МІЖНАРОДНЕ ПУБЛІЧНЕ ТА ПРИВАТНЕ ПРАВО

Воляник В.І.
студентка,
Національний авіаційний університет

ПЕРЕДАННЯ ПЕРСОНАЛЬНИХ ДАНИХ ТА ЇХ ОБМЕЖЕННЯ ЗГІДНО ПРАВИЛ МІЖНАРОДНОГО КОМІТЕТУ ЧЕРВОНОГО ХРЕСТА

Розбудова інформаційного суспільства у будь-якій країні пов'язана, як з розвитком комп'ютерних технологій, так і з розширенням прав людини. Одним із проявів цього є розробка системи захисту персональних даних при їх автоматизованій обробці. Слід зазначити, що за останні 30 років більш ніж у 20 країнах світу були прийняті нормативно-правові акти із захисту персональних даних, у котрих закріплені реальні механізми правого регулювання обігу такої інформації.

У криміналістиці принцип Локарда стверджує, що «кожен контакт залишає слід». Те саме стосується кожної інформації в Інтернеті: SMS, додатки для обміну повідомленнями, програми передачі готівки – генерують постійний потік інформації на високому рівні відстеження [1]. Тим самим викликаючи належним чином обґрунтовані занепокоєння щодо конфіденційності даних. *Це становить небезпеку* для таких організацій, як Міжнародний комітет Червоного Хреста (МКЧХ), який з перших рук працює на полі бою для проведення ефективних гуманітарних дій. МКЧХ пропонує допомогу людям з усіх сторін конфлікту.

В останні пару років МКЧХ невпинно збільшував зусилля для забезпечення вищого рівня захисту даних від третіх сторін [4]. Одним з конкретних прикладів сучасного підходу МКЧХ до стратегій безпеки даних є його нова «Політика щодо обробки біометричних даних», прийнята в серпні 2019 року. Згідно цього були сформовані основні вимоги щодо передання даних та їх обмеження.

Дані можуть передаватися суб'єктам, які перебувають за межами Міжнародного комітету Червоного Хреста, лише за умови виконання наступних умов:

– згода суб'єкта даних;
– життєвий інтерес суб'єкта даних або іншої особи;
– суспільний інтерес, зокрема на основі мандата МКЧХ;
– законні інтереси МКЧХ за умови, що ці інтереси не перекриваються правами і свободами суб'єктів даних;
– виконання договору та дотримання юридичного зобов'язання.

Проводиться оцінка ризику та вживаються відповідні заходи щодо пом'якшення наслідків згідно зі статтею 23. Обсяг та тип персональних даних, які потрібно передавати, суворо обмежуються потребою одержувача в конкретних цілях або для подальшої обробки. Засоби передачі та застосовані методи безпеки повинні бути пропорційними характеру та терміновістю гуманітарних дій, щодо цього має зберігається запис про передачу.

Для систематичних або великих масштабів передачі даних або коли дані для передачі є особливо чутливими – необхідна офіційна угода між одержувачем та суб'єктами даних [2]. Це може бути зроблено за допомогою спеціальних договірних положень про захист даних, партнерському договорі або в меморандумі про взаєморозуміння або у формі спеціальної угоди про передачу даних. Для передачі даних, що не підпадають під дію таких угод, необхідно здійснити такі заходи:

– письмове зобов'язання одержувача, що вони оброблять особисті дані лише для конкретних цілей, для яких вони були передані, і не передаватимуть їх третій стороні;
– визначення відповідальною державою, що одержувач здійснює технічні та організаційні заходи, які забезпечать належний захист переданих персональних даних.

Нерозголошення інформації МКЧХ повинно дотримуватися постійно, і будь-яка відповідь на запит влади про доступ до персональних даних, що зберігається МКЧХ, повинна бути заздалегідь узгоджена з Правовим відділом МКЧХ. Дані повинні бути надані сторонам збройного конфлікту, або суб'єктам, які беруть участь в інших ситуаціях насильства, лише після конфірмації.

Будь-який керівник МКЧХ, який бажає створити або змінити базу даних, повинен, коли це передбачає обробку персональних даних, подати пропозицію, лише тоді будуть внесені зміни. Оцінка впливу на

захист даних повинна використовувати стандартизовані форми та вказівки.

Будь-яке співробітництво з національними або регіональними органами захисту даних не зачіпає привілеїв та імунітетів МКЧХ відповідно до внутрішнього та міжнародного права. З метою повного захисту персональних даних, МКЧХ повинен забезпечити визнання його специфічного статусу та усвідомлення всіма зацікавленими сторонами, що МКЧХ не може бути змушений розкривати будь-яку інформацію, отриману під час виконання своєї роботи [3].

Про будь-яке порушення безпеки, що призводить до випадкового чи незаконного знищення, втрати чи зміни або до несанкціонованого розголошення чи доступу до персональних даних, що передаються, зберігаються чи обробляються іншим чином – завжди слід повідомляти про захист даних МКЧХ.

Персональні дані повинні оброблятися таким чином, щоб був забезпечений належний ступінь безпеки. Для цього повинно бути враховано ряд факторів, а саме: характер даних та ризик як для суб'єктів даних, так і для повноважень МКЧХ. Це включає запобігання несанкціонованому доступу до персональних даних або використання обладнання, яке використовується для обробки даних. Це стосується, зокрема, прав доступу до баз даних, фізичної безпеки, комп'ютерної безпеки чи кібербезпеки.

Якщо збереження персональних даних більше не потрібно, усі записи та резервні копії повинні бути надійно знищені або анонімізовані

Загалом, Міжнародний комітет Червоного Хреста володіє та передає важливі дані. Захист персональних даних – це вміння балансувати між інформаційною відкритістю та закритістю, між двома прагненнями: максимально розширити доступ громадян до невтаємниченої публічної інформації (державної, наукової, освітньої, персональної тощо) і водночас максимально захистити інформацію приватного змісту. Вирішення стратегічних завдань, пов'язаних із удосконаленням інформації про особу полягає у розвитку нових програм, створенні вітчизняних систем захисту та розв'язання протиріч, що виникають у сучасному законодавстві.

Список використаних джерел:

1. Data security in humanitarian action (December 05, 2019) [Electronic resource]. – Access mode: https://leidenlawblog.nl/articles/data-security-in-humanitarian-action (date of appeal 04.05.2020).

2. Enhancing Protection for civilians in armed conflict and other situation of violence [Electronic resource]. – Access mode: https://www.icrc.org/en/publication/0956-enhancing-protection-civilians-armed-conflict-and-other-situations-violence (date of appeal 04.05.2020).

3. Handbook on data protection humanitarian action [Electronic resource]. – Access mode: file:///Users/viky_vegas/Documents/Vlasyslava's%20documents/4305_002_Data_protection_and_humanitarian_action_low.pdf (date of appeal 04.05.2020).

4. ICRC: Protection of victims of armed conflict through respect of International Humanitarian Law [Electronic resource]. – Access mode: https://www.icrc.org/en/doc/resources/documents/misc/57jpzn.htm (date of appeal 04.05.2020).