NUM Law Review; Volume 26, No. 72. June 2025, 41-66
Article https://doi.org/10.22353/nlr.2025.02.03
Received on 2025.03.01; Accepted on 2025.04.25; Published online on 2025.05.31.

Хүний хувийн мэдээллийн хамгаалалт ба үндэсний аюулгүй байдлын уялдаа хамаарал

The Relation Between Personal Data Protection and National Security

Мөнхбаярын Хатанзориг

Хууль зүйн ухааны доктор (Ph.D.).
Шихихутуг их сургуулийн
Хувийн эрх зүйн тэнхимийн дэд профессор,
Улаанбаатар хот, Монгол Улс.
khatanzorig@shihihutug.edu.mn

[Товч утга]

Цахим технологийн хөгжил эрх зүй ба аюулгүй байдлын олон шинэ сорилтыг бий болгосны нэг нь дотоод, гадаадын байгууллагууд улс төрийн зорилгоор хүний эрхийг зөрчиж олон нийтийг тагнах, нарийвчилсан арга технологиор ухуулга сурталчилгаа хийх явдал мөн. Үүнийг улс орнууд аюулгүй байдлын ба хууль зүйн бодлогодоо харгалзаж иргэдийнхээ хувийн мэдээллийг дотоодын улс төрийн бүлэглэл, гэмт этгээдүүд хийгээд гадаад улсын байгууллагаас хамгаалах эрх зүйн орчныг бүрдүүлэхийг хичээж байна. Энэ өгүүлэлд иргэний хувийн мэдээллийн хамгаалалт үндэсний аюулгүй байдлыг хангах эрх зүйн баталгаа болоход нөлөөлсөн хүчин зүйлсийг (1) глобал цахимжилт, (2) өгөгдлийн сангийн тэсрэлт хэмээн тодорхойлж, гурван тохиолдлыг шинжлэн, АНУ, ОХУ, БНХАУ-ын аюулгүй байдлын эрх зүйн бодлогод уг асуудлыг харгалзсан талаар хөндөнө.

[Түлхүүр үг]

Хувийн мэдээлэл хамгаалал, хувийн халдашгүй байх эрх, мэдээллийн аюулгүй байдал, цахим аюулгүй байдал, аюулгүй байдлын эрх зүй.

I. Оршил

Цахим болон тоон технологийн хөгжил нийгмийн өдөр тутмын амьдралд өргөн хүрээнд нэвтэрч буй олон сайн талтай боловч цөөнгүй сөрөг үр дагаврыг үүсгэж байна. Тэдгээрийн нэг нь олон нийтийг тагнах, хэрэглэгчдийн болон сонгогчдын хувийн мэдээлэлд тулгуурлан суртал ухуулга хийх ажиллагаа мөн. Иймм ажиллагааны үр дүнд үндэсний дотоод аюулгүй байдлын баталгаа алдагдах, цаашлаад дэлхийн дэг журамд нөлөөлөхүйц улс төрийн шийдвэр гаргуулах боломжтойг харуулсан фактууд хэдийн олон нийтэд боллоо. Үүний эсрэг улс орнууд кибер аюулгүй байдлын техникийн нөхцөлд үлэмж анхаарахын сацуу мэдээлэл хамгаалах эрх зүйн орчныг аюулгүй байдлын ашиг сонирхлын үүднээс өөрчлөн зохицуулж байна. Энэ үед иргэдийнхээ мэдээллийг хамгаалах эрх зүйн гол үндэслэл нь "privacy law" буюу хувийн халдашгүй байх эрхийг хангах хууль зүйн орчин болно. Манай улсын хувьд ч эл эрхийн талаарх төрийн байгууллага, албан хаагчдын эрх зүйн ухамсар сул[1] бөгөөд үндсэн хуулийн эрх зүйн маргааны түвшинд хөндөгдөх болсон[2] хэдий ч судлагдсан байдлын хувьд харьцангуй хязгаарлагдмал.[3]

---

[1] ҮХЦ-ийн 2023 онд "Гүйцэтгэх ажлын тухай хуулийн 6 дугаар зүйлийн 6.3 дахь хэсгийн зарим заалт Монгол Улсын Үндсэн хуулийн холбогдох заалтыг зөрчсөн эсэх" маргааныг хянан шийдвэрлэхэд УИХ, ТЕГ, УЕПГ "иргэн тагнах, чагнах төхөөрөмжийг илрүүлэгч төхөөрөмжтэй байж болохгүй зохицуулалт нь хүний халдашгүй байх эрхийг зөрчөөгүй" гэх тайлбарыг тууштай баримталж байв. Олон улсын жишгээр иргэн тагнах төхөөрөмж эзэмшиж болохгүй боловч илрүүлэх төхөөрөмж ашиглах эрхтэй байдаг. Уг хэргийг хянан шийдвэрлэхэд МУИС-ын ХЗС-ын дэргэдэх ҮХЭЗХ-ээс дүгнэлт гаргуулж, ҮХЦ мөн оны 03 дугаар сарын 15-ны өдрийн 04 дугаар тогтоолоор уг дүгнэлтийг хүчингүй болгосон байна. Дэлгэрэнгүйг: https://legalinfo.mn/mn/detail?lawId=16960262179051

[2] Үндсэн хуулийн цэцийн 2024 оны 03 дугаар дүгнэлтэд Үндсэн хуулийн Арван зургадугаар зүйлийн 13 дахь заалтыг өргөн агуулгаар тайлбарласан нь үзэл баримтлал, хэрэглээний хувьд зүйтэй, уг эрхийн хамгаалалтын хувьд ач холбогдолтой бөгөөд 2024 оны 04 дүгээр дүгнэлтийн 23 дугаар талд "...Хувийн халдашгүй байх эрх нь хүний хувийн амьдралд үндэслэлгүйгээр халдахаас хамгаалах ..., бусдын хараа хяналтаас ангид, хүсэл зоригийнхоо дагуу амьдралаа удирдан зохицуулах агуулгатай..." хэмээн тайлбарласан байна.

[3] Уг эрхийн талаар монгол хэл дээрх эх сурвалжуудад ихэвчлэн дам, хавсарга байдлаар авч үздэг. Монгол хэл дээрх энэ сэдвийн хүрээнд дэлгэрэнгүйг М.Хатанзоригийн "Хувийн халдашгүй байх эрхийн агуулгыг харилцан хүлцлийн үзэл баримтлалаар тодорхойлох нь" сэдэвт хууль зүйн докторын ажил (2023), М.Хатанзоригийн "Хүний Дангаарших Эрхийн Талаарх Америкийн Нэгдсэн Улсын Дээд Шүүхийн Голлох Шийдвэр, Түүний Зарим Үр Дагавар №1: Катзын Маргаан" эрдэм шинжилгээний өгүүлэл (Хүний эрх сэтгүүл 2021/1), "Хүний Дангаарших Эрхийн Талаарх Америкийн Нэгдсэн Улсын Дээд Шүүхийн Голлох Шийдвэр, Түүний Зарим Үр Дагавар №2: Грисволдын Маргаан" эрдэм шинжилгээний өгүүллээс (Шихихутуг сэтгүүл 2021/тусгай дугаар) үзнэ үү.

Энэхүү өгүүллээр иргэдийнхээ хувийн халдашгүй байдлыг хамгаалах нь нийгэмд нийлбэр утгаараа үндэсний аюулгүй байдлыг хангах ач холбогдолтой хэмээх таамгийг батлахын тулд тодорхой тохиолдлуудад дүн шинжилгээ хийн, гадаад улсуудын эрх зүйн орчныг тоймлон харьцуулах замаар үндэслэл дэвшүүлж байна. Өгүүллийн нэгдүгээр хэсэгт хувийн мэдээллийн ашиглалт, хамгаалалт үндэсний аюулгүй байдалд нөлөөлөх болсон нь глобал цахимжилт, өгөгдлийн сангийн тэсрэлтээс шалтгаалсан талаар мөн авч үзлээ. Өгүүллийн эцэст хувийн халдашгүй байх эрхийг хамгаалах төвлөрсөн хууль тогтоомжийг баталж хэрэгжүүлэх нь хүний эрхийг хамгаалахын сацуу үндэсний аюулгүй байдлыг хангахад ач холбогдолтой талаар санал дэвшүүлэв.

II. Хүний хувийн мэдээллийн ашиглалт үндэсний аюулгүй байдалд нөлөөлөх нь

Их хэмжээний мэдээллийн урсгал ба тэдгээрийг ашиглах боломж, эрсдэл нь цахим ба тоон технологи нийгмийн өдөр тутмын амьдралд өргөн хүрээнд нэвтэрсний голлох үр дагаврууд мөн. Хүний хувийн мэдээллийг цуглуулах замаар улс төр, эдийн засгийн ба бусад шийдвэрт нь нөлөөлөх; олон хүний хувийн мэдээлэлд тулгуурлан нийгмийн сэтгэл зүй, хамтын шийдвэрт нөлөөлөх асар өргөн боломж бүрдсэн байна. Ингэснээр зөвхөн хүний субьектив хувийн халдашгүй байх эрхийг зөрчөөд зогсохгүй, түүгээр дамжин коллектив ашиг сонирхол, тэр дундаа үндэсний аюулгүй байдалд заналхийлэх[4] болжээ. Энэ утгаараа хувийн халдашгүй байдал (эрхээр хамгаалагдах) ба үндэсний аюулгүй байдал олон талаар холбоотой ойлголтууд болсон байна.

Судалгааны объектын хувьд “үндэсний аюулгүй байдал”-ыг тодорхойлох буюу түүний хүрээг тогтооход хүндрэлтэй талаар судлаачид ((Wolfers, 1952) (Buzan & Hansen, 2009) (Taylor, 2012)) тодотгон тэмдэглэдэг. Хэл зүйн хувьд “аюулгүй байдал” аливаа аюул заналаас ангид байх хэмээх утгыг илэрхийлэх нь түгээмэл[5] ба үндэсний аюулгүй байдлыг үзэл баримтлалын хувьслын хувьд

[4] Англи хэлний “threat”, орос хэлний “угроза” буюу “занал” гэдэгт нийтлэг утгаараа бодитойгоор хэрэгжих боломжтой аюул буюу хохирол учрах бодит эрсдийг ойлгоно.

[5] Тухайлбал Оксфордын болон Британника толь бичигт “аюул, заналаас ангид байх нөхцөл байдал” гэж; Кембриджийн толь бичигт “хүн, барилга, байгууллага, улсууд гэмт хэрэг ба гадаад улсын довтолгоо зэрэг аюулаас хамгаалагдсан байдал” гэж; Коллинсын толь бичигт “аюулаас ангид, санаа зовних шаардлагагүй нөхцөл” гэж; Монгол хэлний тайлбар тольд “Аюул байхгүй, айж эмээх, сандрах түгшүүргүй” гэж тодорхойлсон байна.

ерөнхийд нь уламжлалт[6], сонгодог[7], орчин үеийн[8] хэмээн ялгаж үзэх боломжтой. Ялангуяа XX-р зууны хоёрдугаар хагас, XXI-р зууны эхлэл аюулгүй байдал судлал, түүний үзэл баримтлалд багагүй нөлөө үзүүлжээ.[9]

Судлаачдын[10] хүлээн зөвшөөрснөөр хүйтэн дайны төгсгөлөөс хамгийн чухал гурван үр дагаврын хоёр нь[11] (1) олон улсын улс төрийн харилцаанд зэвсэгт хүчний ач холбогдол их хэмжээгээр буурсан; (2) үндэсний аюулгүй байдлын талаар илүү өргөн хүрээний үзэл баримтлалыг тодорхойлох хэрэгцээ үүссэн явдал ажээ. Энэ нь цэрэг, зэвсгийн хүчинд тулгуурласан дайны үеийн аюулгүй байдлын үзэл хандлагаас өргөжиж орчин үеийн олон талт, динамик баримтлалд хөтөлсөн гэж болно. Барри Бузаны тэмдэглэсэнчлэн[12] аюулгүй байдлын үзэл баримтлал өргөн хүрээтэй бөгөөд аль нэг талбараархязгаарлажүлболно.Энэмэтзаримсудлаачүндэснийаюулгүй байдлыгөргөнутгаарньавчүзэхийгдэмждэг.ДевидБалдвиныүзсэнээр[13]

---

[6] Уламжлалт хандлага гэдэгт тусгаар улсын (sovereign) номлол үүсэж хөгжихөөс өмнөх үзэл баримтлал буюу объектын хувьд эзэмшил нутаг, хоол хүнсний эх үүсвэр, хөдөө аж ахуйн баялаг, гишүүдийн өмчид тулгуурласан; байгалийн гамшиг, бусад овог, бүлгийн халдлагаас ангид байхыг ойлгож болох юм. Цаг хугацааны хувьд дундад зуунаас өмнөх үед хамаарах ба заншлын хэм хэмжээгээр голчлон зохицуулагдана. Энэ үзэл хандлагыг зарим эх сурвалжид (Saša Mijalkovic, 2014) "вестфалийн өмнөх үеийн" хэмээн нэрлэсэн байна.

[7] Сонгодог хандлага гэдэгт дотоод асуудлаа бие даасан шийдвэрлэх бүрэн эрх бүхий тусгаар улсуудын номлолд тулгуурласан; газар нутаг, тусгаар тогтнол нь гадаад халдлагаас ангид байх нөхцөл бүхий үзэл баримтлалыг ойлгож болно. Уг хандлага нь "үндэсний аюулгүй байдал" хэмээх ойлголтыг эрх зүйн хувьд анхлан бий болгосон хэлбэр гэж үздэг (Holmes, 2015) (Saša Mijalkovic, 2014). 1555 оны Аугсбүргийн гэрээ, 1635 оны Прагын гэрээ, 1648 оны Вестифалийн гэрээнд тулгуурлан хүлээн зөвшөөрөгдсөн тусгаар улсын үзэл баримтлал нь уг хандлага үүсэх гол үндэслэл болсон.

[8] Орчин үеийн хандлага нь зэвсэгт хүчин, цэргийн халдлагаар үл хязгаарлагдан аюулгүй байдлыг олон талт, динамик ухагдахуун хэмээн үздэг. Үүнд нийгэм, эдийн засаг, хүрээлэн буй орчин, дэд бүтэц зэрэг олон талын хүчин зүйлс хамаарна.

[9] Taylor, 2012 болон энэ бүлгийн ном зүйд дурдагдсан бүтээлүүдээс дэлгэрүүлж үзнэ үү.

[10] Baldwin, D. A. (1995). Security studies and the end of the cold war. World Politics 48, 117-41; May, E. R., Garthoff, R. L., & Jervis, R. (1992). The End of the Cold War: Its Meaning and Implications. (M. J. Hogan, Хян.) New York: Cambridge University Press; Peterson, P. G., Treverton, G. F., & Bicksler, B. A. (1992). Rethinking America's Security: Beyond Cold War to New World Order. (G. Allison, & G. F. Treverton) New York: W. W. Norton.

[11] Гуравдах үр дагавар нь олон улсын харилцаа ба үндэсний аюулгүй байдлын талаарх судлаачдын үзэл хандлагыг эргэн шинжлэх хэрэгцээ тулгарсан явдал.

[12] Аюулгүй байдлын үзэл баримтлал нь олон улсын эдийн засаг, харилцааны онол, энх тайван судлал, хүний эрх, хөгжлийн төлөвлөлт судлал, олон улсын түүх гэх мэт олон талбарыг нийлүүлэхүйц өргөн хүрээг хамардаг (Buzan, B. (1991). People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era, 2d ed. Colorado: Lynne Rienner).

[13] Baldwin, D. A. (1995). Security studies and the end of the cold war. World Politics 48,

(радикал реформын концепц) үндэсний оршин тогтнохуй, сайн сайхан байдалд учрах аюул, занал нь зөвхөн цэрэг, зэвсгийн хүрээгээр үл хайрцаглагдах ба хүрээлэн буй орчин, эдийн засаг, нийгмийн шударга ёс ба хүний эрх зэрэг олон салбарын нэгдмэл талбар болох юм.

Ялангуяа эрх зүйт ёс, ардчилсан дэглэм бүхий нийгэмд хүний эрхийн аюулгүй байдлын ач холбогдлыг чухалчлан анхаарвал зохино. Зарим судлаач[14] энэ талаар цохон тэмдэглэж (АНУ-ын жишээн дээр), "хүний эрхийг аюулгүй байдлын бутач, дэд ойлголт гэх өнцгөөс бус хоорондоо шууд хамааралтай, харилцан биенээ нөхдөг буюу дэмждэг ухагдахуун гэж үзэх нь зүйтэй бөгөөд энэ нь идеалогийн эсвэл норматив үндэслэлээс гадна стратегийн бодит ач холбогдолтой" талаар үндэслэл дэвшүүлжээ. Ач холбогдлын эрэмбээрээ аюулгүй байдал нь хүний эрх хамгаалагдах үндэс, нөхцөл мөн боловч тодорхой тохиолдолд эдгээр нь харилцан биенээ нөхцөлдүүлэгч интердепентент ойлголтууд болно. Ялангуяа глобал цахимжилт, өгөгдлийн сангийн тэсрэлт хүний хувийн халдашгүй байх эрхийн аюулгүй байдлын ач холбогдлыг улам нэмэгдүүлснээр эл эрхийн агуулга, үндэслэлийг гүнзгийрүүлэн судлах, тодорхойлох шаардлагыг өсгөжээ.

Аюулгүй байдалд тулгуурласан хүний эрхийн шинжилгээ нь хүний эрх, тухайн эрхтэй холбоотой феноменүүдийг аюулгүй байдалтай хэрхэн холбогдох буюу түүнд ямар ач холбогдолтой талаас нь авч үзнэ. Хувийн халдашгүй байх эрхийг үндэсний аюулгүй байдалтай хамааруулан шинжлэх шаардлага нь глобал цахимжилт, өгөгдлийн сангийн тэсрэлт гэсэн үндсэн хоёр хүчин зүйлээр нөхцөлдсөн байна.

А. Глобал цахимжилт

Цахимжилт гэдэгт ерөнхийдөө нийгмийн өдөр тутмын амьдрал технологиос салшгүй хамааралтай болох процессыг ойлгож болно. Цахим технологийн тусламжтай хүмүүс хувийн амьдрал, нийгмийн харилцаа, төрийн үйлчилгээ зэрэгт аналог технологи, уламжлалт хэлбэрээс илүү хялбар, боловсронгуй аргаар харьцах, оролцох боломж бүрдсэн байна. Цахимаар хувцас, хүнс, тасалбар зэрэг шаардлагатай бараа, үйлчилгээ захиалах, дүрсээ харж холбогдох, цаасан бус электрон файлууд солилцох, иргэний болон эд хөрөнгө, хуулийн этгээдийн бүртгэл, тодорхойлолт авах, сонгуульд саналаа өгөх, гомдол гаргаж хариу хүлээн авах, мэдээллийн агентлагийн тусламжгүйгээр олон нийтэд мэдээлэл түгээх гэх мэт өргөн хүрээний үйл ажиллагаа явуулах боломжтой.

117-41.

[14] Burke-White, W. W. (2004). Human Rights and National Security: The Strategic Correlation. Harvard Human Rights Journal, 17, 249-280.

Тодорхой утгаар цахимжилтын илрэл нь дуу, дүрс, текст зэрэг аливаа аналог мэдээллийг тоон буюу дижитал мэдээлэлд хувиргах; гар утас, компьютер, зурагт зэрэг цахим технологид суурилсан багаж хэрэгсэл өдөр тутмын амьдралын салшгүй хэсэг болох; ухаалаг төхөөрөмж, интернэт зэргийг ашиглан цахимаар мэдээлэл солилцох буюу харилцаа холбоог цахим хэлбэрт шилжүүлэх; татвар төлөх, даатгалд хамрагдах, тодорхойлолт авах, санал гомдол гаргах, сонгууль зохион байгуулах гэх мэт төрийн үйлчилгээ, Засгийн газрын үйл ажиллагааг тоон системд шилжүүлэх; цахим технологид суурилсан бизнес эдийн засагт өөрийн гэсэн орон зайг эзлэх; цахим технологид суурилсан тооцоолууруар их хэмжээний өгөгдөлд дүн шинжилгээ хийх гэх мэт олон янз байж болно. Цахимжих үйл явцад мэдээлэл, харилцааны технологи чухал байр суурь эзэлнэ.[15]

Электрон тооцооллын технологийн боломж, хэрэглээ асар хурдацтай нэмэгдэж интернэт хэрэглэгчийн тоо 2021 оны байдлаар 4.95 тэрбум хүрч өмнөх оныхоос 300 саяар нэмэгджээ.[16] 2022 оны 1-р сарын байдлаар дэлхийн нийт хүн амын (7.91 тэрбум) 67.1% буюу 5.31 тэрбум хүн гар утас ашиглаж байгаа бөгөөд хэрэглэгчид интернетэд дунджаар 6 цаг 58 минут холбогдож буй нь өдөр тутам унтлагаас бусад цагийн 40 гаран хувийг эзэлж байна.[17] Нийт хэрэглэгчийн 92.1% нь гар утсаараа цахим сүлжээнд холбогддог.[18] Зөвхөн WhatsApp аппликейшны хэрэглэгчид гэхэд өдөрт 65 тэрбум текст мессеж цахимаар солилцож байна. Тус аппликейшн 1 тэрбум гаран хэрэглэгчийн бүлгийг холбодог бөгөөд тэдгээр нь 55 гаран сая дүрсээ харж ярих видео дуудлагыг өдөр тутамдаа ашиглаж буй.

Олон нийтийн цахим сүлжээнд идэвхтэй холбогдогчид 4.64 тэрбум болж дэлхийн хүн амын 58.4%-ийг хамрах болсон ба холбогдох дундаж хугацаа 2 цаг 27 минут (үүнээс 35.2% нь тогтмол онлайн) бөгөөд дэлхийд нийлбэр дүнгээрээ 4 триллон цагийг эл

[15] Мэдээллийн технологийн түүхэн хөгжлийг ерөнхийд нь механикийн өмнөх, механикийн, электромеханикийн, электроны гэсэн дөрвөн эринд хуваадаг. Хүмүүс ХТӨ 3 дахь мянганд бичиг үсэг зохион бүтээсэн цагаас эхлэн мэдээлэл дамжуулах технологийг эрчимтэй хөгжүүлж эхэлсэн (механикийн өмнөх үе) ба 15-19-р зуунд тооны машин зэрэг механик компьютерүүдийг (механикийн үе), 19-20-р зууны дунд үе хүртэл телеграф, морсийн код, телефон утас, радио зэргийг хөгжүүлжээ (электромеханикийн үе). 1940 онд Харвардын их сургуульд 5тонн жинтэй "Марк 1" анхны компьютерийг бүтээсэн нь мөн электромеханикийн үед хамаарна. Тоон системд суурилсан анхны компьютерүүд бүтээгдсэн үеэс электрон мэдээллийн буюу бидний амьдарч буй цаг үе хамаарах эрин эхэлсэн гэж үздэг.

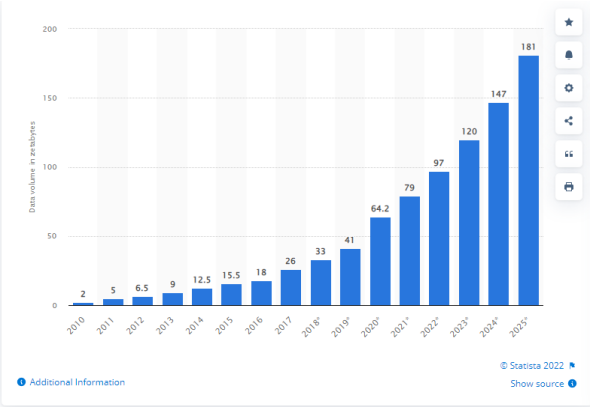
[16] https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

[17] Интернетэд холбогдоогүй хүн ам өмнөд Ази (1.075 сая), зүүн Ази (460 сая), зүүн Африк (341 сая) зэрэг бүс нутагт илүү олон байгаа нь интернет сүлжээний дэд бүтцэд холбогдсон байдал, цахилгаан эрчим хүчний хангамж зэрэгтэй хамааралтай аж (WAS, Hootsuite, Data portal. Digital 2022 Global Overview Report).

[18] WAS, Hootsuite, Data portal. Digital 2022 Global Overview Report

сүлжээнд зарцуулжээ. 13-аас дээш насны хүн амын 74.8% нь олон нийтийн цахим сүлжээ ашигладаг ба нийт интернэт хэрэглэгчдийн 93.4% нь мөн сүлжээнд холбогддог.

16-64 насныхны олон нийтийн цахим сүлжээнд Ватсапп (Whatsapp), Инстаграм (Instagram), Фейсбүүк (Facebook) хамгийн өндөр үнэлгээтэй байна.[19] Андройд үйлдлийн системийн хэрэглэгчид Youtube платформд сар тутам дунджаар 23.7 цаг холбогдсон бол Фейсбүүк системд 19.6 цаг холбогджээ. Эдгээр видео бичлэг их хэмжээгээр агуулдаг платформуудтай харьцуулахад Фейсбүүк мессенжер 3 цаг, Твиттер 5.1 цаг, Телеграм 3 цагийн хэрэглээний үзүүлэлттэй байна. Хэрэглэгчийн тоон статистикаар 2.910 сая (хоёр тэрбум есөн зуун арван сая) хэрэглэгчтэй фейсбүүк нэгдүгээрт, 2.562сая хэрэглэгчтэй youtube хоёрдугаарт эрэмбэлэгджээ.



Эдгээр нь бүгд хувийн мэдээлэл цуглуулах, мэдээлэл түгээх боломжтой хэрэглэгчийн үзүүлэлт болно. Зар сурталчилгааны хувьд ч эдгээр платформууд олон улсад тэргүүлж буй. Тухайлбал, инстаграмын зар сурталчилгаа хүргэх боломжит хэрэглэгчийн тоо 1.48 тэрбум (дэлхийн нийт хүн амын 18.7%, интернэт хэрэглэгчдийн 29.9%) хүрсэн нь өнгөрсөн оны эл үеэс даруй 21% хувиар өсжээ.[20] ТикТок платформын сурталчилгаа 18-аас дээш насны 884.9 сая хэрэглэгчид хүрэх боломжтой бол Линкедин (Linkedin) 808.4 сая, Youtube платформ 2.56 тэрбум хэрэглэгчид, сурталчилгаа, мэдээлэл хүргэх потенциалтай байна. Түүнчлэн, 2021 онд олон нийтийн цахим сүлжээний сурталчилгаанд 154 тэрбум ам. доллароор хэмжигдсэн нь нийт дижитал орчин дахь санхүүгийн зарцуулалтын 33.1%-ийг эзэлжээ.[21]

[19] Гар утасны аппликейшн татаж суулгасан тоогоор ТикТок, Инстаграм, Фейсбүүк тэргүүлж байна.

[20] Үүнээс стори хэсэг дэх сурталчилгаа 1.07 тэрбум, рийлс хэсэг дэх сурталчилгаа 675.3 сая.

[21] https://www.statista.com/studies-and-reports/digital-and-trends

Эдгээр үзүүлэлт дэлхий даяарх цахимжилтын ерөнхий төлөвийг илэрхийлж байна.

Б. Өгөгдлийн сангийн тэсрэлт

Дэлхий даяарх дижитал технологийн хэрэглээнээс улбаалан олон улс дахь өгөгдлийн[22] хэмжээ асар өргөжиж дэлхий дээрх мэдээллийн сан хүн төрөлхтний түүхэн дэх бүхий л мэдээллийн санг нийлүүлснээс ч олон дахин их болжээ. 2010 онд олон улсын өгөгдлийн сангийн хэмжээ 2 зетабайт буюу 2.000.000.000.000 гегабайтад[23] хүрчээ. Энэ хэрэглээ 2021 онд 79 зетабайт болж өссөн бол **2025 онд 181** зетабайтад хүрэх төлөвтэй байна.[24] 2010 – 2020 оны хооронд дэлхийн өгөгдлийн сан 5000%-иар өссөн үзүүлэлттэй гарчээ.[25]

Калифорнын их сургуулийн судлаач Доун Е.Холмс бүтээлдээ (2017) бүтэцчилэгдсэн[26], бүтэцчилэгдээгүй[27], хагас бүтэцчилэгдсэн[28] өгөгдлүүд минут тутамд асар ихээр нэмэгдэж байгааг "их өгөгдлийн тэсрэлт" гэж нэрлэжээ. Тэрээр "Анхандаа 'их өгөгдөл' гэдгээр шинээр үүсэж буй асар их өгөгдлүүдийг хэлж байлаа. Интернэт орчинд үүсэж буй бүтэцчилэгдсэн, бүтэцчилэгдээгүй, хагас бүтэцчилэгдсэн шуудан, цахим хуудас, нийгмийн сүлжээний сайтууд гэх мэт. Дэлхийн нийт өгөгдлийн 80 гаруй хувийг бүтэцчилэгдээгүй мэдээлэл эзэлдэг. Өнөөдөр харин их өгөгдөл гэдэгт цахим хэлбэрээр үүсгэж, хадгалж буй өгөгдлүүдээс гадна цар хэмжээ, нарийн байдлаараа асар өндөр түвшинд хүрсэн тодорхой өгөгдлийн багцуудыг хэлж байна" гээд хайлтын системийн, эрүүл мэндийн, шууд дамжуулалтын (real time), астрономын өгөгдлийг онцолсон байна.[29]

Олон тэрбум мэдрэгч, хүлээн авагч, дамжуулагч зэргээр тоноглогдсон төхөөрөмжид тулгуурласан цахим орчны хэрэглээ урьд нь цуглуулах, хадгалах боломжгүй байсан өгөгдлийг дижитал хэлбэрээр алдалгүй мөшгөх**, хадгалах боломжтой болсон** байна.

[22] Англи хэлний "дата" буюу "датум" гэх үгийн олон тоо. Латин хэлний өгөгдөл гэсэн үгнээс гаралтай. Анх 1648 онд Хэнри Хаммонд англи хэл дээрх шашны бүтээлдээ дурдсан (Оксфордын толь).

[23] Нэг гегабайтад 18.874 ворд файл, 2860 ppt файл, 230 бүрэн хэмжээний дуу багтана. 1гб бичгэн файлаар Дайн ба эрх романы 542 хувийг багтаах боломжтой.

[24] Statista.com

[25] Forbes.com

[26] Төрөлжүүлэн ангилсан, хүснэгтийн хэлбэрт оруулсан буюу шууд оруулах боломжтой цэгцтэй мэдээллийн цогц.

[27] Зураг, дүрс, их хэмжээний текст агуулсан файл зэрэг төрөлжүүлээгүй, ангилалд хамааруулахад хүндрэлтэй хэлбэрээр хадгалагдаж буй мэдээллүүд.

[28] Цахим шуудан зэрэг үндсэн гарчиг, толгой хэсэгтээ метадата агуулсан, дотроо бүтэцчилэгдээгүй мэдээлэл бүхий мэдээллийн төрөл. Бүтэцчиглэгдээгүй болон хагас бүтэцчилэгдсэн мэдээллийг төрөлжүүлэх, бүтэцчилэхийн тулд метадата шошго буюу tag ашиглах нь түгээмэл.

[29] Доун Е.Холмс. Их өгөгдөл. Непко хэвлэлийн газар. 2017, орч 2018 он.

Хүмүүс, аж ахуйн нэгж байгууллага, Засгийн газрууд, хамтарсан болон бие даасан судалгааны хүрээлэнгүүд өдөр тутамдаа асар их хэмжээний мэдээлэл үүсгэж буй нь дэлхий даяар өгөгдлийн сангийн тэсрэлт, тэлэлтийг үүсгэж буй гэж болно. Зөвхөн 2018 онд гэхэд (нийт өгөгдөл 33 зетабайт буюу 2022 оноос 3 дахин бага байсан) интернэт хэрэглэгчид нийлээд 2.8 сая жилийг онлайн төлөвт өнгөрүүлжээ. Уг хугацаанд мэдээлэл солилцох, үүсгэх, хадгалах ажиллагаа тогтмол хийгдэж буй. Ийм их хэмжээний өгөгдөл үндсэн гурван санд (өгөгдлийн сангийн цөм, ирмэг, төгсгөл)[30] хадгалагддаг. Шинжээчид дэлхийн өгөгдлийн сангийн тэлэлт ирээдүйд улам нэмэгдэх бөгөөд эргэж хумигдах, зогсох боломжгүй гэж үзжээ.[31] Өгөгдлийн сан үүсгэх, боловсруулалт хийх ажиллагааг түүхэнд их хэмжээний цахим өгөгдлийн сан үүсэхээс өмнө хэд хэдэн удаа үр дүнтэй гүйцэтгэж байсан тохиолдлууд тэмдэглэгдсэн байдаг.[32]

Орчин үед цугларсан, цаашид улам тэлэх их хэмжээний өгөгдлийг Засгийн газар, компаниуд боловсруулж үйл ажиллагаандаа өргөн хүрээнд ашигласнаар энэ салбарын эдийн засгийн ач холбогдол асар ихээр нэмэгдэж буй.[33] Энэ нь нөгөө талаас уг салбарт олон талын ашиг сонирхол (хүний эрхийн, улс төрийн, эдийн засгийн гэх мэт) зөрчилдөх үндэс болж байна. Товчлон дүгнэвэл, дээр тоймлосон үндсэн хоёр ойлголт (глобал цахимжилт, өгөгдлийн сангийн тэсрэлт) мэдээлэл, харилцааны технологийг аюулгүй байдалд нөлөөлөх хэмжээнд ашиглах боломж, эрсдэлийг бий болгосон объектив шалтгаан гэж үзэх үндэслэлтэй.

---

[30] (1) Өгөгдлийн сангийн цөм буюу “core”. Үүнд уламжлалт дата төвүүдээс гадна орчин үед үүлэн системийн сангууд хамаарна. Олон улсын өгөгдлийн корпорацийн тооцоолсноор 2025 он гэхэд дэлхийн нийт өгөгдлийн 49% нь үүлэн системийн санд суурилах аж. (2) Өгөгдлийн сангийн “ирмэг” буюу “edge” гэгдэх хувийн байгууллагуудын сан, дата төвийн салбарууд хамаарна. Мөн веб сайтуудын мэдээлэл агуулсан хувийн болон энэ төрлийн үйлчилгээ үзүүлэгч байгууллагуудын жижиг хэмжээний серверүүдийг энэ хэсэгт хамааруулж болно. (3) Өгөгдлийн сангийн “төгсгөл” буюу “endpoint” болох хувийн төхөөрөмж – компьютер, гар утас, ухаалаг цаг, хяналтын камерийн хард гэх мэт (David Reinsel, John Gantz, and John Rydning, “The Digitization of the World from Edge to Core,” Data Age 2025 (IDC White Paper, 2018)).

[31] David Reinsel, John Gantz, and John Rydning, “The Digitization of the World from Edge to Core,” Data Age 2025 (IDC White Paper, 2018).

[32] Тухайлбал 1854 онд Лондонд дэгдсэн тахалын үеэр өвчлөлийн мэдээллийг цуглуулан англий эмч Жон Сноу өвчний тархалтын газрын зураг үүсгэснээр хаана, аль эх үүсвэрт илүү өвчтөн халдвар авсан талаар шинжилгээ хийх боломж бүрджээ. Шинжилгээний үр дүнд өвчин агаараар биш, усаар тархсныг таамаглаж бөөгнөрөл бүхий худгийг хааснаар өвчлөлийг бууруулсан байна.

[33] Олон улсад их өгөгдлийн анализ хийх ажиллагааны санхүүгийн хэмжээ 2025 оны байдлаар 68.09 тэрбум америк доллар хүрэх төлөвтэй ба нийт их өгөгдлийн зах зээлийн хэмжээ 274.3 тэрбум америк доллар хүрэх төлөвтэй аж.

III. Хувийн халдашгүй байх эрхийн зөрчил ба үндэсний аюулгүй байдлын ашиг сонирхол

Глобал цахимжилт, өгөгдлийн сангийн тэсрэлтэд тулгуурлан хүний хувийн халдашгүй байх эрхийг уламжлалт бус хэлбэрээр (цахим технологи ашиглан) зөрчих явдал олон улсын хэмжээнд нэмэгдсэн. Үүнээс Засгийн газрын оролцоотой, эсвэл хувийн хэвшлийн байгууллага дангаар буюу Засгийн газар хувийн хэвшилтэй хамтран гүйцэтгэсэн, халдашгүй байдлын зөрчилд тооцох боломжтой хэд хэдэн ажиллагаа аливаа улсын аюулгүй байдалд хүчтэй нөлөөлөхүйц хэмээн үзэх үндэслэлтэй байна. Эдгээр ажиллагааг улсууд (1) дотогшоо чиглүүлэх буюу өөрсдийн иргэд, улс төрийн өрсөлдөгч, сэтгүүлчид зэргийн хувийн халдашгүй байдалд халдах хэлбэрээр; (2) гадагшаа чиглүүлэх буюу өөр улсын иргэд, нийгэмд чиглүүлж санаа бодлыг тандах, өөрчлөх хэлбэрээр зохион байгуулжээ.

Хувийн халдашгүй байдал нь зөрчигдсөн хүний ажил мэргэжил, тооноос шалтгаалан ач холбогдол бүхий нэг буюу цөөн тооны хүмүүст чиглэсэн, эсвэл олон нийтэд чиглэсэн хэмээн ангилж болохоор байна. Сэтгүүлч, улс төрч, дипломат албан хаагч зэрэг олон нийтийн санаа бодол, үндэсний аюулгүй байдалд нөлөө бүхий хүмүүсийг тухайлан цахимаар тагнах хэд хэдэн тохиолдол олон нийтэд ил болсон. Жишээ нь “Пегасус” тагнуулын программаар эрхэлж буй ажил, үзэл бодол, олон нийтэд нөлөөлөх чадвар зэргийн хувьд улс төрийн ач холбогдол бүхий 450 гаруй хүний[34] гар утсыг тагнасан нь тогтоогдсон байна.[35] 2018 онд Пегасус программыг хөгжүүлэгч компанийн эсрэг хоёр ч шүүхийн нэхэмжлэл гарсны нэг нь Омар Абдулазизаас Израйлын шүүхэд Вашингтон Постын нас барсан сэтгүүлч Жамал Хашоггийн

[34] Хохирогч хувь хүмүүс: Азербайжан (эрэн сурвалжлах сэтгүүлч Хадижа Исмаеилова, чөлөөт сэтгүүлч Севинк Вакифкизи нар 2019, 2020 онд), Бахрайн (активист Мүүса Абд-Али 2020 онд, блоггер Юсуф Аль-Жамри 2018 онд /Засгийн газрын дарамтаас шалтгаалан Англид орогнож буй/ бусад хүний эрхийн хамгаалагч нарын хамт), Эл Салвадор (Карлос Мартинез 35 сэтгүүлчийн хамт 2020-2021 онд, Даниел Лизаррага болон бусад), Финланд (дипломат алба хаагчид, тоо тодорхойгүй), Франц (Францын үндэсний радиод захирлын албанд нэр дэвшигч Брүно Делпорт, эрэн сурвалжлах сэтгүүлч Ленайг Бредү гэх мэт), Унгар (фото сэтгүүлч Даниел Немет, улс төрч Золтан Пава, Орбаны дэглэмийг эсэргүүцэгч Адриен Беаүдүйн гэх мэт) зэрэг 35 улсад тус программаар хувь хүмүүсийг тагнасан бөгөөд зарим нь сураггүй болох, аллагад өртөх зэргээр ноцтой хохирол учирсан байна.

[35] Иргэний лаборатор (Citizen lab), Болгоомжил (Lookout) зэрэг судалгааны байгууллагууд тус үйл ажиллагааг илрүүлэхэд идэвхитэй оролцож хүмүүсийн утсыг хакдсан эсэхийг тодорхойлж буй. Дэлгэрэнгүй эх сурвалж: https://www.haaretz.com/israel-news/tech-news/2022-04-05/ty-article-magazine/nso-pegasus-spyware-file-complete-list-of-individuals-targeted/0000017f-ed7a-d3be-ad7f-ff7b5a600000

хэрэгт[36] хөгжүүлэгч компани Сауди Арабын Засгийн газарт тагнуулын программ нийлүүлж оролцсон тухай байв.

Нөгөө талаас мэдээллийн технологийн потенциалыг олон нийтийг тагнах, сэтгэл зүйд нөлөөлөхөд өргөн хүрээгээр ашигласан тохиолдлууд бий. Үүнд, хүн тус бүрийн хувийн мэдээлэлд тулгуурлан олон нийтийн санаа бодлыг чиглүүлэх, улмаар улс төр, эдийн засгийн шийдвэрт нөлөөлсөн Кембридж Аналитика компанийн жишээг дурдаж болно. Тус байгууллага хэд хэдэн улсын сонгууль, олон улсын байгууллагад элсэх эсэх үндэсний санал асуулгад нөлөөлсөн ноцтой үйл ажиллагаанууд зохион байгуулж, оролцсон. Хувийн халдашгүй байдлыг ноцтой зөрчсөн ийм эмпирик фактууд уг зөрчлийг зөвхөн субьектив эрхийн хувьд бус аюулгүй байдлын бодлогод харгалзах шаардлагыг тодорхойлж байна.

А. Тохиолдол шинжлэл №1. Таван нүд

УКУСА-гийн нууц гэрээний[37] үндсэн дээр АНУ, Нэгдсэн Вант Улс, Австрали, Шинэ Зеланд, Канад зэрэг улсууд хүйтэн дайны үед ЗХУ, түүний төв болон зүүн Европ, зүүн болон зүүн өмнөд Ази дахь улсуудыг хянах, долгионы тагнуулын аргаар (SIGINT)[38] мэдээлэл

[36] Жамал Хашогги 2018 оны 10-р сарын 02-нд Истанбул хотод байрлах Сауду Арабын консулын газар бусдын гарт амь алдсан бөгөөд цөөнгүй эх сурвалжид угсаа залгамжлагч Мохаммед бин Салманы ашиг сонирхлын үүднээс түүнийг хөнөөсөн гэж буруутгажээ. (Kirkpatrick David D, Schmitt Eric, Barnes Julian E. (12 November 2018). "Tell your boss: Recording is seen to link Saudi crown prince more strongly to Khashoggi killing". The New York Times; "Jamal Khashoggi: An unauthorized Turkey source says journalist was murdered in Saudi consulate". BBC News. 7 October 2018; "Speakers". International Public Relations Association – Gulf Chapter (IPRA-GC). 2012.

[37] Долгионы тагнуулын ажиллагааны талаар Австрали, Шинэ Зеланд, Канадын дэмжлэг бүхий АНУ, Нэгдсэн Вант Улсын хооронд байгуулсан нууц гэрээ. 1941 оны Атлантын дүрэм (Atlantic charter)-ээс үүдэн 1943 онд байгуулсан Брусагийн хэлцэлд үндэслэсэн ба 1946 оны 03-р сарын 05-ны өдөр албан ёсоор үзэглэсэн. Дайны дараах дэлхийг хянах, ЗХУ-н харилцаа, мэдээллийг тагнах зорилгоор дурдсан улсууд, мөн гэрээний хувьд гуравдагч этгээд болох Швед, Өмнөд Солонгос, Натогийн гишүүн орнууд, Сингапур, Дани, Баруун Герман зэрэг улсууд уг гэрээний хэрэгжилтэнд хамтран ажилласан байна. (Эх сурвалж: Cox, James "Canada and the Five Eyes Intelligence Community"., December 2012; Canadian Defence and Foreign Affairs Institute, 5 February 2014; Gallagher, Ryan "How Secret Partners Expand NSA's Surveillance Dragnet" ., 2014; Norton-Taylor, Richard "Not so secret: deal at the heart of UK-US intelligence"., 2010; Gallagher, Ryan "How Secret Partners Expand NSA's Surveillance Dragnet" ., 2014;) Гэрээ 2005 он хүртэл олон нийтэд нууц хэвээр байсан бөгөөд 2010 оны 06-р сарын 25-нд АНУ болон НВУ-д олон нийтэд дэлгэгдсэн байна.

[38] Хүмүүсийн хоорондын харилцаанд хэрэглэж буй болон шууд бусаар хэрэглэгдэх электрон долгионыг замаас нь барьж мэдээлэл цуглуулах ажиллагаа. Зөвхөн мэдээлэл цуглуулах төдийгүй шифрлсэн мэдээллийг унших зэрэг цогц ажилбар уг агуулгад хамаарч болох бөгөөд харилцаа тагнах ажиллагаа (COMINT), харилцааны бус долгион татах тагнуулын ажиллагаа (ELINT) зэргийг багтаасан ойлголт.

цуглуулах зорилгоор байгуулагдсан тагнуулын хамтын байгууллага нь зөвхөн социалист улсуудын төдийгүй дэлхий нийтийн мэдээллийн сүлжээг хүйтэн дайнаас хойш ч хянаж байсныг "таван нүд" хэмээн нэрлэдэг. Олон нийтийг долгион тагнах ажиллагааны "Echelon" системийг ашиглан тагнадаг байсан ба гол зохион байгуулалтыг АНУ-н Үндэсний Аюулгүй Байдлын Агентлаг хариуцаж дурдсан бусад улсын холбогдох байгууллагууд хамтардаг байжээ. 1960 онд бүтээгдэж, 1971 онд албан ёсоор ажиллаж эхэлсэн ба 20-р зууны сүүлээр зөвхөн цэргийн болон дипломат зорилгоосоо хальж хүмүүсийн хувийн мэдээллийг нууцаар цуглуулдаг, хянадаг болсон аж. Энэ талаар тагнуулын ажилчид, эрэн сурвалжлах сэтгүүлчид хэд хэдэн байдлаар олон нийтэд ил болгон үзүүлсэн ч[39] тухайн үедээ олны анхаарлыг төдий л татаж чадаагүй байна. Харин 1999 оны 03-р сард Австралийн Засгийн газар УКУСА-гийн нууц гэрээний талаарх мэдээллүүд үнэн болохыг анх удаа хүлээн зөвшөөрчээ.

2013 оны 06-р сард АНУ-н УАБА-н гэрээт ажилтан Эдвард Снөүден (Edward Snowden) өндөр нууцлалтай хэд хэдэн мэдээллийг АНУ-н The Washington Post болон Английн The Guardian сонинуудад илчлэн нийтлүүлжээ. Олон нийтийн анхаарлыг ихээхэн татсан уг материалууд тарсны дараа дэлхийн олон улсуудын хэвлэлийн байгууллагууд уг мэдээллийн талаар мөн нийтэлсэн[40] бөгөөд үр дүнд нь УКУСА-н холбоотнуудын тагнуулын цөөнгүй мэдээлэл, хамтын ажиллагаа[41] олон нийтэд ил болжээ. Снөвденийг Засгийн газрын

[39] 1972 онд АНУ-н УАБА-н аналист Perry Fellwock "Ramparts" сэтгүүлд экелоны талаарх анх мэдэгдсэн;
1982 онд эрэн сурвалжлах сэтгүүлч James Bamford УАБА-н үйл ажиллагааны талаар The Puzzle Palace өгүүлэл нийтэлж, "SHAMROCK" нэрийн дор олон нийтийг чагнах нүсэр том ажиллагаа зохион байгуулдаг талаар мэдэгдсэн. Shamrock нь 1975 оны үед хэрэглэгдэж байсан экелоны халхавч нэр байжээ (Bamford, James "The Puzzle Palace: A Report on America's Most Secret Agency" 1982);
1988 онд Margaret Newsham УАБА-д гэрээгээр ажиллаж байх үедээ экелоны талаар конгрессын гишүүдэд мэдэгдэж, бүгд найрамдах улс төрийн баримтлал бүхий сенатор Strom Thurmond-г тагнаж байсан гэжээ;
1988 онд эрэн сурвалжлах сэтгүүлч Duncan Campbell "Хэн нэгэн чагнаж байна" өгүүлэлдээ (New Statesman сэтгүүлд) "Экелон" халхавч нэрийн дор долгионы тагнуулын ажиллагаа явуулж байгаа талаар бичиж, тухайн систем нь иргэдийн теле харилцааны долгионыг сансрын хиймэл дагуулын тусламжтай тагнадаг талаар тайлбарлажээ;
1996 онд Шинэ Зеландын сэтгүүлч Nicky Hager "Нууцлаг хүч: Олон улсын тагнуулын ажиллагаан дахь Шинэ Зеландын оролцоо" номдоо экелоны талаар илүү дэлгэрэнгүй авч үзсэн гэх мэт.

[40] The New York Times (АНУ), the Canadian Broadcasting Corporation (Канад), the Australian Broadcasting Corporation (Австрали), Der Spiegel (Герман), O Globo (Бразил), Le Monde (Франц), L'espresso (Итали), NRC Handelsblad (Недерланд), Dagbladet (Норвеги), El País (Испани), and Sveriges Television (Швед).

[41] Тухайлбал, Герман (BND), Швед (FRA), Австрали (ASD), Британ (GCHQ), Канад (CSE), Дани (PET), Франц (DGSE), Итали (AISE), Недерланд (AIVD), Норвеги

өмчийг хулгайлсан хэргээр ялласан ч тэрээр нууцаар дүрвэж 2013 онд ОХУ-д орогносноос хойш, одоог хүртэл тэнд оршин сууж байна. Тухайн мэдээллийн хэрэгслүүдийг (тухайлбал, Английн Guardian сонин) үндэсний аюулгүй байдлын шалтгаанаар, тэдгээр мэдээллийг цаашид нийтлэхийг хориглож, шахалт үзүүлж байсан ба Guardian-ы редактор Алан Рүсбриджер "Бид 58000 гаруй мэдээллээс ердөө 26-г л нийтэлсэн" хэмээжээ.[42] Ил болсон мэдээлэл нийт агуулгатайгаа харьцуулахад бага хэмжээтэй ч хувийн халдашгүй байх эрхийн ноцтой зөрчилд олон нийтийн анхаарлыг хандуулж, энэ эрхийн ач холбогдлыг үнэлэх шинэ өнцгийг бий болгосон гэж болно.

Европын парламентын тайланд Британийн "RAF Menwith Hill", Японы "Мисавагийн агаарын бааз" зэрэг 12 станцыг уг ажиллагаанд хамааралтай бөгөөд өөр 12 станцыг хамааралтай байх магадлал өндөртэй хэмээн тодорхойлсон.[43] Снөүдений материалд 16 станцын мэдээлэл байсан нь интернэтэд ил тавигдсан. Уг программыг зөвхөн аюулгүй байдалд заналхийлэх гаднын субьект бус дотоодын иргэдийг тагнах, нийгмийг бүхэлд нь хянахад өргөн хүрээгээр ашиглаж байсан нь тодорхой этгээдүүдийн явцуу ашиг сонирхлыг хамгаалах, үндэсний дотоод аюулгүй байдалд сөргөөр нөлөөлөх үр дагавартай байв.

Б. Тохиолдол шинжлэл №2. Кембриж Аналитика

2018 оны гуравдугаар сард Британид үйл ажиллагаа явуулдаг, улс төрийн зөвлөх үйлчилгээний Кэмбридж Аналитика компани Фэйсбүүк сошиал сүлжээний 87 сая хэрэглэгчийн хувийн мэдээллийг хууль бус аргаар цуглуулснаа цөөнгүй улс орнуудын сонгуулийн үйл ажиллагаанд ашиглаж байсан нь илэрсэн юм.[44] Тус компанийн

(NIS), Испани (CNI), Швейцар (NDB), Сингапур (SID), Израйл (ISNU) зэрэг улсуудын тагнуулын байгууллага АНУ-н ҮАБА (NSA)-тай мэдээлэл солилцсон байжээ. Эх сурвалж: Glenn Greenwald; Laura Poitras; Ewen MacAskill (2013). "NSA shares raw intelligence including Americans' data with Israel". The Guardian сонинд; Tim Leslie; Mark Corcoran (2013). "Explained: Australia's involvement with the NSA, the U.S. spy agency at heart of global scandal". Австралийн мэдээллийн корпораци; Greg Weston; Glenn Greenwald; Ryan Gallagher (2013). "Snowden document shows Canada set up spy posts for NSA". Канадын мэдээллийн корпораци; Jacques Follorou (2013). "La France, précieux partenaire de l'espionnage de la NSA". Le Monde; Kjetil Malkenes Hovland (2013). "Norway Monitored Phone Traffic and Shared Data With NSA". The Wall Street Journal-д; гэх мэт.

42 Снөвдений задалсан мэдээллээс ердөө 1%-ийг нь задалсан талаараа редакц нь 2013 онд BBC-д мэдээлжээ.

43 Тайлантай танилцах холбоос: https://web.archive.org/web/20140106052052/https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/eyes_wide_open_v1.pdf ; http://www.spiegel.de/international/world/snowden-documents-show-gchq-targeted-european-and-german-politicians-a-940135-2.html

44 SCL группын охин компанийн "Cambridge Analytica" гэх нэрээр танигдсан бизнесийн үйл ажиллагаа нь зөвхөн Cambridge Analytica бус, түүний толгой болон зэрэгцээ компаниудын хамааралтай ажиллагаа байсан бөгөөд шүүхэд хэргийн хариуцагчаар дараах компаниуд оролцсон юм:

бизнес хөгжлийн газрын захирал асан Бриттани Кайзерын дэлгэсэн баримтуудад авагдсанаар Кэмбридж Аналитика нь дэлхийн 65 улсын сонгуулийн үйл явцад ямар нэг хэмжээгээр оролцсон ажээ. Эдгээрт 2016 оны АНУ-н ерөнхийлөгчийн сонгууль, Британийн Европын холбооноос гарахтай холбоотой "БРЕКСИТ (BREXIT)" багтаж байгаа төдийгүй 2017 оны Монгол Улсын Ерөнхийлөгчийн сонгуульд тус байгууллагатай хамтарсан байж болзошгүй мэдээлэл дэлгэгдсэн.[45] Уг хэргийг (индекс: [2019] EWHC 954 (Ch)) Англи болон Вейлсийн дээд шүүх хянан шийдвэрлэж гэм бурууг тогтоосон байна.[46]

Дээд шүүхийн илтгэгч шүүгч Норрис хуралдааны эхэнд: "Кембридж Аналитика нэрээр олон нийтэд танигдсан групп компаниудын бизнесийн үйл ажиллагааг та бүхэн сонссон байх. Тус бизнес нь хэд хэдэн нийлүүлэгчдээсээ арилжааны шинжтэй өгөгдөл, тэдгээрийн анализ (Кембридж их сургуулийн эрдэмтдийн бүтээсэн моделд тулгуурлан "психологийн профайл" үүсгэж авсан)-ийг авч, тэрхүү анализад тулгуурлан өөрсдийн үйлчлүүлэгчдэд зориулан оновчлолтой сурталчилгаа ("микро-таргет" буюу бичил

- (1) SCL Group Limited;
- (2) SCL Analytics Limited;
- (3) SCL Commercial Limited;
- (4) SCL Social Limited;
- (5) SCL Elections Limited;
- (6) Cambridge Analytica (UK) Limited.

[45] Rosenberg, Matthew; Confessore, Nicholas; Cadwalladr, Carole (2018). "How Trump Consultants Exploited the Facebook Data of Millions". The New York Times; Lewis, Paul; Hilder, Paul (2018). "Leaked: Cambridge Analytica's blueprint for Trump victory". The Guardian; Р.Төмөр (2020) "Монгол Улсын ерөнхийлөгчийн сонгуульд Кэмбриж Аналитика компанийн үйлчилгээг ашигласан байж болзошгүйг мэдээлжээ" Ikon.mn сайт; Британи Кайзерийн дэлгэсэн дотоод мейлийн материалууд.

[46] Хэрэгт (индекс: [2019] EWHC 954 (Ch)) хамааралтай голлох үйл баримтуудаас:
- 2015 оны нэгдүгээр сард Cambridge Analytica (SCL USA) нэг гишүүнтэйгээр байгуулагдсан;
- 2018 оны 3 дугаар сард New York Times, The Observer хэвлэлийн сувгууд тус компанийг хэрэглэгчдийн хувийн мэдээлэлд халдсан талаар мэдэгдсэн байна. Мөн удалгүй Channel 4 News суваг компанийн ажилчдын дүрс бичлэгүүдийг ил болгосноос UK-н Мэдээллийн асуудал эрхэлсэн комисс (ICO) СА компанийн серверийг нэгжих зөвшөөрөл хүссэн;
- ФБ өөрсдийгөө мэхлэгдсэн хэмээн зарлаж, СА-г өөрийн платформ дээр сурталчилгаа явуулах эрхийг хаасан;
- 2018 оны 03-н сарын 23-нд Британы дээд шүүх ICO-д СА-н Лондон дахь оффисыг нэгжих зөвшөөрөл олгосон;
- This is your dijital life аппликейшнээр 87 сая фб хэрэглэгчдийн хувийн мэдээллийг цуглуулсныг мэдсэн ба апп хөгжүүлэгч нь датагаа СА-д өгснөөрөө фб-н үйлчилгээний нөхцөл, журмыг зөрчсөн;
- 2018 оны 03-р сарын 28-нд СА-н захирал асан Alexander Tayler шинээр байгуулагдсан Emerdata-н захирлаар томилогдсон;
- 2018 оны 05-р сарын 1-нд СА болон толгой компани нь төлбөрийн чадваргүйд тооцогдож үйл ажиллагаагаа зогсоосон.

нарийвчлал бүхий) явуулсан байна. Тухайн үйлчлүүлэгчдэд улс төрийн намууд багтаж буй бөгөөд Кембридж аналитика байгууллагын бүтээгдэхүүнийг сонгогчдын зан төлөвт нөлөөлөхийн тулд ашиглажээ.

Уг бизнесийн модель нь дата бааз үүсгэдэг ба тухайн бизнесийг эрхлэгчид өөрсдөө олон нийтэд: 'АНУ-н 230 сая сонгогч тус бүр дээр 5000 дата пойнт мэдээлэл цуглуулсан' хэмээн мэдэгдсэн. Шүүмжлэгчид тэдгээр өгөгдлийн (дата) 87 сая орчим хэрэглэгчид нь олон нийтийн цахим сүлжээний Фейсбүүк платформоос мэдээллээ алдсан хэмээн үзэж байна. Өмнөх сонсголд эл компани 700 терабайт мэдээлэл буюу 52 тэрбум хуудас бүхий өгөгдөл цуглуулсан гэх бөгөөд, үүнийгээ 2016 оны АНУ-н ерөнхийлөгчийн сонгуульд ашигласан байж болзошгүй ..." хэмээн илтгэсэн байна.[47]

Шүгэл үлээгч, Канадийн өгөгдлийн шинжээч Кристофер Уайлигийн хэлснээр "Улс төрийн ухуулгад хүн бүрт зориулж овжин урласан мессежүүдээс илүү үр нөлөөтэй зүйл хаа ч үгүй. Жишээ нь сонгуульд оролцохыг уриалсан мессежийг экстроверт демократ хүнд нэг өөрөөр мөн интроверт, тогтвортой сэтгэл зүйтэй демократ хүнд нэг өөрөөр зориулан хэлэх ёстой. Яг ижил мессежийг хооронд нь сольж илгээхэд эсрэг үр дүн гарч болзошгүй .... Ажлын байр нэмэгдүүлэхээр амлаж буй нэр дэвшигч хөдөлмөрч хүнтэй ярилцаж байгаа бол 'ажлын байр таны амжилтанд хүрэх боломжийг нэмэгдүүлэх тухай', хэрэв нээлттэй хүнтэй ярилцвал 'ажлын байр нэмэгдснээр таныг хувь хүн талаасаа хөгжих боломжоор хэрхэн хангах тухай', нейротик харилцагчтай бол 'ажлын байр нэмэгдснээр таны болон гэр бүлийн тань ирээдүйн тогтвортой байдлыг хангана' гэх мэтээр үгээ сонгох ёстой. ... Өнөөгийн өндөр технологи хүн бүрт тухайлсан өөр өөр мессежийг нэгэн зэрэг хүргэх боломжийг олгож буй."[48]

Энэ утгаараа мэдээллийн технологи олон сая хүнийг нэгэн зэрэг, асар богино хугацаанд нэг бүрчлэн ятгах, улмаар олон нийтийн шийдвэр гаргалтад хүчтэй нөлөөлөх боломжийг бүрдүүлсэн байна. Ялангуяа ардчилсан улс төрийн дэглэм, олон нийтийн санаа бодол улс төр, эдийн засаг, бусад томоохон үр дагавар бүхий шийдвэрт нөлөөлдөг нийгэмд уг үзэл бодол, шийдвэрийг тодорхой ашиг сонирхлын үүднээс чиглүүлэх боломж-эрсдэл нь аюулгүй байдлын хувьд уламжлалт бус сорилт мөн гэж үзэх үндэслэлтэй.

В. Тохиолдол шинжлэл №3. Пегасус

Израйлын кибер зэвсэг хөгжүүлэгч NSO групп анх 2011 онд андройд болон ios үйлдлийн систем бүхий гар утас тагнах чадвартай программ зохион бүтээсэн байна. Пегасус буюу эртний Грекийн

[47] [2019] EWHC 954 (Ch)

[48] Wylie Christopher (2019). "How I Helped Hack Democracy". Intelligencer.

домогт өгүүлэгдэх нисдэг морины нэрээр нэрлэсэн нь агаараар дамжих боломжтой "Троё морь"[49] буюу утасгүй сүлжээгээр хүмүүсийн утсанд байрших боломжтой вирус гэсэн утгийг илэрхийлдэг аж.[50] Программын лицензийг тус компани Узбекстан, Казакстан, Колумб, Тринидад, Тобаго, Уганда, Панам, Мексик зэрэг цөөнгүй улсын Засгийн газруудад худалджээ.[51]

Тус программ гар утсан дээр текст мессеж унших, дуудлага дамжуулах, нууц үгсийг хадгалж авах, байршил тогтоох, утасны дуу болон дүрс дамжуулагч эд ангиудыг ашиглах (камер, микрофон нээх), хэрэглэж буй аппликейшнүүдээс *(WhatsApp, Facebook, Messenger гэх мэт) мэдээлэл татах боломжтой байна.*[52] Эмнэсти олон улсын байгууллагын мэдээлснээр уг программ одоо ч сэтгүүлч, улс төрч, хүний эрхийн активист зэрэг ач холбогдолтой субъектүүдийг тагнах зориулалтаар цөөнгүй улсуудад ашиглагдсаар байгаа аж.[53]

Пегасус программын сүүлийн хувилбарууд утсанд байрших, мэдээлэл цуглуулах арга зүйн хувьд хүний бүтээсэн хамгийн ухаалаг цахим вируст тооцогдож байна. Тус вирус "zero click" буюу "тэг даралт"-ын аргаар хэрэглэгчээс ямар нэгэн үйлдэл шаардахгүйгээр төхөөрөмжид байрших чадвартай. Өөрөөр хэлбэл хэрэглэгчийн тусламжгүйгээр буюу холбоосоор дамжих, товших, компьютерийн гарны товчлуур хийгээд хулганы товч дарах огт шаардлагагүйгээр төхөөрөмжид нэвтрэх[54] чадвартай (жишээ нь үл таних дугаараас залгасан дуудлагыг хэрэглэгч аваагүй байсан ч дуудлага хийх төдийгөөр гар утсанд байрших) бөгөөд ийм халдлагыг "forcedentry" буюу "хүч хэрэглэн нэвтрэх" арга зүй хэмээн нэрлэж болдог.

2016 онд Арабын хүний эрх хамгаалагч Ахмед Мансүүр Арабын

---

[49] Грекчүүд Троё хотыг эзлэхэд ашигласан хөндий модон морийг илэрхийлжээ. Дотор нь цэргүүд байршуулсан том хэмжээний морийг Троёчууд бэлэг гэж андууран хотдоо оруулснаар хамгаалалтын гол давуу тал болох том хэмжээний хана хэрмэн дотроо дайсныг нэвтрүүлсэн нь дайнд ялагдах гол үндэслэл болсон байдаг.

[50] Bouquet, Jonathan (May 19, 2019). "May I have a word about… Pegasus spyware". The Guardian. Archived from the original on January 26, 2021. Retrieved July 18, 2021.

[51] Kirchgaessner, Stephanie; Lewis, Paul; Pegg, David, Cutler, Sam, Lakhani, Nina and Safi, Michael (2021). Revealed: Leak uncovers global abuse of cyber – surveillance weapon; Boot, Max (December 5, 2018). "An Israeli tech firm is selling spy software to dictators, betraying the country's ideals". The Washington Post.

[52] Bergman, Ronen; Mazzetti, Mark (January 28, 2022). "The Battle for the World's Most Powerful Cyberweapon". The New York Times. ISSN 0362-4331; Cox, Joseph (May 12, 2020). "NSO Group Pitched Phone Hacking Tech to American Police". Vice ба бусад өргөн хүрээний эх сурвалжид дурдагдсан байна.

[53] "Forensic Methodology Report: How to catch NSO Group's Pegasus". www.amnesty.org. July 18, 2021.

[54] Тэг даралтын талаар дэлгэрэнгүйг: "Sneaky Zero-Click Attacks Are a Hidden Menace". Wired. ISSN 1059-1028.

Нэгдсэн Эмират улсын хорих ангиудад хүний эрхийг ноцтой зөрчих, хоригдлуудыг тамлан зовоох ажиллагааны талаарх нууц мэдээллийг агуулсан гэх сэжиг бүхий линкийг хүлээн авснаа Торонтогийн их сургуулийн "Иргэний лаб" судалгааны хүрээлэнд илгээснээр анх Пегасусын талаарх дорвитой судалгаа хийгдсэн байна. Энэхүү тохиолдлоос тус программ хэрэглэгчийн хувийн мэдээллийг цуглуулж, боловсруулсны үндсэн дээр ашиглагддаг гэдгийг илрүүлсэн. Ахмед Мансүүрийн хувьд, хорих анги дахь эрүүдэн шүүлтийн талаар түүнд нууц мэдээлэл илгээсэн нь түүний хүний эрх хамгаалах, эрүүдэн шүүлттэй холбоотой ажиллагаа эрхэлж буйг мэдсэний үндсэн дээр хийгдсэн ажиллагаа аж. Программыг гар утсанд нь суулгахын тулд эхлээд тодорхой холбоос мессежээр илгээх ба уг холбоосыг вирус биш, үнэн бодитой хэмээн хүлээн авагчид итгүүлэхийн тулд линктэй хамт илгээх тайлбарыг нь хүний хувийн мэдээлэлд тулгуурлан боловсруулдаг байжээ.

Citizen Lab, Lookout байгууллагуудын судлаачид Ахмед Мансүүрт ирсэн холбоосоор дамжин гар утсанд нь суух программын код NSO группын "Пегасус" нэртэй программын кодтой тун төстэй байгааг олж тогтоосон байна. 2016 оноос Пегасусыг судалсан тус байгууллага Ахмед Мансүүрийн илгээсэн линкийн дагуу шинжилгээ хийгээд 149 сервертэй холбогдсоныг тогтоож, лавшруулан судлаад *NSO групп 500 гаран* кибер аюулгүй байдлын экспертүүдтэй бөгөөд гол бүтээгдэхүүн нь пегасус болохыг тогтоосон байна. Аль Жезийрагийн сурвалжилгад мэдээлснээр тус компанийн ихэнх экспертүүд Израйзлын армийн "8200-р нэгж" буюу кибер аюулгүй байдлын элит хүчний гишүүд байдаг бөгөөд Израйлын хууль тогтоомжийн дагуу ийм төрлийн компани батлан хамгаалах яамны хяналт дор үйл ажиллагаа явуулах ёстой ба тус программ кибер зэвсэгт тооцогддог учир гаднын Засгийн газар, байгууллагуудад худалдахын тулд яамнаас зөвшөөрөл авсан байх шаардлагатай.

Форензик Архитектур байгууллагын судлаач Шүри Молави "Пегасус дэлхийд активистуудын эсрэг кибер дайны шинэ талбарыг бэлдэж байна" гэж дүгнэсэн нь[55] үндэслэлтэй. Тус программ дор хаяж дэлхийн 45 улсад хэрэглэгдсэн бөгөөд хүний цахим төхөөрөмжийг бүрэн хянана гэдэг нь түүний өдөр тутмын амьдрал, итгэл үнэмшил, ирээдүйн төлөвлөгөө, үйл ажиллагааны хэтийн төлөв зэргийг бүрэн хянах боломж мөн. Энэ утгаараа хүний хувийн халдашгүй байх эрхийг ноцтой зөрчиж, цаашлаад үндэсний аюулгүй байдалд заналхийлэл учруулах болсон байна. Тиймээс, тухайлбал АНУ тус улсын "гадаад бодлого, үндэсний аюулгүй байдалд харш" гэсэн үндэслэлээр "хар жагсаалт"-ад оруулжээ.

[55] Vice news. The World's Most Terrifying Spyware | Investigators. 2021.

NSO групп кибер зэвсэглэлийн үйлдвэр, худалдаанд тэргүүлэх байр суурьтай байгаа боловч тэдэнтэй өрсөлдөхүйц хэд хэдэн байгууллага (Италийн "Хакийн баг", Английн Гамма Интернешнл гэх мэт) бий. Эдгээрээс гадна ч, цөөнгүй тагнуулын программ олон нийтэд ил болоод буй.[56] Хакийн баг компани Судан, Бахрайн, Саудийн Араб зэрэг дарангуй дэглэмтэй улсуудад программ нийлүүлсэн нь тогтоогдсон[57] бөгөөд тус компанийн 400 гб мэдээллийг үл мэдэгдэх этгээд олон нийтэд ил болсны дунд Монгол улсыг оролцуулаад нийт 36 улс эл байгууллагын бүтээгдэхүүнийг ашиглаж байгаа талаар мэдээлсэн[58] байна.

Монгол улс "Ac Mongolia" нэрээр 2013-2014 онд тус программыг худалдан авсан ба 799.000 еврогийн үнэ төлсөн, тогтмол хяналт, сайжруулалтын хөлс 100.000 евро төлсөн талаар 2015 онд Хакийн багаас алдагдсан мэдээлэлд дурджээ. Тодруулбал Викиликсд байршуулсан мэдээллээс үзэхэд Монгол Улсаас mmaagaa@yahoo.com, Batbayar Bayarkhuu - Б.Батбаяр (bbayar9199@gmail.com), Tamir Tumurbaatar (tamir_t@iaac.mn)[59], А.Өлзийбаатар - Ulziibadrakh A (ulziibadrakh@iaac.mn) зэрэг нэр, хаягаар d.maglietta@hackingteam.com, rsales@hackingteam.com зэрэг хаягтай олон удаа цахим шуудан, скайп платформоор холбогдсоноос гадна тус байгууллагын төлөөлөгчид Монгол Улсад ирсэн байж болзошгүй[60] талаар агуулга тусгагдсан байна. Тэгэхээр, хүний хувийн мэдээлэлд тулгуурлан хувийн шийдвэрийг удирдах, улмаар улс орон, олон нийтэд чухал хамааралтай үйл явдлуудад нөлөөлөх нь зөвхөн аль нэг улсад төдийгүй олон улсын дэг журамд ч ач холбогдолтой (тухайлбал, Англи Европын холбооноос гарах эсэх олон нийтийн сонгуульд нөлөөлөх) аж. Энэ талаар улс орнууд хэдийн анхааралдаа авч, үндэсний болон олон улсын шинжтэй эрх зүйн зохицуулалтад хувийн халдашгүй байх эрх ба аюулгүй байдлын хамаарлыг харгалзсан агуулгатай хэм хэмжээ тогтоох болжээ.

[56] Европын парламентын тайланд (2022 оны 5 сар) дурдсан программууд: Pegasus-NSO group, Cobwebs Technologies, Cognyte, Black Cube, Blue Hawk CI, BellTroX, Cytrox107, Predator, Candiru, Reign / QuaDream, Paragon; Dark Basin, Circles system, SS7 attack, Cobalt Strike, FinSpy, NetWire, P6 intercept, Galileo, PC 360, Karma, Epeius, StealthAgent, Crimson, Invisible Man, Unlimited Interception System, Skylock, Windshield, Phoreal, Soundbite, OceanLotus tester, Ocean Lotus encryptor, Ocean Lotus Cloudrunner, Ocean Lotus MAC, Komprogo.

[57] https://web.archive.org/web/20190419191315/https://www.ibtimes.co.uk/hacking-team-hacked-spy-tools-sold-oppressive-regimes-sudan-bahrain-kazakhstan-1509460

[58] https://web.archive.org/web/20190419191315/https://www.ibtimes.co.uk/hacking-team-hacked-spy-tools-sold-oppressive-regimes-sudan-bahrain-kazakhstan-1509460

[59] @iaac.mn нь Авлигатай тэмцэх газрын хаяг бүхий цахим шуудан.

[60] 2014 оны 03 сарын 24-нд Улаанбаатар хотод ирэх ба Blue sky барилгад байрших, мөн оны 4-р сарын 2 дахь долоо хоногт Монгол Улсад ирж уулзах зэрэг мэдээлэл солилцсон байна.

IV. Хувийн халдашгүй байдал ба аюулгүй байдлын эрх зүйн бодлого

Хувийн мэдээлэл, шийдвэрт тулгуурлан үндэсний аюулгүй байдалд сөргөөр нөлөөлж болох талаар улсууд үндэсний аюулгүй байдлын стратеги, үзэл баримтлалын баримт бичгүүддээ тусгасан байна. ОХУ 2021 онд баталсан Үндэсний аюулгүй байдлын стратегид мэдээллийн аюулгүй байдлыг онцлон анхаарсан ба мэдээллийн орчинд "худал мэдээлэл" тараах хийгээд бусад "зохион байгуулалттай мэдээллийн ажиллагаа" тус улсын соёлын тусгаар байдалд сөргөөр нөлөөлж буй талаар; мэдээлэл харилцааны технологид тулгуурлан тус улсын дотоод аюулгүй байдалд нөлөөлөх оролдлого нь тусгаар тогтнол, хил хязгаарыг бүхэллэг байдлыг зөрчихийн зэрэгцээ олон улсын энх тайван аюулгүй байдалд заналхийлж байгааг дурджээ.[61] Нөгөө талаас АНУ-ын Ерөнхийлөгчийн захиргаанаас 2022 оны 10-р сард гаргасан Үндэсний аюулгүй байдлын стратегид мөн "Бид өөрсдийн ардчилалд заналхийлэх ... зохион байгуулалттай мэдээллийн ажиллагаа ... зэргийн эсрэг зогсох болно" гэжээ.[62]

БНХАУ мөн "мэдээллийн удирдлага"-ыг орчин үеийн аюулгүй байдлын стратегийн гол хүчин зүйл хэмээн тодотгож байна.[63] Эдгээр бодлогын шинжтэй үзэл баримтлалууд ердийн хуулиудад тусгалаа олж хүний хувийн мэдээллийн талаар улсууд *гадаад улсаас мэдээлэл цуглуулах ба өөрийн дотоод дахь иргэдийн мэдээллийг гадагш алдахгүй байх* хоёр зорилго бүхий хууль тогтоомжийг баталж буй. АНУ 2018 онд "Далайн чанад дахь өгөгдлийн талаарх актыг хэрэглэх тодруулга (Clarifying Lawful Overseas Use of Data Act - CLOUD Act (H.R. 4943))" баталснаар 1986 онд баталсан "Хураагдсан харилцааны мэдээллийн акт (Stored communications act)"-ын үйлчлэлийг улам өргөтгөжээ. Энэ нь хувийн мэдээлэл хамгаалалт дахь аюулгүй байдлын ашиг сонирхлыг эрх зүйн хувьд зөрчилд хүргэсэн үйл явдал болов. 1986 оны өмнөх хуулиар сервер, дата төв зэрэгт хадгалагдаж буй цахим мэдээллийг эрх бүхий байгууллага (Холбооны мөрдөх товчоо - FBI) шалгах буюу хүний хувийн мэдээлэлтэй танилцах эрхийн талаар зохицуулсан.

[61] §49 зүйл.

[62] Biden-Harris Administration's National Security Strategy. Strengthening Our Democracy.

[63] Дэлгэрэнгүйг: Katja Drinhausen, Helena Legarda. "COMPREHENSIVE NATIONAL SECURITY" UNLEASHED. How Xi's approach shapes China's policies at home and abroad. 2022; Cheung, Tai Ming (2022). Innovate to Dominate, The Rise of the Chinese Techno-Security State. Cornell University Press; Li, Yan (2022). "China builds legal Great Wall to safeguard national security: official". April 25; David M. Lampton (2015). Xi Jinping and the National Security Commission: policy coordination and political power, Journal of Contemporary China, 24:95, 759-777; Wuthnow, Joel (2022). "Transforming China's National Security Architecture in the Xi Era".

Харин 2018 оны хуулиар өмнөх хуулийн зохицуулалтыг тодотгож ***АНУ-аас гадна буюу хилийн чанадад байгаа хувийн мэдээлэл агуулсан санд гүйцэтгэх эрх мэдлийн байгууллага нэвтрэх боломжтой*** болгожээ.[64] Өөрөөр хэлбэл АНУ-ын компаниуд гадаад улс дахь мэдээллийн сандаа шаардлагатай зөвшөөрлийн үндсэн дээр төрийн байгууллагын алба хаагчдыг нэвтрүүлэх боломжтой болсон юм. Мета (facebook, instagramm, whatsapp гэх мэт), Алфабет (google, youtube гэх мэт) зэрэг мэдээллийн технологийн корпорациудын толгой компани АНУ-д байрладаг боловч мэдээлэл хадгалдаг томоохон сервер, салбарууд гадаад улсуудад тухайлбал Ирландад өргөн хүрээгээр байршдаг. Энэ утгаараа тус улсын эрх бүхий байгууллага, албан хаагчид гадаад улсын иргэдийн хувийн мэдээлэлтэй танилцах эрхтэй болжээ. Үүнд Америк компанийн бүтээсэн гар утас, компьютер зэргийг ашиглаж буй Монголын хэрэглэгчид ч хамаарна.

2018 оны актаар мөн тус улсын Засгийн газарт бусад улстай иргэний хувийн мэдээлэл солилцох тухай хоёр талын гэрээ байгуулах бүрэн эрхийг олгосон байна. Энэ нь тус улс өөрийн нутаг дэвсгэрт байрлах серверүүдээс гадаад улсын иргэдийн мэдээллийг Засгийн газарт нь шилжүүлж өгөх, өөрсдөө мөн бусад улсаас ийм мэдээлэл авах боломжтой гэсэн үг. Энэ талаар хүний эрхийг хамгаалах хэд хэдэн байгууллага эсэргүүцэж “иргэдэд мэдэгдэлгүй, шүүхийн хяналтгүйгээр хүний хувийн мэдээлэл харилцан солилцох эрхийг Засгийн газарт олгосон нь нэг талаас Үндсэн хуулиар тогтоосон хувийн халдашгүй байх эрхийн зөрчил болох[65] ба нөгөө талаас хүний эрхийн үнэлэмж багатай улсуудад тус мэдээллийг буруу зорилгоор ашиглах боломжтой”[66] талаар анхааруулжээ. Гэвч мэдээж уг зохицуулалтын үндсэн зорилго нь хүний эрхийг хамгаалахад бус аюулгүй байдлаа хангахад шаардлагатай мэдээллийг өргөн хүрээгээр татаж авах боломжийг нэмэгдүүлэхэд оршиж буй. БНХАУ шинээр “Өгөгдлийн аюулгүй байдлын тухай”, “Хувийн мэдээлэл хамгаалах тухай” хуулиудыг баталж 2021 оны 11 сарын 1-ээс хүчин төгөлдөр үйлчилж эхэлсэн. Тус хуулиар 2017 онд баталсан “Цахим аюулгүй байдлын тухай” хуулиар тогтоосон эрх зүйн харилцааг илүү тодруулж, нарийвчилжээ. Энэхүү шинэ зохицуулалтаар мөн Хятад

[64] АНУ-ын Холбооны мөрдөх товчоо Микрософт группээс Ирланд улс дахь серверээс хүний хувийн мэдээлэл гаргуулж авах эрхтэй эсэх талаар шүүхийн маргаан өрнөсөн ч Дээд шүүхэд хэргийг хянах явцад Конгресс тус хуулийг (2018 оны) баталж маргааныг эцэслэжээ.

[65] Mak, Aaron (March 22, 2018). “Congress Put the CLOUD Act in Its Spending Bill. What Does That Mean For Data Privacy?”. Slate; Brandom, Russell; Lecher, Colin (March 22, 2018). “House passes controversial legislation giving the US more access to overseas data”. The Verge.

[66] Watters, Jackie (March 31, 2018). “Microsoft email privacy case no longer needed, DOJ says”. CNN.

улсын газар нутгаас гадна, аюулгүй байдлын ач холбогдолтой гэж үзсэн тохиолдолд бусад улс дахь мэдээлэл хадгалах, солилцох зэрэг харилцаанд үйлчлэх боломжтойгоор зохицуулсан[67] байна. Энэ утгаараа тус хуулийг АНУ-ын 2018 оны хуулиар тогтоосон эрх хэмжээний эсрэг арга хэмжээнд тооцож болно. Өөрөөр хэлбэл хилийн чанадад Хятадын иргэний мэдээллийг цуглуулахын эсрэг экстратерриториал (улсын газар нутгаас гадна үйлчлэх) зохицуулалт юм. Мөн өгөгдлийн аюулгүй байдлын тухай хуулиар Хятадын эрх бүхий этгээдийн зөвшөөрөлгүйгээр Хятад улсад цуглуулсан өгөгдлийг гадаад улсад шилжүүлэн өгөхийг хориглосон байна. Ялангуяа ач холбогдол өндөртэй мэдээллийг далайн чанадад шилжүүлэх этгээд нь Хятадын цахим орчны захиргаанаас аюулгүй байдлын үнэлгээ хийлгэсэн байхыг шаардана.

Хятад улсын үндэсний аюулгүй байдлын зохицуулалтаар улс төрийн нам, төрийн байгууллага, зэвсэгт хүчнээс гадна бүх бизнесийн болон хувийн хэвшлийн бусад байгууллага, иргэд нь үндэсний аюулгүй байдлаа хангаж, хамгаалах үүрэгтэй. Энэ утгаараа АНУ-ын 2018 оны дурдсан хуулийн адилаар Хятадын технологийн байгууллагуудад шаардлагатай бол төрийн эрх бүхийн этгээдэд өөрсдийн хэрэглэгчдийн хувийн мэдээллийг гаргаж өгөх үүргийг хүлээлгэж буй (технологийн салбар дахь өрсөлдөх чадвараас нь үзвэл эл улс зөвхөн иргэдийнхээ мэдээллийг хамгаалаад зогсохгүй гадаад орчноос хувийн мэдээлэл цуглуулах довтолгооны шинжтэй ажиллагаанд оролцох өндөр потенциалтай[68]). Иймэрхүү хэлбэрээр улс орнууд хувийн мэдээлэл, түүнд тулгуурласан хувийн шийдвэр – олон нийтийн санаа бодолд нөлөөлөх боломжтой талбаруудын үндэсний аюулгүй байдлын ач холбогдлыг хүлээн зөвшөөрч, хувийн халдашгүй байх эрхийг хууль тогтоомжоор хамгаалах арга хэмжээ авч буй. Нэг талаас бусад улсаас мэдээлэл цуглуулах, нөгөө талаас дотоодын мэдээллээ хамгаалах буюу бусад нийгмийн үзэл хандлага,

[67] Өгөгдлийн аюулгүй байдлын тухай хуулийн §2-т "... БНХАУ-ын нутаг дэвсгэрээс гаднах өгөгдлийн процесс үндэсний аюулгүй байдал, олон нийтийн ашиг сонирхол, тус улсын иргэн ба хуулийн этгээдийн хууль ёсны эрхэд харшилсан тохиолдолд хуулийн дагуу мөрдөн шалгах, хариуцлага хүлээлгэнэ" гэсэн байна.

[68] Хятадын дотоод олон нийтийн үзэл хандлагын хяналтын системийн судлаач Mareike Ohlberg (German Marshall Fund senior) "Зөвхөн дотооддоо цуглуулсан мэдээллийн асар их тоо, хэмжээг харахад, Хятадууд уг системээ гадаад улсуудруу чиглүүлсэн нь аймшигтай явдал мөн. ... Энэ нь тэдний (Хятадын) хувьд далай дамнасан олон нийтийн үзэл бодлын дайнд тулалцаж, улсаа хамгаалах нь өөрсдийнх нь үүрэг хэмээн итгэж байгааг харуулж байна" гэжээ. 2020 оноос хойш БНХАУ 300 гаруй Засгийн газрын хөтөлбөрөөр төрөл бүрийн эх сурвалжаас (тухайлбал олон нийтийн цахим сүлжээ) мэдээлэл цуглуулах өндөр үнэтэй программууд худалдан авсан байна. Дэлгэрэнгүйг: Cate Cadell. "China harvests masses of data on western targets –documents show" Washington post. 2021.

шийдвэрт нөлөөлөх, иргэдийнхээ үнэмшил, сэтгэл зүйг хамгаалах, шийдвэрийн талбарт хөндлөнгийн нөлөөнд автахаас хамгаалах арга хэмжээг эрх зүйн бодлогод тусган хэрэгжүүлж буй. ОХУ, АНУ, БНХАУ-аас гадна Европ, Африк, Ойрх дорнодын[69] улсууд энэ талбарт онцгойлон анхаарал хандуулж байна.

V. Дүгнэлт

Цахим эринд хүний хувийн халдашгүй байх эрхийн хамгаалалт (ялангуяа хувийн мэдээлэл, шийдвэрийн талбарт) ба үндэсний аюулгүй байдлыг хангах ажиллагаа хоорондоо нягт уялдаа, хамааралтай байна. Глобал цахимжилт, өгөгдлийн сангийн тэсрэлтийн улмаас хувийн халдашгүй байх эрхийн зөрчил нь зөвхөн субьектив асуудал биш, коллектив (нийлбэр) утгаараа үндэсний аюулгүй байдалд сорилт учруулах болсныг улс орнууд аюулгүй байдлын ба эрх зүйн бодлогодоо харгалзжээ.

Манай улсын хувьд ч Хүний хувийн мэдээллийг хамгаалах тухай, Кибер аюулгүй байдлын тухай зэрэг мэдээллийн орчныг зохицуулсан хууль тогтоомжийг батлан хэрэгжүүлж байна. Гадаад улсуудын туршлага, шинжилсэн тохиолдлуудаас үзэхэд хүний хувийн халдашгүй байх эрх, тэр дундаа хувийн мэдээллийг хамгаалсан хууль тогтоомжийг тухайлан баталж хэрэгжүүлэх нь энэ эрхийг хамгаалахад илүү оновчтой бөгөөд үүгээр дамжуулан аюулгүй байдлаа бататгах эрх зүйн баталгаа болдог байна. Тухайлбал АНУ зэрэг зарим улсад тухайлсан хуулийг батлаагүйгээс зөвхөн нэрлэж зохицуулсан зарим салбарт (хүүхэд хамгаалал, боловсрол, эрүүл мэнд гэх мэт) хувийн мэдээлэл хамгаалагдаж, эрх зүйн тогтолцооны бусад хэсэгт хамгаалалтгүй сул орон зай их үлддэг. Улмаар тухайлбал, олон нийтийн цахим сүлжээн дэх хүний хувийн мэдээллийн эрх зүйн хамгаалалт Европын холбоотой харьцуулахад сул гэж дүгнэж болно.

Тиймээс хувийн халдашгүй байх эрхийг хамгаалах тухайлсан хууль тогтоомжийг баталж хэрэгжүүлэх нь хүний эрхийг хамгаалахын сацуу үндэсний аюулгүй байдлыг хангахад илүү ач холбогдолтой. Өөрөөр хэлбэл аюулгүй байдлын нэрийдлээр Засгийн газар иргэдийнхээ хувийн халдашгүй байдлыг зүй бусаар зөрчих аливаа нөхцөлөөс зайлсхийх, кибер орчны аюулгүй байдлыг техник, стандартын хувьд дээд зэргээр хангах, хэрэглэгчийн ба сонгогчдын хувийн мэдээллийг их хэмжээгээр төвлөрүүлэх технологиос сэргийлэх, мэдээллийн хэрэглээнд хяналт тавих зэрэг арга хэмжээг тогтмол сайжруулж байх нь шаардлагатай байна.

[69] Израйл, Арабын Нэгдсэн Эмират Улс, Киргизстан, Казакстан, гэх мэт.

[Ном зүй]

М.Хатанзориг. Хувийн халдашгүй байх эрхийн агуулгыг харилцан хүлцлийн үзэл баримтлалаар тодорхойлох нь. Хууль зүйн докторын судалгааны ажил. Уб., 2023

М.Хатанзориг. Хүний дангаарших эрхийн талаарх Америкийн нэгдсэн улсын Дээд шүүхийн голлох шийдвэр, түүний зарим үр дагавар №1: Катзын маргаан. Хүний эрх сэтгүүл, 2021/1 дугаар

М.Хатанзориг. Хүний дангаарших эрхийн талаарх Америкийн нэгдсэн улсын Дээд шүүхийн голлох шийдвэр, түүний зарим үр дагавар №2: Грисволдын маргаан. Шихихутуг сэтгүүл 2021/тусгай дугаар

Mak, Aaron (March 22, 2018). "Congress Put the CLOUD Act in Its Spending Bill. What Does That Mean For Data Privacy?". Slate; Brandom, Russell; Lecher, Colin (March 22, 2018). "House passes controversial legislation giving the US more access to overseas data". The Verge.

Watters, Jackie (March 31, 2018). "Microsoft email privacy case no longer needed, DOJ says". CNN.

Cate Cadell. "China harvests masses of data on western targets –documents show" Washington post. 2021.

Katja Drinhausen, Helena Legarda. "COMPREHENSIVE NATIONAL SECURITY" UNLEASHED. How Xi's approach shapes China's policies at home and abroad. 2022

Biden-Harris Administration's National Security Strategy. Strengthening Our Democracy.

Vice news. The World's Most Terrifying Spyware Investigators. 2021.

"Sneaky Zero-Click Attacks Are a Hidden Menace". Wired. ISSN 1059-1028

Bergman, Ronen; Mazzetti, Mark (January 28, 2022). "The Battle for the World's Most Powerful Cyberweapon". The New York Times. ISSN 0362-4331

Bouquet, Jonathan (May 19, 2019). "May I have a word about… Pegasus spyware". The Guardian. Archived from the original on January 26, 2021. Retrieved July 18, 2021.

Kirchgaessner, Stephanie; Lewis, Paul; Pegg, David, Cutler, Sam, Lakhani, Nina and Safi, Michael (2021). Revealed: Leak uncovers global abuse of cyber – surveillance weapon

Boot, Max (December 5, 2018). "An Israeli tech firm is selling spy software to dictators, betraying the country's ideals". The Washington Post.

Bouquet, Jonathan (May 19, 2019). "May I have a word about… Pegasus spyware". The Guardian.

Wylie Christopher (2019). "How I Helped Hack Democracy". Intelligencer.

Rosenberg, Matthew; Confessore, Nicholas; Cadwalladr, Carole (2018). "How Trump Consultants Exploited the Facebook Data of Millions". The New York

Times

Lewis, Paul; Hilder, Paul (2018). “Leaked: Cambridge Analytica’s blueprint for Trump victory”. The Guardian;

Доун Е.Холмс. Их өгөгдөл. Непко хэвлэлийн газар. 2017, орч 2018 он.

David Reinsel, John Gantz, and John Rydning, “The Digitization of the World from Edge to Core,” Data Age 2025 (IDC White Paper, 2018).

WAS, Hootsuite, Data portal. Digital 2022 Global Overview Report

Baldwin, D. A. (1995). SECURITY STUDIES AND THE END OF THE COLD WAR. World Politics 48, 117-41.

Buzan, B. (1991). People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era, 2d ed. Colorado: Lynne Rienner.

Buzan, B., & Hansen, L. (2009). The Evolution of International Security. New York: Cambridge University Press.

Gaddis, J. L. (1994). The United States and the End of the Cold War: Implications, Reconsiderations, Provocations. Oxford University Press.

Gross, H. (1967). The concept of privacy. New York.

H.Ullman, R. (1983). Redefining Security. International Security.

Haftendorn, H. (1991). The Security Puzzle: Theory-Building and Discipline-Building in International Security. International Studies Quarterly 35.

May, E. R., Garthoff, R. L., & Jervis, R. (1992). The End of the Cold War: Its Meaning and Implications. (M. J. Hogan, Ed.) New York: Cambridge University Press.

Peterson, P. G., Treverton, G. F., & Bicksler, B. A. (1992). Rethinking America’s Security: Beyond Cold War to New World Order. (G. Allison, & G. F. Treverton, Eds.) New York: W. W. Norton.

Taylor, B. (2012). The Evolution of National Security studies. National Security College Occasional Paper no3.

Wolfers, A. (1952). ‘”National Security” as an Ambiguous Symbol’. Political Science Quarterly, vol.67 no.4,, 481–502.

Монгол Улсын Үндсэн хуулийн цэцийн 2024 оны 11 сарын 22 өдрийн дугаар 04 дүгнэлт

Монгол Улсын Үндсэн хуулийн цэцийн 2024 оны 06 сарын 12 өдрийн дугаар 03 дүгнэлт

[Abstract]

The Relation Between Personal Data Protection and National Security

Munkhbayar Khatanzorig

Doctor of Laws (Ph.D.)

Ulaanbaatar, Mongolia

The development of electronic technology has created many new legal and security challenges. These include domestic and foreign organizations spying on the public and using sophisticated technology to conduct propaganda for political purposes, thereby violating human rights. Countries take this into account in their security and legal policies and seek to create a legal environment to protect the personal data of their citizens from domestic political groups, criminals and foreign state organizations. This article identifies the factors that have contributed to making the protection of citizens' personal data a legal guarantee for ensuring national security, namely (1) global digitalization and (2) the explosion of databases. It analyzes three cases and discusses how the security legal policies of the United States, Russia, and China have taken this issue into account.

[Keywords]

Personal data protection, right to privacy, information security, cyber security, security law.