

პროფილირება და არჩევნები

პასუხისმგებლობის გამომრიცხავი პირობა: ამ ტექსტში გამოთქმული მოსაზრებები გამოხატავს მხოლოდ ავტორის პოზიციას და არ შეიძლება რაიმე ფორმით დაუკავშირდეს იმ ორგანიზაცი(ებ)ის პოზიციას, რომლებთანაც შესაძლოა ავტორი ასოცირდებოდეს. ტექსტის კომენტატორთა მოსაზრებები კი, რა თქმა უნდა მხოლოდ მათ მოსაზრებებს გამოხატავს. ყველა შესაძლო დამთხვევა შემთხვევითია.

ტექნოლოგიურ საუკუნეში პერსონალური მონაცემები ყოველდღიურად მრავალი მიზნით მუშავდება და ამ დამუშავების გარეშე ბევრი სასიცოცხლოდ აუცილებელი სერვისი თუ უბრალოდ დამატებითი მომსახურების მიღება იქნებოდა შეუძლებელი. თუმცა საკითხავია რამდენად შორს მიდის ასეთი დამუშავების შესაძლებლობები და სად გადის ზღვარი, რის მიღმაც ადამიანს შეუძლია საკუთარი პრივატულობა ხელშეუხებლად შეინარჩუნოს. არსებობს კი საერთოდ ასეთი ზღვარი?

ფიზიკურ სამყაროში ადამიანები საკუთარ უსაფრთხოებასა და პრივატულობას ღობის, საკეტისა თუ ფარდების მეშვეობით იცავენ, მაგრამ რა ხდება როდესაც საქმე ვირტუალურ სამყაროზე მიდგება? მზად ვართ იმ რეალობისთვის თვალის გასასწორებლად, როდესაც ჩვენი თითოეული ქმედება თუ ინტერესი აღირიცხება და ამის საფუძველზე ჩვენზე სხვადასხვა დასკვნები კეთდება? პირადი ცხოვრება, იქნება ეს ფიზიკურ თუ ვირტუალურ სივრცეში, ფუნდამენტური უფლებაა და ის, ვინც ჯერ კიდევ არ ფიქრობს, რომ პერსონალურ მონაცემთა დაცვა მნიშვნელოვანია ან ამბობს, რომ არაფერი აქვს დასამალი, უბრალოდ ცრუობს ან არ ფლობს სათანადო ინფორმაციას მონაცემთა გადაჭარბებით დამუშავების თანმდევ შესაძლო რისკებსა და შედეგებზე.

მონაცემთა დამუშავების კანონიერებასა თუ დამუშავების სხვადასხვა ხერხებზე საუბრისას, ერთ-ერთი მნიშვნელოვანი თემაა არჩევნები. მონაცემთა უკონტროლო დამუშავების ყველაზე ცუდი შედეგი სწორედ პოლიტიკურ არჩევანზე ზემოქმედება შეიძლება იყოს, რაც პირდაპირ უკავშირდება ადამიანის თავისუფალი ნების გამოვლინებას, ამომრჩევლით მანიპულირებას და დარტყმის ქვეშ აყენებს კანონიერების, კანონის უზენაესობის პრინციპს.

სწორედ აღნიშნულ თემას და არჩევნების მოსამზადებელ პერიოდში პერსონალური მონაცემების დამუშავებას, შესაძლებლობებს და გამოწვევებს უკავშირდება ბრიტანული ორგანიზაციის Privacy International-ის სტატია პროფილირების თაობაზე (<https://www.privacyinternational.org/case-study/763/case-study-profiling-and-elections-how-political-campaigns-know-our-deepest-secrets>). გთავაზობთ, აღნიშნული სტატიის თარგმანს.

პროფილირება და არჩევნები

როგორ იგებენ პოლიტიკური კამპანიები ჩვენს შავ-ბნელ საიდუმლოებებს

მთელ მსოფლიოში პოლიტიკური კამპანიები მონაცემთა დახელოვნებულ ოპერაციებად იქცა. შტატებში ევენგელისტი ქრისტიანი კანდიდატები მიმართავენ დაურეგისტრირებელ ქრისტიანებს და ქულების (სქორინგის) სისტემის გამოყენებით ცდილობენ წინასწარ განსაზღვრონ რამდენად სერიოზულად იღებს მილიონობით ასეთი ამომრჩეველი მათ რწმენას. ჯერ კიდევ 2008 წელს ობამას კამპანიის დროს გამოყენებული იქნა მეთოდი/ოპერაცია, რომლის მიხედვითაც შტატების თითოეულ ამომრჩეველს მიენიჭა ქულების წყვილი იმის განსასაზღვრად თუ ერთი მხრივ, რამდენად მოსალოდნელი იყო ამომრჩევლის მონაწილეობა არჩევნებში და, მეორე მხრივ, უჭერდნენ თუ არა ისინი მხარს ობამას. ამ ქულებზე დაფუძნებული ვარაუდები კი იმდენად სარწმუნო იყო, რომ ობამას კონსულტანტი კენ სტრასმა პირდაპირ ტრაბახობდა: „ჩვენ მანამდე ვიცოდით ვის მისცემდა ხალხი ხმას, სანამ ამას თვითონ გადაწყვეტდნენ“. ზედმეტად ხომ არ ხდება ამომრჩევლის მიზანში ამოღება?

რა მოხდა

პოლიტიკური კამპანიების დროს მონაცემები რამდენიმე გადაწყვეტილების მიღებას აადვილებს: სად ჩაატარდეს ყრილობა, რომელ შტატებზე ან ამომრჩევლებზე მოხდეს რესურსების მობილიზება და როგორ წარიმართოს პირადი კომუნიკაცია და რეკლამა მხარდამჭერებისთვის, ჩამოუყალიბებელი ამომრჩევლებისათვის და მათთვის, ვინც მხარს არ უჭერს ამა თუ იმ პოლიტიკოსს.

მონაცემებზე დაფუძნებული/აგებული კამპანია ახალი სულაც არ არის. უკვე ათწლეულებია კამპანიების დროს გამოიყენება და უმჯობესდება სამიზნის განსაზღვრა (თარგეტინგი). ამომრჩევისათვის მნიშვნელოვანი და მასტიმულირებელი საკითხებისა და ღირებულებების განსასაზღვრად დაკვირვება ხდება წინა ჯერზე მიცემულ ხმებზე, რელიგიურ აფილირებაზე, დემოგრაფიაზე, ჟურნალების გამოწერასა და მყიდველის ჩვევებზე.

თუმცა, სიახლეა კამპანიების წარმართვისას ხელმისაწვდომი მონაცემების დეტალურობის ხარისხი. შტატების ეროვნული რესპუბლიკური კომიტეტი, მაგალითად ყველა რესპუბლიკელ კანდიდატს სთავაზობს უფასო წვდომას „მონაცემთა ბაზასთან/ცენტრთან“ - მოთხოვნებისა და მონაცემების მართვის ინსტრუმენტთან, რომელიც აკავშირებს 20 მილიონი ამომრჩევლის 300 ტერაბაიტზე მეტ მონაცემებს, მათ შორის 7,700,545,385 მიკროტარგეტირებულ მონაცემს. მსგავსია მონაცემთა ანალიზისა და ამომრჩეველთან საკონტაქტო კომპანია i360, რომელსაც ძმები კოხები აფინანსებენ და რომელიც ამუშავებს აშშ-ის 250 მილიონ მოქალაქისა და ამომრჩევლის ათასობით მონაცემს, რომელიც ქმნის „სრულ სურათს თუ ვინ არიან

ისინი, სად ცხოვრობენ, რას აკეთებენ და რა ხდება მათ გარშემო“. მილიონობით ელექტრონული ფოსტის მისამართის, ტელეფონის ნომერის და შემოწირულობების, ყრილობებისა და ვაჭრობის საშუალებით შეგროვებულ სხვა პერსონალური მონაცემების საშუალებით პოლიტიკური კამპანიების მწარმოებლებისთვის ჩვენი შავ-ბნელი საიდუმლოებებიც ცნობილი გახდა.

ამავე კონტექსტში უნდა განვიხილოთ Cambridge Analytica, გაერთიანებულ სამეფოში დაფუძნებული ანალიტიკური ფირმა, რომელიც სცენაზე 2016 წელს უეცრად გამოჩნდა და გაჩნდა მითქმა-მოთქმა მის შესაძლო როლზე როგორც შეერთებული შტატების არჩევნებში, ისე ბრეგზიტის რეფერენდუმში. კომპანია ამტკიცებს, რომ ფლობს 220 მლნ ამერიკელის შესახებ 5000 მონაცემს, რომელიც შექმნილია ფეისბუქიდან შერჩეული ფსიქოლოგიური მონაცემების გაერთიანებით მონაცემებით მოვაჭრე კომპანიებისაგან მიღებულ მომხმარებლების უამრავ მონაცემებთან.

მონაცემთა ბროკერები და მონაცემებით მოვაჭრე კომპანიები აგროვებენ ან მოიპოვებენ ინფორმაციას ადამიანის შესახებ (დათვალიერების (browsing) ისტორია, ადგილმდებარეობის მონაცემები, ვინ არიან შენი მეგობრები ან რამდენად ხშირად მუხტავთ ელემენტს და ა.შ) და შემდეგ იყენებენ ამ ინფორმაციას თქვენს შესახებ დამატებითი, აქამდე უცნობი ინფორმაციის გამოსაყვანად. მისაღებად (რას იყიდით შემდეგ, რა ალბათობაა რო იყოთ მდებარეობითი სქესის ან კონსერვატორი, თქვენი ამჟამინდელი ემოციური მდომარეობა, რამდენად სანდო ხართ, ხართ თუ არა ჰეტეროსექსუალი და ა.შ.)

ამომრჩევლების კვალის მიდევნებაც (თრეკინგი) მხოლოდ ონლაინ არ ხდება. აიოვას პარტიის სხდომის (caucus) შემდეგ მალევე, 2016 წლის დასაწყისში Dstillery-ს, „დიდი მონაცემების სადაზვერვო/შემგროვებელი კომპანიის“ აღმასრულებელმა დირექტორმა საჯარო რადიო პროგრამა მარკეტპლეისს უთხრა რომ კომპანია თვალს ადევნებდა (tracked) სხდომის 16000 დამსწრეს მათი ტელეფონების მეშვეობით და აკავშირებდა მათ ონლაინ პროფილებთან. Dstillery-მ შეძლო დაეიდენტიფიცირებინა საინტერესო ქცევითი მოდელები, მაგალითად აიოვაში, ადამიანებმა ვისაც უყვარს გრილზე შეწვა ან თავიანთ გაზონებზე გადამეტებულად მუშაობენ, ხმა ტრამპს მისცეს.

ისეთი კომპანიები როგორცაა Cambridge Analytica და i360 ძირითადად ორ რამეს აკეთებენ: 1) უდიდესი რაოდენობის მონაცემებს აგროვებენ ადამიანებზე და იყენებენ ამ მონაცემებს მათი პროფილებისათვის და ადამიანების შესახებ კიდევ უფრო სანდო და დეტალური ინფორმაციის განსაჭვრეტად და 2) იყენებენ ამ პროფილებსა და ვარაუდებს როგორც პოლიტიკური გზავნილების პერსონალიზებისთვის, მაგალითად სოციალურ მედიაში რეკლამების სახით, ასევე კამპანიების სტრატეგიული გადაწყვეტილებებისთვის ინფორმაციის მისაწოდებლად.

მაშინ როდესაც პოლიტიკური კამპანები მონაცემთა საგანძურის გამოყენების შედეგებს იმკიან, მედიაშიც რადიკალურად იცვლება ზოგადი სურათი. მიუხედავად იმისა, რომ ტელევიზია, გაზეთები და რადიო კვლავ მნიშვნელოვან როლს თამაშობენ, სულ უფრო მეტი ადამიანი იღებს ინფორმაციას და ეცნობა პოლიტიკურ კანდიდატებს სოციალური ქსელების საშუალებით. მეტიც, ეს ქსელები იმის აღქმის საშუალებასაც იძლევა, რას შეიძლება ფიქრობდნენ სხვები ამა თუ იმ საკითხზე თუ კანდიდატზე.

სოციალური მედიის საიტები ყველაფერს აკეთებენ რათა თავი ნეტრალურ პლატფორმად წარმოაჩინონ, რომელიც ცხადად განსხვავდება დღისწესრიგის მქონე და ამბების შემქმნელი ტრადიციული მედიისაგან, თუმცა, რაღა თქმა უნდა, მათაც აქვთ თავიანთი გადახრები/მიკერძოებულობა. ეს, როგორც წესი ძალიან პერსონიფიცირებული, სივრცეები ისეა მოწყობილი, რომ მეტი ჩართულობა უზრუნველყოს და აგებულია რეკლამირებაზე. სიახლეების ზოლის (newsfeed) ალგორითმიდან შინაარსის ცვლილებამდე სოციალური მედიის საიტები განსაზღვრავენ რას ვხედავთ და რამდენად ხშირად ვხვდებით იმ ინფორმაციასა და ხალხს, ვისაც არ ვეთანხმებით.

ამ ცვალებად გარემოში კი პოლიტიკური კამპანიების დროს ონლაინ რეკლამებით, პერსონიფიცირებული ზარებითა თუ ვიზიტებით ხდება ამომრჩევლების მიკროტარგეტირება მათი ქცევის შესაცვლელად. რას ფიქრობენ ადამიანები პოლიტიკურ კანდიდატზე, საბოლოოდ ვის აძლევენ ხმას, საერთოდ მიდიან თუ არა არჩევნებზე ამ ყველაფერზე გარკვეულ ფაქტორებს აქვს გავლენა. კვლევები ცხადჰყოფს, რომ ამინდსაც კი შეუძლია გავლენა მოახდინოს საარჩევნო ქცევაზე. ჩვენი ცნობიერი გადაწყვეტილებები მუდმივად განიცდის არაცნობიერის - ფიქრის პროცესის, ემოციების და წინასწარი განწყობების გავლენას. სწორედ ამით აიხსნება კომერციული და პოლიტიკური PR-ის ძალისხმევის მიმართვა ჩვენ შესახებ კიდევ უფრო სანდო პროფილები შექმნისავენ. დაუჯერეთ გუგლის იუტუბის რეკლამების მარკეტინგის დირექტორის: „ამომრჩევლები გადაწყვეტილებებს თავიანთ მისაღებში, ტელევიზორის წინ იღებდნენ. დღეს ეს გადაწყვეტილებები სულ უფრო მეტად მიიღება მიკრო-მომენტებში, მობილურ მოწყობილობებზე. საარჩევნო მიკრო-მომენტები კი მაშინ ხდება, როდესაც ამომრჩეველი მიმართავს მოწყობილობას კანდიდატის, ღონისძიების ან რამე საკითხის შესახებ რამის გასაგებად“.

რა არის პრობლემა?

არჩევნებისა და პოლიტიკური კამპანიების დროს მონაცემთა გამოყენების გზები პირადი ცხოვრებაში ძალიან იჭრება/ინვაზიურია, უსაფრთხოების მხრივ ბევრ კითხვას ბადებს და შესაძლოა დემოკრატიული პროცესისადმი ნდობა შეარყიოს.

კამპანიის დროს ხშირად შეიძლება ისეთი მონაცემები იქნას გამოყენებული, რომელთა გამჟღავნებაზეც ადამიანებს თანხმობა არ გაუციათ. ამომრჩევლების მონაცემთა დიდი ბაზებიც მაღალი სანდოობის პროფილების შექმნისას ხშირად ეყრდნობა მონაცემთა ბროკერებთან ხელმისაწვდომ კომერციულ მონაცემებს ან საჯაროდ ხელმისაწვდომ ჩანაწერებსა და ონლაინ არსებულ მონაცემებს. ეს განსაკუთრებით შემაშფოთებელია როდესაც პროფილირების საფუძველზე სრულიად დაუკავშირებელ მონაცემებზე დაყრდნობით სენსიტიური ინფორმაციის შესახებ კეთდება დასკვნები, მაგ. პოლიტიკური შეხედულებების ან პიროვნული მახასიათებლების თაობაზე. მაგალითად პიროვნული მახასიათებლებზე დასკვნის გაკეთება სოციალურ მედიაში მოწონებების მიხედვით არის შესაძლებელი. ბევრი ადამიანისთვის მოულოდნელია ის ფაქტი, რომ კომერციული მონაცემები, საჯარო ჩანაწერები და ყველა ტიპის ნაწარმოები ინფორმაცია გამოიყენება პოლიტიკური კამპანიების დროს.

ასევე, სენსიტიური მონაცემების შეგროვებას უსაფრთხოების კომპონენტიც აქვს. მონაცემთა ბაზები რომლებიც შექმნილია სტრატეგიული პოლიტიკური კომუნიკაციისათვის ხშირად შეიცავს ძალიან სენსიტიურ ინფორმაციას. როგორც 2017 წელს ამერიკის თითქმის 200 მლნ მოქალაქის პერსონალური მონაცემების შემცველი ბაზის შემთხვევითი გამჟღავნება ცხადჰყოფს, ასეთი მონაცემთა ბაზები ხშირად ხდება კიბერშეტევის სამინზე, ხდება ინფორმაციის გაჟონვა, მას იპარავენ ან უბრალოდ აზიარებენ. მონაცემთა უსაფრთხოებას ისიც უქმნის საფრთხეს, რომ ეს ბაზები ხშირად ხდება საზიარო არჩევნების დასრულებისას ან მას შემდეგ, რაც კანდიდატი გამოეთიშება არჩევნებს. 2016 წლის საპრეზიდენტო არჩევნების თითქმის ყველა კანდიდატმა სხვა კანდიდატებს, მარკეტინგულ კომპანიებს, საქველმოქმედო დაწესებულებებს ან კერძო ფირმებს მიჰყიდა, მიაქირავა ან ასესხა მხარდამჭერების პერსონალური მონაცემები.

ამომრჩევლების პროფილირება სხვა ფუნდამენტურ საკითხებსაც წამოსწევს. მონაცემების არჩევნების დროს გამოყენება აისბერგის წვერიც კი არ არის იმ ეკონომიკისთვის, სადაც მომხმარებლები სულ უფრო მეტად თავად ხდებიან პროდუქტი. მთლიანი (ონლაინ) სარეკლამო ეკოსისტემა ორგანიზებულია ადამიანების ცხოვრების შესახებ მონაცემების რეალურ დროში ბრუნვის გარშემო და მოგების მისაღებად აწყობილია ისე, რომ შეცვალოს ადამიანების ქცევა. კომპანიები, რომლებიც წლების განმავლობაში აგროვებდნენ სენსიტიურ მონაცემებს მთელ მსოფლიოში მილიონობით ადამიანზე, მართლაც შეძლებენ მასშტაბურად შეცვალოდნ ადამიანების რეალური ქცევა.

რა არის გამოსავალი?

ისეთი სამყაროსკენ მივდივართ, სადაც სავარცხელს - მიკროფონი, ხოლო ტოსტერს კამერა აქვს, სადაც სივრცე, რომელშიც შევდივართ აღჭურვილია სენსორით და ამძრავით, რომლებიც ჩვენ შესახებ რეალურ დროში იღებენ გადაწყვეტილებებს. ყველა ეს მოწყობილობა შექმნის, შეაგროვებს და გააზიარებს დიდი ოდენობით პერსონალურ მონაცემებს, რომლებიც გამოყენებული იქნება იმ დასკვნების გასაკეთებლად თუ ვინ ვართ და რის გაკეთებას ვაპირებთ.

ამომრჩევლების პროფილირება გზას უხსნის ნაკლებად რეგულირებულ წვდომას ძალიან პერსონალურ მასობრივ მონაცემებზე არა მხოლოდ პოლიტიკური კამპანიის მიზნებისთვის. ადამიანებმა უნდა იცოდნენ რა მოსდის მათ მონაცემებს, ვის შეუძლია მათი გამოყენება და რა მიზნით. მეტიც, მხოლოდ კამპანიებისა და არჩევნების დროს გაკეთებული შეწირულობების ოდენობა კი არ უნდა დარეგულირდეს, არამედ მონაცემებიც უნდა განიხილებოდეს როგორც ძალაუფლების ახალი წყარო.

მონაცემების გენერირების შემთხვევაში, ადამიანებს უნდა ჰქონდეთ საშუალება გაარკვიონ მათ შესახებ რომელ ორგანიზაციას და რა ტიპის მონაცემები აქვთ. პროფილირება ადამიანების პიროვნებაზე, ქცევასა თუ რწმენაზე ძალიან სენსიტიურ დასკვნებსა და ვარაუდებს ქმნის. ადამიანებს ამ დასკვნებსა და ვარაუდებზეც უნდა ჰქონდეთ წვდომა.

და ბოლოს, უზრუნველყოფილი უნდა იყოს ამომრჩევლების მონაცემთა ბაზების უსაფრთხოება.