за певними ознаками).

Профілювання, у свою чергу призведе до розвитку сервісів автоматизованого прийняття рішень[6], зокрема на базі технологій штучного інтелекту.

[6] **Автоматизованими** вважаються **рішення** прийняті алгоритмами програмного забезпечення (ботами) без участі людини.

У цьому контексті викликає занепокоєння можливість реалізації права знати, механізм автоматизованої обробки персональних даних та права на захист від автоматизованого рішення[7], зокрема в частині права на перегляд такого рішення за участю людини.

Розмивання відповідальності за безпеку персональних даних між зростаючою кількістю різних учасників мережі

Розвиток нових сервісів поєднаний з можливістю поділу мережі на необмежену кількість логічно ізольованих мереж (Network Slicing) під різні потреби та задачі, призведе до зростання кількості осіб, які надають послуги і контролюють кожну з таких мереж, та фактично набувають статусу контролерів, спільних контролерів, та операторів (володільців, співволодільців і розпорядників) персональних даних.

Це може призвести до невизначеності хто саме несе відповідальність за обробку персональних даних та/або за той чи інший інцидент із даними. Також, може бути складно визначити до кого користувач - суб'єкт персональних даних повинен звертатися за захистом чи реалізацією своїх прав. Тобто, виникає ризик зниження рівня відповідальності як з боку контролерів, так і з боку операторів.

Прозорість обробки персональних даних та реалізація права на інформацію щодо такої обробки

Збільшення кількості послуг та осіб, які обробляють персональні дані, а це контролерів, спільних контролерів та операторів (володільців, співволодільців і розпорядників) персональних даних, може призвести до значного ускладнення для фізичних осіб реалізації їх права знати про обробку персональних даних. Навіть якщо кожен з осіб, які обробляють персональні дані, буде сумлінно надавати суб'єкту персональних даних всю інформацію про обробку, яка вимагається законодавством, виникають обґрунтовані сумніви, що користувач (суб'єкт персональних даних) буде здатним її сприйняти та усвідомити. Що породжує наступний ризик у сфері захисту персональних даних.

Втрата користувачем контролю над своїми даними

З урахуванням зростаючої кількості персональних даних, що збираються різними учасниками мережі 5G, передаються та обробляються

[7] **Право на захист від автоматизованого рішення** полягає у тому, що кожен, стосовно кого було прийнято автоматизоване рішення, має беззаперечне право вимагати його перегляду. І такий перегляд повинен здійснюватися за участю людини (не програми).

у різних точках планети, користувач втрачає можливість відслідкувати та проконтролювати:

- хто має доступ до його даних;
- до яких саме даних має доступ кожен конкретній учасник мережі;
- як використовуються його персональні дані;
- куди передаються та де зберігаються персональні дані (транскордонна передача);
- точність та достовірність персональних даних;
- як довго зберігаються персональні дані.

Крім того, технології 5G передбачають використання розподіленої та динамічної обробки, в якій персональні дані можуть переміщатися в реальному часі, у тому числі неодноразово перетинаючи кордони, а операції обробки можуть здійснюватися на обладнанні, розміщеному у різних країнах, в залежності від того, де така обробка буде більш ефективною.

Збільшення поверхні кібератак (cyber-attacks surface)

Збільшення кількості послуг, можливостей підключення, взаємодії, залучених осіб, точок входу та точок управління в мережі, кількості осіб, які впливають на роботу мережі (виробники обладнання, віртуальні оператори тощо) - як наслідок, збільшується кількість вразливостей, якими можна скористатися для створення загроз конфіденційності. У мережах 5G буде використовуватися більше компонентів ніж у бездротових мережах попередніх поколінь, що може надати зловмисникам різноманітні можливості для незаконного втручання у роботу мережі та трафік даних. Хоча виробники обладнання 5G та постачальники послуг підвищують безпеку за рахунок удосконалення технологій, зловмисники можуть використовувати як застарілі, так і нові вразливості.

Крім того, розвиток інтернету речей призводить до підключення саме мережі 5G численних та потенційно менш безпечних пристроїв.

Технології програмно-визначеної мережі (SDN) та віртуалізації мережевих функцій (NFV) також породжують додаткові ризики та вразливості. В ситуації коли мережею керує програмне забезпечення, ключовим питанням постає досконаліть та безпека такого програмного забезпечення. Швидкий розвиток потреб та зростаючі запити ринку можуть спровокувати квапливе розгортання нових мережевих функцій без належної перевірки відповідного програмного забезпечення.

Висновки та шляхи мінімізації ризиків

Впровадження нових технологій найчастіше породжує низку ризиків. Більшість з них можна спрогнозувати та вжити попереджувальних заходів. Деякі ризики можна буде виявити лише на практиці.

З метою мінімізації ризиків та належного реагування на нововиявлені ризики, слід сконцентрувати зусилля на розвитку таких напрямків:

- Сертифікація;
- Законодавче регулювання;
- Контроль;
- Підвищення правової культури.

Сертифікація та стандартизація

Сертифікація обладнання та програмного забезпечення і стандартизація електрозв'язку сприяє ефективному попередженню ризиків.

Необхідною умовою для забезпечення належного рівня безпеки майбутньої інфраструктури 5G є розробка стандартів технології 5G. Міжнародні організації з розробки стандартів електрозв'язку розробляють технічні стандарти та заходи безпеки, які впливатимуть на дизайн та архітектуру нових технологій. Враховуючи вплив, який ці рішення роблять на впровадження технологій 5G, дуже важливо, щоб міжнародні стандарти та політики ґрунтувалися на консенсусі, були прозорими, відкритими і технологічно нейтральними.

Водночас, навіть ідеальні стандарти не принесуть користі, якщо виробники обладнання, розробники програмного забезпечення та постачальники послуг не будуть їх дотримуватися.

Законодавче регулювання

Технології завжди випереджають законодавство. Проте, важливо не допускати, щоб таке відставання було дуже суттєвим.

З розвитком технологій мобільного зв'язку, з'являються і нові технології та способи обробки персональних даних, які не охоплені існуючим законодавчим регулюванням. Внаслідок чого права людей та, зокрема право на приватність, можуть опинитися під загрозою.

Оновлення законодавства про захист персональних даних - є один із способів забезпечити, щоб технології залишалися безпечними та дружніми для людини. У цьому контексті, важливим кроком для нашої країни є прийняття нової редакції Закону України “Про захист персональних даних”,

яка встановить вимоги до рівня захисту персональних даних не нижчі ніж це передбачено у Загальному регламенті ЄС про захист даних.

Контроль

Виправданим кроком є державний контроль за дотриманням стандартів електрозв'язку усіма гравцями ринку. Проте, при здійснені заходів контролю критично важливо забезпечити технологічну нейтральність та конкурентне середовище. Продиктовані політичними мотивами, невиправдані обмеження застосування тих чи інших технологічних рішень чи заборону на ринок певних виробників обладнання, або навпаки надання переваг деяким виробникам, може призвести до зниження якості та безпечності послуг і обладнання.

В контексті України, важливим кроком буде створення незалежного наглядового органу у сфері захисту персональних даних, який буде мати достатньо повноважень та ресурсів (включаючи людські ресурси) для забезпечення виконання вимог законодавства про захист персональних даних, зокрема у сфері електрозв'язку.

Підвищення правової культури

Підвищення правової культури як надавачів послуг (контролерів і операторів персональних даних) так і користувачів послуг (суб'єктів персональних даних сприяє усвідомленню та підвищенню рівня відповідальності кожної із сторін правовідносин.

В Україні потрібно запровадити нові і ефективні правила регулювання сфери електрозв'язку, але не потрібно допускати надмірної зарегульованості цього ринку щоб не стримувати його розвиток.