

**ციფრულ გარემოში არასრულწლოვანთა პერსონალური მონაცემების დაცვა მშობლებისა და შვილების განსხვავებული მოლოდინების პირობებში**

ყველა ბავშვს აქვს მისი ძირითადი უფლებებისა და თავისუფლებების დაცვისა და პატივისცემის უფლება როგორც ჩვეულებრივ, ასევე ციფრულ გარემოში. შესაბამისად, ასაკისა და დამუშავების პლატფორმის მიუხედავად, დაცული უნდა იყოს მათი პირადი ცხოვრების ხელშეუხებლობა და პერსონალური მონაცემები.

ევროპული და ამერიკული საკანონმდებლო ნორმები (ზოგ შემთხვევაში, ასევე სასამართლო პრაქტიკა) ბავშვის პირადი ცხოვრების დაცვის მთავარ ფიგურად მშობელს მოიაზრებს, რადგან მას აქვს ბავშვის ინფორმაციის დამუშავებაზე ექსკლუზიური კონტროლის უფლება. საკანონმდებლო ნორმები, როგორც წესი, არ არეგულირებს მშობლების მიერ შვილის პერსონალური მონაცემების დამუშავების სამართლებრივ ასპექტებს მშობლის მხრიდან შვილის უფლებების შეზღუდვის ქრილში. აღნიშნული ნაწილობრივ გამოწვეულია საზოგადოებაში დამკვიდრებული შეხედულებით, რომ მშობლის მოქმედებები ყოველთვის განპირობებულია ბავშვის საუკეთესო ინტერესით, ასევე იმ ფაქტორით, რომ „გაციფრულებული ბავშვები“ ჯერ კიდევ პატარები არიან და იურიდიულ წრეებში ციფრულ გარემოში მშობლების მიმართ მათი უფლებების დაცვის საკითხებზე მსჯელობა ჯერ არ დაწყებულია.

სასამართლო პრაქტიკა ადასტურებს, რომ „მშობლის თვალთ“ დანახული ბავშვის საუკეთესო ინტერესი ყოველთვის არ არის თანხვედრაში „შვილის თვალთ“ აღქმულ საუკეთესო ინტერესთან. შესაბამისად, თანამედროვე ეპოქაში გამოიკვეთა მშობლებისა და არასრულწლოვანი შვილების განსხვავებული მოლოდინები და შეხედულებები ციფრულ გარემოში არასრულწლოვანთა პერსონალური

---

\* ნიუ ვიკენ უნივერსიტეტის სამართლის სკოლის დოქტორანტი; შავი ზღვის საერთაშორისო უნივერსიტეტის მოწვეული ლექტორი, იურიდიული სამსახურის უფროსი.

მონაცემების დაცულობის ასპექტში. წინამდებარე კვლევა მიზნად ისახავს იმგვარი მექანიზმების განხილვას, რომლებიც არასრულწლოვანთა პერსონალური მონაცემების დაცვის გზით უზრუნველყოფს ციფრულ გარემოში მშობლებისა და არასრულწლოვანი შვილების მოლოდინების მართებულ ფორმირებას.

**საკვანძო სიტყვები:** პერსონალური მონაცემები, არასრულწლოვანი, ციფრული გარემო, თანხმობა.

## 1. შესავალი

პერსონალური მონაცემი თანამედროვე ეპოქის ახალი ვალუტაა. მისი მონეტარული ღირებულება მზარდია და მრავალი კომპანიისათვის მნიშვნელოვან აქტივს წარმოადგენს.<sup>1</sup> დღევანდელ ეპოქაში პერსონალური მონაცემი ნავთობსაც კი შეედრება – იგი ღირებულია, თუმცა გადამუშავების გარეშე გამოუსადეგარი.<sup>2</sup>

სწორედ ამ „ნავთობის“ მოპოვებაზე ორიენტირებული კომპანიების „ობიექტებს“ წარმოადგენს ინდივიდი და მისი არასრულწლოვანი შვილი, რომელთა პრივატულობის საკითხი, განსაკუთრებით კი ტექნოლოგიურ შესაძლებლობების განვითარების ფონზე, კითხვის ნიშნის ქვეშ დგას. სიტუაციას კიდევ უფრო ამძაფრებს არასრულწლოვანთა მხრიდან საინფორმაციო ტექნოლოგიების გამოყენების მაღალი ამპლიტუდა<sup>3</sup> და ამ მიმართულებით საგანგაშო სტატისტიკა.<sup>4</sup>

რამდენადაც ყველა ბავშვს აქვს მისი (ადამიანის) ძირითადი უფლებებისა და თავისუფლების დაცვისა და პატივისცემის უფლება როგორც ჩვეულებრივ, ასევე

<sup>1</sup> *Schwartz P. M.*, Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2004, 2056, <<https://www.jstor.org/stable/4093335>> [27.06.2022].

<sup>2</sup> *Joshua N.*, Why do People Still Think Data is the New Oil? Center for Data Innovation, 2018, <<https://www.datainnovation.org/2018/01/why-do-people-still-think-data-is-the-new-oil/>> [27.06.2022].

<sup>3</sup> მსოფლიოს მასშტაბით, ყოველი სამი ინტერნეტ მომხმარებელიდან ერთი არასრულწლოვანია. იხ. *Macenaite M., Kosta E.*, Consent for Processing Children’s Personal Data in the EU: Following in US Footsteps?, Tilburg Institute for Law, Technology and Society (TILT), Tilburg University, Tilburg, Netherlands, 146, 2017, <<https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096>> [27.06.2022].

<sup>4</sup> *Office for Children’s Commissioner for England*, Children’s Commissioner’s Report Calls on Internet Giants and Toy Manufacturers to be Transparent About Collection of Children’s Data, 2018, <<https://www.childrenscommissioner.gov.uk/2018/11/08/childrens-commissioners-report-calls-on-internet-giants-and-toy-manufacturers-to-be-transparent-about-collection-of-childrens-data/#:~:text=The%20report%20calls%20on%20companies,collected%20and%20for%20what%20purposes>> [27.06.2022].

ციფრულ გარემოში,<sup>5</sup> ასაკის და დამუშავების პლატფორმის მიუხედავად, დაცული უნდა იყოს მათი პირადი ცხოვრების ხელშეუხებლობა და პერსონალური მონაცემები.<sup>6</sup>

როგორც ევროპული<sup>7</sup>, ასევე ამერიკული<sup>8</sup> საკანონმდებლო ნორმები ბავშვის პირადი ცხოვრების დაცვის მთავარ ფიგურად მშობელს მოიაზრებს.<sup>9</sup> თუმცა საკანონმდებლო დონეზე, როგორც წესი, არ არის მოწესრიგებული მშობლების მიერ შვილის პერსონალური მონაცემების დამუშავების სამართლებრივი ასპექტები მშობლის მხრიდან შვილის უფლებების შეზღუდვის ჭრილში. სასამართლო პრაქტიკა<sup>10</sup> ადასტურებს, რომ „მშობლის თვალით“ დანახული ბავშვის საუკეთესო ინტერესი ყოველთვის არ არის თანხვედრაში „შვილის თვალით“ დანახულ მის (ბავშვის) საუკეთესო ინტერესთან. შესაბამისად, თანამედროვე ეპოქაში გამოიკვეთა მშობლებისა და არასრულწლოვანი შვილების განსხვავებული მოლოდინები და შეხედულებები ციფრულ გარემოში არასრულწლოვანთა პერსონალური მონაცემების დაცულობის ასპექტში.

წინამდებარე კვლევის ფარგლებში, მშობლისა და მისი არასრულწლოვანი შვილის მოლოდინები განხილული იქნება მშობლების მიერ არასრულწლოვანი

---

<sup>5</sup> *Council of Europe, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment, Recommendation CM/Rec(2018)7 of the Committee of Ministers*, <<https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html>> [27.06.2022].

<sup>6</sup> პირადი ცხოვრების ხელშეუხებლობის უფლებისა და პერსონალური მონაცემების დაცვის უფლების ურთიერთკავშირზე დეტალურად იხ.: *საგინაშვილი ნ.*, პერსონალური მონაცემების დაცვა და პირადი ცხოვრების ხელშეუხებლობა, ადამიანის უფლებათა სტანდარტების გავლენა საქართველოს კანონმდებლობასა და პრაქტიკაზე, სტატიათა კრებული, *კორკელია კ. (რედ.)*, 2015, 166-19, <<http://ewmi-prolog.org/images/files/7110HRStandardsImpact.pdf>> [27.06.2022]; ასევე *Hustinx P.*, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, Collected Courses of the European University Institute's Academy of European Law, 24th Session on European Union Law, 1-12 July 2013, 2, <[https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive\\_en](https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en)> [27.06.2022]; *European Union Agency for Fundamental Rights and Council of Europe*, Handbook on European Data Protection Law, 2018, 20, <<https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition>> [27.06.2022].

<sup>7</sup> *Gligorijevic J.*, Children's Privacy: The Role of Parental Control and Consent, *Human Rights Law Review*, 2019, 19, 201-229, <<https://academic.oup.com/hrlr/article/19/2/201/5522387?login=true>> [27.06.2022].

<sup>8</sup> *Steinberg S. B.*, Sharenting: Children's Privacy in the Age of Social Media, 66 *Emory L.J.* 839, 2017, 861, <<https://scholarlycommons.law.emory.edu/elj/vol66/iss4/2/>> [27.06.2022].

<sup>9</sup> ანალოგიური მოწესრიგებაა ეროვნულ კანონმდებლობაშიც. იხ. „ბავშვის უფლებათა კოდექსის“ (5004-ის, 20/09/2019) 24-ე მუხლის მე-3 ნაწილი. ასევე, საქართველოს სამოქალაქო კოდექსის (საქართველოს პარლამენტის უწყებანი, 31, 24/07/1997) 1198-ე მუხლის მე-6 ნაწილი.

<sup>10</sup> „2017 წელს, 16 წლის არასრულწლოვანმა მიმართა სასამართლოს, მშობლის მიერ სოციალურ ქსელში მისი ფოტოს თანხმობის გარეშე განთავსების გამო. სასამართლომ მშობელს დაავალა ფოტოს წაშლა, წინააღმდეგ შემთხვევაში სანქციის სახით განუსაზღვრა ჯარიმა 10 000 ევროს ოდენობით. 2016 წელს ავსტრალიელმა თინეიჯერმა სარჩელი შეიტანა მშობლების წინააღმდეგ სასამართლოში, რომლებმაც ბოლო 7 წლის განმავლობაში განათავსეს 500-მდე „სამარცხვინო“ ფოტოები სოციალურ ქსელში, შვილის თანხმობის გარეშე“. იხილეთ ციტირება: *Goshadze K.*, Legal Implications of “Shattering”, *International Journal of Law: “Law And World”*, №15, Vol. 6, Issue 2, 2020, 5.

შვილების პერსონალური მონაცემების სოციალურ ქსელებში სისტემატური განთავსების („მარენტინგის“<sup>11</sup>) კონტექსტში. აღნიშნული საფრთხის ქვეშ აყენებს არასრულწლოვნის პირადი ცხოვრების ხელშეუხებლობის უფლებასა და ამ ჭრილში მათი პერსონალური მონაცემების დაცვას. ამ პროცესში, მშობლის ვარაუდი მისი ქმედების „უვნებელი“ ხასიათის შესახებ არ არის თანხვედრაში შვილის შეხედულებებთან და ინფორმაციის გავრცელების ობიექტურ საჭიროებებთან. მშობელი ვერ (არ) ამართლებს არასრულწლოვნის მიერ ჩამოყალიბებულ პერსონალურ მონაცემების დაცვის მოლოდინს.

კვლევის ფარგლებში, წარმოჩენილია საკითხის მნიშვნელობა, შეფასებულია „მარენტინგის“ უარყოფითი შედეგები და გავლენა არასრულწლოვნის უფლებრივ მდგომარეობაზე, იდენტიფიცირებულია პრობლემის გადაჭრის შესაძლო სამართლებრივი მექანიზმები.

კვლევა ეფუძნება შედარებით სამართლებრივ მეთოდს. ეროვნულ მოწესრიგებასთან ერთად, გაანალიზებულია პერსონალურ მონაცემთა დაცვის საკითხების მარეგულირებელი საერთაშორისო აქტები, ოფიციალური გზამკვლევები, რეკომენდაციები და მოსაზრებები, ასევე საერთაშორისო სასამართლო პრაქტიკა. მსჯელობის ფარგლებში, ცალკეულ საკითხებზე ასევე გაანალიზებულია ევროპის კავშირის წევრი ქვეყნების კანონმდებლობა და სასამართლო პრაქტიკა.

## 2. „მარენტინგი“ – მშობლის მიერ შექმნილი თანამედროვე საფრთხე არასრულწლოვნის პერსონალური მონაცემებისათვის

მშობლის მიერ სოციალურ ქსელში მისი არასრულწლოვანი შვილის შესახებ ინფორმაციის სისტემატური განთავსება, ბავშვის<sup>12</sup> ყოველდღიური ცხოვრების აღწერა ფოტოების, ვიდეოებისა და ბლოგების წარმოების ფორმით დღევანდელი ცხოვრების ჩვეული ნაწილია.<sup>13</sup> აღნიშნული, როგორც წესი, წარმოადგენს მშობლის სტატუსთან

<sup>11</sup> სიტყვა “Sharenting” გამომდინარეობს სიტყვების “parent” (მშობელი) და “share” (გაზიარება) კომბინაციიდან. მითითებულია: *Goshadze K.*, დასახელებული ნაშრომი, 1.

<sup>12</sup> „ბავშვის უფლებათა კოდექსის“ მიხედვით, ბავშვად მიიჩნევა პირი 18 წლის ასაკის მიღწევამდე (იხ. მე-3 მუხლის „ა“ ქვეპუნქტი). შესაბამისად, წინამდებარე კვლევაში თანაბარმნიშვნელოვნად არის გამოყენებული ტერმინები „ბავშვი“ და „არასრულწლოვანი“.

<sup>13</sup> *Siibak A.*, *Educating 21st Century Children*, Chapter 6, *Digital parenting and the Datafied Child*, Institute of Social Studies, University of Tartu, Estonia, 2019, <<https://www.oecd-ilibrary.org/sites/313a9b21-en/index.html?itemId=/content/component/313a9b21-en>> [28.06.2022]. “Google“-ის ყოფილი დირექტორის, *ერიკ შმიდტის* განმარტებით, როგორც პირადი მიზეზით, ასევე მშობლების დამსახურებით, გარკვეული დროის შემდეგ ჩვენ მივადწევთ ისეთ წერტილს, როდესაც თითოეულ ადამიანს ექნება სამარცხვინო ინფორმაცია და ფოტოები განთავსებული სოციალურ ქსელში. იხ. *Steinberg S. B.*, დასახელებული ნაშრომი, 855.

დაკავშირებული დადებითი ემოციების გაზიარების, ბავშვის აღზრდასთან დაკავშირებული გამოწვევების გამოხატვისა და ცალკეულ საკითხებზე რჩევებისა და რეკომენდაციების მიღების საშუალებას.<sup>14;15</sup>

„მარენტინგის“ მასშტაბები საკმაოდ ფართოა<sup>16</sup> და ზოგ შემთხვევაში ის ჯერ კიდევ ბავშვის დაბადებამდე იწყება.<sup>17</sup> კვლევები ცხადყოფს, რომ არასრულწლოვნები, ასაკის მატებასთან ერთად, განიცდიან დისკომფორტს მშობლების მიერ მათი პერსონალური მონაცემების გასაჯაროების გამო.<sup>18</sup> თუმცა იმის გათვალისწინებით, რომ ამ პრაქტიკის „მსხვერპლი“ არასრულწლოვნები ჯერ კიდევ პატარები არიან<sup>19</sup> და აკადემიურ წრეებში ამ საკითხებზე საუბარი ჯერ არ დაწყებულა,<sup>20</sup> საკითხი სამართლებრივად მოწესრიგებული არ არის.

ციფრულ გარემოში მონაცემების განთავსებისას მშობლები, როგორც წესი, ინფორმაციას კონკრეტულ აუდიტორიას უზიარებენ, თუმცა გადაზიარების ფუნქციის საშუალებით, მისი ფართო აუდიტორიისათვის ხელმისაწვდომობა მარტივად შესაძლებელია. ასევე, საძიებო სისტემების „ქეშირების“ ფუნქცია საშუალებას იძლევა განუსაზღვრელი ვადის შემდეგ მოხდეს ერთხელ გასაჯაროებული ინფორმაციის მოძიება.<sup>21</sup> ამდენად, ჩვენს მიერ სოციალურ ქსელში განთავსებული ინფორმაცია „უკიდევანო“ არეალში იკარგება, რაც ზრდის არასრულწლოვნების პერსონალური მონაცემების შელახვის რისკებს.

---

<sup>14</sup> Siibak A., დასახელებული ნაშრომი.

<sup>15</sup> ზოგიერთი მკვლევრის მოსაზრებით (მაგ. Lazard L. et al., Sharenting: Pride, Affect and the Day-to-Day Politics of Digital Mothering, *Social and Personality Psychology Compass*, Vol. 13/4, 2019, e12443,) მსგავსი ქმედებები „კარგი მშობლის“ სამაგალითო ფსიქოლოგიურ ტრენდადაც იქცა.

<sup>16</sup> მიჩიგანის უნივერსიტეტის მიერ ჩატარებული კვლევის მიხედვით, მშობლების 56% პოტენციურად სამარცხვინო ინფორმაციას აქვეყნებდა, 51%-ის მიერ განთავსებული ინფორმაცია ახდენდა ბავშვის ადგილმდებარეობის იდენტიფიკაციას კონკრეტული მომენტისათვის, ხოლო 27% აქვეყნებდა შეუფერებელ ფოტოებს. იხ. “Sharenting” Trends: Do Parents Share Too Much About Their Kids on Social Media? C.S. Mott Children’s Hospital, Mar. 16, 2015, მითითებულია: Steinberg S. B., დასახელებული ნაშრომი, 848.

<sup>17</sup> ორსული დედების ¼, ბავშვის დაბადებამდე ათავსებს ექსკოპიის ფოტოს სოციალურ ქსელში. იხ.: Steinberg S. B., დასახელებული ნაშრომი, 849.

<sup>18</sup> გაერთიანებულ სამეფოში, 2017 წელს ჩატარებული კვლევის მიხედვით, 12-16 ასაკობრივი კატეგორიის 1000 მოზარდიდან, 71.3 % მიიჩნევდა, რომ მშობლები პატივს არ სცემდნენ მათ პირადი ცხოვრების ხელშეუხებლობას ციფრულ გარემოში, ხოლო 39.8% თვლიდა, რომ მშობლებმა სამარცხვინო ფოტოები განათავსეს სოციალურ ქსელებში. იხ. Levy E., Parenting in the Digital Age: How Are We Doing?, *Parent Zone: Making the Internet Work for Families*, 2017, <chrome-extension://efaidhbmnnnibpcajpcgiclfndmkaj/https://parentzone.org.uk/sites/default/files/2021-12/PZ\_Parenting\_in\_the\_Digital\_Age\_2017.pdf> [26.06.2022].

<sup>19</sup> დღევანდელი ბავშვები არიან „გაციფრულებული ბავშვების“ პირველი თაობა. *United Nations Children’s Fund (UNICEF)*, *Children’s Online Privacy and Freedom of Expression: Industry Toolkit*, 2018, 4, <https://www.coursehero.com/file/95867628/UNICEF-Childrens-Online-Privacy-and-Freedom-of-Expression1pdf/> [28.06.2022].

<sup>20</sup> Siibak A., დასახელებული ნაშრომი.

<sup>21</sup> Steinberg S. B., დასახელებული ნაშრომი, 844, 850.

პირადი ცხოვრების ხელშეუხებლობის უფლების დარღვევის გამო ფსიქოლოგიური და ემოციური დისკომფორტის<sup>22</sup> გარდა, „შარენტიგს“ ასევე შესაძლოა მოჰყვეს კონკრეტული უარყოფითი შედეგები პიროვნების „ციფრული გატაცების“,<sup>23</sup> პედოფილიისა<sup>24</sup> და კრიმინალური ქმედებების<sup>25</sup> სახითაც.

## 2.1. სამართლებრივი მოწესრიგება

არასრულწლოვნის პირადი ცხოვრების ხელშეუხებლობის უფლება დაცულია არაერთი სამართლებრივი აქტით, როგორც ეროვნულ,<sup>26</sup> ასევე საერთაშორისო დონეზე.<sup>27</sup> პერსონალური მონაცემების დაცვის კონტექსტში, არასრულწლოვნის უფლებების დაცულობას ეროვნულ დონეზე უზრუნველყოფს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი (შემდგომში – „პერსონალურ მონაცემთა დაცვის კანონი“),<sup>28</sup> ხოლო საერთაშორისო დონეზე „პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპის საბჭოს 1981 წლის 28 იანვრის №108 კონვენცია (შემდგომში – „108-ე კონვენცია“).

მონაცემთა დაცვის ეროვნული კანონმდებლობა თავის მხრივ ეფუძნება ევროპარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის პერსონალურ მონაცემთა დაცვასა და ასეთი ტიპის მონაცემთა თავისუფალ გადაადგილებასთან მიმართებით ინდივიდების დაცვის თაობაზე დირექტივას (95/46/EC) (შემდგომში – „1995 წლის დირექტივა“). ეროვნულ დონეზე დღეს მოქმედი საკანონმდებლო ნორმების უმეტესი ნაწილი სწორედ 1995 წლის დირექტივის ტექსტს ეფუძნება. 2018 წელს, დირექტივა

<sup>22</sup> „მატრენინგიდან“ გამომდინარე ფსიქოლოგიური და ემოციური დისკომფორტის შესახებ დაწვრილებით იხ. *Siibak A., Lipu M., 'Take it down!': Estonian Parents' and Pre-teens' Opinions and Experiences with Sharenting, Media International Australia Incorporating Culture and Policy, 2019, 1–11, 4, 7, <[https://www.researchgate.net/publication/331411236\\_'Take\\_it\\_down'\\_Estonian\\_parents'\\_and\\_pre-teens'\\_opinions\\_and\\_experiences\\_with\\_sharenting](https://www.researchgate.net/publication/331411236_'Take_it_down'_Estonian_parents'_and_pre-teens'_opinions_and_experiences_with_sharenting)> [18.05.2022], აგრეთვე: *Goshadze K.*, დასახელებული ნაშრომი, 3.*

<sup>23</sup> ციფრული გატაცების (“digital kidnapping”) შესახებ, დაწვრილებით იხ. *Siibak A.*, დასახელებული ნაშრომი; ასევე *Steinberg S. B.*, დასახელებული ნაშრომი, 854.

<sup>24</sup> იხ. *Battersby L.*, Millions of Social Media Photos Found on Child Exploitation Sharing Sites, *Sydney Morning Herald*, Vol. 30, 2015, <<http://www.smh.com.au/national/millions-of-socialmedia-photos-found-on-child-exploitation-sharing-sites-20150929-gjxe55.html>> [28.06.2022].

<sup>25</sup> იხ.: *Donovan S.*, “Sharenting”: The Forgotten Children of the GDPR, *Peace Human Rights Governance*, 4(1), 2020, 42, <<http://phrg.padovauniversitypress.it/2020/1/2/>> [28.06.2022].

<sup>26</sup> საქართველოს კონსტიტუციის მე-15 მუხლი (საქართველოს პარლამენტის უწყებები, 31-33, 24/08/1999); ბავშვის უფლებათა კოდექსის მე-9 მუხლი.

<sup>27</sup> ბავშვის უფლებების შესახებ კონვენციის (02/07/1994, ვებგვერდი) მე-16 მუხლი; ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენციის (20/05/1999, 16/11/1999, 1950) მე-8 მუხლი.

<sup>28</sup> „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011.

ჩაანაცვლა მონაცემთა დაცვის ზოგადმა რეგულაციამ<sup>29</sup> (შემდგომში – „ზოგადი რეგულაცია“),<sup>30</sup> ხოლო რეგულაციასთან ეროვნული კანონმდებლობის შესაბამისობაში მოყვანის მიზნით, პარლამენტში წარდგენილ იქნა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ახალი პროექტი.<sup>31</sup>

შესაბამისად, „შარენტინგის“ სამართლებრივი მოწესრიგების ჭრილში საკითხის განხილვისათვის, გაანალიზებული იქნება ეროვნული კანონმდებლობის, ეროვნულ დონეზე ინიცირებული ცვლილებისა და ზოგადი რეგულაციის შესაბამისი ნორმები.

„პერსონალურ მონაცემთა დაცვის კანონის“ შესაბამისად, კანონის მოქმედების სფერო არ ვრცელდება „ფიზიკური პირის მიერ მონაცემთა აშკარად პირადი მიზნებისათვის დამუშავებაზე, როდესაც მათი დამუშავება დაკავშირებული არ არის მის სამეწარმეო ან პროფესიულ საქმიანობასთან;“<sup>32</sup> მსგავსი ფორმულირება არის წარმოდგენილი ზოგადი რეგულაციითაც, მათ შორის პირადი მიზნების განმარტების ნაწილში უშუალოდ „სოციალურ ქსელებში მოღვაწეობისა“ და „ინტერნეტ აქტივობის“ დაკონკრეტებით.<sup>33</sup>

შესაბამისად, ზემოაღნიშნული ფორმულირებების სიტყვა-სიტყვითი განმარტებიდან გამომდინარე, მშობლების მიერ არასრულწლოვანი შვილების პერსონალური მონაცემების ციფრულ გარემოში განთავსება<sup>34</sup> წარმოადგენს პირადი მიზნებისათვის მონაცემების დამუშავებას და მასზე არ ვრცელდება მონაცემთა დაცვის სამართლის ნორმები არც ეროვნული<sup>35</sup> და არც საერთაშორისო<sup>36</sup> მოწესრიგებით.

---

<sup>29</sup> General Data Protection Regulation (GDPR). რეგულაციის ოფიციალური ქართულენოვანი თარგმანი იხ. <<https://personaldata.ge/ka/legislation>> [28.06.2022].

<sup>30</sup> ქართულ იურიდიულ წრეებში აღნიშნულ დოკუმენტს ასევე მოიხსენიებენ *მონაცემთა დაცვის საერთო რეგულაციის* სახელწოდებით, თუმცა წინამდებარე ნაშრომის მიზნებისათვის, გამოყენებული იქნება სახელმწიფო ინსპექტორის სამსახურის მიერ მომზადებულ ოფიციალურ თარგმანში გამოყენებულია სახელწოდება „მონაცემთა დაცვის ზოგადი რეგულაცია“.

<sup>31</sup> რეგ. N07-3/353/9, თარიღი 22.05.2019.

<sup>32</sup> კანონის მე-3 მუხლის 3 „ა“ ქვეპუნქტი. პირადი მიზნებით დამუშავებას ასევე გამორიცხავდა 1995 წლის დირექტივა და 108-ე მოდერნიზებული კონვენციის 3.2 მუხლი.

<sup>33</sup> „...პირადი და ოჯახური საქმიანობა შეიძლება მოიცავდეს მიმოწერას და მისამართების შენახვას, სოციალურ ქსელებში მოღვაწეობას და ინტერნეტ აქტივობას, რომელიც ასეთი საქმიანობის კონტექსტში ხორციელდება“. ზოგადი რეგულაციის პრეამბულის მე-18 პარაგრაფი.

<sup>34</sup> მით უფრო რეგულაციის ნორმის ფორმულირებაში „სოციალურ ქსელებში მოღვაწეობას და ინტერნეტ აქტივობას“-ზე მითითების შემდეგ. ამასთან, 1995 წლის დირექტივის ტექსტი პირდაპირ მითითებას არ აკეთებდა სოციალურ ქსელში მოღვაწეობასა და ინტერნეტ აქტივობაზე.

<sup>35</sup> „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-3 მუხლის „ა“ პუნქტი.

<sup>36</sup> „2016 წელს მონაცემთა დაცვის ზოგადი რეგულაცია შემუშავდა იმ სულისკვეთებით, რომ დაცვის მაღალი სტანდარტი დაეწესებინა ინდივიდების (განსაკუთრებით ბავშვების) პერსონალური მონაცემების დაცვისათვის. თუმცა, რეგულაცია მცირეწლოვნების „ციფრულ პრივატულობას“ (digital privacy) ტოვებს მშობლების ხელში, მათი ციფრული კომპეტენციების მიუხედავად.“ „... რეგულაცია ნაკლებ ყურადღებას ამახვილებს პატარა ბავშვების პრივატულობის დაცვაზე, რომელთა პრივატულობაც ღიაა მშობლების მიერ ონლაინ პოსტების გათავისების პირობებში“. იხილეთ ციტირება: *Donovan S.*, დასახელებული ნაშრომი, 35, 36.

აღსანიშნავია, რომ მონაცემთა დაცვის ზოგადი რეგულაცია, განსაკუთრებულ ყურადღებას ამახვილებს ბავშვებზე<sup>37</sup> და მსგავსი განმარტებით, მონაცემთა დაცვის სამართლის ნორმების გაუვრცელებლობით, მშობლებისაგან დაუცველ მდგომარეობაში ხვდებიან „მარენტინგი“-ს მსხვერპლი არასრულწლოვანი შვილები,<sup>38</sup> რაც მონაცემთა დაცვის სამართლის პრინციპებიდან გამომდინარე, აზრს მოკლებულია.

ზოგადად, პირადი და საოჯახო მიზნებით დამუშავების კონტექსტში, მონაცემთა დაცვის სამართლის მოქმედების გაუვრცელებლობა განპირობებულია ჟურნალისტიკის, სახელოვნებო და ლიტერატურული გამონატულების ხელშეწყობის ისტორიული პრაქტიკით<sup>39</sup> და მიზნად ისახავს ინდივიდის გამონატვის თავისუფლების დაცვას.<sup>40</sup> მეორე მხრივ, გამონატვის თავისუფლების დაცვის სანაცვლოდ, არსებობს ინდივიდუალური ოჯახის წევრების პერსონალური მონაცემების დარღვევის რისკი.<sup>41</sup> შედეგად, სახეზე გვაქვს ამ ორი უფლების ურთიერთდაპირისპირება.<sup>42</sup>

ადამიანის უფლებების დაცვის ქრილში, ერთი მხრივ დაცული უნდა იყოს გამონატვის თავისუფლება, ხოლო მეორე მხრივ ოჯახის ცალკეული წევრის (ინდივიდის) უფლებები, მათი პირადი ცხოვრების ხელშეუხებლობისა და კონკრეტულად კი პერსონალური მონაცემების დაცულობის კონტექსტში. სამართლიანი ბალანსის დადგენისათვის, მართლმსაჯულების ევროპული სასამართლოს პრაქტიკით „პირადი და საოჯახო მიზნით დამუშავება“ მაქსიმალურად ვიწროდ განიმარტება.<sup>43</sup> ასეთი ვიწრო განმარტების სასამართლო პრაქტიკა არსებობდა როგორც 1995 წლის დირექტივის მოქმედების პერიოდში,<sup>44</sup> ასევე რეგულაციის არსებობის დროსაც.<sup>45</sup> სასამართლოს შეფასებით,

<sup>37</sup> იხ. ზოგადი რეგულაციის პრეამბულის 38-ე პარაგრაფი.

<sup>38</sup> *Donovan S.*, დასახელებული ნაშრომი, 39.

<sup>39</sup> *WP 29, Annex 2 Proposals for Amendments Regarding Exemption for Personal or Household Activities*, 1-2, <[https://ec.europa.eu/justice/article-29/documentation/other-document/index\\_en.htm](https://ec.europa.eu/justice/article-29/documentation/other-document/index_en.htm)> [28.06.2022]. WP29-ე სამუშაო ჯგუფის უფლებამოსილებთან და მნიშვნელობასთან დაკავშირებით იხ.: *ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო*, მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2019, 15.

<sup>40</sup> ამასთან, კერძო ინდივიდის მიერ განხორციელებული ყველა ქმედება ონლაინ სივრცეში არ წარმოადგენს ჟურნალისტიკის, სახელოვნებო ან ლიტერატურულ გამონატულებას.

<sup>41</sup> *Donovan S.*, დასახელებული ნაშრომი, 39.

<sup>42</sup> *WP 29, Annex 2 Proposals for Amendments Regarding Exemption for Personal or Household Activities*, 1-2.

<sup>43</sup> რეგულაციაშიც ასევე პირადი და საოჯახო მიზნით დამუშავების ვიწრო განმარტებას ემსახურება ნორმის ფორმულირების ტექსტში გამოყენებულია ტერმინი „წმინდა“ [“purely”]. იხ. რეგულაციის პრეამბულის მე-18 ნაწილი.

<sup>44</sup> იხ. “*Bodil Lindqvist*” საქმე (სქოლიო 47). ამ საქმის განხილვა მოხდა 1995 წლის დირექტივის საფუძველზე, რომლის ტექსტში პირდაპირ არ იყო მითითებული სოციალური მედიის ფარგლებში საქმიანობა, როგორც პირადი მიზნებით საქმიანობის ერთ-ერთი სახე (იხ. დირექტივის მე-3 მუხლის მე-2 ნაწილი).

<sup>45</sup> “*Sergejs Buivids v. the Augstākā Tiesa*”-ის საქმე, იხ. სქოლიო 49. რეგულაციის ფორმულირებაში ფორმულირებაში პირდაპირ არის მითითებული სოციალური მედია. (იხ. რეგულაციის პრეამბულის მე-18 ნაწილი).



ვიწრო განმარტების საჭიროება გამომდინარეობს ევროპის კავშირის ძირითად უფლებათა ქარტილიდან.<sup>46</sup>

მართლმსაჯულების ევროპული სასამართლოს პრაქტიკით, ვიწრო განმარტების ერთ-ერთი მთავარი საკვანძო კრიტერიუმია მონაცემების გავრცელების ფარგლები. სასამართლომ “Lindqvist”<sup>47</sup>-ის საქმეზე დაადგინა, რომ „ბლოგის“ ტიპის ვებგვერდის გზით მონაცემების პირთა განუსაზღვრელი წრისათვის გავრცელება არ წარმოადგენს „აშკარად პირადი მიზნებით დამუშავებას“<sup>48</sup> და შესაბამისად ხვდება 1995 წლის დირექტივის მოქმედების ფარგლებში. ასევე “Sergejs Buivids”-ის<sup>49</sup> საქმეზე, სასამართლომ დაადასტურა ასეთი ვიწრო ინტერპრეტაცია.<sup>50</sup> მსგავსი განმარტება შენარჩუნდა მონაცემთა დაცვის ზოგადი რეგულაციის ძალაში შესვლის შემდეგაც – ნიდერლანდების პირველი ინსტანციის სასამართლომ,<sup>51</sup> არ ჩათვალა ბების (მოპასუხე) მიერ შვილიშვილის ფოტოსურათის “Facebook” და “Pinterest” გვერდებზე განთავსება აშკარად პირადი მიზნებით დამუშავებად, რადგანაც: ა) სახეზე არ იყო მცირეწლოვანი ბავშვის მშობლის (მოსარჩელის) თანხმობა და ბ) ბების “Facebook” და “Pinterest” გვერდებით გაზიარებული ინფორმაცია შესაძლებელია მოხვედრილიყო მესამე პირთა ხელში.<sup>52</sup> აღნიშნული გადაწყვეტილებით, სასამართლო პრაქტიკით, კიდევ ერთხელ დადასტურდა, „პირადი და საოჯახო მიზნებით დამუშავების“ ვიწრო ინტერპრეტაცია.

ონლაინ სივრცეში არასრულწლოვნის ინფორმაციის ციფრულ გარემოში გავრცელებისას პირადი მიზნებით დამუშავების „გამონაკლისიდან“ „გამოყვანას“ განამტკიცებს ასევე ზოგიერთი ქვეყნის საკანონმდებლო მოწესრიგებაც.<sup>53</sup>

სასამართლო პრაქტიკისგან განსხვავებით, 29-ე სამუშაო ჯგუფი<sup>54</sup> პირადი მიზნებით დამუშავების „გამონაკლისის“ შეფასებისას უფრო ფართო განმარტებას აკეთებს და მხოლოდ გავრცელების ფარგლების კრიტერიუმს არ ეფუძნება. აღნიშნულმა ორგანომ განსაზღვრა კრიტერიუმები, რომელთა კომბინაციითაც, შეიძლება იდენტიფიცირება, რამდენად ხვდება კონკრეტული დამუშავება პირადი მიზნებით დამუშავების

---

<sup>46</sup> მართლმსაჯულების ევროპულმა სასამართლომ საქმეზე CJEU, Case C- 212/ 13, *Ryneš* [2014] განმარტა, რომ „ქარტიის მე-7 მუხლის შესაბამისად, გადახვევები და შეზღუდვები პერსონალური მონაცემების დაცულობის კონტექსტში უნდა იყოს გამოყენებული მხოლოდ მაშინ, როცა ის მკაცრად საჭიროა“. იხ. გადაწყვეტილების §48.

<sup>47</sup> CJEU, Case C-101/01, *Bodil Lindqvist*, [2003].

<sup>48</sup> გადაწყვეტილების §31.

<sup>49</sup> CJEU, C-345/17 – *Buivids*, [2019].

<sup>50</sup> იხ. გადაწყვეტილების §43.

<sup>51</sup> 2020 წლის 13 მაისის გადაწყვეტილება.

<sup>52</sup> მოპასუხეს არ ჰქონდა დაყენებული უსაფრთხოების შესაბამისი პარამეტრები. საქმის დეტალები იხ.: *Fenech Farrugia Fiott Legal*, <<https://www.fff-legal.com/the-household-exemption-in-gdpr/>> [01.07.2022].

<sup>53</sup> მაგ., დანიის კანონმდებლობით, 16 წლამდე არასრულწლოვნის ფოტოების ინტერნეტსივრცეში განთავსებამდე, სავალდებულოა მისი კანონიერი წარმომადგენლ(ებ)ის თანხმობა. იხ. *Fenech Farrugia Fiott Legal*, <<https://www.fff-legal.com/the-household-exemption-in-gdpr/>> [01.07.2022].

<sup>54</sup> WP29, Annex 2 Proposals for Amendments Regarding Exemption for Personal or Household Activities, 4.

„გამონაკლისის“ ფარგლებში. ამ კრიტერიუმებს შორის, გავრცელების პირთა წრე ერთ-ერთი პარამეტრია,<sup>55</sup> თუმცა არა განმსაზღვრელი. 29-ე სამუშაო ჯგუფის შეფასებით, მხოლოდ გავრცელების ფარგლების კრიტერიუმზე დაყრდნობა არ შეიძლება, რადგანაც დაპირისპირებული უფლებების (დამმუშავებლის მხარეზე – გამოხატვის თავისუფლება, ხოლო მონაცემთა სუბიექტის მხარეს – პერსონალური მონაცემების დაცვა (ავტ.)) შეფასების კუთხით, ასევე ლოგისტიკური კუთხით, სოციალური ქსელების მომხმარებლებისა და ბლოგერების მონაცემთა დაცვის სამართლის მოქმედების სფეროში სრული მოცულობით შეყვანა შეუძლებელია.<sup>56</sup> მხოლოდ გავრცელების ფარგლების კრიტერიუმზე დაყრდნობით, ასეთი კატეგორიის დამუშავებაც მოხვდება მონაცემთა დაცვის სამართლის ნორმების მოქმედების სფეროში, რაც გაართულებს მონაცემთა დაცვის სამართლის პრინციპებისა და ნორმების იმპლემენტაციასა და საზედამხედველო ორგანოების მიერ მათ შესრულებაზე კონტროლს.

შესაბამისად, გამოხატვის თავისუფლების უფლებასა და ოჯახის წევრების პირადი ცხოვრების ხელშეუხებლობის უფლებებს შორის სამართლიანი ბალანსის დადგენისათვის, 29-ე სამუშაო ჯგუფმა განსაზღვრა პირადი მიზნებით დამუშავებისას ზოგადი რეგულაციის გავრცელების შემდეგი შესაძლებლობები:

- ა) რეგულაციის საბაზო უსაფრთხოების მოთხოვნების დაცვა „მსუბუქი“ ფორმით;
- ბ) სხვა ინდივიდის წვდომის,<sup>57</sup> გასწორებისა<sup>58</sup> და დავიწყების უფლებების<sup>59</sup> პატივისცემა;<sup>60</sup>
- გ) დამუშავებისას მონაცემთა დაცვის პრინციპების დაცვა (მონაცემების სანდოობა და სიახლე);
- დ) დამუშავების საფუძვლის არსებობა;
- ე) სხვა პირების ინფორმირება, მათი მონაცემების განთავსების შესახებ, რათა მათ ჰქონდეთ მონაცემების წაშლის მოთხოვნის შესაძლებლობა.<sup>61</sup>

<sup>55</sup> გამონაკლისის შეფასებისათვის, გავრცელების პირთა წრესთან ერთად, 29-ე სამუშაო ჯგუფი აღგენს სხვა პარამეტრებსაც, როგორცაა „ეკუთვნის თუ არა პერსონალური მონაცემები ისეთ პირს, ვისაც არ აქვს პირადი ან საოჯახო ურთიერთობა დამმუშავებელთან“; „განთავსების სიხშირე და მასშტაბი ხომ არ ქმნის პროფესიული ან სრული დატვირთვის საქმიანობის ვარაუდს“, „არის თუ არა სახეზე ინდივიდზე პოტენციური გავლენის მოხდენის შესაძლებლობა, მათ შორის პრივატულობაში ჩარევის ფორმით“. იხ.: WP29, Annex 2 Proposals for Amendments Regarding Exemption for Personal or Household Activities, 4.

<sup>56</sup> იქვე.

<sup>57</sup> Right to Access. იხ. მონაცემთა დაცვის ზოგადი რეგულაციის მე-14 მუხლი, პერსონალურ მონაცემთა დაცვის შესახებ კანონის 22-ე მუხლი.

<sup>58</sup> Right to Rectification. იხ. მონაცემთა დაცვის ზოგადი რეგულაციის მე-16 მუხლი, მუხლი, პერსონალურ მონაცემთა დაცვის შესახებ კანონის 22-ე მუხლი.

<sup>59</sup> Right to erasure (“right to be forgotten”) იხ. მონაცემთა დაცვის ზოგადი რეგულაციის მე-17 მუხლი, მუხლი, პერსონალურ მონაცემთა დაცვის შესახებ კანონის 22-ე მუხლი.

<sup>60</sup> მაგალითად, მეგობარმა მოგთხოვათ სოციალური ქსელიდან ფოტოს ჩამოხსნა. *Donovan S.*, დასახელებული ნაშრომი, 36.

<sup>61</sup> WP 29, Annex 2 Proposals for Amendments Regarding Exemption for Personal or Household Activities, 5. ასევე, 29-ე სამუშაო ჯგუფის მოსაზრებით, საზედამხედველო ორგანოებს უნდა ჰქონდეთ მოკვლევის ჩატარების

ზემოაღნიშნულიდან გამომდინარე, მონაცემთა დაცვის სამართალი „სრული მოცულობით“ ვერ გავრცელდება „შარენტინგის“ შემთხვევებზე პირადი მიზნებით დამუშავების გამონაკლისის არსებობის გამო. ამასთან, მისი გაუვრცელებლობა აშკარად შელახავს არასრულწლოვანების პერსონალური მონაცემების დაცვის უფლებას. შესაბამისად, „შარენტინგი“ არ უნდა განიმარტოს, როგორც პირადი მიზნებით დამუშავება (ვიწრო განმარტების შესაბამისად) იმ შემთხვევაში, როცა ინფორმაციის მიმღები პირთა წრე განუსაზღვრელი ან ძალიან ფართეა.

თუმცა ამ შემთხვევაშიც, მონაცემთა დაცვის სამართალი უნდა გავრცელდეს არა სრულად,<sup>62</sup> არამედ მხოლოდ „მსუბუქი“ ფორმით – კონკრეტულ სამართლებრივ მექანიზმებზე დაყრდნობით.

## **2.2. პრევენციის სამართლებრივი მექანიზმები**

წინამდებარე კვლევის ფარგლებში წარმოდგენილია „შარენტინგის“ პრევენციის სამი სამართლებრივი მექანიზმი: ა) არასრულწლოვანის თანხმობა; ბ) არასრულწლოვანის მიერ „დავიწყების უფლების“ გამოყენება და გ) არასრულწლოვანის მიერ ზიანის ანაზღაურების მოთხოვნის უფლება. მექანიზმების განხილვისას, შეფასებულია მათი დადებითი და უარყოფითი მხარეები. კვლევაში მექანიზმები წარმოდგენილია მათი ეფექტიანობის პრიორიტეტულობით – ყველაზე ეფექტიანობიდან ნაკლებად ეფექტიანობისკენ.

### **2.2.1. არასრულწლოვანის თანხმობა**

არასრულწლოვანებთან მიმართებით სამართლებრივი ურთიერთობის თითქმის ყველა სიბრტყეში, მშობელი (კანონიერი წარმომადგენელი) მოიაზრება არასრულწლოვანის საუკეთესო ინტერესის განმახორციელებლად. აღნიშნული

---

შესაძლებლობა, რათა განსაზღვრონ, მიეკუთვნება თუ არა დამუშავება პირადი მიზნებით დამუშავებას. ევროპის კავშირის არაერთი ქვეყნის კანონმდებლობით (მაგ. საფრანგეთი - the French Act No. 2018-493 of 20 June 2018, art.2.3 <<https://www.dataguidance.com/notes/france-data-protection-overview>> [05.05.2022]; გერმანია - Federal Data Protection Act of 30 June 2017, art. 2.3 <<https://www.dataguidance.com/notes/germany-data-protection-overview>> [05.05.2022]), პირადი და საოჯახო მიზნით მონაცემების დამუშავებაზე არ ვრცელდება მონაცემთა დაცვის ეროვნული სამართალი. თუმცა, ცალკეულ შემთხვევებში, ვრცელდება საზედადამხედველო ორგანოს უფლებამოსილება მოკვლევის განხორციელების კონტექსტში. იხ. W/P 29, Annex 2 Proposals for Amendments Regarding Exemption for Personal or Household Activities, 1.

<sup>62</sup> სრულ გავრცელებაში მოიაზრება ყველა პრინციპისა და საფუძვლის, ანგარიშვალდებულებისა და სხვა ყველა სავალდებულო მოთხოვნის დაცვა. სრული გავრცელება ფაქტობრივად შეუძლებელია და ვერ მოხდება მისი კონტროლი და სათანადო ლოჯისტიკა. შესაბამისად ნორმა იქნება უმოქმედო.

გარკვეულწილად ეფუძნება კერძო სამართლით განმტკიცებულ შეზღუდული ქმედუნარიანობის ინსტიტუტს, რაც კანონიერი წარმომადგენლის ნების გამოვლენას (წინასწარი თანხმობა ან შემდგომი მოწონება) უკავშირებს არასრულწლოვნის მიერ გამოვლენილი ნების ნამდვილობას.<sup>63</sup>

მსგავსი მოწესრიგება არის წარმოდგენილი არასრულწლოვნის პერსონალური მონაცემების დაცვის კონტექსტშიც.<sup>64</sup> ამასთან, ციფრულ გარემოში მშობლის უფლება გადაწყვიტოს და აკონტროლოს შვილის ინფორმაციის გავრცელების ფარგლები, უნდა დაექვემდებაროს გარკვეულ შეზღუდვებს. განსხვავებით სამოქალაქოსამართლებრივი ურთიერთობებისაგან, როცა არასრულწლოვნის „დამოუკიდებელმა“ ნების გამოვლენამ, შესაძლოა ზიანი მიაყენოს როგორც თავად არასრულწლოვანს, ასევე სამოქალაქო ბრუნვის სხვა მონაწილეებს, „მარენტინგის“ შემთხვევაში ასეთი „ზიანი“ პრაქტიკულად არ არსებობს.<sup>65</sup>

კვლევები ცხადყოფს,<sup>66</sup> რომ მშობლებისა და შვილების შეხედულებებს შორის ციფრულ გარემოში ინფორმაციის განთავსებამდე მშობლის მიერ შვილის თანხმობის მოპოვების თვალსაზრისით, აზრთა დიდი სხვაობაა. მშობლები, როგორც წესი, არ იღებენ თანხმობას მათი შვილებისაგან, ხოლო შვილების მიერ პროტესტის გამოხატვის შემთხვევაში, არ ახდენენ მასზე რეაგირებას. აღნიშნული კი იწვევს „პრივატულობის საზღვრების ტურბულენტობას“ მშობლებსა და შვილებს შორის. იქმნება ინტერესთა დისბალანსი, რაც იწვევს ურთიერთობის დაძაბულობას.

ავტორთა ნაწილი<sup>67</sup> მიიჩნევს რომ, მშობელმა სრულად უნდა დაიცვას შვილის პრივატულობა და არ უნდა გაამჟღავნოს მისი ინფორმაცია, მეორე ნაწილის<sup>68</sup> შეფასებით კი უპირატესობა უნდა მიენიჭოს ბავშვზე ორიენტირებული პერსპექტივიდან გამომდინარე მშობლის უფლებას,<sup>69</sup> რაც მოიაზრებს მშობლისათვის მინიჭებული უფლებამოსილების განხორციელებას შვილის საუკეთესო ინტერესების ქრილში.

<sup>63</sup> იხ. საქართველოს სამოქალაქო კოდექსის 63-ე მუხლის პირველი ნაწილი.

<sup>64</sup> იხ. ზოგადი რეგულაციის პრეამბულის 38-ე ნაწილი და მე-8 მუხლი, ხოლო ეროვნულ დონეზე - ინიცირებული კანონპროექტის მე-7 მუხლი.

<sup>65</sup> ამასთან, სამოქალაქოსამართლებრივ ურთიერთობებშიც არსებობს გარკვეული ფარგლები, როდესაც არასრულწლოვნები თავისუფლები არიან თავის ნების გამოვლენაში (როდესაც პირი გარიგებით იღებს სარგებელს (მაგ. ჩუქების ხელშეკრულების დადებისას), ასევე ემანსიპაციის შემთხვევაში (იხ. საქართველოს სამოქალაქო კოდექსის 65-ე მუხლი).

<sup>66</sup> Siibak A., Lipu M., დასახელებული ნაშრომი, 3.

<sup>67</sup> Sorensen S., Protecting Children’s Right To Privacy In The Digital Age: Parents as Trustees of Children’s Rights. Children’s Legal Rights Journal 36(3), 2016, 202–203. მითითებულია Siibak A., Lipu M., დასახელებული ნაშრომი, 3.

<sup>68</sup> Steinberg S. B., Sharenting: Children’s Privacy in the Age of Social, Gainesville, FL: UF Law Scholarship Repository, University of Florida Levin College of Law, 2017, მითითებულია Siibak A., Lipu M., დასახელებული ნაშრომი, 3.

<sup>69</sup> “Child-centred Perspective on Parents’ Rights’. ციტირებულია: Siibak A., Lipu M., დასახელებული ნაშრომი, 4.

კვლევის მიხედვით,<sup>70</sup> მშობლების ნაწილი (მიუხედავად იმისა, რომ ინფორმირებულები არიან შვილის პროტესტის შესახებ) კვლავ აგრძელებენ „შარენტინგის“ პრაქტიკას. მშობლების გარკვეული კატეგორიის აზრით, ბავშვები ჯერ ახალგაზრდები არიან და მათი აზრი მნიშვნელოვანი არ არის „შარენტინგის“ პროცესში. ასევე ზოგიერთი მიიჩნევს, რომ მათ როგორც მშობელს, აქვთ შვილის ინფორმაციაზე სრული კონტროლის უფლება<sup>71</sup> (შესაბამისად, თანხმობის მიღებაც არ არის საჭირო (ავტ.)) თუმცა, გარკვეული ნაწილი ცვლის საკუთარ პრაქტიკას შვილისაგან თანხმობის მიღების კონტექსტში<sup>72</sup> (და იღებს თანხმობას შვილისაგან (ავტ.)).

თანხმობის მიღების ვალდებულების ფორმირების შესაძლებლობას ამყარებს „ბავშვის უფლებების შესახებ“ კონვენციის მე-12 მუხლი, ასევე ბავშვის უფლებათა კოდექსის მე-14 მუხლი.

ბავშვის უფლებათა კოდექსის შესაბამისად, განსაზღვრულია ბავშვის საუკეთესო ინტერესი<sup>73</sup>, შესაბამისად, ზემოაღნიშნული ნორმების საფუძველზე, შეიძლება დავასკვნათ, რომ ბავშვის პერსონალური მონაცემები დაცვა ასევე წარმოადგენს მისი ინტერესის საგანს, რომელიც უნდა დაცული იქნეს მშობლის მიერ ბავშვის მონაწილეობითა და მოსაზრებების გათვალისწინებით.<sup>74,75</sup>

რამდენადაც, მშობელთა ნაწილი თანახმაა, რომ თანხმობა მიიღოს მისი შვილებისაგან, საზოგადოებრივი ცნობიერების ამაღლება (უარზე მყოფი მშობლების მიდგომების შეცვლის მიზნით) და საკანონმდებლო დონეზე არასრულწლოვნის

---

<sup>70</sup> იხ. სქოლიო 66.

<sup>71</sup> Siibak A., Lipu M., დასახელებული ნაშრომი, 7.

<sup>72</sup> Siibak A., Lipu M., დასახელებული ნაშრომი, 8.

<sup>73</sup> კოდექსის მე-3 მუხლის „თ“ პუნქტი.

<sup>74</sup> პერსონალური მონაცემების დამუშავების კონტექსტში, ბავშვის საუკეთესო ინტერესებზე აქცენტს აკეთებს ასევე, სახელმწიფო ინსპექტორის სამსახური. „ბავშვების მონაცემების დამუშავებელმა პირებმა უპირველეს ყოვლისა უნდა გაითვალისწინონ ბავშვის საუკეთესო ინტერესები. ყველა საჯარო და კერძო დაწესებულება ვალდებულია უზრუნველყოს არასრულწლოვანთა პერსონალური მონაცემების კანონიერი დამუშავება და ისეთი დარღვევების პრევენცია, რომლებმაც შესაძლოა გამოიწვიოს ბავშვის ღირსების შელახვა, მისი სტიგმატიზაცია, ბულინგი, დისკრიმინაცია ან ნეგატიური გავლენა მის ემოციურ მდგომარეობასა და განვითარებაზე. ტექნოლოგიური პროგრესის პირობებში არასრულწლოვანთა პირადი ცნობების ხელშეუხებლობის უფლებამ კიდევ უფრო მეტი მნიშვნელობა შეიძინა, რადგან ახალ შესაძლებლობებთან ერთად იზრდება ამ უფლებაში გაუმართლებელი ჩარევის საფრთხეები“. „არასრულწლოვანთა პერსონალური მონაცემების დამუშავება“, სახელმწიფო ინსპექტორის გადაწყვეტილებები, 2020, 4 <<https://personaldata.ge/>> [03.07.2022].

<sup>75</sup> სწორედ ბავშვის საუკეთესო ინტერესებზე დაფუძნებით, მისთვის მშობლისაგან „ცალკე მდგომი“ უფლებების მინიჭება განხორციელდა 2012 წელს, ირლანდიის კონსტიტუციის 31-ე ცვლილებით. (ცვლილების შესახებ დაწვრილებით იხ.: *Donovan S.*, დასახელებული ნაშრომი, 2020, 39, 43).

ზოგიერთი ავტორი ასეთი უფლების მინიჭების შესაძლებლობას განსაზღვრავს ასევე ინგლისური სამართლისთვისაც (მითითებულია: *Bessant C.*, *Sharenting: Balancing the Conflicting Rights of Parents and Children*, *Journal of Communications Law*, Vol. 23, 2018, 20, <[https://www.researchgate.net/publication/325594690\\_Sharenting\\_Balancing\\_the\\_conflicting\\_rights\\_of\\_parents\\_and\\_children](https://www.researchgate.net/publication/325594690_Sharenting_Balancing_the_conflicting_rights_of_parents_and_children)> [03.07.2022].

თანხმობის სავალდებულოების განსაზღვრა, საკითხის რეგულირებას ერთ-ერთ ყველაზე ეფექტიან მექანიზმს წარმოადგენს.

ამასთან, თანხმობის შესაბამისი ასაკის განსაზღვრისათვის, მნიშვნელოვანია რამდენიმე ფაქტორის მხედველობაში მიღება – მშობლების შეფასებით, მათ (მშობლებს) აქვთ შვილის ინფორმაციის კონტროლის უფლება, განსაკუთრებით კი როცა ბავშვი პატარაა. შესაბამისად, თანხმობის საჭიროება უნდა დადგეს იმ ასაკიდან, როდესაც ბავშვი საკმაოდ მომწიფებულია, რომ შეაფასოს მისი ინფორმაციის განთავსების „ბედი“, ხოლო ამავდროულად „საშუალო მშობელი“ უნდა მიიჩნევდეს, რომ მისი შვილი საკმაოდ დიდია, რათა მისგან მიიღოს თანხმობა მისი ინფორმაციის განთავსებაზე.<sup>76</sup> მომწიფებულობის დონეზე ყურადღებას ამახვილებს ასევე ბავშვის უფლებათა კოდექსი.<sup>77</sup>

ამასთან, სამართლებრივი ურთიერთობების სხვადასხვა სიბრტყეებში არის დადგენილი გამონაკლისები, არასრულწლოვნების მიმართ მშობლის უპირატესი უფლებისაგან. არასრულწლოვანს შეუძლია თავად მიიღოს გადაწყვეტილება სამართლებრივი ურთიერთობის სხვადასხვა საკითხებზე, კანონიერი წარმომადგენლის ჩარევის გარეშე.<sup>78</sup> მსგავსი გამონაკლისი არსებობს ელექტრონული მომსახურების შეთავაზების ეტაპზეც. მონაცემთა დაცვის ზოგადი რეგულაციით, 13-დან 16 წლამდე ასაკი განისაზღვრა პერიოდად, როცა ბავშვებს მინიჭებული აქვთ უფლება, პირდაპირ მიიღონ ელექტრონული მომსახურება კანონიერი წარმომადგენლის თანხმობის გარეშე.<sup>79</sup> კანონპროექტის მიხედვით, ეს ასაკი არის 14 წელი.

ზემოაღნიშნულიდან გამომდინარე, რაკი მონაცემთა დაცვის საერთაშორისო კანონმდებლობა 13 წლიდან მიიჩნევს არასრულწლოვანს სათანადოდ მომწიფებულად, რომ მისთვის შეთავაზებული ელექტრონული მომსახურებით ისარგებლოს კანონიერი წარმომადგენლის თანხმობის გარეშე, ანალოგიური მომწიფებულობის ხარისხი ივარაუდება, ციფრულ გარემოში მის შესახებ ინფორმაციის განთავსებაზე თანხმობის გამოსატყვის ასაკადაც.<sup>80</sup> შესაბამისად, 13 წელი შესაძლოა, განისაზღვროს როგორც ზღვარი, რის შემდეგაც მშობელს წარმოეშობა ვალდებულება მიიღოს შვილისაგან

<sup>76</sup> მშობლის აზრის გათვალისწინება ერთ-ერთი მნიშვნელოვანი ფაქტორია. როგორც ზემოთ აღინიშნა, მშობლები მიიჩნევენ რომ მათ აქვთ არასრულწლოვანი შვილის ინფორმაციაზე სრული კონტროლის უფლება (იხ. სქოლიო 66).

<sup>77</sup> იხ. მე-5 მუხლის მე-2 ნაწილი.

<sup>78</sup> იხ.: „პაციენტის უფლებების შესახებ“ საქართველოს კანონის (სსმ, 19, 25/05/2000) მე-4 მუხლის მე-2 ნაწილის „ბ“ და „გ“ ქვეპუნქტები; საქართველოს სამოქალაქო კოდექსის 65-ე და 1196-ე მუხლები.

<sup>79</sup> ეს ასაკი ქვეყნების მიხედვით მერყეობს 13-დან 15 წლამდე მონაკვეთში. ევროპის ქვეყნების მიხედვით თანხმობის ასაკები იხ.: <<https://euconsent.eu/digital-age-of-consent-under-the-gdpr/>> [03.07.2022].

<sup>80</sup> წინამდებარე კვლევის საგანს წარმოადგენს არა კონკრეტული ასაკის დადგენა, არამედ არასრულწლოვნის სავალდებულო თანხმობის სახით სამართლებრივი მექანიზმის შეთავაზება „მარნეტიზმის“ უარყოფითი შედეგების თავიდან აცილებისათვის. კონკრეტული ასაკი უნდა განისაზღვროს დარგის სხვა სპეციალისტების მიერ.

თანხმობა მისი პერსონალური მონაცემების ციფრულ გარემოში განთავსების შესახებ, როცა ასეთი განთავსება განპირობებულია მხოლოდ მშობლის გამონატვის თავისუფლებით.<sup>81</sup> აქვე აღსანიშნავია, რომ ბავშვისათვის მინიჭებული უფლება, თანხმობა განაცხადოს მშობლის მიერ მის შესახებ ინფორმაციის განთავსებაზე, დამოკიდებული უნდა იყოს როგორც ბავშვის ასაკზე, ასევე განთავსებული ინფორმაციის ხასიათზე. შესაბამისად, ინფორმაციის ხასიათის გათვალისწინებით (მაგალითად, სამედიცინო ხასიათის ინფორმაციის განთავსება „ბლოგის“ ტიპის ვებგვერდზე) ბავშვის მიერ თანხმობის გაცემის ასაკი შესაძლოა დაიწყოს უფრო მცირე ასაკიდანაც (მაგალითად, 10 წლიდან),<sup>82</sup> რამეთუ მონაცემთა ბუნებიდან გამომდინარე,<sup>83</sup> ასეთი ტიპის ინფორმაციის გასაჯაროებამ შეიძლება, სერიოზულად დააზიანოს მისი ემოციური მდგომარეობა ან არასასურველი შედეგი გამოიწვიოს ბავშვის სამომავლო პროფესიული და პირადი ცხოვრებისათვის.

ბუნებრივია რომ, დაინტერესებული მხარეების<sup>84</sup> ჩართულობის გარეშე ეს ბერკეტი მხოლოდ საკანონმდებლო ცვლილებით (კონკრეტული ასაკის მითითებით) ვერ ამუშავდება.<sup>85</sup> ბავშვის საუკეთესო ინტერესებიდან გამომდინარე შექმნილი საზიარო პასუხისმგებლობის ფარგლებში, მშობელმა, კერძო და საჯარო ორგანიზაციებმა ერთად უნდა იკისრონ პასუხისმგებლობა ციფრულ გარემოში ბავშვის უფლებების დაცვისათვის.<sup>86</sup> საზოგადოების ცნობიერების ამაღლება<sup>87</sup> ამ საზიარო პასუხისმგებლობის გამონატვის ერთ – ერთი ფორმაა. განსაკუთრებული აქცენტი უნდა გაკეთდეს შშმ პირებზე და სხვა მოწყვლად ჯგუფებს მიკუთვნებულ ბავშვებზე.<sup>88</sup>

---

<sup>81</sup> ამ შემთხვევაში სახეზე არ უნდა იყოს ბავშვის ინტერესებიდან გამომდინარე, სხვა აუცილებელი საჭიროება. მაგ. საკანონმდებლო ვალდებულების ან ბავშვის სასიცოცხლო ინტერესის საფუძვლით ინფორმაციის საჯაროდ განთავსება.

<sup>82</sup> ეროვნული კანონმდებლობის ანალიზის საფუძველზე შეიძლება ითქვას რომ, 10 წელი წარმოადგენს გარდამტეხ ასაკს ბავშვის მომწიფებულობის ხარისხის განსაზღვრის მიზნებისათვის. კერძოდ, საქართველოს სამოქალაქო კოდექსის მიხედვით, პირის დელიქტუნარიანობა იწყება 10 წლის ასაკიდან (იხ. 994-ე მუხლის პირველი ნაწილი); გვარის შეცვლის შემთხვევაში, 10 წლიდან სავალდებულოა ბავშვის თანხმობა (იხ. 1196-ე მუხლი), ხოლო ბავშვის უფლებათა კოდექსის მიხედვით, ხოლო 10 - დან 18 წლამდე ბავშვი ითვლება მოზარდად (იხ. კოდექსის მე-3 მუხლის „ბ“ პუნქტი).

<sup>83</sup> იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-2 მუხლის „ბ“ პუნქტი.

<sup>84</sup> სახელმწიფო, კერძო სექტორი, მშობლები, არასამთავრობო სექტორი.

<sup>85</sup> ციფრულ გარემოში ბავშვთა უფლებების დაცვის პროცესში დაინტერესებული მხარეების ჩართულობის როლსა და მნიშვნელობაზე იხ.: *Council of Europe, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment.*

<sup>86</sup> *United Nations Children’s Fund (UNICEF), Children’s Online Privacy and Freedom of Expression: Industry Toolkit, 7; Council of Europe, Recommendation CM/Rec (2018)7, 11.*

<sup>87</sup> არასრულწლოვნების უფლებების დაცვის მიზნით, “Public Health Model“-ის გამოყენება პოპულარული მეთოდია. მეთოდი ეფუძნება საზოგადოებრივი ცნობიერების ამაღლებით კონკრეტული შედეგის მიღებას. “Public Health Model“-ის შესახებ დაწვრილებით იხ.: *Steinberg S., დასახელებული ნაშრომი, 866.*

<sup>88</sup> *Council of Europe, Recommendation CM/Rec (2018)7, 11, 14.*

არასრულწლოვნის თანხმობის, როგორც „მარნტინგის“ პრევენციის ერთ-ერთი მექანიზმის ეფექტიანობის კიდევ ერთ ნაკლოვანებას წარმოადგენს „საჯარო ფიგურის“ არასრულწლოვანი შვილების შემთხვევაში „თანხმობის სავალდებულოების“ არაეფექტიანობა. საჯარო ფიგურის არასრულწლოვან შვილებს, მათი სტატუსიდან გამომდინარე, აქვთ თმენის ვალდებულება მშობლების მიერ მათი ფოტოების განთავსების შესახებ.<sup>89</sup> შესაბამისად, ამ ნაწილში თანხმობის გაცემის წესები შესაძლოა, განსხვავებულად მოწესრიგდეს.<sup>90</sup>

### 2.2.2 არასრულწლოვნის მიერ „დავიწყების უფლების“ გამოყენება

„მარნტინგის“ უარყოფითი შედეგების თავიდან არიდების ერთ-ერთ ალტერნატიულ მექანიზმს წარმოადგენს არასრულწლოვანისათვის მონაცემთა დაცვის სამართლით განსაზღვრული „დავიწყების უფლების“ მინიჭება.<sup>91</sup> პირადი ცხოვრების ხელშეუხებლობის უფლების დაცულობის კონტექსტში, შედეგობრივად არასრულწლოვნის წინასწარი თანხმობა უფრო ეფექტიანი მექანიზმია,<sup>92</sup> თუმცა „დავიწყების უფლების“ გამოყენება შესაძლოა, ნაკლებად ეფექტიან, თუმცა ერთ-ერთ ალტერნატიულ გზად განვიხილოთ.

არასრულწლოვანისათვის „დავიწყების უფლების“ მინიჭების მაგალითს წარმოადგენს კალიფორნიის შტატის კანონმდებლობა. აღნიშნული შტატი, რომელიც წარმოადგენს ლიდერს ციფრული გარემოში პრივატულობის დაცვის კუთხით, მცირეწლოვნებს აძლევს უფლებას, მოითხოვონ მათი მონაცემების წაშლა ონლაინ ფორუმებიდან.<sup>93</sup> მართალია, ეს ეხება მათ მიერ განთავსებულ ინფორმაციას, მაგრამ ანალოგიის კუთხით შეიძლება, გამოყენებულ იქნეს მშობლების მიერ განთავსებულ ინფორმაციაზეც.

ამასთან, ციფრული გარემოს სპეციფიკის გათვალისწინებით, მშობლების მიერ გაზიარებული ინფორმაცია იკარგება „უკიდევანო“ სივრცეში, ხშირია ინფორმაციის

<sup>89</sup> Steinberg S., დასახელებული ნაშრომი, 859.

<sup>90</sup> აღნიშნული საკითხი არ არის განხილული წინამდებარე ნაშრომის ფარგლებში, რადგანაც წარმოადგენს დამოუკიდებელი კვლევის საგანს.

<sup>91</sup> ასევე, ცნობილია როგორც მონაცემების წაშლის უფლება. იხ: <<https://gdpr.eu/right-to-be-forgotten/>> [03.07.2022]. „დავიწყების უფლება“ არაპირდაპირი ფორმით არსებობდა ჯერ კიდევ 1995 წლის დირექტივაში. მოგვიანებით, მისი ფორმალიზაცია განხორციელდა რეგულაციის ძალაში შესვლის შემდეგ (იხ. რეგულაციის მე-17 მუხლი). „დავიწყების უფლება“ განსაკუთრებით პოპულარული გახდა ადამიანის უფლებათა ევროპული სასამართლოს მიერ 2014 წელს “Google Spain”-ის საქმეზე (Case of Google Spain, [2014], ECHR, C-131/12) მიღებული გადაწყვეტილების შემდეგ, რომელმაც რეგულაციით განსაზღვრული „დავიწყების უფლების“ ერთგვარი პრეცედენტი შექმნა.

<sup>92</sup> თანხმობის შემთხვევაში, არასრულწლოვნის უფლებები პრევენციულად დაცულია.

<sup>93</sup> Steinberg S., დასახელებული ნაშრომი, 864.



მეორადი გამოყენებაც. შედეგად, ზოგჯერ, არასრულწლოვანს არ შეუძლია სთხოვოს მშობელს ინტერნეტში განთავსებული ინფორმაციის წაშლა.<sup>94</sup> ასევე რთულია „დავიწყების უფლების“ რეალიზაციის ტექნიკური მხარეც.<sup>95</sup> შესაბამისად, თანხმობასთან შედარებით, „დავიწყების უფლების“ გამოყენება შესაძლოა განვიხილოთ „შარენტინგის“ უარყოფითი შედეგების თავიდან აცილების ერთ-ერთ ნაკლებად ეფექტიან მექანიზმად.

### 2.2.3 არასრულწლოვნის მიერ ზიანის ანაზღაურების მოთხოვნის უფლება

არასრულწლოვნის მიერ ზიანის ანაზღაურების მოთხოვნის უფლება, „შარენტინგის“ უარყოფითი შედეგების მაკომპენსირებელ საშუალებას წარმოადგენს. ზოგადად, ყველა ბავშვს აქვს ზიანის ანაზღაურების მოთხოვნის უფლება, როცა მისი უფლებები ილახება.<sup>96</sup> თუმცა არასრულწლოვნის თანხმობის მექანიზმისგან განსხვავებით, ზიანის ანაზღაურების მოთხოვნის მექანიზმი არ ახდენს საკითხის პრევენციას და არც „დავიწყების უფლების“ მსგავსად „აჩერებს“ არასრულწლოვანისათვის მიყენებული „ზიანის გამომწვევ“ წყაროს. შესაბამისად, მისი დატვირთვის „სიმსუბუქიდან“ გამომდინარე, ის ნაკლებად პრიორიტეტული, თუმცა ერთ-ერთი ალტერნატიული მექანიზმია.

არასრულწლოვნის მიერ ზიანის ანაზღაურების მოთხოვნის უფლება საერთაშორისო დონეზე განმტკიცებულია „ბავშვის უფლებების შესახებ“ კონვენციის მე-12 მუხლის მე-2 ნაწილით, ეროვნულ დონეზე კი – საქართველოს სამოქალაქო კოდექსის მე-18 მუხლით, რომელიც პირადი არაქონებრივი უფლებების დაცვის საფუძველს ქმნის<sup>97</sup> და ბავშვის უფლებათა კოდექსის მე-13 მუხლის პირველი ნაწილით.

თუმცა შვილის მიმართ მშობლის განსაკუთრებული სტატუსიდან გამომდინარე, გასაჩივრების შესაძლებლობა, გარკვეულწილად, შეზღუდულია. მაგალითად, ამერიკული დელიქტური სამართლის მიხედვით, შვილის მიერ მშობლის წინააღმდეგ ზიანის ანაზღაურების მოთხოვნით სარჩელის შეტანის შესაძლებლობა, სამეცნიერო ლიტერატურაში განხილული არ არის,<sup>98</sup> ხოლო ზოგიერთი შტატი საერთოდ ზღუდავს

---

<sup>94</sup> *Steinberg S.*, დასახელებული ნაშრომი, 875.

<sup>95</sup> *Ambrose M. L., Ausloos J.*, დასახელებული ნაშრომი, 18.

<sup>96</sup> Committee on the Rights of the Child, General Comment no. 5; Human Rights Committee, General Comment No. 5; United Nations Human Rights Council, Resolution on the Rights of the Child: Access to justice, A/HRC/25/L.10, 25 March 2014, მითითებულია: *United Nations Children's Fund (UNICEF)*, *Children's Online Privacy and Freedom of Expression: Industry Toolkit*, 10.

<sup>97</sup> *Goshadze K.*, დასახელებული ნაშრომი, 4.

<sup>98</sup> *Porter E. G.*, *Tort Liability in the Age of the Helicopter Parent*, 64 ALA. L. REV. 533, 537 (2013). მითითებულია: *Steinberg S.*, დასახელებული ნაშრომი, 875.

არასრულწლოვანი შვილის მიერ მშობლის წინაშე სარჩელის შეტანის უფლებას.<sup>99</sup> ასევე, საქართველოს შემთხვევაში, ამკრძალავი ნორმის არარსებობის მიუხედავად, ნაკლებად წარმოსადგენია შვილის მიერ ამ უფლების გამოყენება.<sup>100</sup>

### 3. დასკვნა

„თანამედროვე ბავშვი იბადება და იზრდება სამყაროში, რომელიც ტექნოლოგიური პროცესებით ზედმიწევნით კონტროლდება, აანალიზდება და მანიპულირდება“.<sup>101</sup> ამ პირობებში კითხვის ნიშნის ქვეშ დგება „ციფრული ბავშვების“<sup>102</sup> პირადი ცხოვრების ხელშეუხებლობის უფლება და პერსონალური მონაცემების დაცვის საკითხები. მით უფრო, როცა ამ უფლების დარღვევის პროვოცირებას თავად მშობელი ახდენს.

წინამდებარე კვლევის ფარგლებში წარმოჩენილი პრობლემა გამოიხატება მშობლის მიერ შვილის პერსონალური მონაცემების სოციალური ქსელებში სისტემატური განთავსებით („შარენტინგით“). შედეგად, რისკის ქვეშ დგება ბავშვის როგორც არსებული, ასევე სამომავლო<sup>103</sup> უფლებრივი მდგომარეობა. ამავდროულად, „შარენტინგის“ პრაქტიკით, ერთმანეთს უპირისპირდება მშობლის გამომხატვის თავისუფლება და ბავშვის პირადი ცხოვრების ხელშეუხებლობის უფლებები.<sup>104</sup>

კვლევის შედეგად გამოიკვეთა, რომ პირადი მიზნებით მონაცემების დამუშავების ვიწრო ინტერპრეტაციის პირობებში, მშობლის მიერ არასრულწლოვანი შვილის შესახებ ინფორმაციის სოციალურ ქსელებში გავრცელების მონაცემთა დაცვის სამართლის ნორმების მოქმედების ქვეშ მოქცევით, შესაძლებელი ხდება „შარენტინგის“ უარყოფითი შედეგების თავიდან აცილება, ხოლო ზოგ შემთხვევაში – შემცირება. ამ მიმართულებით კვლევის ფარგლებში განხილულია შემდეგი სამართლებრივი მექანიზმები: არასრულწლოვანის სავალდებულო თანხმობა, არასრულწლოვანის მიერ „დავიწყების უფლების“ გამოყენება და ზიანის ანაზღაურების მოთხოვნის მექანიზმის გამოყენება. ზემოაღნიშნული მექანიზმები განსხვავებული სიძლიერით უზრუნველყოფენ „შარენტინგის“ პირობებში არასრულწლოვანის უფლებრივი წონასწორობის შენარჩუნებას და ამ კონტექსტში მისი პერსონალური მონაცემების დაცვლობას.

<sup>99</sup> *Wingerter I.*, Parent-Child Tort Immunity, 50 LA. L. REV. 1131 (1990). მითითებულია: *Steinberg S.*, დასახელებული ნაშრომი, 875.

<sup>100</sup> *Goshadze K.*, დასახელებული ნაშრომი, 5.

<sup>101</sup> ციტირებულია: *Wilson M.* (2019), 'Raising the ideal child? Algorithms, quantification and prediction', *Media, Culture & Society*, 41(5), 620-636. შემდგომი მითითებით: *Donovan S.*, დასახელებული ნაშრომი, 40.

<sup>102</sup> "Datafied child". დეტალებისათვის იხ. სქოლიო 19.

<sup>103</sup> „შარენტინგის“ უარყოფითი შედეგები შეიძლება არ იყოს იმწუთიერი. ციტირებულია: *Donovan S.*, დასახელებული ნაშრომი, 43

<sup>104</sup> *Steinberg S.*, დასახელებული ნაშრომი, 869.

## ბიბლიოგრაფია:

1. საქართველოს კონსტიტუცია, საქართველოს პარლამენტის უწყებები, 31-33, 24/08/1999.
2. „ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის“ კონვენცია, 20/05/1999.
3. „პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპის საბჭოს №108 კონვენცია, 1981.
4. „ბავშვის უფლებების შესახებ“ კონვენცია, 02/07/1994.
5. „საქართველოს სამოქალაქო კოდექსი“, საქართველოს პარლამენტის უწყებანი, 31, 24/07/1997.
6. „ბავშვის უფლებათა კოდექსი“, 5004-ის, 20/09/2019.
7. „პაციენტის უფლებების შესახებ“ საქართველოს კანონი, სსმ, 19, 25/05/2000.
8. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011.
9. ევროპარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის პერსონალურ მონაცემთა დაცვასა და ასეთი ტიპის მონაცემთა თავისუფალ გადაადგილებასთან მიმართებით ინდივიდების დაცვის თაობაზე დირექტივას (95/46/EC);
10. საგინაშვილი ნ., პერსონალური მონაცემების დაცვა და პირადი ცხოვრების ხელშეუხებლობა, ადამიანის უფლებათა სტანდარტების გავლენა საქართველოს კანონმდებლობასა და პრაქტიკაზე, სტატიათა კრებული, კორკელია კ. (რედ.), 2015, 166-191;
11. ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო, მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2019, 15.
12. არასრულწლოვანთა მონაცემების დამუშავება, სახელმწიფო ინსპექტორის სამსახურის გადაწყვეტილებები, 2020, 4;
13. Regulation (EU) 2016/679 of the European Parliament and of 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 Protection Regulation), OJ L 119, 4/5/2016, 1–88.
14. Battersby L., Millions of Social Media Photos Found on Child Exploitation Sharing Sites, Sydney Morning Herald, Vol. 30, 2015, <<http://www.smh.com.au/national/millions-of-social-media-photos-found-on-child-exploitation-sharing-sites-20150929-gjxe55.html>> [28.06.2022].

15. *Donovan S.*, “Sharenting”: The Forgotten Children of the GDPR’, *Peace Human Rights Governance*, 4(1), 2020, 36, 39–43.
16. *European Union Agency for Fundamental Rights and Council of Europe*, *Handbook on European data protection law*, 2018, 20.
17. *Gligorijevi’ C. J.*, Children’s Privacy: The Role of Parental Control and Consent, *Human Rights Law Review*, 2019, 19, 201–229.
18. *Goshadze K.*, Legal Implications of “Shattering”, *International Journal of Law: “Law And World”*, № 15, Vol. 6, Issue 2, December 2020, 1-5.
19. *Hustinx P.*, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, *Collected Courses of the European University Institute's Academy of European Law*, 24th Session on European Union Law, 1-12 July 2013, 2.
20. *Joshua N.*, *Why Do People Still Think Data Is the New Oil?* Center for Data Innovation, January 16, 2018. *Livingstone S.*, *Children: A Special Case for Privacy?*, *InterMEDIA*, International Institute of Communications, July 2018, Vol 4, 6, Issue 2.
21. *Levy E.*, *Parenting in the Digital Age: How Are We Doing?*, *Parent Zone: Making the Internet Work for Families*, 2017, <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://parentzone.org.uk/sites/default/files/2021-12/PZ\_Parenting\_in\_the\_Digital\_Age\_2017.pdf> [26.06.2022].
22. *Macenaite M.*, *Kosta E.*, *Consent for Processing Children’s Personal Data in the EU: Following in US Footsteps?*, *Tilburg Institute for Law, Technology and Society (TILT)*, Tilburg University, Tilburg, Netherlands, 146, 2017, <https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096> [27.06.2022].
23. *Schwartz P. M.*, *Property, Privacy, and Personal Data*, 117 *Harv. L. Rev.* 2004, 2056.
24. *Siiibak A.*, *Lipu M.*, ‘Take it down!’: Estonian Parents’ and Pre-teens’ Opinions and Experiences with Sharenting, *Media International Australia Incorporating Culture and Policy*, February 2019 1–11, 2019, 3-4, 7.
25. *Steinberg S. B.*, *Sharenting: Children's Privacy in the Age of Social Media*, 66 *Emory L.J.* 839, 2017, 844, 848-849, 850, 854-855, 861.
26. *Council of Europe*, “Guidelines to respect, protect and fulfil the rights of the child in the digital environment,” *Recommendation CM/Rec(2018)7 of the Committee of Ministers”*.
27. *WP 29*, *Annex 2 Proposals for Amendments regarding exemption for personal or household Activities*.
28. *Office for Children’s Commissioner for England*, *Children’s Commissioner’s Report Calls on Internet Giants and Toy Manufacturers to be Transparent About Collection of Children’s Data*, 2018.
29. *United Nations Children’s Fund (UNICEF)*, *Children’s Online Privacy and Freedom of Expression: Industry Toolkit*, 2018, 4, 7, 10.

30. *Siibak A.*, *Educating 21st Century Children*, Chapter 6. Digital parenting and the datafied child, Institute of Social Studies, University of Tartu, Estonia, 2019.
31. *CJEU*, Case C-101/01, *Bodil Lindqvist*, [2003];
32. *Google Spain*, [2014], ECHR, C-131/12;
33. *CJEU*, Case C- 212/ 13, *Ryneš* [2014];
34. *CJEU*, C-345/17 – *Buivids*, [2019].
35. <[www.ec.europa.eu](http://www.ec.europa.eu)> [28.06.2022].
36. <[www.fff-legal.com](http://www.fff-legal.com)> [01.07.2022].
37. <[www.dataguidance.com](http://www.dataguidance.com)> [05.05.2022];
38. <[www.euconsent.eu](http://www.euconsent.eu)> [03.07.2022].
39. <[www.gdpr.eu](http://www.gdpr.eu)> [03.07.2022].
40. <[www.personaldata.ge](http://www.personaldata.ge)> [03.07.2022].

## კორპორაციული მართვის სისტემაში მონაცემთა დაცვის ოფიცრის ინსტიტუციური როლის ინტერდისციპლინური ანალიზი

მსხვილი კორპორაციების მიერ პერსონალურ მონაცემთა სისტემური და ფართომასშტაბიანი დამუშავების მზარდმა ტენდენციამ განაპირობა პერსონალურ მონაცემთა დაცვის საკანონმდებლო მოწესრიგების გაძლიერება, განსაკუთრებით კი მონაცემთა სუბიექტების უფლებებისა და ინტერესების დაცვის თვალსაზრისით. მონაცემთა დაცვის ოფიცრის ინსტიტუტი, რომელიც მართალია, ეროვნულ კანონმდებლობაში ჯერ-ჯერობით არ არის ასახული, მონაცემთა დამუშავების კანონიერების, კორპორაციისა და მონაცემთა სუბიექტის ინტერესების თანაფარდობის უზრუნველყოფის ერთგვარი მექანიზმია. წინამდებარე ნაშრომი ამ ინსტიტუტის ინტერდისციპლინურ გააზრებას ეთმობა, ერთი მხრივ, საკორპორაციო სამართლის პერსპექტივით, ხოლო მეორე მხრივ — პერსონალურ მონაცემთა დაცვის სამართლის თვალსაზრისით, რათა განისაზღვროს მისი ინსტიტუციური ფუნქცია კერძო სამართლის იურიდიული პირის ორგანიზაციულ სტრუქტურაში.

**საკვანძო სიტყვები:** კორპორაციული მართვა, მონაცემთა დაცვა, მონაცემთა დაცვის ოფიცერი, მონაცემთა დაცვის ზოგადი რეგულაცია.

### 1. შესავალი

პოზიტიურსამართლებრივი დებულებები დროში თვითმყოფად არსებობას სამართალშემოქმედებითი ტრანსფორმაციის ძალით განაგრძობს. ქართული

---

\* ივ. ჯავახიშვილის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის დოქტორანტი, კერძო სამართლის მიმართულების ასისტენტი; პერსონალურ მონაცემთა დაცვის სამსახურის საერთაშორისო ურთიერთობების, ანალიტიკისა და სტრატეგიული განვითარების დეპარტამენტის უფროსი.

სამართლის ევროპულ სამართალთან ჰარმონიზაციაზე მსჯელობის საზრისი, ალბათ, შემდეგ კითხვაზე პასუხის ძიებით იწყება: სამართალი გარდაქმნის საზოგადოებას თუ პირიქით — საზოგადოება გარდაქმნის მას? სოციუმის საყოველთაო კეთილდღეობას სამართალი, როგორც დროში განვითარებადი სისტემა, ქცევის სავალდებულო დებულებების განსაზღვრით ქმნის.<sup>1</sup> თუმცა თვალსაჩინოა, რომ თავისუფალი საბაზრო ეკონომიკის აღზევებას, ინდუსტრიათა და ეკონომიკური აქტორების თვითრეგულირება, ხოლო დეკოდიფიკაციის შემდგომ — სოციალურ-ეკონომიკურ ურთიერთობათა თვითნებური მოწესრიგება მოჰყვა<sup>2</sup>. ეს უფრო სპონტანურად, „მოთხოვნისა და მიწოდების პრინციპის“ გამო, ერთი მხრივ, კონკურენტუნარიანობის შესანარჩუნებლად, მეორე მხრივ კი სოციალური პასუხისმგებლობის ზეწოლით განხორციელდა.<sup>3</sup> სწორედ ამგვარად ჩამოყალიბდა კორპორაციების ნებაყოფლობითი ანგარიშვალდებულებაც სამოქალაქო საზოგადოების წინაშე.

თანამედროვე ტენდენციების გათვალისწინებით, მეგა-კორპორაციების ეკონომიკური საქმიანობის მასშტაბითა და ზეგავლენის თვალსაზრისით, კანონმდებლის ყურადღების ეპიცენტრში „დაკავშირებულ პირთა“<sup>4</sup>, მათ შორის, მომხმარებელების და რაც მთავარია, წარმოდგენილი კვლევის ინტერესიდან გამომდინარე — მონაცემთა სუბიექტების უფლებრივი მდგომარეობა ექცევა. საკანონმდებლო მოწესრიგების სიხისტე სწორედ კორპორაციათა სამეწარმეო საქმიანობის „დაინტერესებულ პირთა“ ინტერესებზე ზეგავლენის ხარისხით ფასდება და ყალიბდება. მაშასადამე, ნათელია, იმპერტიული მოწესრიგების გზით, თუ რატომ ადგენს, ერთი მხრივ, საკორპორაციო სამართალი, ხოლო მეორე მხრივ — პერსონალურ მონაცემთა დაცვის სამართალი კორპორაციების მიმართ გარკვეულ ორგანიზაციულსამართლებრივ ვალდებულებებს. სწორედ ამგვარ მოთხოვნათა რიცხვს განეკუთვნება მონაცემთა დაცვის ოფიცრის ინსტიტუტის ინტეგრირება კორპორაციული მართვის სისტემაში.

მონაცემთა დაცვის ოფიცერი კორპორაციულსამართლებრივი მნიშვნელობით შიდაორგანიზაციული სტრუქტურის ინტეგრალური ელემენტია, ხოლო პერსონალურ

<sup>1</sup> Bentham J., *Of Laws in General*, Hart H. L. A. (ed.), 1970, 31-33.

<sup>2</sup> Magnier V., *Comparative Corporate Governance, Legal Perspectives*, 2017, 1-4. ამ მიზანს გამოხატავს კორპორაციული მართვის „რბილი მოწესრიგების“ რეჟიმი, რომელიც ევროპის კომისიის წინაშე პროფ. პოლ დევისის მიერ 1997 წელს იქნა წარდგენილი იმ იდეით, რომ კომისიას განესაზღვრა სუპრანაციონალური კორპორაციული მართვის სტანდარტი, ხოლო თითოეულ წევრ ქვეყანას „დაემორჩილე ან განმარტეს“ პრინციპით ეხელმძღვანელა ნაციონალური სამართლის ფარგლებში, Johnson A., *Soft Law*, in: *EC Regulation of Corporate Governance*, UK, 2009, 343-347.

<sup>3</sup> Picciotto S., *Regulating Global Corporate Capitalism*, 2011, 61-65, 193-200.

<sup>4</sup> სამეცნიერო ლიტერატურაში მოცემული „დაკავშირებულ პირთა“ (“Stakeholder”) ტერმინოლოგიური განმარტება იძლევა იმის შესაძლებლობას, რომ მასში მონაცემთა სუბიექტიც იყოს მოაზრებული, რამეთუ მასში იგულისხმება ნებისმიერი ისეთი პირი, რომლის ინტერესზე კორპორაციის საქმიანობა ზეგავლენის მომხდენია. იხ. *მახარობლიძევილი გ.*, კორპორაციული მართვის ზოგადი ანალიზი, 2015, 313-317.

მონაცემთა დაცვის სამართლის პერსპექტივიდან — მონაცემთა კანონიერი დამუშავებისა და მონაცემთა სუბიექტის უფლებების დაცვის ერთგვარი გარანტი. შესაბამისად, წინამდებარე კვლევის მიზანია შემდეგი თეზისის ქეშმარიტების დადგენა: მონაცემთა დაცვის ოფიცერი უზრუნველყოფს კორპორაციისა და მონაცემთა სუბიექტის ინტერესებისა და უფლებების გონივრულ თანაფარდობას.

კვლევის ინტერდისციპლინური ხასიათი საკორპორაციო სამართლისა და პერსონალურ მონაცემთა დაცვის სამართლის ურთიერთდაკავშირების ერთგვარი მცდელობის შედეგია. და რაკი „[...] ყოველგვარი შეცნობა არის განმარტება“<sup>5</sup>, საკვლევი საკითხისა და დარგის ცნებითი კატეგორიების გადმოსაცემად, ნაშრომი დესკრიფციული ხასიათისაა; გამოყენებულია ანალიტიკურ-სინთეზური მეთოდი შუალედური შედეგების ერთიან სისტემაში ფორმულირებისა და კვლევის მიზანთან მათი ლოგიკური კავშირის წარმოსაჩენად.

## **2. პერსონალურ მონაცემთა დაცვაზე ორიენტირი, როგორც კორპორაციული მართვის თანამედროვე მოდელი**

ლიტერატურაში გამოთქმული პოზიციის თანახმად, არამატერიალური ეკონომიკის აღზევების ეპოქამ განაპირობა კაპიტალიზმის არსებობა კაპიტალის გარეშე.<sup>6</sup> პერსონალური მონაცემები სწორედ ასეთი არამატერიალური, თანამედროვე ტიპის კაპიტალია. მონაცემთა კანონიერი დამუშავების ვალდებულება კორპორაციის მიერ სათანადო ტექნიკური და ორგანიზაციული ღონისძიებების გატარებას, შესაბამისი შიდაორგანიზაციული სტრუქტურის ფორმირებასა და მართვის სისტემის დანერგვას საჭიროებს. კორპორაციული მართვა თავისი არსით არის საკუთრების (სამეწარმეო საზოგადოებაში განხორციელებული აქციონერული კაპიტალის) და კონტროლის (გაერთიანებულ კაპიტალზე მართვის უფლებამოსილების მქონე ორგანოს) გამიჯვნის, მართვისა და ხელმძღვანელობის იმგვარი სისტემა, რომელშიც გათვალისწინებულია აქციონერთა და დაინტერესებულ პირთა სამართლებრივი ინტერესები.<sup>7</sup> მართვის აღნიშნული სისტემა, ორგანიზაციული თვალსაზრისით შესაძლებელია, განხორციელდეს მონისტური ან დუალისტური სქემით.<sup>8</sup>

---

<sup>5</sup> იასკესრი კ., ფილოსოფიის შესავალი, გორგიშელი ვ. (თარგმ.), 2019, 73.

<sup>6</sup> იხ. Haskel J., Westlake S., Capitalism without Capital: The Rise of the Intangible Economy, 2018, 3-10.

<sup>7</sup> ბურდული ი., მახრობლიძვილი გ., თოხაძე ა., ზუბიტაშვილი ნ., ალადაშვილი გ., მადრაძე გ., ეგნატაშვილი დ., საკორპორაციო სამართალი, 2022, 634-638.

<sup>8</sup> აღნიშნულს რიგ შემთხვევაში საწესდებო ავტონმია, ხოლო რიგ შემთხვევაში საკანონმდებლო მოთხოვნა უდევს საფუძვლად, იხ. მუხლები 124 და 182, „მეწარმეთა შესახებ“ საქართველოს კანონი, 875-Vრს-XXმპ, 02/08/2021.



კორპორაციულ მართვის სისტემას გააჩნია რამდენიმე სახის მოდელი, რომელიც გამოხატავს მის ძირითად ორიენტირს (*მაგალითად, არსებობს მენეჯერული მოდელი, აქციონერთა ქონებრივი მდგომარეობის მაქსიმიზაციაზე ორიენტირებული მოდელი, დასაქმებულ პირთა და დაინტერესებულ პირთა ინტერესების დაცვაზე ორიენტირებული მოდელი*).<sup>9</sup> ვიწრო გაგებით მოდელებს შორის სხვადასხვაობა განპირობებულია სწორედ კორპორაციის მმართველობითი პოლიტიკითა და სტრატეგიით, უფრო განზოგადებით კი — იმ გარემოს ეკონომიკური და სამართლებრივი ფაქტორებით, რომლის ფარგლებში ოპერირებს კორპორაცია.<sup>10</sup> შესაბამისად, თითოეული კორპორაციის მართვის მოდელი ინდივიდუალური სამეწარმეო საქმიანობის სფეროსა და მენეჯერული პოლიტიკის მიხედვით განსხვავდება. პერსონალურ მონაცემთა დაცვის ორიენტირით კორპორაციული მართვის განხორციელება ზემოხსენებულ მოდელთა ერთ-ერთ ნაირსახეობად შეიძლება შეფასდეს. ამგვარი მოდელი განსაკუთრებით საგულისხმოა ისეთი ეკონომიკური აქტორებისათვის, რომლებიც ახორციელებენ პერსონალური მონაცემების განსაკუთრებულად დიდი ოდენობით დამუშავებას, ასევე, რომელთა სამეწარმეო საქმიანობა არსებით ზეგავლენას ახდენს მონაცემთა სუბიექტების ინტერესებზე.

კორპორაციული მართვის ფუნდამენტური პრინციპებიდან<sup>11</sup> ერთ-ერთს წარმოადგენს გახსნილობა და გამჭვირვალობა, რომელიც ითვალისწინებს კორპორაციის ფინანსურ მდგომარეობასთან, მმართველობით სტრუქტურასთან, მართვასა და მენეჯმენტთან დაკავშირებული ინფორმაციის დროულ გამჟღავნებას. საგულისხმოა, რომ მონაცემთა დამუშავების პრინციპებიდან ერთ-ერთი სწორედ გამჭვირვალობის უზრუნველყოფას შეეხება, რომელიც ავალდებულებს დამმუშავებელს, უზრუნველყოს მონაცემთა სუბიექტისთვის მარტივი წვდომა ნებისმიერ ისეთ ინფორმაციაზე, რომელიც მონაცემთა დამუშავებას უკავშირდება.<sup>12</sup> აღსანიშნავია, რომ ევროპის საბჭოს კანონმდებლობაც<sup>13</sup> ადგენს მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის ანგარიშვალდებულების მოვალეობას და დამატებით ვალდებულებებს პერსონალურ მონაცემთა ეფექტიანი

<sup>9</sup> Tokhadze A., Enhancement of Corporate Social Responsibility – An Analysis from the Perspective of Economic and Sectoral Cooperation under the Three Association Agreements, in: Legal Aspects of the EU Association Agreements with Georgia, Moldova and Ukraine in the Context of the EU Eastern Partnership Initiative, Trunk A., Panych N., Rieckhof S. (eds.), 2017, 104-106.

<sup>10</sup> მახრობლიძეილი გ., კორპორაციული მართვის ზოგადი ანალიზი, 2015, 161, 162-163.

<sup>11</sup> G20/OECD, Principles of Corporate Governance, 2015.

<sup>12</sup> პრეამბულა, §39, Regulation (EU) 2016/679 of the European Parliament and of 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 Protection Regulation), OJ L 119, 4/5/2016, 1–88. მე-4 მუხლის 1-ლი პუნქტის „ა“ ქვეპუნქტი, მე-15 მუხლი „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011.

<sup>13</sup> §84, Article 10, Council of Europe, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf(2018)15-final), 18/05/2018.

დაცვის უზრუნველსაყოფად.<sup>14</sup> ამგვარ ღონისძიებათა ერთ-ერთ ფორმად მონაცემთა დაცვის ოფიცრის ინსტიტუტი მიიჩნევა.<sup>15</sup>

მაშასადამე, მონაცემთა დაცვაზე ორიენტირებული კორპორაციული მართვის მოდელს მეწარმე სუბიექტის სამეწარმეო საქმიანობის სფერო, მის ფარგლებში პერსონალური მონაცემის დამუშავების ინტენსივობა და მოცულობა აყალიბებს. მეორე მხრივ, სწორედ კორპორაციული მართვის ამგვარი მოდელის წიაღში ხორციელდება მონაცემთა სუბიექტის, როგორც „დაინტერესებული პირის“, სამართლებრივი ინტერესების გათვალისწინება. შესაბამისად, მონაცემთა დაცვაზე ორიენტირებული კორპორაციული მართვის მოდელის მიზანია: ა) კორპორაციის, როგორც მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის სრული შესაბამისობა მონაცემთა დაცვის საკანონმდებლო მოწესრიგებასთან; ბ) მონაცემთა სუბიექტის, როგორც „დაინტერესებული პირის“, უფლებების დაცვა.

### **3. მონაცემთა დაცვის ოფიცერი, როგორც პერსონალურ მონაცემთა დაცვაზე ორიენტირებული კორპორაციული მართვის მოდელის ელემენტი**

ოფიცრის ინსტიტუტი მონაცემთა დაცვაზე ორიენტირებული კორპორაციული მართვის მოდელის ერთ-ერთი ელემენტია, თუმცა არა ერთადერთი. მონაცემთა დაცვის ზეგავლენის რისკების შეფასება (“Data Protection Impact Assessment”), მონაცემთა დაცვის შიდა პოლიტიკის არსებობა ანგარიშვალდებულების ერთგვარი გამოხატულებაა. ნაშრომის ფორმატიდან გამომდინარე, შეუძლებელია ოფიცრის ინსტიტუტის ყველა სამართლებრივი ასპექტის განხილვა, ამდენად, წინამდებარე თავიც ინსტიტუტის ძირითად მახასიათებლებზე აქცენტირდება.

#### **3.1. მონაცემთა დაცვის ოფიცრისა და კორპორაციული შესაბამისობის ოფიცრის ფუნქციური ურთიერთგამიჯვნა**

მონაცემთა დაცვის ოფიცერი არის მონაცემთა დაცვის კვალიფიციური ექსპერტი, რომლის ფუნქციაა კორპორაციის ხელმძღვანელობას კონსულტაცია გაუწიოს მონაცემთა დაცვის წესებთან შესაბამისობის უზრუნველსაყოფად.<sup>16</sup> განსხვავებით კორპორაციის ხელმძღვანელი პირებისაგან, მონაცემთა დაცვის ოფიცერი არ არის სამეწარმეო

---

<sup>14</sup> Council of Europe, Explanatory Report, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf(2018)15-final), 18/05/2018, მუხლი 10.

<sup>15</sup> იქვე, § 87.

<sup>16</sup> ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო, მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 198.

საზოგადოების ფიდუციარი<sup>17</sup> (სხვა სიტყვებით კი სამეწარმეო საზოგადოების საუკეთესო ინტერესის განმახორციელებელი წარმომადგენელი). იგი არც კორპორაციული შესაბამისობის ოფიცერია. თუმცა პარალელის გავლების მიზნით, შესაძლებელია ამ ორი ინსტიტუტის ფუნქციების ზოგადი შედარება.

კორპორაციული შესაბამისობა ანგლო-ამერიკული სამართლის ოჯახის პირმშოა. იგი აერთიანებს რიგ ღონისძიებებს, რომლის მეშვეობით ხორციელდება კორპორაციულ ინსაიდერთა (ხელმძღვანელების, თანამშრომლების) საქმიანობა საკანონმდებლო ნორმების შესაბამისად.<sup>18</sup> სწორედ კორპორაციული შესაბამისობის ოფიცერზე ხდება სამართლებრივი თუ ეკონომიკური გამოწვევებისა და ამონაცემის განსაზღვრის დელეგირება. ერთი შეხედვით, მათი ფუნქციები თითქოს თანმხვედრია, თუმცა დაუშვებელია კორპორაციული შესაბამისობის ოფიცრისა და მონაცემთა დაცვის ოფიცრის ინსტიტუციური როლის ურთიერთადრევა. ამ თვალსაზრისით საინტერესოა, რომ ინტერესთა კონფლიქტის მოტივით, ბელგიის მონაცემთა დაცვის საზედამხდველო ორგანომ დამმუშავებელი 50 000 ევროს ოდენობით დააჯარიმა, რადგან მონაცემთა ოფიცრის პოზიციაზე დაინიშნა პირი, რომელიც ამავდროულად იყო კორპორაციული შესაბამისობის სამსახურის უფროსი, ფულის გათეთრების ანგარიშგების ოფიცერი.<sup>19</sup>

გარდა ამისა, აუცილებელია, რომ მონაცემთა დაცვის ოფიცერს ჰქონდეს სათანადო კვალიფიკაცია, მონაცემთა დაცვის დარგის საექსპერტო ცოდნა და შესაძლებლობა, რომ დამოუკიდებლად განახორციელოს მასზე დაკისრებული მოვალეობა.<sup>20</sup> ამდენად, მის მიმართ მოქმედებს კომპეტენტურობის პრინციპი. მონაცემთა დაცვის ოფიცერი ანგარიშვალდებულია უშუალოდ მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის პირველი რანგის ხელმძღვანელთა წინაშე,<sup>21</sup> რაც პერიოდული ანგარიშის წარდგენასაც მოიაზრებს როგორც ანგარიშვალდებულების პრინციპის პრაქტიკული გამოხატულება. ოფიცრის დამოუკიდებლობის უზრუნველყოფის მიზნით, დაუშვებელია მისთვის დამმუშავებლის ან უფლებამოსილის მიერ რაიმე სახის ინსტრუქციის ან დავალებების მიცემა.<sup>22</sup> საპირწონედ, კორპორაციული შესაბამისობის ოფიცრის ფუნქცია შესაძლებელია, რომ კორპორაციის რომელიმე სტრუქტურულ ერთეულში დაინერგოს. ამას გარდა, განსხვავებით კორპორაციული შესაბამისობის ოფიცრისგან, მონაცემთა

<sup>17</sup> ფიდუციალური მოვალეობის მატარებელნი არიან კორპორაციის ხელმძღვანელი პირები, რომლებიც სამეწარმეო გადაწყვეტილებას საზოგადოების საუკეთესო ინტერესებიდან გამომდინარე იღებენ. *Schneeman A.*, Law of Corporations and Other Business Organizations, 2010, 39.

<sup>18</sup> იქვე, 363.

<sup>19</sup> Autorité de protection des données, Dossiernummer: DOS-2019-04309, 2020, <<https://cedpo.eu/dpo-case-law/>> [20.01.2023].

<sup>20</sup> *Voigt P., Bussche A.*, The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 56-57.

<sup>21</sup> მუხლი 38(3), Regulation (EU) 2016/679 of the European Parliament and of 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 Protection Regulation), OJ L 119, 4/5/2016, 1–88.

<sup>22</sup> *Voigt P., Bussche A.*, The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 59.

დაცვის ოფიცრს აქტიური კავშირი აქვს გარე აქტორებთანაც (მაგალითად, მონაცემთა სუბიექტთან, მონაცემთა დაცვის საზედამხედველო ორგანოსთან). შესაბამისად, სავალდებულოა მისი საკონტაქტო ინფორმაციის გამჟღავნება, ხოლო ოფიცრის დანიშვნის თაობაზე მონაცემთა დაცვის საზედამხედველო ორგანოს ინფორმირება.<sup>23</sup>

მონაცემთა დაცვის ოფიცრის ფუნქცია სამ სეგმენტს მოიცავს: ინფორმირების, თანამშრომლობისა და ზედამხედველობის ვალდებულებებს.<sup>24</sup> პირველში მოიაზრება დამმუშავებლისათვის/უფლებამოსილი პირისთვის მონაცემთა დამუშავების თაობაზე სათანადო კონსულტაციის გაწევა; მეორე გულისხმობს მონაცემთა დაცვის საზედამხედველო ორგანოსთან აქტიურ კავშირსა და თანამშრომლობას; მესამე კი — მონაცემთა დაცვის მომწესრიგებელ კანონმდებლობასთან შესაბამისობის ზედამხედველობას.<sup>25</sup> ამ ფუნქციების ჯეროვნად განხორციელების მიზნით, იგი უფლებამოსილია, ჩაატაროს ინსპექტირება, ჰქონდეს წვდომა პერსონალურ მონაცემებზე, გაეცნოს მონაცემთა სუბიექტების განცხადებებს და ამ მიზნით დამოუკიდებლად განახორციელოს ნებისმიერი ქმედება ეთიკის სტანდარტის ფარგლებში.<sup>26</sup>

### **3.1. მონაცემთა დაცვის ოფიცრის დანიშვნის წინაპირობა**

ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულებას სამ ცალკეულ შემთხვევაში ითვალისწინებს.<sup>27</sup> კერძო სექტორში ოპერირებადი მეწარმე სუბიექტში ოფიცრის ინსტიტუტის არსებობა უკავშირდება დამმუშავებლის ან უფლებამოსილი პირის იმგვარ ძირითად საქმიანობას, რომლის ფარგლებში განხორციელებული ოპერაციები ფართო მასშტაბით ითვალისწინებს მონაცემთა სუბიექტის რეგულარულ, სისტემურ მონიტორინგს ან თუკი მათი ძირითადი საქმიანობა უკავშირდება განსაკუთრებული კატეგორიის მონაცემთა ფართომასშტაბიან დამუშავებას.<sup>28</sup> აღნიშნულ განმარტებაში საგულისხმოა დამმუშავებლის ან უფლებამოსილი პირის „ძირითადი საქმიანობა“ და მის ფარგლებში განხორციელებული ოპერაციების „კვალიტატური“ (ე. ი. „ხარისხობრივი“) და

---

<sup>23</sup> Article 29 Data Protection Working Group, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2016, 10.

<sup>24</sup> Voigt P., Bussche A., The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 60.

<sup>25</sup> იქვე.

<sup>26</sup> Data Protection Officer, Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working under Regulation (EC) 45/2011, 2010, 12-13.

<sup>27</sup> მუხლი 37, Regulation (EU) 2016/679 of the European Parliament and of 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 Protection Regulation), OJ L 119, 4/5/2016, 1–88.

<sup>28</sup> იქვე, მუხლი 37(1).

„კვანტიტატური“ (ე. ი. „რაოდენობრივი“) მაჩვენებლები. რაკი კორპორაციულსამართლებრივი გაგებით ძირითადი, იგივე ჩვეულებრივი სამეწარმეო საქმიანობა და კერძო სამართლის იურიდიული პირის ზოგადი უფლებაუნარიანობის ფარგლებში განხორციელებული დამხმარე ეკონომიკური საქმიანობა სხვადასხვა ცნებებია<sup>29</sup>, ოფიცრის დასანიშნად მნიშვნელოვანია, რომ მეწარმე სუბიექტის მიერ პერსონალური მონაცემები მუშავდებოდეს მოგების მიღების მიზნით, ორგანიზებულად, მართლზომიერად, არაერთჯერადად და დამოუკიდებლად განხორციელებული<sup>30</sup> ძირითადი სამეწარმეო საქმიანობის ფარგლებში. ასევე უნდა შეფასდეს, პერსონალურ მონაცემთა დამუშავების მასშტაბი, რომელიც განისაზღვრება შემდეგი კრიტერიუმებით: ა) მონაცემთა სუბიექტების რაოდენობა; ბ) დამუშავებულ მონაცემთა მოცულობა; გ) დამუშავების ხანგრძლივობა; დ) დამუშავების გეოგრაფიული დაფარვა.<sup>31</sup> ეროვნული კანონმდებლობა შესაძლებელია, ითვალისწინებდეს მონაცემთა დაცვის ოფიცრის დანიშვნის სხვა საფუძვლებსაც. მაგალითად, გერმანიის მონაცემთა დაცვის ფედერალური აქტის თანახმად, იმ კერძო კომპანიაში, რომელშიც დასაქმებულია სულ მცირე 20 თანამშრომელი, რომელსაც შემხებლობა აქვს პერსონალურ მონაცემთა ავტომატურ დამუშავებასთან, სავალდებულოა მონაცემთა დაცვის ოფიცრის დანიშვნა.<sup>32</sup> ოფიცრის არსებობა ასევე აუცილებელია, თუკი ხორციელდება მონაცემთა იმგვარი დამუშავება, რომელიც ექვემდებარება დამუშავების ზეგავლენის შეფასების კვლევას ან თუკი პერსონალური მონაცემები მუშავდება კომერციული გადაცემის, ანონიმური გადაცემის ან ბაზრის ან აზრის კვლევის მიზნებისთვის.<sup>33</sup>

რაც შეეხება მონაცემთა დაცვის ოფიცრის კლასიფიკაციას — განასხვავებენ შიდა და გარე ოფიცრის ინსტიტუტებს.<sup>34</sup> შიდა ოფიცერი კორპორაციაში დასაქმებული პირია, ხოლო მეორე — კორპორაციასთან გარიგებითსამართლებრივი გზით (*ხელშეკრულებით*) დაკავშირებული პირი. ასევე შესაძლებელია სავალდებულო და ნებაყოფლობითი ოფიცრის ინსტიტუტების გამიჯვნა. როგორც წინა პარაგრაფში იქნა წარმოჩენილი, განხილულ შემთხვევებში ოფიცრის განსაზღვრა სავალდებულოა<sup>35</sup>, თუმცა აღნიშნული არ გამორიცხავს კომპანიის მიერ ოფიცრის ნებაყოფლობით, თვითრეგულირებისა და

<sup>29</sup> ბურდული ი., მახარობლიძევილი გ., თოხაძე ა., ზუბიტაშვილი ნ., ალადაშვილი გ., მადრაძე გ., ეგნატაშვილი დ., საკორპორაციო სამართალი, 2022, 60-63.

<sup>30</sup> მე-2 მუხლის მე-2 პუნქტი, „მეწარმეთა შესახებ“ საქართველოს კანონი, №875-VRს-XXIII, 02/08/2021.

<sup>31</sup> *Kuner Ch., Bygrave L., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford, 2020, 693.*

<sup>32</sup> § 38, Bundesdatenschutzgesetz, (BDSG), 30/06/2017.

<sup>33</sup> იქვე.

<sup>34</sup> *Voigt P., Bussche A., The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 57.*

<sup>35</sup> სტატის მიზნებიდან გამომდინარე, ნაშრომში არ განიხილება მონაცემთა დაცვის ოფიცრის სავალდებულო დანიშვნის შემთხვევა საჯარო უწყებაში. იხ. მუხლი 37(1), Regulation (EU) 2016/679 of the European Parliament and of 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 Protection Regulation), OJ L 119, 4/5/2016, 1–88.

საწესდებო ავტონომიის ფარგლებში დანიშვნას. ცხადია, ეს კორპორაციული მართვის კარგ კულტურასა და ანგარიშვალდებულების მაღალ სტანდარტზე მიუთითებს. მონაცემთა დაცვის ზოგადი რეგულაცია (მუხლი 37(2)) განსაზღვრავს საერთო ოფიცრის ინსტიტუტსაც, როდესაც რამდენიმე დამმუშავებელს/უფლებამოსილ პირს ჰყავს ერთი ოფიცერი. აღნიშნული საკმაოდ პრაქტიკულია კორპორაციული კონსორციუმებისთვის, ორგანიზაციათა ჯგუფისთვის, ჰოლდინგური კომპანიებისათვის.

როგორც ზემოთ აღინიშნა, დანიშვნის ერთ-ერთ წინაპირობას სათანადო პროფესიული კვალიფიკაცია წარმოადგენს. კომენტატორული ლიტერატურის თანახმად, ეს ოფიცრის სერტიფიცირებას, ბიზნეს სექტორის ადმინისტრირების ზოგადი წესების ცოდნას უკავშირდება.<sup>36</sup>

### 3.2. ოფიცრის დამოუკიდებლობა და ინტერესთა კონფლიქტის აკრძალვა

მონაცემთა დაცვის ოფიცერი უნდა იყოს აღჭურვილი შესაბამისი რესურსით, რაც უზრუნველყოფს მის მიერ საკუთარი მოვალეობის დამოუკიდებლად, დროულად და კვალიფიციურად შესრულებას.<sup>37</sup> აკრძალულია მასზე რაიმე სახის ზეგავლენა ან ზეწოლა. ასევე დაუშვებელია, რომ კორპორაციაში იგი იკავებდეს იმგვარ პოზიციას, რომელიც მას შესაძლებლობას მისცემს, განსაზღვროს მონაცემთა დამმუშავების მიზანი და საშუალება.<sup>38</sup> შესაბამისად, იგი არ უნდა იყოს მონაცემთა დამმუშავებელი ან უფლებამოსილი პირი. ამასთანავე აღსანიშნავია, რომ მონაცემთა დაცვის ოფიცერმა შესაძლებელია, შეითავსოს სხვა ფუნქციები იმ პირობით, თუკი აღნიშნული არ იწვევს ინტერესთა კონფლიქტს.<sup>39</sup> ინტერესთა კონფლიქტი სწორედ მაშინ არის სახეზე, როდესაც ოფიცერი პარალელურად იმგვარ ფუნქციას ასრულებს, რომელიც პირდაპირ წინააღმდეგობაში მოდის იმ ორგანიზაციის მონაცემთა დაცვის ინტერესთან, რომელშიც იგი ფუნქციონირებს.<sup>40</sup> მოცემულ შემთხვევაში, აუცილებელია მონაცემთა დაცვის ოფიცრის მხრიდან მსგავსი ინტერესთა კონფლიქტის გაცხადება, გამჟღავნება. კორპორაციულსამართლებრივი თვალსაზრისით ინტერესთა კონფლიქტის საკითხი დღის წესრიგში არ დგას, როდესაც ორგანიზაციათა გარკვეულ ჯგუფს საერთო ოფიცერი

---

<sup>36</sup> *Kuner Ch., Bygrave L., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford, 2020, 695.*

<sup>37</sup> *Voigt P., Bussche A., The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 58-59.*

<sup>38</sup> *Article 29 Data Protection Working Group, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2016, 24.*

<sup>39</sup> *Voigt P., Bussche A., The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 60.*

<sup>40</sup> *Data Protection Officer, Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working under Regulation (EC) 45/2011, 2010, 15.*

ჰყავს. თუმცა, როგორც ეს ზემოთ იქნა აღნიშნული, მონაცემთა დაცვის ოფიცერს უნდა შეეძლოს საკუთარი ფუნქციის სრულყოფილი განხორციელება.

საინტერესოა მონაცემთა დაცვის საზედამხედველო ორგანოების პრაქტიკა: სლოვენის მონაცემთა დაცვის საზედამხედველო ორგანომ კომპანიის მთავარი აღმასრულებელი დირექტორის ან დირექტორთა ბორდის წევრის მონაცემთა დაცვის ოფიცრად დანიშვნის ფაქტი ინტერესთა კონფლიქტად ცნო და დაუშვებლად მიიჩნია.<sup>41</sup> 2019 წელს ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანომ ერთ-ერთი კორპორაცია 25 000 ევროს ოდენობით დააჯარიმა, რადგან მონაცემთა დაცვის ოფიცრის ფუნქცია შიდაკორპორაციულ სტრუქტურაში შექმნილ ორგანოს ე. წ. „მონაცემთა დაცვის შიდა ბორდს“ მიანიჭა, რომელიც დამმუშავებლის განმარტებით, სწორედ იმავე ფუნქციას ასრულებდა, რასაც მონაცემთა დაცვის ოფიცერი.<sup>42</sup>

ევროპის მონაცემთა დაცვის ზედამხედველის (*European Data Protection Supervisor*) რეკომენდაციის თანახმად, მონაცემთა დაცვის ოფიცერი არ უნდა იყოს კორპორაციაში ვადიანი ან მოკლევადიანი ხელშეკრულებით დასაქმებული პირი; მას უნდა ჰქონდეს ეკონომიკური სახსრების დამოუკიდებლად განკარგვის შესაძლებლობა და უნდა იყოს ანგარიშვალდებული მხოლოდ კორპორაციის ტოპ-მენეჯმენტის წინაშე.<sup>43</sup>

შესაბამისად, მონაცემთა დაცვის ოფიცრის მიმართ, სხვა ზემოხსენებულ პრინციპებთან ერთად, ასევე მოქმედებს დამოუკიდებლობის პრინციპი და ინტერესთა კონფლიქტის აკრძალვის მოთხოვნა. დამოუკიდებლობისა და მიუკერძოებლობის პრინციპის ლოგიკური გაგრძელებაა სათანადო ანაზღაურების წესი, რასაც საკორპორაციო სამართლაშიც ხელმძღვანელ პირთა დამოუკიდებლობის უზრუნველყოფის თვალსაზრისით<sup>44</sup> გარკვეული მნიშვნელობა აქვს მინიჭებული.

### 3.3. ოფიცრის პასუხისმგებლობის საკითხი

ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია არ შეიცავს მონაცემთა დაცვის ოფიცრის პასუხისმგებლობის მომწესრიგებელ ცალკეულ დებულებას. მონაცემთა დაცვის მომწესრიგებელ კანონმდებლობასთან შეუსაბამობისათვის მონაცემთა დაცვის ოფიცრის პერსონალური პასუხისმგებლობა არ დგება. თუმცა აღსანიშნავია, რომ მასზე

<sup>41</sup>Informacijski pooblaščenec, Advisory Opinion, N07121-1/2021/577, 2021, <[https://gdprhub.eu/index.php?title=IP\\_-\\_07121-1/2021/577#Facts](https://gdprhub.eu/index.php?title=IP_-_07121-1/2021/577#Facts)> [22.01.2023].

<sup>42</sup> Agencia Española Protección Datos, Resolución de procedimiento sancionador, Procedimiento Nº: PS/00417/2019, იხ.: <<https://cedpo.eu/dpo-case-law/>> [22.01.2023].

<sup>43</sup> European Data Protection Supervisor, Data Protection Officer (DPO), <[https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo\\_en](https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en)> [20.01.2023].

<sup>44</sup> ხელმძღვანელ პირთა ანაზღაურების წესზე იხ. Schneeman A., Law of Corporations and Other Business Organizations, 2010, 348-349.

ვრცელდება ერთგულების მოვალეობა სწორედ იმ ორგანიზაციის მიმართ, რომელშიც იგი იქნა დანიშნული.<sup>45</sup> ოფიცერი მოქმედებს შინაგანი პროფესიული რწმენის საფუძველზე, რაც გულისხმობს პრინციპს უკავშირდება. შესაბამისად, მას აქვს თითოეული შემთხვევის გულისხმიერად და დაყოვნების გარეშე შესწავლის ვალდებულება.<sup>46</sup>

მონაცემთა დაცვის ოფიცერზე ასევე ვრცელდება კონფიდენციალურობის ვალდებულება.<sup>47</sup> კორპორაციული მართვის სისტემაში დუმილის მოვალეობის კონცეფციაც, რომელიც ხელმძღვანელ პირებსა და სამეთვალყურეო საბჭოს წევრებს აკისრიათ, სწორედ ინსაიდერული ინფორმაციის დაცვის მიზანს ემსახურება.<sup>48</sup> მისი შემსუბუქება ან გამორიცხვა დაუშვებელია.<sup>49</sup>

ნაკისრ ვალდებულებათა არაკეთილსინდისიერი და არაჯეროვანი შესრულება მონაცემთა დაცვის ოფიცრის პირდაპირ პასუხისმგებლობას უკავშირდება. ამ თვალსაზრისით სამეცნიერო ლიტერატურაში საუბარია გარე ოფიცრის სახელშეკრულებოსამართლებრივ პასუხისმგებლობაზე, ხოლო მონაცემთა სუბიექტის ჭრილში — მის დელიქტურ პასუხისმგებლობაზე.<sup>50</sup> რაც შეეხება შიდა ოფიცერს, მისი პასუხისმგებლობა შრომითსამართლებრივი საფუძვლით დგება.<sup>51</sup>

### 3.4. ოფიცრის გაწვევა

ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია არ აწესრიგებს ოფიცრის გაწვევის, მასთან სამართლებრივი ურთიერთობის შეწყვეტის საკითხს. შესაბამისად, აღნიშნული ევროკავშირის წევრი სახელმწიფოს ეროვნული კანონმდებლობით რეგულირების საგანს წარმოადგენს. რეგულაციის 38(3)-ე მუხლის თანახმად, დაუშვებელია ოფიცრის სამსახურიდან დათხოვნა ან ჯარიმის დაკისრება, მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის მიერ მასზე დაკისრებული ფუნქციების შესრულების გამო. ოფიცერი ვერ იქნება გაწვეული მარტოოდენ იმ მიზეზით, რომ მონაცემთა დამმუშავების შესახებ მის მიერ გაცემულ კონსულტაციას არ ეთანხმება

---

<sup>45</sup> *Data Protection Officer*, Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working under Regulation (EC) 45/2011, 2010, 14-15.

<sup>46</sup> იქვე, 15.

<sup>47</sup> მუხლი 38(5), Regulation (EU) 2016/679 of the European Parliament and of 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 Protection Regulation), OJ L 119, 4/5/2016, 1–88.

<sup>48</sup> *ჭანტურია ლ.*, კორპორაციული მართვა და ხელმძღვანელთა პასუხისმგებლობა საკორპორაციო სამართალში, 2006, 360-361.

<sup>49</sup> იქვე, 362.

<sup>50</sup> *Paal P. B., Pauly D. A.*, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, Kommentar, 3. Aufl., 2021, Art. 39, para. 11, 12.

<sup>51</sup> იქვე.



მონაცემთა დამმუშავებელი ან უფლებამოსილი პირი.<sup>52</sup> საკითხის ამგვარად რეგულირება ქმნის დამმუშავებლის/უფლებამოსილი პირის ზეწოლისაგან ოფიცრის დაცვის მაღალ სტანდარტს, რაც, ბუნებრივია, დადებითად აისახება მის დამოუკიდებლობაზე. მეორე მხრივ, აღნიშნული არ მიემართება ოფიცერთა მხრიდან უხეშ გაუფრთხილებლობას ან კანონდარღვევის შემთხვევებს.

ევროპული მართლმსაჯულების სასამართლომ 2022 წლის 22 ივნისის გადაწყვეტილებაში საქმეზე: “Leistritz AG v. LH” აღნიშნა, რომ რეგულაციის ზემოხსენებული მოთხოვნა (რეგულაციის 38(3)-ე მუხლის ფარგლებში) ვრცელდება როგორც შიდა, ისე გარე ოფიცრზე; წევრი სახელმწიფოს ეროვნული კანონმდებლობა შესაძლებელია, ითვალისწინებდეს ოფიცერთან ხელშეკრულების შეწყვეტის შესაძლებლობას მხოლოდ სამართლიანი საფუძვლით, მაშინაც კი, თუკი ხელშეკრულების შეწყვეტა არ უკავშირდება ოფიცრის ამოცანების შესრულებას, რამდენადაც ეს ხელს არ უშლის ზოგადი რეგულაციით დასახული მიზნის მიღწევას.<sup>53</sup> აღნიშნული წარმოადგენს ოფიცრის დამოუკიდებლობის დამატებით გარანტს, რაც თავის მხრივ უზრუნველყოფს ევროკავშირის მასშტაბით მონაცემთა დამმუშავებასთან დაკავშირებული უფლებების მომწესრიგებელი რეგულაციების ჰომოგენურ და თანმიმდევრულ განხორციელებას.<sup>54</sup> უფრო მეტიც, ეროვნული კანონმდებლობა შესაძლებელია, ითვალისწინებდეს ოფიცრის განთავისუფლებისაგან გაცილებით ძლიერი დაცვის მექანიზმს, ვიდრე ეს ევროკავშირის ზოგადი რეგულაციითაა დადგენილი.<sup>55</sup>

#### 4. დასკვნა

პერსონალურ მონაცემთა დაცვის საერთაშორისო დონეზე აღიარებულმა სტანდარტები კორპორაციების მმართველობის სტრატეგიაზეც აისახა. აღნიშნული განაპირობებს კორპორაციული მართვის ახალი მოდელის ჩამოყალიბებას, რომელიც მონაცემთა სუბიექტის უფლებებისა და ინტერესის დაცვაზეა ორიენტირებული. ამგვარი მმართველობითი პოლიტიკა წინამდებარე სტატიამი დასახელებულია, როგორც პერსონალურ მონაცემთა დაცვაზე ორიენტირებული კორპორაციული მართვის მოდელი. მისი მმართველობით სისტემაში დანერგვა უზრუნველყოფს კორპორაციის შესაბამისობას მონაცემთა დაცვის მომწესრიგებელ კანონმდებლობასთან, აგრეთვე,

<sup>52</sup> Article 29 Data Protection Working Group, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2016, 15.

<sup>53</sup> CJEU, C-534/20, *Leistritz AG v. LH* [2022], პარა. 23-24, 36.

<sup>54</sup> იქვე, პარა. 26.

<sup>55</sup> იქვე, პარა. 33-36.

მონაცემთა სუბიექტის – როგორც „დაინტერესებული პირის“ ინტერესების გათვალისწინებას კორპორაციული მართვის სისტემაში. ამგვარი მოდელის ერთ-ერთ ელემენტს მონაცემთა დაცვის ოფიცერი წარმოადგენს. იგი უზრუნველყოფს, ერთი მხრივ, მეწარმე სუბიექტის, ხოლო მეორე მხრივ – მონაცემთა სუბიექტის სამართლებრივი და ეკონომიკური ინტერესების თანაფარდობას. აღნიშნული მიზნის განსახორციელებლად, ოფიცერი აღჭურვილია შესაბამისი სამართლებრივი ბერკეტებით. კერძოდ, მის მიმართ მოქმედებს დამოუკიდებლობის, კონფიდენციალურობის, კომპეტენტურობის, ანგარიშვალდებულების პრინციპები. გარდა ამისა, იგი დაცულია კორპორაციულ ინსაიდერთა (იგულისხმებიან ხელმძღვანელები, სამეთვალყურეო საბჭოს წევრები) პირდაპირი ან არაპირდაპირი ზეგავლენისგან. თავის მხრივ ოფიცრის მიმართ მოქმედი კომპეტენტურობის, გულისხმიერების პრინციპები, ასევე, ინტერესთა კონფლიქტის აკრძალვა ემსახურება მონაცემთა სუბიექტის უფლების დაცვის ეფექტიან განხორციელებას და კორპორაციის მონაცემთა დაცვის მარეგულირებელ აქტებთან შესაბამისობას.

მონაცემთა დაცვის ოფიცრის ინსტიტუტის ეკონომიკურ-სამართლებრივ ანალიზზე<sup>56</sup> დაყრდნობით შეიძლება ითქვას, რომ იგი უზრუნველყოფს კორპორაციულ შესაბამისობასთან დაკავშირებულ იმ დამატებითი ხარჯის შემცირებას, რაც მეწარმე სუბიექტმა მონაცემთა დაცვის მომწესრიგებელ აქტებთან შეუსაბამობით (მაგალითად, დაკისრებული ჯარიმის სახით) შეიძლება, რომ განიცადოს. ოფიცრის ნებაყოფლობითი დანიშვნა სწორედ ამ ეკონომიკური ხარჯის შემცირებას ემსახურება და როგორც ეს ნაშრომში არის შეფასებული, კორპორაციული მართვის, პერსონალურ მონაცემთა დაცვის მაღალ კულტურაზე მიანიშნებს.

დღესდღეობით მონაცემთა დაცვის ოფიცრის ინსტიტუტი ჯერ-ჯერობით უცხოა ეროვნული საკანონმდებლო მოწესრიგებისათვის. მიუხედავად ამისა, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პროექტი<sup>57</sup> მის ინსტიტუტიურ მოწესრიგებას ითვალისწინებს, რაც დადებით ზეგავლენას იქონიებს, მათ შორის, სამეწარმეო საზოგადოებების პერსონალურ მონაცემთა დამუშავებისადმი ცნობიერების ამაღლებასა და კორპორაციული მართვის თანამედროვე მოდელის პრაქტიკაში დამკვიდრებაზე.

---

<sup>56</sup> იგულისხმება სამართლის ეკონომიკური ანალიზი, როგორც სამართლის მეცნიერებაში დამკვიდრებული მეთოდი, Posner R., *Economic Analysis of Law*, 2011, 1-3.

<sup>57</sup> მუხლი 33, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პროექტი № 07-3/353/9, 22/05/2019, <www.parliament.ge> [23.01.2023].

**ბიბლიოგრაფია:**

1. „მეწარმეთა შესახებ“ საქართველოს კანონი, 875-Vრს-Xმპ, 02/08/2021.
2. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 5669-რს, 28/12/2011.
3. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პროექტი, № 07-3/353/9, 22/05/2019, <www.parliament.ge> [23.01.2023].
4. ბურდული ი., მახარობლიძევილი გ., თოხაძე ა., ზუბიტაშვილი ნ., აღადაშვილი გ., მადრაძე გ., ეგნატაშვილი დ., საკორპორაციო სამართალი, 2022, 60-63, 634-638.
5. ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო და ევროპის საბჭო, მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 198.
6. იასესრი კ., ფილოსოფიის შესავალი, გორგიშელი ვ. (თარგმ.), 2019, 73.
7. მახარობლიძევილი გ., კორპორაციული მართვის ზოგადი ანალიზი, 2015, 161, 162-163, 313-317.
8. ჭანტურია ლ., კორპორაციული მართვა და ხელმძღვანელთა პასუხისმგებლობა საკორპორაციო სამართალში, 2006, 360-36, 362.
9. Regulation (EU) 2016/679 of the European Parliament and of 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 Protection Regulation), OJ L 119, 4/5/2016, 1–88.
10. *Council of Europe*, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf(2018)15-final), 18/05/2018.
11. *Council of Europe*, Explanatory Report, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf(2018)15-final), 18/05/2018.
12. Bundesdatenschutzgesetz, (BDSG), 30/06/2017.
13. *OECD*, Principles of Corporate Governance, 2015.
14. *Article 29 Data Protection Working Group*, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2016, 10, 15, 24.
15. *Bentham J.*, Of Laws in General, *Hart H. L. A. (ed.)*, 1970, 31-33.
16. *Data Protection Officer*, Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working under Regulation (EC) 45/2011, 2010, 12-13, 14-15.
17. *European Data Protection Supervisor*, Data Protection Officer (DPO), <[https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo\\_en](https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en)> [20.01.2023].
18. *Haskel J., Westlake S.*, Capitalism without Capital: The Rise of the Intangible Economy, Princeton, 2018, 3-10.

19. *Johnson A.*, Soft Law, in: EC Regulation of Corporate Governance, UK, 2009, 343-347.
20. *Kuner Ch., Bygrave L., Docksey Ch.*, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford, 2020, 693, 695.
21. *Magnier V.*, Comparative Corporate Governance, Legal Perspectives, 2017, 1-4.
22. *Paal P. B., Pauly D. A.*, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, Kommentar, 3. Aufl., 2021, Art. 39, para. 11, 12.
23. *Posner R.*, Economic Analysis of Law, 2011, 1-3.
24. *Picciotto S.*, Regulating Global Corporate Capitalism, 2011, 61-65, 193-200.
25. *Schneeman A.*, Law of Corporations and Other Business Organizations, 2010, 39, 348-349, 363.
26. *Tokhadze A.*, Enhancement of Corporate Social Responsibility – An Analysis from the Perspective of Economic and Sectoral Cooperation under the Three Association Agreements, in: Legal Aspects of the EU Association Agreements with Georgia, Moldova and Ukraine in the Context of the EU Eastern Partnership Initiative, *Trunk A., Panych N., Rieckhof S. (eds.)*, 2017, 104-106.
27. *Voigt P., Bussche A.*, The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 56-60.
28. CJEU, C-534/20, *Leistritz AG v. LH* [2022].
29. *Autorité de protection des données*, Dossiernummer: DOS-2019-04309, 2020, <<https://cedpo.eu/dpo-case-law/>> [20.01.2023].
30. *Agencia Española Protección Datos*, Resolución de procedimiento sancionador, Procedimiento N°: PS/00417/2019, nb.: <<https://cedpo.eu/dpo-case-law/>> [22.01.2023].
31. *Informacijski pooblaščenec*, Advisory Opinion, N07121-1/2021/577, 2021, <[https://gdprhub.eu/index.php?title=IP\\_-\\_07121-1/2021/577#Facts](https://gdprhub.eu/index.php?title=IP_-_07121-1/2021/577#Facts)> [22.01.2023].