„Защита на правата в Метавселената“

Анатали Георгиева

Софийски университет „Св. Климент Охридски”

IV курс, Право

Технологичната еволюция, която наблюдаваме от началото на XXI в., е основополагаща за бъдещото развитие на обществените отношения. Обществени отношения, които ще бъдат обект на наблюдение не в реалния свят, а в неговото дигитално отражение. Именно поради липсата на фактическото възприятие на отделни явления, в корена на очертаващия се проблем за нормирането на човешкото поведение, е зараждащата се „метавселена".

Започнала като идея в научно-фантастичния труд „Снежен крах" на Нийл Стивънсън, „метавселената" придобива реално изражение в идеологията на технологичния гигант „Мета" и неговия създател – Марк Зукърбърг. През 1992 г. Нийл Стивънсън описва метавселената като виртуален свят, в който потребителите могат да се включат чрез специални устройства, а вътре да бъдат представлявани от различни аватари.[1] През 2022 г. представата за метавселените е развита до нива, в които могат да се обособят „затворени" или „публични" метавселени.[2]

Наличието на различни нива на метавселени обуславя нуждата от прогресивно развитие на законодателството и по-конкретно, правните норми, които целят да защитят потребителите и данните, които те предоставят.[3] Предизвикателството да се осигури защитата на потребителите в метавселените е пряко свързано и с тяхното изграждане от алгоритми, които използват изкуствен интелект.[4] Поради естеството на работа на тези алгоритми и способността им да се развиват сами чрез самообучение въз основа на събрана база данни, се налага да се използват очила за виртуална реалност, които да наблюдават поведението на потребителите. Въз основа на събраната информация от очилата за виртуална реалност, изкуственият интелект разполага с база данни, която да персонализира съдържанието, което ще бъде предоставено на потребителя. Това съдържание е продукт от чувствителните данни, които са събрани от очилата за виртуална реалност, т.нар. биометрична психография.[5]

---

[1] Wang Yu., Zhou S., Zhang N., Xing R., Liu D., Luan T., Shen X., *A Survey on Metaverse: Fundamentals, Security and Privacy*, Sep. 2022, p. 1

[2] Seidel St., Berente N., Yepes Gr., Nickerson J., *Designing the Metaverse*, 55th Hawaii International Conference on System Sciences, 2022, p. 6 702

[3] European Parliament, *Metaverse: Opportunities, risks and policy implications*, 2022

[4] Wang Yu., Zhou S., Zhang N., Xing R., Liu D., Luan T., Shen X., *A Survey on Metaverse: Fundamentals, Security and Privacy*, Sep. 2022, p. 2

[5] *ibid.* p. 2

Този термин е представен от Брайтън Хелър и нейният труд „*Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*“. Биометричната психография представлява това ниво на биологична информация, което компаниите ще могат да събират за лицата, използвайки комбинация от анатомични и личностни данни.[6] Именно събирането и обработването на данни от биометрична психография, представлява опасност за неприкосновеността на личността на всеки един потребител.

Събирането на подобни данни цели да се индивидуализира метавселената, в която потребителят участва и по-конкретно, чрез профилиране той да получава единствено информация, към която има интерес. Това профилиране крие рискове за сигурността на индивидите, тъй като те следва да „разрешат“ достъп до ежедневния си живот. Достъпът до разположение, навици и начин на живот на отделните индивиди могат да доведат до прекомерно събиране на данни.[7] Предоставянето на информация относно ежедневния живот живот на лицето и виртуалния му еквивалент, с ясна цел и двете да бъдат синхронизирани, води до високи нива на зависимост между двата реалма. Свързването на реална личност с виртуала такава съставлява опасност от имперсонификация от трети лица.[8] Именно поради опасността един индивид да бъде неправомерно представляван от друг, събирането на данни от нелицензирани оператори следва да бъда забранено, за да се запази сигурността на участниците в „метавселените“.[9] Всички тези усложнения при предоставянето на лични данни във виртуалната среда е нужно да бъдат адресирани от международната общност поради високото ниво на поверителна информация, която се обработва ежедневно.

Към момента правните инструменти, които задават стандартите за функционирането на метавселените са съставени от Международната организация по стандартизация („ISO“). Въпросите, които тези стандарти

---

[6] Heller B., *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*, 23 Vanderbilt Journal of Entertainment and Technology Law 1 (2021), p. 27; Carbonneau S., *Biometric Psychography and its Implications on Personal Autonomy*, last accessed: 29 Nov. 2022 (https://www.extendedmind.io/the-extended-mind-blog/biometric-psychography-and-its-implications-on-personal-autonomy)

[7] *ibid.* p. 15

[8] *ibid.* p. 16

[9] *ibid.* p. 16; Ometov A., Bezzateev S. V., Kannisto J., Harju J., Andreev S., and Koucheryavy Y., *Facilitating the delegation of use for private devices in the era of the internet of wearable things*, IEEE Internet of Things Journal, vol. 4, no. 4, pp. 843–854, Aug 2017

регулират са свързани с правилното предаване на информация и обмен на данни между реалния и дигиталния свят (ISO/IEC 23005 (MPEGV)) [10], както и синхронизирането на киберпространството и физическия свят (IEEE 2888)[11]. Тези стандарти не разглеждат нуждата от прозрачно събиране на данни. Именно поради тази причина се налага да се насочим към регионалните и националните инструменти за защита на лични данни. В Европейския съюз такъв инструмент е Регламент 2016/679 („GDPR“).

GDPR очертава основните права на потребителите, когато техни лични данни са събрани и анализирани в интернет пространството. Поради естеството на настоящата работа следва да анализираме дали определението за лични данни, дадено ни в чл. 4, пара. 1 от GDPR включва събирането на биометрични данни. Европейският законодател дефинира лични данни като всяка информация, чрез която може да се идентифицира едно физическо лице.[12] Посочено е, че личните данни могат да включват специфични фактори като физически, физиологични, генетични, психични и други аспекти, чрез които потребителят предоставя информация.[13] От изведената дефиниция личи, че законодателят е целял да включи в най-широк обем данните, които биха могли да бъдат предоставяни от потребителите.

Проблемът в GDPR към настоящия момент е липсата на механизъм, който да следи за правилното събиране на биометрични данни. Съгласно настоящите разпоредби, проверка за неправомерно събиране на биометрични данни може да бъде започната в случаите, когато има подаден сигнал от потребител, чието право се смята за нарушено, или в хипотеза на пробив в базата данни на оператора. Тоест дружествата разполагат със свободата да обработват данни, вкл. и извън нуждите, за които са им необходими, като потенциални негативни последици може да се установят единствено в случаите на гореспоменатите неизправности. С оглед на чувствителната информация, която се предоставя при събирането на биометрични данни, е нужно да се регулират условията, при които същите могат да бъдат обработвани, като отделна и специална форма на предоставени лични данни. Целта на подобно специфично разглеждане на биометричните данни е да

---

[10] ISO/IEC 23005-1:2020, *Information technology — Media context and control — Part 1: Architecture*
[11] IEEE 2888, last accessed: 16 Nov. 2022 (https://sagroups.ieee.org/2888/)
[12] Регламент 2016/679, чл. 4: Дефиниции, пара. 1
[13] *ibid.*

защити максимално личността на потребителите и да предотврати евентуалната им неправомерна персонификация в метавселените.

На национално ниво следва да се отбележат опитите на няколко американски щата за нормиране на събирането на биометрични данни.[14] Безспорно най-успешният от тях е Законът за защита на биометричната информация на щата Илинойс. В него американският законодател е очертал две отделни определения за биометрично идентифициране и за биометрична информация.[15] Целта на този закон е ясно да се отграничат двете определения и да се зададат граници, в които може да се събира биометрична информация. Самият закон изключва определени данни от обхвата на биометричните данни, напр. снимки, подписи, описание на външен вид и т.н.[16] Въпреки наличието на подобен закон, неясноти относно събирането на биометрични данни все още са налични. Брайтън Хелър резонно задава въпроса дали софтуерите за лицево разпознаване събират биометрични данни.[17] Неточността в конкретната хипотеза, посочва Хелър, е разбирането, че лицевата геометрия представлява биометрична информация, но видео и снимкови материали са изключени от обхвата на Закона на щата Илинойс.[18] Следователно правоприлагащите органи са поставени в хипотеза, в която разполагат с правните инструменти за защита на потребителите, но тези правни инструменти водят до двусмислени изводи за приложението им.

Анализа на три различни инструмента за регулация на отношенията в метавселената показва, че все още има различия при дефинирането на биометричните данни, които са в основополагащи за участието на потребителите в метавселените. Това разминаване в разбиранията води до несигурно и неравно събиране на чувствителна информация за личния живот на потребителите. Липсата на единно законодателство на международно ниво води до застрашаване

---

[14] Heller B., *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*, 23 Vanderbilt Journal of Entertainment and Technology Law 1 (2021), p. 34

[15] 740 ILCS 14, Biometric Information Privacy Act, Sec. 10

[16] 740 ILCS 14, Biometric Information Privacy Act, Sec. 10

[17] Heller B., *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*, 23 Vanderbilt Journal of Entertainment and Technology Law 1 (2021), p. 34

[18] *ibid.,* p. 35

на фундаментални права на човека, а именно правото на лична сигурност[19] и неприкосновеност на личния живот[20].

[19] Всеобща декларация за правата на човека, чл. 3
[20] Всеобща декларация за правата на човека, чл. 12