ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В СОЦИАЛНОТО ОСИГУРЯВАНЕ В УСЛОВИЯТА НА ЦИФРОВИЗАЦИЯ

доц. д-р Христина Благойчева
Икономически университет – Варна

PROTECTION OF PERSONAL DATA IN SOCIAL SECURITY IN THE SETTINGS OF DIGITALIZATION

*Assoc. Prof. Hristina Blagoycheva, PhD
University of Economics - Varna, Bulgaria*

Резюме: Цифровизацията увеличава потенциала на социалното осигуряване за по-висока ефективност при предоставянето на нови услуги и разгръщането на мащабни социални програми. Съществува обаче възможността тези технологии да станат предпоставка за не-регламентиран достъп до информация и лични данни, съхранявани в цифровата мрежа. Затова целта на доклада е да се изведат някои предизвикателства в тази насока и да се потърсят възможни решения.

Ключови думи: *социално осигуряване, цифровизация, поверителност, лични данни*

Abstract: Digitization increases the potential of social security for greater efficiency in the provision of new services and the deployment of large-scale social programs. However, there is a possibility that these technologies will become a prerequisite for unregulated access to information and personal data stored in the digital network. Therefore, the purpose of the report is to identify some challenges in this direction and to seek possible solutions.

Keywords: *social security, digitization, confidentiality, personal data*

DOI: <https://doi.org/10.36997/PPDD2021.86>

Въведение

Функционирането на социалното осигуряване се обуславя от необходимостта за задоволяване на широк спектър индивидуални потребности, свързани с издръжката на живота. То може да се разглежда

като вид защитна мрежа, предпазваща осигурените лица от бедност и други икономически последици при временна или постоянна загуба на трудови доходи. В тази връзка и осигурителната система се въвежда в законодателствата като гаранция за закрила на базисни човешки потребности, възникващи както при загубата на способности за полагане на труд, така и предвид подпомагане и солидарна съпричастност на маргинални житейски условия на индивида, лишавачи го от средства за достойно и социално приемливо съществуване (Йолова 2016: 181). Логично социалното осигуряване е една от най-значимите съвременни правителствени програми и в обхвата му попада огромна част от населението на съответната страна. То работи като икономически, социален и политически стабилизатор, редуцира доходните неравенства до приемливи нива и осигурява механизми за облекчаване и предотвратяване на бедността .

За да подобрят ефективността и качеството на услугите за бенефициентите си, социалноосигурителните институции все по-широко се отварят към използването на цифровите технологии. Цифровизацията позволява нови услуги, ориентирани към потребителите и разгръщането на мащабни социални програми, включващи дори организации на национално и до известна степен на международно ниво. Автоматизираната обработка на данните спомага програмите за социална защита да се прилагат на основата на информационно обосновани решения. А увеличеното използване на мобилни технологии дава по-добър достъп на гражданите до социалноосигурителни онлайн услуги.

Успоредно с многото ползи обаче съществува и възможността цифровите технологии да създадат предпоставки за нерегламентиран достъп до информация и лични данни, съхранявани в различни възли на социалноосигурителната мрежа. Затова въпросът за гарантиране на сигурността на данните и зачитане на правото на гражданите на поверителност е по-значителен отвсякога. Използването на цифровите технологии за подобряване на социалноосигурителните мероприятия не трябва да се осъществява в противоречие със защитата на личните данни.

Целта на настоящия доклад е както да се изведат основните предизвикателства, които цифровизацията поставя пред социалноосигурителните институции по защитата на информацията и личните данни, така и да се потърсят възможни решения. В тази връзка се

разглеждат предимствата за социалноосигурителната система от използването на цифровите технологии и възможните рискове за поверителността и сигурността на личните данни на обхванатите лица. Представят се и както предприетите мерки, така и някои допълнителни решения.

1. Използването на лични данни в цифрова среда

Институциите, провеждащи социалноосигурителните мероприятия, не могат да функционират без достъп до лични данни. Те съхраняват и ежедневно оперират с огромно количество лична информация. Тази информация може допълнително да се използва за генериране на услуги с добавена стойност, за подобряване на дизайна на програмата или дори за прогнозиране на бъдещи ползи.

Някои от ползите са систематизирани в табл. 1

Таблица 1

Предимства от интегрирането на данните в цифровите системи

За политиката и планирането в социално-осигуряване	За администраторите на програмите	За бенефициентите
Идентифициране на планираните популации, профилиране на нуждите и характеристиките	Споделени ресурси за прием и регистрация във „фронт офис“	Насърчаване на осведомеността и достъпа до множество предимства и услуги
Подобрена ефективност, точност и качество на данните => по-добро използване на публичните разходи	По-ниски административни разходи	Може да кандидатстват за много програми едновременно с по-прости процедури, спестявайки време – разходи – посещения
Мониторинг кой какви програми получава, идентифициране на пропуски в обхвата, дублиране, допълване	Подобрена точност, качество на данните, ефективност, прозрачност => по-малко дублиране и грешки	Достъп до техните данни, информация за получените обезщетения и статут на допустимост

Улесняване на координираното реагиране на социалните програми на кризи	Улесняване на посредничеството и сезиране, интегрирано управление на случаи	По-ефективни и координирани обществени услуги
--	---	---

Източник: адаптирано по Socialprotection.org. (2019).

Очевидно дигитализирането на информацията в социалното осигуряване има широк потенциал за подобряване на дейността му. Тя може да ограничи фрагментираните, изолирани интервенции за социална защита, подкрепяйки системния подход към универсализирането им и да свърже бенефициентите на системата с други услуги и възможности за подкрепа. Цифровите технологии могат да поддържат по-точни и ефективни услуги, чрез автоматизиране и подобро управление на данните. Те редуцират натоварването на персонала в социалноосигурителните институции и позволяват по-информирани управленски решения. Т.е. могат да предоставят по-удобни, по-бързи и по-сигурни услуги на бенефициентите (Handayani et al. 2017).

Успоредно с ползите обаче могат да възникнат някои предизвикателства и рискове, сред които както увеличаване на разходите и сложността, така и рискове за поверителността и сигурността на личните данни. Това безспорно следва да е свързано с изключителни нива на защита при управлението и използването на данните (Андреева, Йолова 2018: 259). Варса (2017 : 43) подчертава, че „някои категории данни могат да бъдат по-спорни от други, що се отнася до съображения за поверителност и сигурност на данните“. Т.е. цифровизирането на информацията може да не отчете в достатъчна степен защитата на данните и правото на гражданите на поверителност. Съществува дори и мнението, че технологията сама по себе си не гарантира добро управление на информацията (Varca 2017: 55). В този контекст въпросът за поверителността на данните е крайно належащ за разглеждане.

При изпълнението си програмите за социална защита обработват значителни количества лични данни (име, възраст, пол, адрес, здравословно състояние, биометрични данни като пръстови отпечатъци и много други), събирани от лица, семейства и домакинства и сред които се среща и чувствителна информация, която би следвало да подлежи на специфични условия на обработване. В тази връзка

Европейската комисия дава отговор на въпроса кои лични данни се считат за „чувствителни“¹:

- лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения;
- членство в професионална организация;
- генетични данни, биометрични данни, обработвани единствено с цел идентификацията Ви като човешко същество;
- данни за здравословното състояние;
- данни за сексуалния живот или сексуалната ориентация на дадено лице.

Липсата на достатъчни предпазни мерки понякога е предпоставка за злоупотреба с такива чувствителни данни (информация за самоличността, адреса, здравето, имущество и банковите сметки на бенефициента на социалните програми) чрез неправомерен достъп от трети страни.

В тази връзка като предпоставки за неправомерен достъп могат да се изведат:

- прекомерно разширяване на обема на събираната, обработваната и съхраняваната информация;
- широко използване на компютърни мрежи и тяхната интеграция в обработката и съхраняването на информацията с лични данни;
- широк брой на потребителите, получили достъп до системата и информационните ресурси;
- използване на база данни, в която са обединени различни информационни фондове.

При по-ниско ниво на сигурност на информационната система тя става уязвима за кибератаки, които целят достъп до лична информация. Такива атаки може да са насочени към отделен компютър, мрежова връзка или цяла мрежова инфраструктура, както и към (или чрез) телекомуникационните мрежи и оператори.

2. Мерки за защита на личните данни

Защитата на данните е важна за спазване на правото на гражданите на неприкосновеност на личния им живот. Правото на неприкосновеност е международно признато право на човека, заложено

¹ https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_bg

още през 1948 г. във Всеобщата декларация на правата на човека на ООН, а впоследствие и в различни конвенции на регионално ниво и национални конституции и закони. Неприкосновеността на личния живот може да се представи като право на индивидите да разполагат с лично пространство, свободно от намеса на други хора и организации (Кларк 1999). От своя страна правото на защита на данните гарантира „основното право на неприкосновеност на личния живот чрез регулиране на обработването на лични данни: осигуряване на права на индивида върху техните данни и създаване на системи за отчетност и ясни задължения за тези, които контролират или приемат обработката на данни “ (Privacy International 2018: 12).

Всяко лице има право на защита на своите лични данни (Oostveen, Irion: 2018). Следователно защитата на данните има важно значение за упражняването на правото на личен живот. Отчитайки това значение, през 2016 г., Международната асоциация за социално осигуряване (ISSA) разработи Насоки за информационни и комуникационни технологии (ISSA 2016), извеждайки на преден план управление при висока информационна сигурност и неприкосновеност на личния живот в институциите за социална сигурност. Насоките подчертават от една страна значението на създаването на адекватна рамка за защита на данните, съобразена с правната и регулаторна среда, а от друга – необходимостта от въвеждане на глобална система за защита на личните данни в съответствие с изискванията, свързани с международния обмен на данни.

В тази връзка може да се посочат и Директива 2002/58/СЕ за защита на личните данни в електронните комуникации, Директива 2006/24/СЕ относно запазването на данни за трафика при предоставянето на обществено достъпни електронни съобщителни услуги (2006) и Общият регламент за защита на данните от 2016 г., който влезе в сила на 28 май 2018 г. (Regulation (EU) 2016). Пак през 2018 г. ООН прие Принципи за защита на личните данни и поверителност (UN 2018).

Увеличените кибератаки в кризисното време на пандемията COVID 19 изведоха на преден план необходимостта от стабилна защита, съобразена с очакваното бъдеще на публичните институции в областта на здравеопазването, социалното осигуряване и др. системи. Затова в края на 2020 г. Европейската комисия и върховният представител на Съюза по въпросите на външните работи и политиката

на сигурност представиха нова стратегия на ЕС за киберсигурност. Фокусът на стратегията е върху изграждането на колективни способности за реакция при големи кибератаки и работа с партньори по целия свят, за гарантиране на международната сигурност и стабилност в киберпространството. (European Commission 2021a). А чрез Програмата за цифрова Европа за периода 2021 г. – 2027 г. се планира инвестиция от 1,9 милиарда евро в капацитета за киберсигурност и широкото разполагане на инфраструктури и инструменти за киберсигурност в целия ЕС за публични администрации, предприятия и физически лица (European Commission 2021b).

Според едно глобално проучване, към ноември 2019 г., 13 държави са приели закони за защита на данните/поверителността, други 30 държави и юрисдикции имат предстоящи инициативи за защита на личните данни, притежавани от частни и публични органи (Банисар 2021).

Очевидно, за да се запази доверието на осигурените лица към институцията, са необходими силни практики за защита на данните и ефективно законодателство, което да съдейства за свеждане до минимум на киберриска от страничното наблюдение и използването на данни. Например подобрения в сигурността на използваните данни може да се постигнат и с няколко допълнителни стъпки:

- информиране на обхванатите лица за естеството и целта на събиране на данните;
- създаване на механизъм за обратна връзка при забелязани нарушения;
- постоянни процедури по наблюдение и оценка на риска;
- въвеждане на правила и стандарти за всеки етап от процеса на събиране и използване на данните;
- при необходимост от споделяне на данни – сключване на споразумения с партньора за неразкриване на информация;
- защитено архивиране на данните и специално оторизиране на лице, което да отговаря за процедурите.

Набирането на лични данни изисква съгласие на собствениците им. А при обработката им е необходимо спазването на такива принципи като законност, справедливост и прозрачност. Самите институции също трябва да гарантират, че данните са адекватно защитени и да разработят убедително ценностно предложение, демонстриращо ползата за потребителя. За целта те трябва да са наясно към какви

рискове са уязвими и какво могат да направят, за да се смекчат заплахите и евентуалното въздействие.

Заключение

Дигиталните технологии променят начина на проектиране и прилагане на системите за социална защита. Въвеждат се нови системи за идентификация, информационни системи за управление, информационни системи за социална защита, цифрови плащания и др. Цифровите технологии могат да улеснят и ускорят процесите по предоставяне на социална защита, да намалят някои разходи, да подобрят прозрачността и приобщаването на субектите в системата и като цяло, да повишат нейните ефективност и ефикасност. Но те носят и специфични предизвикателства, сред които високи технологични разходи, сложност (необходимост от различни умения на персонала), възможни компромиси (например намаляване на общата ефективност) и сериозни рискове за поверителността и личните данни. Затова работата с лични данни трябва да се извършва при запазване на поверителността и строга защита.

Поради тази причина всички институции, които обработват лични данни, трябва да разработят и прилагат ясна и бърза политика за защита на данните като част от политиката за сигурност на информацията и политиката за сигурност на национално и международно ниво.

Използвана литература

Aloisi, A., E. Gramano (2019). Workers without workplaces and unions without unity: Non-standard forms of employment, platform work and collective bargaining. // Bulletin of Comparative Labour Relations. Employment Relations in the 21st Century: Challenges for Theory and Research in a Changing World of Work, Chapter: 4. Alphen aan den Rijn, Zuid-Holland: Kluwer Law International.

Banisar, D. (2021). National Comprehensive Data Protection/Privacy Laws and Bills, (<https://ssrn.com/abstract=1951416> or <http://dx.doi.org/10.2139/ssrn.1951416> , 01.10.2021).

Barca, V. (2017). Integrating data and information management for social protection: Social registries and integrated beneficiary registries.

Canberra: Commonwealth of Australia, Department of Foreign Affairs and Trade, (<https://socialprotection.org/discover/publications/integrating-data-and-information-management-social-protection-social>, 07.09.2021).

CaLP. (2013). Protecting Beneficiary Privacy: Principles and Operational Standards for the Secure Use of Personal Data in Cash and E-transfer Programmes. Oxford: Cash Learning Partnership (CaLP) (<https://reliefweb.int/sites/reliefweb.int/files/resources/calp-beneficiary-privacy-web.pdf>, 27.09.2021).

Clarke, R. Internet privacy concerns confirm the case for intervention. // Communications of the ACM, 1999, Vol. 42, №2, pp. 60 – 67, (<http://dx.doi.org/10.1145/293411.293475>).

European Commission. (2021a). Cybersecurity Policies, (<https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies>, 15.09.2021).

European Commission. (2021b). The Digital Europe Programme, (<https://digital-strategy.ec.europa.eu/en/activities/digital-programme>, 15.09.2021).

Handayani, S. et al. (2017). Improving the delivery of social protection through ICT – Case studies in Mongolia, Nepal, and VietNam. ADB Sustainable Development Working Paper 50. Manilla: Asian Development Bank, (<https://www.adb.org/sites/default/files/publication/384386/sdwp-50.pdf>, 07.09.2021).

ISSA. (2016). ISSA Guidelines on information and communication technology. Geneva: International Social Security Association, (<https://ww1.issa.int/guidelines/ict/174551>, 29.08.2021).

Oostveen, M, U. Irion (2018). The golden age of personal data: How to regulate an enabling fundamental right? // Personal Data in Competition, Consumer Protection and Intellectual Property Law. Singapore: Springer, pp. 7 – 26, (https://link.springer.com/chapter/10.1007/978-3-662-57646-5_2, 47.09. 2021).

Privacy International (2018). The Keys to Data Protection: A Guide for Policy Engagement on Data Protection, Privacy International, London, (<https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf>, 19.09.2021).

Regulation (EU) 2916/679 of the European Parliament and the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protect Regulation),

European Commission, 2016, (<https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex%3A32016R0679>).

Socialprotection.org. (2019). Digital social protection – innovation for effectiveness. The fourth webinar of the USP2030 webinar series, organised by socialprotection.org and in collaboration with the International Policy Centre for Inclusive Growth, (<https://socialprotection.org/digital-social-protection-%E2%80%93-innovation-effectiveness>, 11.09.2021).

UN. (2018). UN Principles for the Protection of Personal Data and Privacy, (https://archives.un.org/sites/archives.un.org/files/_un-principles-on-personal-data-protection-privacy-hlcm-2018.pdf, 22.09.2021).

Андреева, А., Г. Йолова (2018). Тенденции при антидискриминационните политики в сферата на здравното осигуряване в условията на дигиталното общество. Защита срещу дискриминацията: Правна уредба, проблеми и тенденции. // Сборник с доклади от национална научна конференция на ИУ – Варна. Варна : СТЕНО, с. 259.

Йолова, Г. (2016). За социалната роля на осигуряването. Правната наука и бизнесът – заедно за устойчиво развитие на икономиката. Варна: Наука и икономика, с.181.

За контакти: доц. д-р Христина Благойчева
Икономически университет – Варна
e-mail: hrblagoycheva@ue-varna.bg