Інтернет речей: нове поле для правового регулювання

Фелікс АРОНОВИЧ,
SDM Partners Law Firm

Свого часу революційний вплив на розвиток людської цивілізації здійснила можливість використання електроенергії, радіо, телебачення. Зараз ми переживаємо новий переломний епізод у цивілізаційному поступі. Планетарного масштабу набуває таке явище як інтернет речей (IP, Internet of Things, IoT). Як зазвичай буває, за технологічними інноваціями не зовсім встигають економічні, політичні та правові інституції суспільства. В питаннях правового регулювання інтернету речей наша держава «не пасе задніх» і не випереджає сусідів. Для України в цій сфері характерні такі самі тенденції, як і для переважної більшості інших країн світу.

Інтернет речей (IP) — це екосистема технічних пристроїв та програмних ресурсів, інтегрованих у мережу інтернет, які можуть збирати, передавати та обробляти дані для здійснення певних дій. Переважно йдеться про пристрої з мікропроцесорами, сенсорами, накопичувачами даних. В чому ж полягає проблема?

Безпека

Експерти ІТ-сфери сходяться на думці про те, що саме 2019 р. стане точкою відліку настання повномасштабної IP-ери. Згідно з підрахунками консалтингової компанії Gartner, до кінця поточного року у світі будуть активовані 14,2 млрд пристроїв, підключених до інтернету. До переліку таких пристроїв належать телевізори, smart-годинники та навіть деяка побутова техніка. Такі пристрої нерідко стають мішенями для кібератак. Серед цілей злочинних діянь — крадіжка особистих даних, шпіонаж за користувачами, управління пристроями у віддаленому режимі для нанесення шкоди користувачам або для певних зловживань.

За прогнозами експертів, у 2020 р. кількість пристроїв в екосистемі IP має сягнути фантастичної цифри — до 20-26 млрд. Серед них 60-65% складатимуть споживацькі пристрої. До 2025–2030 рр. кількість підключень зросте до 80-100 млрд. Віртуальний світ поступово інтегрується з фізичним. З одного боку, це феномен, що викликає захоплення, а з іншого — обставина, яка пробуджує занепокоєння. Користувачі вже не можуть відмовитися від використання у повсякденному житті пристроїв, що є частиною IP, але перебувають у зоні ризику щодо кібербезпеки.

Правники з усього світу беруть до уваги таку ситуацію. Розробляються нормативно-правові акти, що зобов'язують виробників та продавців IP-пристроїв певним чином гарантувати безпеку користувачів. Поки що це дуже мляві та невпевнені кроки. Ймовірно, ситуація поступово буде змінюватися в міру зростання занепокоєння користувачів IP-пристроїв. Зокрема, в результаті нещодавнього опитування в країнах ЄС було виявлено, що 72% користувачів дуже стурбовані з приводу безконтрольної передачі їхніх особистих даних у мережі Інтернет. Що можна зробити?

Правові норми

Передусім, необхідно сформулювати правові та етичні норми щодо IP-пристроїв. Для галузі IP варто розробити комплексні рішення, які забезпечуватимуть захист усього ланцюга вразливостей від кінцевих точок до «хмари», куди стікаються всі дані. Не можна перекладати відповідальність за безпеку на користувача. Людина схильна до помилок, неправильного застосування паролів та інших хибних дій. Проблеми мають вирішуватися на зовсім іншому рівні, тобто виробниками пристроїв, яких до цього має спонукати законодавча база.

Законодавці та особи, причетні до розробки нових правил кібербезпеки, повинні розглядати питання безпеки не тільки на рівні програмного забезпечення, але й на рівні кінцевої точки (пристрою, що підключений до інтернету). Йдеться про брандмауери, які вбудовуються в маршрутизатори (роутери), засоби безпеки та системи блокування атак безпосередньо у процесорах, інструменти автентифікації доступу, застосування безпечного завантаження тощо.

Необхідно усвідомлювати, що певні ризики стосовно кібербезпеки не можуть зупинити процес невпинного поширення IP. Адже це відкриває занадто вагомі перспективи для покращення життя у різних сферах. Зокрема, це Smart City («розумне місто»), оптимізація транспортного трафіку в мегаполісах, великі позитивні зрушення в галузі охорони здоров'я, збільшення врожайності, зменшення витрат на логістику, раціональне використання енергії, запобігання злочинності. Інтернет речей допомагатиме суспільству ставати більш ефективним, безпечним, інноваційним, стабільним, інклюзивним. Що вже зроблено?

Закони про кібербезпеку IP

Певні кроки з боку законотворців щодо правового врегулювання кібербезпеки в IP вже були зроблені. Зокрема, увагу привертає США. Минулого року Каліфорнія стала першим штатом США, де був прийнятий закон про кібербезпеку щодо IP-пристроїв (Закон №SB-327). Цей нормативно-правовий акт має набрати чинності у 2020 р.

В законі викладені вимоги до виробників пристроїв, які напряму чи опосередковано підключаються до інтернету. Такі пристрої повинні передбачати «розумні» функції безпеки для запобігання несанкціонованого доступу, знищення, зміни чи крадіжки інформації. Положення закону спрямовані на захист звичайних користувачів. Законодавчі ініціативи щодо більш масштабних корпоративних рішень ще попереду.

Уряд Великобританії в минулому році випустив Звід практичних правил для забезпечення безпеки IP. В цьому нормативному акті акцент робиться на тому, що потрібно забезпечити кібербезпеку пристроїв, а не працювати над оновленням програмного забезпечення для посилення безпеки.

Значну увагу питанню кібербезпеки IP-пристроїв приділяє уряд Японії. В лютому 2019 р. японські чиновники з Національного інституту інформаційних та комунікаційних технологій оголосили про перевірку ефективності безпеки 200 млн IP-адрес у країні. Мета цього масштабного дослідження — виявити пристрої з низьким рівнем безпеки. Ця програма допоможе інтернет-провайдерам і телекомунікаційним компаніям краще зрозуміти вразливості в мережах та пристроях.

В ЄС закон про кібербезпеку набрав чинності 27.06.2019 р. Його положення закріплюють індивідуальні схеми сертифікації для певних категорій продуктів, процесів та послуг з IP-сфери. У сертифікатах має позначатися рівень гарантії безпеки та довіри до продукту, процесу чи послуги. Передбачається три рівні довіри. Найвищий відзначає успішне проходження всіх тестувань щодо кібербезпеки та повну гарантію для користувачів від виробника. Поки що застосування схем сертифікації не є обов'язковою вимогою для виробників IP-пристроїв. Це лише перші ініціативи, які намічають подальший напрямок законотворчості в цій сфері.

Отже, створення надійних механізмів правового регулювання у сфері інтернету речей ще попереду. Ймовірно, йдеться як про розробку національних нормативно-правових актів, так і про появу міжнародних правил забезпечення кібербезпеки IP. Українські юристи охоче долучаються до розробки та обговорення правових норм у цій сфері, адже це революційне явище, яке змінює світ.

> ***Певні ризики стосовно кібербезпеки не можуть зупинити процес невпинного поширення IP***