**УЛСЫН ИХ ХУРЛЫН ТАМГЫН ГАЗАР**

ПАРЛАМЕНТЫН СУДАЛГАА СУРГАЛТЫН ХҮРЭЭЛЭН

# ЦАХИМ ОРЧИН ДАХЬ МЭДЭЭЛЛИЙН АГУУЛГЫН ШҮҮЛТҮҮРИЙН ТАЛААРХ ГАДААДЫН ЗАРИМ ОРНЫ ТУРШЛАГА

***Харьцуулсан судалгаа***

Судалгааны код: **СТ-23/201**

2023.03.03


Хянасан: Парламентын судалгаа, сургалтын хүрээлэнгийн захирал Ц.Цогзолмаа

Хянасан: Парламентын судалгаа, сургалтын хүрээлэнгийн эрдэмтэн нарийн бичгийн дарга, Ахлах зөвлөх Ц.Норовдондог

Судлаачид: ЭНБД, Ахлах зөвлөх, доктор (Ph.D) Ц.Норовдондог;
ЭШАА О.Билгүүтэй;
Референт Б.Батцэцэг;
ЭША С.Золжаргал;
ЭША Э.Дашзэгвэ;
ЭША Б.Баянмөнх.



УЛААНБААТАР ХОТ
2023 ОН

**АГУУЛГА**


УДИРТГАЛ....2
СУДАЛГААНЫ ХУРААНГУЙ....3
СУДАЛГААНЫ ДЭЛГЭРЭНГҮЙ....13
НЭГДҮГЭЭР БҮЛЭГ. ЦАХИМ ОРЧИН ДАХЬ АГУУЛГЫН ШҮҮЛТҮҮР (КОНТЕНТ ФИЛЬТЕР)-ИЙН ТАЛААРХ ОЛОН УЛСЫН ТУРШЛАГА, ЧИГ ХАНДЛАГА....13
1. Интернэт шүүлтүүрийн эрх зүйн орчин ба үр дагавар....13
2. Шүүлтүүрийн дэглэм ба холбогдох хууль, журам....15
3. Интернэт шүүлтүүрийн эрх зүйн орчны тулгамдсан асуудлууд....17
4. Контент фильтерийн практик хэрэглээ....23
5. 2021 оны контент шүүлтийн шилдэг 8 туршлага....27
ХОЁРДУГААР БҮЛЭГ. ГАДААДЫН ЗАРИМ ОРНЫ ТУРШЛАГА....31
ЭСТОНИ УЛС....31
1. Цахим засаглалын бодлого зохицуулалт, эрх зүйн орчин....31
2. Эстони Улсын нэгдэн орсон олон улсын конвенц....34
3. 2019-2022 оны Кибер аюулгүй байдлын стратеги зорилго....34
4. Цахим орчин дахь агуулгын шүүлтүүр....34
5. Цахим орчин дахь зөрчилд хүлээлгэх хариуцлага....36
БНСУ....37
1. Цахим засаглалын бодлого, зохицуулалт....37
2. Цахим орчин дахь мэдээллийн шүүлтүүр, эрх зүйн орчин....38
3. Цахим орчин дахь хууль бус мэдээллийг хязгаарлах хэрэгслүүр....39
ДАНИ УЛС....40
1. Цахим орчин дахь эрх зүйн зохицуулалт....41
2. Цахим орчин дахь зөрчлийг шийдвэрлэх журам....44
ПОЛЬШ УЛС....46
1. Польш Улсын цахим орчин дахь контент шүүлт....46
2. Европын холбооны “Цахим үйлчилгээний тухай хууль”....47
3. Үндэсний өв, соёлын яам....47
4. Дотоод хэргийн яам....48
5. Европын холбооны цахим орчин дахь контент шүүлт....49
ЯПОН УЛС....50
1. Цахим орчин дахь эрх зүйн зохицуулалт....50
2. Цахим орчин дахь шүүлтүүрийн зохицуулалт....53
ЭХ СУРВАЛЖИЙН ЖАГСААЛТ....54

**УДИРТГАЛ**

**“**Цахим орчин дахь агуулгын шүүлтүүр (контент фильтер)-ийн талаарх гадаадын зарим орны туршлага” сэдэвт харьцуулсан судалгааг Улсын Их Хурлын Тамгын газрын Парламентын судалгаа, сургалтын хүрээлэнд гүйцэтгэв. Хүрээлэнгийн Эрдэмтэн нарийн бичгийн дарга, Ахлах зөвлөх, доктор (Ph.D) Ц.Норовдондог судалгааны 1-р бүлэг болон хураангуй хэсгийг, ЭШАА О.Билгүүтэй БНСУ-ын улсын туршлагыг, Референт Б.Батцэцэг Эстони Улсын туршлагыг ЭША Э.Дашзэгвэ Дани Улсын туршлагыг, ЭША С.Золжаргал Япон Улсын туршлагыг, ЭША Б.Баянмөнх Польш Улсын туршлагыг тус тус хариуцан боловсруулав.

***Судалгааны зорилго:***

Цахим орчинд иргэдийн эрхийг хамгаалах, гэмт хэргээс урьдчилан сэргийлэх зорилгоор цахим орчин дахь мэдээлэлд агуулгын шүүлтүүр хийж буй улс орнуудын туршлагыг бодлого, эрх зүйн орчин, хууль тогтоомжийн хэрэгжилтээс үүдэн гарч буй үр дагаврын хүрээнд судалж, цаашид анхаарах асуудлуудыг тодруулан гаргахад чиглэгдэнэ.

***Хамрах хүрээ:***

Судалгаанд цахим орчинд агуулгын шүүлтүүр хэрэглэж буй орнууд, тэдгээрийн туршлага, эрх зүйн орчны талаар олон улсын байгууллагуудаас гаргасан судалгааны үр дүн, орчин үеийн чиг хандлага, нийтлэг асуудлууд болон судалгаанд авагдсан Эстони, БНСУ, Дани, Япон, Польш зэрэг орнуудын цахим орчин дахь хууль бус үйлдлээс урьдчилан сэргийлэх эрх зүйн орчны зохицуулалт, хариуцсан төрийн байгууллагын эрх, үүрэг гэх мэт тогтолцоотой холбоотой асуудлуудыг судлав.

***Судалгааны бүтэц:***

Судалгааны ***<u>Нэгдүгээр бүлэгт</u>*** цахим орчин дахь агуулгын шүүлтүүрийн талаарх олон улсын туршлага, эрх зүйн зохицуулалтын хүрээнд анхаарах асуудлууд болон олон улсын чиг хандлагыг, ***<u>Хоёрдугаар бүлэгт</u>*** гадаадын зарим орны цахим орчин дахь агуулгын шүүлтүүрийн талаар баримталж буй бодлого, эрх зүйн орчин, практик туршлагыг тус тус дэлгэрэнгүй байдлаар судалсан болно.

***Түлхүүр үг:*** *Веб контентын шүүлтүүр, цахим орчин дахь контент шүүлтүүр, цахим гэмт хэрэг, агуулгын шүүлтүүр, цензур тогтоох, интернэтийн үйлчилгээ үзүүлэгч*

***Key words:*** *web content filter, Internet content filter, cyber crime, content filtering, censorship, internet service provider*

## СУДАЛГААНЫ ХУРААНГУЙ

Цахим орчин дахь мэдээллийн агуулгын шүүлтүүр буюу веб контент фильтер нь зохисгүй, доромжилсон, эрсдэлтэй веб контентод хандах хандалтыг хянаж, хязгаарладаг шийдлүүдийн багц юм. Судалгаанаас үзэхэд, дэлхийн улс орнуудад үндэсний аюулгүй байдал, олон нийтийн хэм хэмжээний стандартыг хангах зэрэг үндэслэлээр цахим орчны мэдээлэлд шүүлтүүр тавих практик туршлага байх боловч цензур тогтоох хяналтын механизм, мэдээллийн хамрах хүрээ нь харьцангуй өөр өөр байна.

Учир нь шүүлтүүрийн дэглэм тогтоох нь хүний эрх, эрх чөлөө, олон улсын эрх зүйн хэм хэмжээ, интернэт орчны засаглалын асуудалтай зөрчилдөж, хэвлэл мэдээлэл, олон нийтийн зүгээс байнгын шүүмжлэл дагуулж байдаг тул Үндсэн хуулиар олгогдсон үг хэлэх, үзэл бодлоо илэрхийлэх, хэвлэн нийтлэх иргэний эрхийг зөрчихгүйгээр цахим орчинд мэдээллийн аюулгүй байдлыг хангах асуудал ардчилсан улс орнуудын өмнө сорилт болон тавигдаж байна. Дэлхий даяар хариуцлагатай, үр нөлөөтэй харилцаа холбооны системийг хөгжүүлэхийн төлөө зорьж байгаа энэ цаг үед цахим орчны ил тод, хариуцлагатай, хүртээмжтэй байдлыг хангах асуудалд улс орнууд тэргүүлэх ач холбогдол өгч байна. Иймд интернэт шүүлтүүр тавих асуудалтай холбоотойгоор зөвхөн мэдээлэл, харилцаа холбооны салбарт төдийгүй бодлого боловсруулах, шийдвэр гаргах түвшинд уг шийдвэрийн үр дагавар, зөрчилдөөнт байдал их бөгөөд өргөн цар хүрээтэй гэдгийг анхаарч үзэхийг судлаачид зөвлөж байна.

Судалгааны 1-р бүлэгт, цахим орчин дахь мэдээллийн агуулгад шүүлтүүр хийдэг орнуудын практик туршлага, эрх зүйн зохицуулалт, зохицуулалтын хүрээнд олон улсын хэмжээнд анхаарах асуудлууд болон цахим шүүлтүүр тавих арга механизм, бусад орнуудын сайн туршлагыг системтэйгээр авч үзэхийг зорьсон.

2004 онд OpenNet Initiative (Нээлттэй сүлжээний санаачилга, ONI) олон улсын байгууллагаас “Интернэт шүүлтүүрийн эрх зүйн орчны үр дагавар”[1] сэдэвт судалгааны тайлан гаргасан байх бөгөөд цахим орчинд шүүлтүүр тавьж, мэдээллийн агуулгыг хянах хууль тогтоомжтой улс орнуудын туршлага, эрх зүйн зохицуулалтаас үүдэн гарч буй үр дагаврыг судалж, олон улсын хэмжээнд анхаарах шаардлагатай асуудлуудыг тодруулан гаргасан. Уг судалгаанд хяналтын механизмыг хэрэгжүүлж буй веб хөтчүүд болон блоклогдсон, хаагдсан сайтуудыг өргөнөөр хамруулж, эмпирик мэдээлэлд тулгуурлан дүгнэлт гаргасан байх бөгөөд өөр ийм томоохон хэмжээний суурь судалгаа үгүй тул судалгаанд эх сурвалж болгон ашиглав.

2021 онд олон улсын мэдээллийн технологийн ажилтнуудад зориулсан www.spicework.com сайтад нийтлэгдсэн контент фильтертэй холбоотой онол, арга зүй, олон улсын туршлага, Ковид-19 цар тахлын дараах чиг хандлагын талаарх мэдээллийг мөн энэ судалгаанд ашиглав.[2]

---

[1] https://opennet.net/docs/Legal_Implications.pdf

[2] https://www.spiceworks.com/it-security/network-security/articles/what-is-content-filtering-definition-types-and-best-practices/

Судалгааны 2-р бүлэгт, судалгаанд авагдсан орнуудын туршлага, эрх зүйн орчны талаарх мэдээллийг тухайн улс орны холбогдох мэдээллийн сайт, интернэтийн нээлттэй эх сурвалжуудыг ашиглан боловсруулав.

Олон улсын туршлагаас үзэхэд, интернэтийн агуулгыг ямар нэг байдлаар цензурддаг орнуудад ихэвчлэн тодорхой веб сайт руу нэвтрэхийг хориглох, цахим шуудангийн урсгалыг хаах, дахин чиглүүлэх, эсвэл хэрэглэгчийн хүссэнээс өөр хайлтын илэрцүүдийг гаргах гэх мэт аргуудыг хэрэглэдэг байна.

Иймд судалгааны 1-р бүлэгт дараах асуудлуудыг тодруулан авч үзлээ. Үүнд:

- Интернэт орчинд хэн шүүлтүүр тавьдаг вэ?
- Интернэт орчинд хэрхэн шүүлтүүр тавьдаг вэ?
- Интернэт орчинд ямар эрх зүйн үндэслэлээр, ямар эрх мэдлийн хүрээнд шүүлтүүр тавьдаг вэ?
- Интернэт орчинд шүүлтүүр тавихад олон улсын хэмжээнд хүний эрхийн болон хууль зүйн ямар үр дагавар гардаг вэ?
- Интернэт орчинд шүүлтүүр тавихтай холбоотой сүүлийн үеийн туршлагууд гэх мэт

**СУДАЛГААНЫ ҮР ДҮНГИЙН ТОЙМ:**

Дэлхийн улс орнуудад, тэр дундаа ардчилсан зарчим, иргэний эрх, эрх чөлөөг эрхэмлэдэг улс орнуудад ч гэсэн ямар нэгэн байдлаар интернэтийн агуулгыг шүүж, цензурдах сонирхол, хүсэл эрмэлзэл түгээмэл ажиглагдаж байна. Гэвч шүүлтүүрийн байршил, тоо хэмжээ, хэрэгжүүлж буй арга механизм, мэдээллийг хязгаарлах цар хүрээ нь тухайн улс орны засаглалын онцлог, цахим орчны талаар баримталж буй бодлогоос шалтгаалан харилцан адилгүй байна. Тухайлбал, Хятад, Саудын Араб, Иран, Бирм болон ТУХН (Тусгаар Улсуудын Хамтын Нөхөрлөл)-ийн орнууд, Азийн зарим орнуудад улс орны хэмжээнд иргэний эрх, эрх чөлөөг хязгаарлах байдлаар илүү өргөн хүрээтэй хязгаарлалт хийдэг бол ардчилсан улс орнуудад иргэдийнхээ Үндсэн хуулиар олгогдсон эрх, эрх чөлөөг хүндэтгэх бөгөөд зөвхөн насанд хүрээгүй хүүхдүүдийг цахим орчин дахь зохисгүй мэдээлэл, түүний сөрөг үр дагавраас хамгаалах үүднээс айл өрх, албан байгууллага, сургуулийн орчин, номын сан зэрэг тодорхой орчинд хязгаарлагдмал байдлаар хэрэгжүүлдэг туршлага ажиглагдаж байна.

Мөн түүнчлэн сүүлийн үед хил хязгааргүй интернэтийн орон зай нэмэгдэж, мэдээллийн технологийн хөгжлийг дагаад цахим үйлчилгээ, хэрэглээ нэмэгдсэн, Ковид-19 цар тахлын улмаас цахим ажлын байрны орчин бүрдүүлэх, зайнаас ажиллах хэрэгцээ шаардлага бий болсны улмаас интернэт орчин дахь мэдээллийн аюулгүй байдал, гэмт хэрэг зөрчлөөс урьдчилан сэргийлэх асуудалд дэлхийн ихэнх орнууд анхаарал хандуулж байна. Ингэхдээ хамгийн гол нь иргэний мэдээлэл авах, мэдэх эрхийг хязгаарлахгүй байх, тодорхой зорилгод нийцүүлэн зохистой байдлаар зохицуулах шаардлагатай тулгарч байна.

Судалгаанаас үзэхэд хувийн компаниуд, албан байгууллага, айл өрхүүд ихэвчлэн интернэтийн шүүлтүүр тавьдаг байна. Засгийн газраас шүүлтүүр

тавихыг үүрэг болгосон  тохиолдолд төрийн өмчит интернэтийн үйлчилгээ үзүүлэгч компани тухайлсан удирдамжийн дагуу энэ үүргийг хэрэгжүүлж байна. Зарим хувийн компаниуд хэрэглэгчийг тодорхой веб сайт руу нэвтрэхийг хориглодог программ хангамж үйлдвэрлэдэг. Энэ шүүлтүүр нь бүрэн хувийн зориулалтаар ашиглагддаг бөгөөд бага насны хүүхдүүдийг хориотой мэдээлэлд хандахаас хамгаалах зорилготой хувь хүмүүсийн гэрийн хэрэгцээндээ зориулан гаргасан шүүлтүүрийн программ юм. Засгийн газрын хувьд хувийн шүүлтүүрийн программыг ашиглахгүй ч гэсэн хувийн программ хангамжийн компаниудаар тодорхой зорилго бүхий шүүлтүүрийн программыг аутсорсингоор хийлгэдэг туршлага зарим оронд байна.

**ШҮҮЛТҮҮР ТОГТООХ ЭРХ ЗҮЙН ОРЧНЫ ТУХАЙД:**

Контентын шүүлтүүрийн дэглэм тогтоох, хэрэгжүүлэхтэй холбоотой бодлого, эрх зүйн орчин улс орнуудад харилцан адилгүй байна.  Тухайлбал, Хятад Улсад интернэтэд нэвтрэх эрхийн хязгаарлалтыг хуулиар тогтоосон байхаас гадна засгийн газар болон интернэтийн үйлчилгээ үзүүлэгч провайдер (ISP) компани хооронд байгуулсан гэрээгээр зохицуулдаг байна.  Хятадад ердөө 9 (ISP) интернэтийн үйлчилгээ үзүүлэх тусгай зөвшөөрөлтэй компани байдаг бөгөөд энэ нь засгийн газар интернэт орчныг хяналтдаа байлгахад хялбар болгодог байна. Хятад Улс Google болон бусад хайлтын систем дахь илэрцийн үр дүнг хязгаарласан бөгөөд нийт 60 гаруй хууль тогтоомжоор веб хэрэглэгчдийн ашиглах боломжтой контентыг хязгаарласан байдаг. Хууль тогтоомжид ямар агуулгыг шүүх, ямар зөвшөөрлөөр шүүх талаар тодорхой заагаагүй, энэ талаар ямар нэгэн стандарт тогтоогоогүй.

Тэгвэл Бирм зэрэг улсад интернэтийн агуулгыг хянахын тулд хэвлэл мэдээллийн хэрэгслийг зохицуулах ерөнхий хууль тогтоомжийг ашигладаг бол Энэтхэгт Харилцаа холбооны конвергенцийн тухай хуулиар мэдээллийн хэрэгслийн төрлөөс үл хамааран улсын хэмжээний бүх харилцаа холбооны агуулга, дамжуулалтыг өргөн хүрээтэй зохицуулдаг. Зарим улс орнуудад интернэтийн хандалт болон агуулгын олон нийтэд үзүүлэх үр нөлөөг харгалзан тогтсон үйл ажиллагаа явуулж байгаа хэвлэл мэдээллийн хэрэгслүүдэд анхаарал хандуулдаг.

Ихэнх улс орнуудад интернэтийн агуулгыг хязгаарлахын тулд ихэвчлэн ерөнхий хууль тогтоомжийг ашигладаг. Тухайлбал, хэд хэдэн улс оронд Оюуны өмчийн тухай хуулийн хүрээнд зохиогчийн эрхийн дэглэмийг ашиглан контентыг хязгаарладаг бол зарим оронд тодорхой веб сайт руу нэвтрэх болон гүтгэлгийг хориглосон хуулийн зохицуулалтыг ашигладаг. Энэ нь ихэвчлэн улс төрчид, улс төрийн намуудын болгоомжлох сэдэлтэй холбоотой бөгөөд гүтгэсэн, гутаан доромжилсон мэдээллийг хязгаарлахад чиглэж байна. Интернэтийн тусгайлсан дүрэм, журамгүй ч гэлээ засгийн газрын үйл ажиллагааны эсрэг чиглэсэн мэдээллийг хязгаарлах зохицуулалт буюу дефакто цензур тогтоох практик мөн ажиглагдаж байна.

**Интернэт орчинд шүүлтүүр тавих эрх зүйн орчны хүрээнд анхаарах асуудлууд:**

## 1. *Иргэний үг хэлэх, үзэл бодлоо илэрхийлэх, хэвлэн нийтлэх, хувь хүний нууцыг хадгалах, шашин шүтэх, эвлэлдэн нэгдэх гэх мэт эрх, эрх чөлөөнд нөлөөлөх тухай асуудал*

Интернэт шүүлтүүр нь иргэний хууль ёсны эрх, эрх чөлөөг зөрчих эрсдэлтэй байдаг. Ихэнх улс оронд иргэд үзэл бодлоо илэрхийлэх, хувийн нууц хадгалах, шашин шүтэх, эвлэлдэн нэгдэх эрх чөлөөтэй байдаг. Шүүлтүүрийн дэглэм тогтоож мэдээллийг блоклох нь үг хэлэх, үзэл бодлоо илэрхийлэх эрх чөлөөг дэмждэг болон интернэт контентын сөрөг нөлөөнд санаа зовдог хүмүүсийн хувьд харьцангуй өөр өөр хандлагаар илэрдэг. Гол асуудал нь шүүлтүүрийн программ хангамжаар тухайлсан бодлого, зорилгод хамааралгүй маш их материалыг автоматаар хааж, алга болгож байгаа нь стандартыг зөрчиж байгаа тул шүүлтүүрийн технологи ихээхэн шүүмжлэл дагуулж байгаа юм.

Өөрөөр хэлбэл, интернэт шүүлтүүр нь нэг талаас төр нь иргэддээ хохирол учруулахаас урьдчилан сэргийлж, мэдээллийн цензур тогтоож байгаа мэт боловч нөгөө талаас иргэдийн интернэтийн контент ашиглах бодит боломжийг бууруулж, мэдээлэл авах, үзэл бодлоо илэрхийлэх гэх мэт эрхийг хөнддөг учраас төвөгтэй байдал үүсгэдэг. Үүний ард улс төрийн нам, эрх баригчдын зүгээс хүсээгүй контентыг иргэдэд хүргэхээс сэргийлэх эрмэлзэл нуугдаж байгаа хэмээн олон нийтийн зүгээс  шүүмжлэлтэй ханддаг байна.

## 2. *Шүүхийн харьяаллыг хэрхэн  тогтоох тухай асуудал*

Хууль зүйн хувьд харьяалал гэдэг нь тухайн улс орон, бүс нутаг болон асуудлыг зохицуулах, хянах эрх бүхий этгээдийн эрх мэдлээ хэрэгжүүлэх хил хязгаар, эрх хэмжээний тухай асуудал юм. Улс орон бүр зөвхөн  өөрсдийн газар нутгийн харьяаллын хүрээнд эрх мэдлийн хяналт тогтоож, хууль тогтоомж батлан хэрэгжүүлдэг. Гэвч интернэт орчинд улс орны хил хязгаарыг давсан үйл ажиллагаа явагдаж байдаг. Иймээс жишээлбэл, АНУ-ын иргэн Монголд байгаа хүмүүсийг хохироох үйлдэл хийвэл аль улсын шүүхийн харьяалалд хамаарах вэ? гэдэг асуудал гарч ирнэ.

Тэгвэл интернэт шүүлтүүрийн тухайд үүн дээр асуудал үүсдэг бөгөөд тухайн муж, улс өөрийн газарзүйн хил хязгаарын хүрээнд сүлжээгээр дамжиж буй хэрэг маргааныг шүүхээс гадна өөрийн нутаг дэвсгэрийн гадна дэлхий даяар интернэт сүлжээнд холбогдож буй иргэдийн харилцааг зохицуулж, нөлөөлөх шаардлагатай тулгардаг. Шүүлтүүр нь тухайн улсын хилийн дотор тодорхой веб сайт руу нэвтрэхийг хааж, эсвэл хил доторх сүлжээний урсгалыг өөрчлөхдөө хил хязгааргүй орон зайд харьяат бус хүмүүсийг ч нэвтрэхийг хязгаарлаж болзошгүй тул интернэтийн хяналт нь газарзүйн хувьд тархмал, олон улсын эрх ашгийг хөндөх үр дагавартай байдаг. Иймд энэ төрлийн хэрэг маргааны харьяаллын асуудлыг зохицуулахын тулд 1) шүүх эрх мэдлийн харьяаллыг тогтоох, 2) баримтлах хууль эрх зүйн актын сонголт хийх, 3) хууль хэрэгжүүлэх процессыг тодорхой болгох гэсэн 3 үндсэн асуудлыг зайлшгүй авч үзэх шаардлагатай болдог байна.

## 3. *Шүүхийн шийдвэрийг хэрэгжүүлэх тухай асуудал*

Шүүхийн шийдвэрийг хэрэгжүүлэх нь тухай улсын шүүхийн шийдвэр биелүүлэх хараат бус байдал, чадавхаас хамаарах бөгөөд шүүхийн шийдвэр гүйцэтгэхийн тулд тухайн улс орон нь хариуцагч болон түүний хөрөнгийг шууд хянах эрхтэй байх, эсхүл өөр муж, улстай шүүхийн шийдвэр заавал биелүүлэх тусгайлсан гэрээтэй байх шаардлагатай болдог.

Шүүлтүүр тогтоох нь өөрөө тодорхой эрх мэдлийг бий болгодог учраас төрөөс интернэтийн дэд бүтэц, интернэтийн үйлчилгээ үзүүлэгч, контент нийлүүлэгч болон хэрэглэгчдэд шүүлтээр дамжуулан хяналт тавьж, шийдвэрээ хэрэгжүүлэх хангалттай боломжийг эдэлж байдаг. Гэвч тухайн муж, улсын газарзүйн хил хязгаарт хариуцагч тал харьяалагдахгүй тохиолдолд албадлагын эрх мэдэл хязгаарлагддаг. Тэгвэл шүүлтүүр тавьснаар тухайн улс орны харилцаа холбооны дэд бүтцэд нь нэвтрэх эрхийг нь хязгаарлах, хориглох замаар шийдвэрийн хэрэгжилтийг хангуулж чадна.

### 4. *Интернэтийн засаглалын асуудал*

Интернэтийн засаглал гэдэг нь эрх бүхий олон улсын байгууллага болон стандарт тогтоогч байгууллагуудаас улс орнууд болон интернэтийн үйлчилгээ үзүүлэгч провайдер компаниудыг хянах тогтолцоог бий болгох тухай асуудал юм. Энэ асуудал 2003 оноос хойш олон улсын анхаарлын төвд орж эхэлсэн бөгөөд олон улсын хэмжээнд домэйн нэрийн хуваарилалт, Internet Corporation for Assigned Names and Numbers (ICANN)-ийн бүтэц, зохион байгуулалт болон шүүлтүүр, спам, сүлжээний аюулгүй байдал болон бусад төвөгтэй, түгээмэл тохиолддог өргөн хүрээний асуудлуудыг хамарсан нэгдсэн ойлголцол, зөвшилцөлд хүрэхийг зорьж байна.

### 5. *Олон улсын зохицуулалтын асуудал*

Улс орнууд ихэвчлэн олон талт хэлэлцээрээр энэхүү харилцааг зохицуулдаг. Гэвч зарим тохиолдолд тухайлбал, улс хоорондын чөлөөт худалдааны хэлэлцээрийн шаардлагыг тухайн улс орнуудын иргэд, хуулийн этгээдийн хооронд хийгдэж байгаа арилжааны гүйлгээнд шүүлтүүр тавих замаар зөрчих байдал практикт үүсэж болзошгүй юм. Мөн түүнчлэн зарим контентыг “эмзэг” хэмээн үзэж блоклох нь олон улсын хүний эрхийн тухай хууль, конвенцыг зөрчихөд хүргэдэг. Энэхүү нарийн төвөгтэй байдлаас болоод иргэдийнхээ интернэтийн хэрэглээнд системтэй хяналт тавьж байгаа үед аль нэг компани, улс орныг “хүний эрхийг зөрчигч” хэмээх ангилалд оруулж эхэлсэн. Иймээс олон улсын хүмүүнлэг эрх зүйн системийг хөгжүүлэх хүрээнд харилцаа холбооны системд хүний эрхийг хамгаалах асуудлыг сүүлийн үед хөндөж ярих болсон байна.

Интернэт шүүлтүүрийн хамгийн чухал код нь хууль, эрх зүйн код биш харин компьютерын код юм. Интернэт шүүлтүүрийг ихэвчлэн тодорхой бодлого, хууль тогтоомж, зохицуулалтын актын хүрээнд практикт нэвтрүүлдэг боловч хамгийн гол нь программчлагдсан байдгаараа онцлогтой. Программ хангамж нь хууль ёсны түншийнхээ харьяаллын алдаанаас ангид, автоматжсан байдаг учраас улс орнууд код нэвтрүүлэхийн тулд холбогдох муж, улс орнуудтай гэрээ байгуулдаг. Хууль тогтоомжоор шүүлтүүрийн горимыг тойрч гарахыг хориглоно. Иймээс олон улсын хэмжээнд интернэтийн шүүлтүүр тавихтай холбоотой

шийдвэрлэх, тулгамдсан асуудлууд олон байгаа нь судалгаанаас харагдаж байна.

### *6. Контент шүүлтийн сүүлийн үеийн туршлага, чиг хандлага*

Сүүлийн 20 шахам жилийн хугацаанд интернэт дэлхий даяар бизнесийн үйл ажиллагаанд улам бүр чухал үүрэг гүйцэтгэх болсон бөгөөд 2020 онд Ковид-19 цар тахал гарсны улмаас хүн төрөлхтөн зайнаас ажиллах, цахим горимд шилжих хэрэгцээ шаардлага бүр ч ихээр нэмэгдсэн. Өмнө нь алсаас хийх боломжгүй гэж бодож байсан ажлууд удалгүй бүхэлдээ онлайнаар шилжсэн.

Сургууль, компани, төрийн болон төрийн бус бүх байгууллагууд “гэрээсээ ажиллах" загварт шилжсэнтэй холбоотойгоор контент шүүлтүүрийн янз бүрийн шийдлүүд, технологийн, өрсөлдөөнт зах зээл бий болж байна. Тухайлбал, интернэт шүүлтүүрийг ашиглах дараах хэлбэрүүдийг бий болгосон. Үүнд:

#### *Алсын зайнаас шүүлтүүр байршуулах*

Ковид-19 цар тахлын үед дэлхийн олон компаниуд гэрээсээ ажиллах загвараар үйл ажиллагаагаа явуулсаар ирсэн. Олон байгууллага ажилтнуудынхаа дотоод системд агуулгын шүүлтүүр тавиагүй байхдаа алсын зайн ажлын нөхцөлд шилжсэн. Энэ тохиолдолд байгууллагын зүгээс агуулгын шүүлтүүрийг алсаас ашиглах дараах 3 аргыг хэрэглэсэн:

- Хэрэглэгчийн зааварчилгаа өгөх (ажилтнууд контент шүүлтүүрийг өөрсдөө суулгаж ашиглах)
- Алсын зайнаас байршуулах (IT ажилтнууд агуулгын шүүлтүүрийг тавьж ажилчдын системийг алсаас удирддаг)
- Интернэтийн провайдер үйлчилгээ үзүүлэгчээ солих (Google Workspace гэх мэт агуулгын шүүлтүүрийг санал болгодог платформ руу шилжих)

#### *Дотоод харилцаа холбооны системийг ашиглах*

Ковид-19 цар тахлын нөлөөгөөр дотоод харилцаа холбооны үүрэг роль улам нэмэгдсэн. Цахим шуудан болон виртуал уулзалтууд нь албан байгууллагын өдөр тутмын үйл ажиллагаа, дотоод мэдээлэл, хүний нөөц гэх мэт компанийн чухал функцуудыг өөр горимд шилжүүлсэн учраас оффисын системд өөр хүмүүс нэвтэрч, байгууллагын дотоод мэдээлэл, нууц мэдээллийг хулгайлах, хакердах оролдлого гарч болзошгүй хэмээн үзэж, агуулгын шүүлтүүр тавих замаар эдгээр оролдлогыг хааж, компанийн системийн бүрэн бүтэн, аюулгүй байлгах арга хэмжээ авч эхэлсэн.

#### *Либерал ажлын байрны бодлого хэрэгжүүлэх*

Ковид-19 цар тахлын дараагаар ч гэсэн дэлхийн олон компаниуд ажилтнууддаа гэрээс ажиллах боломж олгож, цаашид зарим нь байнгын алсын зайн ажлын загварт шилжихээр төлөвлөж байна. Гэрээсээ ажиллаж байгаа тохиолдолд ажилтны ажлын цаг ашиглалтыг минут, секундээр хянах боломжгүй тул либерал ажлын байрны бодлогын хүрээнд компаниудын зүгээс үйл явцад биш үр дүн, гарцад чиглэсэн илүү чөлөөтэй, шинэ ажлын байрны бодлогыг хэрэгжүүлэхийг зорьж байна. Өмнө нь ажилчдын зүгээс кибер аюулгүй байдлаа хангахад төдийлөн анхаардаггүй байсан ба системийг түгжээгүй, хараа хяналтгүй орхих, компанийн зөөврийн компьютерийг найз нөхөд, гэр бүлийнхээ хувийн

хэрэгцээнд ашиглуулах зэргээр хайнга ханддаг байсан бол одоо дэлгэцэн дээрх мэдээллийг нууцлах, мэдээллийн аюулгүй байдлыг хангах зэрэг шинэ шаардлагууд гарч ирсэн. Иймд компанийн систем, мэдээллийн баазын аюулгүй байдлыг хангах, санамсаргүй эсвэл санаатайгаар алдаа гаргахаас зайлсхийх, урьдчилан сэргийлэх зорилгоор компаниуд хамгийн сүүлийн үеийн шүүлтүүр суурилуулах арга хэмжээ авч байна.

Мөн түүнчлэн насанд хүрэгчдэд зориулсан контент, зэвсэг, хар тамхины мэдээлэл, үл тэвчих, хортой контентын хандалтыг хаах зорилгоор шүүлтүүр тавих, байгууллагууд компанийн бүтээмжийг бууруулахгүйгээр системийн бүрэн бүтэн байдлаа хангах зорилгоор агуулгын шүүлтүүр тавих практик түгээмэл байна.

Санхүүгийн байгууллагын тухайд сегментчилсэн албан сүлжээтэй байх бөгөөд харилцагчийн мэдээлэлд хандах эрхтэй хэлтэс, алба нь илүү их хязгаарлалттайгаар контентыг шүүх дабль стандартыг нэвтрүүлэх шаардлагатай болдог.

Интернэт нь хэмжээлшгүй өргөн уудам орон зайд аюул заналхийллийг зөвхөн нэг товшилтоор хүлээн авах боломжтой боловч, зөвхөн "мэдэгдэж байгаа" эрсдэлт хүчин зүйлсийг хаах нь учир дутагдалтай. Учир нь үл мэдэгдэх бүх зүйлийг хааснаар бусад хүмүүст чухал ач холбогдолтой байж болох мэдээллийн нөөцөд хандах хандалтыг хязгаарлах болдог. Иймээс агуулгын шүүлтүүрийн шийдэл нь "ухаалаг" бөгөөд "динамик" шинж чанартай, аюулгүй байдал, бүтээмжийн төгс тэнцвэрийг хангасан байх шаардлагатай хэмээн үзэж судалгаа, үнэлгээний ажлууд компанийн түвшинд хийгдэж байна.

## СУДАЛГААНД АВАГДСАН ОРНУУДЫН ТУРШЛАГА

### *Эстони Улс*

Эстони Улс нь цахим засаглалын хэрэгжилтээр 193 орноос 15 дугаарт, ил тод байдлын үзүүлэлтээр 177 орноос 28 дугаарт ордог. Тус улсад цахим орчинд агуулгын шүүлтүүр хийдэг тусгайлсан хууль байхгүй бөгөөд цахим орчны харилцааг Цахим харилцааны тухай хууль, Хувийн мэдээлэл хамгаалах тухай хууль, Нийгмийн үйлчилгээний тухай хууль, Нийтийн мэдээллийн тухай хууль, Тоон гарын үсгийн тухай хууль, Кибер аюулгүй байдлын тухай хууль, Эрүүгийн хууль, Иргэний хууль болон холбогдох дүрэм журмаар зохицуулж байна.

Интернэт үйлчилгээ үзүүлж байгаа тал агуулгыг хянах болон хэрэглэгчийн дамжуулсан хууль бус контентын төлөө хариуцлага хүлээдэггүй бөгөөд нийгмийн мэдээллийн сүлжээнд хууль бус, ёс журам зөрчсөн үйлдлээс урьдчилан сэргийлэх, хариу арга хэмжээ авах зорилгоор Rahvaalgatus.ee платформыг ашигладаг. Хууль тогтоогчдын үйл ажиллагааг хянах, олон улсын сүлжээ Inhope, Insafe зэрэг ашгийн бус байгууллагуудтай хамтран цахим орчин дахь хүүхдийн хүчирхийллийг хянах, Web constables вэбсайт нь цахим орчинд бэлгийн болон бусад төрлийн хүчирхийллийн агуулгатай мэдээлэл, мессежийг хянаж цагдаагийн газарт мэдээлэх гэх мэт техникийн болон хууль эрх зүйн хэд хэдэн арга хэрэгсэл байна.

Эстони Улсын Үндсэн хуулиар мэдээлэл олж авах, үг хэлэх, үзэл бодлоо чөлөөтэй илэрхийлэх эрхийг баталгаажуулсан тул цахим орчинд үзэл бодлоо

илэрхийлэхэд үндэс угсаа, арьс өнгө, шашин шүтлэг, нийгмийн гарал үүсэл, бэлгийн чиг баримжаа, санхүүгийн байдал, хэл, соёл зэргээр ялгаварлан гадуурхаж бусдыг гутаан доромжлох зэрэгт Эрүүгийн болон Иргэний хуулийн дагуу хариуцлага хүлээлгэдэг.

***БНСУ***

БНСУ-ын цахим орчны эрх зүйн зохицуулалт нь Эрүүгийн хууль (Criminal Law), Бэлгийн хүчирхийллийн эсрэг хууль (Sexual Violence Punishment Act); Мэдээлэл, харилцаа холбооны сүлжээний тухай хууль (Information and Communication Network Act), Мэдээлэл, харилцаа холбооны хяналтын журам (Information and Communication Reviewing Regulation) зэрэг хэд хэдэн хууль тогтоомжоос бүрддэг байна. 2019 оны 2 дугаар сард ***Солонгосын Харилцаа Холбооны Хорооноос*** (KCC) цахим орчин дахь хууль бус үйлдлээс урьдчилан сэргийлэх, мэдээллийн шүүлтүүр хийх бодлогыг шинэчлэн баталсан байна. БНСУ-ын Засгийн газраас мөрийтэй тоглоом, порнографын сайт зэрэг хууль бус цахим хуудсанд нэвтрэхийг хориглох зохицуулалтыг цахим орчинд хэрэгжүүлж байна[3].

Дээрх зохицуулалтыг хэрэгжүүлэхдээ хууль бус агуулга бүхий цахим контентыг илрүүлж хуулийн хүрээнд хаах (блоклох) зэрэг арга хэмжээ авч байна. Гэсэн хэдий ч БНСУ-ын Засгийн газар цахим орчинд иргэдийн эрхийг хамгаалах үүднээс аль болох тэнцвэртэй байдлаар интернэтийн нээлттэй байдлыг хангаж ажилладаг. БНСУ-д цахим орчин дахь хууль бус мэдээллийг хязгаарлахдаа Transport Layer Security (TLS) интернэтийн протоколыг ашигладаг байна. TLS протокол нь интернэт хөтөч болон контентыг байршуулах сервер хоорондын урсгалыг шифрлэдэг аюулгүй байдлын протокол бөгөөд SNI (Серверийн нэрийн заалт) нь серверт зөвшөөрөгдсөн домайныг таньж, аль хост хаанаас аль хөтчийг ашиглан хүсэлт илгээж байгааг тодорхойлдог байна.

***Дани Улс***

Дани Улс цахим шилжилт, бүх нийтийн цахимжуулалтын чиглэлээр дэлхийд тэргүүлэгч орны нэг бөгөөд энэхүү үзүүлэлтээр НҮБ, ЕХ-ны гишүүн орнуудын дунд удаа дараа тэргүүн байранд эрэмбэлэгдэж ирсэн. Дани Улсад интернэтийн орчинд хууль бус контентыг хаах, шүүлтүүрдэх, устгах харилцааг тусгайлан зохицуулсан бие даасан хууль тогтоомж, интернэт орчинд хяналт тавих тусгайлсан чиг үүрэг бүхий төрийн байгууллага, албан тушаалтан байдаггүй. Ерөнхий зохицуулалтууд нь эрх зүйн хэд хэдэн салбарт хамаарах бөгөөд тус тусын чиглэлээр хууль бус контентоос урьдчилан сэргийлэх зохицуулалтуудыг тусгасан байдаг. Тэдгээрийг эрх зүйн салбар, хүрээгээр нь эрүү, иргэн, захиргааны эрх зүйн болон зөөлөн эрх зүйн (soft law) зохицуулалт хэмээн 4 үндсэн чиглэлд авч үзсэн байдаг. Хууль бус интернэт контентыг ихэнхдээ хэрэглэгчийн DNS, эсхүл IP хаягийг хаах, хязгаарлах замаар хянадаг учраас голлох зохицуулалт нь интернэт провайдер буюу интернэтийн үйлчилгээ үзүүлэгч (ISP)-дийн үйл ажиллагаатай холбоотой байдаг. Интернэтийн үйлчилгээ

[3] Analysis: South Korea's New tool for filtering illegal internet content By Robert Morgus, Justin Sherman, and Seonghyun Nam

үзүүлэгчид нь хууль бус интернэт контентыг хаах, устгах арга хэмжээг зөвхөн шүүхийн шийдвэрийн дагуу гүйцэтгэдэг.

Данийн Үндсэн хуулийн 77-р зүйлд иргэний үзэл бодлоо чөлөөтэй илэрхийлэх эрхийг баталгаажуулсан байдаг ба энэхүү эрх чөлөөнд халдаж болзошгүй нөхцөл байдлыг үүсгэж, байнгын эргэлзээ, шүүмж дагуулж байдаг учраас тус улсад интернэтийн контентыг өргөн хүрээнд, системтэйгээр хянах, шүүлтүүрдэх арга хэмжээг хэрэгжүүлдэггүй байна.

***Польш Улс***

Польш Улсын цахим орчны эрх зүйн зохицуулалт нь Цахимаар үйлчилгээ үзүүлэх тухай хууль (Providing Services by Electronic Means) болон Европын Холбооны Цахим үйлчилгээ үзүүлэх тухай хуулийг (Digital Services Act) үндэслэж Польш Улсын Эрүүгийн хууль, Кибер аюулгүй байдлын тухай хууль, Терроризмын эсрэг хууль зэрэг бусад холбогдох хууль тогтоомжоос бүрддэг байна. Польш Улсын цахим орчныг зохицуулагч төрийн байгууллага нь Польш Улсын Цахим Харилцааны Яам (Ministry of Digital Affairs) байх бөгөөд тус яамны контентын зохицуулалттай холбоотой үйл ажиллагааны тэргүүлэх чиглэл нь үг хэлэх, үзэл бодлоо илэрхийлэх эрх чөлөөний үндсэн эрхийг хамгаалж, хууль бус мэдээлэлд хандах хандалтыг мэдээллэх, хаах журмыг тодорхойлох, тэдгээрийг уялдуулахад чиглэж байна.

Хууль бус контентын зохицуулалтыг Европын Холбооны Контент Шүүлтүүрийн хуулиар зохицуулж байна. Тус хуулинд насанд хүрээгүй хүүхдийг садар самуунд уруу татах, арьс өнгөөр ялгаварлах, гүтгэх, гутаан доромжлох, террорист суртал ухуулгыг сурталчлах зэрэг цахим орчны хууль бус контентыг цензурдэж, шүүлтүүрдэх тухай заасан байна.

Польш Улс нь автомат шүүлтүүр буюу “Тоон Цензур (Digital Censorship)”-г цахим орчны хууль бус контентыг шүүхэд ашиглаж байна. Энэ нь өгөгдсөн алгоритмын дагуу хэрэглэгчийн үүсгэсэн контентод шүүлт хийж, хууль бус агуулгыг илрүүлэн устгаж хориглох эсвэл нийтлэх үүрэгтэй автомат шүүлт юм.

***Япон Улс***

Япон Улсын хувьд цахим орчин дахь  контент түгээлт нь олон нийтэд нээлттэй өргөн нэвтрүүлгийн адилаар мэдээллийг түгээх хүчтэй хэрэгсэлд тооцогддог. Тиймээс  олон нийтийн харилцааны хэрэгсэл дэх контентыг иргэний үзэл бодлоо илэрхийлэх талбар хэмээн үзэж, эрх чөлөөгөөр хангахыг чухалчлан үздэг. Зүй бус мэдээллийг хязгаарлахын тухайд, интернэтийн сайтуудыг тодорхой шалгуурын дагуу үнэлж, шүүлтүүр хийдэг байна. Интернэтийн үйлчилгээ үзүүлэгчид болон үүрэн телефоны байгууллагууд  тусгайлсан программ хангамжийн тусламжтайгаар мэдээллийг цахим орчинд нийтлэхийг зөвшөөрөх, хориглох байдлаар шүүлтүүр хийдэг.

Япон Улсад цахим орчныг хөгжүүлэх, контент шүүлтүүртэй холбоотой асуудлыг зохицуулах зорилгоор “Интернэтийг аюулгүй  ашиглах орчныг хөгжүүлэх тухай хуулийг”  2008 оны 6 сард баталсан. Уг хуулийн зорилго нь цахим орчинд насанд хүрээгүй хүүхдийг зохисгүй мэдээллээс хамгаалах, урьдчилан сэргийлэх үүднээс зүй бус мэдээллийг шүүх программ хангамжийг хөгжүүлэхэд чиглэгдсэн.

Засгийн газар, орон нутгийн засаг захиргааны зүгээс цахим орчин дахь зүй бус мэдээллийг шүүх программ хангамжийн хэрэглээг түгээн дэлгэрүүлэх чиглэлээр шаардлагатай арга хэмжээг авч ажиллаж байна. Энэхүү үйл ажиллагааг зохицуулах, хянах чиг үүргийг Дотоод хэрэг, харилцаа холбооны яам, Эдийн засаг, худалдаа аж үйлдвэрийн яам гүйцэтгэдэг. Мөн Японы Интернэт Үйлчилгээ Үзүүлэгчдийн Холбоо (JAIPA) нь хувийн байгууллагууд болон хэрэглэгчдийг дээрх яамтай холбож, хамтарч ажиллах үүрэг гүйцэтгэдэг.

(Дэлгэрэнгүй мэдээллийг судалгааны хэсгээс үзнэ үү)

## СУДАЛГААНЫ ДЭЛГЭРЭНГҮЙ

## НЭГДҮГЭЭР БҮЛЭГ. ЦАХИМ ОРЧИН ДАХЬ АГУУЛГЫН ШҮҮЛТҮҮР (КОНТЕНТ ФИЛЬТЕР)-ИЙН ТАЛААРХ ОЛОН УЛСЫН ТУРШЛАГА, ЧИГ ХАНДЛАГА

### 1. Интернэт шүүлтүүрийн эрх зүйн орчин ба үр дагавар

OpenNet Initiative (Нээлттэй сүлжээний санаачилга, ONI) олон улсын байгууллагаас 2004 онд “Интернэт шүүлтүүрийн эрх зүйн орчны үр дагавар”[4] сэдэвт судалгааны тайланг гаргасан байна. Уг судалгааг Торонтогийн Их сургуулийн Иргэний лабораторийн дэргэдэх Беркманы төв, Кембрижийн их

[4] https://opennet.net/docs/Legal_Implications.pdf

сургуулийн дэргэдэх Аюулгүй байдлын хөтөлбөртэй хамтран гүйцэтгэсэн бөгөөд шүүлтүүрээр дамжуулан интернэтийн агуулгад хандах хандалтыг хянах чиглэлээр зарим орнуудад батлан хэрэгжүүлж байгаа хууль тогтоомжийн эрх зүйн үр дагаврыг харьцуулан судалсан байна. Уг судалгааны зорилго нь веб хөтчүүдийг хянагч субьектууд болон блоклогдсон, хаагдсан сайтуудын талаар эмпирик мэдээлэл цуглуулж, эдгээр өгөгдлийн хууль ёсны үр дагаврыг судлахад чиглэгдсэн.

Судалгаанаас үзэхэд, дэлхийн улс орнуудын Засгийн газрууд үндэсний аюулгүй байдал, олон нийтийн хэм хэмжээний стандартыг хангах зэрэг олон шалтгаан, үндэслэл гаргах замаар интернэтийн орчинд шүүлтүүр тавих хүсэл эрмэлзэлтэй байдаг. Гэвч шүүлтүүрийн дэглэм тогтоох нь хүний эрх, эрх чөлөө, олон улсын эрх зүйн хэм хэмжээ, интернэт орчны засаглал зэрэг олон асуудлыг хөндөж, зарим талаар зөрчил үүсгэж байдаг тул интернэтийн орчинд цензур тогтоох хяналтын механизм харьцангуй цөөн, түгээмэл биш байна. Дэлхий даяар хариуцлагатай, үр нөлөөтэй харилцаа холбооны системийг хөгжүүлэхийн төлөө зорьж байгаа энэ цаг үед цахим орчны ил тод, хариуцлагатай, хүртээмжтэй байдлыг хангах асуудал юуны өмнө чухлаар тавигдаж байна.

Интернэтийн агуулгыг ямар нэг байдлаар цензурддаг орнуудад ихэвчлэн иргэдийнхээ үзэх боломжтой веб сайтуудыг хязгаарладаг байна. Иймээс хэрвээ интернэт шүүлтүүрийн асуудлыг хөндөн ярьж байгаа бол мэдээлэл, харилцаа холбооны технологийн салбарын ажилтнууд, бодлого боловсруулагчдын зүгээс уг арга хэмжээний үр дагавар асар их бөгөөд өргөн цар хүрээтэй гэдгийг анхаарч үзэхийг судлаачид зөвлөж байна.

Иймд судалгааны явцад дараах асуудлуудыг тодруулан авч үзлээ. Үүнд:

- Интернэт орчинд хэн шүүлтүүр тавьдаг вэ?
- Интернэтийн орчинд ямар төрлийн мэдээллийн агуулгыг шүүдэг вэ?
- Шүүлтүүрийг хэрхэн тавьдаг вэ?
- Тухайн орны иргэд интернэт орчинд шүүлтүүр тавьсан тухай хэр зэрэг мэдлэг, мэдээлэлтэй байдаг вэ?
- Иргэд интернэт орчинд шүүлтүүр тавьсан тухай мэдээллийг хэрхэн олж авах боломжтой байдаг вэ?

Судалгаанд авагдсан орнуудад ямар эрх зүйн үндэслэлээр, ямар эрх мэдлийн хүрээнд интернэтийг шүүдэг вэ? Хэрэв интернэт шүүлтүүр хэрэглэдэг бол интернэтийн агуулгыг цензурт оруулахад ямар нэгэн хязгаарлалт байдаг уу? Эрх зүйн орчны хүрээнд энэ асуудлыг хэрхэн хуульчилж байгаа вэ? гэх мэт практик асуудлуудыг авч үзсэн болно.

**Интернэт орчинд хэн шүүлтүүр тавьдаг вэ?**

Эрх зүйн шинжилгээний үр дүн нь тухайн үйлдлийг хэн хийхээс ихээхэн хамаардаг. Хэрэгжүүлэгч тал нь төр байх уу, хувийн хэвшлийн оролцогч байх уу гэдгээс хамаарч асуудалд ялгаатай хандах шаардлага бий болдог.

### 1.1 Төрийн шүүлтүүр: Засгийн газар

Интернэт орчныг төрөөс буюу засгийн газраас шүүх асуудал сүүлийн үед түгээмэл болж байна. Холбооны улсуудын бараг бүх муж, тэр дундаа ардчилсан зарчим, иргэний эрх чөлөөг эрхэмлэдэг улс орнууд ч гэсэн ямар нэгэн байдлаар интернэтийн агуулгыг шүүж, цензурдах сонирхолтой байх бөгөөд шүүлтүүрийн байршил, тоо хэмжээ, хэрэгжүүлж буй арга нь өөр хоорондоо ялгаатай байна. Тухайлбал, АНУ-д интернэтийн шүүлтийг ихэвчлэн Засгийн газрын бодлогод “харшлах ашиг сонирхол"-ыг илрүүлэх зорилгоор сургуулийн орчин, номын санд хийхээр зохицуулсан бол Хятад, Саудын Араб, Иран, Сингапур, Бирм болон ТУХН-ийн орнууд, Азийн зарим орнуудад ихэвчлэн иргэний эрх, эрх чөлөөг хязгаарлах байдлаар илүү өргөн хүрээтэй хийдэг байна. Тухайлбал, тодорхой веб сайт руу нэвтрэхийг хориглох, цахим шуудангийн урсгалыг хаах, дахин чиглүүлэх, эсвэл хэрэглэгчийн хүссэнээс өөр хайлтын илэрцүүдийг гаргах гэх мэт.

Ардчилсан орнуудаас Австрали улс шүүлтүүрийг практикт өргөн хэрэглэдэг. Австралийн засгийн газраас 2000 онд хууль баталж, 18-аас доош насны хүмүүсийн "сэтгэл санааг цочроох, хор хөнөөлтэй" гэж үзсэн контентыг серверээсээ устгахыг шаардсан. Хэрэгжилтийн хувьд, Австралийн иргэд ямар нэгэн хориглох программ авч ашиглах шаардлагагүй бөгөөд хувийн компаниуд шүүлтүүртээ тодорхой контентуудыг нэмж оруулах замаар шийдвэрлэхийг зөвлөжээ. Энэ хууль нь зөвхөн тухайн улсын дотоодод байршуулсан контентод үйлчлэх ёстой гэдгээрээ Хятад гэх мэтийн хатуу хориглолт хийдэг орнуудад мөрддөг блоклох схемээс ялгаатай байна. Гэсэн хэдий ч энэхүү хязгаарлалт нь ардчилсан улс орны хувьд Австрали улс иргэдийнхээ интернэтэд нэвтрэх эрхийг хязгаарлаж, дэлхийн өнцөг булан бүрд хэрэглэгчдэд хүргэж байгаа интернэтийн материалыг үзэх эрхийг нь хязгаарлах идэвхтэй оролдлого хийж байна гэсэн шүүмжийг дагуулж байна.

### 1.2 Хувийн шүүлтүүр: Компаниуд

Хувийн компаниуд ихэвчлэн интернэтийн шүүлтүүр тавьдаг. Засгийн газраас шүүлтүүр тавихыг үүрэг болгосон тохиолдолд төрийн өмчит интернэтийн үйлчилгээ үзүүлэгч компани энэ удирдамжийг хэрэгжүүлж байна. Бусад тохиолдолд засгийн газраас хувийн компаниудтай гэрээ байгуулан бодлогоо хэрэгжүүлдэг. Интернэтийн үйлчилгээ үзүүлэгч компаниуд нь шүүлтүүр тавихыг хүсэж байгаа тухайн улсад үйл ажиллагаа явуулдаггүй гадны компани байлаа ч гэсэн янз бүрийн ашиг сонирхлоор, тухайлбал санхүүгийн ашиг олох, интернэтийн үйлчилгээ үзүүлэх тусгай зөвшөөрөл авах гэх мэт шалтгааны улмаас эзэн орны засгийн газрын хүслийг биелүүлж ажилладаг тохиолдол байна.

Жишээ нь, 2001 онд дэлхийн хамгийн алдартай хайлтын систем болох Google компани Франц, Германы Засгийн газраас гаргасан хүсэлтийн дагуу Google хайлтын системийн орон нутгийн хувилбарыг холбогдох мужуудад http://www.google.fr/ болон /www.google.de/ хаягаар байршуулж, хайлтын системээс "нацистыг дэмжигч" эсвэл арьс өнгөөр ялгаварлан гадуурхах зарим сайтуудыг устгасан. Франц, Германы засгийн газар эдгээр веб сайтад хандах хандалтыг тодорхой хориглоогүй ч Google компанитай тохиролцож хасалт хийлгэснээр хэрэглэгчдээс холбогдох мэдээллийг нууж, Google-ийг 2 улсын засгийн газрын тухайд бараг шүүлтүүр болгон ашигласан байна.

Зарим хувийн компаниуд хэрэглэгчийг тодорхой веб сайт руу нэвтрэхийг хориглодог программ хангамж үйлдвэрлэдэг. Энэ шүүлтүүр нь бүрэн хувийн зориулалтаар ашиглагддаг бөгөөд бага насны хүүхдүүдийг хориотой мэдээлэлд хандахаас хамгаалах зорилготой хувь хүмүүс гэрийн хэрэгцээндээ зориулан компаниас худалдан авдаг шүүлтүүрийн программ юм. Тухайлбал, АНУ-ын хэд хэдэн муж улсад эдгээр программ хангамжийг ашигладаг бөгөөд ихэнхийг нь АНУ-ын компаниуд үйлдвэрлэдэг.

Засгийн газрын хувьд, хувийн шүүлтүүрийн програмыг ашиглахгүй ч гэсэн хувийн программ хангамжийн компаниудаар тодорхой зорилго бүхий шүүлтүүрийг автоматжуулах захиалгат ажлыг аутсорсингоор хийлгэдэг туршлага зарим оронд байна. Тухайлбал, Саудын Арабын Вант улс нь Secure Computing-ийн SmartFilter программ хангамжийг ашиглан порнограф  гэх мэтийн зохисгүй контент руу нэвтрэхийг хориглодог.

## 2. Шүүлтүүрийн дэглэм ба холбогдох хууль, журам

Шүүлтүүрийн дэглэмийн 2 үндсэн бүрэлдэхүүн хэсэг нь I) тодорхой мэдээллийг хаах үндэслэл тодорхой байх, II) шүүлтүүр тавихтай холбоотой багц хууль тогтоомжийг батлан гаргасан байх явдал юм.

### *2.1 Шүүлтүүр хийх хэрэгцээ шаардлага ба хууль тогтоомжийн үндэслэл*

Шүүлтүүр хийх эхний нийтлэг үндэслэл нь “*ёс зүйн”* болон *“олон нийтийн стандарт”* хэм хэмжээг сахиулах, хоёрдугаар үндэслэл нь "үндэсний аюулгүй байдлыг хангах" хэрэгцээ шаардлага бөгөөд үүгээр шүүлт хийх тухай хууль тогтоомжийг батлан гаргасан ихэнх орнууд эрх зүйн үндэслэлээ зөвтгөдөг.

#### *2.1.1 Олон нийтийн стандарт хэм хэмжээг сахиулах*

Интернэт нь олон төрлийн мэдээллийг хялбар бөгөөд чөлөөтэй үзэх боломжийг олгодог учраас зарим үзэгчдийн хувьд ёс суртахууны уур хилэн хөдлөх, айдас төрөх, иргэдийн соёлд сөргөөр нөлөөлөх магадлалтай гэж үзсэн ийм төрлийн контентын хандалтыг устгах буюу хориглох замаар улс орнууд олон нийтийн стандарт хэм хэмжээг хангахыг эрмэлздэг. Ихэнх тохиолдолд хүүхдүүд үүнд ихээр өртдөг тул  насанд хүрээгүй хүүхдүүдийг садар самуун контентод нэвтрэхийг хориглоход зарим орнууд гол анхаарлаа хандуулдаг.

Ёс суртахууныг эрхэмлэх хүчин чармайлт нь улс орон бүрд янз бүр байдаг бөгөөд үүнийг "зохисгүй байдал", "садар самуун" гэсэн хууль, эрх зүйн ойлголтуудаар илэрхийлдэг. Шүүлтүүрийн дэглэмийг дэмждэг орны хуулиудад эдгээр тодорхойлолтын хүрээнд юуг авч үзэх вэ гэдгийг ялгаатай байдлаар тусгасан байна. Тухайлбал, БНСУ-д хакердахтай холбоотой контентыг хориглосон байдаг бол, Ирактын барьцаалагдсан Солонгос хүний толгойг аймшигт хэрцгийгээр таслан авч буй бичлэгийг хаахыг орон нутгийн интернэт үйлчилгээ үзүүлэгчид тушаажээ. Тэгвэл Энэтхэгийн хууль тогтоомжоор "давж заалдсан" сайтуудыг хаасан байдаг бол Австралийн хуулиар зохистой ашиг сонирхолд нийцүүлэн “гэмт хэрэг, хар тамхины хэрэглээ”-ний талаарх мэдээлэл агуулсан сайтуудыг хориглодог байна.

Олон нийтийн стандартыг сахин хамгаалах төрийн хүчин чармайлт нь порнограф, хүчирхийллийн контентыг хориглохоос авхуулаад шашны болон улс

төрийн мэдээ, материалыг хянахад чиглэгдэж байна. Тухайлбал, Египет Улсад ерөнхийлөгчөө шүүмжилсэн интернэт агуулгыг хориглосон бол Узбекистан Улсад мөн ерөнхийлөгчийг шүүмжилсэн, эсвэл шашны хэт даврагч үзэлд тулгуурласан материалд хандахыг хориглодог. Улс орнуудад олон нийтийн стандарт хэм хэмжээний тодорхойлолт, ил тод байдал харилцан адилгүй байна.

### *2.1.2.Үндэсний аюулгүй байдлыг хангах*

Интернэт шүүлтүүр тавих хоёр дахь гол үндэслэл нь *үндэсний аюулгүй байдал* юм. 2001 оны 9-р сарын 11-нд АНУ-д террорист халдлага болсны дараагаар хэд хэдэн муж улсад интернэтийн агуулгад илүү их хязгаарлалт тавих болсон. Учир нь алан хядагчид хоорондоо харилцаа холбоо тогтоохын тулд интернэт сүлжээг ашигласан, цаашид ийм эрсдэл гарч болзошгүй гэж үзсэн учраас эрсдэлийг бууруулах арга хэмжээний хүрээнд дээрх үндэслэлд түлхүү анхаарах болсон.

Сүүлийн үеийн чиг хандлагаас харахад улс орны засгийн газрууд иргэдийнхээ үзэж байгаа интернэтийн агуулгыг хянах, цензур тавихад чиглэсэн хууль тогтоомжуудыг нэлээд батлах болсон. Ялангуяа тоталитар дэглэмтэй, ардчилал бага хөгжсөн орнуудад үндэсний аюулгүй байдлыг хадгалахын тулд ийм цензур зайлшгүй шаардлагатай гэж үзэн интернэтийг илүү өргөнөөр шүүж байна. Жишээ нь, Хятадад үндэсний аюулгүй байдлыг хамгаалах зорилгоор "үндэсний эв нэгдэл"-д заналхийлсэн үг хэллэг ашиглахыг хориглодог. Бирм, Египет, Малайз Улсад эрх баригч намыг шүүмжилсэн аливаа контентыг хориглодог бол Либери Улсад "Либерийн эсрэг мэдээлэл" агуулсан веб сайтуудыг хаасан, Зимбабве Улсад " аюултай байдал, цөхрөл төрүүлэх" аливаа контентыг нийтэлсэн гадаадын аливаа сайтыг оруулахгүй гэх мэтчилэн хуульчилсан.

### *2.2 Шүүлтүүр тогтоох эрх зүйн орчин, хууль тогтоомжууд*

Улс орнуудад контентын шүүлтүүрийн дэглэм тогтоох, хэрэгжүүлэхтэй холбоотой бодлого, эрх зүйн орчин харилцан адилгүй байдаг. Зарим орон, муж улсуудад интернэтэд зориулсан тусгайлсан зохицуулалтыг ашигладаг. Жишээлбэл, Хятад Улсын интернэтэд нэвтрэх эрхийн хязгаарлалтыг хуулиар тогтоосон байхаас гадна засгийн газар болон интернэтийн үйлчилгээ үзүүлэгч провайдер (ISP) компани хоорондоо байгуулсан гэрээгээр зохицуулдаг байна. Хятадад ердөө 9 (ISP) интернэтийн үйлчилгээ үзүүлэх тусгай зөвшөөрөлтэй компани байдаг бөгөөд энэ нь засгийн газар интернэт орчныг хяналтдаа байлгахад хялбар болгодог байна. Хятад Улс Google болон бусад хайлтын систем дахь илэрцийн үр дүнг хязгаарласан бөгөөд нийт 60 гаруй хууль тогтоомжоор веб хэрэглэгчдийн ашиглах боломжтой контентыг хязгаарласан байдаг. Хууль тогтоомжид ямар агуулгыг шүүх, ямар зөвшөөрлөөр шүүх талаар тодорхой заагаагүй, энэ талаар ямар нэгэн стандарт тогтоогоогүй.

Тэгвэл Бирм зэрэг улсад интернэтийн агуулгыг хянахын тулд хэвлэл мэдээллийн хэрэгслийг зохицуулах ерөнхий хууль тогтоомжийг ашигладаг бол Энэтхэгт Харилцаа холбооны конвергенцийн тухай хуулиар мэдээллийн хэрэгслийн төрлөөс үл хамааран улсын хэмжээний бүх харилцаа холбооны агуулга, дамжуулалтыг өргөн хүрээтэй зохицуулдаг.

Зарим улс орнуудад интернэтийн хандалт болон агуулгын олон нийтэд үзүүлэх үр нөлөөг харгалзан тогтсон үйл ажиллагаа явуулж байгаа хэвлэл мэдээллийн хэрэгслүүдэд анхаарал хандуулдаг. Жишээлбэл, Канад Улсын өргөн нэвтрүүлгийн тогтсон журамд хөндлөнгөөс орж ирж буй видеоны урсгалыг хязгаарладаг. Зарим мужууд ихэвчлэн төрийн мэдэлд байдаг монопол харилцаа холбооны үйлчилгээ үзүүлэгчдийн эсэргүүцлийг харгалзан Voice Over Internet Protocol (VoIP)-оор дамжих интернэт утасны холболтыг хязгаарладаг.

Дүгнэж хэлбэл, улс орнууд интернэтийн агуулгыг хязгаарлахын тулд ихэвчлэн ерөнхий хууль тогтоомжийг ашигладаг. Тухайлбал, хэд хэдэн улс орнууд Оюуны өмчийн тухай хуулиар зугаа цэнгэлээс авхуулаад мэдээ хүртэлх контентыг хязгаарлахын тулд зохиогчийн эрхийн дэглэмийг ашигладаг. Зарим орнуудад зарим веб сайт руу нэвтрэхээс урьдчилан сэргийлэхийн тулд гүтгэлэг, гүтгэлгийг хориглосон хуулийг ашигладаг. Учир нь тэд улс төрийн нам, төрийн зүтгэлтнүүдийг гутаан доромжилсон мэдээллийг түлхүү нийтэлснээр огцруулах үндэслэл болж болзошгүй гэж үздэг. Тухайлбал, 2001 оны 10-р сарын 26-нд АНУ-ын Конгрессоос “АНУ-ын эх орончдын тухай” хууль баталсан нь АНУ-ын засгийн газрын албан тушаалтнуудын зүгээс хэрэглэгчийн интернэтийн урсгалыг хянахад хялбар болгосон.[5] Интернэтийн тусгайлсан дүрэм журам байхгүй байсан ч гэсэн засгийн газрууд интернэтийн дефакто цензурийг бий болгохын тулд засгийн газрын эсрэг үйл ажиллагаа явуулахыг хориглосон хуулийн зохицуулалтыг ашиглаж байна.

## 3. Интернэт шүүлтүүрийн эрх зүйн орчны тулгамдсан асуудлууд

*Иргэний эрх, эрх чөлөөнд нөлөөлөх нь : Үг хэлэх, үзэл бодлоо илэрхийлэх, хэвлэн нийтлэх, хувийн нууц, шашин шүтлэг, холбоо нийгэмлэг гэх мэт.*

Интернэт шүүлтүүр нь иргэний хууль ёсны эрх, эрх чөлөөг зөрчих эрсдэлтэй байдаг. Ихэнх улс оронд иргэд үзэл бодлоо илэрхийлэх (хувь хүн эсвэл хэвлэл мэдээллийн ажилтны хувьд), хувийн нууц хадгалах, шашин шүтэх, эвлэлдэн нэгдэх эрх чөлөөтэй байдаг. Иргэний эрх чөлөөний мөн чанар, цар хүрээ улс орнуудад ялгаатай. Тухайлбал, АНУ-д иргэний эрх чөлөө нь хүчтэй байдаг бол зарим улс оронд иргэдийн эрх чөлөөг хамгаалах хамгаалалт огт байдаггүй. Иргэний эрх чөлөөний хамгаалалт нь уг харилцаанд оролцогч талуудын хүсэл зоригоос ихээхэн шалтгаална. АНУ-д “Харилцаа холбооны ёс зүйн тухай” [6] хуулиар энэ асуудлыг зохицуулж байна.

Шүүлтүүрийн дэглэм тогтоож мэдээллийг блоклох нь үг хэлэх, үзэл бодлоо илэрхийлэх эрх чөлөөг дэмждэг хүмүүс болон интернэт контентын сөрөг нөлөөнд санаа зовдог хүмүүсийн хувьд харьцангуй өөр өөр хандлагаар илэрдэг. Зарим үед шүүхээс тодорхой зорилготойгоор иргэний эрх чөлөөг хязгаарлах шийдвэр гаргах ч тохиолдол байна. Жишээлбэл, АНУ-ын Дээд шүүхээс Холбооны улсын санхүүгийн дэмжлэг авахын тулд нийтийн номын сангууд дахь "насанд хүрээгүй хүүхдүүдэд хортой" материалыг шүүх интернэт шүүлтүүрийг баталсан

[5] Bill Summary & Status, USA PATRIOT Act http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.03162

[6] *http://www.epic.org/free_speech/CDA/ (хамгийн сүүлд 2002 оны 2-р сарын 2-нд шинэчлэгдсэн) цахим нууцлалын мэдээллийн төв, Харилцаа холбооны ёс зүйн акт*

байдаг.  Гол асуудал нь шүүлтүүрийн программ хангамжууд тухайлсан бодлого, зорилгод хамааралгүй маш их материалыг автоматаар хааж, алга болгож байгаа нь стандартыг зөрчиж  байгаа тул шүүлтүүрийн одоогийн технологи ихээхэн шүүмжлэл дагуулж байгаа юм.

### *3.1 Шүүхийн харьяалал*

Хууль зүйн хувьд харьяалал гэдэг нь тухайн улс орон, бүс нутаг болон асуудлыг зохицуулах, хянах эрх бүхий этгээдийн эрх мэдэл, хүсэл эрмэлзлийн тухай асуудал юм. Уламжлал ёсоор улс орон, муж улсууд өөрсдийн эзэмшдэг газар нутаг, оршин суугч иргэдийн бүрэн эрхт байдал, хил хязгаарын харьяалалтай байдаг. Иймээс улс орнууд өөрсдийн харьяаллын хүрээнд эрх мэдлийн хяналт тогтоохын тулд хууль тогтоомж баталж хэрэгжүүлдэг. Гэвч улс орны хил хязгаарыг давсан үйл ажиллагаа интернэт орчинд явагдаж байдаг. Жишээлбэл, АНУ-ын иргэн Японд, Бразилд хүмүүсийг хохироох үйлдэл хийвэл аль улсын харьяалалд хамаарах вэ?

Тэгвэл интернэт шүүлтүүрийн тухайд үүн дээр асуудал үүсдэг. Интернэт шүүлтүүртэй холбоотой асуудлаар тухайн муж, улс өөрийн газарзүйн хил хязгаарын хүрээнд сүлжээгээр дамжиж буй пакетуудтай холбоотой хэрэг маргааныг шүүхээс гадна өөрийн нутаг дэвсгэрийн гадна дэлхий даяар интернэт сүлжээнд холбогдож буй иргэдийн харилцааг зохицуулж, нөлөөлөх шаардлагатай тулгардаг. Жишээ нь, цахим шууданг шүүлтүүртэй орны иргэнээс шүүлтүүргүй орны иргэнд явуулж болно, тэгвэл энэ тохиолдолд шүүлтүүр тавьсан орны зүгээс харилцагч 2 улсын иргэний хооронд мэдээлэл солилцох  үйл ажиллагааны аль алинд нь нөлөөлж, хязгаарлалт тавьж байна гэсэн үг. Шүүлтүүр нь тухайн улсын хилийн дотор тодорхой веб сайт руу нэвтрэхийг хааж, эсвэл хил доторх сүлжээний урсгалыг өөрчлөхдөө харьяат бус хүмүүсийг ч нэвтрэхийг хязгаарлаж болзошгүй тул интернэтийн хяналт нь газарзүйн хувьд тархмал, олон улсын эрх ашгийг хөндөх үр дагавартай. Аль нэг улсын улс төрийн нам өөр улсын аль нэг намд хор хөнөөл учруулахуйц байдлаар интернэт ашиглалтын зөрчил үүсгэж болзошгүй учраас ийм төрлийн хэрэг маргааны харьяаллын асуудлыг зохицуулахын тулд 1) хувийн болон маргааны төрлийг шүүх эрх мэдлийн харьяаллыг тогтоох, 2) мөрдөх хууль эрх зүйн актын сонголт хийх, 3) хуулийг хэрэгжүүлэх гэсэн 3 үндсэн категорийн хүрээнд уг асуудлыг авч үздэг.

*Хувийн болон маргааны төрлийг шүүх эрх мэдлийн харьяаллын асуудал*

Шүүх эрх мэдлийн хүрээнд хууль ёсны маргааны хариуцагчийг тогтоох (хувийн харьяалал), хянах шаардлагатай маргааны төрлийг тогтоох (субъектийн харьяалал) гэсэн хоёр чиглэлээр харьяаллын асуудлыг авч үздэг.

Хувийн харьяалал гэдэг нь тухайн хүн тухайн орны төрийн зохицуулалтад захирагдах ёстой эсэх, төрөөс өөрийн бүрэн эрхээ үр дүнтэй хэрэгжүүлэх мандатын эрхтэй эсэх зэрэг асуудлуудыг хамардаг. Субъектийн харьяаллаар хянах нь байгууллагын чадамжаас ихээхэн хамаарна, тухайлбал тухайн шүүх хэргийг хянан шийдэх эрхтэй эсэх, институцийн хувьд тухайн маргааныг хянан шийдвэрлэхэд шаардлагатай мэдлэг чадвартай эсэх гэх мэт.

Интернэтийн зохицуулалт нь ялангуяа хувийн харьяаллын дагуу шүүх эрх мэдлийг хэрэгжүүлэхэд чухал үүрэтэй байна.

***Кейс 1.*** *Австралийн бизнесмен Жозеф Гутник АНУ-ын Dow Jones хэвлэлийн компанийг Австралид шүүхэд өгсөн. Учир нь Dow Jones Barron's сэтгүүлийн онлайн дугаарт түүнийг шүүмжилсэн нийтлэл гарсан бөгөөд түүнийг гүтгэсэн гэж Гутник мэдэгджээ. Австралийн Дээд шүүхээс Dow Jones-ын Barron's сэтгүүлийг онлайн захиалгаар Австраличуудад худалдсан, мөн Гутник Австралийн иргэншилтэй зэргийг үндэслэн харьяаллыг нотолсон.*

***Кейс 2.*** *Францын дээд шүүхээс АНУ-д төвтэй Yahoo! компани Францын хуулийг зөрчиж Франц иргэдийг нацистын эд зүйлсийн дуудлага худалдаанд оролцохыг зөвшөөрсөн агуулгатай мэдээлэл түгээсэн хэрэгт Францын шүүхээс Yahoo! компаниас Францын иргэдийг хориотой нацист контент бүхий сайт руу нэвтрэхээс хамгаалах техникийн боломжит бүх арга хэмжээ авахыг шаардаж, компанийг 10000 франкаар торгох шийдвэр гаргасан. Үүний эсрэг АНУ-ын Холбооны давж заалдах шатны шүүхээс гаргасан шийдвэрт Yahoo! компанийн кэйс дээр ажилласан Францын 2 компани америкийн талтай хангалттай хэмжээнд хамтарч ажиллаагүй, энэ асуудлыг шийдвэрлэхэд оролцох хэмжээний эрх мэдэлтэй компани биш гэсэн үндэслэлээр уг шийдвэрийг хэрэгжүүлэхээс татгалзсан.*

Шүүхийн харьяалал нь нэхэмжлэл гаргах зарим боломжийг хязгаарладаг бөгөөд ялангуяа гадаадын засгийн газрын интернэтийн шүүлтүүрт өртсөн талын хувьд хууль эрх зүйн боломж нь хязгаарлагдмал байдаг. Учир нь тухайн муж, улсын шүүхэд нэхэмжлэл гаргах, эсхүл өөрийн харьяаллын дагуу шүүхэд нэхэмжлэл гаргахын аль нэгийг сонгох ёстой болдог. Гадаад орны шүүхээр шийдвэрлүүлэх тохиолдолд тухайн орны хуулийг баримтлах тул амжилтгүй болох магадлалтай.

Интернэттэй холбоотой асуудлаар улс хооронд, муж улсуудын хооронд гарч буй эрх зүйн зөрчил нь хууль, эрх зүйн болон худалдааны маргаанд хүргэж болзошгүй юм. Жишээлбэл, Калифорни мужийн холбооны дүүргийн шүүх Yahoo!-ийн эсрэг Францын асуудлаар шүүхийн шийдвэр гаргасан хэдий ч АНУ-ын Үндсэн хуулиар иргэдийн үг хэлэх эрхийг хамгаалсан учир Францад хориотой асуудал хэдий ч АНУ-д зөвшөөрөгддөг үйл ажиллагаа байсан. Иймээс АНУ-ын шүүхүүд Францын байгууллагуудыг АНУ-д хувийн харьяалалгүй гэж үзэн давж заалдах шатны шүүхээс шийдвэрийг хүчингүй болгосон. Учир нь тэд Yahoo!-ийн Америк дахь үйл ажиллагааны эсрэг Францын шүүхийн шийдвэрийг биелүүлэх боломжгүй гэж үзсэн. Энэ мэтээр улс, муж хооронд шүүхийн шийдвэр, түүнийг хэрэгжүүлэхтэй холбоотой асуудлаар зөрчил үүсэх магадлалтай. Зөрчлийг олон улсын зохицуулах байгууллага, эсвэл улс хоорондын хэлэлцээр шийдвэрлэж болох авч харьяаллаас үүдэн өөр өөр үр дүнд хүргэж болзошгүй.

*Хуулийн сонголт*

Хуулийн сонголт (олон улсын хувийн эрх зүй гэж нэрлэдэг) гэдэг нь маргаан, зөрчилдөөнийг аль харьяаллын хуулиар хянан шийдвэрлэх ёстойг шийдэх тухай асуудал юм. Энэ нь хувь хүний болон субъектийн харьяаллаас

хамаарахгүй бөгөөд улс орон, муж улс хэргийг дотооддоо хянан шийдэж болох ч өөр улсын хуулийг хэрэглэх боломжтой гэсэн үг. Нэгээс олон харьяаллын хууль хэрэглэх боломжтой тохиолдолд шүүхүүд ихэвчлэн хэлцэл хийх, эсхүл хэрэг маргаан нь аль харьяалалд хамгийн чухал хамааралтай болохыг тодорхойлохыг оролддог.

Контент нийлүүлэгч, интернэтийн үйлчилгээ үзүүлэгч болон хэрэглэгчийн аль аль нь эрх мэдлийнхээ хүрээнд нэхэмжлэл гаргаж болох ч интернэтэд суурилсан маргааны хувьд асуудлыг шийдэхэд хэцүү байдаг. Тиймээс улс орнууд энэ асуудлыг олон талт хэлэлцээрээр зохицуулахыг оролдож байна. Жишээлбэл, Европын Холбооны Брюсселийн журмаар Европын холбооны ихэнх орнуудын шийдвэрийг зохицуулдаг.

Гэвч бодит байдал дээр улс орнууд маргааныг шийдвэрлэхдээ өөрсдийн хууль тогтоомжийг хэрэгжүүлэхийг илүүд үздэг. Маргааныг шүүхэд төрийн бүрэн эрхт байдлын үндсэн цөм 2 асуудлыг анхаарах ёстой. 1) засгийн газраас харилцаа холбооны дэд бүтцийг зохицуулах эрх мэдэл, 2) контентыг хориглох үндэслэлийг тогтоосон соёлын стандарт. Эдгээрийг харгалзан улс орнууд аль улсын, ямар хууль хэрэглэхээ тогтоодог бөгөөд олон улсын хувийн эрх зүйн актыг баримтлах уу, маргааны асуудал нь өөрийн дотоодын хууль тогтоомжоор шийдэгдэх давуу хамааралтай байна уу гэдгийг ялгаж салгаж тогтоох нь чухал.

### *3.2 Шүүхийн шийдвэрийг хэрэгжүүлэх*

Шүүхийн шийдвэрийг хэрэгжүүлэх нь тухай улсын шүүхийн шийдвэр биелүүлэх хараат бус байдал, чадавхаас хамаарна. Шийдвэр хэрэгжихгүй байна гэдэг нь тухайн улс орон, мужийн төр засаг болон нэхэмжлэгчийн эрхийг хамгаалах үнэ цэнтэй шийдвэр хэвээр байх боловч ерөнхийдөө шүүгдэгчийн зан үйлийг өөрчлөх эсвэл дуулгавартай байхыг албадах ёсгүй гэж үздэг. Тиймээс Yahoo! компанитай холбоотой АНУ-ын холбооны дүүргийн шүүхийн шийдвэр нь Францын нутаг дэвсгэрийн хүрээнд зохисгүй контент тогтоох эрх мэдлийг хүндэтгэсэн боловч Yahoo! нь америкийн компани учир өөрийн өмчийн эсрэг шийдвэр гаргахгүй гэдэг үүднээс Францын шүүхийн шийдвэрийг хэрэгжүүлэхээс татгалзсан байх жишээтэй.

Уламжлал ёсоор шүүхийн шийдвэр гүйцэтгэхийн тулд тухайн улс орон, муж нь хариуцагч болон түүний хөрөнгийг шууд хянах эрхтэй байх, эсхүл өөр муж, улстай шүүхийн шийдвэр заавал биелүүлэх тусгайлсан гэрээтэй байх шаардлагатай болдог. Тухайлбал, олон улсын хувийн эрх зүйн гаалийн шүүхээс иргэний болон арилжааны асуудлаар гаргасан шүүхийн шийдвэр болон гадаад орны шүүхийн шийдвэрийн хэрэгжилтийг хангах асуудлыг зохицуулах конвенцын төслийг боловсруулсан. Энэхүү конвенц батлагдсанаар Америкийн муж улсууд бие биеийнхээ гаргасан шийдвэрийг заавал биелүүлэх үүрэг хүлээх бөгөөд ийм зохицуулалт үгүй тохиолдолд аль нэг муж улс өөрийн хилээс гадуур гаргасан шийдвэрийг заавал хэрэгжүүлэх үүрэг хүлээхгүй гэсэн үг юм.

Гэсэн хэдий ч шүүлтүүр тогтоох нь өөрөө эрх мэдлээ хэрэгжүүлэх боломжийг бий болгодог гэж үздэг. Төрийн зүгээс интернэтийн дэд бүтэц, интернэтийн үйлчилгээ үзүүлэгч, контент нийлүүлэгч болон хэрэглэгчдэд шүүлтээр дамжуулан хяналт тавьж, шийдвэрээ хэрэгжүүлэх хангалттай боломжийг эдэлж байдаг байна. Ерөнхийдөө, тухайн муж улсын газарзүйн хил

хязгаарт хариуцагч өөрөө болон компани, эд хөрөнгө нь харьяалагдахгүй үед албадлагын эрх мэдэл хязгаарлагддаг. Тэгвэл шүүлтүүр тавьснаар тухайн улс орон, муж харилцаа холбооны дэд бүтцэд нь нэвтрэх эрхийг хязгаарлах, хориглох замаар шийдвэрийн хэрэгжилтийг хангуулж чадна. Шийдвэрийг хэрэгжүүлэх нь шийтгэл биш, урьдчилан сэргийлэх арга хэмжээ байх ёстой.

Ялангуяа хөгжиж буй орнуудад үүнийг хэрэгжүүлэх боломжит цэг нь Интернэт солилцооны цэг (IXP-internet exchange point) юм. Интернэт солилцооны цэгүүд нь хэрэглэгчдэд интернэтийн мэдээллийг өөрийн улсын хил хязгаар дотор солилцох, ашиглах боломжийг олгож, үр ашгийг нэмэгдүүлж, зардлыг бууруулдаг. Олон интернэтийн үйлчилгээ үзүүлэгч (ISP)-тэй улс орнуудад IXP-г ашиглах нь үйлчилгээ үзүүлэгч болон хэрэглэгчдийн зардлыг бууруулах талтай. Тэгвэл хиймэл дагуулын антен (satellite dishes) ашиглаж интернэт холболт хийдэг орнууд АНУ, эсхүл Европт байрладаг интернэтийн үйлчилгээ үзүүлэгч компани руу хиймэл дагуулаар дамжуулан мэдээллийн урсгалыг чиглүүлэх замаар мэдээллийг тойруу замаар хүлээж авдаг. Жишээ нь, А улсаас В улс руу илгээсэн хэрэглэгчийн и-мэйл А улсын серверээс В улсын серверээр дамжин эзэндээ очдог гэх мэт. Тиймээс дотооддоо интернэтийн үйлчилгээний провайдергүй орны хувьд энэ нь харьцангуй өртөг зардал өндөртэй тусдаг байна.

Интернэтийн шүүлтүүр нь тухайн орны эрх баригчдын зүгээс эрх мэдлээ ашигтайгаар хэрэгжүүлэхэд нөлөө үзүүлэх талтай. Интернэт шүүлтүүрийн тусламжтайгаар улс төрийн нам, эрх баригчдын зүгээс хүсээгүй контентыг иргэдэд хүргэхээс сэргийлэх эрмэлзэлтэй байдаг. Нэг талаас төр нь иргэддээ хохирол учруулахаас урьдчилан сэргийлж, мэдээллийн цензур тогтоож байгаа мэт боловч нөгөө талаас иргэдийн интернэтийн контентыг ашиглах бодит боломжийг бууруулж, мэдээлэл авах, үзэл бодлоо илэрхийлэх гэх мэтийн эрхийг хөнддөг учраас төвөгтэй байдал үүсгэдэг.

### *3.3 Интернэтийн засаглал*

Интернэтийн засаглалын асуудал нь олон улсын байгууллага болон стандарт тогтоогч байгууллагуудаас үр ашигтай хяналтын системийг хөгжүүлэх хүрээнд улс орнууд болон интернэтийн үйлчилгээ үзүүлэгч провайдер компаниудыг хянах бие даасан этгээдийг байгуулахтай холбоотой гарч ирсэн. 2003 оны 12-р сард болсон Мэдээллийн Нийгэмлэг (WSIS)-ийн дэлхийн дээд хэмжээний уулзалтаас интернэтийн засаглалын асуудлыг анх удаа олон улсын анхаарлын төвд оруулсан. Уг уулзалтаас домэйн нэрийн хуваарилалт, Internet Corporation for Assigned Names and Numbers (ICANN)-ийн бүтэц, зохион байгуулалтын асуудлаас эхлээд шүүлтүүр, спам, сүлжээний аюулгүй байдал болон бусад төвөгтэй, түгээмэл тохиолддог өргөн хүрээний асуудлууд руу анхаарал хандуулсан боловч тодорхой зөвшилцөлд хүрээгүй байна. Гэвч 2005 онд Тунист болсон WSIS-ийн дараагийн уулзалтын хооронд хүмүүс интернэтийн засаглалд анхаарлаа хандуулж эхэлсэн бөгөөд Женевийн WSIS уулзалтаас гаргасан зөвлөмжийн дагуу "үйл ажиллагаа явуулах" уриалга гаргасан байдаг. Интернэтийн засаглал нь интернэтийн шүүлтүүрийг бүхэлд нь хамарч, магадгүй дэлхийн хэмжээнд цензур тогтоох асуудлыг хөндөж болох ч найдвартай эмпирик судалгаанд үндэслэсэн мэтгэлцээний үндсэн дээр шийдэх асуудал байж болох юм гэж үзсэн.

### *3.4 Олон улсын эрх зүй*

Улс орнууд ихэвчлэн интернэтийн хууль болон зохицуулалт дээр суурилсан олон талт хэлэлцээрээр энэхүү харилцааг зохицуулдаг. Тухайлбал, худалдааны гэрээнд ихэвчлэн оюуны өмчтэй холбоотой заалтууд багтдаг хэдий ч интернэт шүүлтүүрийн асуудал ч үүнд хөндөгдөх талтай. Улс хоорондын чөлөөт худалдааны хэлэлцээрийн шаардлагуудыг тухайн улс орнуудын иргэд, хуулийн этгээдийн хооронд хийгдэж байгаа арилжааны гүйлгээнд шүүлтүүр хийх замаар зөрчиж болзошгүй бөгөөд үүнээс үүдэн практикт асуудал үүсэж болзошгүй юм. Мөн түүнчлэн зарим контентыг “эмзэг” ( ж/нь, CAPC гэх мэтийн веб-д суурилсан нийгмийн эрүүл мэндийн өргөн хүрээтэй асуудал) хэмээн үзэж блоклох нь олон улсын хүний эрхийн тухай хууль, конвенцид хамааралтай асуудал юм. Энэхүү нарийн төвөгтэй байдлаас болоод иргэдийнхээ интернэтийн хэрэглээнд системтэй хяналт тавьж байгаа үед  аль нэг компани, улс орныг хүний эрхийг зөрчигч  хэмээх ангилалд оруулж эхэлсэн. Олон улсын хүмүүнлэгийн эрх зүйн системийн хөгжлийн дараагийн үе шатанд харилцаа холбооны системд хүний эрхийг хамгаалах асуудлыг хөндөж ярьдаг болсон байна.

### *3.5 Харилцаа холбооны тухай хууль*

Олон улсын эрх зүйн нэгэн адил олон улсын  болон үндэсний харилцаа холбооны зохицуулалтын дэглэмүүд нь интернэтийн шүүлтүүртэй холбоотой. Өмнө нь  интернэт болон харилцаа холбооны системийг тусад нь авч үздэг байсан  ба харилцаа холбооны харилцааг өргөн хүрээнд, интернэтийн харилцаа зохицуулалт багатай явж ирсэн. Интернэтийн шүүлтүүр хэрэглэх практик нь харилцаа холбооны хууль тогтоомжийг зөрчих магадлал багатай ч харилцаа холбооны салбарын бодлого тодорхойлох, хууль тогтоомжийг батлан гаргахад тодорхой хамааралтай.

### *3.6 Бусад*

Интернэт шүүлтүүрийн хамгийн чухал код нь хууль эрх зүйн код биш харин компьютерын код юм. Интернэт шүүлтүүрийг ихэвчлэн хууль тогтоомж, зохицуулалтын акт, бодлогын дагуу практикт нэвтрүүлдэг боловч хамгийн гол нь программ хангамж юм. Программ хангамжийн код нь хууль ёсны түншийнхээ харьяаллын алдаанаас ангид, хэрэгжилт нь автомат бөгөөд онолын хувьд үнэмлэхүй юм. Улс орнууд код нэвтрүүлэхийн тулд холбогдох улс орон, муж улсуудтай гэрээ байгуулдаг. Хууль тогтоомжоор шүүлтүүрийн горимыг тойрч гарахыг хориглоно. Кодын хэлбэр, түүнчлэн нийгмийн хэм хэмжээ, арилжааны гүйлгээтэй холбоотой асуудал нь олон улсын хэмжээнд интернэтийн шүүлтүүр тавихтай холбоотой шийдвэрлэх, тулгамдсан асуудал болж байна.

## 4. Контент фильтерийн практик хэрэглээ

### *4.1 Контент фильтер гэж юу вэ?*

Контент фильтер буюу “агуулгын шүүлтүүр” гэдэг нь цахим шуудан эсвэл веб хуудас руу нэвтрэх эрхийг шалгах, зохисгүй мэдээллийг хасахыг хэлнэ. Контент шүүлтүүр хийх загварын шийдлүүд нь агуулгын хэв маягийг тогтоох, текстийн мөр болон зураг дээр ажиглалт хийсний үндсэн дээр программ хангамж

нь контентыг дамжуулах, эсэргүүцэх, эсхүл ямар нэгэн байдлаар блоклох, хориглох зэрэг үйлдлүүдийг хийнэ.

Агуулгын шүүлтүүр буюу веб контентын шүүлтүүр нь зохисгүй, доромжилсон, эсхүл эрсдэлтэй байж болзошгүй веб контентод хандах хандалтыг хянаж, хязгаарладаг шийдлүүдийн багц юм. Компаниуд “галт хана”-ын контент шүүлтүүрийг ашигладаг бол нийтлэг биш ч гэлээ гэрийн компьютер ашиглагчид контент шүүх шийдлүүдийг ашигладаг байна. Гэрийн нөхцөлд агуулгын шүүлтүүр тавьснаар бага насны хүүхдийг зохисгүй контентоос хамгаалдаг бол компаниудын тухайд тодорхой төрлийн контент руу нэвтрэх эрхийг хаах замаар шүүлтүүр тавьдаг. Тухайлбал, Redmond-based технологийн аварга компани нь системийн администраторуудад веб сайт руу хандах хандалтыг хянах, зохицуулах боломжийг олгодог веб контент шүүлтүүрийн функц бүхий хамгаалалтын нэгдсэн платформ болох Defender ATP-ийг өргөжүүлэн хөгжүүлсэн.[7]

Майкрософт компани 2020 онд Microsoft Defender Advanced Threat Protection (MDATP)-ийн нэг хэсэг болгон Веб контент шүүлтүүрийг санал болгож байгаагаа зарласан. Уг функцийг 2020 оны 1-р сард олон нийтэд танилцуулсан бөгөөд одоо хэрэглэгчдэдээ хүргэж байна.

Веб контент шүүлтүүрийн тусламжтайгаар системийн администраторууд тогтсон бодлогын хүрээнд эцсийн цэгүүдэд веб хандалтын протоколуудыг зааж өгөх боломжтой болсон. Мөн заасан агуулгын ангилалд тулгуурлан вебсайт руу хандах хандалтыг хянах, тохируулах боломжийг системийн хамгаалалтын багуудад олгодог байна.

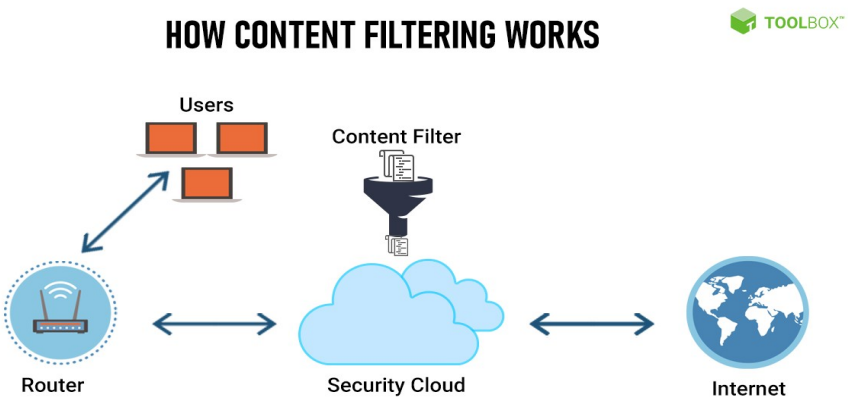
MDATP-ийн дагуу веб контентыг шүүх шүүлт нь Edge, Chrome, Firefox гэх мэт бүх гол хөтчүүд дээр ажилладаг бөгөөд агуулгыг блоклоход SmartScreen болон сүлжээний хамгаалалт зэрэг суурилуулсан веб шүүлтүүрийг ашигладаг.

### *4.2 Агуулгын шүүлтүүр хэрхэн ажилладаг вэ?*

Олон тооны тэргүүлэх интернэт “галт хана” нь агуулгын шүүлтүүрийг техник хангамж эсвэл программ хангамж болгон суулгасан функц болгон санал болгодог. Агуулгын шүүлтүүрийн давхар давуу тал нь кибер аюулгүй байдал, компанийн мэдээллийн системийг ашиглахтай холбоотой компанийн бодлогыг хэрэгжүүлэхэд чухал нөлөөтэй. Жишээлбэл, эдгээр шүүлтүүрүүд нь кибер аюулгүй байдлын үүднээс аюултай сайтууд болон компанийн бодлогын хүрээнд зохисгүй нийгмийн сүлжээний сайтуудыг хаах болно.

Зураг 1. Цахим шүүлтүүр хэрхэн ажилладаг талаарх схем

[7] https://www.spiceworks.com/it-security/security-general/news/microsoft-defender-atp-beefs-up-threat-detection-with-web-content-filtering/




Өнөөдрийн байдлаар корпорацууд хамгийн бага мэдээллийн гажилттай, аюулгүй ажлын байр бий болгохыг хичээж байна. Үүнд агуулгын шүүлтүүр чухал үүрэг гүйцэтгэдэг. Байгууллагын системийн бүрэн бүтэн байдлыг хангах, сахилга хариуцлагыг төлөвшүүлэх, ажилтнуудын аятай тухтай байдлыг хангахын тулд ажлын байран дээр зохисгүй, хууль бус контентыг ашиглахыг хязгаарлаж байна.

Тухайлбал, садар самууны агуулга нь ажлын орчныг бэлгийн дарамттай, дайсагнасан, доромжилсон өнгө аястай болгодог бол спам веб сайтууд нь ажлын
компьютерт хортой программ дамжуулах өндөр эрсдэлтэй байдаг. Хортой агуулгын бусад жишээнд ажилчдын аюулгүй байдлыг алдагдуулж болзошгүй үзэн ядсан, хүчирхийллийн агуулгатай вебсайтууд, ажилчдын бүтээмж, үр ашгийг бууруулах хандлагатай компанийн имиж, нийгмийн сүлжээний сайтууд багтана.

Агуулгын шүүлтүүрийн шийдлүүд нь ажлын байран дахь хортой вебсайт руу нэвтрэх эрхийг хааж, эдгээр асуудлуудыг тойрсон компанийн бодлого, зааг ялгааг тодорхой болгоход тусалдаг. Өөрөөр хэлбэл, хууль бус, зохисгүй контентыг байгууллагын зүгээс үл тэвчих хандлагыг харуулж байгаа юм.

### *4.3 Агуулгын шүүлтүүрийн сувгууд*

Агуулгын шүүлтүүрийг дараах сувгуудаар дамжуулан хийдэг. Тухайлбал:

**Имэйл:** Алсын зайнаас ажиллах үед ихэнх байгууллагуудын харилцааны үндсэн хэлбэр нь цахим шуудан юм. Имэйлүүд нь спам илгээгчдийн дайралтад ихээхэн өртдөг бөгөөд хортой программ болон бусад хүсээгүй контентыг хамгийн их магадлалтайгаар дамжуулах мэдээллийн хэрэгслүүдийн нэг юм. Агуулгын шүүлтүүр нь янз бүрийн аргаар имэйлийн аюулгүй байдлыг хангадаг бөгөөд эдгээр шийдлүүдийн нэг нь имэйлийн агуулгыг сканнердах юм. Хэрэв тодорхой үг, хэллэг, хавсралт, бусад зохисгүй контент илэрсэн бол имэйлийг хүлээн авагчийн хог хаягдлын хавтсанд байрлуулах, эсхүл "хүргэх боломжгүй" гэж тэмдэглээд буцаах шийдлийг тусгасан.

**Веб:** Интернэт бол дэлхий даяарх корпорацуудын амин сүнс бөгөөд контент шүүх шийдэл нь урьдчилан тодорхойлсон дүрмийн дагуу веб траффикийг шүүж компанийн нөөцийг аюулгүй байлгахад тусалдаг.

**Программын файлууд**: Бүх ажилчид технологийн мэдлэгтэй байдаггүй. Заримдаа ажилтан хортой программыг татаж аваад ажиллуулахыг оролдож болно. Агуулгын шүүлтүүр нь ийм программын файлуудыг хэрэглэгчийн систем

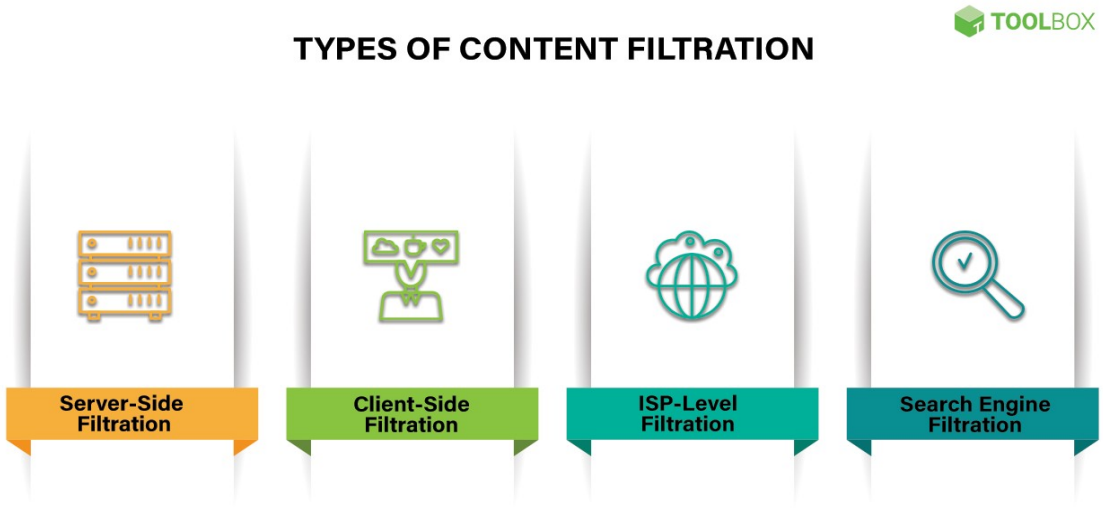
эсвэл компанийн сүлжээнд хор хөнөөл учруулахаас өмнө хаах зорилготой юм. Агуулгын шүүлтүүрийг ашиглахын гол зорилго нь тааламжгүй гэж үзэж болох контент руу нэвтрэх эрхийг хаах явдал юм. Ийм хязгаарлалт нь гэрийн хэрэглэгч спамыг блоклохоос эхлүүлээд улс үндэстний хэмжээнд хууль тогтоомжийг хэрэгжүүлэх, дагаж мөрдүүлэх засгийн газар хүртэлх бүх түвшинд хамаарна. Нийгэм, улс төр, ёс суртахууны асуудлуудыг оруулаад тооцвол контентын шүүлтүүрийн хамрах хүрээ өргөн бөгөөд эдгээр шийдлүүд нь хувийн, байгууллагын болон үндэсний цахим аюулгүй байдлыг хангахад чиглэсэн томоохон алхам болно хэмээн үздэг байна.

### *4.4 Агуулгын шүүлтүүрийн төрлүүд*

"Мэдээллийн супер зам" гэгддэг интернэт бол мэдлэгийг дамжуулахад таатай хэрэгсэл юм. Гэсэн хэдий ч энэ нь хэзээ ч агуулгыг түгээх жинхэнэ аюулгүй хэрэгсэл болж байгаагүй. Интернэтийн энгийн хэрэглэгч худал мэдээлэл, хортой программ болон бусад хортой элементүүдэд үргэлж өртөмтгий байдаг. Тиймээс интернэтэд нэвтэрч буй хүмүүс болон системийг хамгаалахын тулд контент шүүлтүүрийг ашиглах ёстой.

Агуулгын шүүлтүүр нь ажил олгогчид, системийн администраторууд, засгийн газрууд болон хувийн хэрэглэгчдэд өөрсдийгөө болон тэдний хамааралтай хүмүүсийг хүсээгүй материалаас хамгаалахад тусалдаг. Хэрэглээний өргөн цар хүрээтэй учраас янз бүрийн төрлийн агуулгын шүүлтүүрүүд байдаг бөгөөд ихэнхийг нь тодорхой хэрэглэгчдийн хэрэгцээнд нийцүүлэн өөрчлөх боломжтой.

Зураг.2 Цахим шүүлтүүрийн төрөл




### *4.5 Сервер талын шүүлтүүр*

Сервер талын контент шүүлтүүр нь тодорхой сүлжээний хэрэглэгч бүрийн веб урсгалыг удирддаг. Үйлчилгээ үзүүлэгч эсвэл администратор нь сүлжээн дэх бүх компьютертэй холбосон төв сервер дээр сервер талын агуулгын шүүлтүүрийг суулгана. Агуулга шүүлтүүрийн ийм шийдэл нь томоохон байгууллагуудын интернэт хэрэглээг хянахад тустай.

Эдгээр шийдлүүд нь серверт суурилсан тул администраторуудад агуулгыг шүүх нэг багц дүрмийг бий болгож, сүлжээний бүх хэрэглэгчдэд хэрэглэх боломжийг олгодог. ISP-д суурилсан шүүлтүүрээс ялгаатай нь компани бүрэн хяналтыг хадгалж, өөрчлөн тохируулахыг динамик, энгийн болгодог.

Сервер талын контент шүүлтүүрт өөр өөр ангиллын хэрэглэгчдэд янз бүрийн түвшний хандалтыг оноох нь маш хялбар болдог. Олон шийдэл нийлүүлэгчид зөвхөн байгууллагын түвшинд бага зэрэг өөрчлөлт оруулах шаардлагатай урьдчилан боловсруулсан контент шүүлтүүрийг санал болгодог.

### *4.6 Үйлчлүүлэгч талын шүүлтүүр*

Үйлчлүүлэгчийн контентын шүүлтүүрийг эцсийн хэрэглэгчийн системд суулгасан. Гэсэн хэдий ч эцсийн хэрэглэгч үүнийг өөрчлөх эсвэл устгах боломжгүй байж магадгүй юм. Энэхүү хязгаарлалтыг ихэвчлэн программыг нууц үгээр хамгаалах эсвэл админ эрхээр дамжуулан эцсийн хэрэглэгчийн системийн чадавхыг хязгаарлах замаар хийдэг.

Үйлчлүүлэгч талын шүүлтүүрийн ажиллагааг хязгаарласнаар администратор үйлчлүүлэгч түүний хязгаарлалтыг тойрч гарах боломжгүй гэдэгт итгэлтэй байж болно. Үйлчлүүлэгчийн шүүлтүүр нь гэрийн хэрэглээнд маш тохиромжтой.Тэд мөн тодорхой компьютерт шүүлтүүр шаарддаг бизнесийн орчинд тохиромжтой. Гэсэн хэдий ч байгууллагын хэмжээ нэмэгдэхийн хэрээр үйлчлүүлэгчийн контентын шүүлтүүрийг удирдах нь уйтгартай (эсвэл зарим тохиолдолд бараг боломжгүй юм) болдог.

### *4.7 ISP түвшний шүүлтүүр*

Агуулгын шүүлтүүрийн хувьд интернэтийн үйлчилгээ үзүүлэгч (ISP) нь байгууллага эсвэл засгийн газраас тогтоосон дүрмийн дагуу веб урсгалыг хязгаарлаж болно. ISP контент шүүлтүүрийг хэрэгжүүлэх үед эдгээр хязгаарлалт нь хэрэглэгч бүрт нөлөөлдөг.

ISP нь зохисгүй веб урсгалыг шүүж, чат болон имэйлийг хянах боломжтой. Бусад төрлийн контент шүүлтүүрийн нэгэн адил ISP-ууд нь удирдамж шинэчлэгдэх тусам үйлчилгээг динамикаар хаах эсвэл блокоос гаргах боломжтой. Хүчин төгөлдөр мөрдөгдөж буй үйлчилгээ үзүүлэгчийн бодлогод үндэслэн ISP-ууд нь үйлчлүүлэгчдэд тодорхой хэрэглэгчийн ангилалд зориулж шүүгдэх контентын төрлийг сонгох боломжийг олгодог.

Гэсэн хэдий ч, контентын шүүлтүүрийг ISP-д шилжүүлэх нь шууд хяналтыг арилгаж, өөрчлөх шаардлагатай тохиолдолд өөрчлөх үйл явцыг уртасгадаг гэдгийг тэмдэглэх нь зүйтэй.

### *4.8 Хайлтын системийн шүүлтүүр*

КОВИД-19 цар тахлын үед алсаас ажиллах нь жишиг болсон тул Google Workspace, Microsoft 365 for Business зэрэг шийдлүүд нь VPN эсвэл үйлчлүүлэгчийн программ хангамж ашиглахгүйгээр хэрэглэгчийн үйл ажиллагааг хянах боломжийг байгууллагуудад олгодог. Ажилчдын веб траффикийг хяналтдаа авснаар ажил олгогчид нэмэлт хамгаалалтын шүүлтүүрийг алсаас хэрэгжүүлэх боломжтой. Эдгээр шүүлтүүрийг асаасан үед хайлтын системүүд зөвхөн компанийн бодлогод нийцсэн үр дүнг харуулах болно. Цаашилбал,

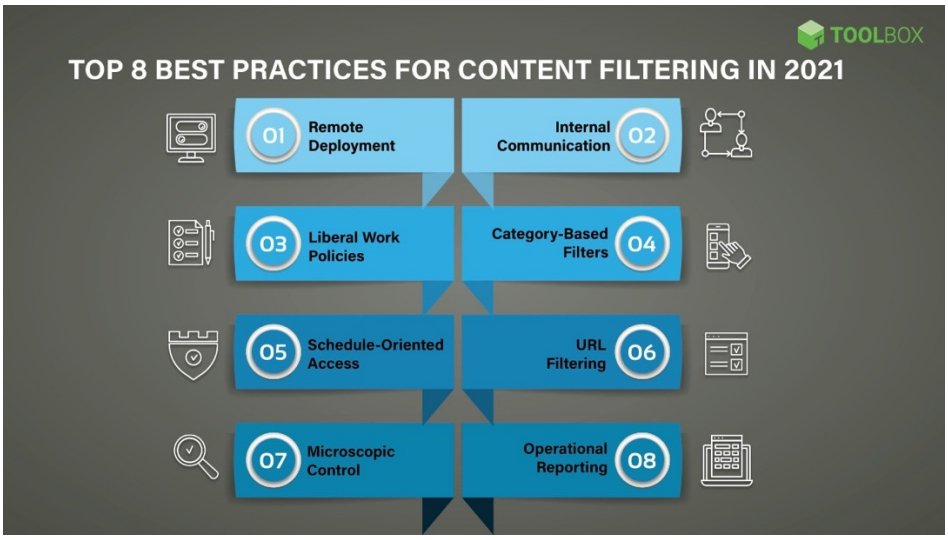
байгууллага тодорхой хориглоогүй боловч шийдэл нийлүүлэгчийн зүгээс хортой гэж үзсэн зохисгүй контентыг мөн блоклож болно.

Гэсэн хэдий ч хайлтын системийн шүүлтүүр нь URL шүүлтүүртэй адил биш гэдгийг тэмдэглэх нь зүйтэй. Энэ хоёрын хооронд тодорхой түвшний давхцал байж болох ч тусгайлан хориглоогүй веб сайтын URL-г мэддэг ажилчид хайлтын систем ашиглахгүйгээр нэвтрэх боломжтой хэвээр байж болно. Гэрийн түвшинд Kiddle, Wacky Safe зэрэг хайлтын системүүд хүүхдүүдэд чиглэсэн шүүлтүүрүүдийг санал болгодог. Эдгээр үйлчилгээ үзүүлэгчдийн хайлтын үр дүнг хүүхдэд тохирсон эсэхийг баталгаажуулахын тулд урьдчилан шүүдэг. Ийм контентын шүүлтүүрүүд нь хүүхэд болон бусад хамааралтай хүмүүст интернэтэд хяналтгүйгээр нэвтрэх боломжийг олгодог бөгөөд аюулгүй эсвэл зохисгүй контент агуулсан вебсайтаас хол байхыг баталгаажуулдаг.

## 5. 2021 оны контент шүүлтийн шилдэг 8 туршлага

Сүүлийн хорин жилийн хугацаанд интернэт дэлхий даяарх бизнесүүдийн өдөр тутмын үйл ажиллагаанд улам бүр чухал үүрэг гүйцэтгэж байгаа нь 2020 онд хүн төрөлхтнийг гэрээсээ ажиллах горимд шилжүүлсэн КОВИД-19 цар тахлын улмаас дээд цэгтээ хүрсэн чиг хандлага юм. Өмнө нь алсаас хийх боломжгүй гэж бодож байсан ажлууд удалгүй бүхэлдээ онлайнаар шилжсэн. Сургуулийн өмнөх насны болон бага насны хүүхдүүд хүртэл сургуульдаа явж, гэрийн даалгавраа онлайнаар өгдөг, мөн бүх байгууллага "гэрээсээ ажиллах" загварт шилжиж байгаа тул контент шүүлтүүрийн шийдлүүдийн хэрэгцээ урьд өмнө байгаагүй. Корпорацууд дижитал хувиргах шийдлүүдийг улам бүр нэвтрүүлэхийн хэрээр технологи, ялангуяа интернэт нь улам эрч хүчтэй, өрсөлдөөнтэй зах зээлд бизнесийн өсөлтийг хангах үндсэн шаардлага гэж үздэг.

Зураг 3. 2021 оны шилдэг 8 цахим шүүлтүүр




Интернэт нь зардлыг бууруулж, хурдыг нэмэгдүүлж, бүтээмжийг урьд өмнө хэзээ ч байгаагүй түвшинд нэмэгдүүлэх замаар байгууллагын үйл явцыг сайжруулдаг гэдгийг үгүйсгэх аргагүй юм. Гэсэн хэдий ч зарим байгууллагууд, ялангуяа тахлын улмаас үүнийг хэрэгжүүлэхэд түлхэц болсон байгууллагууд алсын зайнаас ажиллахыг зайлшгүй муу зүйл гэж үзэж болно, учир нь анхаарал

сарниулах эсвэл хортой агуулга нь үр дүнгээ алдагдуулж, кибер аюулгүй байдал, бүтээмжид нөлөөлдөг.

Түүнчлэн корпораци, компаниудад ажиллаж байгаа ажилтнуудын технологийн мэдлэг, интернэт орчинд ажиллах чадвар харилцан адилгүй байдгаас үндсэн ажилтай холбоогүй өөр агуулгад нэвтрэх явдал түгээмэл гардаг тул агуулгын шүүлтүүр тавих шаардлагатай болдог.

Мөн эрүүл мэндийн тусламж үйлчилгээ гэх мэт эмзэг мэдээлэлтэй ажилладаг байгууллага, салбарууд өгөгдлийг хадгалах, хуваалцах, ашиглах тал дээр өндөр хяналттай байх шаардлагатай. Ийм шаардлагыг алслагдсан орчинд хэрэгжүүлэхэд илүү төвөгтэй байдаг.

Агуулгын шүүлтүүрийг ашигласнаар салбар, сегмент, газарзүйн байршлын дагуу корпорацууд өөрсдийн ажиллах хүчнийхээ интернэтийн хэрэглээг үр ашигтайгаар удирдаж, алсын зайнаас эсвэл оффисын орчноос үл хамааран байгууллагын орчныг хамгаалах боломжтой. Агуулгын шүүлтүүр нь бүтээмжийг дээшлүүлж, ажилчдын дэд ангилал тус бүр дээр компанийн хяналтыг хувь хүний түвшинд аваачиж, улам бүр тэлж буй онлайн ертөнцөд байгууллага болон түүний ажилтнуудын аюулгүй байдлыг хангахад чиглэдэг.

## Агуулгын шүүлтүүрийн 2021 оны шилдэг найман туршлага

### 1. Алсын зайнаас байршуулах

КОВИД-19 цар тахлын улмаас ихэнх компаниуд гэрээсээ ажиллах загвараар үйл ажиллагаагаа явуулах болсон. Олон байгууллага дотоод ажлынхаа системд агуулгын шүүлтүүр тавихаас өмнө алсын зайн ажлын нөхцөлд шилжсэн. Энэ тохиолдолд агуулгын шүүлтүүрийг алсын зайнаас ашиглах нь чухал ач холбогдолтой байлаа.

Агуулгын шүүлтүүрийг алсаас ашиглах гурван гол чиг хандлага байна:

- Үйлчлүүлэгчийн зааварчилгаа (ажилтнууд контент шүүлтүүрийг өөрсдөө суулгах)
- Алсын зайнаас байршуулах (мэдээллийн технологийн ажилтнууд агуулгын шүүлтүүр тавьж, ажилчдын системийг алсаас удирддаг)
- Үйлчилгээ үзүүлэгчдийг солих (Google Workspace гэх мэт агуулгын шүүлтүүр санал болгодог платформ руу шилжих)

### 2. Дотоод харилцаа холбоо

КОВИД-19 цар тахлаас өмнө дотоод харилцаа холбоо тодорхой үүрэг гүйцэтгэдэг байсан зайнаас ажиллах эрэлт хэрэгцээ нэмэгдэхийн хэрээр ач холбогдол нь улам бүр нэмэгдэж байна. Цахим шуудан явуулах, виртуал уулзалт, хэлэлцүүлэг хийх гэх мэтийн байгууллагын үндсэн үйл ажиллагаанд гарч буй өөрчлөлтүүдийг даган мэдээллийн технологийн хэлтсүүд шинэ нөхцөл байдалд хурдан дасан зохицох шаардлагатай болсон. Хакерууд оффисын системд нэвтэрч, нууц мэдээлэлд нэвтрэхийн тулд тухайн компанийн хүний нөөцийн ажитан, эсхүл мэдээллийн технологийн ажилтны дүрээр нэвтрэх оролдлого хийх тохиолдол гардаг тул агуулгын шүүлтүүр нь эдгээр оролдлогыг хааж, компанийн системийн аюулгүй байдлыг хангахад чиглэнэ.

## 3. Либерал ажлын байрны бодлого

Дэлхий даяар цар тахлын нөлөөгөөр компаниуд алсын зайнаас ажиллах байнгын ажлын байрны загварт шилжихээр төлөвлөж байна. Гэрээсээ ажиллаж байгаа тохиолдолд ажилтны ажлын цаг ашиглалтыг минут, секундээр хянах боломжгүй тул ихэнх компаниуд үйл явцад биш, үр дүн, гарцад чиглэсэн илүү чөлөөтэй, шинэ ажлын байрны бодлогыг хэрэгжүүлэхийг зорьж байна. Өмнө нь ажилчид кибер аюулгүй байдлыг хангахад төдийлөн анхаардаггүй байсан бол системийг түгжээгүй, хараа хяналтгүй орхих, компанийн зөөврийн компьютерыг найз нөхөд, гэр бүлийнхээ хувийн хэрэгцээнд ашиглуулах, дэлгэцэн дээрх мэдээллийг нууцлах зэрэг шинэ шаардлагууд бий болсон. Иймд компанийн систем, мэдээллийн баазын аюулгүй байдлыг хангах, санамсаргүй эсвэл санаатайгаар алдаа гаргахаас зайлсхийх, урьдчилан сэргийлэх зорилгоор компаниуд сүүлийн үед шүүлтүүр суурилуулах арга хэмжээ авч байна.

Насанд хүрэгсдэд зориулсан контент, зэвсэг, хар тамхины мэдээлэл, үл тэвчих, хортой контентын хандалтыг хаах шүүлтүүр тавих, компанийн бүтээмжийг бууруулахгүйгээр системийн бүрэн бүтэн байдлаа хангах зорилгоор байгууллагууд агуулгын шүүлтүүр тавьдаг болсон.

Санхүүгийн байгууллагын хувьд, ихэвчлэн сегментчилсэн албан сүлжээтэй байх бөгөөд харилцагчийн мэдээлэлтэй ажилладаг хэлтсийн хувьд илүү их хязгаарлалттайгаар контентыг шүүх дабль стандартыг нэвтрүүлэх шаардлагатай байж болно.

Интернэтийн хил хязгааргүй өргөн уудам орон зайд нэг товшилтоор аюул заналхийллийг хүлээн авах эрсдэлтэй тул зөвхөн "мэдэгдэж байгаа" эрсдэлт хүчин зүйлсийг хаах нь учир дутагдалтай. Учир нь үл мэдэгдэх бүх зүйлийг хааснаар чухал ач холбогдолтой байж болох мэдээллийн нөөцийг хаах, хандалтыг хязгаарлах асуудал үүснэ. Иймд агуулгын шүүлтүүр тавих шийдэл нь тодорхой төрлийн онлайн нөөцөд хандахыг “зөвшөөрөх” эсвэл “хаах” эсэхийг тодорхойлох "ухаалаг" бөгөөд "динамик" шинж чанартай байх шаардлагатай. Иймээс компанийн удирдлагын зүгээс аюулгүй байдал, бүтээмжийн тэнцвэрийг хангасан агуулгын шүүлтүүр тавих шийдлүүдийг сайтар судалж, үнэлэх шаардлагатай болдог байна.

## 4. Ангилалд суурилсан шүүлтүүрүүд

2021 оны контент шүүх шийдлүүд нь категорид суурилсан шүүлтүүртэй байх бөгөөд шашны, зугаа цэнгэлийн, мөрийтэй тоглоомын, насанд хүрэгчдийн, тоглоомын, банкны, онлайн худалдааны гэх мэт вебсайтуудыг тодорхой хэрэглэгчийн ангилалд зориулан хязгаарлах боломжийг олгодог болсон.

Эдгээр шийдлүүдийн тусламжтайгаар мэдээллийн технологийн хэлтсүүд хязгаарлалттай вебсайтуудын жагсаалт гаргах, контент шүүлтүүрийн хуучин аргуудыг ашиглах шаардлагагүй болсон. Үүний оронд аюулгүй, зөвшөөрөгдсөн хандалтуудад анхаарлаа төвлөрүүлж, бүтээмжид саад учруулахгүйгээр хортой программ болон хортой контентыг блоклоход анхаарлаа төвлөрүүлэх болсон.

## *5.* Хуваарьт чиглэсэн хандалт

Алсын зайнаас ажиллах үед тодорхой хугацаанд тасралтгүй ажилласны дараа ажилтнууд тухайн мэдээллээс түр хөндийрөх, өөр мэдээлэлд нэвтрэх, чөлөөт цагаа өнгөрөөх шаардлагатай болдог. Хуваарьт чиглэсэн контент шүүлтүүрийн зорилго нь үндсэн ажилтай холбоогүй мэдээлэлд нэвтрэх "өдөр тутмын хэрэглээний квот"-ын тухай асуудал юм. Учир нь ихэнх компаниуд компанийн дотоод сүлжээнээс олон нийтийн мэдээллийн сүлжээнд хандах хандалтыг хаадаг. Алсын зайнаас ажиллах арга хэлбэр түгээмэл болохын хэрээр зарим компаниуд цагийн хуваарьт суурилсан контент шүүлтүүрийг нэвтрүүлж, ажилчдаа тодорхой интервалаар, эсхүл өдөрт тодорхой цагийн хуваарьтайгаар олон нийтийн мэдээллийн хэрэгсэлд хандах боломжийг нь нээж өгдөг байна. Ийм шийдэл нь ажилтнуудын ёс суртахуун болон ажлын бүтээмжид нөлөөлөхгүй байх бодлогыг баримталдаг.

**6. URL шүүлтүүр**

URL шүүлтүүрийн шийдлийг ашигласнаар байгууллагууд вебд суурилсан аюул заналхийллээс өөрсдийгөө хамгаалах, ажилчдынхаа веб үйл ажиллагааг энгийн аргаар хянах боломжтой. URL шүүлтүүр нь байгууллагын бизнесийн программтай зохицон ажиллах "зөвшөөрөх дүрэм"-ийг бий болгох замаар ажилладаг.

Администратор нь URL-ын ангиллыг хянаж, хортой гэж ангилагдсан мэдээллийг блоклох боломжтой. Энэ нь том хэмжээний контент шүүлтүүрийг худалдан авахгүйгээр URL шүүлтүүр ашиглах, мөн ажилтнуудынхаа хэрэгцээт контентод хандах хандалтыг хязгаарлахгүйгээр онлайн аюул заналд өртөх эрсдлийг бууруулах энгийн арга юм.

**7. Микроскопын хяналт**

Заримдаа тухайлсан ажилтан, эсхүл баг, байгууллагаараа хязгаарлагдсан контентод шууд хандах шаардлагатай болдог. Жишээлбэл, дижитал маркетингийн менежер албан бус хаягаараа брэндийн борлуулалтын гүйцэтгэлийг онлайнаар хянахыг хүсэж болох боловч компаниуд ихэвчлэн босоо удирдлагын тогтолцоотой байдгаас шалтгаалан корпорацийн сүлжээгээр олон нийтийн мэдээллийн хэрэгсэлд хандахыг зөвшөөрдөггүй. Нэг талаас энэ нь бизнесийн хууль ёсны шаардлага боловч, нөгөө талаас кибер аюулгүй байдал, зохицуулалтын дагаж мөрдөх журам юм.

Үүнийг шийдэхийн тулд сүүлийн үед кибер аюулгүй байдлыг хангасан байдлаар ажилтан, баг, бүлэг, хэлтэс тус бүрийг микроскопоор хянах контент шүүлтүүрийг ашиглах болсон. Энэ нь хандалтын эрхийг өдөр, долоо хоног, сараар гэх мэтчилэн тодорхой хугацаагаар тохируулсан, ажилчдад зориулсан шүүлтүүр юм.

**8. Үйл ажиллагааны тайлан**

2021 он гэхэд олон компаниуд үйлчлүүлэгчдийнхээ хүлээлтэд нийцэж ажиллахын тулд хувь хүн, баг, хэлтэс, тэр ч байтугай байгууллагынхаа түвшинд бүх ажилчдынхаа онлайн үйл ажиллагааг үр дүнтэй хянах боломжийг

бүрдүүлэхийн тулд график болон текстэн өгөгдлийг харуулсан автоматжуулсан тайлагнах системийг нэвтрүүлж эхэлсэн. Эдгээр тайлангуудыг тогтмол, эсхүл удирдлагаас өгсөн үүргийн дагуу гаргаж, тодорхой интервалтайгаар цахим шуудангаар илгээх боломжтой. Ихэнх контент шүүлтүүрийн шийдлүүд нь байгууллагын удирдлага, мэдээллийн технологи, хүний нөөцийн багуудад бодит цагийн өгөгдлийг судлах боломжийг олгоход чиглэсэн.

## ХОЁРДУГААР БҮЛЭГ. ГАДААДЫН ЗАРИМ ОРНЫ ТУРШЛАГА

## ЭСТОНИ УЛС

Эстони Улс нь дэлхийн хамгийн дэвшилтэт цахим улсуудын нэг юм. Эстони Улс нь цахим засаглалын хэрэгжилтээр 193 орноос 15 дугаарт, ил тод байдлын үзүүлэлтээр 177 орноос 28 дугаарт ордог байна. 2022 оны Статистикийн агентлагийн мэдээллээр нийт өрхийн 92.4% нь интернэтэд холбогдсон, 16-44 насны хүмүүсийн 98% нь өдөр бүр интернэт ашигладаг байна. 2019 оны байдлаар төрийн үйлчилгээний 99 хувь нь цахимаар хүрдэг, нийт хүн амын 70 хувь нь ID карт тогтмол хэрэглэдэг. ID карт, цахим санал, цахим албан татвар, цахим бизнес гэх зэрэг олон үйлчилгээг нэгтгэсэн X-зам (X-road) системийг (платформыг) боловсруулан хөгжүүлжээ. Эстони Улсад албан ёсоор харилцаа холбооны үйлчилгээ үзүүлэх байгууллагууд “Хэрэглэгчийн эрх ашгийг хамгаалах” техникийн зохицуулалтын газарт бүртгүүлж, үзүүлэх үйлчилгээнээс хамаарч бүртгэлийн хураамжийг Төрийн хураамжийн тухай хуулиар зохицуулдаг.

### 1. Цахим засаглалын бодлого зохицуулалт, эрх зүйн орчин

Эстони Улс нийгмийн хөгжлийг түргэтгэх, хүмүүсийн амьдралын чанарыг сайжруулах, амар тайван, тав тухтай амьдрах нөхцөл боломжийг бүрдүүлэх зорилгоор цахим засаглалыг тууштай дэмжиж, нийгмийн тулгамдсан асуудлыг шийдвэрлэх үе шаттай арга хэмжээнүүдийг авсаар байна. Үүнээс хамгийн гол 2 арга хэмжээ нь нэгдүгээрт, дижитал үнэмлэхжүүлэх, хоёрдугаарт, нэгдсэн мэдээлэл солилцооны порталыг бий болгосон явдал юм. 2001 онд улс орон даяар интернэт сүлжээнд холбогдох цэгүүдийн системийг бий болгосны дараагаар иргэд цахим үнэмлэхээрээ нэвтрэн ордог X-Road мэдээлэл солилцооны системийг байгуулжээ. Төр-хувийн хамтын ажиллагаанд тулгуурласан X-Road системийг нэвтрүүлснээр иргэд татварын үйлчилгээ, засгийн газрын бүхий л үйлчилгээг авах, бизнесийн үйл ажиллагаа явуулах боломжтой болсноос гадна мэдээллээ олон дахин өгөх шаардлагагүй бөгөөд хууль боловсруулах, шийдвэр гаргах үйл ажиллагаанд иргэдийн оролцоог нэмэгдүүлэх боломж бүрдсэн байна. 2019 оны байдлаар төрийн үйлчилгээний 99 хувь нь цахимаар хүрдэг бөгөөд нийт Эстоничуудын 70 хувь нь ID карт тогтмол хэрэглэдэг. Эстоничуудын хэрэглэдэг цахим үнэмлэх нь тухайн хүнийг таних үнэмлэх ба дижитал гарын үсэг гэсэн хоёр PIN код бүхий цахим чиптэй. Энэхүү цахим үнэмлэхийг 2002 оноос нэвтрүүлсэн ба тухайн хүний мэдээллийн аюулгүй байдлыг бүрэн хангасан байдаг.

Эстони Улсад цахим орчинд агуулгын шүүлтүүр хийдэг тусгайлсан хууль байхгүй бөгөөд дараах холбогдох хуулиудаар зохицуулдаг.

1. ***Цахим харилцааны тухай хууль*** (Electronic Communications Act)[8]- нь 2022 оноос хүчин төгөлдөр болсон нийт 15 бүлэг 206 зүйл заалттай хууль юм. Энэхүү хуулийн гол зорилго нь тодорхой технологид давуу эрх олголгүйгээр цахим харилцаа холбооны сүлжээ болон үйлчилгээний чөлөөт зах зээлийг хөгжүүлэх, шударга өрсөлдөөнийг хөгжүүлэхэд шаардлагатай нөхцөлийг бүрдүүлэх, цахим хэрэглэгчдийн эрх ашгийг хамгаалахад оршино.

**Тус хуулийн 87 дугаар зүйлд харилцаа холбооны сүлжээ, үйлчилгээний аюулгүй байдлыг хангахтай холбоотой дараах зохицуулалтуудыг тусгасан байна:**

- ***Харилцаа холбооны байгууллага нь*** харилцаа холбооны үйлчилгээ, сүлжээний аюулгүй байдал, холбогдох эрсдлийг удирдах, болзошгүй онцгой нөхцөл байдлын үеийн арга хэмжээг зохион байгуулах, хэрэглэгчийн аюулгүй байдлыг хангасан үйлчилгээг тасралтгүй үзүүлэх нөхцлийг бүрдүүлэх ёстой.
- ***Харилцаа холбооны байгууллага нь*** харилцаа холбооны үйлчилгээнд гарсан зөрчил дутагдал, учирсан хохирол зэрэг бүх тохиолдолд авч хэрэгжүүлсэн арга хэмжээгээ Эстоний мэдээллийн системийн төв байгууллагуудад мэдэгдэх ёстой.
- ***Мэдээллийн системийн төв байгууллага нь*** ирсэн мэдэгдлийг Европын Комисст жил тутам тайлан бичиж хүргүүлнэ.

**Тус хуулийн 102 дугаар зүйлд Мэдээллийг хамгаалах ерөнхий зарчмыг дараах байдлаар тусгасан байна.**

Харилцаа холбооны байгууллага нь дараах үүрэгтэй байна. Үүнд:

- харилцаа холбооны үйлчилгээг ашиглахтай холбоотой тодорхой мэдээлэл;
- харилцаа холбооны сүлжээгээр дамжуулж буй мессежний агуулга болон хэлбэр;
- мессеж дамжуулах цаг болон дамжуулах арга хэлбэр зэрэг нууцыг хадгалах үүрэгтэй байна.

2. **Хувийн мэдээллийг хамгаалах тухай хууль** (Personal Data Protection Act)[9]- 1996 онд батлагдсан 7 бүлэг 76 зүйл заалттай. Энэ хуулийн зохицуулалтууд нь Европын Холбооны Мэдээллийг хамгаалах тухай 95/46/EC захирамжтай бүрэн нийцдэг. Тус хууль нь нийтийн хэрэгцээнд зориулсан аливаа мэдээллийг чөлөөтэй авах хувь хүний эрх, эрх чөлөөтэй нийцсэн бөгөөд иргэдийн өөрсдийнхөө тухай мэдээллийг боловсруулах явц дахь үндсэн эрх, эрх чөлөөг хамгаална. Бие даасан хяналт, мэдээлэл боловсруулах явц дахь үүрэг хариуцлагын талаарх тодорхой заалтууд нь энэхүү хамгаалалтын системийн тулгуур багана болдог.
3. **Нийгмийн үйлчилгээний мэдээллийн тухай хууль** (Information Society Services Act)[10]- 2004 онд батлагдсан 18 бүлэгтэй. Тус хууль нь Европын

[8] Electronic Communications Act https://www.riigiteataja.ee/en/eli/501042015003/consolide
[9] Personal Data Protection Act https://www.riigiteataja.ee/en/eli/523012019001/consolide
[10] Information Society Services Act https://www.riigiteataja.ee/en/eli/504112013008/consolide

Холбооны мэдээллийн нийгмийн үйлчилгээ, ялангуяа, цахим арилжааны, дотоод зах зээлийн зарим тодорхой хуулийн талуудын тухай 2000/31/EC захирамжтай уялдан гарсан. Үүнд мэдээллийн үйлчилгээгээр хангагчдад болон удирдан хянах байгууллага, зөрчсөн тохиолдлын шийтгэл зэргийн талаар хуульчилсан байна.

4. **Нийтийн мэдээллийн тухай хууль** (Public Information Act)[11]- 2000 онд батлагдсан 7 бүлэг 69 зүйл заалттай. Энэхүү хуулийн зорилго нь нийтийн мэдээлэл (public information), түүнд хандах, дахин ашиглах, тэдгээрийн зохион байгуулалт, мэдээлэл эзэмшигчийн үүргийг зохицуулахаас гадна бүхэлдээ дата засаглал бүрдүүлэхэд чиглэсэн харилцааг зохицуулахад оршино. Түүнчлэн мэдээллийн ил тод байдлын тухай, мэдээлэл авах эрхийн тухай, төрийн болон албаны мэдээллийн нууцлал, түүнд хандах эрхийн тухай, нээлттэй өгөгдөл бий болгох, цахим засгийн харилцааны технологийн үндэс суурь болсон мэдээллийн сан, систем, тэдгээрийн чиг үүрэг, үйл ажиллагааг зохицуулсан дүрэм, журмын эрх зүйн үндсийг тогтоож өгсөн байна. Цахим засаглалын үүднээс Нийтийн мэдээллийн тухай хууль нь дараах зүйлсийг зохицуулдаг. Үүнд:
   - Үндэсний мэдээллийн системийн менежмент (Мэдээллийн системийн захиргаа)
   - X-Road мэдээллийн системийн мэдээлэл солилцооны давхарга
   - бусад мэдээллийн системийн аюулгүй байдлын асуудлууд зэрэг болно.
5. ***Хүн амын бүртгэлийн тухай хууль*** (Population register Act)[12]- 2000 онд батлагдсан 16 зүйл 104 зүйл заалттай. Энэхүү хууль нь дижитал нийгмийн тулгын чулууны нэг болсон зарчмуудад үндэслэсэн ба хувь хүний өвөрмөцөөр ялгарах кодыг хуульчилсан. Энэ хуулийн дагуу Эстонид ажиллаж амьдарч байгаа болон цахимаар бүртгүүлсэн оршин суугч хүн бүр насан туршдаа хэрэглэх 11 оронтой (тоон) код буюу Эстоний таниулга кодыг авах үүрэгтэй. ID код бол цахимаар хууль ёсны үйл ажиллагаа эрхлэх үндсэн элемент юм. Цахим шилжүүлгээс гадна тэрхүү кодыг хувь хүн өөрийгөө таниулах шаардлагатай бусад бүх утга агуулгаар хэрэглэнэ.
6. ***Тоон гарын үсгийн тухай хууль*** (Digital Signatures Act)[13] – 2000 онд батлагдсан 10 бүлэг 47 зүйл заалттай. Энэхүү хуулиар тоон болон бичмэл гарын үсэгт хуулийн адил тэгш статус олгох ба, улсын бүх байгууллагуудыг тоон гарын үсэг бүхий бичиг баримтыг хүлээн зөвшөөрөх шаардлагыг тавина. Энэ хууль бас гэрчилгээ олгох ба цаг тамгалах үйлчилгээ үзүүлэгчдийг Засгийн газраас удирдан чиглүүлэхийг зохицуулсан тусгай нэг бүлэгтэй. Энэхүү хууль нь цахим үнэмлэх ба Европын дотоод зах зээл цахим шилжүүлгийн үйлчилгээний тухай Европын Холбооны № 910/2014 зохицуулалттай уялдаатай юм.
7. ***Кибер аюулгүй байдлын тухай хууль*** (Cybersecurity Act)[14]- 2018 онд батлагдсан 6 бүлэг 29 зүйл заалттай. Тус хуулиар нийгэм улс төрийн мэдээллийн системийн үйл ажиллагаанд зайлшгүй шаардлагатай

[11] Public Information Act https://www.riigiteataja.ee/en/eli/ee/522122014002/consolide/current
[12] Population register Act https://www.riigiteataja.ee/en/eli/516012014003/consolide
[13] Digital Signatures Act https://www.riigiteataja.ee/en/eli/530102013080/consolide
[14] Cybersecurity Act https://www.riigiteataja.ee/en/eli/523052018003/consolide

мэдээллийн системийн аюулгүй байдал, засвар үйлчилгээ, хариуцлага, хяналт, кибер гэмт хэргээс урьдчилан сэргийлэх, шийдвэрлэх үндэслэлийг тусгажээ.

**2. Эстони Улсын нэгдэн орсон олон улсын конвенц**

Эстони Улс дараах конвенцуудыг соёрхон баталсан. Үүнд:

- Цахим гэмт хэргийн тухай конвенц (Council of Europe Convention on Cybercrime)
- Терроризмоос урьдчилан сэргийлэх тухай конвенц (Council of Europe Convention on the Prevention of Terrorism)
- Арьс өнгөөр ялгаварлан гадуурхах бүх хэлбэрийг устгах тухай конвенц (United Nations International Convention on the Elimination of All Forms of Racial Discrimination)
- Хүүхдийн бэлгийн мөлжлөг, бэлгийн дарамтаас хамгаалах тухай конвенц (Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual
- Abuse)
- Хүүхдийн эрхийн тухай конвенц (United Nations Optional Protocol to the Convention on the Rights of the Child ) байна.

**3. 2019-2022 оны Кибер аюулгүй байдлын стратеги зорилго *нь*** дижитал нийгмийг тогтвортой байлгах, кибер аюулгүй байдлын салбарын хөгжлийг судалгаанд суурилж дэмжих, олон улсад тэргүүлэгч хувь нэмэр оруулагч болох, кибер бичиг үсэгт тайлагдсан нийгэм болох гэсэн 4 гол зорилтыг дэвшүүлсэн. Стратегийн үндсэн зарчим нь:

- Цахим орчинд үндсэн эрх чөлөөг хамгаалах хөхүлэн дэмжих;
- Кибер аюулгүй байдал нь Эстони Улсын нийгэм эдийн засгийн өсөлтийн үндэс, дижитал хөгжлийг дэмжих хөдөлгөгч хүч болгох;
- Криптограф шийдлийн аюулгүй байдал нь дижитал экосистемийн үндэс суурь болох;
- Ил тод байдал, олон нийтийн итгэл нь дижитал нийгмийн үндэс суурь болно гэж үзжээ.

**4. Цахим орчин дахь агуулгын шүүлтүүр (Content filtering)**

Эстони Улсад интернэт үйлчилгээ үзүүлж байгаа тал нь агуулгыг хянах болон хэрэглэгчийн дамжуулсан хууль бус контентын төлөө хариуцлага хүлээдэггүй байна. Нийгмийн мэдээллийн сүлжээнд хууль бус, ёс журам зөрчсөн зүйлсээс урьдчилан сэргийлэх, хариу арга хэмжээ авах техникийн болон хууль эрх зүйн хэд хэдэн арга хэрэгсэл байна. Үүнд:

- Self-regulation - Уламжлалт мэдээллийн хэрэгсэл болох телевиз, радио, олон нийтийн нэвтрүүлгээр интернэтэд идэвхтэй байгаа блог, цахим хуудсыг сурталчилж, сэдэвчилсэн байдлаар ангилж үйл ажиллагааг нь олон нийтэд мэдээлдэг.
- Хэвлэл мэдээллийн үйлчилгээний тухай хуулийн 22 зүйлд “хэвлэл мэдээллийн үйлчилгээ үзүүлэгч нь өөрсдийн санаачлагаар холбоо байгуулж, холбоо нь өөрсдөө мэдээллийн үйлчилгээнд стандарт тогтоох,

сайн туршлагыг дэлгэрүүлэх дүрэм журмыг баталж болно” гэж заасан байдаг. Мөн тус холбоод нь интернэтийн аюулгүй байдлын талаар сургалт явуулдаг байна.

- Эстоний сонины нийгэмлэг нь “цахим орчинд сэтгэгдэл бичих” дүрмийн дагуу үгэнд шүүлтүүр хийх, IP хаягыг хаах, хуулийн байгууллагад хандах зэрэг арга хэмжээг авч хэрэгжүүлдэг.
- Мэдээлэл хамгаалах хяналтын газраас гаргасан заавар зөвлөгөөг зөрчсөн хууль бус контент, бүрэн мэдээлэлгүй дансны мэдээлэл, хууль бус хувийн мэдээлэл, гүтгэлгийн шинжтэй үг хэллэгтэй мэдээллийг админ олон нийтэд нийтлэхгүй хасаж болно.
- Web constables – Цагдаа, хил хамгаалах газраас боловсруулсан тус вебсайт нь цахим орчинд бэлгийн болон бусад төрлийн хүчирхийллийн агуулгатай мэдээлэл, мессеж нийтлэгдэхэд цагдаагийн ажилтнуудад мэдэгдэж нийтэлсэн этгээдийн мэдээллийг олж мөрдөн шалгах боломжоор хангадаг.
- Олон улсын сүлжээ болох Inhope, Insafe зэрэг ашгийн бус байгууллагуудтай хамтран цахим орчин дахь хүүхдийн хүчирхийллийг хянадаг.
- 2014 оноос Rahvaalgatus.ee платформыг хууль тогтоогчдын үйл ажиллагааг хянах зорилгоор ажиллуулж, 1000-аас доошгүй иргэдийн тоон гарын үсэг цуглуулсан өргөдөл гомдол ирсэн тохиолдолд парламентад илгээдэг байна. Мөн энэхүү платформ нь орон нутгийн иргэдийн өргөдөл гомдлын асуудлыг хөнгөвчилдөг байна.

Дараах хяналтын байгууллагууд цахим орчны агуулгын хууль ёсны байдлыг үнэлж, түүнд холбогдох шийдвэр гаргах, хариуцлага тооцох эрхтэй байна.

1. **Мэдээллийн системийн ерөнхий байгууллага** (Information System Authority)[15]- Цахим орчин дахь мэдээллийн аюулгүй байдлыг хангах, гарсан зөрчлийг арилгах арга хэмжээ авах, мэдээллийн системийг боловсруулах, мэдээллийн системийн харилцан үйлчлэлийг хангах чиг үүрэгтэй Эдийн засаг харилцаа холбооны яаманд харьяалагддаг. Тус байгууллагын CERT-EE нь 2006 онд байгуулагдсан цахим орчинд гарсан зөрчлийг хариуцдаг хэлтэс юм. *CERT-EE-ийн зорилго:*

- Мэдээллийн аюулгүй байдалд гарсан зөрчил дутагдлын талаар мэдээлэл цуглуулж хяналт тавих;
- Мэдээллийн аюулгүй байдлын зөрчил дутагдлаас урьдчилан сэргийлэх, эрсдлийг бууруулах арга хэмжээг зохион байгуулах;
- Зөрчил дутагдлыг засах арилгах тал дээр хууль хяналтын байгууллагад мэргэжлийн туслалцаа үзүүлэх, хамтран ажиллах болно.

*CERT-EE үйлчилгээ:*

- Онлайн вирус сканнер - төрийн болон хувийн хэвшлийн мэдээллийн сүлжээ хэрэглэгчдэд зориулсан сэжигтэй цахим шуудан болон файлыг сканнердах хэрэгсэл.

[15] Information System Authority https://www.ria.ee/en/cyber-security/handling-cyber-incidents-cert-ee/monitoring-cyberspace-and-impeding-incidents

- Sandbox - мэдээллийн технологийн мэргэжилтнүүдэд зориулсан файлын шинжилгээний хэрэгсэл.
- File transfer environment – фишинг (phishing) цахим шуудан, хортой программын дээжийг шинжилгээнд илгээх хэрэгсэл.
- Suricata4all - автомат хяналтын шийдэл нь цахим орчны халдлагыг төв хяналтын системд мэдээлдэг.
- DNS программ- хортой программ, фишинг хийхийг блоклодог IOS, Android үйлдлийн систем дээр ажилладаг программ юм.

**2. Мэдээлэл хамгаалах хяналтын газар** – Хууль зүйн яамны харьяанд байдаг тус байгууллага нь:

- Олон нийтийн сүлжээнд хувийн мэдээллийг хамгаалах;
- Мэдээлэл боловсруулахад заавар зөвлөгөө өгөх;
- Хувийн мэдээллийг хамгаалах тухай хуулийн хэрэгжилтэд хяналт тавих;
- Тодруулга мэдээллийн ажлыг зохион байгуулах;
- Олон нийтийн мэдээллийн санг бүртгэх, зохицуулах чиг үүрэгтэй байгууллага юм.

**3.Татвар гаалийн зөвлөл** – Олон нийтийн сүлжээнд мөрийтэй тоглоомын үйлчилгээ үзүүлдэг байгууллагыг олон нийтэд ил тод мэдээлэх, үйл ажиллагааг хянах, хууль бус үйл ажиллагаа явуулсан тохиолдолд цахим орчинд домэйнийг хаах үүрэгтэй.

**4. Оюуны өмчийн эрхийг хамгаалах газар** – Зохиогчийн эрхээр хамгаалагдсан бүтээлтэй ижил төстэй агуулгаар хийгдсэн контентыг устгах эрхтэй.

**5. Цахим орчин дахь зөрчилд хүлээлгэх хариуцлага**

Эстони Улсын Үндсэн хуулиар бүх иргэн мэдээлэл олж авах, үзэл бодлоо чөлөөтэй илэрхийлэх эрхтэй гэж баталгаажуулсан. Цахим орчинд үзэл бодлоо илэрхийлэх эрх чөлөөнд цөөн хэдэн хязгаарлалт болох үндэс угсаа, арьс өнгө, шашин шүтлэг, нийгмийн гарал үүсэл, бэлгийн чиг баримжаа, санхүүгийн байдал, хэл, соёл зэргээр ялгаварлан гадуурхаж цахим орчинд бусдыг гутаан доромжилсон тохиолдолд 3200 еврогийн торгууль ногдуулна. Энэхүү гутаан доромжлох үг хэллэг, мэдээлэл нь *“Хүний амь нас эрүүл мэндэд ноцтой хохирол учруулсан”* тохиолдолд 3 хүртэлх жил хорих ялын шийтгэлтэй гэж Эрүүгийн хуульд заасан байна. Мөн цахим орчинд насанд хүрээгүй хүүхдийг садар самуун контент, бичлэг, кино, видео клип, зар сурталчилгаанд ашиглах зэргийг Эрүүгийн хуулийн “*Насанд хүрээгүй хүүхдийн эсрэг гэмт хэрэг”* гэсэн бүлэгт тусгайлан зохицуулалтыг зааж өгсөн байна. 2002 оноос гүтгэлгийг гэмт хэрэг биш болгон хохирлын хэмжээнээс хамааран “*Иргэний тухай хууль*”-ийн дагуу хариуцлага ногдуулдаг болсон.

Улс төр, нийгэм, соёлын харилцаа холбооны үйлчилгээ үзүүлдэг байгууллага олон байдаг бөгөөд тэдгээрээс олон нийтийг төөрөгдүүлсэн мэдээ мэдээлэл түгээсэн тохиолдолд тухайн байгууллагыг “*Нийгмийн үйлчилгээний мэдээллийн тухай хууль”*-ийн дагуу 9,600 еврогоор торгодог. Үйл ажиллагаа явуулах зөвшөөрөл аваагүй цахим сайтыг “*Хэрэглэгчийн эрх ашгийг хамгаалах техникийн зохицуулалтын газар*”-с хааж хар жагсаалтыг олон нийтэд мэдээлдэг байна.

## БНСУ

### 1. Цахим засаглалын бодлого, зохицуулалт

2019 оны 2-р сард ***Солонгосын Харилцаа Холбооны Хорооноос*** (KCC) анх БНСУ дахь цахим орчин дахь хууль бус үйлдлээс урьдчилан сэргийлэх, мэдээллийн шүүлтүүр хийх бодлогын өөрчлөлт, шинэчлэлтийг зарласан. Үүнтэй холбоотойгоор ***Солонгосын Харилцаа холбооны стандартын хороо*** (KCSC) хариуцан ажиллаж дээрх бодлогын дагуу арга хэмжээ авч байна. Солонгосын Засгийн газрын байгууллагаас цахим орчинд зохицуулалт хийж, хянан мөрийтэй тоглоом, порнографын сайт зэрэг хууль бус цахим хуудсууд руу нэвтрэхийг хориглох замаар хууль тогтоомжийг цахим орчинд хэрэгжүүлж байна[16].

Энэхүү цахим орчин дахь хяналт, урьдчилан сэргийлэх арга хэмжээ, бодлогын хэлбэрийг мэргэжилтнүүд Орос, Хятадын цахим орчин дахь хуультай[17] адилтган үзэж байна. БНСУ-ын дээрх цахим орчин дахь хяналтын бодлого нь бусад орнуудаас илүү хурдан шуурхай хяналтыг хийж, ардчилсан замаар шүүлтүүрийн хөтөлбөрийг үндэслэсэн хуулиудыг хэрэгжүүлж байна. Гэсэн хэдий ч цахим орчинд иргэд үзэл бодлоо илэрхийлэх, хууль бус үйлдэл хийх хоёр асуудлыг хооронд нь ялгаж салгаж, интернэтийн эрх чөлөөг хязгаарлахгүй байх нь чухал хэмээн үзжээ.

Дээрх БНСУ-ын хэрэгжүүлж буй цахим орчин дахь зохицуулалт нь хуулийн хүрээнд, хууль бус агуулга бүхий цахим контентыг илрүүлж хаах (блоклох) зэрэг арга хэмжээ авч байна. Гэвч БНСУ-ын Засгийн газар цахим орчинд иргэдээ хамгаалах үүрэг хариуцлагыг тэнцвэртэй хэрэгжүүлж, интернэтийн нээлттэй байдлыг хадгалж ажиллаж байна. Мөн түүнчлэн Солонгосын бэлгийн хүчирхийллийн эсрэг төв (Korean Sexual Violence Center) төрийн бус байгууллагууд хэвлэл мэдээллийн хэрэгслээр засгийн газраас хууль бус веб сайт руу нэвтрэхийг хориглох чадавхыг сайжруулах тал дээр хамтарч ажилладаг байна.

**Солонгосын харилцаа холбооны хороо** (KCC- Korean Communications Commission)

Цахим орчин дахь хууль бус үйлдэл, худал мэдээллийн улмаас хохирол амссан бүх төрлийн гомдол саналыг Солонгосын харилцаа холбооны хороо хүлээн авдаг байна. Хууль бус ташаа мэдээлэл (Illegal Information) гэдэгт БНСУ-ын хуулийн эсрэг бүх төрлийн мэдээлэл, мөн олон нийтийн эрх ашиг хөндөгдсөн мэдээллүүд багтдаг байна. Хортой мэдээлэл (harmful information) гэдэгт интернэт дэх ёс суртахуунгүй, хүчирхийлэл, садар самуун, нийгэмд харш зэрэг мэдээллүүдийг хэлнэ хэмээн Солонгосын харилцаа холбооны хороо болон Залуучуудын эрхийг хамгаалах хорооноос (Commission on Youth Protection) тодорхойлсон байна.

БНСУ-ын харилцаа холбооны хороо цахим орчин дахь зохицуулалтыг дараах бүтэц зохион байгуулалтаар хийж байна[18].

---

[16] Analysis: South Korea's New tool for filtering illegal internet content By Robert Morgus, Justin Sherman, and Seonghyun Nam

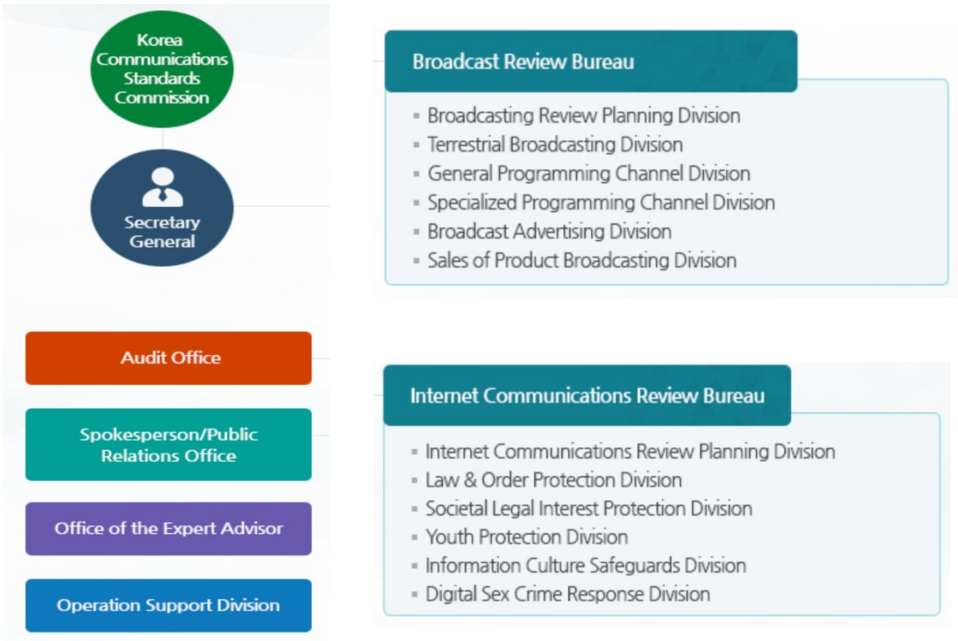
[17] Analysis: Russia's Plans for a National internet https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/russias-plans-for-a-national-internet/

[18] http://service.kocsc.or.kr/eng/PageLink.do

*Интернэт харилцааны хяналтын товчоо (Internet communication review bureau)*

- интернэт харилцааны тойм төлөвлөлтийн хэлтэс;
- хуулийн хэрэгжилтийг хамгаалах хянах хэлтэс;
- нийгмийн эрх зүйн ашиг сонирхлыг хамгаалах хэлтэс;
- залуучууд хамгааллын хэлтэс;
- мэдээллийн соёлын хамгаалалтын хэлтэс;
- дижитал бэлгийн гэмт хэрэгтэй тэмцэх хэлтэс;

Зураг 4. Солонгосын харилцаа холбооны стандартын хороо түүний бүтэц.




## 2. Цахим орчин дахь мэдээллийн шүүлтүүр, эрх зүйн орчин

Цахим орчин дахь мэдээллийн шүүлтүүрийн дээрх хэрэгслүүр нь бодлогын хувьд шинэ зүйл биш бөгөөд одоогоор хүчин төгөлдөр мөрдөгдөж буй холбогдох хууль тогтоомжийн хэрэгжилтийг сайжруулж буй техникийн шинэ арга юм. БНСУ-ын цахим орчин дахь эрх зүйн орчин, зохицуулалтын хувьд:

- Эрүүгийн хууль (Criminal Law);
- Бэлгийн хүчирхийллийн эсрэг хууль (Sexual Violence Punishment Act); Мэдээлэл, харилцааны сүлжээний тухай хууль (Information and Communication Network Act);
- Мэдээлэл, харилцаа холбооны хяналтын журам (Information and Communication Reviewing Regulation) зэрэг хэд хэдэн хууль тогтоомжоос бүрддэг байна.

Эдгээр хуулийн хүрээнд Солонгосын Харилцаа холбооны стандартын хороо (KCSC) нь БНСУ болон бусад орны серверүүд дээр байршуулсан хууль бус материалыг устгах, хууль бус мэдээллийн хүсэлтийг блоклох зэрэг арга хэмжээг авч байна.

Солонгосын Харилцаа холбооны хорооноос (KCC) хүүхдийн порнограф, хууль бус мөрийтэй тоглоомын сайтуудыг хаах веб сайтуудын төрлийг ил

болгосон байна. Харин улс төрийн агуулга бүхий контент мэдээллийг хаах, блоклох арга хэмжээ ихэнх тохиолдолд авдаггүй ба зарим тохиолдолд Хойд Солонгосыг хэт их магтан дуулсан улс төрийн контент үзэл суртал бүхий мэдээллийг Солонгосын Харилцаа холбооны стандартын хороо (KCSC) блоклосон тохиолдол байдаг байна.

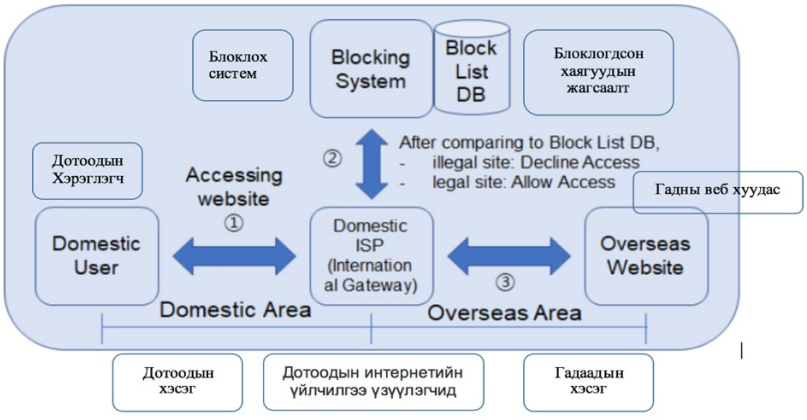
Солонгосын Харилцаа холбооны стандартын хороо гаднаас буюу бусад улсуудаас ирж буй цахим орчин дахь хууль бус материалын хүсэлтийг хааж дамжуулдаггүй байна. Мөн хууль бус контентыг байршуулсан веб хуудсуудыг хар жагсаалтад оруулж түүгээр сан үүсгэн дахин тухайн хуудсуудыг цахим орчинд нэвтрүүлдэггүй байна. Мөн Server Name Indication (Серверийн нэрийн заалт) ашиглан хар жагсаалтад орсон веб сайтуудын IP хаягаар хаанаас хандаж байгааг ажиглаж мэдээллийн ерөнхий агуулагыг хянах боломжтой болсон байна. Ийнхүү Солонгосын Харилцаа холбооны стандартын хороо KCSC нь хар жагсаалтад орсон зарим домэйныг блоклохын тулд ISP-internet service provider ашиглан автоматаар цаг алдалгүй түргэн шуурхай шүүлтүүр хийдэг байна.

### 3. Цахим орчин дахь хууль бус мэдээллийг хязгаарлах хэрэгслүүр

Цахим орчин дахь хууль бус мэдээллийг хязгаарлахад интернэтийн Transport Layer Security (TLS) протоколыг ашигладаг байна. TLS протокол нь интернэт хөтөч болон хүссэн контентыг байршуулах сервер хоорондын урсгалыг шифрлэдэг аюулгүй байдлын протокол юм.

Сүүлийн үед ашиглаж байгаа "виртуал хостинг" хэмээх аргын тусламжтайгаар серверүүд нэг IP хаяг ашиглан олон веб хаягийг байршуулах боломжтой болсон. SNI (Серверийн нэрийн заалт) нь серверт хүссэн домайныг таньж, илгээхэд нь туслах замаар нэг IP хаягтай эдгээр серверүүдэд олон веб хаягийг байршуулах боломжийг олгодог хэрэгсэл юм. SNI талбар нь  аль хост хаанаас аль хөтчийг ашиглан хүсэлт илгээж байгааг тодорхойлдог байна. TLS нь цахим хөдөлгөөний агуулгыг шифрлэдэг ч энэ нь SNI-ний хүссэн серверийн нэрийг шифрлэдэггүй.

Зураг 5. Цахим орчин дахь хууль бус мэдээллийг шүүх схем.




*Эх сурвалж: Blocking Illegal Overseas Websites Is Not Censorship or Infringing Freedom of Expression*)[19]

[19] http://www.korea.kr/news/actuallyView.do?newsId=148858720.

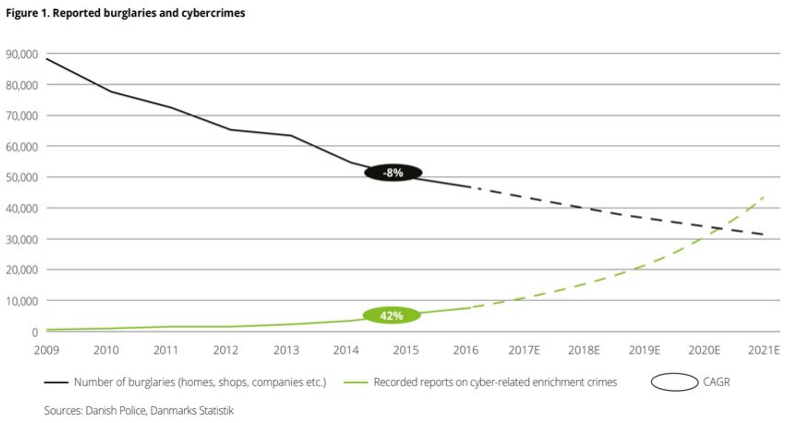
Мэдээлэл дамжуулах явцад серверийн нэр нээлттэй байдаг тул серверийн хаяг заалтыг нь хянах KCSC-ийн хар жагсаалтад орсон эсэхийг серверийн нэрээр таних, хаах боломжтой байна. Энэ нь хэд хэдэн веб сайтын домэйнтэй байж болох IP хаягийг бүхэлд нь хаах замаар эрсдэлээс зайлсхийдэг.

**ДАНИ УЛС**

Дани Улс нь 42,933 хавтгай дөрвөлжин километр газар нутагтай, газар зүйн хувьд Европ тивийн хойд хэсэгт оршдог Скандинавын улс бөгөөд улсын нийслэл хот нь Копенхаген, нийт хүн амын тоо нь 5.9 сая[20], боловсрол, эрүүл мэнд, иргэний эрх чөлөө, ардчилсан засаглал, ижил хүйстнүүдийн эрх, аз жаргалын индекс гэх мэт олон үзүүлэлтээр дэлхийд дээгүүр байранд ордог, нэг хүнд ногдох ДНБ 68.008 ам доллар[21] бүхий өндөр хөгжилтэй орон юм[22].

Дани Улс нийгмийн цахим шилжилтийн чиглэлээр дэлхийд тэргүүлэгч орнуудын нэг бөгөөд Европын Комиссоос гаргадаг Цахим эдийн засаг, нийгмийн индекс (*European Commission's Digital Economy and Society Index*[23] *(DESI)*)-ийн 2021 оны судалгаагаар Европын Холбооны (ЕХ) орнуудаас нэгдүгээрт орсон. Мөн НҮБ-аас хийгддэг цахим засгийн газрын судалгаагаар 193 орноос 2018, 2020[24] онуудад тус тус нэгдүгээрт эрэмбэлэгдсэн.

2022 онд Дани Улсын Засгийн газар "Цахимжуулалтын үндэсний стратеги", "Кибер болон мэдээллийн аюулгүй байдлын 2022-2024 онд хэрэгжүүлэх үндэсний стратеги"-уудаа тус тус шинэчлэн танилцуулсан. Тэдгээр цахимжуулах бодлогыг Сангийн яамны харьяа Цахим засаглалын агентлаг (Agency for Digital Government)[25] хэрэгжүүлдэг.




Зураг 6. Сүүлийн 10 жилд үйлдэгдсэн орон байрны хулгай болон кибер орчинд хөрөнгө завшсан гэмт хэргийн мэдээлэл

Цахим шилжилт нь нийгэмд маш их эерэг өөрчлөлтийг бий болгож байгаа хэдий ч цахим орчинд садар самуун, хүчирхийлэл, ялгаварлан гадуурхалт,

[20] Дани Улсын хүн ам. https://www.dst.dk/en/Statistik/emner/borgere/befolkning

[21] Дани Улсын нэг хүнд ногдох ДНБ, Дэлхийн Банк. https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=DK

[22] Британника цахим нэвтэрхий толь. https://www.britannica.com/place/Denmark

[23] Цахим эдийн засаг, нийгмийн индекс(DESI). https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2021

[24] E-Government Survey 2020, UN. https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf

[25] Дани Улсын Цахим засаглалын агентлагийн цахим хуудас.https://en.digst.dk

терроризм сурталчлах, луйвар, залилан хийх зэрэг багагүй сөрөг үр дагавар үүсгэж байна. Жишээ нь Дани Улсад сүүлийн 10 жилд үйлдэгдсэн орон байрны хулгай болон кибер орчинд хөрөнгө завшсан гэмт хэргийн гаралтын тоог харьцуулан харуулав[26].

**1. Цахим орчин дахь эрх зүйн зохицуулалт**

Дани Улсад интернэт дэх хууль бус контентыг хаах, шүүлтүүрдэх, устгах талаарх харилцааг тусгайлан зохицуулсан бие даасан хууль тогтоомж байдаггүй. Харин түүний оронд эрх зүйн хэд хэдэн салбарт хуваагдсан, нарийвчилсан зохицуулалтууд байдаг бөгөөд ерөнхийдөө тус тусын чиглэлээр хууль бус контентоос урьдчилан сэргийлэх чиг үүрэг гүйцэтгэдэг. Эдгээр холбогдох зохицуулалтуудыг эрх зүйн салбар, хүрээгээр нь ангилан үзвэл:

- Эрүүгийн эрх зүйн хүрээнд;
- Иргэний эрх зүйн хүрээнд;
- Захиргааны эрх зүйн хүрээнд;
- Зөөлөн эрх зүйн зохицуулалтын (soft law) хүрээнд гэсэн 4 үндсэн чиглэлд харьяалуулан авч үзэж болно.

**Эрүүгийн эрх зүйн хүрээнд:**

Дани Улс 2005 оны 6-р сарын 21-нд Европын Зөвлөлийн “Кибер гэмт хэргийн тухай” конвенцыг соёрхон баталж, 2005 оны 10-р сарын 1-нээс уг конвенц тус улсад дотоодын хууль тогтоомжийн нэгэн адил хүчин төгөлдөр үйлчилж эхэлсэн байдаг. Тус конвенц нь интернэт болон бусад компьютерын сүлжээнд үйлдэгддэг гэмт хэрэг, ялангуяа зохиогчийн эрхийн зөрчил, компьютертай холбоотой залилан, хүүхдийг садар самуунд ашиглах, заналхийлэх гэмт хэрэг, сүлжээний аюулгүй байдлын эсрэг гэмт хэрэг зэрэг хэргүүдтэй холбоотой бөгөөд эдгээр гэмт хэргийн зохицуулалт Дани Улсын эрүүгийн хуульд тусгалаа олсон. Компьютерын сүлжээгээр дамжуулан арьс өнгөөр ялгаварлан гадуурхах, гадаадын иргэдийг үзэн ядах, ялгаварлан гадуурхах шинжтэй үйлдлийг гэмт хэрэгт тооцох тухай нэмэлт протоколыг Дани Улс мөн хүлээн зөвшөөрч соёрхон баталсан.

2004 оноос Европын Холбоонд хэрэгжиж эхэлсэн “Интернэттэй холбоотой хүүхдийн хүчирхийллийн төсөл”-д (CIRCAMP) Дани Улс тэргүүлэгч орны хувиар идэвхтэй оролцсон ба 2006 оны намар төслийн үйл ажиллагааны II төлөвлөгөөг баталж, хууль сахиулах байгууллагуудад хүүхдийн хүчирхийллийн хууль бус веб хуудсыг хянах, таслан зогсоох боломжийг олгосон цогц механизмыг бий болгосон.  2005 онд Дани Улсын Үндэсний цагдаагийн газар, Данийн "Хүүхдийг ивээх сан" ТББ болон интернэтийн үйлчилгээ үзүүлэгч байгууллагууд хамтран хүүхэд ашигласан садар самуун контентоос шүүлтүүр ашиглан урьдчилан сэргийлэх сайн дурын хамтын гэрээ, хэлэлцээр байгуулсан. Энэ хүрээнд Дани Улсын Үндэсний цагдаагийн газар “Хүүхдийг ивээх сан”-тай хамтран цахим хуудаснуудад үнэлгээ хийж, хууль бус материал агуулсан веб хуудасны жагсаалтыг интернэт үйлчилгээ үзүүлэгч рүү илгээдэг. Тус жагсаалтыг үндэслэн

[26] The Future Market for Cybersecurity in Denmark, 2022.https://innovationsfonden.dk/sites/default/files/2018-07/thefuturemarketforcybersecurityindenmark.pdf

интернэт үйлчилгээ үзүүлэгч нар тэдгээр веб хуудсыг хаадаг байна. Харин хувь хүмүүс хууль бус контентын талаар Үндэсний цагдаагийн газар эсхүл “Хүүхдийг ивээх сан”-д мэдэгдэж болно.

Дани Улсын Эрүүгийн хуульд бусдыг гүтгэсэн, доромжилсон, арьс өнгө бусад байдлаар ялгаварлан гадуурхсан үйлдлийг гэмт хэрэг гэж үздэг бөгөөд эдгээр гэмт хэргийг интернэт орчинд үйлдэгдсэн бол мөн адил хамаарахаар заасан.

Интернэтээр үйлдэгдсэн тухайн төрлийн гэмт хэргээс урьдчилан сэргийлэх зорилгоор эсхүл онцгой нөхцөл байдлын улмаас шаардлагатай гэж үзвэл шүүхийн шийдвэрийн дагуу хууль бус контент бүхий веб хуудсыг гэмт хэргийн объект хэмээн үзэж хураан авч, хааж болдог.

**Иргэний эрх зүйн хүрээнд:**

Бусдын нэр хүнд, хууль ёсны эрхийг хамгаалах талаарх Иргэний хуулийн заалтуудын хувьд оюуны өмчийн эдийн болон ёс суртахууны эрх ашгийг Зохиогчийн эрхийн тухай хууль, Барааны тэмдгийн тухай хууль, Барааны загвар(Design)-ын тухай зэрэг хэд хэдэн хуулиар хамгаалдаг.

Интернэт үйлчилгээ үзүүлэгчээс интернэт дэх хууль бус контентыг хаах, устгахыг шаардахаас өмнө хууль бус мэдээллийг дэлгэсэн анхдагч эх сурвалж буюу бодитоор зөрчил гаргасан этгээдийн эсрэг захирамж гаргах ёстой. Ийнхүү захирамж гаргахад тодорхой хууль зүйн шаардлага хангагдсан байх учиртай. Тухайлбал:

1. Захирамж гаргуулахаар хүссэн тал нь ийнхүү эрхээ хамгаалуулах эрхтэй байх;
2. Зөрчил гаргагчийн зан үйл нь зайлшгүй захирамж гаргах шаардлагатай байх;
3. Хэрэв тухайн тал үндсэн эрх зүйн маргааны шийдвэрийг хүлээх ёстой тохиолдолд өөрийн эрхийг хамгаалуулахаар захирамж гаргуулах хүсэлт гаргасан талын боломж алдагдана гэсэн утгаараа яаралтай байх.

Цаашдаа захирамж гаргуулах хүсэлт өгсөн тал нь шүүхийн шийдвэр хүчин төгөлдөр болсноос хойш хоёр долоо хоногийн дотор үндсэн эрх зүйн маргаантай холбоотой бодит зөрчигчийн эсрэг шүүх ажиллагаа эхлүүлэх ёстой.

Дани Улсын интернэт үйлчилгээ үзүүлэгчид хууль бус үйлдэл гарсан эсэхийг тогтоох үүрэг хүлээхгүй. Энэ нь хохирсон тал болон зөрчил гаргасан гэж таамаглаж буй талуудын хооронд хэрэг хянан шийдвэрлэх ажиллагааны явцад тогтоогддог. Дани Улсын шүүхээс үйлчилгээ үзүүлэгчдийн эсрэг тодорхой веб хуудаснуудыг татан буулгах, хандахыг хориглох захирамж гаргасан тохиолдолд тэд шүүхийн шийдвэрийг шууд биелүүлнэ.

Зарим тохиолдолд шийдвэр гүйцэтгэх шүүх (the Enforcement court) нь оюуны өмчийн эрхийг зөрчсөн гэх үндэслэлээр холбогдох нотлох баримтыг илрүүлэхийн тулд нэгжлэг хийхийг даалгаж болно. Холбогдох нотлох баримтыг хадгалах шаардлагатай гэж үзвэл баримт бичиг, компьютерын мэдээлэл, программ болон бусад холбогдох материалыг хураан авч, хуулбарлаж болно.

**Захиргааны эрх зүйн хүрээнд:**

Дани Улсад захиргааны эрх бүхий байгууллага хууль бус интернэт контентоос урьдчилан сэргийлэх арга хэмжээ авч болдог.

Жишээлбэл: Мөрийтэй тоглоом нь Данийн засгийн газрын хатуу хяналтад байдаг бөгөөд мөрийтэй тоглоомын бүхий л үйл ажиллагаанд Данийн Тоглоомын газраас тусгай зөвшөөрөл авдаг. Уг журмын хүрээнд зөвшөөрөлгүй зохион байгуулагч руу мөнгө шилжүүлэх, түүнээс мөнгө хүлээн авах, харилцаа холбооны сүлжээгээр дамжуулан хууль бус тоглоомын системд холбогдох, мэдээлэл дамжуулахыг хориглодог байна. Хэрвээ зөвшөөрөлгүй мөрийтэй тоглоом зохион байгуулагч Данийн тоглоомын газрын мэдэгдэлийн дагуу үйл ажиллагаагаа зогсоохгүй байвал тус газраас  холбогдох төлбөрийн болон интернэтийн үйлчилгээ үзүүлэгчийн төлбөрийн гүйлгээ ба интернэт хуудсыг хаадаг. Ингэхдээ интернэт үйлчилгээ үзүүлэгч нар үйлчлүүлэгчдийнхээ хууль тогтоомж мөрдөж буй эсэхэд байнгын хяналт тавих үүрэг хүлээдэггүй учраас Данийн тоглоомын газраас аль домэйн тусгай зөвшөөрөлгүй талаарх мэдээллийг хүсэлт хэлбэрээр тухай бүр интернэт үйлчилгээ үзүүлэгч-д түргэн шуурхай хүргэдэг. Интернэт үйлчилгээ үзүүлэгч энэхүү хүсэлтийн дагуу домэйн хаягийг хаадаг бөгөөд зөрчил арилсан тохиолдолд мөн Данийн тоглоомын газрын мэдэгдлийн дагуу хоригийг цуцладаг. Хэрвээ интернэт үйлчилгээ үзүүлэгч Данийн тоглоомын газрын хүсэлтийг хүлээж аваагүй бол хуулийн дагуу шүүхийн захирамж гаргуулдаг байна.

Түүнчлэн интернэтээр эмийн үйлчилгээ үзүүлэхтэй холбоотой харилцаанд дээрхтэй адил журам мөрдөгдөж байсан боловч хүчингүй болжээ.

**Зөөлөн эрх зүй (**soft law**) зохицуулалтын хүрээнд:**

Европын Холбооны “Цахим худалдааны удирдамж” гэх зэрэг олон улсын стандарт хэм хэмжээнүүд нь энэ чиглэлээр сайн дурын гэрээ хэлэлцээрүүд болон зөөлөн эрх зүйн зохицуулалт (soft law)-ыг бий болгох эрх зүйн үндэслэл болдог байна.

Зөөлөн эрх зүйн зохицуулалтын гол арга хэрэгсэл нь сайн дурын гэрээ, хэлэлцээр ба ёс зүйн дүрэм хэлбэртэй байна. Тухайлбал:

- “DK Hostmaster” корпораци нь .dk-домэйн дор Дани Улсад түгээлт, бүртгэлийг хариуцдаг бөгөөд бүхэлдээ Данийн Интернэт Форум (DIFO) байгууллагын мэдэлд байдаг. “DK Hostmaster”-ын гүйцэтгэх захирал болон Данийн Интернэт Форумийн захирлуудын зөвлөлийн дарга нар харилцан тохиролцож, тухайн домэйныг ашиглах нь 3 дагч этгээдийн оюуны өмчийн эрхийг зөрчих төөрөгдөл үүсгэхээр бол эсхүл тухайн домэйнд хэт доромжилсон, зүй бус контент тавигдсан, фишинг(хэрэглэгчийн хувийн мэдээллийг хууль бусаар авах) хийх, хортой программ(malware) суулгах оролдлого гаргасан зэрэг үндэслэл бүхий байвал домэйныг түдгэлзүүлэх шийдвэр гаргаж болно. Домэйн нь илт хууль бус үйлдэл, эс үйлдэлд ашиглагдах, эсвэл бараг ижил домэйн нэр ашигласан тохиолдолд “DK Hostmaster” тухайн домэйнийг түдгэлзүүлж, хааж эсвэл устгаж болно;

- Данийн харилцаа холбооны салбарын мэргэжлийн байгууллага болох Teleindustrien (TI) нь 2014 оны 9-р сарын байдлаар хууль бус интернэт контентыг хаах, устгах талаар сайн дурын гэрээ байгуулсан. Мөн домэйнийг хориглох, хязгаарлах шийдвэрийн хэрэгжилтийг илүү хялбар, үр ашигтай болгох үүднээс “TI-ийн ёс зүйн дүрэм”-ийг баталсан. Энэхүү ёс зүйн дүрмийг гишүүн байгууллагууд заавал дагаж мөрдөнө. Жишээлбэл: Шүүхээс TI-ын аль нэг гишүүний эзэмшдэг домэйнийг хаах, түдгэлзүүлэх шийдвэр гаргасан тохиолдолд бусад бүх гишүүд тухайн шийдвэрийг 7 хоногийн дотор биелүүлэх үүрэг хүлээдэг;
- Дани Улсын Соёлын яам Ёс зүйн дүрмийн талаар харилцан ойлголцлын санамж бичиг байгуулсан: Тус санамж бичигт Соёлын яам, Эрхийн холбоо болон бусад эрх эзэмшигчид, интернэт үйлчилгээ үзүүлэгчид, төлбөрийн шилжүүлэгийн байгууллагууд (Diners, MasterCard болон Nets), зар сурталчилгааны компаниуд, веб хостинг компаниуд, домэйн бүртгэгчид, Google, Microsoft компаниуд хамрагдсан.

**2. Цахим орчин дахь зөрчлийг шийдвэрлэх журам**

Дани Улсад интернэт контентыг ерөнхийд нь хянадаг тусгайлсан эрх бүхий байгууллага, албан тушаалтан байдаггүй[27]. Харин тухайн чиглэл, чиглэлийн байгууллагууд өөр өөрийн эрх хэмжээний хүрээнд оролцдог.

2007 оноос гэмт хэргээс урьдчилан сэргийлэх, гэмт хэргийг мөрдөн шалгах ажиллагаанд ашиглах зорилгоор интернэт үйлчилгээ үзүүлэгчдэд эцсийн хэрэглэгчийн холболтын замыг харуулах ***(internet traffic monitoring)*** буюу хэрэглэгч ямар, ямар веб хуудсанд зочилсон гэх мэт холбогдох мэдээллийг бүртгэж, хадгалах үүрэг хүлээлгэсэн хэдий ч энэхүү зохицуулалт нь тавьсан зорилгодоо хүрэхүйц тохиромжтой биш гэдэг нь тогтоогдсон гэж үзэж 2014 оны 06 сарын 22-ноос хүчингүй болгосон байна.

Хууль бус интернэт контентыг ихэнхдээ хэрэглэгчийн DNS эсвэл IP хаягийг хаах, хязгаарлах замаар хянадаг учраас голлох зохицуулалт нь зайлшгүй интернэт үйлчилгээ үзүүлэгч нартай холбоотой байдаг. Гэсэн хэдий ч интернэт үйлчилгээ үзүүлэгч нар өөрийн хэрэглэгчдийн дамжуулсан, хадгалсан мэдээлэл хуульд нийцэж байгаа эсэхийг байнга хянах ерөнхий хяналтын үүрэг хүлээдэггүй. Мөн хууль бус үйл ажиллагааны талаар ч заавал мэдээлэх үүрэггүй боловч үндэсний аюулгүй байдал, бусдын амь нас, нийгмийн үнэт зүйл, сайн, сайхан байдлын эсрэг зэрэг тодорхой гэмт хэргийн талаар хэрэв мэдсэн бол мэдээллийг холбогдох байгууллагад дамжуулахаар тус улсын хууль тогтоомжоор зохицуулжээ.

Интернэт үйлчилгээ үзүүлэгчээс хууль бус интернэт контентыг хаах, устгах арга хэмжээг ерөнхийдөө шүүхийн захирамжийн дагуу гүйцэтгэдэг. Холбогдох хүсэлтийн дагуу үндэслэл бүхий байдал тогтоогдвол тухайн захирамжийг дүүргийн, далайн, худалдааны шүүхээс гаргаж болно. Захирамжийн биелэлтийг гүйцэтгэх шүүх ***(Enforcement court)*** хариуцдаг. Шүүхийн удирдлагын тухай хуульд

[27] Comparative Study on Blocking, Filtering and Take-down of Illegal Internet Content, 2015

зааснаар тус захирамжийг Дээд шүүхэд давж заалдаж болно. Ийнхүү давж заалдсан нь захирамжийн биелэлтийг түдгэлзүүлэх үндэслэл болдоггүй.

Мөрийтэй тоглоомын үйл ажиллагаа эрхлэгч Данийн тоглоомын газраас гаргасан шийдвэрийг Үндэсний татварын шүүхэд давж заалдаж болно. Хэрэв интернэт үйлчилгээ үзүүлэгч Данийн тоглоомын газраас ирүүлсэн хууль бус онлайн үйл ажиллагааг хориглох тухай хүсэлтийг биелүүлэхгүй бол шүүхээс захирамж гаргаж шийдвэрлэнэ.

Интернэт домэйнийг түдгэлзүүлэх, хаах, устгахтай холбоотой DK Hostmaster-ийн шийдвэрийг Домэйн нэрийн талаарх Гомдлын Зөвлөлд давж заалддаг. Домэйн нэрийн талаарх гомдлын зөвлөл нь Бизнес, хөгжлийн сайдын томилдог бие даасан зөвлөл юм. Удирдах зөвлөлийн дарга, дэд дарга нар нь гомдлын зөвлөлийн бүрэлдэхүүнд ордог бөгөөд тус зөвлөл нь хууль зүйн онол, практикийн мэдлэгтэй хоёр гишүүн, хэрэглэгчийн болон бизнесийн ашиг сонирхлыг төлөөлдөг хоёр гишүүнээс тус тус бүрдэнэ. Домэйн нэрийн талаарх Гомдлын зөвлөлийн шийдвэрийг Удирдах зөвлөлийн веб хуудсанд нийтэлдэг.

Интернэт дэх контентыг хаах, шүүлтүүрдэх, устгах асуудал нь иргэдийн үзэл бодлоо нээлттэй, чөлөөтэй илэрхийлэх эрх чөлөө болон хууль, эрх зүй олон нийтэд тодорхой, ойлгомжтой байх зарчимтай холбоотойгоор маргаан, мэтгэлцээний асуудал үүсгэдэг.

**Дани Улсын Үндсэн Хуулийн 77 дугаар зүйл[28]:**

*Хэн боловч өөрийн үзэл бодлоо чөлөөтэй илэрхийлэх, бичих, хэвлэн нийтлэх эрхтэй боловч түүнийгээ шүүхийн өмнө бүрэн хариуцах ёстой. Энэ тухайтад цензур болон бусад урьдчилан хянах арга хэмжээг дахин хэзээ ч нэвтрүүлэхгүй.*

Интернэт контентыг шүүлтүүрдэж интернэтэд ерөнхий хяналт тавих, интернэт контентыг хаах, устгах нь Данийн Үндсэн хуулийн 77-р зүйл, мөн Европын Хүний эрхийн тухай конвенцын 10-р зүйлд заасан үзэл бодлоо илэрхийлэх эрх чөлөөнд нийцэж байгаа эсэх хэмээсэн байнгын эргэлзээг агуулж байдаг. Иймээс Дани Улсад интернэт дэх контентыг өргөн хүрээнд, системтэйгээр хянах, шүүлтүүрдэх арга хэмжээ хэрэгжээгүй байна.

## ПОЛЬШ УЛС

### 1. Польш Улсын цахим орчин дахь контент шүүлт

Дэлхий дахинд дижитал үйлчилгээ тархаж, хурдацтай хөгжиж байгаатай зэрэгцэн хууль бус контент буюу бага насны хүүхдийг садар самуунд уруу татах, арьс өнгөөр ялгаварлан гадуурах, худал гүтгэх, доромжлох, үзэн ядсан үг хэллэг, нэр төрд халдах, олон нийтийг худал мэдээлэлээр өдөөн турхирах, онлайн орчид залилах, эд хөрөнгө болон сэтгэл зүйд хохирол учируулах олон сөрөг зүйлс олон нийтийн мэдээллийн сүлжээ цахим орчинд дэлгэрч байна. Иймд дэлхий дахинд хууль бус контентыг түгээхээс сэргийлж, тэдгээрийг шүүлтүүрдэх, хаах үр дүнтэй аргыг бий болгох хэрэгцээ улам бүр нэмэгдсээр байна. Интернэт орчин нь нийгмийн харилцааны чухал хэсэг болж мэдээ мэдээллийг түгээхэд дэмжлэг

[28] Дани Улсын Үндсэн хууль. https://www.thedanishparliament.dk/-/media/sites/ft/pdf/publikationer/engelske-publikationer-pdf/my_constitutional_act_with_explanations.ashx

үзүүлж, санаа бодлоо чөлөөтэй солилцохын оронд үзэн ядсан үг хэллэг, хууль бус үйлдлийг сурталчлах платформ болж байна.

Польш Улсын хүн амын 84.5% буюу 31.97 сая хүн интернэт хэрэглэгч байна. Интернэт орчны харилцааг зохицуулахад олон хуулийн хэрэглээг хамааруулж үзэх шаардлагатай байна. Польш Улсын интернэт орчин дахь цахим харилцааны үндсэн чиг үүргийг хэрэгжүүлэх байгууллага нь "Польш Улсын Цахим харилцааны яам" байна.

Цахим харилцааны яам нь 2002 оны 7 дугаар сарын 18-ны өдрийн "Цахим хэрэгслээр үйлчилгээ үзүүлэх тухай хууль[29]" болон Европын холбооны Зөвлөлийн 2000 оны 6 дугаар сарын 8-ны өдрийн 2000/31/ЕС тоот тогтоолоор батлсан "Цахим үйлчилгээний тухай хууль[30]"-г тус тус суурь болгон үндэслэж олон нийтийн мэдээллийн хэрэгсэл, цахим платформууд болон тухайн платформын хэрэглэгчдийн хууль бус онлайн контентыг хязгаарлах, шүүлтүүрдэх, устгах, мөн бусад арга хэмжээг авч хэрэгжүүлдэг байна. Цахим хэрэгслээр үйлчилгээ үзүүлэх тухай хуулийн 14-р зүйлд ямар тохиолдолд цахим үйлчилгээ үзүүлэгч байгууллага нь хэрэглэгчийн байршуулсан өгөгдөлд болон контентод хандах хандалтыг ямар нөхцөлд хязгаарлаж, хаахыг хялбаршуулсан байдлаар заасан байдаг. Харин тухайн цахим үйлчилгээ үзүүлэгч аж ахуйн нэгж байгууллага нь хэрэглэгчийн байршуулсан контентыг устгахын тулд эхлээд тухайн контентыг хууль бус эсэхийг, өөрөөр хэлбэл, хэрэглэгч үүнийг байршуулсан нь нийтээр дагаж мөрддөг хуулийн заалтыг зөрчсөн эсэхийг тодорхойлох шаардлагатай болно. Хэрэв агуулга нь өөрөө, эсвэл байрлуулсан нь хуулийн заалтыг зөрчөөгүй бол түүнийг устгахыг шаардах үндэслэл байхгүй болно.

Цахим харилцааны яамны контентын зохицуулалттай холбоотой үйл ажиллагааны тэргүүлэх чиглэл бол үг хэлэх, үзэл бодлоо илэрхийлэх эрх чөлөө, хууль бус онлайн контент нийтлэх замаар эрх нь зөрчигдөж буй хүмүүсийн эрхийг хамгаалах үндсэн эрхүүдийн тэнцвэрийг хадгалах явдал юм. Тиймээс Цахим харилцааны яам нь цахим орчин дахь хууль бус мэдээлэлд хандах хандалтыг мэдээлэх, хаах журмыг тодорхойлох, тэдгээрийг уялдуулахад чиглэн ажиллаж байна.

Цахим орчин дахь контентыг хувь хүн, аж ахуй нэгж, байгууллага, олон нийтийн эрх ашигт сөргөөр нөлөөлж байгаа эсэх тухай болон тухайн хууль бус контентын агуулгыг шүүлтүүрдэж, хориглохын тулд дараах хуулиудыг болон бусад холбогдох хуулиудыг судлах шаадлагатай байна. Үүнд:

- Польш Улсын Үндсэн хууль;
- Цахим үйлчилгээний тухай хууль (Европын Холбооны Зөвлөлийн);
- Хэвлэлийн мэдээллийн тухай хууль;
- Кибер аюулгүй байдлын тухай хууль;
- Эрүүгийн хууль;
- Терроризмын эсрэг хууль.

## 2. Европын холбооны "Цахим үйлчилгээний тухай хууль"

Цахим орчныг харилцаа холбооны эрх чөлөөтэй холбож үздэг. Энэ нь олон сая хэрэглэгчдэд өөрийн санал, үзэл бодлоо илэрхийлэх боломжтой хил

[29] https://www.giodo.gov.pl/data/filemanager_en/51.pdf
[30] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2022:277:FULL&from=EN

хязгааргүй орон зай юм. Үүний үр дүнд цахим ертөнц дэх үг хэлэх эрх чөлөөний хязгаарлалтын талаар хэлэлцэх оролдлого нь ихэвчлэн шүүмжлэлд өртөж, онцгой тохиолдолд нийгмийн эмх замбараагүй байдалд хүргэдэг. Гэсэн хэдий ч цахим орчин нь нийгэмд хүчирхийлэл, гүтгэлэг, гадуурхсан контентыг түгээх, сурталчлах, түүнчлэн гэмт хэрэг, тэр дундаа терроризмыг өдөөн турхирч, сурталчлах газар болгож байна.

Европын Холбооны (ЕХ) хууль тогтоох байгууллагын идэвх чармайлтын үр дүнд дижитал үйлчилгээ үзүүлэгч байгууллагууд нь контент шүүлтүүрийн арга хэмжээг автоматаар, мөн урьдчилан сэргийлэх зорилгоор ашиглах нь нэмэгдэж байна. Дижитал үйлчилгээ үзүүлэгч байгууллагууд ихэвчлэн автомат шүүлтүүр буюу "тоон цензур[31] (Digital censorship)"-ыг ашиглаж байна.

Европын холбооны Цахим үйлчилгээний тухай хуульд онлайн контент шүүлтийн тухайд гурван үндсэн чиглэлийг авч үзнэ. Үүнд:

1. гүтгэлэг, үзэн ядсан үг хэллэгээс хамгаалах;
2. оюуны өмчийн эрхийг хамгаалах;
3. олон нийтийн аюулгүй байдлыг хамгаалах арга хэмжээ.

### 3. Үндэсний өв, соёлын яам (The ministry of Culture and National Heritage)

Польш дахь үг хэлэх, хэвлэн нийтлэх эрх чөлөөг “Польш Улсын Үндсэн хууль” болон “Хэвлэлийн тухай хууль”-д заасан байдаг. Польшийн Үндсэн хуулийн 54 дүгээр зүйлийн 1 дэх хэсэгт зааснаар хүн бүр үзэл бодлоо илэрхийлэх, мэдээлэл олж авах, түгээх эрх чөлөөг хангана. Мөн хуулийн 54 дүгээр зүйлийн 2 дахь хэсэгт нийгмийн харилцааны хэрэгсэлд урьдчилан сэргийлэх цензур, хэвлэл мэдээллийн тусгай зөвшөөрөл олгохыг хориглоно гэж заасан[32]. Түүнчлэн Хэвлэлийн тухай хуулийн 1-р зүйлд Үндсэн хуулиар олгогдсон хэвлэлийн эрх чөлөөг заасан байдаг. Дээр дурдсан хууль, журам болон Польш Улсын Үндсэн хуульд заасны дагуу хэвлэл нь үзэл бодлоо чөлөөтэй илэрхийлэх эрхтэй бөгөөд иргэдийн найдвартай мэдээлэл авах, нийгмийн амьдралын ил тод байдал, түүнчлэн нийгмийн хяналт, шүүмжлэлд өртөх эрхийг хэрэгжүүлдэг байна.

Интернэт дэх үзэл бодлоо илэрхийлэх эрх чөлөөний холбогдох хууль эрх зүйн зохицуулалтыг судлахдаа Польшийн Эрүүгийн хуулийн заалтуудыг мөн судлах шаардлагатай.

Эрүүгийн хуулийн 212-р зүйлийн 2-т гүтгэх гэмт хэргийн төрлийг олон нийтийн мэдээллийн хэрэгслээр үйлдэх тухай заасан байна. Тус заалт нь:

Хувь хүн, хэсэг бүлэг хүмүүс болон аж ахуйн нэгж, байгууллага олон нийтийн санаа бодлыг эсэргүүцэн гутаан доромжлох, тэдгээрийн албан тушаал, ажил мэргэжил, үйл ажиллагаанд болон эрх ашгийг нь алдагдуулахуйц хэмжээнд гүтгэсэн бол тухайн иргэнийг торгох эсвэл эрх чөлөөг хязгаарлах шийтгэл ногдуулдаг байна.

### 4. Дотоод хэргийн яам (Ministry of Interior and Administration)

[31] https://www.sciencedirect.com/science/article/pii/S0267364922000826
[32] https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/ContentRegulation/Poland.pdf

Тодорхой заалтуудын тухайд, 2016 оны 6 дугаар сарын 10-ны өдрийн “Терроризмын эсрэг үйл ажиллагааны тухай хууль”-аар мөн 2002 оны 5 дугаар сарын 24-ний өдрийн "Дотоодын аюулгүй байдлын газар, Гадаад тагнуулын газрын тухай хууль”-д нэмэлт, өөрчлөлт оруулснаар цахим орчин дахь террорист суртал ухуулгатай тэмцэхэд чиглэсэн арга хэмжээнүүдийг тусгаж, тусгайлсан террорист үйл явдал үүсгэх зорилготой интернэтийн мэдээлэл, үйлчилгээг хааж ашиглахыг хориглохоор заасан байна[33].

“Дотоод аюулгүй байдлын алба, Гадаад тагнуулын газрын тухай хууль”-ийн 32-р зүйлийн 1 дэх хэсэгт заасны дагуу шүүх (Ерөнхий прокурорын зөвшөөрлөөр гаргасан Дотоод аюулгүй байдлын газрын даргын өргөдлийн дагуу) цахим үйлчилгээ үзүүлэгч байгууллагууд нь тодорхой заасан мэдээлэлд нэвтрэх эрхийг хориглох, эсвэл террорист үйл явдалтай холбоотой болон террорист үйл явдал үүсгэхэд ашиглагдах мэдээлэл үйлчилгээг устгах зэрэг арга хэмжээг авч болно. Дээр дурдсан эрх мэдлийг зөвхөн терроризмын гэмт хэргээс урьдчилан сэргийлэх, таслан зогсоох, мөрдөн шалгах зорилгоор ашиглаж болно. "Террорист гэмт хэрэг" гэсэн ойлголтыг Польшийн Эрүүгийн хуульд нарийн тодорхойлсон байна. 1997 оны 6-р сарын 6-ны өдрийн Эрүүгийн хуулийн 115-р зүйлийн 20-д зааснаар террорист гэмт хэрэг нь дараах зорилгоор үйлдэхийг хориглосон үйлдэл юм. Үүнд:

1. олон нийтийг ноцтой айлган сүрдүүлэх;
2. Польш Улс, бусад улсын төрийн байгууллага, олон улсын байгууллагын эрх бүхий байгууллагыг тодорхой үйл ажиллагаа явуулах, эсхүл татгалзахыг албадах;
3. Польш Улсын эдийн засагт ноцтой хохирол учруулах, түүнчлэн ийм үйлдэл хийхээр заналхийлэх.

Террорист үйл явдалтай холбоотой, эсвэл террорист үйл явдал үүсгэхэд ашиглагдаж байгаа мэдээлэл, үйлчилгээнд хандах хандалтыг зөвхөн террорист гэмт хэргээс урьдчилан сэргийлэх, эсэргүүцэх, мөрдөн шалгах зорилгоор хаахыг зөвшөөрдөг байна. Энэ нь олон улсын хууль тогтоомжид нийцсэн байна.

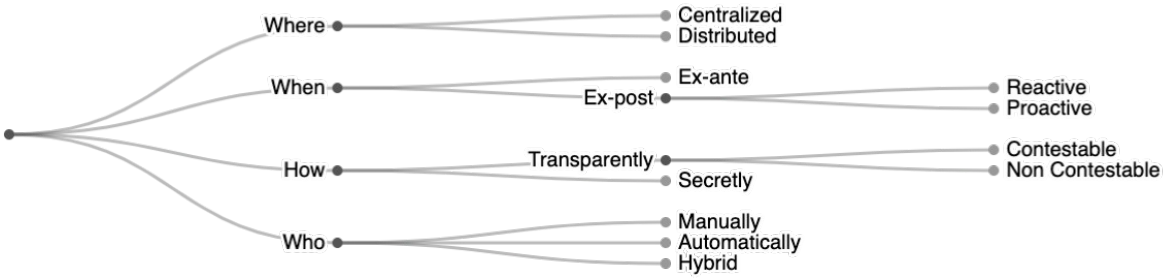
## 5. Европын холбооны цахим орчин дахь контент шүүлт

Шүүлтүүрийг хаана хэрэглэгдэж байгаа болон тухайн цахим үйлчилгээ үзүүлэгч байгууллагын бүтэц зохион байгуулалтын төрлөөс хамааран дараах байдлаар ангилна[34].

1. Centralized - Төвлөрсөн шүүлт буюу бүх платформ дээр хэрэгжих нэгдсэн бодлогын дагуу нэг зохицуулах нэгжээс хэрэгжүүлдэг төвлөрсөн шүүлтүүр.
2. Distributed - Төвлөрсөн бус шүүлтүүр буюу олон хуваарилагдсан зохицуулагч нар тус тусын тодорхой хэмжээнд бие даасан байдлаар ажиллаж, платформ доторх дэд бүлгүүдэд өөр өөр бодлогыг хэрэгжүүлдэг байна.
3. Ex-ante - Контент нь платформ дээр тавигдахаас өмнө хэрэглэгдэх шүүлтүүр;

[33]https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/ContentRegulation/Poland.pdf
[34] https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU(2020)657101_EN.pdf

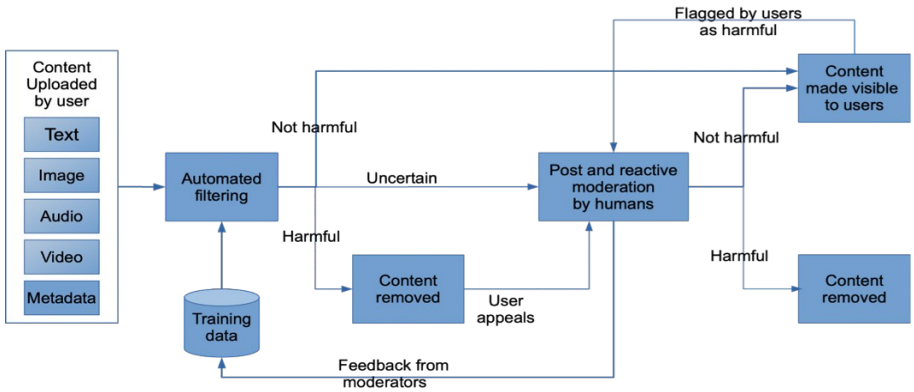
4. Ex-post - Контент нь платформ дээр тавигдсан, хэрэглэгчид хандах боломжтой контентод хэрэглэгдэх шүүлтүүр;
5. Transparently - Платформоос тухайн контентыг хассан тухай мэдээлэл өгдөг ил тод шүүлтүүр;
6. Secretly - Нууц шүүлтүүр, энэ нь хассан талаар ямар ч мэдээлэл өгдөггүй;
7. Contestable - Платформ нь байршуулагчдад шүүлтийн үр дүнг эсэргүүцэх, тухайн асуудлаар шинэ шийдвэр гаргах арга замыг санал болгодог маргаантай шүүлтүүр;
8. Non Contestable - Байршуулагчдад ямар ч арга хэмжээ авах боломжгүй, маргаангүй шүүлтүүр;
9. Manually - Гараар шүүх, хүнээр гүйцэтгэдэг;
10. Automatically - Алгоритмын хэрэглүүрээр гүйцэтгэдэг автомат шүүлтүүр;
11. Hybrid - Энэ нь хүн болон автоматжуулсан хэрэгслүүдийн хослолоор гүйцэтгэдэг.




Зураг 4. Цахим орчин дахь контент шүүлтийн төрлүүд.

Автомат шүүлтүүр нь хэрэглэгчийн үүсгэсэн контентыг боловсруулж эхний шүүлтийн алхмыг хийнэ. Шүүлтүүр нь өөрөө тодорхой зүйлийг зүй бус гэж ангилж болох бөгөөд энэ нь эдгээр зүйлсийг автоматаар устгахад хүргэх эсвэл тодорхой хор хөнөөлгүй гэж ангилдаг.

Автомат шүүлтүүр нь зарим хэвийн боловч утга агуулга нь тодорхой бус контентыг бүрэн таньж чадаагүйн улмаас хор хөнөөл учруулж болзошгүй гэж ангилж болох бөгөөд үүний дагуу блоклох эсвэл устгах боломжтой юм. Энэ тохиолдолд автомат устгалын эсрэг хэрэглэгчийн гомдлын дагуу тухайн контентыг таньж нийтлэхийн тулд хүний оролцоотойгоор дахин шүүж болно.




Зураг 7. Цахим орчин дахь контентын автомат шүүлтүүр.

## ЯПОН УЛС

Япон Улсад цахим орчин дахь контент түгээлт нь олон нийтэд нээлттэй, өргөн нэвтрүүлгийн адилаар мэдээллийг хүчтэй түгээх хэрэгсэлд тооцогддог. Тиймээс олон нийтийн харилцааны контентыг үзэл бодлоо илэрхийлэх эрх чөлөөгөөр хангах ёстой гэж үздэг[35]. Үүний гол хүчин зүйл нь интернэт орчныг сайжруулж, зүй зохистой ашиглах, эзэмших болон нийгэмд хортой, зүй бус мэдээллийг хязгаарлах арга хэмжээнд чиглэгддэг.

### 1. Цахим орчин дахь эрх зүйн зохицуулалт

Зүй бус мэдээллийг хязгаарлахын тулд интернэтийн сайтуудыг тодорхой шалгуурын дагуу үнэлж, ялгаж салгах шүүлтүүр хэрэгтэй болдог. Шүүлтүүр нь интернэтийн үйлчилгээ үзүүлэгч болон үүрэн телефоны операторуудын ажиллуулдаг компьютер, программ хангамжийн тусламжтайгаар мэдээллийг зөвшөөрөх болон хориглох үйлдлийг хийнэ.
Шүүлтүүрийн хоёр арга байдаг:

1. Цагаан жагсаалтын арга: Зөвхөн хүүхдэд аюулгүй, тодорхой шалгуур, стандартыг хангасан сайтуудад хандах боломж олгодог бөгөөд бусад сайтуудад орох эрхийг хязгаарлана;
2. Хар жагсаалтын арга: Зарчмын хувьд бүх сайт руу нэвтэрч болно. Гэхдээ насанд хүрэгчдийн болон мөрийтэй тоглоом тоглох гэх мэт зүй бус гэж үзсэн тодорхой сайтуудад хандах хандалтыг хязгаарладаг арга юм.

Үүрэн телефоны операторууд болон бусад компаниуд дээрх шүүлтүүрийн үйлчилгээг үзүүлдэг. Цахим орчин дахь мэдээллийн заримыг нь нас, гэр бүлийн нөхцөл байдлын дагуу тохируулах боломжтой байдаг.

Мөн зүй бус, насны хязгаарлалттай мэдээллийн хуудсууд насанд хүрэгчдийн хуудас, болзох хуудсууд гэх мэт хүүхдүүд нэвтрэхийг хориглосон, хууль бус мэдээллийн хуудсууд орно.

2009 оны 3 сард ***Хүүхдийн садар самуунаас урьдчилан сэргийлэх зөвлөлөөс*** [36]Цагдаагийн ерөнхий газрын судалгааны ажлын хэсгийн Аюулгүй байдлын эсрэг иж бүрэн зөвлөлийн тайланд интернэт хэрэглэгчид шүүлтүүр ашиглах, үйлчилгээ үзүүлэгчээс хаах нь гэмт хэргээс урьдчилан сэргийлнэ гэж заасан байна.

Япон Улсад цахим орчин дахь контентын шүүлтүүрийн талаарх тусгайлан зохицуулсан хууль тогтоомж байдаггүй бөгөөд цахим орчныг хөгжүүлэх талаар эрх зүйн тогтолцоондоо дараах хуулиар зүй бус мэдээллийн шүүлтүүрийн талаар зохицуулсан.

***Интернэтийг аюулгүй ашиглах орчныг хөгжүүлэх тухай хууль***[37] нь 2008 оны 6 сард батлагдсан. Тус хууль нь 6 бүлэг 31 зүйлтэй.

---

[35] Судалгаа https://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/shohi/pdf/070911_2_15-5_2.pdf
[36] Хүүхдийн садар самууныг түгээхээс урьдчилан сэргийлэх зөвлөл https://www.iajapan.org/press/20090602-press.html
[37] Залуучуудын интернэтийг аюулгүй ашиглах орчныг хөгжүүлэх тухай хууль https://elaws.e-gov.go.jp/document?lawid=420AC1000000079

**Хуулийн зорилго нь:** цахим орчинд насанд хүрээгүй хүүхдэд зүй бус мэдээлэл өргөн тархаж байгаатай холбогдуулан энэ хуулиар насанд хүрээгүй хүүхдэд интернэтийг зүй зохистой ашиглах чадварыг эзэмшүүлэхэд шаардлагатай арга хэмжээг авч, зүй бус мэдээллийг шүүх программ хангамжийн ажиллагааг сайжруулсан.

Энэхүү хууль нь 2018, 2019 оны шинэчилсэн найруулгаар шүүлтүүрийн зорилтыг "Үүрэн телефоны шугам ашиглан интернэтэд нэвтрэх боломжтой төхөөрөмжүүд" болгон өргөжүүлсэн бөгөөд ухаалаг утас, таблет терминалууд ч шүүлтүүрт хамрагдах болно гэдгийг тодруулсан.

Үүний зэрэгцээ цахим хэрэглэгч нь асран хамгаалагчийн нэр дээр байсан ч хэрэв хэрэглэгч хүүхэд бол хүүхэд, асран хамгаалагчид шүүлтүүрийн талаар мэдээлэл өгдөг байна. Үүнээс гадна цахим орчин дахь зүй бус мэдээллийг хамгаалдаг шүүлтүүрийн программ хангамжийг эхнээс нь суулгаж урьдчилан сэргийлдэг байна.

Тус хуульд “Насанд хүрээгүй хүүхдэд зүй бус мэдээллийг хязгаарлах программ хангамж”-ийг тодорхойлсон байна. Интернэтээр дамжуулан олон нийтэд үзэх боломжтой мэдээллийг тодорхой шалгуурын дагуу хязгаарлахаар заасан байдаг.

Тус хуульд цахим орчин дахь шүүлтүүрийн зохицуулалт нь дараах зүйл заалтуудад тусгагдсан байна.

**10 дугаар зүйл.** Засгийн газар, орон нутгийн засаг захиргаа нь өсвөр насны хүүхдүүд гэртээ интернэт ашиглах үед насанд хүрээгүй хүүхдэд зүй бус мэдээллийг шүүх программ хангамжийн хэрэглээг түгээн дэлгэрүүлэхэд шаардлагатай арга хэмжээг авна.

**15 дугаар зүйл**. Үйлчилгээний гэрээний нөгөө тал буюу үйлчилгээний гэрээний үүрэн телефоны терминалын хэрэглэгч нь насанд хүрээгүй хүн бол үүрэн телефоны интернэт холболтын үйлчилгээ үзүүлэгч нь насанд хүрээгүй хүүхдэд хор хөнөөлтэй мэдээллийг шүүх үйлчилгээг ашиглана. Гэхдээ насанд хүрээгүй хүүхдийн асран хамгаалагч нь насанд хүрээгүй хүүхдэд зүй бус мэдээллийг шүүх үйлчилгээг ашиглахгүй байх хүсэлт гаргасан бол энэ нь хамаарахгүй.

**16 дугаар зүйл**. Гар утасны интернэт холболтын үйлчилгээ үзүүлэгч байгууллага нь насанд хүрээгүй хүүхдэд зүй бус мэдээллийг шүүх боломжийг олгодог.

**20 дугаар зүйл**. Насанд хүрээгүй хүүхдэд зүй бус мэдээллийг өгөхгүй байх талаар гэрээ хийдэг байна. Үүнд:

1. Өсвөр насны хүүхдийн хөгжлийн үе шат, хэрэглэгчийн сонголтоос хамааран үзэхийг хязгаарласан мэдээллийн нарийвчилсан тохиргоог идэвхжүүлэх.
2. Зарим хязгаарлах шаардлагагүй мэдээллийг чөлөөтэй өгнө.

**24 дүгээр зүйл (5-р бүлэг)** Хувийн байгууллагууд интернэтийг зүй зохистой ашиглахтай холбоотой бүртгэл.

1. Насанд хүрээгүй хүүхдэд зүй бус мэдээллийг шүүх программ хангамжийн үйл ажиллагааг сайжруулах үйл ажиллагааг Дотоод хэрэг, харилцаа холбооны сайд болон Эдийн засаг, худалдаа, аж үйлдвэрийн сайд нар хариуцдаг ба дараах үүрэгтэй.

- Насанд хүрээгүй хүүхдэд зүй бус мэдээллийг хязгаарлах асуудлыг судлах, олон нийтэд таниулах, мэдээлэл өгөх;
- Цахим орчин дахь мэдээллийг шүүх программ хангамжийн технологийн хөгжүүлэхийг дэмжих;

2. Бүртгэлийг авах хүсэлтэй байгууллага нь хуульд заасны дагуу Дотоод хэрэг, харилцаа холбооны сайд, Эдийн засаг, худалдаа, аж үйлдвэрийн сайдад хүсэлт гаргаснаар бүртгэнэ.
3. Интернэтээр хангах боломжтой тоног төхөөрөмжтэй байгууллагууд дараах шалгуурыг хангасан байна.

- Насанд хүрээгүй хүүхдэд зүй бус мэдээллийг шүүх программ хангамж боловсруулах туршлагатай эсвэл нэг жил ба түүнээс дээш жил тухайн салбарт ажилласан туршлагатай байх;

4. Шүүлтүүр сурталчилгааны ажлыг зохих ёсоор явуулахын тулд дараах арга хэмжээг авна.

- Цахим орчин дахь шүүлтүүрийн арга хэмжээг олонд таниулах ажлыг хариуцсан эрх мэдэл бүхий этгээдийг (админ) томилно.
- Цахим орчин дахь шүүлтүүрийн арга хэмжээг олонд таниулах ажилтай холбоотой баримт бичгүүдийг бэлтгэнэ.
  - Бүртгэлийн огноо, бүртгэлийн дугаар
  - Бүртгэлтэй этгээдийн нэр, хаяг;
  - Шүүлтүүрийг дэмжих байгууллага нь шүүлтүүрийг дэмжих бизнес эрхэлдэг оффисын байршил;

## 2. Цахим орчин дахь шүүлтүүрийн зохицуулалт

### Дотоод хэрэг харилцаа холбооны яам[38]

Цахим орчин дах хууль бус, зүй бус үйлдлийн талаар мэдээлэл авч, зохих хариу арга хэмжээний талаар мэргэжлийн зөвлөгөө өгдөг. ***Хууль бус, зүй бус мэдээллийн зөвлөлдөх төв***[39]-ийг Дотоод хэрэг, харилцаа холбооны яам комисс байгуулж, ажиллуулдаг.

**Хууль бус, зүй бус мэдээллийн зөвлөгөө өгөх төв нь** интернэт дэх хууль бус, хор хөнөөлтэй мэдээлэлд зохих хариу арга хэмжээг олон нийтэд таниулах, сурталчлах зорилготой.

Интернэтийн ерөнхий хэрэглэгчид, үйлчилгээ үзүүлэгчид, мэдээллийн салбарын менежерүүд, сургуулийн удирдлагууд, хэрэглэгчийн асуудал эрхэлсэн зөвлөх төв, хууль зүйн товчоо, хүний эрхийг хамгаалах байгууллага гэх мэт интернэтийн орчинтой холбоотой өргөн хүрээний хүмүүсээс зөвлөгөө авдаг.

### Эдийн засаг, худалдаа аж үйлдвэрийн яам[40]

Эдийн засаг, худалдаа, аж үйлдвэрийн яам нь интернэт дэх шүүлтүүрт ашигладаг төрөл бүрийн контентын үнэлгээний стандартыг боловсруулж, хувийн байгууллагуудтай хамтран мэдээлэл сурталчилгааны ажлыг зохион байгуулж, интернэтийн аюулгүй, найдвартай хэрэглээг дэмжих зорилготой байна.

### Японы интернэт үйлчилгээ үзүүлэгчдийн холбоо[41] (JAIPA)

[38] Дотоод хэрэг харилцаа холбооны яам https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/filtering.html
[39] Хууль бус, хор хөнөөлтэй мэдээллийн зөвлөлдөх төв https://ihaho.jp/
[40] Эдийн засаг, худалдаа аж үйлдвэрийн яам https://www.meti.go.jp/policy/it_policy/policy/filtering.html
[41] Японы интернэт үйлчилгээ үзүүлэгчдийн холбоо https://www.jaipa.or.jp/about/

Тус холбоо нь интернэтийн үйлчилгээг хэрэглэгчдэд шууд үзүүлэх бөгөөд хэрэглэгчдийн интернэттэй холбоотой асуудлуудад хамтран ажиллаж, хэрэглэгчдийн нийтлэг эрх ашгийг хамгаална. Түүнчлэн Засгийн газар болон хувийн байгууллагуудтай харилцах, холбох үүргийг гүйцэтгэдэг.

**ЭХ СУРВАЛЖИЙН ЖАГСААЛТ**

**ЭСТОНИ**

- Uropean Electronic Communications Code https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1547633333762&uri=CELEX:32018L1972
- Electronic Communications Act https://www.riigiteataja.ee/en/eli/501042015003/consolide
- Persocnal Data Protection Act https://www.riigiteataja.ee/en/eli/523012019001/consolide
- Information Society Services Act https://www.riigiteataja.ee/en/eli/504112013008/consolide
- Public Information Act https://www.riigiteataja.ee/en/eli/ee/522122014002/consolide/current
- Population register Act https://www.riigiteataja.ee/en/eli/516012014003/consolide
- Digital Signatures Act https://www.riigiteataja.ee/en/eli/530102013080/consolide
- Cybersecurity Act https://www.riigiteataja.ee/en/eli/523052018003/consolide
- E-Governance https://ega.ee/wp-content/uploads/2016/06/e-Estonia-e-Governance-in-Practice.pdf
- Estonian internet freedom https://freedomhouse.org/country/estonia/freedom-net/2022#footnote3_20ljfol
- Information System Authority https://www.ria.ee/en/cyber-security/handling-cyber-incidents-cert-ee/monitoring-cyberspace-and-impeding-incidents

**БНСУ**

- Analysis: South Korea’s New tool for filtering illegal internet content By Robert Morgus, Justin Sherman, and Seonghyun Nam
- Analysis: Russia’s Plans for a National internet https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/russias-plans-for-a-national-internet/
- http://service.kocsc.or.kr/eng/PageLink.do
- https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/analysis-south-koreas-sni-monitoring/
- http://www.korea.kr/news/actuallyView.do?newsId=148858720
-

**ДАНИ**

- Дани Улсын албан ёсны цахим хуудас. https://denmark.dk
- Британника цахим нэвтэрхий толь. https://www.britannica.com/place/Denmark
- Дани Улсын хүн ам. https://www.dst.dk/en/Statistik/emner/borgere/befolkning
- Дани Улсын нэг хүнд ногдох ДНБ, Дэлхийн Банк. https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=DK
- Цахим эдийн засаг, нийгмийн индекс(DESI) https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2021

- E-Government Survey 2020, UN. https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf
- Дани Улсын Цахим засаглалын агентлагийн цахим хуудас. https://en.digst.dk
- The Future Market for Cybersecurity in Denmark, 2022. https://innovationsfonden.dk/sites/default/files/2018-07/thefuturemarketforcybersecurityindenmark.pdf
- Danish Censorship. https://censorship.fandom.com/wiki/Denmark
- What Is Content Filtering? Definition, Types, and Best Practices. https://www.spiceworks.com/it-security/network-security/articles/what-is-content-filtering-definition-types-and-best-practices/
- Comparative Study on Blocking, Filtering and Take-down of Illegal Internet Content. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680658546
- Дани Улсын Үндсэн хууль. https://www.thedanishparliament.dk/-/media/sites/ft/pdf/publikationer/engelske-publikationer-pdf/my_constitutional_act_with_explanations.ashx

**ПОЛЬШ**

- Польш Улсын Цахим хэрэгслээр үйлчилгээ үзүүлэх тухай хууль (Providing Services by Electronic Means) - https://www.giodo.gov.pl/data/filemanager_en/51.pdf
- Европын Холбооны Цахим үйлчилгээ үзүүлэх тухай хууль (Digital Services Act) - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2022:277:FULL&from=EN
- Европын Холбооны Контент Шүүлтүүрийн хууль - https://www.sciencedirect.com/science/article/pii/S0267364922000826
- Польш Улсын цахим орчны хууль, эрх зүйн зохицуулалт бодлого - https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/ContentRegulation/Poland.pdf
- Европын Холбооны Контент шүүлтийн төрөл, арга хэрэгсэл - https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU(2020)657101_EN.pdf

**ЯПОН**

- https://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/shohi/pdf/070911_2_15-5_2.pdf
- Хүүхдийн садар самууныг түгээхээс урьдчилан сэргийлэх зөвлөл https://www.iajapan.org/press/20090602-press.html
- Залуучуудын интернэтийг аюулгүй ашиглах орчныг хөгжүүлэх тухай хууль https://elaws.e-gov.go.jp/document?lawid=420AC1000000079
- Дотоод хэрэг харилцаа холбооны яам https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/filtering.html

- Хууль бус, хор хөнөөлтэй мэдээллийн зөвлөлдөх төв https://ihaho.jp/
- Эдийн засаг, худалдаа аж үйлдвэрийн яам https://www.meti.go.jp/policy/it_policy/policy/filtering.html
- Японы интернэт үйлчилгээ үзүүлэгчдийн холбоо https://www.jaipa.or.jp/about/