3-дәріс. Үлкен деректер қауіпсіздігі

Тарихы және қазіргі заманы

Деректерді қорғау қажеттілігі сол деректер құпиялылыққа қауіп төндірген кезде деректердің өзімен бірге пайда болды. Осындай жағдайлардың бірі — король Давидтің әлемді бағындырудағы табыстарын көру мақсатында ұйымдастырған алғашқы санақ. Санақтың өзін шіркеу мақұлдамағанымен, оның нәтижесіне көңілі толатынын айта кеткен жөн.

Екінші белгілі санақ б.з.б. 28 жылы император Октаврдың патшалық кезінде болды, бұл Рим империясының халқы 4 036 мың адамды құрағанын көрсетеді. Бәлкім, бұл билік қызығушылығын тудырған ересек еркін ерлердің саны болған шығар, сондықтан адамдардың жалпы саны құлдарды санамағанда 10 млн-ға жуық адам болуы мүмкін. Дегенмен, бірқатар тарихшылар бітікшілер барлық еркін азаматтарды санаған деген пікірде.

Қауіпсіздік тақырыбына қайта оралайық. Ортағасырлық тарихшылар балалардың өліміне, яғни король Геродтың бұйрығы бойынша нәрестелерді союға себеп болған санақ деген пікірге келді.

Өсиетті жақсы білген Британ парламентінің депутаттары 1753 жылы үкімет ұсынған санаққа қарсы дауыс берді. Көп кешікпей оның үлкен пайдасы болуы мүмкін екенін мойындады, бірақ екінші жағынан, олар тарихи тәжірибені еске түсіріп, бұл статистика қарсылас елдерге жетеді деп қорқытты. Ал бұл Англия жауларына ол туралы ақпарат берер еді, ол ешбір жағдайда жария етілмеуі тиіс еді. Бұл елдің қауіпсіздігі мәселесі. Осындай қорқыныштың кесірінен еуропаның көптеген елдері санақтан бас тартты. Жау жалпы халық санын да, соғысқа қатыса алатын ересек аталықтардың санын да білмеуі тиіс. Швециядағы алғашқы статистика 1744 жылы жарияланды. Зерттеу бір қалада (Уппсала) жүргізілді, бірақ ол еш жерде айтылмаған.

Сондай-ақ, тұрғындар мемлекеттің олар туралы көбірек ақпарат алғанын қаламады. Олар санақтың жаңа салықтарға әкелетініне, мемлекетке белгілі болған жас өспірімдердің әскер қатарына шақырылатынына, отбасылық бизнестен немесе әрқашан қосымша қол талап етілетін жерден «тығылып» қалатынына күмәнданбады. Британияда санақ жүргізу қажеттілігі тек 1801 жылы бүкіл ел бойынша азық-түлік тапшылығынан кейін ғана танылды. Оларды тарату үшін мемлекет онда қанша адам өмір сүргенін білуі қажет болды.

Осы уақытқа дейін барлық елдердің адамдары халық санағына қатысуға ынталы емес. Бәлкім, тарихи жады іске қосылған шығар. Керісінше, бұрынғыдай, біз үкіметтің біз туралы қосымша ақпаратқа ие болғанын және оны бізге қарсы қолданғанын қаламаймыз. Қазіргі заманда лаңкестікпен күресу қажеттілігі адамдарды деректерді ашу қажеттігін түсінуге итермелейді.

Айта кету керек, *Amazon, Apple, Google* сияқты компаниялар үкіметпен және құқық қорғау органдарымен өз еркімен ақпарат алмасуға дайын емес. Мысалы, 2016 жылдың екінші жартысында ғана *Apple* ұлттық қауіпсіздік туралы 6 мыңға жуық сұрау алды. Бірақ компания ұлттық қауіпсіздікті құпиялылыққа нұқсан келтірмей қамтамасыз етуге болады деп нық сенеді.

Компанияға ақпаратты жария ету және белгілі бір іс-әрекеттерді орындау туралы ресми сұрау салулар үнемі келіп отырады. Бұл билік органдарының, құқық қорғау органдарының, жеке компаниялардың сұраулары болуы мүмкін. Жеке тұлғалардың сұрау салулары, әдетте, сот талқылауын көздейді. Кәсіпорында олардың әрқайсысы жеке қаралады.

Әріптестермен және қызметтерді жеткізушілермен қарым-қатынасты құру кезінде кәсіпорын олардан мемлекеттік органдардың талаптарына жауап бере отырып, өзінің стандарттарын сақтауды талап етеді. Компанияның заңгерлері мәліметтерді ұсынуды талап ету үшін заңды негіздердің бар-жоғын мұқият тексереді. Бар болған жағдайда деректер қажетті шамада ғана ұсынылады. Егер сұрау салу негізсіз, түсініксіз немесе дұрыс болмаса, ешқандай ақпарат ұсынылмайды.

Apple өнімдері мен қызметтерінде ешқашан әмбебап кілттер немесе оларға салынған рұқсат етілмеген қолжетімділік құралдары болған емес. Компания ешқашан өз қызметтеріне құқық қорғау органдарына тікелей қол жеткізуді қамтамасыз етпейді дейді.

Құқық қорғау органдары құрылғыларға сұрау жібергенде (жоғалған және ұрлық болған жағдайда), компания көмектесуге тырысады. Компанияға қаржылық идентификаторларға сұраулар келіп түседі, мысалы, Apple өнімдерін сатып алу үшін басқа біреудің несие картасы туралы ақпаратты пайдалану . Пайдаланушы жасаған мазмұнға қол жеткізу, егер бұл жағдай АҚШ-та орын алса, іздеу ордерімен ғана беріледі.

Егер бизнеске АҚШ-тың дата-орталықтарында сақталған контентке қол жеткізу туралы халықаралық сұрау салулар келіп түсетін болса, онда ол оларды өңдеу үшін АҚШ-тың «Электрондық байланысты қорғау туралы» Заңына сәйкес келуі тиіс. Егер компания құқық қорғау органдарына *iCloud-да* сақталған деректер туралы ақпарат берсе, ол, егер хабарламаға заңмен тыйым салынбаса, пайдаланушыны алдын ала хабардар етеді.

Apple компаниясының қатысуымен қызықты жағдай 2016 жылы орын алды. Компания Сан-Бернардино шабуылынан кейін ФБР-дің өтініші бойынша телефонды соғудан бас тартты. Сан-Бернардино атысы 2015 жылдың 2 желтоқсанында өтті. Сайд Фарук пен оның әйелі Ташфин Мәлік мүмкіндігі шектеулі жандарға арналған орталықта от ашты. 14 адам қаза тапты, тағы 21-і түрлі ауырлықтағы жарақаттар алды. ФБР мәліметі бойынша, Фарук екі шетелдік лаңкестік ұйыммен, Жабхат әл-Нусра және Әш-Ша Бабпен байланыста болды. АҚШ-та болған оқиға лаңкестік шабуыл деп танылды. *Apple компаниясының* бас директоры Тим Кук бұл прецедент басқа азаматтарға соққы беруі мүмкін екенін айтты, және олар өз мәліметтерінің қауіпсіздігіне сенімді болуы керек. Компанияның веб-сайтында клиенттерге үндеу жарияланып, биліктің iPhone-ға қол жеткізу талабына және онда атқыш Сайд Фарукқа келіп түскен хабарларға қарсылық білдірілді. Компанияның мәліметі бойынша, сұрау *Apple клиенттерінің қауіпсіздігіне қауіп төндірді,* Ал прецеденттің салдары «құқықтық база шегінен әлдеқайда асып кетеді». Лос-Анджелестегі аудандық сот 16 ақпанда Apple ФБР-дің Фаруктың iPhone деректеріне қол жеткізуі үшін «ақылға қонымды техникалық көмек» көрсетуі тиіс деген шешім шығарды. ФБР компаниядан парольді енгізу әрекеттері санының шегін алып тастауды талап етті, содан кейін құпия сөзді автоматты крекинг жүйесі Фаруктың смартфонына соққан болар еді. Тим Кук оны «iPhone-ның іргетасын» жасау деп атады. Кук сайтта жазды. Сот шешімінен кейінгі күні (2016 жылдың 17 ақпаны): «Үкімет *Apple компаниясынан* өз пайдаланушыларымыздың құрылғыларына соққанын және клиенттерді, соның ішінде американдық азаматтарды, керемет хакерлер мен киберқылмыскерлерден қорғау жөніндегі ондаған жылдар бойы жұмыс істеуіне нұқсан келтіруін сұрады».

Кейінірек АҚШ Әділет министрлігі құқық қорғау органдарының Фаруктың смартфонының қауіпсіздігіне соққанын жариялады (себебі, онда талантты адамдар да жұмыс істейді). Осылайша, *компаниядан ашуға көмек көрсетуді талап еткен Apple мен ФБР арасындағы дау тоқтатылды.* Apple компаниясы ынтымақтаса алмады.

Apple ФБР немесе үкіметтен соққан смартфондарға көмектесуді сұраған жалғыз АҚШ компаниясы емес. Google сондай-ақ осындай талаптарды алды , мысалы, 2015 жылы есірткі трафигіне байланысты іс бойынша тергеу жүргізілген кезде. Калифорния соты компанияға телефондарды ашуға қатысуды бұйырды. Осындай шешімдер Алабамада, Солтүстік Дакотада және басқа да бірнеше мемлекеттерде қабылданды, бірақ Google-дың *Google-ға* бағынышты болғаны белгісізосы талаптардың болуы.

Google өкілі компанияға apple-дағыдай өз өнімдерінің қауіпсіздігін тоқтатуға мүмкіндік беретін қосымша құрал жасау туралы ешқашан өтініш түспегенін ресми түрде жариялады . «Егер мұндай талап болса, біз оған қатты дау айтар едік», - деп атап өтті Google . Яғни, *Apple* мен *Google* АҚШ үкіметінің саясатына қарсы, бірақ өз клиенттерінің мәліметтерінің қатаң құпиялылығын қолдайды.

Біз бақылап отырмыз

Егер теледидардан детективтік сериалдарды немесе фильмдердегі триллерлерді көрсеңіз, бейнебақылау кадрларын мұқият зерттейтін полиция қызметкерлерін немесе тергеушілерді көрген шығарсыз. Осылайша олар не көлікті, не адамды табуға тырысады. «Үлкен деректер» деген сөздерді айтсақ, ойға келетін бірінші нәрсе — сандар. Бірақ бейнежазбалар тек электрондық кесте немесе мәлімдеме сияқты, әсіресе сандық бейне сияқты. Адам көрнекі деректерге сезімтал.

Әрине, кейбір адамдар жазбаша мәтінді қабылдауда жақсы, басқалары ақпаратты тыңдауда жақсы, бірақ біз бәріміз көз алдымыздан алынған ақпаратты өңдеуге қабілеттіміз. Бұл адам табиғатының бір бөлігі. Бірақ қабілеті көптеген визуалды штамммен нашарлайды. Мысалы, егер полиция қызметкеріне жазудың көптеген сағаттарын көру қажет болса, оның назар аудару аралығы сөзсіз төмендейді. Адам шаршайды. Сондықтан бейнежазбаларды талдау Үлкен *деректер* алгоритмдерін пайдаланудың тамаша мүмкіндігі болып табылады.Бүгінгі таңда олар құқық қорғау органдарының жұмысында, сондай-ақ осы мәселе бойынша ритейлерлердің жұмысында жиі қолданылады. Бейнебақылау камералары барлық жерде, тіпті біз оларды байқамаймыз және олардың бар екенін білмейміз. Яғни, қазір біздің қалалар, ең болмағанда дамыған елдерде, алып күмбезбен жабылған сияқты.

Белгілі бір ғимаратқа немесе мысалы, белгілі бір рейстегі жолаушыларға қажетті сағатты анықтауға көмектесетін тиісті бағдарламалар бар. Бүгінгі таңда супермаркеттер мен басқа да дүкендердегі камералардың жұмысына ешкім таң қалмайды. Егер біз оларды көрмесек, ең болмағанда АҚШ-та таң қалар едік. Бұл камералар қауіпсіздік мақсатында орнатылған деп есептейміз, ал олардың көмегімен келушілерді супермаркеттің күзет қызметі немесе тіпті қандай да бір орталық бақылау пунктінен мемлекеттік құқық қорғау органдары бақылайды. Бірақ үлкен деректер келушілерді бақылау мүмкіндігін ғана қамтамасыз етпейді. Олардың көмегімен дүкен сөрелердің назарын аударатынын бақылап отырады.

Мойындау жүйесі де осылай жұмыс істейді , және іздестіріліп жатқан адамдарды ғана емес, сонымен қатар тұрақты клиенттерді де (дүкенге қызығушылық танытатындар) қадағалайды. Дәл осындай мойындау жүйесі тізбектің берілген дүкенінің немесе тізбектің көптеген дүкендерінің тұрақты клиенттерін әлеуметтік желілердегі тіркелгілерімен одан әрі байланыстырады және оларға мақсатты жарнама немесе ұсыныстар жіберіледі. Бұл тек *Big Data технологияларының арқасында мүмкін болды.*

Деректерді жинаудың тағы бір қызықты жүйесі *7-11 желісінде орнатылған,* әлемнің 18 елінде жұмыс істейтін және 36 000-нан астам сауда нүктелері бар — шағын супермаркеттер. Оларда клиенттердің ағыны және әрбір кассадан қанша адам өтетіні

туралы ақпарат жинайтын жүйе бар. Жүйе клиенттердің санын және әрбір кассир қызмет көрсететін клиенттердің санын сәйкестендіреді, ең стресстік уақыт пен тыныш сағаттар есептеледі. Бірқатар елдерде бұл ыңғайлы дүкендер, себебі, мысалы, Таиландтың курорттарында олардың қызметтеріне тәулік бойы сұраныс бар. Өзіңіздің иелігіңіздегі барлық осы ақпараттың көмегімен клиенттердің ең көп ағынды сағаттарында кассирлер санын көбейтуге және клиенттер болмаған кезде сол сағаттарда оларды алып тастауға болады. Ал бұл сағаттар бір елдің әр түрлі елдері мен қалаларында ерекшеленеді. Бұл жерде Big *Data* технологиялары көп көмектеседі.

Сондай-ақ, бейнебақылауды пайдаланатын бұл технологиялар қандай сатушылардың бірге жақсы жұмыс істейтінін және кімнің бір ауысымға салмағанын анықтауға көмектеседі. Психологтарды жалдаудың немесе қымбат тестілеу жүргізудің қажеті жоқ. Алгоритм мұның бәрін жасайды! Кейбіреулері шуақты күндері жақсы жұмыс істейді, ал басқалары жаңбырлы күндері жақсы жұмыс істейді. Мұны ескеруге болады. Жүйені американдық *Percolata компаниясы ойлап тапты,*ол маркетингті оңтайландырудың сан алуан шешімдерін ұсынады. Компания өз жүйесі қолданылатын дүкендерде кірісті 10-нан 30%-ға дейін ұлғайтуға болатынын есептеп шығарды. Әрине, мұндай тәсіл қызметкерлерді бақытты етпейді, сондай-ақ алгоритммен басқарылатын кез келген жұмыс. Себебі, жұмыстан босату басталады немесе қызметкерлер олар үшін ыңғайсыз сағаттарда, нақты кестесіз жұмыс істеуге мәжбүр, бірақ жүйе жұмыс беруші үшін оларды жүктеуді тиімді деп есептегенде. Екінші жағынан, осындай жүйемен жақсы қызметкерлер марапатталып, марапатталуы мүмкін, ал жамандары кәдеге жаратылуы мүмкін. Және, әрине, жүйені «қуып жетіп» жатыр.

Мұндай бақылау жүйелері көшелерде, ең болмағанда дамыған елдерде бұрыннан қолданылып келеді. Олар полиция мен билік жұмысының таптырмас бөлігіне айналды. Әрине, тәулік бойы бақылау жүйесі мен мойындау жүйесінсіз қандай да бір заманауи әуежайды немесе теміржол вокзалын елестету мүмкін емес. Көшелер мен үй-жайларда бейнекамералар ілініп қана қоймай, біздің көліктер сызықшалы жұдырықшалармен жабдықталған, оларды кейбір лауазымды тұлғалардан (мысалы, жол полициясының қызметкерлерінен) көруге болады, ал біздің орналасқан жерімізді телефон арқылы бақылап отыруға болады.

Үлкен деректер жүйелеріне *кіретін бейне деректер дұрыс пайдаланылатынына сенімдіміз* бе? Әрине, жоқ. Олардың көмегімен біз күнделікті орындайтын іс-әрекеттерімізді, өмірімізді, іс-әрекеттерімізді көбірек бақылай аламыз. Американың кейбір бөліктерінде билік бейнебақылаумен шектелмейді — парк орындықтары мен саябақтарында микрофондар орнатылды. Әңгімелер *Big Data технологияларын пайдалана отырып талданады.*

Бәлкім, бейнебақылау полиция жұмысының маңызды бөлігі екенін ешкім де дауламайтын шығар. Ал бейнедәлел сотта анағұрлым салмақты. Олар анағұрлым үмітті, адам факторына ешқандай кедергі жоқ, дегенмен сот отырыстары барысында адам куәгерлерінің айғақтары әлі де ескеріліп, судьялар мен алқабилер олардың негізінде шешім қабылдайды. Бірақ оларға сүйенуге болмайды! Адамдар әдейі жала жапқандықтан емес, әр адам жағдайды басқаша көретіндіктен.

Мысалы, австриялық және неміс заңгері, қылмыстық және халықаралық құқық саласындағы маман Франц фон Шторктың (1851-1919) 1901 жылы қайтадан жүргізген экспериментін еске түсіре аламыз. Берлинде өткен семинар барысында қызу аргумент (зерттеушінің әдейі арандатуы), содан кейін оққа ұшты, ал шәкірттерінің бірі (экспериментке қатысушы) «қаза тапты». Әркім қорқынышты қатып қалды. Бірнеше минуттан кейін «өлтірілген» оқушы тұрды, ал фон Лист ешкім зардап шекпегенін және болған оқиға семинар бағдарламасының бір бөлігі екенін түсіндірді. Содан кейін ол әр оқушыдан көз алдында сыныпта не болғанын егжей-тегжейлі сипаттауды сұрады.

Олар болашақ заңгерлер болды, және олар сотта айғақтар беру кезіндегідей апталар, тіпті айлар бұрын емес, жай ғана болған оқиғаны сипаттады. Шәкірттері тынышталып, ешкім зардап шекпегенін, басқа адамның өмірі де, тағдыры да олардың айғақтарына байланысты болмайтынын, кінәсіздер түрмеге шықпайтынын, айыптайтын ешкім мүлдем жоқ екенін түсінді.

Бәлкім, Франц фон Шторктың өзі мұндай нәтижені күтпеген шығар – ол болған оқиға туралы мүлдем басқа сипаттамалар алды. Оқушылардың көпшілігі уақыт коэффициентімен қателесті. Оқиғалардың бірізділігі көбінесе қате көрсетілді. Кейбіреулер жыртқыштың сыныптан қалай шығып кеткенін және ол қашып кетпегенін сипаттады. Ал шәкірттерге әлі күнге дейін «кісі өлтірушінің» атын айтуға тура келді (фон Листтің тағы бір көмекшісі). 8 түрлі адам аталды. Ендеше, осыдан кейін адамдардың айғақтарына сенуге болады ма?!

Адам жады жетілмеген. Бейнежазбаны дұрыс есте сақтау мүмкін емес. Ол нақты не болғанын жазады. Тек бір жазба. Ал *Үлкен деректер жүйесіне* жазба енгізілген кезде оны пайдаланудың қосымша мүмкіндіктері бар. Өкінішке орай, кино милясын көруге сағат жұмсайтын полиция қызметкерлері бұл ауыр тапсырмадан құтылуға болады. Ал полиция да куәгерлер сияқты адамдар. Олар шаршап, жазудағы маңызды нүктені жіберіп алуы мүмкін: Адам факторы іске қосылады. Біз бұл жерде кәсіби емес, тіпті ықылассыздық туралы айта алмаймыз. Ол қасақана және қауырт бақылады, бірақ алты-сегіз сағат бойы түзу! Егер жасанды интеллект бізді іздесе, әлдеқайда жақсы нәтиже күтуге болады. *Big Data жүйелері керемет деп айта алмаймыз*, бірақ олар адамдардың жұмысын әлдеқайда жеңілдетеді, мысалы, олар қазірдің өзінде адамдар мұқият қарап жатқан бірнеше сағаттық жазбалардан бірнеше маңызды минут шығарып алады.

Мойын немесе автомобиль тану бағдарламалық жасақтамасының көмегімен адамның немесе автомобильдің қала төңірегіндегі қозғалысын қадағалау қарапайым. Камералар әр кез ілінбейді, бірақ камерадан камераға дейінгі жолды жүріп өту қиын емес. Қазіргі жүйе қозғалыстарыңыз туралы жан-жақты білуге мүмкіндік береді! Мысалы, АҚШ пен АҚШ-та осындай қадағалау тіркелмеген автомобильдерді аулау үшін қолданылады. Бұл жүйелер хабар-ошарсыз кеткен адамдарды іздеу үшін де белсенді қолданылады. Ал сол жолмен көп адам табылды.

Бізді үнемі бақылау жақсы ма, әлде жаман нәрсе ме? Біз әлеуетті коммуналдық қызмет пен қауіпсіздік үшін жеке өмірімізге қол сұқпаушылыққа қандай дәрежеде төтеп беруге дайынбыз? Хабар-ошарсыз кеткен адамдарды іздеу, қылмыскерлерді қуып жету, иә. Егер деректер дұрыс және заңды тергеулер жүргізу кезінде дәлелдемелерді ұсыну үшін ғана пайдаланылса, ол орынды болып көрінеді.

Іс-әрекетімізді болжау

Барлау органдары біз туралы бәрін біледі деп күтуге болады. Бірақ мәселе мынада, олар біздің ертең, бір айдан, тіпті бір жылдан кейін қайда болатынымызды біле алады. Ал үлкен деректер оларға көмектеседі. Қазіргі таңда бүкіл әлемде арнайы қызметтер жаңа технологияларға қызығушылық танытып, осы технологияларды жақсы меңгерген жас мамандарды тартады. Және олар әркім туралы деректер жинап қана қоймай, жеке адамдардың немесе адамдар тобының мінез-құлқын модельдеуде озық әзірлемелер жасайды. Бізде жақын арада тәртіпсіздіктер, төңкерістер немесе сол сияқты нәрселер қайда болатынын нақты болжау технологиясы әлі жоқ, бірақ ол жүріп жатыр және оған көп ақша салынды. Біз осыны қалаймыз ба? Интеллекттің дамуын арнайы қызметтердің мейірімінде қалдыруға болады ма? Бұл үлкен тепе-теңсіздікке әкеліп соқпай ма?

Уақыт өте келе, XIX ғасырға қайта оралайық. Тырысқақ эпидемиясы Лондонда 1854 жылы, Широкий көшесі ауданында (қазіргі Широкий көшесі) басталды. Осы оқиғаның арқасында лондондық дәрігер Джон Сноу жұқтыру көзін анықтап, әйгілі болып, тарихқа енді. Ол өте ерекше су жинағыштан алынған су еді. Қар тырысқақтың өршуін ауыз судың ластануына байланыстыра алды. Қар заманның басым миазма теориясына сенбеді, соған сәйкес тырысқақ, оба сияқты аурулар ауаның сау еместігінен туындайды деп ойлаған. Джон Сноу СоХо ауданындағы барлық үйлердің тұрғындарынан бір-бірден сұрасып, өз суларын алған бұлақтардан картаға түсірді (өздеріңіз елестеткендей, ағынды су әлі болмады, кәріздің орнына шұңқырлар пайдаланылды). Ол зертханалық әдістерді қолдана отырып, суды зерттей алмады, бірақ «зиянды» су тартуды анықтай алды. Ол «тырысқақ картасын» жасады. Онда су жинау станциялары мен белгілі бір ғимараттағы жағдайлардың саны белгіленді, ал Қар жергілікті билікке су көзі мен аурудың таралуы арасындағы байланысты дәлелдей алды. Билік дозатордан сорғыш тұтқасын алып тастағаннан кейін эпидемия төмендей бастады. Доктор Сноудың еңбегін жергілікті халық жоғары бағалады. Сәл кейінірек оның дұрыстығының тағы бір дәлелі пайда болды. Сол су сорғысынан алыс емес жерде орналасқан монастырьда ешкім қаза тапқан жоқ. Бірақ монахтар монастырь сыра қайнату зауытында ғана сыра қайнататыны белгілі болды. Қарды тексеру эпидемиология, медициналық география тарихындағы ірі оқиға, сондай-ақ халықтың денсаулығы мен жалпы адам қауіпсіздігі тарихындағы маңызды кезең болып саналады.

Ал Snow қолданатын әдіс білімнің түрлі салаларында қолданыла бастады. Қылмыстарды болжауға арналған бағдарламалық өнімдер қазірдің өзінде пайда болды және қолданылуда. Джон Сноу өзінің «тырысқақ картасын» жасау үшін қолданған талдау принципін қайта-қайта қолданады, бірақ олар үлкен көлемде деректермен жұмыс істейді. Ықтимал қылмыс көріністерінің ең танымал «болжамшыларының» бірі *PredPol* болып табылады.Бұл Калифорния университетінің қатысуымен және полициямен тығыз ынтымақтастықта әзірленген бағдарламалық пакет. Бұл «қылмысты болжау», полиция қызметкерлеріне не іздеу керектігін баяндайтын аналитикалық құрал. Ол қылмыстың қашан және қайда болатынын анықтауға мүмкіндік береді: ұрлық, тонау, жол-көлік оқиғасы, есірткіге байланысты қылмыс, көше бандаларының белсенділігінің артуы. Яғни қылмыс түрі туралы болжам беріледі, орны мен уақыты, бірақ кінәлінің жеке басы емес. Болжамдардың дәлдігі туралы деректер жоқ: әзірлеушілер мен өндірушілер бұл туралы үнсіз қалуды жөн көреді. Кент (Ұлыбритания) полициясы тұрақты патрульдеу кезіндегіден гөрі PredPol-ды пайдаланатын қылмыстар мен құқық бұзушылықтардың көп санын (10 есе!) сол жерде анықтау және алдын алу туралы ресми түрде жариялағанымен .

Алгоритмде жылдар мен ондаған жылдардағы қылмыстар туралы хабарламалар қолданылады және келесісін жасауы әбден мүмкін салалар анықталады. Қала картасында ол мұндай аудандарды қызыл шаршылармен белгілейді. Шындығында олардың көлемі 150 х 150 метр. Банкоматорлардың орналасуы, көше камераларымен жабылған орындар және «сұр» аймақтар, қылмыстық өткен адамдар тұратын жерлер, тәуліктің белгілі бір уақытында көшелерде адамдар ағыны ескеріледі. Сондай-ақ күн мезгілі, апта күні, ұлттық және діни мерекелер ескеріледі. Жүйе ықтимал қауіпті деп санайтын аумаққа полиция қызметкері немесе патрульдік автомобиль жіберілуі мүмкін. Қызметкерлер біреудің бос үйдің есігіндегі құлыпты таңдап алып, басқа біреудің автокөлігін ашып, пассажды шабуылдан құтқарып қалуға тырысатынын табуы мүмкін. Бірақ олай болмауы мүмкін. Таңдалған аймақты басып, құқық бұзушылық тарихымен таныса аласыз.

Бірақ жүйенің жақсы жұмыс істеуі үшін барлық құқық бұзушылықтар туралы полицияға хабарлау қажет, әсіресе тұрғындар этникалық тұрғыдан қоныстанған

аудандарда олай емес. Немесе адамдар ұрланған әнимені сонда да қайтара алмайтынын біле отырып, полициямен сөйлескісі келмейді. Оның әмиянында қолма-қол ақшамен бір доллар емес, банк карталары ғана болған. Адам банкке қоңырау шалып, карталарды бөгеп тастайды, жақын арада оларға не тегін, не ең аз ақыға жаңаларын береді. Барлық жекпе-жектер полицияның мәліметтер базасына енгізілмейді, ал ұлттық азшылықтар тұратын аудандарда тек зардап шеккендер болған жағдайда ғана күреседі, содан кейін әрдайым болмайды.

ПредПолдың негізін антрополог Геоффри Брэнтингем қалаған, статистика негізінде қылмыстық жер асты әлемін зерттейтін, Калифорния университетінде, Берклиде және Санта-Клара университетінде математик Джордж Молер. Ойлап табылған жүйе АҚШ армиясының пайдалануға берген жұмысына негізделген. Ғалымдар жауынгерлік операциялар кезінде қаза тапқандардың санын және Ауғанстан мен Ирактағы лаңкестердің мінез-құлқын болжау үшін модельдер жасады. Бұл веб-сайтта сипатталған жоба болды АҚШ Қорғаныс министрлігі. Ол «Терроризм көріністерін ақпараттық қолдау және оған қарсы күрес үшін спатио-темп-ралық сызықтық емес сүзгіні қолдану» деп аталды. Оған 2008 жылдан бастап қылмыстық әрекеттің статистикалық үлгілерін жасап келе жатқан Джеффри Брантигам қатысты.

АҚШ-тағы бұл жүйені Калифорния, Флорида, Мэриленд, Пенсильвания, Алабама, Вашингтон штаттарындағы полиция бөлімдері қолданады. 2014 жылдан бастап LAPD қолданып келеді. АҚШ-тан тыс, ол қазірдің өзінде айтылғандай Кент қаласында (Ұлыбритания) және Монтевидео (Уругвай) қаласында қолданылды. Лицензиялау құны қаладан қалаға өзгеріп отырады: Колумбия үшін (134 мың халқы бар Оңтүстік Каролина штатының астанасы), ол жылына 37,5 мың АҚШ долларын құрайды; Калифорниядағы Альхамбра үшін (85 мың адам), яғни жылына 22 000 АҚШ доллары.

PredPol-дың *көптеген* қарсыластары бар, олар жүйенің тиімділігі дәлелденбеген деп санайды, ал танымалдылығы маркетологтардың жақсы жұмысы. Бірақ полиция бұл құралды қабылдап, оны пайдаланады.

Хитачи, тұрмыстық техника, электроника және медициналық жабдықтар өндірушісі, *ақылды қала кешенінің бір бөлігі ретінде қылмысты болжау үшін қылмысты болжау үшін* өзінің Болжамды қылмыс талдау (PCA) модулін ұсынды. *Hitachi Visualise Suite (HVS)* деп аталатын бұлтқа негізделген платформа, ол 911 деректерін, бейнебақылау камераларын, нөмірлік белгілерді оқырмандарды және мылтық датчиктерін пайдаланады. Техаста қолданылады және Калифорния.

Әзірлеушілер Марк Жюль мен Даррин Липскомб қауіпсіздік мәселелерімен айналысты. Олардың компаниясын Hitachi компаниясы 2014 жылы сатып алды . RSA қылмыстық әрекет, ауа райы, қозғалыс, қоғамдық көлік маршруттары, бейнебақылау кадрлары және әлеуметтік желілердегі посттар туралы деректерді пайдаланады. Жүйе белгілі бір қалада не болып жатқанын түсіну үшін жергілікті сленгке негізделген твиттерді талдайды. Барлық түсініксіз хабарлар ұсталады. Әзірлеушілер мысал келтіреді. RSA McDonald's-тен сорғы сатып алу ұсынысы бар хабарды ұстайды. Бұл қалыпты емес. Жүйе бірден әрекет етеді, жергілікті сленгті талдап, McDonald's амфетаминді сатады деген қорытындыға келеді.

Түрлі-түсті блоктар қалалық картада осы жүйеде пайда болады, неғұрлым қараңғы болса, қылмыстық әрекеттің ықтималдығы соншалықты жоғары. Масштабы 0-ден 100-ге дейін. Шаршының көлемі 200 х 200 метрді құрайды. PCA әзірлеушілері ықтимал қылмыскердің жеке басын анықтау мүмкіндігі туралы да айтады. Жүйе PredPol сияқты қылмысты болжауға төтеп бере алмайды . Майдангерлерге көшелерде көмектеспейді, тіпті өз кеңселеріндегі сарапшылар оны жоғары бағалайды.

Нью-Йоркте NYPD тапсырысы бойынша әзірленген *Домен туралы хабардар болу жүйесі* деп аталатын *Microsoft дамуы* қолданылады. Жүйе 3000-нан астам бейнебақылау камераларына, полиция есептеріне, құтқару қоңырауларының жазбаларына, көлік құралдарының мәліметтер базасына және радиациялық датчиктерге қол жеткізе алады. Ол қала полициясына күдікті қызмет туралы пайдалы ақпарат береді, деректерді қорытындылайды және көрнекілендіреді. Бірақ бұл жүйе бұл қорытынды жасамайды. келесі қылмыс қайда және қашан болады.

Яғни, полицейлер бейнекамералардан жазбаларға лезде қол жеткізе алады, тергеушілер күдіктілерді қамауға алуды бақылайды, полиция дәл осы саладағы ұқсас қылмыстарды қадағалайды, қылмыстық схемаларды, ұқсас және соған байланысты оқиғаларды анықтап, бір ай бұрын қылмыскердің автокөлігінің қайда болғанын бақылап отыруға болады. Аудандағы қылмыстық әрекетке байланысты басшылар күштерді дұрыс бөле алады. Егер күдікті қапшық бір жерден табылса, жазбаны қайта жаңғыртып, оны кім әкелгенін көруге болады.

Қытайда Қытайдың әскери қажеттіліктері үшін орналасқан жері жабдықтары мен электрондық компоненттерді өндіруші *China Electronics Technology Group* террористік актілердің алдын алу жүйесі бойынша жұмыс жүргізуде, бірақ ол адамдарды толық бақылау жүйесі сияқты сипатталған.

Бұл жүйе адамның орындайтын жұмысы, карточкалар мен банк шоттарындағы ақша қозғалысы, хоббиі, сатып алынатын тауарлар мен қызметтердің түрлері мен жиілігі туралы деректерді талдай алады, сондай-ақ бұл деректерді бейнебақылау камераларының деректерімен салыстыра алады. Бұл ақпарат адам үшін ерекше әрекеттерді анықтау үшін қолданылады: кенеттен көп ақша біреудің шотына түседі, кенеттен біреу АҚШ-қа үнемі қоңырау шала бастайды.

Бұл жүйелердің барлығы үлкен деректерді пайдаланады. Мұндай компьютерлік жүйе ондаған жылдар бойы жасалып келе жатқан тәсілдерді автоматтандырып, құқық қорғау органдары «қолмен», «кенеттен мағлұматтар» ойлағаннан кейін және фотосуреттер мен жазбаларға қарағаннан кейін қазір әлдеқайда жылдам болып келеді.

Американдық детективтік фильмдерде детектив туралы бұл мағлұмат көбінесе өте тиімді көрсетіледі. Қазір машина оны көп сағат талдаусыз жасайды. Деректердің үлкен көлемін өңдеу үшін адам мүмкіндіктері шектеулі сананы пайдаланады, ал мұнда түзетуге, қайта конфигурлауға болатын машина бар, әрі ол одан да тиімдірек болады.

Бұл жүйелер қарапайым азаматтардың қауіпсіздігін қамтамасыз етуге көмектеседі. Мысалы, жүйе белгілі бір ауданда немесе алаңда қылмыстың өршуін күту керек деген болжам жасайды. Полицейлер қылмысты сол жерде көрсетіп, алдын алып немесе ашады, тіпті адамдар басқаша есеп бермейтіндер де бар. Қылмыс азайып барады.

Ірі қалаларда жүйеге тек ауыр құқық бұзушылықтар ғана жүктеледі, әйтпесе Нью-Йорк сияқты қалада полиция жай ғана төтеп бере алмайды. Ал Кентте олар бәрін, тіпті ең кішкентай құқық бұзушылықтарды да жүктейді. Жемісі – көрікті.

Біздікі не және біздікі емес

Әр түрлі елдерде көптеген адамдар шетелдік бағдарламалық қамтамасыз етуге тәуелді, көбінесе американдық, ал теориялық тұрғыдан кейбір елде (мысалы, Ресейде) Windows бұғатталуы мүмкін. *Бүгінгі* таңда барлық дерлік бағдарламалық қамтамасыз ету мен барлық дерлік аппараттық құралдар, яғни кез келген бағдарламалық-аппараттық құралдар қашықтан басқарылады. Яғни, олар жеткізушіге байланған. Көп жағдайда кейбір ақпарат алу үшін жеткізушіге хабарласатын кіріктірілген модульдер бар. Бұл жүйеге қашықтан және тіпті ажыратылуы мүмкін дегенді білдіреді.

Жеткізуші жүйеге қолжетімділікті сақтап қалғысы келеді. Бұл түсінікті. Ол техникалық қолдау көрсетуі қажет. Қазіргі заманғы технологиялар жүйені қашықтан орнатуға мүмкіндік береді, егер онда бірдеңе бұзылса немесе қағып кетсе. Сондай-ақ, жеткізуші клиенттерді өзіне байлап, оларды ілмектеп ұстағысы келеді.

Сондықтан, өз қауіпсіздігіне қамқорлық жасайтын кез келген елдің басқа елдердің, әсіресе оның ең жақсы қарым-қатынасы жоқ елдердің технологиясына тәуелді инфрақұрылымға ие болуға құқығы жоқ. Кибершабуылдар қаупі бұл күндері ешкімді таң қалдырмайды. Бірақ қандай да бір себептермен кейбіреулер әлі күнге дейін өз болмысына сенбейді. Бірақ босқа кетіп жатыр. Иә, қарапайым адамға бір елдің басқа жарықты өшіре алатынын елестету қиын. Мүмкін! Егер қуат жүйесі Интернетке қосылған модульдермен басқарылса, онда бұл қауіпсіздіктің төмен деңгейін білдіреді. Талантты хакерлер бұл жүйеге жақсы енуі мүмкін. Ал жеткізуші араласа алады.

Бағдарламалық жасақтама пайдаланушыға шпионаж жасау мүмкіндігін ашады. Ал бұл бағдарламалық жасақтама келген шет ел осы бағдарламалық жасақтама қолданылатын басқа мемлекеттің азаматтарына шпионаж жасай алады. Бұл жаппай бақылау болуы мүмкін. Пайдаланушы деректерін смартфондар, әлеуметтік желілер, фитнес-білезіктер және барлық заманауи гаджеттер жинайды. Деректер платформада жиналады, талданады және көбінесе серіктестермен бөліседі мақсатты жарнама үшін. Жоғарыда айтылғандай, *Apple* да, *Google да* деректерді ФБР-ға бергісі келмейді, керісінше, олар өз пайдаланушыларының деректерін қорғауды жақтайды. Бірақ бүгінгі әлемде деректерді қорғауға сенімді бола алмаймыз. Себебі, ФБР Сайд Фаруктың смартфонына соққы бере алды, дегенмен *Apple* үзілді-кесілді әмбебап кілтті әзірлеуден бас тартты.

Сондай-ақ, қандай да бір себептермен белгілі бір тұлғаны бақылап отыруға болады, тапсырыс берушінің, мысалы, шет ел үшін қызығушылығын тудырады. Бұл саясаткер немесе шенеунік немесе клиент үшін маңызды нәрсені білетін бизнесмен болуы мүмкін. Бүгінгі таңда сілтемені басшылыққа алуды, жүлделі жеребеге қатысуды немесе SMS арқылы қатысуды ұсына отырып, вирусты немесе Троянды смартфонға іске қосу қиын емес. Троя бағдарламалық жасақтамасын отырғызу құралдарын әзірлеушілер әлеуметтік инженерия мамандары болып табылады. Бұл нағыздары. Клиент басатын ұсыныстарды ойлап тапқан кәсіпқойлар және солай. Шпиондық бағдарламалар дұрыс адамның смартфонында тұрып, болып жатқанның бәрін қадағалайды. Сондай-ақ, басқа біреудің компьютеріне қосылуға болады, әсіресе, егер адам ноутбукпен барлық жерде жүрсе. Ол дәмханада керек пе? Егер сіз *кез келген жерде Wi-Fi-ге* жабыссаңыз, сіз кейбір виртуалды нәрселерді алуға міндеттісіз. Сіз мемлекеттік құпияларды немесе тіпті корпоративтік құпияны сақтаушы болмауыңыз мүмкін, бірақ сізде біраз ақша бар. Оларды жоғалтқаныңызға кешірім сұрайсыз. Сондықтан планетамыздағы ең бай және жоғары лауазымды адамдардың қазір қарапайым итеру-түйме телефондарына қайта оралғаны таң қалдырмайды.

Шпионды жеке гаджеттерге ғана емес, корпоративтік желіге де іске қосуға болады. Дегенмен, ол белгілі бір смартфонға немесе компьютерге қосылудан әлдеқайда күрделі. Егер компьютер корпоративтік желіге қосылған болса және оны кеңседен шығару мүмкін болмаса, онда оған Трояны енгізу үшін корпоративтік желіні соққан жөн.

Ресейлік хакерлер сайлауға дейін АҚШ Демократиялық партиясының серверіне соққан деп айыпталды. Егер олар шын мәнінде ақпаратты алса, ресейлік хакерлер шын мәнінде кінәлі ме? Себебі, олар бір нәрсені соққанға дейін (егер солай істесе), қауіпсіздік ережелері өрескел бұзылған. Құпия ақпараттың құпия желіден шығарылуы ресейлік хакерлер кінәсінен болған жоқ. Құпия деректер үй компьютерінде аяқталды. Ресей хакерлерінің кінәсі бар ма?

Хакерлер әлемдегі оқиғаларға шынымен де әсер ете алатыны туралы көп айтылады. Иә, олар жасай алады! Кибер соғыс - қарсыластың инфрақұрылымын өшіру немесе ақпаратты ұрлау мақсатында вирустық бағдарламаларды немесе кодты жазу. 2017 жылы кибершабуылдар әлемнің 150 еліндегі ұйымдардың жұмысын бөгеп тастады, және бұл ұялы байланыс операторларын, мемлекеттік органдарды қоса алғанда, түрлі ұйымдар болды. Қазіргі заманда мұндай шабуылдар анонимді, ұйымдастырушыны немесе бастамашыны анықтау қиынға соққан. Осыдан келіп «ресейлік хакерлер» деген айыптаулар бар. Көбіне қаржы институттарына қарсы шабуылдар ұйымдастырылып, олардың саны артып келеді. Мемлекеттер өз қарсыластарымен күресу үшін әзірлеген құралдарды ұрлауға болады, ал шетелдік шпион енді шет елге физикалық жол жүруге тиіс емес. Мысалы, 2017 жылы жүргізілген кибершабуыл, соның нәтижесінде CIA әзірлеген *WannaCry вирусын* ұрлады. Бұл рансоматор тіпті «жыл вирусы» атағын алды. Барлығы 500 мыңнан астам компьютер зардап шекті.

Кибер қарудың алғашқы және белгілі үлгілерінің бірі *Stuxnet вирусы* болып табылады.Ол Microsoft Windows операциялық жүйесін *іске қосатын компьютерлерді жұқтыратын компьютер құрты*.Бұл компьютер құртын өнеркәсіптік зауыттарда, электр станцияларында және әуежайларда деректерді рұқсатсыз жинау және диверсиялау үшін пайдалануға болады. Бұл тарихта алғаш рет вирус инфрақұрылымды физикалық тұрғыдан жойды. Бұл АҚШ пен Израильдің барлау қызметтері қабылдаған өте жоғары білікті даму. Ол Иранның ядролық жобасына қарсы бағытталған деп есептеледі. Американдық журналист Дэвид Сэнгер өзінің «Қарсы тұру және жасыру: Обаманың астыртын соғыстары және Америка күшінің таңқаларлық қолданылуы» американдық үкімет жобалаған Иранға қарсы «Олимпиада ойындары» операциясының бір бөлігі деп мәлімдейді. 2011 жылы АҚШ Мемлекеттік хатшысы Хиллари Клинтон *Stuxnet* жобасының өте табысты болғанын және Иранның ядролық бағдарламасы бірнеше жылға созылғанын мәлімдеді. Израильдіктер оны Негев шөліндегі орталығында сынақтан өткізді деп мәлімдеген.

Вирус Microsoft Windows *жүйесіндегі төрт осал тұсты пайдаланды* және тек үш жылдан кейін (даму сәтінен бастап ашылған сәтке дейін) табылды. Мұны «VirusBlokAdada» компаниясының белорустық сарапшысы Сиархей Уласен жасады. Операция барысында вирус Ирандағы уранды байыту зауытында центрифугаларды ажыратып қана қоймай, әлемнің түкпір-түкпіріндегі бірқатар нысандарды ластауға қол жеткізді. мысалы, Ұлыбритания мен Ресейде.

Әдетте вирус бірнеше сағат немесе тіпті минуттарда әлдеқайда жылдам анықталады. *Stuxnet-пен* жағдай ерекше және бір түрлі. Мүмкін, себебі әзірлеушілердің өте жоғары біліктілігі. Бірақ болашақта бірде-бір әзірлеуші вирусты бақылай алмайды — оны «босатқаннан» кейін. Ал вирус тек өзі әзірленген елде ғана емес, нысаналарды жұқтыруы мүмкін, бірақ кез келген басқа, оның ішінде құрылыс салушы елге де. Ал көп жағдайда компьютерлік вирустардың авторлығын анықтау мүмкін емес. Егер әзірлеуші қаламаса, онда вирустың «ұлтын» анықтау мүмкін емес.

Әлемнің көптеген дамыған (және тек қана емес) елдерінде киберқауіптерден қорғау үшін мамандандырылған орталықтар немесе бөлімшелер құрылды, компьютерлік шабуылдарды анықтаудың, алдын алудың және жоюдың мемлекеттік жүйелері жұмыс істейді. Олар ең алдымен мемлекетке тікелей де, жанама да зиян келтіруі мүмкін қауіп-қатерлермен айналысады.

Қытайда «Қытайдың Ұлы брандмауэрі» деп аталатын, оны алтын қалқан деп те атайды. Ол интернет арқылы сырттан келіп түсетін барлық ақпаратты сүзеді. Жобаны әзірлеу 1998 жылы басталып, 2003 жылы бүкіл ел бойынша іске асырылды. Жүйеде

бірнеше кіші жүйелер бар, мысалы, қауіпсіздікті басқару, ысқыру, жол қозғалысын басқару, ақпараттың кіруін бақылау және т.б.

«Алтын қалқан» ҚХР аумағынан бірқатар шетелдік веб-сайттарға кіруді шектейді. Мысалы, Facebook Қытайда жұмыс істемейді . ҚХР-да орналасқан веб-сайттарға арнайы алдын ала мақұлдаусыз шетелдік веб-сайттардан немесе БАҚ-тан жаңалықтарды жариялауға немесе тіпті сілтеме жасауға рұқсат етілмейді. Сүзгілеу мемлекеттік қауіпсіздікке байланысты кілт сөздерде жүргізіледі. Сондай-ақ, веб-сайт мекенжайларының қара тізімі бар.

Яғни, қытайлықтар ірі платформаларды бөгеп үлгерді, ал ақпараттық технологиялар арқылы Қытайды сырттан бақылау мүмкін емес. Қытайдың өз әлеуметтік желілері мен түрлі жүйелері бар. Бірақ, қалай болғанда да, Интернет халықаралық желі болып табылады, ал кейбір қауіп-қатерлер әлі де таралатын болады.

Ортақ адамға арналған кеңестер

Егер әлеуметтік желілерді және бұлтты сақтаудың кез келген қызметтерін пайдалансаңыз, бұл ақпараттың жалпыға қолжетімді екенін түсінуіңіз қажет. Сіздің отбасыңыздан, достарыңыздан, жұмыс берушілеріңізден басқа ешкім сізді қызықтырмайды деп есептейсіз. Смартфонды пайдаланып, әлеуметтік желілерді үнемі пайдаланасыз. Сіз жариялаған ақпаратқа ешкім қызығушылық танытпайтынына әбден сенімдісіз бе?

Сіз тек әлеуметтік желілерде достарыңыздың шағын шеңберімен ғана тұрсыз деп ойлайсыз. Жоқ. Сіз ақпаратты сол жерден шығарып жатырсыз. Бұл ақпаратқа миллиондаған адам қол жеткізе алады. Ал сіздің басылымыңыздың одан арғы өмірін бақылауға мүмкіндігіңіз жоқ. Оны жойып, біреу көшіріп алса да, ол өз өмірін сенсіз өмір сүреді де, оған ықпал ете алмайсың. Достарыңыздың шағын үйірмесі үшін бірдеңе жариялайсыз, ал досыңыз оны алып, миллиондаған немесе нақты қызығушылық танытқан адамдарға ұсынады. Және тағы да ештеңе істей алмайсың. Сондықтан ештеңені онлайн режимінде орналастырмас бұрын өте мұқият ойланыңыз. Сіздің ескі көкек немесе жай ғана құбылмалы фотосуреттеріңіз бірнеше жылдан кейін жақсы жұмысқа кірісуге кедергі келтіруі мүмкін.

Сондай-ақ, қазіргі заманғы гаджеттеріңіздің ешқайсысы технологияны әзірлеушіге тиесілі екенін ұмытпаңыздар. Оған не салды? Операциялық жүйеге өзгерістер енгізуге тырыссаңыз, ол қалай әрекет етеді? Платформа және бағдарлама жеткізушілері құрылғыларыңызда сақталатын ақпаратқа қатынаса алады. Орналасқан жеріңізді телефон арқылы анықтауға болады. Бұл сіз туралы ақпараттың қазына трофейі.

Біз әдетте Facebook *сияқты сайттарға не жүктейміз*? Онда біз тұратын демографиямызды, отбасымыз бен достарымызды, достарымызды, мүдделерімізді, құштарлықтарымызды, білім алуымызды, үй жануарларын, фотосуреттерді, бейнелерді және т.б. таба аласыз. Біздің замандасымыз, танымал математик Стивен Вольфрам, сондай-ақ Вольфрам Альфа деген атпен белгілі «білімнің есептеу қозғалтқышын» жасаушы, «*Facebook үшін жеке аналитика» деген атпен белгілі тұтыну бағдарламалық өнімін жасады.*Бір минуттың ішінде бұл бағдарламалық жасақтама сіз және сіздің әлеуметтік байланыстарыңыз туралы деректер мен графиктердің орасан зор жиынтығын түкіреді. Вольфрамның өзі оны «өмір бойы бақылау тақтасы» деп атады. Егер сіз *Facebook желісінде* тіркелсеңіз, онда сізге жеке нұсқасыңызды көруге кеңес беремін, ол тегін: *http://www.wolframalpha.com/facebook/. Бағдарлама* Facebook желісінде жарияланған барлық ақпаратты шығарып, барлық жазбаларыңыздан деректерді бұлтпен сақтауды, сапарыңыздың нақты уақытын және жұмыс істеу

тәртібін, ұнатуларыңыз бен комментарийлеріңізді, сізге ең ұнаған жазбаны, ең көп түсініктемелер алған жазбаны, барлық достарыңыздың демографиясын жасайтындықтан, көріп отырғандарыңыз *кішкене ыңғайсыз болуы мүмкін*, оның ішінде орналасқан жері, жергілікті уақыты мен туған күндері, сіздің әлеуметтік байланыстарыңыздың карталары, достарыңыз бен отбасыңызды, ықпалын, көршілерін, байланыстардың әлеуметтік элементтерін, кездейсоқ және жақын адамдарды бөліп көрсететін әлем картасы.

Кімде-кімнің білгісі келе ме? Олай болмаса, бірдеңені онлайн жазудан бұрын ойланыңыз немесе әлеуметтік желілердегі бетіңізге, тіпті ең тар шеңбер үшін де бірдеңені кері жүктеңіз.

Сілтемелер :

1. Жай үлкен деректер. Санкт-Петербург қаласы, Страта Публ., 2019 жыл. - 148 б.