



EU 집행위원회 초청
한국 - EU 전문가 포럼

디지털 서비스법 **DSA의 균형모델과 한국형 입법의 실천적 과제**

2026년 4월 8일 (수) 14시 · 제2소회의실

사회 오경미 오픈넷 연구원

세션1 DSA 심층 분석

기조발제 DSA Overview

Joris van Hoboken 암스테르담 대학교 교수

발제 1 DSA의 Architecture

Menno Cox 유럽연합 집행위원회(EC) 디지털 서비스 글로벌 섹터장

2 거버넌스 시스템

Julian Ringhof 유럽연합 집행위원회(EC) DSA 정책관

세션2 한국형 디지털서비스법 입법의 실천적 과제

발제 1 행정심치, 의무적 임시조치 그리고 표현의 자유

박경신 고려대학교 법학전문대학원 교수

2 정통방법 체계와 DSA 구조적 정합성 진단 그리고 '협력적 거버넌스'

오병일 디지털정의네트워크 대표

주최



국회의원 **이주희 · 김우영 · 한민수 · 전진숙 · 박지혜**



21조넷

PROGRAM

세션1. DSA 심층 분석

기초발제	DSA Overview
	Joris van Hoboken 암스테르담 대학교 교수
발제1	DSA의 Architecture
	Menno Cox 유럽연합 집행위원회(EC) 디지털 서비스 글로벌 섹터장
발제2	거버넌스 시스템
	Julian Ringhof 유럽연합 집행위원회(EC) DSA 정책관

세션2. 한국형 디지털서비스업 입법의 실천적 과제

발제1	행정심의, 의무적 임시조치 그리고 표현의 자유
	박경신 고려대학교 법학전문대학원 교수
발제2	정통방법 체계와 DSA 구조적 정합성 진단 그리고 '협력적 거버넌스'
	오병일 디지털정의네트워크 대표

목차

인사말	6
이주희, 전진숙, 박지혜, 한민수 국회의원	
DSA Overview	13
Joris van Hoboken 암스테르담 대학교 교수	
DSA의 Architecture	39
Menno Cox 유럽연합 집행위원회(EC) 디지털 서비스 글로벌 섹터장	
거버넌스 시스템	41
Julian Ringhof 유럽연합 집행위원회(EC) DSA 정책관	
행정심의, 의무적 임시조치 그리고 표현의 자유	43
박경신 고려대학교 법학전문대학원 교수	
정통방법 체계와 DSA 구조적 정합성 진단 그리고 '협력적 거버넌스'	59
오병일 디지털정의네트워크 대표	

인사말 1



안녕하십니까. 이주희 국회의원입니다.

‘EU 집행위원회 전문가 초청 한-EU 전문가 포럼: DSA의 균형 모델과 한국형 입법의 실천적 과제’에 함께해주신 모든 분들께 깊이 감사드립니다. 바쁘신 가운데 뜻깊은 자리에 함께해주신 국내외 발제자와 토론자, 관계자 여러분께 환영의 말씀을 드립니다. 이번 포럼은 EU 디지털서비스법(DSA)의 구조와 운영 경험을 면밀히 살펴보고, 이를 바탕으로 한국 사회에 필요한 디지털서비스법의 방향과 실천 과제를 모색하기 위해 마련되었습니다.

오늘날 디지털 공론장은 민주주의와 시민의 일상에 막대한 영향을 미치고 있습니다. 특히 인공지능 기술의 확산과 플랫폼의 고도화는 정보 유통의 속도와 규모를 비약적으로 키웠고, 그만큼 허위정보와 혐오표현, 각종 유해정보가 사회에 미치는 파장도 훨씬 커졌습니다. 그러나 그 대응이 국가에 의한 과도한 통제나 표현의 자유 침해로 이어져서는 안 됩니다. 정보의 건전성을 확보하는 일과 표현의 자유를 지키는 일은 서로 배치되는 가치가 아니라, 함께 지켜내야 할 민주주의의 핵심 원칙입니다. 이번 포럼이 바로 그 균형점을 찾기 위한 진지한 논의의 장이 되기를 기대합니다.

EU의 DSA는 온라인 안전, 민주주의적 절차의 보호, 기본권 보장을 함께 고려한 규율 체계라는 점에서 중요한 시사점을 줍니다. 동시에 한국은 방송미디어통신심의위원회 중심의 행정심의, 의무적 임시조치, 정보통신망법 체계 등 고유한 제도적 경로를 가지고 있습니다. 따라서 우리는 유럽의 제도를 단순히 모방하는 데 그쳐서는 안 됩니다. 한국 사회의 현실, 우리의 법체계, 시민의 기본권 보장 원칙에 비추어 어떤 제도가 실질적으로 작동할 수 있는지 치열하게 검토해야 합니다. 오늘 이 자리에서 DSA의 구조, 거버넌스, 위험기반 접근, 그리고 한국적 적용 가능성에 대한 깊이 있는 논의가 이뤄지기를 바랍니다.

이번 포럼에는 유럽집행위원회 실무 책임자와 학계 전문가, 그리고 국내의 법률·정책 전문가들이 함께합니다. DSA의 전반적 구조와 설계 원칙, 유럽의 감독 체계, 그리고 한국 인터넷 규제의 특수성과 협력적 거버넌스의 과제를 함께 논의하는 오늘의 자리가 앞으로 우리 국회의 입법 논의에도 매우 소중한 자산이 될 것이라고 생각합니다. 특히 온라인 플랫폼의 책임성과 투명성, 이용자 권리구제, 공적 감독과 다자간 협력 구조를 어떻게 정교하게 설계할 것인지에 대한 실질적 해법이 도출되기를 기대합니다.

디지털 공간의 질서를 새롭게 설계하는 일은 더 이상 미룰 수 없는 과제입니다. 이용자 보호와 표현의 자유, 혁신과 책임, 안전과 권리 보장이 조화를 이루는 한국형 디지털서비스법의 방향을 찾는 데 국회도 책임 있게 역할을 다하겠습니다. 오늘 포럼이 그 출발점이자 디딤돌이 되기를 바랍니다.

다시 한번 함께해주신 모든 분들께 감사드립니다.

2026년 4월 8일
국회 과학기술정보방송통신위원회
더불어민주당 국회의원 이주희

인사말 2



안녕하십니까.

국회 보건복지위원회와 성평등가족위원회 위원으로 활동하고 있는 광주 복구를 더불어민주당 국회의원 전진숙입니다.

오늘 「EU집행위 전문가 초청 포럼(DSA의 균형 모델과 한국형 입법의 실천적 과제)」을 함께하게 되어 매우 뜻깊게 생각합니다. 귀한 자리를 마련해주신 관계자 여러분과 함께해주신 전문가 여러분께 깊이 감사드립니다.

디지털 플랫폼은 이제 단순한 소통 공간이 아니라 뉴스 소비와 여론 형성, 일상과 민주주의를 좌우하는 핵심 인프라가 되었습니다. 그만큼 플랫폼의 책임과 공적 규율도 더 이상 미룰 수 없는 과제가 되었습니다.

작년부터 이주희의원께서 꾸준히 국회 토론회를 진행하시며 한국형 DSA(Digital Services Act, 디지털서비스법)의 입법 필요성과 허위조작정보 대응, 플랫폼 책임성 강화, 알고리즘 투명성, 이용자 권리보호라는 방향을 제시해주시고 있다는 것을 잘 압니다.

특히 최근에는 딥페이크 성착취물, 여성혐오적 콘텐츠, 성별 고정관념을 강화하는 추천 알고리즘 구조가 심각한 사회문제로 떠오르고 있습니다. 경찰청은 약 7개월간의 집중단속에서 딥페이크 성범죄 관련 963명을 검거하고 59명을 구속했다고 밝혔고, 2024년 디지털성범죄 피해자 지원 인원도 1만 305명으로 전년보다 14.7% 증가했습니다. 국가인권위원회 조사에서는 온라인 혐오표현의 주요 대상이 여성이라는 응답이 80.4%로 가장 높게 나타났습니다. 이는 디지털 안전의 문제가 곧 성평등의 문제이기도 하다는 점을 보여주는 중요한 지표라고 생각합니다.

플랫폼이 방치한 혐오와 왜곡, 딥페이크와 디지털 성폭력, 편향적 추천 구조는 단지 온라인상의 불쾌함이나 일시적 부작용이 아닙니다. 그것은 여성과 아동·청소년, 사회적 소수자의 존엄과 안전, 평등한 참여권을 침해하는 구조적 폭력이며, 결국 민주주의의 기반을 훼손하는 문제입니다. 이러한 문제의식은 작년 자료집에서 강조된 “안전한 디지털 환경”과 “이용자의 기본권 보호”라는 한국형 DSA 논의의 방향과도 맞닿아 있습니다.

유럽 「디지털서비스법」이 보여준 것은 국가의 일방적 통제가 아니라, 플랫폼의 시스템적 위험을 점검하고 이용자 권리를 함께 보호하는 균형 있는 규율 모델입니다. 한국형 입법도 허위조작정보 대응을 넘어, 젠더 기반 온라인 폭력과 알고리즘 편향까지 포괄하는 실천적 입법으로 나아가야 합니다.

오늘 포럼이 더 안전하고 더 평등한 디지털 공론장을 만들기 위한 뜻깊은 출발점이 되기를 기대합니다.

감사합니다.

2026년 4월
국회의원 전진숙

인사말 3



안녕하십니까. 더불어민주당 의정부시갑 박지혜 국회의원입니다.

오늘 「한-EU 전문가 포럼 - 디지털 서비스법(DSA)의 균형 모델과 한국형 입법의 실천적 과제」 토론회 개최를 진심으로 뜻깊게 생각합니다. 무엇보다 바쁜 일정에도 불구하고 발제와 토론을 위해 함께해 주신 국내외 전문가 여러분께 깊이 감사드립니다.

오늘 우리가 논의하고자 하는 디지털 서비스법, 즉 DSA는 단순한 플랫폼 규제 법안을 넘어, 표현의 자유와 정보의 건전성이라는 두 가치 사이의 균형을 어떻게 설계할 것인가라는 매우 근본적인 질문을 던지고 있습니다.

특히 인공지능과 알고리즘이 정보 유통의 중심이 된 시대에서, 이 문제는 더 이상 선택이 아니라 반드시 해결해야 할 과제가 되었습니다. 유럽연합의 DSA는 국가의 직접적 통제를 최소화하면서도 플랫폼의 책임성과 투명성을 높이려는 ‘균형 모델’이라는 점에서 매우 중요한 시사점을 제공해 준다고 생각합니다.

유럽의 제도를 그대로 가져오기 보다는 한국의 법제도와 역사, 그리고 사회적 맥락에 맞게 재설계 되어야 한다고 생각합니다. 이런 측면에서 오늘 토론회는 유럽의 경험을 배우고 동시에 한국만의 방향을 모색하는 매우 중요한 공론의 장이라고 생각합니다.

저 또한 국회의 구성원으로서, 디지털 환경에서의 자유와 책임이 균형을 이루고, 국민의 기본권이 더욱 두텁게 보호될 수 있도록 함께 노력해 나가겠습니다.

오늘 논의가 한국 사회에 꼭 필요한 현실적이고 실천적인 정책 대안으로 이어지기를 기대합니다. 다시 한 번 귀한 자리 함께해 주신 모든 분들께 감사드리며, 토론회가 생산적인 논의의 장이 되기를 기대합니다.

감사합니다.

인사말 4



존경하는 국민 여러분, 그리고 「DSA의 균형 모델과 한국형 입법의 실천적 과제」 한-EU 전문가 포럼에 참석해 주신 내외 귀빈 여러분! 안녕하십니까. 국회 과학기술정보방송통신위원회 소속 국회의원 한민수입니다.

오늘 디지털 민주주의의 미래를 함께 설계하는 뜻 깊은 자리에 함께해 주셔서 감사드립니다. 본 포럼을 공동 주최해주신 더불어민주당 이주희, 김우영, 전진숙, 박지혜 의원님과 오픈넷, 21조넷 대표님과 발제를 맡아주신 전문가 여러분께 진심으로 감사드립니다.

우리는 지금 인공지능 기술이 인간의 사고와 소통, 그리고 민주주의 작동 방식을 근본적으로 바꾸어 놓는 역사적 전환점에 서 있습니다. 생성형 AI의 급속한 발전은 정보 생산의 문턱을 낮추었고, 그 결과 허위조작정보의 생산과 유통 속도 역시 전례 없는 수준으로 빨라졌습니다.

우리 국민의 81%가 가짜뉴스의 심각성에 공감하고, 국내 최대 동영상 플랫폼인 유튜브의 일일 평균 사용 시간이 140분에 달하는 오늘의 현실은, 인공지능으로 파생되는 문제를 더 이상 미룰 수 없다는 것을 반증합니다.

먹방 유튜버를 향한 헐박과 금품 갈취, 제주항공 참사를 둘러싼 CG 조작설, 이태원 참사 희생자에 대한 음모론, 그리고 민주주의의 근간을 흔드는 부정선거 음모론에 이르기까지, 허위조작 정보는 개인의 삶을 파괴하고 헌법 질서를 위협하는 지경에 다다랐습니다.

저를 비롯해 여러 의원님이 발의한 인공지능기본법이 24년말 통과돼 올해부터 시행중입니다. 이 법의 핵심은 AI 기술 혁신은 촉진하되, 그 혁신이 반드시 인권 존중과 민주적 가치의 틀 안에서 이루어져야 한다는 것입니다.

AI가 생산하고 유통하는 정보의 영향력이 갈수록 커지는 시대에 알고리즘의 투명성과 플랫폼의 책임성을 제도적으로 담보하는 일은 규제가 아니라 AI기술을 지속 가능하게 하는 조건입니다.

오늘 논의될 디지털서비스법(DSA) 역시 바로 이런 맥락에서 이해해야 한다고 생각합니다.

DSA는 과거 전자상거래 지침의 한계를 극복하며 등장한 새로운 플랫폼 규제 패러다임입니다. 정부가 개별 콘텐츠를 직접 심의·제재하는 방식 대신, 플랫폼이 자율적 운영 정책에 따라 불법 정보에 스스로 대응하도록 하고, 공적 기관은 그 시스템의 작동 여부를 투명성 보고서로 간접 감독하는 구조입니다.

서비스의 성격과 규모에 따라 의무를 차등 부과하고, 알고리즘과 데이터의 투명성을 의무화하며, 중개자의 책임을 명확히 규정하는 패러다임은 표현의 자유와 정보 건전성이라는 두 가치를 동시에 만족시키는 균형의 산물입니다.

한국도 이러한 DSA법의 취지를 적극 수용해야 합니다. 방송미디어통신심의위원회로 이어져 온 우리의 '국가 주도형' 행정심의 역사는 DSA의 정신을 내포하고 있습니다. 내용심의 중심의 현행 법제를 절차와 시스템 감독 중심의 체제로 전환하는 일은 단순한 조문의 이식이 아니라 규제 철학의 전환을 요구합니다.

오늘 포럼이 바로 그 전환의 출발점이 되리라 믿습니다. EU의 실제 경험을 통해 DSA가 유럽 시민들의 디지털 소통 환경에 어떤 변화를 가져왔는지, 그 성과와 한계는 무엇인지를 면밀히 살펴보고, 한국의 현실과 제도적 특수성을 명확하게 진단하는 심층 논의가 이루어지기를 기대합니다.

특히, 권위주의적 통제의 경직성을 배제하면서도 허위조작정보에 실효적으로 대응할 수 있는 '한국형 협력적 거버넌스' 모델의 윤곽이 오늘 이 자리에서 구체화되기를 바랍니다.

저 역시 국회 과학기술정보방송통신위원회의 일원으로서 오늘 논의가 입법적 성과로 이어지도록 최선을 다하겠습니다. AI 시대의 기술 혁신과 민주주의 가치가 상충하지 않고, 기술이 인권을 강화하고 인권이 다시 기술의 지속 가능성을 뒷받침하는 선순환적 제도 틀을 함께 만들어가도록 노력하겠습니다.

참석해주신 모든 분들의 건강과 행운을 기원하며, 오늘 포럼이 풍성한 성과를 거두기를 진심으로 기원합니다. 감사합니다.

2025년 4월 8일
국회의원 한민수

EU 집행위원회 초청

한국-EU 전문가 포럼

디지털
서비스법

DSA의 균형모델과 한국형 입법의 실천적 과제

세션1 DSA 심층 분석

DSA Overview

Joris van Hoboken
암스테르담 대학교 교수

EU Intermediary Liability and the DSA

Prof. dr. Joris van Hoboken

Professor of Information Law with Special Emphasis on Law and Digital Infrastructure

Institute for Information Law (IViR)

Faculty of Law, University of Amsterdam;

What is intermediary liability and Responsibility?

Liability and responsibility of service providers for their involvement in the illegal content and activity of their users (or other third parties)

Liability (narrow): liability for damages (private law) and criminal liability;

Liability (broad): narrow sense + potential target of injunctions and legal duties of service providers to assist in addressing harm / assisting with legal action against perpetrators;

Responsibility: legal and regulatory duties in view of the (potential) illegal/unlawful/harmful content and activities of users/third parties and their interests, including

- duties of care to prevent or minimize harm
- duties to organize services and application of particular technologies in ways that prevent or minimize harm;
- procedural obligations;
- risk assessments, etc;

Why go after platforms and intermediaries in the first place?

- They (can) act as a control point, including for the enforcement of existing law;
- To receive compensation for damages (deep pockets);
- To get a relevant injunction (content removed, users blocked, preventive action, etc..)
- Attribution (intermediaries may hold relevant data to identify perpetrators);
- To set enforceable legal standards and precedents in your favor;
- To get (more) control over relevant value chains (and drive particular intermediary service models out of the market);

Types of illegal/unlawful/harmful content & activity

Large variety of underlying legal norms (at MS and EU level) including:

- Copyright and neighbouring rights violations;
- Trademark violations;
- Counterfeiting;
- Consumer protection law violations;
- Privacy, insult, libel and defamation law violations;
- Data protection law violations;
- Group insult, hate speech and incitement to violence law violations;
- Child sexual abuse material (CSAM) and non-consensual nudity;
- Harassment and stalking;
- Holocaust denial (Germany, France);

Harmful content categories:

- Content that is restricted due to the protection of minors (violence, nudity);
- Legal forms of disinformation;
- ‘Lawful but awful speech’;

Intermediary liability frameworks: why do we have them?

- Legal certainty, while balancing competing three overarching goals:
 1. Preventing and addressing illegal content and harm;
 2. Stimulating innovation and eCommerce;
 3. Ensuring the free flow of information, freedom of expression, and user rights;
- EU internal market and avoiding legal fragmentation (Europe);
- Incentivizing private ordering: Safe harbors provide legal certainty to service providers in the shadow of which they are free and asked/incentivized to address illegal and harmful content through self- and co-regulation;

Intermediary liability frameworks: sources of law before DSA

- *United States*

- *1996: Communications Decency Act, Section 230: absolute immunity for illegal content, outside of intellectual property and criminal law (so including defamation, privacy violations);*
- *Digital Millennium Copyright Act 1998: conditional immunity in the area of copyright for mere conduit, caching, hosting and information location tools;*
- *Other specific regimes apply in niche areas;*

- *European Union*

- *Until 2000: some national level intermediary liability laws, for instance in Germany;*
- *Electronic Commerce Directive (2000/31/EC): modelled after US DMCA;*
- *EU Charter of Fundamental Rights, in particular private life and confidentiality of communications, protection of personal data, freedom of expression and the right to conduct a business and right to an effective remedy;*
- *CSAM; AVSMD; GDPR; Copyright in the DSM; TERREG;*
- *Self-and co-regulation in area of Notice and Action, hate speech, disinformation;*

Electronic Commerce Directive (2000/31/EC)

- ECD established country of origin principle for information society services;
 - Article 3(2) ECD: “Member States may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State.”
- Access and hosting activities of service providers get horizontal conditional safe harbors;
 - Applicable to legally defined information society services;
 - Article 12-14 ECD provide for a harmonized liability shield;
 - Article 12-14 ECD do not establish liability, they (can) only limit it;
 - Horizontal: applicable across types of illegal/unlawful concern, including criminal;
 - Conditional: no initiative (for mere conduit) & no knowledge/ awareness (for hosting);
- Injunctions
 - Article 12-14 ECD allow for possible injunctions, including prohibitory, and national level duties of care (recital 48);
 - Article 15 ECD prohibits general monitoring obligations;

Article 15 No general obligation to monitor

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

Notice and Takedown before the DSA

- Ecommerce Directive (ECD) contained an implicit expectation for services acting as hosting service providers to follow notice and takedown procedures as a result of the conditions of Article 14(1) ECD.
- ECD did not specify Notice and Takedown requirements and procedures
 - Services could make their own choices and follow their own procedures, within the boundaries of relevant national law(s);
 - Some countries, including Netherlands, promoted developed self-regulatory codes;
 - US-based service providers tend(ed) to follow DMCA for copyright violations;
- Characteristics NTD:
 - Reactive procedure to deal with illegal/unlawful activity;
 - Typically dealt with by the service on the basis of terms of service;
 - Review standards depended on the services' procedures and resources;
 - Raised privatized enforcement issues (e.g. chilling effects project);

Scope of the safe harbors

- The Article 12-15 ECD compromise between competing goals was originally aimed at Internet Service Providers in particular:
 - Internet access providers and internet hosting providers;
 - Broad enough wording to be applied to variety of online/internet-based service providers acting as mere conduit or hosting;
- Questions relating to scope are a significant source of legal uncertainty over time;
- Since 2000, the service landscape has widened and diversified and due to the increasing dominance of Online Service Providers and the success of the platform model, the variety of service providers that can invoke Article 12-14 has grown significantly;
- Major developments include:
 - The rise of cloud computing;
 - Mobile access and smartphones;
 - The social turn and web 2.0;
 - Industrial scale content moderation by the largest platforms;

Leading up to the DSA proposal

- Significant pressure on (ever more dominant and not very responsible) platforms to take more responsibility for harm and illegal content (hate speech, disinformation, terrorism content, etc)
 - **calling into question the balance struck by the ecommerce directive safe harbors;**
- Questions about content moderation practices, platforms impacts on society and economy, and due process in content moderation and protection of user rights
 - **calling for more transparency and better procedural guarantees;**
- EU Member States enact laws (such as NetzDG in Germany) to further responsabilize online platforms
 - **leading to legal fragmentation in the EU;**

Situation in the end of the 2010s, in summary

- Erosion of the ECD safe harbors and core principles through case law, new verticals, and MS developments;
- Significant legal fragmentation;
- Increasing pressure on big tech in view of adverse societal impact(s), questioning of the status quo;

Question the European Commission had at the time (2017): How come the platforms are continuing to say that they have 'no knowledge', even though they are analysing everything their users are doing online?

Intermediary liability: toward a new approach

Into the late 2010s we can observe a maximum responsabilization of platforms within the legal boundaries set by the Ecommerce Directive (only reactive responsibility, no general monitoring, no strict liability), for specific instances of illegal content.

New solution coming into focus: the possibility to focus on systemic requirements and issues, instead of the question of whether there is liability in particular cases of illegal content or hard, and the idea to impose requirements to identify and address more systemic issues and risks.

The EU Digital Services Act

The DSA entails a broad intermediary service and online platform regulation package at the EU level;

Deals with the question of intermediary liability and platform responsibility and imposes a new framework of due diligence obligations with respect to illegal content online;

Establishes a new framework for oversight and enforcement for intermediary services;

Shift from self-regulation -> public regulation for online platforms;

Primary focus: social media and online marketplaces, but all online services dealing with third party content are in scope.

Special regime for Very Large Online Platforms (and SEs) (45M+ active recipients) with risk management obligations, audits, and centralized oversight.

Signed into law in Oct 2022, entered into force in stages (VLOPs early '23, national level early '24).

What stayed the same:

Safe harbors left intact;

Ban on general monitoring obligations remains in place (with good Samaritan defense added);

Notice and takedown as the default practice for addressing illegal content;

A new tiered approach in the design of **due diligence** obligations

Most basic obligations: all intermediary services;

Additional due diligence requirements: hosting services;

Additional due diligence requirements: consumer-facing hosting services that make things public ('online platform' definition);

Additional due diligence requirements (asymmetric): largest online platforms and search engines, including risk-management, auditing and crisis protocol.

A legal definition of content moderation

DSA, Article 3 (t) (t) 'content moderation' means the activities, whether automated or not, undertaken by providers of intermediary services, that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetisation, disabling of access to, or removal thereof, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient's account;

Relevance:

- Scoping of regulation of Terms of Service for content moderation (art 14);
- Scope of transparency, due process, and transparency reporting obligations;
- Scope of risk management framework for dominant platforms;

Good Samaritan Defense (Article 7)

DSA, Article 3 (t) (t) 'content moderation' means the activities, whether automated or not, undertaken by providers of intermediary services, that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetisation, disabling of access to, or removal thereof, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient's account;

Relevance:

- Scoping of regulation of Terms of Service for content moderation (art 14);
- scope of transparency, due process, and transparency reporting obligations;
- scope of risk management framework for dominant platforms;

Regulation of Terms of Service (Regulation of Platform Governance)

Article 14 DSA; (what some scholars call ‘hybrid governance’)

Transparency and completeness requirement (14(1))

- Restrictions on use of service should be included in the service’s Terms of Service;
- The “policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review” should be included;

ToS enforcement requirements (14(4))

- Restrictions on the use of their service in respect of user content should be applied in a “diligent, objective and proportionate manner”
- Additional general requirement: “with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service, such as the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter;

From self-regulation to public regulation

Regulatory oversight (Digital Service Coordinators & European Commission);

Centralized enforcement for the obligations on dominant platforms by the European Commission (to save the country-of-origin principle);

Codification soft-law instruments of the last decade (e.g. Notice and Takedown) and legal anchoring of codes of conduct (like code of practice disinfo);

From illegal content process to a broader set of requirements on content moderation, advertising, recommender systems, etc;

Individual complaint procedures vis a vis the platform (e.g. removals) and Digital Service Coordinators (non-compliance);

NB: there are opportunities for private enforcement, too! (See our report)

Transparency and accountability

DSA requires a host of new data and reporting on content moderation and related platform governance (recommender systems, advertising) to become available;

- Transparency about content moderation in terms of service (art 14);
- Transparency reporting obligations (art 15);
- Statement of reasons for individual content moderation decisions (art 17);
- Risk-management obligations for the largest online platforms and search engines (art 34-35), and auditing requirement (article 37);
- Specific research data access requirements on dominant platforms for vetted researchers;

Risk-based approach for dominant platforms

Additional due diligence requirements (asymmetric): largest online platforms and search engines;

Risk is explicitly introduced in two ways in the DSA

1. To legitimize the introduction of asymmetric obligations for the most impactful online platforms (proxy -> average number of monthly users);
2. The requirement to manage systemic risks related to content moderation (art 34-35) and audit such risk management practices (art 37);

The DSA's risk-based approach

Requirement for online platforms and search engines with the most users to assess and address risks in four key areas:

- Illegal content;
- Fundamental rights impacts;
- Civic discourse, electoral processes, and public security;
- Gender-based violence, public health and minors, physical and mental well-being;

Risk mitigation is required to be “reasonable, proportionate and effective”, and has to take into account the impacts of possible measures on fundamental rights of users (those rights include freedom of expression, non-discrimination, personal data protection, privacy);

EU 집행위원회 초청

한국-EU 전문가 포럼

디지털
서비스법

DSA의 균형모델과 한국형 입법의 실천적 과제

세션1 DSA 심층 분석

DSA의 Architecture

Menno Cox

유럽연합 집행위원회(EC)
디지털 서비스 글로벌 센터장

EU 집행위원회 초청

한국-EU 전문가 포럼

디지털
서비스법

DSA의 균형모델과 한국형 입법의 실천적 과제

세션1 DSA 심층 분석

거버넌스 시스템

Julian Ringhof

유럽연합 집행위원회(EC) DSA 정책관

EU 집행위원회 초청

한국-EU 전문가 포럼

디지털
서비스법

DSA의 균형모델과 한국형 입법의 실천적 과제

세션2 한국형 디지털서비스업
입법의 실천적 과제

행정심의,
의무적 임시조치
그리고 표현의 자유

박 경 신

고려대학교 법학전문대학원 교수

한국의 온라인게시물관리 법제의 현황과 전망-DISA 및 DMCA와의 비교 중심으로

박경신

고려대학교 법학전문대학원 교수

사단법인 오픈넷 이사

현재 한국상황

1. **의무적** notice and takedown – 정보통신망법 44조의2:
“권리침해가 신고가 되면 서비스제공자는 임시/삭제조치를 취해야 한다.”
→ “권리침해가 있는지 어떻게 아는가?” → **비대칭적 동기** → 합법콘텐츠 삭제 <> 비교: 미국DMCA와 유럽DSA: **선택적** notice and takedown
2. 방송통신심의위원회의 시정요구 – 방(미)통위설치법 22조의4호:
“**건전한 통신윤리의 함양을 위하여 필요한 사항**으로서 대통령령으로 정하는 정보의 심의 및 시정요구”
→ “누구의 윤리적 잣대로 차단하는가” 예) womenonweb.org, northkoreatech.org, 윤석열 비판 영상 차단
3. **정보매개자책임제한**의 부재 → 불법게시물 차단 동기 약함, 합법게시물 차단 위험

의무적 노티스앤테이크다운의 문제점: 합법적 게시물의 항구적 차단 (2016년 오픈넷 " 벙커")

- 지배구조 이해하면 뉴스가 보인다... 중앙일보의 삼성, 국민일보의 조용기, 세계일보의 통일교 (블로거: 브이포벤데타)
- 삼성화재 다이렉트 자동차 보험 갱신 / 보험료 미친 상승 (블로거: 불끈)
- 삼성 X파일 '떡값 검사' 어떻게 살고 있을까? (블로거: 아이엠펙터)
- 고 심성민씨의 가족은 피해자다 (블로거: DEULPUL)
- 남양유업의 갑질은 계속된다.- 명예훼손을 이유로 블로그 게시중단 요청하다 (블로거: 브이포벤데타)
- 하늘에서와 같이 땅에서도 (블로거: DEULPUL)
- '청부칼럼' 쓰는 배인준 동아일보 논설주간님 (블로거: 미디어후비기 짜라시후비기)
- 그래도 대선 지지율 (블로거: DEULPUL)

행정기관 심의의 문제점

- 행정기구의 친여 편향성 → 류희림 방심위 사태, northkoreatech.org, 부당삭제사례들 transparency.kr
 - 2016년 8월 30일 방심위, 사드(THAAD)의 유해성 언급한 인터넷 게시물 12건 삭제
 - 2016년 7월 1일, 방심위, 인터넷 개인 방송 사이트 '쌈TV' 폐쇄 결정
 - 2015년 9월 16일 방심위, '세월호 국정원 개입설' 주장 글, '사회적 혼란 야기' 이유로 삭제 의결
- 절차적 보호장치 결여 → 게시자에게 실제로 연락하는 심의사건의 비율이 매우 낮음(10% 미만)
- 기소자와 심의자의 일치 → 99% 넘는 심의사건들은 삭제/차단결정으로 이어짐.
- 해외: 최고법원들(미국, 프랑스, 스페인, 필리핀, 터키) “행정기관이 표현의 자유에 직접 개입할 수 없다”
- 독일의 2017년 NetzDG입법 이후로 아시아와 유럽에 행정심의기관들 출현. 그러나 2023년 DSA 통과 후 ⁴⁸NetzDG개정됨.

정보매개자책임제한의 부재

- 면책조건의 불명확성
 - 사업자들에 의한 자발적인 신속대량삭제에 대한 동기 부재
 - 사업자들에 의한 자발적인 관리가 책임론을 강화하여 자발적인 관리를 꺼려하게 됨 → " 임의적 임시조치" 반대론
- 네이버 - 복원 요청시 30일 후 복원? (심의결과에 따름. 블로거 [계룡도령춘원](#))
- [카카오](#) - 복원 요청시 "심의결과에 따름"
 - 심의는 비대칭적인 동기로부터 자유로운가?
 - 불법게시물에 대한 신속대량삭제 동기도 없고 합법게시물에 대한 복원동기도 약해진 상황

표현의 자유 논란없이 불법정보를 되도록 많이 빨리 삭제차단시키는 방법 1

- 미국저작권법(DMCA): ‘불법정보를 신고(notice)시 삭제차단(takedown), 복원요청시 복원’의 절차를 거치면 모든 불법정보에 대한 책임에서 면책됨. → 신고물에 대한 대량 및 신속한 삭제 동기부여 → " 표현의 자유 침해"? 복원요청물에 대한 대량 및 신속복원 → " 불법물의 복원"? 실제로 복원요청의 비율은 5-10% 즉 불법신고의 90-95%는 표현의 자유 논란없이 삭제차단됨.

DSA는 DMCA의 성공을 불법정보 전반에 확산하려는 시도

- DSA: 2000년 전자상거래지침의 정보매개자책임제한 :
“정보사회서비스(플랫폼)는 자신이 몰랐던 불법물에 대해 면책된다” + DSA: “모든 게시물신고에 대해 삭제든 유지든 합리적 노력(Due Diligence)을 기울여야 한다. 결정은 조정(mediation: out of court settlement)에 부쳐질 수 있어야 한다.” → DMCA와 비슷한 결과?

DSA/DMCA 비교

DSA 시행 2 년간

- 30 억 삭제차단
 - 99% 자진삭제 (2025년 전반)
- 1억6천5백만 이의제기
(**전체삭제차단의 5.5%**)
- 30% 복원
- 1,840 조정 회부 (전체복원건의 0.003%) → 50% 재삭제차단
- 조정결과에 대한 거부 및 소송?
→ 0건

DMCA in 2025

- 35억 삭제차단
- 이의제기 (**전체의 1% 미만**)
- 이의제기의 상당수 복원 (50% 이상)

허위조작정보근절법 (2025)의 효과

- 불법정보 외에도 허위정보, 허위조작정보 등의 개념을 만들어 삭제 → 2021 UN표현의자유 특별보고관, 2010 헌법재판소 - 표현은 진위 여부만으로 규제될 수는 없고 공익침해는 규제사유로 너무 불분명 → 행정심의회 위험 확대
- 허위조작정보에 대한 행정심의회에 의한 삭제차단 → 행정심의회 위험 확대
- 허위조작정보 **게시**에 대한 5배수 배상 -> 언론의 역할 약화
- 피해입증이 어려운 불법정보, 허위정보, 허위조작정보 **유통**에 대해서 민사배상 및 손해배상추정 → 정보매개자책임제한 위반
- 허위조작정보 반복 게시에 대한 10억 손해

교훈

- DSA는 규제대상 정보의 범위를 확대하지 않았다
- DSA는 국가에 의한 행정심의 체제가 아니다.
- DSA는 ‘모르는 정보’에 대한 매개자책임제한을 재확인했고 특정정보를 삭제차단하지 않았다고 해서 책임을 부과하는 법이 아니다.
- DSA는 이용자와 피해자의 목소리에 응대함에 있어서 ‘합리적 노력(due diligence)’을 기울이지 않는 것에 대한 책임을 부과하는 법
- DSA는 DMCA처럼 동기부여체계만 잘 만들어두면 표현의 자유 침해없이 플랫폼들이 자발적으로 신속대량삭제를 할 것이라는 믿음에 기초한 법이다.

프랑스 및 독일의 행정심의 규모

- [France](#) – about 2,000 in 2025 (대부분 저작권침해)
- [Germany](#) – [about 30,000](#) in 2025 (대부분 강제성없는 요청)

France

- **Illegal Streaming Blocking (Mid-2025):** The French Council of State reported on cases regarding Arcom's blocking of websites for illegal streaming of sports, including specific decisions on illegal streaming in July 2025.
- **Pornographic Websites and Age Verification:** On **February 26, 2025**, Arcom designated 17 pornographic websites and content-sharing platforms to comply with age verification obligations.
- **Escalated Enforcement (August 2025):** In August 2025, Arcom escalated its approach by issuing formal notices to five EU-based porn sites to comply with age verification, following the February designations.
- **IPTV Services:** While 1,769 IPTV services were blocked in 2024, data for 2025 continues to show a high focus on fighting piracy, with legal challenges to Arcom's framework noted as unsuccessful in 2025.

Germany

- **Non-Compliant Equipment (Online):** In 2025, the BNetzA identified **1,266 non-compliant types of equipment** being offered for sale online (e.g., smartwatches, radios) and notified sales platforms to remove them from the market.
- **Customs Cooperation:** In 2025, the BNetzA and customs authorities found roughly 89% of 8,202 reported suspicious goods consignments to be non-compliant, preventing them from entering the market.
- Regarding broader "takedown requests" for illegal content online, reports indicate that the **Federal Criminal Police Office (BKA)**, rather than BNetzA, sent approximately **29,792** non-binding deletion requests ("referrals") to hosting services in 2025.

Resources

- <https://www.chosun.com/english/national-en/2025/10/21/O5DVRVGT3JHE3C7ALZKTW4RFZM/>
- <https://cm.asiae.co.kr/en/article/2025121014354258215>
- <https://hateaid.org/en/mixed-feelings-digital-services-act-replaces-netzdg>
- <https://www.hoganlovells.com/en/publications/digital-platform-regulation-germanys-implementation-draft-bill-of-the-digital-services-act>
- <https://www.opennet.or.kr/26574>(Korean only)
- [The Democratic Party’s Push for the ‘Korean-Style DSA’ Must Align with International Human Rights Standards | OPEN NET](#) (English translation)
- Bantam Books, Inc. v. Sullivan, 372 U.S. 58 (1963); Little Sisters Book & Art Emporium v. Canada (Minister of Justice), 2000 SCC 69 (2000) (Can.); Rappler, Inc., Petitioner v. Andres D. Bautista, Respondent, [2016] PHSC 85 (Hong Kong); Poland v. Parliament and Council, 62019CJ0401 (EU); Disini v. The Secretary of Justice, [2014] G.R. No. 203335 (Philippines); French Constitutional Court — Decision n 2009-580 DC of 10 June 2009 (only in French, June 10, 2009); French Constitutional Court — Decision n 2020-801 DC of 18 June 2020; Turkish Constitutional Court, nos. 2014/149 (October 2, 2014, annulling the law), followed by no. 2014/3986 (April 2, 2014, lifting Twitter.com ban), no. 2014/4705 (May 29, 2014, lifting YouTube.com ban); Women On Web v. AEMPS, no.1362/2022, Spain Supreme Court, October 3, 2022.

EU 집행위원회 초청

한국-EU 전문가 포럼

디지털
서비스법

DSA의 균형모델과 한국형 입법의 실천적 과제

세션2 한국형 디지털서비스업
입법의 실천적 과제

정통방법 체계와
DSA 구조적 정합성 진단
그리고 '협력적 거버넌스'

오 병 일

디지털정의네트워크 대표

Content Regulation in Korea

Moving from State Censorship toward Platform Accountability

Byoungil Oh / Digital Justice Network

Regulation Model

South Korea
Network Act

State Regulation

The state agency(KCSC) actively monitors content, judges appropriateness, and issues de facto deletion orders directly. The platform plays a purely passive role.

EU
Digital Service Act

Co-regulation

Platforms are designated as the 'primary regulators' responsible for their own internal rules. The state acts only as a secondary supervisor, ensuring the procedural architecture is fair, rather than judging individual posts.

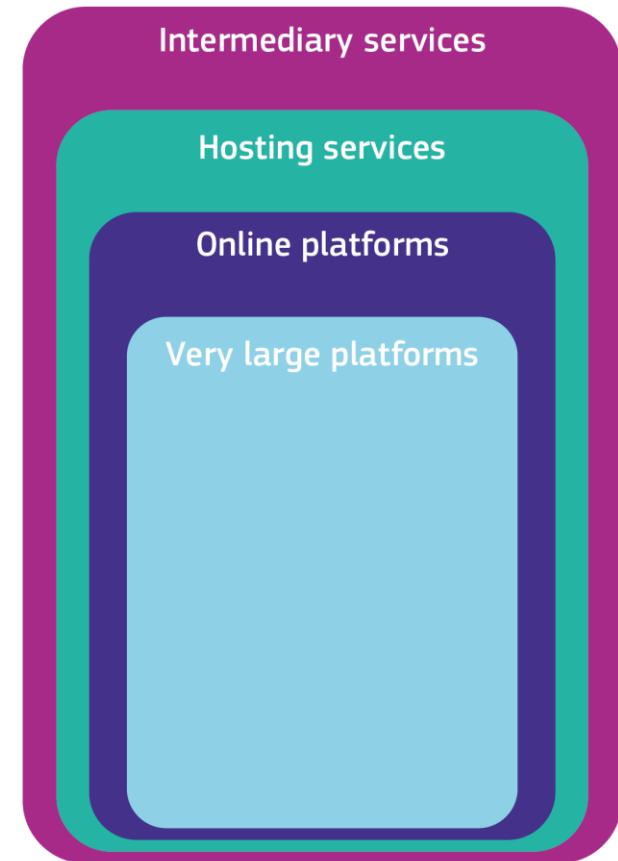
Scope and Structure

South Korea
Network Act

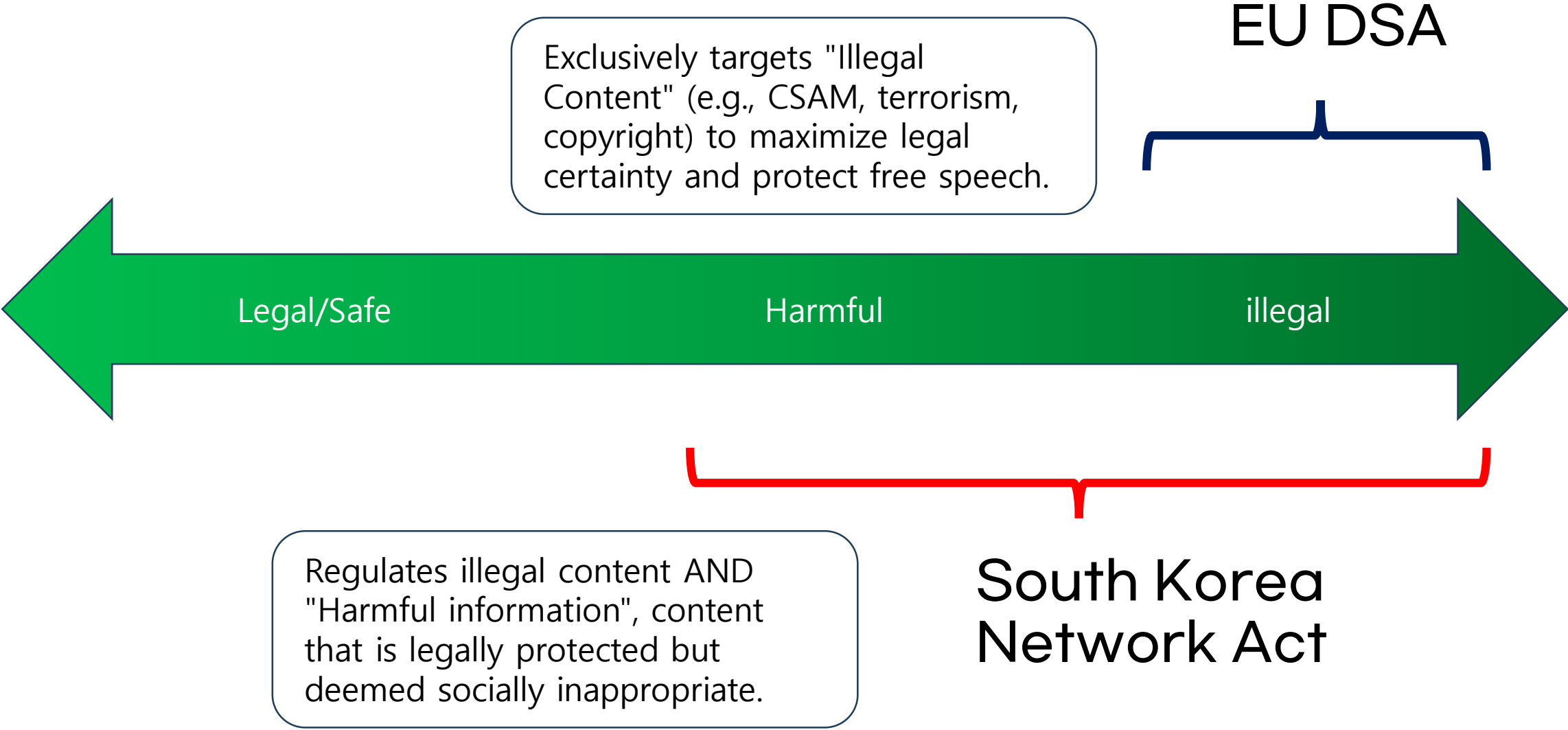
The Network Act applies the same heavy regulatory burden to all online intermediaries. Certain provisions apply to specific ISPs. (Certain provisions apply to specific ISPs.)

EU
Digital Service Act

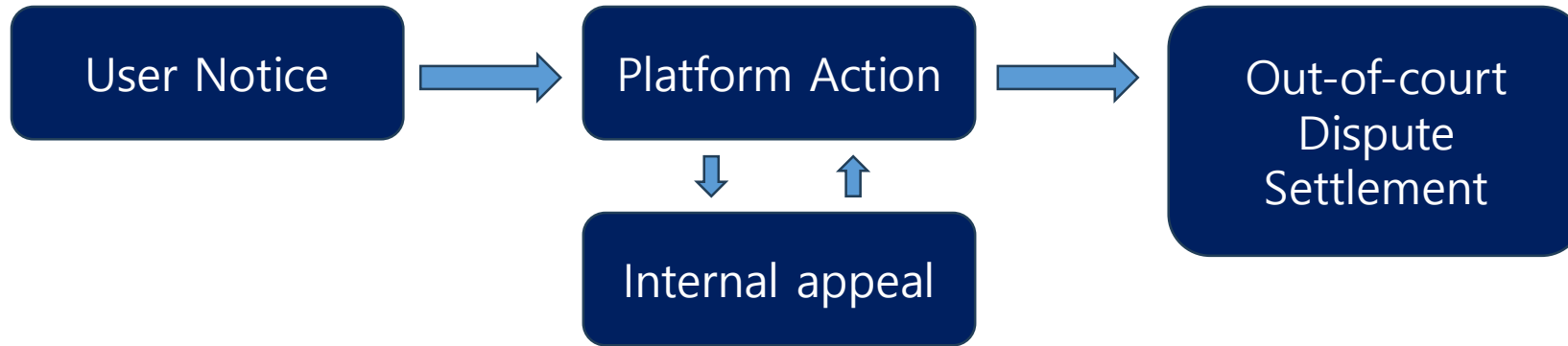
Cumulative, asymmetric obligations based on societal impact. While basic conduits require only transparency, VLOPs trigger rigorous systemic risk assessment and audits.



The Scope of Regulated Content



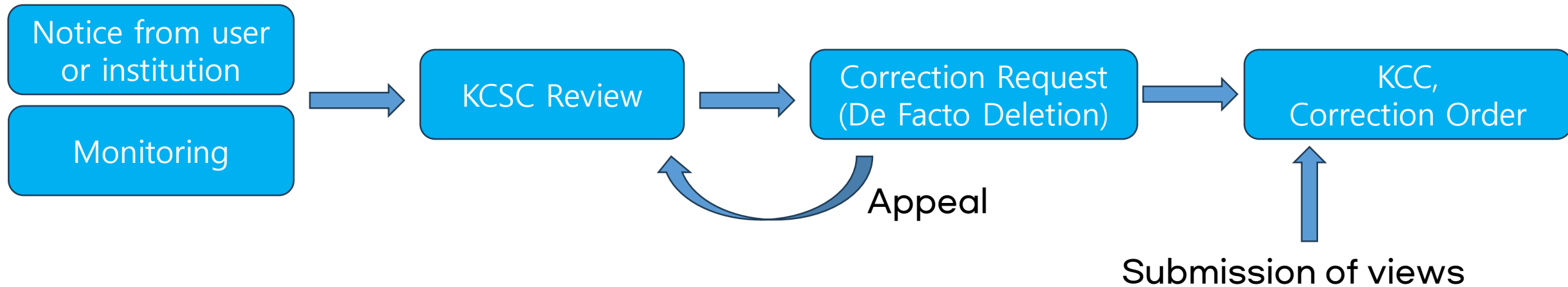
Procedures for Handling Illegal Content



EU DSA

Redress Mechanism : Built on mandatory "Notice & Action". Platforms must provide detailed reasons for deletion and maintain appeals system. If unresolved, the case shall be referred to Out-of-Court Dispute Resolution.

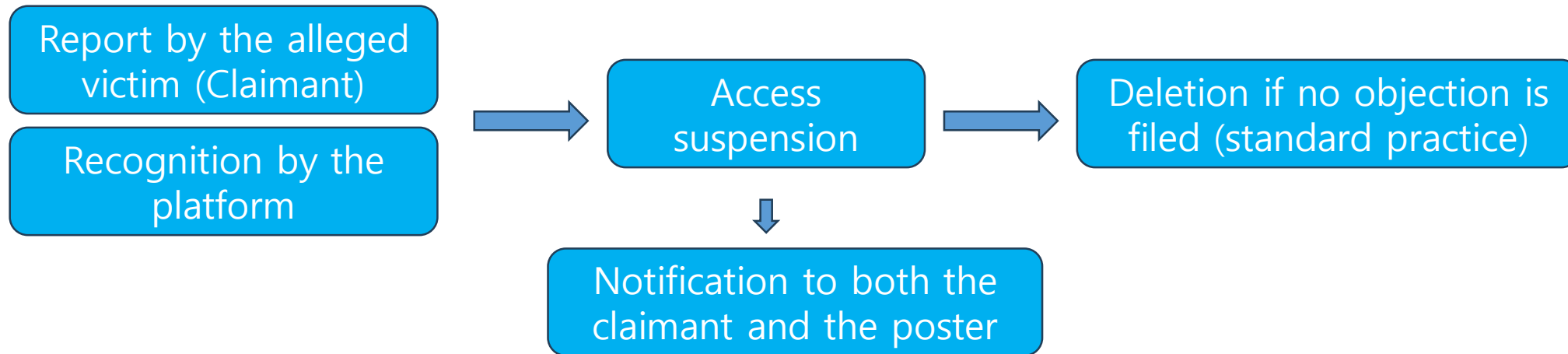
Procedures for Handling Illegal Content



South Korea Network Act

Internal Remedy: Technical "recommendation" of KCSC hold binding power. Content is deleted without prior notice, explanation, or a meaningful right of reply for the original poster. No independent remedy mechanism.

Procedures for Temporary Measure



South Korea Network Act

Temporary Measure for regarding content involving defamation or infringement of privacy : The 30-day blocking : platforms must initiate a 'temporary measure' blocking content for 30 days upon an infringement claim. The poster is practically stripped of their ability to challenge this during the critical window. No specific regulations regarding the procedures for handling disputes.

Procedures for Handling Harmful Content



South Korea Network Act

While the process is similar to how illegal content is handled, the KCC cannot issue corrective orders. However, the KCSC's recommendations are virtually mandatory in practice.

The KCSC utilizes highly abstract criteria for administrative review, such as 'concerns over causing significant social confusion'.

Responses to disinformation

South Korea Network Act

- Ban on the dissemination of disinformation (Revised Jan 6, 2026; Effective July 7, 2026)
- Is disinformation subject to KCSC deliberation?
- Weak fact-checking practices

EU Digital Service Act

The EU explicitly avoids treating disinformation as 'illegal content' subject to deletion. Instead, it is managed as a structural vulnerability of the platform's architectural design.

The Tools : Strengthened Code of Practice, 2022

Transparency

South Korea Network Act

Inconsistent Transparency Framework

Terms of Service transparency is limited to specific provisions; Transparency Report obligations were only recently reinforced through amendments.

EU Digital Service Act

Systemic Transparency

Terms of Service, Transparency Reports, Ad Transparency, Platform data access for researchers etc

Amendment to the Network Act

Revised: January 6, 2026 (Effective July 7, 2026)

- Inclusion of **hate speech** under the category of illegal information
- Prohibition of the distribution of **disinformation** (manipulated false information)
- **Aggravated liability** for damages for those who cause harm to others by distributing illegal information or disinformation, whether intentionally or through negligence
 - Prohibition of filing aggravated damage lawsuits for the purpose of hindering legitimate criticism or monitoring activities intended for the public interest
- **Reporting and action** systems for intermediaries regarding illegal contents and disinformation
- Requirement for large-scale service providers to prepare and publish **transparency reports**
- Support for **fact-checking** activities regarding false information and the establishment of Transparency Centers
- Expansion and reorganization of the Defamation Dispute Mediation Committee into a general Dispute Mediation Committee

→ Partial introduction of provisions similar to the EU Digital Services Act (DSA); however, civil society has expressed concerns regarding the potential infringement on freedom of expression.

Reform Measures for the Content Regulation System

from State Censorship toward Platform Accountability

- Abolition of the KCSC as a censorship body or minimizing the scope of its deliberation (e.g., limiting to SCAM-related content)
- Guaranteeing the right to appeal for both users and posters
- Vitalizing Out-of-Court Dispute Settlement (ADR) mechanisms
- Imposing asymmetric (tiered) obligations based on the role, level of intervention, and social impact of intermediaries (e.g., mere conduits, hosting services, online platforms, and VLOPs)
- Strictly limiting the scope of legal regulation to "illegal content" only
- Promoting and institutionalizing fact-checking practices
- Enhancing platform transparency and accountability: including transparency of recommender systems, advertising transparency, and systemic risk assessments for VLOPs

Thank you

for your attention and commitment to digital justice