ნორბერტ ბერნსდორფი*

ევროპის კავშირის „მონაცემთა დაცვის სამართალი“**

1. მონაცემთა დაცვა და ევროპის კომისიის 2022 წლის 17 ივნისის მოთხოვნები

ჩემი მოხსენება მინდა დავიწყო შეკითხვით: ევროპული კომისია - ევროკავშირის კომისია - გამოხატავს თუ არა უკმაყოფილებას საქართველოში მონაცემთა დაცვის დეფიციტთან დაკავშირებით? და თუ ეს ასეა, ეს დასაბუთებულია თუ მონაცემთა დაცვის კანონი უბრალოდ დახვეწას საჭიროებს?

2022 წლის 17 ივნისს ევროკავშირის კომისიის მიერ გამოთქმული მოსაზრება წინააღმდეგობრივია: კომისია მოითხოვს - პირველი, „პერსონალურ მონაცემთა დაცვის სერვისის ... აღჭურვას მისი მანდატის შესაბამისი რესურსებით“ და მეორე, „მისი ინსტიტუციური დამოუკიდებლობის უზრუნველყოფას, იგი ადგენს, რომ „პერსონალურ მონაცემთა დაცვის სამსახურმა... ჯერ კიდევ უნდა დაამტკიცოს თავისი ეფექტურობა და დამოუკიდებლობა“. სულ ეს არის მისი მოსაზრება.

ჩემს პირველ მოხსენებაში მე უკვე მივუთითე ე.წ. „კოპენჰაგენის კრიტერიუმზე“, რომელიც განმცხადებელმა ქვეყანამ უნდა შეასრულოს. ერთ-ერთი ამ კრიტერიუმებიდან არის “acquis criterion” („ევროკავშირის კანონმდებლობის კრიტერიუმი“ / ფრანგული სიტყვიდან “acquis communautaire”), რომლის მიხედვით კანდიდატმა სახელმწიფომ უნდა აღიაროს ევროკავშირის წესებისა და რეგულაციების მთელი ნაკრები, რაც გულისხმობს რამდენიმე 10 000 გვერდიანი იურიდიული ტექსტების ეროვნულ სამართალში ინტეგრირებას და დანერგვას შესაბამის ადმინისტრაციულ და სასამართლო სტრუქტურებში. ის, რასაც “acquis” მოიცავს ევროპული მონაცემთა დაცვის კანონის სფეროში, წარმოადგენს 2014 წლის ევროკავშირისა და საქართველოს შორის „ასოცირების ხელშეკრულების“ შედეგს. „ხელშეკრულების“ მე-14 და 327-ე მუხლის დანართში (I / XV-b) არის მითითება ევროსაბჭოს მონაცემთა დაცვის კანონზე და ახლა უკვე მოძველებულ - უკვე არა ვალიდურ - ევროკავშირის კანონზე, რაც იძლევა კიდევ ერთ მიზეზს, რომ დავაკვირდეთ ახლანდელ, სრულიად შეცვლილ სამართლებრივ სიტუაციას ევროკავშირში.

---

* მარბურგის ფილიპეს სახელობის უნივერსიტეტის პროფესორი, სამართლის დოქტორი; გერმანიის სოციალურ საკითხთა ფედერალური სასამართლოს ყოფილი მოსამართლე.

** პუბლიკაცია წარმოადგენს ავტორის მიერ ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტისა და ადმინისტრაციულ მეცნიერებათა ინსტიტუტის თანამშრომლობით ჩატარებული საჯარო ლექციების ფარგლებში წარდგენილი მოხსენების ტექსტს. ღონისძიება ეძღვნებოდა ევროკავშირთან საქართველოს დაახლოებისა და ინტეგრაციის საკითხებს.

2. აღიარება, დანერგვა, აღსრულება

უპირველეს ყოვლისა, იმისათვის, რომ საკითხი გასაგები იყოს, საჭიროა მისი დაზუსტება: როცა კანდიდატმა ქვეყანამ უნდა აღიაროს ევროკავშირის წესების კრებული, როგორ ხდება აღნიშნული ტექნიკურად?

ევროკავშირს არ გააჩნია სამართლებრივი საშუალებები რომ მოახდინოს მისი კანონის ინტეგრირება კანდიდატი სახელმწიფოს ეროვნულ სამართალში. მსგავსად გაწევრიანებისა, ესეც ხდება კანდიდატი ქვეყნის სურვილით. ევროკავშირის კანონმდებლობაში ინტეგრირების სამი ეტაპი არსებობს: „აღიარება“, „დანერგვა“ და „აღსრულება“, რაც გულისხმობს „კანონის ცხოვრებაში გატარებას“. პირველი ორი ეტაპისათვის ასევე ფართოდ გამოიყენება ტერმინები „ტრანსპოზიცია“ - რაც გულისხმობს კანონის ტრანსფორმაციას და „გამოყენება“ - რაც ნიშნავს კანონისადმი დამორჩილებას. ევროკავშირის კანონმდებლობის ეროვნულ სამართალში ინტეგრაცია ჩვეულებრივი აპოლიტიკური პროცესია. აქ უფრო ნაკლები იქნება ე.წ. „ვეტოს უფლებით მოთამაშეები“, რადგან კანდიდატ ქვეყნებში პოლიტიკური დებატები ადრევე გაიმართა, კერძოდ, წევრობისათვის განაცხადის წარდგენამდე.

რას ნიშნავს ტერმინი „შესაბამისობა“ ამ კონტექსტში?

„შესაბამისობა“ ან „არაშესაბამისობა“ დაკავშირებულია ევროკავშირში გაწევრიანების შემდგომ ფაზასთან. აქ საუბარია იმაზე, თუ როგორ იცავს წევრი სახელმწიფო მის მიერ აღიარებულ ევროკავშირის კანონმდებლობას - სრულად თუ საერთოდ არ იცავს, მხოლოდ არასრულად თუ დაგვიანებით. ამის მონიტორინგი ხდება ევროკავშირის კომისიის და ევროკავშირის მართლმსაჯულების სასამართლოს (CJEU) მიერ. აქ საკვანძო სიტყვას წარმოადგენს: სამართალდარღვევათა საქმის წარმოება!

წარმოადგენს თუ არა „აღიარება“ და „ტრანსპოზიცია“ ევროკავშირის კანონმდებლობაში ინტეგრაციის პირველი ეტაპს?

დიახ! - ამის ტექნიკურ საშუალებას წარმოადგენს კანდიდატი ქვეყნის „გაწევრიანება“. ეს ხდება ევროკავშირში ყველა სხვა წევრ-სახელმწიფოს გაწევრიანების ხელშეკრულებით (საერთაშორისო სამართლის მიხედვით). გაწევრიანების თარიღიდან კანდიდატი ქვეყანა ევროკავშირის ყველა ხელშეკრულების მოქმედ ვერსიაში ხდება მხარე. ევროკავშირის ყველა კანონი, რომელიც მიღებულია ამ ხელშეკრულებების საფუძველზე გაწევრიანების თარიღამდე, ავტომატურად ხდება დამავალდებულებელი გაწევრიანების პროცესში მყოფი ქვეყნებისთვის. ევროკავშირის კანონმდებლობა უპირატესია ნებისმიერ ეროვნულ კანონმდებლობაზე. ეს ერთმნიშვნელოვნად არის აღიარებული გაწევრიანების ხელშეკრულებაში (საერთაშორისო სამართლის მიხედვით) კანდიდატი ქვეყნის მიერ.

რას ნიშნავს ეს ევროკავშირის მონაცემთა დაცვის სამართლისთვის? – გაწევრიანებით ესეც ასევე იქნება „ათვისებული“, როგორც პრიორიტეტული უფლება ეროვნულ სამართლებრივ სისტემაში!

ამ ლექციაში არ მინდა მონაცემთა დაცვის ქართული და ევროპული სამართლის ერთმანეთთან შედარება. ჩემი მიზანი არ არის წარმატებების ან წარუმატებლობის ძიება მომავალ „აღიარებასა“ თუ „ტრანსპოზიციაში“. არც შემიძლია ამის გაკეთება, რადგან არ მაქვს ე.წ. ანგარიში ჩატარებულ საქმიანობაზე - „ანგარიში ასოცირების პროცესის განხორციელების შესახებ“, რომელიც კეთდება ყოველწლიურად 2016 წლიდან. ეს ხდება ევროკავშირის კომისიის ან საქართველოს კომპეტენტური ორგანოების მიერ; მე კი არც ევროკავშირის თანამშრომელი ვარ და არც წევრ

სახელმწიფოს გერმანიის ოფიციალური წარმომადგენელი. ასეთი შედარების გაკეთება, ევროკავშირის კომისიის „ტექნიკური დახმარებისა და ინფორმაციის გაცვლის“ ჯგუფის (TAIEX) მოვალეობაა, რომელიც გასული წლიდან უნდა არსებობდეს საქართველოში.

რა არის ჩემი ამოცანა დღეს?

მინდა წარმოგიდგინოთ შემდეგი საკითხები:

- პირველი: ევროკავშირის ე.წ. პირველადი კანონმდებლობა და ე.წ. მეორეული კანონმდებლობა, და პირველ რიგში „მონაცემთა დაცვის ძირითადი რეგულაცია“;
- მეორე: ევროკავშირის მონაცემთა დაცვის კანონმდებლობაში არსებული კონფლიქტები;
- მესამე: ახალი სამართლებრივი ცვლილებები და
- მეოთხე: ევროპული კანონმდებლობის მოთხოვნები მონაცემთა დაცვის ეფექტურად კონტროლისადმი.

3. ევროკავშირის პირველადი კანონმდებლობა მონაცემთა დაცვის შესახებ

ევროკავშირის ყველა ქმედება ეფუძნება ევროპულ ხელშეკრულებებს. ამ ხელშეკრულებებში, რომლებიც წევრ სახელმწიფოებს შორის არის დადებული, განსაზღვრულია ევროკავშირის დაწესებულებების ამოცანები და წესები, ასევე გადაწყვეტილების მიღების პროცესი და ევროკავშირსა და მის წევრ-სახელმწიფოებს შორის ურთიერთდამოკიდებულება. ხელშეკრულებები წარმოადგენენ ევროკავშირის კანონმდებლობის საფუძველს და ეწოდებათ ევროკავშირის „პირველადი კანონმდებლობა“. კანონმდებლობას, რომელსაც საფუძვლად უდევს ამ ხელშეკრულებების ნორმები და ამოცანები ეწოდება „მეორეული კანონმდებლობა“ და მოიცავს რეგულაციებს, დირექტივებს, გადაწყვეტილებებს, რეკომენდაციებსა და მოსაზრებებს.

ა. პირველადი და მეორეული კანონმდებლობა

2009 წლიდან, როცა ლისაბონის ხელშეკრულება შევიდა ძალაში, მონაცემთა დაცვის სამართლებრივ ჩარჩოს ევროპული პირველადი კანონმდებლობისთვის წარმოადგენდა ევროკავშირის ქარტია ფუნდამენტური უფლებების შესახებ - ფუნდამენტური უფლებების ევროპული ქარტია, ამ შემთხვევაში მე-8 მუხლი. მიუხედავად იმისა, რომ პირველადი კანონმდებლობა ასევე შეიცავს 1981 წლის ადამიანთა უფლებების შესახებ ევროპული კონვენციისა და ევროპის საბჭოს კონვენციის მე-8 მუხლს, ჩემი მოხსენება ყურადღებას ამახვილებს ფუნდამენტური უფლებების ევროპული ქარტიის მე-8 მუხლზე.

იმისათვის რომ ჩემი ლექცია არ გახდეს არაკონტროლირებადი, შემოვიფარგლები მხოლოდ მონაცემთა დაცვის მეორეული კანონმდებლობის პრეზენტაციით. მიუხედავად იმისა, რომ ახლა ევროკავშირის უამრავი მეორეული რეგულაციები და დირექტივები არსებობს, მე მხოლოდ მონაცემთა ძირითად რეგულაციაზე გავამახვილებ ყურადღებას, რომელიც ძალაშია 2018 წლიდან. იგი წარმოადგენს პერსონალურ მონაცემთა დაცვის ძირითად სამართლებრივ ინსტიტუტს ევროპაში, და შედეგად მოიტანა რადიკალური ცვლილებები მონაცემთა დაცვის ევროკავშირის კანონმდებლობაში.

ბ. ფუნდამენტური უფლებების ევროპული ქარტიის მე-7 და მე-8 მუხლები

პერსონალური მონაცემთა დაცვა პირადი ცხოვრების დაცვის არსებითი ასპექტია. ეს უკანასკნელი რეგულირებულია ძირითადი უფლებების ევროპული ქარტიის მე-7 მუხლით და რადგანაც მას ასეთი დიდი მნიშვნელობა ენიჭება, ევროკავშირმა ცალკე სპეციალური დებულება მიუძღვნა მონაცემთა დაცვას - ამ შემთხვევაში ადამიანის უფლებების ევროპული კონვენციისგან განსხვავებული ფორმით, სახელდობრ, მე-8 მუხლით. მონაცემთა დაცვის ფუნდამენტური უფლება დაცული უნდა იყოს ევროკავშირის ინსტიტუციების, ორგანოებისა და სააგენტოების მიერ, აგრეთვე ევროკავშირის თითოეული წევრ-სახელმწიფოს მიერ ევროპული კანონმდებლობის განხორციელებისას.

რას ნიშნავს „ევროკავშირის კანონის დანერგვა“ ამ კონტექსტში?

უპირველეს ყოვლისა, უნდა აღინიშნოს, რომ ევროკავშირის წევრ-სახელმწიფოები არ არიან შებოჭილები ევროკავშირის ძირითადი უფლებებით, თუ ისინი ექსკლუზიურად იყენებენ თავიანთ ეროვნულ კანონმდებლობას. ამ შემთხვევაში ძალაშია ეროვნული ძირითადი უფლებები. საქმე სხვანაირად არის, როცა ევროკავშირის კანონის მაგალითად ევროპული დირექტივის გამოყენება ხდება. ესეც ევროკავშირის წევრ-სახელმწიფოების ეროვნული „საკანონმდებლო აქტების“ საშუალებით ხდება. თუმცა, ესენი მხოლოდ „შუალედური“ კანონებია და საბოლოოდ, ემსახურებიან ევროკავშირის სუვერენიტეტის „გაფართოებას“. ეროვნულმა სასამართლოებმა უნდა გამოიყენონ ევროპული ფუნდამენტური უფლებები ეროვნულთან ერთად. ეს რთული ჩანს, მაგრამ მარტივია, თუ ჩავუღრმავდებით.

გ. ძირითადი საფუძვლები

არ მინდა დიდხანს გესაუბროთ დოგმატურ ნიუანსებზე. ამიტომ, ამ ეტაპზე მხოლოდ რამდენიმე მინიშნება:

ფუნდამენტური უფლებების ევროპული ქარტიის მე-8 მუხლი წარმოადგენს სარჩელის ძალის მქონე უფლებას. მსგავსად ნებისმიერი კლასიკური ძირითადი უფლებისა, იგი უპირველეს ყოვლისა, წარმოადგენს სახელმწიფოსა და მისი ხელისუფლებისგან დაცვის უფლებას. თუმცა, მე-8 მუხლი ასევე ავალდებულებს კერძო პირებს უზრუნველყონ პერსონალურ მონაცემთა დაცვა. ამრიგად, მონაცემთა დაცვის ძირითად უფლებას ასევე აქვს ე.წ. მესამე მხარის ეფექტი.

მონაცემთა დაცვის სფერო, ძირითადი უფლებების ევროპული ქარტიის მე-8 მუხლი შეიცავს ფორმულირებებს დაცვის ფარგლების შესახებ და თუ როდის არის გამართლებული პერსონალურ მონაცემთა დაცვის უფლებაში ჩარევა; უფრო მეტიც, მე-8 მუხლი მოითხოვს „დამოუკიდებელი ორგანოს“ შექმნას მონაცემთა დაცვის კანონის შესრულების მონიტორინგის მიზნით. საკითხი იმის შესახებ, ფუნდამენტური უფლებების მფლობელები არიან თუ არა იურიდიული პირებიც, ჯერ არ არის გარკვეული ევროკავშირში.

მონაცემთა დაცვის ფუნდამენტურ უფლებას აქვს განსაკუთრებული თვისება - და ეს არის ბოლო რის თქმასაც ვაპირებ: იგი წარმოადგენს „შებრუნებულ ინჟინერიას!“ - გერმანიაში მას მოიხსენიებენ როგორც „ნორმატიულად შექმნილი“.

რას ნიშნავს ეს? - ეს ნიშნავს, რომ მონაცემთა დაცვის ძირითადი უფლება წინასწარ განსაზღვრულია ყველა დონეზე შესაბამისი მოქმედი ევროპული

მეორეული კანონმდებლობით - ამ შემთხვევაში მონაცემთა დაცვის ძირითადი რეგულაციით. მე-8 მუხლის შინაარსი, რომელიც წარმოადგენს ევროკავშირის პირველადი კანონმდებლობის ნაწილს, „ერთი ერთში“ ეფუძნება მეორეული კანონის შინაარსს, რომელიც ბევრად უფრო დაბალ ნორმატიულ დონეზეა. თუ შეიცვლება მეორეული კანონმდებლობა, ასევე შეიცვლება ძირითადი უფლებაც. ეს არის ის შედეგი, რაც სინამდვილეში არ არის შეთავსებადი ე.წ. ნორმატივების იერარქიის პრინციპთან.

რა არის ევროკავშირის მოტივაცია?

პერსონალურ მონაცემთა დამუშავების დარგი დინამიკურად ვითარდება. მისი მიზანი იყო მონაცემთა დაცვის ძირითადი უფლება „გაღებულიყო მომავლისთვის“. მეორეული სამართლის ამ პროცესებთან ადაპტირება უფრო სწრაფად და მარტივად არის შესაძლებელი, ვიდრე პირველადი სამართლის.

4. მეორეული სამართალი: მონაცემთა დაცვის ძირითადი რეგულაცია

2018 წლის მაისის შემდეგ, მონაცემთა დაცვის ძირითადი რეგულაცია - აბრევიატურით “GDPR” - ძალაშია მეორეული კანონმდებლობის დონეზე. მან ჩაანაცვლა ევროპული დირექტივა, ე.წ. მონაცემთა დაცვის დირექტივა (95/46/EC), რომელიც არსებობდა 1995 წლიდან.

ა. განსხვავება ევროკავშირის რეგულაციასა და ევროკავშირის დირექტივას შორის

თუ რა გავლენა აქვს ამას ევროპულ მონაცემთა დაცვაზე ცხადი ხდება მხოლოდ მაშინ, როცა ხედავ განსხვავებას ევროკავშირის რეგულაციასა და ევროკავშირის დირექტივას შორის:

დირექტივები შემოიფარგლებიან ევროკავშირის წევრი სახელმწიფოებისთვის მხოლოდ კონკრეტული შედეგის დადგენით. თუმცა, ამ შედეგების მიღწევა თვითონ წევრი სახელმწიფოების ვალდებულებაა. მათ უნდა მოახდინონ დირექტივების ტრანსფორმირება თავიანთი საკუთარი სამართლებრივი აქტების მეშვეობით კონკრეტულ ვადებში. ამისგან განსხვავებით, ევროკავშირის რეგულაციებს აქვთ პირდაპირი და მყისიერი დამავალდებულებელი ძალა ევროკავშირის ყველა წევრი სახელმწიფოსთვის, და არა მხოლოდ შედეგის მიღწევასთან მიმართებაში, დირექტივის მსგავსად.

რამ აიძულა ევროკავშირი, რომ ყოფილი მონაცემთა დაცვის დირექტივა ჩაენაცვლებინა რეგულაციით?

ყოფილი მონაცემთა დაცვის დირექტივის მიხედვით, ევროკავშირის ყველა წევრ-სახელმწიფო ეყრდნობოდა ერთსა და იმავე სამართლებრივ საფუძველს. თუმცა, მათ შეეძლოთ თვითონ გადაეწყვიტათ მონაცემთა დაცვის განხორციელება. შესაბამისად, ევროკავშირის ინდივიდუალურ წევრ სახელმწიფოებში არსებობდა მნიშვნელოვანი დისბალანსი მონაცემთა დაცვის დონესთან მიმართებით. მონაცემთა დაცვის ძირითადი რეგულაციის (GDPR) დანერგვით, რომელსაც გააჩნია პირდაპირი და მყისიერი სამართლებრივად სავალდებულო ძალა ყველა წევრ სახელმწიფოში, უნდა აღმოიფხვრას ეს დისბალანსი.

ამასთან დაკავშირებით კიდევ ერთი შენიშვნა! - რადგანაც მე-8 მუხლით განსაზღვრულ მონაცემთა დაცვის ძირითადი უფლებას უფრო სრულყოფილს ხდის ძირითადი რეგულაციის (GDPR) მეორეული კანონი, რაზეც ეს-ესაა მოგახსენეთ,

რეგულაცია ამაღლდა ძირითადი უფლების ხარისხამდე. თუმცა ეს საკითხი სადავოა ევროპის სამართლებრივ დოგმატიკაში.

ბ. მონაცემთა დაცვის ძირითადი რეგულაციის პრინციპები და საკვანძო საკითხები

მინდა გაგაცნოთ მონაცემთა დაცვის ძირითადი რეგულაციის ზოგიერთი ძირითადი დებულება. არ ვამტკიცებ რომ ვიქნები ამომწურავი, თუმცა, უნდა გაირკვეს თუ მონაცემთა დაცვის რა დონისკენ ისწრაფვის ევროკავშირი 2018 წლის მაისიდან.

(1) ერთი მხრივ, არ უნდა შეიზღუდოს მონაცემთა დაცვა სარისკო საინფორმაციო პროცესებამდე

მონაცემთა დაცვის ძირითადი რეგულაცია (GDPR) არ ზღუდავს მის გამოყენებას მხოლოდ სარისკო საინფორმაციო პროცესებამდე, როგორიცაა „სკორინგი“ და ე.წ. „ხელოვნური ინტელექტის“ გამოყენება. პირიქით, იგი გამოიყენება ყველგან უნივერსალურად. და ეს სამართლიანია, რადგანაც საყოველთაო გამომთვლელმა ტექნიკამ გზა გაუკვალა „დიდ მონაცემებს“ ყველა დონეზე. სახელმწიფოსა თუ კერძო პირების ხელთ არსებული მონაცემთა დამუშავების ძალა იზრდება. თუმცა, ფიზიკურმა პირებმა უნდა შეინარჩუნონ კონტროლი საკუთარ მონაცემებზე და ამგვარად შეძლონ გამორიცხონ მესამე მხარის მიერ ამ მონაცემის მოპოვება და გამოყენება. მათ უნდა შეეძლოთ მოიპოვონ ინფორმაცია მათი პირადი მონაცემების შეგროვებასთან დაკავშირებით და შეძლონ მათი წაშლა. რადგანაც პერსონალური მონაცემების მოპოვება ყველგან არის შესაძლებელი, ასეთი მონაცემები დაცული უნდა იყოს არა მარტო კრიტიკულ სფეროებში არამედ ყოველდღიურ ცხოვრებაშიც.

(2) მეორე მხრივ: ეკონომიკური განვითარების არავითარი „შეფერხება“

ბოლო ხანებში, გერმანიის ფედერალური სახელმწიფოს მონაცემთა დაცვის კომისარი გადადგა თანამდებობიდან. იგი არის გერმანიის „თავისუფალი დემოკრატიული პარტიის წევრი“, რომელიც თავიდანვე წარმოადგენს ბიზნესისა და ეკონომიკის ინტერესებს. გადადგომის მიზეზად დაასახელა: „ევროპული მონაცემთა დაცვა ეწინააღმდეგება ბიზნესს. საერთაშორისო კონკურენციაში იგი ევროკავშირის ეკონომიკას არამომგებიან მდგომარეობაში აყენებს. მონაცემთა დაცვა ვერ ახერხებს აღიაროს რომ პერსონალურ მონაცემებსაც გააჩნიათ ეკონომიკური პოტენციალი, ეკონომიკური ღირებულება“.

აქ აუცილებელია ფართოდ გავრცელებული ცრურწმენის გაფანტვა!- მონაცემთა დაცვის ძირითადი რეგულაცია (GDPR) კი არ კრძალავს ეკონომიკაში მონაცემთა დაცვის გამოყენებას, არამედ იცავს მას. მონაცემთა დაცვის ძირითადი რეგულაციის (GDPR) პირველი მუხლი ერთმნიშვნელოვნად იცავს „პერსონალურ მონაცემთა თავისუფალ გადაადგილებას“. აქედან გამომდინარე, მონაცემთა დაცვა არ შეიძლება იყოს მისი არც შეზღუდვის და არც სრულად აკრძალვის მიზეზი. ამიტომ, მონაცემთა დაცვა ეკონომიკაში არ არის აკრძალული; მან მხოლოდ უნდა დაიცვას დამუშავების ის პირობები, რომლებიც რეგულირებულია მონაცემთა დაცვის ძირითადი რეგულაციის (GDPR) მე-6 მუხლით. იმის უზრუნველსაყოფად, რომ ევროპულმა

მონაცემთა დაცვამ არ „ჩაახშოს“ ეკონომიკის დიგიტალიზაცია - „ფაილზე დაფუძნებული თუ ხელოვნური ინტელექტის აპლიკაციები“, ზედამხედველი ორგანოები და სასამართლოები ევროკავშირში მნიშვნელოვანი ამოცანის წინაშე დგანან: მონაცემთა დაცვაზე არც გადამეტებულად უნდა გამახვილდეს აქცენტი და არც უნდა „გახდეს აბსოლუტური“, არამედ აუცილებელია ეკონომიკური ინტერესების პერსონალურ მონაცემთა დაცვასთან სათანადო ბალანსირება.

აქტუალური მაგალითი: რადგანაც ამ მხრივ მონაცემთა დაცვა მიჩნეულია აბსოლუტურად, მართლმსაჯულების ევროპული სასამართლო კრძალავს ვიდეო კონფერენციის სისტემისათვის პროგრამული უზრუნველყოფის გამოყენებას თუ იგი შემოდის ევროპის გარედან - ამ კონკრეტულ შემთხვევაში, აშშ-დან: Zoom, Microsoft Teams, Cisco Webex, ა.შ. მაგრამ თუ არ არსებობს შესაბამისი ტექნიკური ალტერნატივა ევროპაში, მაშინ ევროპულ ეკონომიკისთვის ისინი საჭიროა.

(3) გამოყენების სფეროები, შექმნის პრინციპი, ბაზრის ადგილის პრინციპი, მონაცემთა გადატანა მესამე ქვეყნებში

სიტუაცია, რომელშიც GDPR გამოიყენება იმართება რეგულაციის მე-2 მუხლით. ეს ფართოდ უნდა იყოს გააზრებული; პრინციპში, ეს გამოყენებადობა ყოვლისმომცველია. GDPR სამართლებრივად დამავალდებულებელია როგორც საჯარო ისე არასაჯარო ორგანიზაციებისთვის და ასევე გულისხმობს კერძო მხარეებს; თუმცა, ეს არ ვრცელდება პოლიციის აქტივობებზე და კანონის ცხოვრებაში გატარებაზე. აქ გამოიყენება ცალკე, მაგრამ ანალოგიურად სტრუქტურირებული დირექტივა.

GDPR უშვებს მონაცემთა ავტომატურ დამუშავებას. ეს ფართოდ უნდა იყოს გააზრებული. ამ მხრივ, მე-2 მუხლი არის „ტექნოლოგიურად - ნეიტრალური“. იგი არ მოიცავს მონაცემთა ზუსტად ანალოგიურ შენახვას და წმინდად ხელით დამუშავებას - ინდექს ბარათებზე, დოკუმენტის ფორმებზე და ა.შ. გამონაკლისს წარმოადგენს მონაცემთა დამუშავება ოჯახურ გარემოში, რაზეც მონაცემთა დამუშავების ძირითადი კანონი არ ვრცელდება და ეწოდება საოჯახო პრივილეგია.

GDPR მხოლოდ ევროკავშირში გამოიყენება თუ მთელ მსოფლიოში, მონაცემთა საზღვრებს გარეთ მათი გლობალური გადინების გამო?

ჩვენს ონლაინ სამყაროში, პერსონალურ მონაცემთა დამუშავებამ არ იცის ტექნიკური საზღვრები. ამიტომ, GDPR -ს გამოყენება ტერიტორიულად შეზღუდული უნდა იყოს. რადგანაც ევროკავშირის ყველა წევრი სახელმწიფო ვალდებულია უზრუნველყოს მონაცემთა ერთი და იგივე დონით დაცვა, იგი, ბუნებრივია, გამოიყენება ევროკავშირის ტერიტორიაზე ყოველგვარი შეზღუდვის გარეშე. თუმცა, განსაკუთრებული სიფრთხილეა საჭირო მონაცემთა არა-ევროპული კომპანიების მიერ დამუშავების შემთხვევაში. ასევე ეჭვს იწვევს მონაცემების გადატანა ევროკავშირის გარეთ ქვეყნებში. იქ მონაცემთა დაცვის დონე ხშირად მნიშვნელოვნად დაბალია. GDPR ამ პრობლემებს გადაჭრის მე-3 მუხლში განსაზღვრული დაფუძნებისა და მოქმედების ტერიტორიული სფეროს პრინციპით. არაევროპული ქვეყნები, რომლებსაც წარმომადგენლობა ჰყავთ ევროკავშირის ტერიტორიაზე, ვალდებულნი არიან დაიცვან რეგულაცია, მაგრამ ამისათვის არ არის საკმარისი უბრალოდ საფოსტო ყუთი ევროკავშირში. თუ ასეთ კომპანიას არ ჰყავს წარმომადგენლობა ევროკავშირის ტერიტორიაზე, იგი მაინც ვალდებულია, დაიცვას GDPR, თუ იგი ფუნქციონირებს ევროკავშირის შიდა ბაზარზე. ამიტომ, Google and Facebook – Meta ექვემდებარებიან ევროპის მონაცემთა დაცვის კანონს.

რა ვუყოთ პერსონალ მონაცემთა ღრუბელს? არსებობს აქ „ამბრაზურა“? - არა! - ეს შემთხვევა დამოკიდებულია იმაზე, თუ სად მდებარეობს სერვერი.

თუ მონაცემები იმპორტირებულია მესამე ქვეყნებში, შესაფერისი დაცვის დონე უნდა იყოს უზრუნველყოფილი. მონაცემთა ევროკავშირის გარეთ დაცვა - ხანდახან მოიხსენიებენ როგორც „მონაცემთა დაცვის ოქროს სტანდარტი“ - ხშირად ვერ ხერხდება. GDPR-ის 45-ე მუხლის მიხედვით, ასეთი მონაცემების გადატანა ნებადართული უნდა იყოს ევროკავშირის კომისიის ე.წ. ადეკვატური გადაწყვეტილებით. მე მონაცემთა დაცვის ხელშეკრულებებს დავუბრუნდები აშშ-სთან ერთად მოგვიანებით.

(4) ძირითადი აკრძალვა ნებართვის, უფლებამოსილებისა და თანხმობის შენარჩუნებით

ევროპულ მონაცემთა დაცვის კანონზე ვრცელდება შემდეგი პრინციპები: ამოსავალ წერტილს წარმოადგენს ზოგადი აკრძალვა ნებართვის შენარჩუნებით.

რას ნიშნავს ეს? პერსონალურ მონაცემთა დამუშავება ზოგადად არის აკრძალული თუ იგი არ არის კანონით დაშვებული ან თუ მონაცემების მფლობელი - მონაცემთა სუბიექტი- წინასწარ იძლევა თავის თანხმობას. ევროკავშირი ამგვარად თანხმდება პრევენციულ მიდგომაზე, რითაც პერსონალურ მონაცემთა დაცვა ხდება უკიდურესად პრიორიტეტული.

GDPR-ს მე-6 მუხლი არეგულირებს, თუ როდის არის პერსონალურ მონაცემთა დაცვა ნებადართული. აქ არ მინდა სიღრმეებში შესვლა; ამიტომ, ძალიან მოკლედ! ხუთი საფუძველი არსებობს ნებართვის გაცემისთვის: მონაცემთა დაცვა კანონიერია, როცა ის დაკავშირებულია კონტრაქტის დადებასთან ან შესრულებასთან; თუმცა, საკონტრაქტო ურთიერთობის დასრულების შემდეგ, პერსონალური მონაცემები უნდა წაიშალოს. მონაცემთა დამუშავება ასევე შეიძლება მოხდეს, თუ მონაცემთა სუბიექტის სასიცოცხლოდ მნიშვნელოვანი ინტერესები ზარალდება, მაგალითად, პანდემია კორონას ან ბუნებრივი უბედურებების წინააღმდეგ ბრძოლის დროს. დამუშავება ასევე ნებადართულია მონაცემთა დამმუშავებელი პირის ლეგიტიმური ინტერესის არსებობის შემთხვევაში. ეს ის შემთხვევაა, როცა „მონაცემთა სუბიექტი“ დამმუშავებლის კლიენტია ბიზნესის საქმისწარმოებებში ან უბრალოდ დასაქმებულია მის მიერ. ასეთი კანონიერი ინტერესია, მაგალითად, „მონაცემთა სუბიექტის მიერ თაღლითობის ჩადენის პრევენცია.“ და ბოლოს, სახელმწიფო დავალებების შესრულება საკმარისი საფუძველია მონაცემთა დამუშავებისთვის. ამ მხრივ, ევროპული პრეცედენტული სამართალი ახლა პრაქტიკულად უმართავია.

როგორც ნებართვის მიცემის ალტერნატივა, მონაცემთა სუბიექტის თანხმობა შეიძლება გახდეს პერსონალურ მონაცემთა დამუშავების საფუძველი. აქაც მხოლოდ რამდენიმე შენიშვნა: თანხმობა უნდა იყოს ნებაყოფლობითი, და შესაბამისმა „მონაცემთა სუბიექტმა“ უნდა იცოდეს თავისი თანხმობის მნიშვნელობა. როგორც წესი, მცირეწლოვნებს 14 წლის ასაკამდე არ შეუძლიათ კანონიერი თანხმობის მიცემა. მონაცემთა დამუშავების შემდგომ გაცემული თანხმობა, რომელსაც „ავტორიზაცია“ ეწოდება იურიდიულ ტერმინოლოგიაში - არ არის საკმარისი დამუშავების გასამართლებლად.

(5) მონაცემთა კლასიფიკაცია

შესაძლებელია პერსონალური მონაცემების კლასიფიცირება. ზოგიერთი მონაცემის მოპოვება შესაძლებელია ზოგადად ხელმისაწვდომი წყაროებიდან - ტელეფონის და მისამართების წიგნიდან, ინტერნეტიდან, სხვა მონაცემების მიღება კი უფრო გართულებული გზით არის შესაძლებელი. ზოგი მონაცემები საჭიროა პიროვნების ინტეგრაციისათვის - ზოგი სენსიტიურია, ზოგი არა. უმეტეს შემთხვევაში, ზოგადად ხელმისაწვდომი და ნაკლებად სენსიტიური მონაცემები ნაკლებად მნიშვნელოვანია მონაცემთა სუბიექტის თვალსაზრისით. რადგანაც GDPR-ის მე-6 მუხლი არ ახდენს კლასიფიცირებას, რეგულაციის მე-9 მუხლი ითვალისწინებს კვალიფიცირებული მონაცემების უფრო საიმედო დაცვას, რომელიც მოიცავს, მაგალითად, ეთნიკურ წარმომავლობასთან, რელიგიურ და პოლიტიკურ რწმენასა, ასევე ჯანმრთელობისა და სექსუალურ ორიენტაციასთან დაკავშირებული მონაცემებს.

რას ითვალისწინებს ევროპული მონაცემთა დაცვა ე. წ. საჯარო პირებისთვის - პოლიტიკოსები, მოსამართლეები, მსახიობები, ა.შ.?

საზოგადოება დიდ ინტერესს ავლენს იმ პიროვნებების მიმართ, რომლებიც გამოჩენილები არიან, ანუ რომლებიც სარგებლობენ გარკვეული ხარისხის ცნობადობით. ე.წ. საზოგადოებრივ სფეროში საჯარო გამოჩენის ან საჯარო განცხადების გაკეთების შემთხვევაში ამ პიროვნებების მონაცემთა დაცვა შეზღუდულია. ამ სფეროში, პერსონალური მონაცემები შეიძლება შეგროვდეს, მაგ. ფოტოსურათების გადაღებით მათი თანხმობის გარეშე. საქმე ეხება ე.წ. პრივატულ ან ინტიმურ სფეროსაც კი შინაური სფერო და ოჯახი-, სადაც ისეთივე დაცვა არსებობს როგორც არაცნობადი პირებისთვის. მაშინ GDPR-ის მე-9 მუხლი გამოიყენება შეზღუდვების გარეშე.

(6) საინფორმაციო ვალდებულებები, წვდომის, შესწორების, წაშლის და დაბლოკვის უფლებები

როგორც სიახლე წინა სამართლებრივი სიტუაციასთან შედარებით, GDPR უზრუნველყოფს მონაცემთა მფლობელებისთვის მთელ რიგ უფლებებს მე-12 და მე-17 მუხლების მეშვეობით. მათი მიზანია დაცვის უფლების მოქმედებაში მოყვანის ხელშეწყობა მონაცემთა დაცვის კანონის მიხედვით. ეს იწყება ინფორმირების ვალდებულებით, რომელიც პერსონალურ მონაცემთა უფლებამოსილი პირის მოვალეობაა და რომელმაც ამგვარად უნდა „გახსნას“ დამუშავების „შავი ყუთი“. ეს ვრცელდება, პირველ რიგში, „მონაცემთა უსაფრთხოების დარღვევის“ ყველა შემთხვევაზე, როცა ხდება მონაცემთა არაკონტროლირებადი გადინება. დაცვის საშუალებები, რომლებიც „მონაცემთა სუბიექტისგან“ მოითხოვენ გამოიჩინონ ინიციატივა, არიან წვდომის უფლება და შესწორების უფლება მონაცემთა უფლებამოსილი პირთან მიმართებით.

განსაკუთრებით აღსანიშნავია მონაცემთა სუბიექტის უფლება საკუთარი მონაცემების წაშლასთან დაკავშირებით, რომელიც უზრუნველყოფილია GDPR-ის მე-17 მუხლით. ბოლო წლებში იგი ცნობილი გახდა როგორც „დავიწყების უფლება“. ევროპის მართლმსაჯულების სასამართლომ განმარტა ეს უფლება თავის ოთხ გადაწყვეტილებაში Google-ის წინააღმდეგ 2014 წლის შემდეგ. თუ არ წაიშლება პერსონალური მონაცემები ისინი უნდა დაიბლოკოს მომხმარებლისთვის.

(7) „წინასწარი“ მონაცემების დაცვა: მონაცემთა დაცვა „მომსახურების შექმნის პროცესში“ (by design) და „პირველად პარამეტრად“ (by default)

ევროპის მონაცემთა დაცვის კანონის ნოვატორული ინოვაციაა აგრეთვე ის, რომ დამმუშავებელმა უნდა მიიღოს პრევენციული ზომები და თავიდან აიცილოს „წინასწარ“ მონაცემთა უსაფრთხოების დარღვევა. დღემდე, ამ სფეროში ერთადერთი ხელმისაწვდომ იურიდიულ საშუალებას წარმოადგენდა რეგულაციები ე.წ. მონაცემთა ეკონომია ან მონაცემთა მინიმიზაცია. ახლა კი, პერსონალურ მონაცემთა ზომიერი გამოყენება უნდა განხორციელდეს ტექნიკური ან ორგანიზაციული სიფრთხილის ზომების გამოყენებით - „მომსახურების შექმნის პროცესში“ (by design) ან - სტანდარტული პარამეტრებით - „პირველად პარამეტრად“ (by default). პირველი სფერო შეიცავს, მაგალითად, ე.წ. „ფსევდონიმიზაციას“, მეორე სფერო კი ე.წ. ნიმუშებს. ამ პრინციპების დარღვევა ისჯება ჯარიმით.

გ. ექსკურსი: საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“

მომზადებისას, მე ძალიან სწრაფად და ზედაპირულად გადავხედე საქართველოს კანონს პერსონალური მონაცემების დაცვის შესახებ, რომელიც ვნახე პერსონალურ მონაცემთა დაცვის სამსახური მთავარ გვერდზე. მე ვფიქრობ, ეს ისევ აქტუალურია. ამისთვის 2016 წლის დეკემბერს კანონში მიღებული ბოლო ცვლილებებიდან, როგორც ჩანს, მოდელად გამოყენებულია ევროპული მონაცემთა დაცვის ყოფილი დირექტივა (95/46/EC). თუმცა, როგორც ეს განვიხილეთ, GDPR ახლა განსაზღვრავს ახალ პრიორიტეტებს. ორმა საკითხმა გამაოცა: ერთის მხრივ, ქართული კანონი მნიშვნელოვანი ხარისხით ათავისუფლებს მედიას მონაცემთა დაცვის კანონის გამოყენებისგან ჟურნალისტური მიზნებისთვის მონაცემების შეგროვებისას. მეორეს მხრივ, კანონი- როგორც მე წავიკითხე - ასევე ვრცელდება ანალოგიურ მონაცემთა დამუშავებაზე- „მონაცემთა დამუშავება არა-ავტომატური საშუალებებით“.

5. კონფლიქტების ახლანდელი სფეროები ევროპის კავშირში

როგორც უკვე აღვნიშნე ჩემს პრეზენტაციაში, პერსონალურ მონაცემთა დაცვის უფლება არ წარმოადგენს „სუპერ ფუნდამენტურ უფლებას“. მისი მინიჭება არ ხდება სრულფასოვნად, შეზღუდვებისა და პირობების გარეშე. მაგალითად, ის შესაძლოა წინააღმდეგობაში მოვიდეს ასევე დაცულ ინტერნეტ მომხმარებლების უფლებასა და მედია კომპანიების უფლებებთან ინფორმაციის მოპოვებასთან დაკავშირებით. მაგრამ იგი ასევე შეიძლება კონფლიქტში მოვიდეს ხელოვნების, მეცნიერების და კვლევის თავისუფლებებთან. ამას ხშირად „მულტიპოლარულ კონფლიქტს“ უწოდებენ. ამ შემთხვევებში, სხვადასხვა ინტერესები უნდა აიწონოს ერთმანეთის საპირწონედ და დაბალანსდეს: ე.წ. პრაქტიკული შესაბამისობა.

ა. მონაცემთა დაცვა და ინფორმაციის თავისუფლება - ინტერნეტის მომხმარებლები და მედია კომპანიები

ევროკავშირში ყოველთვის ემოციური დებატები იმართება მონაცემთა დაცვის კანონსა და ინფორმაციის თავისუფლებას შორის; ეს უკანასკნელი წარმოადგენს

გამოხატვის თავისუფლების მანიფესტაციას. ეს რატომაც ხდება ადვილი ასახსნელია: მონაცემთა სუბიექტს სურს შეინარჩუნოს კონტროლი თავის პერსონალურ მონაცემებზე. როგორც წესი, ინტერნეტის მომხმარებლებსა და მედია კომპანიებს ჩვეულებრივ უნდათ პირად ცხოვრებაში შეჭრა, რამდენადაც ეს შესაძლებელია.

შეკითხვა: შეიცავს GDPR ამ კონფლიქტის გადაჭრის გზებს?

დიახ! - თუმცა, ევროკავშირი თვითონ ვერ აბალანსებს ინტერესების კონფლიქტს. ნაცვლად ამისა, GDPR- ის 85-ე მუხლი ამას ავალებს ევროკავშირის წევრ-სახელმწიფოებს. მათ ამ მიზნით უნდა გამოსცენ საკანონმდებლო დებულებები. 85-ე მუხლი წარმოადგენს ე.წ. შესავალ პუნქტს, რომელიც სთავაზობს წევრ სახელმწიფოებს „მოქმედების თავისუფლებას“. თუმცა, GDPR ასევე იძლევა ერთ მითითებას: ზემოხსენებული დებულების მე-2 პარაგრაფი ავალდებულებს წევრ-სახელმწიფოებს მოახდინონ GDPR-ს „შესუსტება“ და მისგან „გათავისუფლება“ იმ შემთხვევაში, თუ მონაცემთა დამუშავება ემსახურება ჟურნალისტურ მიზნებს. ფონი: ასეთი „მედიის პრივილეგია“ იყო და ახლაც ფართოდაა გავრცელებული ევროკავშირის წევრ-სახელმწიფოების ეროვნულ კანონში

უბრალოდ ინტერესისთვის: რა ზომებს განიხილავენ წევრი სახელმწიფოები ამ შემთხვევაში?

ერთი საშუალება, მაგალითად, არის დაავალდებულო პლატფორმის ოპერატორები დააყენონ ფილტრაციის სისტემები - ე.წ. ფილტრების ჩატვირთვა. თუმცა, ჩატვირთული ფილტრების სისტემამ, რომელიც ძალიან მასშტაბურია და არ გააჩნია კონტურები და რასაც მივყავართ შინაარსის „ზედმეტად ბლოკირებამდე“, რაც არ წარმოადგენს პრობლემას მონაცემთა დაცვის კუთხით, შესაძლებელია დაარღვიოს ინფორმაციის თავისუფლება.

ბ. მონაცემთა შეკავების მუდმივი პრობლემა

საკითხს, რომელიც ამჟამად იპყრობს მედიის ყურადღებას, წარმოადგენს ე.წ. მონაცემთა შეკავება. ეს შეეხება ტელეკომუნიკაციის კომპანიების ვალდებულებას შეინახონ მომხმარებელთა მდებარეობისა და სერვისების მოძრაობის შესახებ მონაცემები კონკრეტული მიზეზის გარეშე და დიდ ხნის განმავლობაში. ამის მიზანია გაუადვილონ უსაფრთხოების ორგანოებს შეებრძოლონ სერიოზულ დანაშაულსა და საერთაშორისო ტერორიზმს.

ე.წ. მონაცემთა შეკავებამ უკვე შექმნა სამართლებრივი ისტორია: თავდაპირველად, ევროპულმა დირექტივამ მოითხოვა ევროკავშირის წევრ-სახელმწიფოებისგან წინასწარ შეინახონ მდებარეობისა და მოძრაობის მონაცემები. ევროპული მართლმსაჯულების სასამართლოს თავდაპირველი თავშეკავების შემდეგ დირექტივა გამოცხადდა არავალიდურად 2014 წელს. მიზეზი: დირექტივა არაპროპორციულად ზღუდავდა პერსონალურ მონაცემთა დაცვას.

მომდევნო პერიოდში მართლმსაჯულების ევროპულმა სასამართლომ ხელახლა განიხილა კანონები ე.წ. მონაცემთა შეკავების შესახებ. შედეგად, იგი დარჩა უცვლელი თავისი საწყისი პოზიციით, რომლის მიხედვით ასეთი შეკავება წარმოადგენს მონაცემთა დაცვის კანონის არაპროპორციულ ხელყოფას. მიუხედავად ამისა, ევროკავშირის წევრი სახელმწიფოები გამუდმებით გამოსცემდნენ რეგულაციებს ე.წ. მონაცემთა შეკავების შესახებ. მთლიანობაში, ევროპულმა მართლმსაჯულების სასამართლომ შვიდი გადაწყვეტილება გამოიტანა გერმანიის, ესტონეთის, საფრანგეთის, ირლანდიის, ავსტრიის და შვედეთის წინააღმდეგ ბოლო ათი წლის განმავლობაში. პოლიტიკურ არენაზე, ახლა განიხილება ე.წ. მონაცემთა

შეკავების საკითხი: ე.წ. სისტემაში შესვლის მახე და ე.წ. „სწრაფი გაყინვის“ პროცედურა. ე.წ. სისტემაში შესვლის (login) მახე იძლევა კრიმინალების IP მისამართების ავტომატური შენახვის საშუალებას მასიური მეთვალყურეობის ჩატარების გარეშე. ე.წ. „სწრაფი გაყინვის“ პროცედურის საშუალებით უსაფრთხოების ორგანოებს შეუძლიათ გაყინონ მდებარეობისა და მოძრაობის შესახებ მონაცემები პროვაიდერთან. ისინი შემდგომში შეძლებენ მიიღონ მათზე წვდომა სასამართლოს გადაწყვეტილებით

გ. ხელოვნური ინტელექტის გამოყენება: ChatGPT

ე.წ. ხელოვნური ინტელექტის გამოყენება პრინციპში არ არის რეგულაციის საგანი GDPR-ის მიხედვით. მიუხედავად ამისა, მან შესაძლოა პრობლემები წარმოშვას მონაცემთა დაცვის კანონის მხრივ.

ერთ-ერთ მაგალითს წარმოადგენს ტექსტ რობოტი "ChatGPT"; “GPT" ნიშნავს „გენერაციულ წინასწარ მომზადებულ ტრანსფორმერს“. იგი ბაზარზეა უკვე 2022 წლის ნოემბრიდან და ამჟამად იპყრობს დიდ ყურადღებას მთელ მსოფლიოში. იმისათვის, რომ მოხდეს მისი კლასიფიცირება მონაცემთა დაცვის კუთხით, საჭიროა ცოდნა იმისა თუ როგორ მუშაობს: "ChatGPT" უნდა შეიმუშაოს ტექსტები მომხმარებლის შენატანის საფუძველზე. ეს დამოკიდებულია ე.წ. ხელოვნურ ინტელექტზე, რომელიც უზარმაზარ მონაცემებზეა მომზადებული. ინდივიდუალურ მომხმარებელს მართლაც შეუძლია დაიცვას თავისი პერსონალური მონაცემები, თუ არ შეიყვანს მათ პროგრამაში. თუმცა, მთავარი მონაცემთა დაცვის პრობლემა სხვაგანაა. ის დაკავშირებულია ტექსტ რობოტის მონაცემთა ბაზაზე. არსებობს რისკი რომ მოსამზადებელი მასალა ასევე შეიცავს პერსონალური ხასიათის მონაცემებს. ეჭვის შემთხვევაში მათმა დამუშავებამ შეიძლება გამოიწვიოს მონაცემთა უსაფრთხოების დარღვევა რაზეც პასუხისმგებლობა ეკისრება მომხმარებელს. GDPR-ით გათვალისწინებული ჯარიმები მაღალია.

დ. პერსონალურ მონაცემთა გადატანა პორტირება (გადატანა) აშშ-ში

მონაცემთა ტრანსსასაზღვრო პორტირება მესამე ქვეყანაში ვაჭრობისა და ბიზნესისთვის აუცილებელია, მაგრამ რისკის ქვეშ აყენებს მონაცემთა დაცვას. GDPR -ის 45-ე მუხლის მიხედვით, ასეთი მონაცემთა გადატანა მოითხოვს ევროკავშირის კომისიის მიერ ე.წ. ადეკვატური გადაწყვეტილების მიღებას. ეს ასევე ეხება მონაცემთა პორტირებას აშშ-ში.

„ედვარდ სნოუდენის“ საქმისა და აშშ დაზვერვის სამსახურების მიერ მასზე განხორციელებული მეთვალყურეობის შემდეგ ამერიკული მონაცემთა დაცვისადმი ნდობა ევროკავშირში მეტ-ნაკლებად დაიკარგა. ევროკავშირის მოქალაქეები ასევე შეიძლება აღმოჩნდნენ მეთვალყურეობის ქვეშ აშშ-ში, მაგალითად, როცა ისინი აგზავნიან შეტყობინებებს ამერიკული Facebook ქსელის- Meta მეშვეობით.

2000 წელს, ევროკავშირის კომისიამ გააფორმა მონაცემთა დაცვის ხელშეკრულება აშშ-თან, რომელსაც ეწოდება „უსაფრთხო ნავსადგური“ (Safe Harbour). იგი არეგულირებდა მონაცემთა დაცვის კანონის შესრულებას, რომელიც მოეთხოვებოდათ ამერიკულ კომპანიებს და გამიზნული იყო აშშ-ში მონაცემთა დაცვის დონის ევროპულამდე აწევაზე. ხუთი წლის შემდეგ, ევროპის მართლმსაჯულების სასამართლომ გამოაცხადა ეს შეთანხმება -„უსაფრთხო

ნავსადგური“ ძალადაკარგულად. სასამართლომ მიუთითა კანონზე USA PATRIOT, რომელიც საშუალებას აძლევდა ამერიკულ დაზვერვის სამსახურებს ჰქონოდათ წვდომა პერსონალურ მონაცემებზე მონაცემთა სუბიექტის თანხმობის გარეშე.

შემდეგ წელს კი, მოლაპარაკება გაიმართა ახალ შეთანხმებაზე აშშ-სთან, „EU-US Privacy Shield“ (შეთანხმება ევროკავშირსა და აშშ შორის „პირადი ცხოვრების ფარი“). მიუხედავად იმისა რომ იგი უზრუნველყოფდა მონაცემთა დაცვის სრულყოფას, მაინც არ იყო საკმარისი ევროპული სასამართლოსთვის. 2020 წელს, სასამართლომ ასევე მიიჩნია ეს ხელშეკრულება და ევროკავშირის კომისიის ე.წ. ადეკვატური გადაწყვეტილება არაკანონიერად. გასაგებია ეს რასაც ნიშნავს: ამჟამად, მონაცემთა დაცვის კანონის შესაბამისად, ჯერ კიდევ არაკანონიერია გარკვეული პერსონალურ მონაცემთა პორტირება ევროკავშირიდან აშშ-ში. ცნობისათვის, ამჟამად ევროკავშირის კომისია ევროკავშირ-აშშ მონაცემთა დაცვის მესამე ხელშეკრულების დამუშავების პროცესშია.

6. მონაცემთა დაცვის კანონის მომავალი განვითარება - ევროპული კომისიის რეგულაციური გააფთრება

ახლა მინდა რამდენიმე სიტყვა გითხრათ სამართლებრივ განვითარების შესახებ ევროკავშირში!

მონაცემები ყველგანაა და სუნთქვაშემკვრელი ტემპით იზრდება. მასთან ასოცირებულ სარგებლობას ბიზნესისთვის, მეცნიერებისა და ადმინისტრირებისთვის ეიფორიულად მიესალმებიან. მონაცემები გახდა საკვანძო უპირატესობა ეკონომიკისთვის. ამავე დროს, ჩივიან ასევე პერსონალურ მონაცემთა დაცვის ნაკლზეც, რაც არის მონაცემთა თავისუფალი გადინების შედეგი. ზოგჯერ ორივე შეხედულება ცალსახად ურთიერთსაწინააღმდეგოა. თუმცა, თანხმდებიან იმაზე, რომ ევროპას ჭირდება სამართლებრივი ბაზა, რომელიც სცილდება მონაცემთა დაცვის ძირითადი რეგულაციის ფარგლებს.

2020 წლიდან ევროკავშირის კომისია მუშაობს ე.წ. ევროპულ სტრატეგიაზე მონაცემების კუთხით; ამით, მას სურს უზრუნველყოს, რომ მონაცემთა ერთიანი ბაზარი რაც შეიძლება თავისუფალი იყოს ევროკავშირის ეკონომიკისა და მისი გლობალური კონკურენტუნარიანობის ინტერესებიდან გამომდინარე. ამ მხრივ, მან წამოაყენა წინადადებები ოთხი ევროპული რეგულაციის შესახებ: პირველი, „მონაცემთა მართვის კანონი“, რომლითაც სურს შექმნას „მონაცემთა შუამავალი სერვისის პროვაიდერი“, რომელიც, როგორც ნეიტრალური ორგანო და რომელსაც არ გააჩნია ეკონომიკური თვით-ინტერესები, შეაგროვებს მონაცემებს და, თუ დააკმაყოფილებს გარკვეულ სამართლებრივ მოთხოვნებს, მიაწოდებს მათ დაინტერესებულ მხარეებს. ამ პრინციპს ეწოდება „მონაცემთა ალტრუიზმი“. ამ გზით, მას სურს შეზღუდოს მონაცემთა მონოპოლისტების როგორიცაა Apple, Amazon, Facebook – Meta და Google-ს ძალაუფლება. მეორე წინადადება, როგორიცაა „მონაცემთა კანონი“ უფრო შორს მიდის: მან უნდა დაარეგულიროს თუ ვის ეკუთვნის მონაცემები რომლებსაც აწარმოებენ თვითონ ქსელური მოწყობილობების მომხმარებლები, როგორიცაა სამეთვალყურეო (CCTV) სისტემები ან ავტონომიური მანქანები. ჯერჯერობით, მხოლოდ ასეთი სისტემების პროვაიდერებს აქვს მათზე წვდომა და არა მომხმარებლებს.

მაგრამ ევროკავშირის კომისია ამას ასე არ ტოვებს!

იგეგმება, რომ „ციფრული მომსახურების კანონი“, რომელიც მიზნად ისახავს ონლაინ პლატფორმების რეგულირებას და მიმართულია ინტერნეტ პროვაიდერების,

ღრუბლის სერვისების, აპლიკაციის მარაგების და სოციალური მედიისკენ. ასეთმა კომპანიებმა უნდა მიიღონ ზომები რომ აღმოაჩინონ და მოსპონ არაკანონიერი პროდუქტი და შინაარსი ადრეული საფეხურიდანვე. კანონის დამრღვევებს მოუწევთ ჯარიმის გადახდა რაც შეადგენს წლიური ბრუნვის 6 პროცენტს. ბოლოს, “ციფრული ბაზრის კანონი“ მომზადების პროცესშია. ის გამიზნულია მხოლოდ დიდი „კარის მცველებისკენ“: Apple, Amazon, Facebook - Meta, Google and Microsoft. ამის მიხედვით, მესენჯერის სერვისების პროვაიდერები და სოციალური მედია ვალდებულნი არიან შემოგვთავაზონ ე.წ. თავსებადი სერვისები. WhatsApp-ის მესიჯები მაშინ მიღებულ უნდა იყოს “Threemo-Messenger” და “Signal”-ის საშუალებით. Apple-ს მსგავს კომპანიებსაც უნდა ჰქონდეთ წვდომა სხვა აპლიკაციების მარაგზე (app stores). მე არ ვაპირებ უფრო შორს წასვლას ამასთან დაკავშირებით. ზოგიერთი ასეთი რეგულაცია უკვე შევიდა ძალაში.

რადგანაც მონაცემთა დამცველებმა უკვე აღარ იციან ევროკომისიის ინიციატივების ციფრულ ჯუნგლებში სად არის „ზემოთ“ და სად „ქვემოთ“, ისინი მოუწოდებენ მონაცემთა დაცვის ახალი, უფრო ეფექტური საშუალებებისაკენ. ერთ-ერთი ასეთი ინსტრუმენტია „მონაცემთა დაცვის რეჟიმის“ შექმნა. როგორც საკუთრების ფლობა, ამან უნდა დაარეგულიროს ვის აქვს უფლებამოსილება განკარგოს და გამოიყენოს პერსონალური მონაცემები. შედარებები კეთდება საავტორო უფლების კანონთან. შეუძლიათ ხალხს გაყიდონ ან გადაიტანონ თავისი მონაცემები? - კიდევ ერთი მიზანი გამომდინარეობს „ევროპის კავშირის ფუნდამენტური ციფრული უფლებების ქარტიიდან“, რომელიც შემოთავაზებულია მონაცემთა დაცვის ექსპერტების მიერ. იგი მიზნად ისახავს ფუნდამენტური უფლებების ევროპული კანონის შევსებას მე-8 მუხლი და პერსონალურ მონაცემთა უკეთესად დაცვას სპეციალური ფუნდამენტური უფლების მეშვეობით. რევოლუციური კონცეფციაა!

7. მონაცემთა დაცვის კონტროლი - „მონაცემთა დაცვის კანონთან შესაბამისობა“ და გარე სამეთვალყურეო ორგანოები

მონაცემთა ეფექტურ დაცვას მონიტორინგი ჭირდება. ვერც ერთი უფლება ვერ იქნება ეფექტური თუ არ არსებობს მისი დაცვის კონტროლი. პერსონალურ მონაცემთა დაცვის უფლება განსაკუთრებით სენსიტიურია, რადგანაც ინდივიდუალური დარღვევები ხშირად შეუმჩნეველი რჩება. მონაცემთა დაცვის კონტროლმა ეს უნდა გაითვალისწინოს.

როგორ განიხილება ეს საკითხი ევროკავშირის კანონში?

თუ გადავხედავთ საწყისს კანონს, ანუ ფუნდამენტური უფლებების ევროპულ ქარტიას, პასუხს ვერ მივიღებთ. მონაცემთა დაცვის ფუნდამენტური უფლების მე-3 პარაგრაფი ნამდვილად მოითხოვს „დამოუკიდებელი ორგანოს“ დაფუძნებას პერსონალური მონაცემების დაცვის შესრულების მონიტორინგისათვის. თუმცა, ამ მოთხოვნის სამართლებრივი მნიშვნელობა საკამათოა ევროკავშირში. მხოლოდ რამდენიმე ექსპერტი უყურებს მას როგორც ნამდვილ ინსტიტუციურ გარანტიას.

ამ შემთხვევაში GDPR უფრო დეტალურია. იგი „ორმხრივია“ და სისტემურად განასხვავებს ერთმანეთისგან „შინაგან კონტროლს“ და „გარეგან კონტროლს“. ამის მიხედვით, მონიტორინგის ჩატარება თავდაპირველად ევალებოდა მონაცემთა უფლებამოსილ პირს, ორგანოებს და კომპანიებს. GDPR-ის 37-ე მუხლის მიხედვით, ისინი ვალდებულნი არიან დანიშნონ მონაცემთა დაცვის ოფიცერი, რომელიც

დამოუკიდებელია საზედამხედველო ორგანოებსა და კომპანიების ფარგლებში. მართალია, მონაცემთა დაცვის ოფიცერს არ მოეთხოვება ორგანოებისა და კომპანიების მნიშვნელოვან გადაწყვეტილებებში მონაწილეობის მიღება, მაგრამ მას აქვს თავისუფალი წვდომა ყველა დამუშავების ოპერაციაზე და ჩართულია მათთან დაკავშირებულ გადაწყვეტილებებში. საინტერესოა აღვნიშნოთ, რომ ასეთი ვალდებულება „მონაცემთა დაცვის უზრუნველყოფისათვის“ არ არსებობდა მონაცემთა დაცვის დირექტივის კანონის(95/46/EC) მიხედვით, რომელიც ძალაში იყო 2018 წლამდე.

შეუძლია ევროპულ კანონმდებლობას ყველაფერი დატოვოს უბრალო თვითრეგულაციის დონეზე?

პასუხია: არა! - ასეთი მონაცემთა დაცვის ოფიცრების მიერ შინაგანი კონტროლის განხორციელებას მართლაც აქვს აზრი; რადგანაც ისინი კარგად იცნობენ თავიანთი ორგანოებისა თუ კომპანიების პროცესებსა და სტრუქტურას და ამიტომ შეუძლიათ ეფექტურად განახორციელონ სისტემატური და რეგულარული კონტროლი. თუმცა, ასეთი შინაგანი კონტროლები ასევე ხასიათდებიან როგორც იერარქიული და დამოკიდებული ურთიერთობები. ამიტომ, GDPR ასევე ეყრდნობა „გარეგანი კონტროლის“ კონცეფციას, რომელსაც მონაცემთა დაცვის გარეგანი სამეთვალყურეო ორგანოები განახორციელებენ.

რისი ცოდნა არის საჭირო ამ „გარეგანი კონტროლის“ შესახებ ევროკავშირის წევრ-სახელმწიფოების დონეზე? - მე მხოლოდ მოკლედ გადმოგცემთ მონაცემთა დაცვის სამეთვალყურეო სისტემის შესახებ მონაცემთა დაცვის ძირითად რეგულაციაში:

GDPR-ის 51-ე მუხლი ითვალისწინებს დამოუკიდებელი საზედამხედველო ორგანოების არსებობას. „დამოუკიდებელი“ ნიშნავს „სრულიად დამოუკიდებელს“. ევროპის მართლმსაჯულების სასამართლოს აზრით, ეს ნიშნავს რომ მონაცემთა დაცვის საზედამხედველო ორგანო შორს უნდა იყოს მთავრობისგან, რაც გულისხმობს რომ საზედამხედველო ორგანო არ უნდა ექვემდებარებოდეს სამინისტროს. „მედია პრივილეგიის“ გამო საზედამხედველო ორგანოების აქტივობებისგან გამონაკლისს წარმოადგენს მედია, ასევე ეკლესიები და, GDPR-ის 55-ე მუხლის მიხედვით, სასამართლოები. ფონი: ეს ხდება სასამართლო სისტემის დამოუკიდებლობის უზრუნველყოფისათვის. მონაცემთა დაცვის ორგანოების ძირითადი ამოცანაა კლასიკური საზედამხედველო მოქმედება, რითაც შესაძლებელია 10 მილიონ ევრომდე ჯარიმის დაკისრება. სამეთვალყურეო ორგანოები სააპელაციო ორგანოებსაც წარმოადგენენ. მათი გადაწყვეტილებები შეიძლება გასაჩივრდეს სასამართლოებში

ჩემი მოხსენების დასკვნის სახით, შემდეგ ხუმრობას მოგახსენებთ: კარგად არის ცნობილი, რომ მასიურად „კონტროლის დეფიციტია“ მონაცემთა დაცვის კანონში ევროკავშირის ყველა წევრ სახელმწიფოში. ახლახან, ვიღაცამ გამოითვალა, რომ გერმანიაში აღნიშნული საკითხების მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ განხილვას მოელიან ყოველ 200 წელიწადში ერთხელ (!)