

이슈보고서

EU 디지털서비스법의 시스템적 위험평가와 집행의 실효성

국내 정책적 시사점

2026년 9월

사단법인 정보인권연구소

오병일, 장여경, 희우

 **정보인권연구소**
Institute for Digital Rights

 **HEINRICH BÖLL STIFTUNG**
서울
동아시아 | 국제 대화

정보인권연구소 이슈보고서

EU 디지털서비스법의 시스템적 위험평가와 집행의 실효성 : 국내 정책적 시사점

발행일 2026년 9월

발행처 사단법인 정보인권연구소, idrsec@proton.me



저자 오병일 (정보인권연구소 연구위원)
장여경 (정보인권연구소 상임이사)
희우 (디지털정의네트워크 활동가)

후원 하인리히뵐 재단



사단법인 정보인권연구소는 시민사회 관점에서 정보인권을 지지하는
대안적 정책을 연구하고 생산하기 위해 활동하고 있습니다.

<https://idr.jinbo.net>



정보인권연구소 이슈보고서
EU 디지털서비스법의 시스템적 위험평가와 집행의 실효성
: 국내 정책적 시사점

목 차

1/ 들어가며	4
2/ 플랫폼의 시스템적 위험 관리 제도의 실효성과 한계	8
3/ 플랫폼 데이터에 대한 연구자 접근 제도의 현황	44
4/ 시스템적 위험에 대한 DSA의 집행 현황	53
5/ 한국에 대한 시사점	74

1/ 들어가며

지난 2025년 12월 24일, 허위조작정보의 유통 방지를 명분으로 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(정보통신망법) 개정안이 국회를 통과하였고, 2026년 7월 7일부터 시행되었다. 이 개정안은 허위조작정보 유통 방지 조치의 하나로서 대규모 정보통신서비스 제공자의 정보통신망에서 유통되는 불법정보와 허위조작정보를 누구든지 신고할 수 있도록 하였고, 정당한 이유가 있을 경우 신고를 접수한 대규모 정보통신서비스 제공자가 해당 정보를 삭제하거나 게시자 계정을 정지하는 등의 조치를 취하도록 한 조항(제44조의12)을 신설하였다.

대규모 정보통신서비스 제공자가 운영·관리하는 정보통신망만을 대상으로 하고, 불법정보뿐 아니라 허위조작정보까지 신고할 수 있도록 하는 등 세부적인 내용이 다소 다르기는 하지만, 이 조항은 유럽연합(EU) 디지털서비스법(Digital Services Act, DSA)에서 가져온 것이다. 이뿐만 아니라, 대규모 정보통신서비스 제공자의 투명성 보고서 작성 의무화, 신고에 따른 대규모 정보통신서비스 제공자의 조치에 대한 이의신청과 분쟁조정 등의 제도 역시 EU DSA를 참조한 것이다.

그럼에도 불구하고, 한국은 여전히 불법·유해정보를 심의하고 정보통신서비스 제공자에게 삭제 등의 조치를 권고할 수 있는 방송미디어통신심의위원회라는 국가행정기구를 운영하고 있다는 점에서, 불법·유해정보에 대한 규제 접근방식이 EU와는 다르다. 인터넷 초창기부터 끊임없이 제기되어 온 국가검열 논란과 이용자 소통이 글로벌 플랫폼으로 옮겨가는 경향을 고려할 때, 국내 내용규제 접근방식을 EU DSA와 같이 ‘규제된 자율규제’¹⁾로 전환할 필요성도 제기되고 있다.

국가적 내용규제 체제의 전환과 관련하여 또 다른 검토가 필요한 부분은, 현행 내용규제 체제가 특정한 불법·유해정보 통제에 초점을 두고 있다는 점이다. 그러나 어떤 불법·유해정보가 사회적인 영향력을 획득하는 것은 개별 콘텐츠를 넘어 수많은 이용자들이 상호 작용한 결과인 경우가 많다. 가령 혐오 표현으로 인한 피해는 불법임이 명백한 몇 개의 혐오 표현이 아니라 그 경계가 모호하거나 심지어 표현 자체로는 불법이라고 보기 힘든, 혐오 표현에 대한 동조와 지지에서 기인한다. 어떤 허위조작정보가 급속하고 광범하게 유통되는 것은 수많은 사람들이 해당 정보를 추천하거나 공유하기 때문이다. 플랫폼의 콘텐츠 추천 알고리즘은 어떤 콘텐츠에 대한 이용자의 반응을 평가하고, 이용자들의 관심사와 성향을 고려하여, 어떤 이용자에게 어떤 콘텐츠를 보여줄지 조정한다. 이 과정에서 어떤 콘텐츠는 더 잘 유통되고, 어떤 콘텐츠는 잘 전파되지 않는다. 좋은 콘텐츠가 더 잘 유통되고 불법·유해 콘텐츠의 유통이 제한되면 좋겠지만, 현실은 그렇지 않다. 만일 허위조작정보나 혐오표현이 정보통신망에 올라오더라도 그 유통 범위가 매우 제한적이었다면 지금과 같이 큰 사회적 문제로 인식되지 않았을 것이다.

그러나 불법·유해정보에 대한 심의와 차단에만 초점을 맞추는 규제 체제는 콘텐츠 유통에 대한 플랫폼의 책임을 누락하고 있다. 지금까지는 플랫폼을 비롯한 정보통신서비스 제공자에 대하여 이용자 표현물을 단순히 매개하는 전달자로 인식하여 온 측면이 있다. 물론 통신망 사업자나 이용자 콘텐츠를 단순히 저장하는 호스팅 서비스 제공자는 여전히 단순 정보매개자일 수 있다. 그러나 추천 알고리즘을 운용하며 플랫폼에 올라온 수많은 콘텐츠 중에서 어떠한 콘텐츠를 우선적으로 보여줄지

1) ‘규제된 자율규제’에 대해 다양한 정의가 있지만, 대체로 국가의 법적 틀과 개입 속에서 민간(기업이나 업계 단체)이 스스로 규칙을 만들고 집행하는 혼합형 규제 방식을 의미하는데, EU DSA가 ‘규제된 자율규제’ 방식을 취하고 있다고 해석된다(이권일, 2024).

결정할 권한이 있는 플랫폼의 경우 이제는 단순한 정보매개자로 볼 수 있을지 의문이다.

EU는 플랫폼을 중심으로 한 소통 환경 변화에 주목하고, 이에 대응하는 규제 방법을 개발해왔다. EU DSA는 플랫폼으로 하여금 개별적인 불법정보에 대해 신고를 받고 적절한 조치를 취하도록 요구할 뿐 아니라, 플랫폼의 기술적, 제도적 시스템이 불법정보의 유통, 인권과 민주주의에 미치는 부정적인 영향에 대해 평가하고 사전적인 조치를 취하도록 요구하였다. DSA는 제34조(위험평가), 제35조(위험완화), 제37조(독립적 감사) 등에서 이러한 내용을 규정하고 있다. EU DSA는 2022년 7월 5일 유럽의회를 최종 통과하여 2022년 11월 25일 발효되었고, 2023년 4월에 시스템적 위험평가 의무 대상인 초대형온라인플랫폼(Very Large Online Platform, VLOP) 및 초대형온라인검색엔진(Very Large Online Search Engine, VLOSE) 사업자가 지정되었으며, 2024년 말부터 첫 위험평가 보고서가 공개되기 시작했다.

이는 EU 차원의 규제이기는 하지만, 주요 글로벌 빅테크 업체의 위험평가 보고서와 감사 보고서가 공개되었기 때문에 세계 여러 나라 규제기관과 연구자들이 참고할 수 있다. 한국에서도 국가검열로부터 표현의 자유를 보호하면서도 플랫폼 사업자의 책임성을 강화하는 방향으로 내용규제 체제를 개편하는 논의를 효과적으로 전개하기 위해서는, 앞서 시행한 유럽의 선례를 참고할 필요가 있다.²⁾

한편, 최근 전 세계적으로 소셜미디어의 폐해로부터 아동을 어떻게 보호할 것인지에 대한 논의와 제도화가 진행되고 있다. 호주는 2025년 12월, 세계 최초로 청소년의 소셜미디어 가입을 전면 금지하였으며,

2) 이 외에도 긴급 대응 메커니즘, 투명성 보고서, 광고 투명성 등 플랫폼의 책임성을 강화하기 위한 여러 조치들이 있지만, 이 보고서에서는 다루지 않는다.

2026년 3월 미국 로스앤젤레스 법원은 소셜미디어의 ‘중독성 설계’가 청소년 정신 건강에 해를 끼쳤다는 원고의 주장을 인정하며 메타와 유튜브에 배상 판결을 내렸다.³⁾ 우리 방송미디어통신위원회도 2026년 7월 16일 대통령 업무보고에서, “14세 미만은 서비스 가입을 제한하고 14세 이상 19세 이하 청소년에게는 과몰입을 유도하는 중독성 설계와 추천 알고리즘 노출을 제한하는 방안을 단계적으로 검토하고 있다”고 보고하였다.⁴⁾ EU DSA에서는 소셜미디어 플랫폼의 중독성 설계 역시 시스템적 위험평가의 대상이 될 수 있다. 따라서 아동·청소년의 소셜미디어 이용 정책이 건설적으로 논의되기 위해서 EU DSA의 사례를 검토할 필요가 있다.

이에 본 보고서에서는 플랫폼 사업자의 책임성 강화를 위해 도입된 제도들, 즉, EU DSA의 시스템적 위험평가와 위험 완화 제도 및 독립적 감사 제도의 현황, 효과성과 그 한계에 대하여 검토해 보고자 한다. 또한 EU DSA는 시스템적 위험평가가 사업자 스스로에 의해 수행되는 한계를 극복하기 위하여 독립적인 연구자가 플랫폼 데이터에 접근할 수 있도록 허용(DSA 제40조)하고 있는 바, 이러한 데이터 접근 제도가 실효성을 갖고 운영되고 있는지도 함께 살펴보고자 한다. 더불어, DSA가 실효성을 갖기 위해서는 효과적인 집행이 중요하다는 점에서, 2022년 11월 발효 이후 글로벌 플랫폼의 DSA 의무 이행과 관련한 쟁점이 무엇이고, DSA 집행이 제대로 되고 있는지에 대한 현황도 정리해 본다.

3) 포춘코리아. (2026, 3, 26).

4) 연합뉴스. (2026, 7, 16).

2/ 플랫폼의 시스템적 위험 관리 제도의 실효성과 한계

가. 시스템적 위험 관리 메커니즘 개요

EU DSA는 초대형 온라인 플랫폼(VLOP)과 초대형 온라인 검색엔진(VLOSE)에 대하여, 디지털 생태계 전반의 안전과 기본권 보호를 위해 ‘시스템적 위험 관리’라는 특별한 의무를 부과하고 있다. 시스템적 위험 관리 규제는 자체적인 시스템적 위험평가(제34조) → 위험완화(제35조) → 독립적인 감사(제37조) → 이행 보고(제42조) 등 일련의 절차를 통해서 보완적으로 이루어진다. 전통적인 규제와 달리 플랫폼의 시스템적 위험에 대한 대응은 사전에 명확한 기준을 제시하기 힘들다. 플랫폼 알고리즘 자체가 플랫폼에 따라 다양하고 복잡하며, 기술의 발전에 따라 위험의 양상이 지속적으로 변화하기 때문이다. 그래서 EU DSA는 자체 평가를 통해 유연성을 보장하되, 독립적인 감사를 통해 객관성을 강화하고, 보고서의 공개나 제3자 연구자의 데이터 접근을 통해 외부에서도 검증할 수 있는 구조를 취하고 있다. 물론 이러한 설계가 효과적으로 작동하기 위해서는 지속적인 모니터링과 개선 과정이 필요할 것이다.

1) 적용대상

시스템적 위험 관리 규제가 모든 온라인 플랫폼에 적용되는 것은 아니다. 유럽연합 집행위원회(EC)가 지정한 VLOP과 VLOSE에만 적용된다. VLOP와 VLOSE의 정량적 기준은 EU 내 평균 월간 활성 이용자가

4,500만 명 이상인데, 이는 대략 EU 인구의 10%에 해당하는 수치이다(DSA 제33조). 이정도 기준을 초과하면 EU 인구에 상당한 영향력이 존재한다고 보는 것이다.⁵⁾

2023년 4월 25일에 AliExpress, Amazon Store, Apple AppStore, Bing, Booking.com, Facebook, Instagram, Google Maps / Play / Search / Shopping, YouTube, LinkedIn, Pinterest, Snapchat, TikTok, Wikipedia, X, Zalando 등 19개 플랫폼이 1차로 VLOP 및 VLOSE로 지정되었다. 이후 Pornhub, Stripchat, XVideos(이상 2023. 12.), Shein(2024. 4.), Temu(2024. 5.), XNXX(2024. 7.), WhatsApp(2026. 1.)이 추가로 지정되어 26개 사업자가 지정된 바 있으며, 이후 Stripchat이 지정 해제되었다. 이후 EC는 2026년 8월 31일, 챗GPT를 VLOSE로, 온라인 커뮤니티 레딧(Reddit)과 게임 플랫폼 로블록스(Roblox)를 VLOP로 추가 지정하였다. 이에 2026년 9월 현재 VLOP 및 VLOSE로 지정된 플랫폼은 28개이다.⁶⁾

VLOP와 VLOSE의 의무는 EC가 해당 사업자에게 지정 사실을 통지한 후 4개월이 경과한 시점부터 적용된다(DSA 제33조 제6항). 앞으로 살펴볼 시스템적 위험평가 의무도 지정 통지 후 4개월 후부터 적용된다.

2) 시스템적 위험평가(제34조)

DSA 제34조는 VLOP와 VLOSE 사업자로 하여금 자신의 서비스 및 이와 관련된 시스템에 대하여 ‘시스템적 위험(systemic risks)’을 평가하도록 하였다. 여기서 시스템은 알고리즘 시스템을 포함하며, 시스템적

5) DSA, recital 76.

6) 지정된 사업자 목록은 아래 사이트에서 확인할 수 있다.
<<https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>>.

위험은 서비스와 이와 관련된 시스템의 “설계 또는 운영으로부터 발생하는 위험”과 “서비스의 이용으로부터 발생하는 위험”을 모두 포함한다. 기존의 개별 콘텐츠의 규제에서 시스템 설계 규제로 패러다임이 전환되었음을 알 수 있다. 또한 이러한 평가를 성실하게(diligently) 수행하도록 함으로써, 형식적 이행이 아닌 실질적 평가 의무를 부과하고 있다.

이 평가는 적어도 매년 1회, 그리고 식별된 위험에 중대한 영향을 미칠 가능성이 있는 기능을 배치하기 전에 수행되어야 한다. 2026년 1월에 EC는 플랫폼 X에 대해 새로운 공식 조사(IP/26/203)를 개시하였는데, 그 이유는 X가 생성형 AI인 그록(Grok) 기능을 X 시스템에 통합하기 전에 사전적인 위험평가를 제대로 수행했는지 조사하기 위한 것이었다.⁷⁾

시스템적 위험평가는 다음의 네 가지 범주의 위험을 포함해야 한다.

- 불법 콘텐츠의 확산
- 기본권에 미치는 현실적이거나 예상 가능한 부정적 영향. 기본권은 인간의 존엄성, 사생활 및 가족생활의 존중, 개인정보에 대한 권리, 언론의 자유와 다양성을 포함한 표현 및 정보의 자유, 차별 금지, 아동의 권리, 소비자 권리 등을 포함한다.
- 시민 담론, 선거 절차, 그리고 공공 안전에 미치는 현실적이거나 예상 가능한 부정적 영향
- 젠더 기반 폭력, 공공보건 및 미성년자 보호와 관련하여 현실적이거나 예상 가능한 부정적 영향, 그리고 개인의 신체적·정신적 안녕에 미치는 중대한 부정적 결과

7) European Commission. (2026, 1, 26).

그러나 이는 최소 요건일 뿐이며, 서비스의 특성에 맞춰 다른 시스템적 위험도 평가해야 한다.

제34조 제2항은 시스템적 위험평가를 수행할 때 고려해야 할 ‘영향 요인(influence factors)’에 대해서 규정하고 있다. 즉 다음 요인들이 앞서 명시된 시스템적 위험 중 어느 것에 어떤 방식으로 영향을 미치는지 고려해야 한다.

- 추천시스템 및 기타 관련 알고리즘 시스템의 설계
- 콘텐츠 중재 시스템
- 적용 가능한 이용약관 및 그 집행
- 광고의 선정 및 표시를 위한 시스템
- 공급자의 데이터 관련 관행

이와 함께 서비스의 의도적인 조작(가짜 계정이나 자동화된 이용 포함), 불법정보나 약관 위반 정보의 증폭이나 빠른 확산, 지역적·언어적 특성 등 추가적으로 고려해야 할 요소도 제시되어 있다.

위험평가 관련 문서는 최소 3년간 보관해야 한다. 집행 당국이 요청할 때 이 문서를 제공해야 한다(제34조 제3항). 이 규정은 집행 당국의 사후 조사 및 감독의 가능성을 확보하기 위한 것이다.

3) 위험 완화조치(제35조)

제35조는 사업자가 제34조에 따라 식별된 위험을 완화할 수 있는 조치를 마련할 것을 규정하고 있다. 위험 완화조치는 구체적인 시스템적 위험에 맞춤형되어야 하고, 이러한 조치가 기본권에 미치는 영향을 특별히 고려해야 하며, ‘합리적, 비례적, 효과적’이어야 한다. 합리적이라는 것은 불가능하거나 터무니없는 개입까지는 아니더라도 최소한의 노력

이상을 기울여야 한다는 것이고, 비례적이어야 함은 위험의 심각도에 비례해야 하며 과도한 조치를 취해서는 안 된다는 의미이다. 효과적이어야 한다는 것은, 보여주기식으로 그쳐서는 안 되며 실제로 확인된 위험을 줄여야 한다는 의미로 해석된다.⁸⁾ 불법으로 의심되는 콘텐츠를 과도하게 필터링하는 것과 같이, 위험을 완화한다는 명분으로 도입된 조치가 오히려 표현의 자유를 침해할 수 있기 때문에, 완화조치가 기본권에 미치는 영향에 대해서도 특별히 고려할 것을 요구하고 있다.

제35조 제1항은 도입 가능한 위험 완화조치의 예시를 제공하고 있는데 다음과 같다.

- 온라인 인터페이스를 포함하여 서비스의 설계, 기능 또는 운영의 조정
- 이용약관 및 그 집행의 조정
- 콘텐츠 중재 프로세스의 조정(특정 유형의 불법 콘텐츠와 관련된 통지 처리의 속도 및 품질, 그리고 적절한 경우 불법 혐오 표현이나 사이버 폭력과 관련하여 특히 통지된 콘텐츠의 신속한 삭제 또는 접근 차단, 콘텐츠 중재 관련 의사결정 프로세스 및 전담 자원의 조정을 포함함)
- 추천시스템을 포함한 알고리즘 시스템의 테스트 및 조정
- 광고 시스템의 조정 및 자사 제공 서비스와 연계된 광고의 노출을 제한 또는 조정하기 위한 타겟팅 조치의 채택
- 내부 프로세스, 자원, 테스트, 문서화, 특히 시스템적 위험 감지와 관련된 모든 활동의 감독 강화
- 신뢰할 수 있는 신고자(trusted flaggers)와의 협력 개시 또는

8) 이 해석은 비공식 교육 사이트인 dsa-library.com의 해석을 참고한 것이다. 그러나 이 규정의 표현이 추상적인 관계로 그 구체적인 의미에 대해 학술적으로 여러 해석이 제기되고 있다.

조정, 그리고 재판 외 분쟁 해결 기구의 결정 이행

- 행동 규범(codes of conduct) 및 위기 대응 방안(crisis protocols)을 통한, 다른 온라인 플랫폼 또는 온라인 검색엔진 공급자와의 협력 개시 또는 조정
- 인식 제고 조치의 채택 및 온라인 인터페이스의 조정
- 아동 권리를 보호하기 위한 타겟팅 조치(연령 확인 및 자녀 보호 도구, 미성년자가 학대를 신고하거나 지원을 받을 수 있도록 돕는 도구 등 적절한 조치를 포함함)
- 딥페이크(생성되거나 조작된 이미지, 오디오 또는 비디오가 기존의 인물, 사물, 장소, 그 밖의 실체나 사건과 현저히 유사하여 이용자에게 진위가 확인되었거나 사실인 것처럼 잘못 인식되는 정보)에 대한 눈에 띄는 표시와 이용자에게 대한 표시(신고) 도구의 제공

이 모든 조치들을 모두 의무적으로 포함해야 하는 것은 아니며, 플랫폼은 각자 특정한 위험에 따라 적합한 조치를 선택할 수 있으며, 여기에 열거되지 않은 다른 조치들도 포함할 수 있다.

제35조 제2항은 유럽디지털서비스이사회(European Board for Digital Services, EBDS)로 하여금 EC와 협력하여 매년 종합보고서를 발표하도록 하였다. 이는 VLOP, VLOSE 사업자뿐만 아니라 시민사회나 학계 등 다른 정보원을 통해 수집된 정보를 바탕으로 하며, 가장 두드러지고 반복되는 시스템적 위험을 식별, 평가하고 이를 완화하기 위한 모범 사례를 포함해야 한다. 필요할 경우 위험이 발생한 회원국별 및 EU 전체 차원으로 시스템적 위험을 제시해야 한다. EBDS는 2025년 11월 18일, 제16차 회의에서 “온라인상 주요 반복적 위험의 지형에 대한 첫 번째 보고서”를 채택하였다.⁹⁾

위험평가 및 완화조치가 플랫폼의 자율적인 활동에 그친다면 그 결과물

이 자기합리화에 그칠 가능성이 클 것이다. 이를 보완하기 위해 DSA 제35조 제3항은 EC가 각국 디지털서비스조정관(Digital Service Coordinator, DSC)들과 협력하여 특정 위험에 관한 완화조치 적용에 대하여 지침(가이드라인)을 발행할 수 있도록 하고 있다. 이 지침은 모범 사례를 제시하고 권장 조치를 안내하는 역할을 한다. EC는 2024년 3월, 선거 과정의 시스템적 위험 완화에 대한 가이드라인을 발표하였으며¹⁰⁾, 2025년 7월에는 미성년자 보호 가이드라인을 발표하였다.¹¹⁾ 이 가이드라인은 2026년 4월 29일에 메타의 인스타그램과 페이스북에 대한 예비 결정의 핵심 근거가 되었다.¹²⁾

4) 독립적 감사(제37조)

시스템적 위험의 평가 및 완화조치는 자율적으로 수행되는 것이므로 이해상충을 배제하기 힘들다. DSA 제37조 독립적 감사는 외부 검증을 통해 이를 보완하기 위한 장치이다. 제37조는 VLOP와 VLOSE 사업자로 하여금 ‘자체 비용’으로 연 1회 이상 독립적인 감사를 받도록 하고 있다. 감사 대상은 DSA 제3장에서 규정하고 있는 의무와 제45조 및 제46조에 언급된 행동 규범(codes of conduct) 및 제48조에 언급된 위기 대응 절차(crisis protocols)에 따라 수행된 모든 약속이 포함된다.

사업자는 감사가 효과적으로 이루어질 수 있도록 협력과 지원을 제공해야 하고, 감사를 방해해서는 안 된다. 협력 및 지원에는 데이터와 구내에 대한 접근과 구두·서면 질의에 대한 답변이 포함된다(제37조 제2항).

9) European Commission. (2025, 11, 20).

10) European Commission. (2024, 3, 26).

11) European Commission. (2025, 7, 14).

12) European Commission. (2026, 4, 29).

제37조 제3항은 감사인의 요건을 규정하고 있는데, 감사 대상으로부터 독립적이어야 하고, 위험 관리 분야에서 입증된 전문성, 기술적 역량 및 능력을 갖추어야 하며, 객관성과 직업 윤리를 갖추어야 한다. 제4항은 감사 보고서의 필수 내용을 규정하고 있는데, 감사 주요 결과 요약, 감사 결론의 도출 근거 목록과 함께, 감사 의견을 포함한다. 감사 의견은 ‘적정(positive)’, ‘의견제시가 있는 적정(positive with comments)’ 또는 ‘부적정(negative)’ 중 하나이며, 감사 의견이 ‘적정’이 아닌 경우, 준수를 달성하기 위한 구체적인 조치에 관한 운영상 권고사항 및 이행 시한을 포함해야 한다.

만일 특정 요소를 감사할 수 없었거나 의견을 표명할 수 없는 경우에는 그 상황과 이유를 설명해야 한다(제5항). ‘적정’이 아닌 감사 보고서를 받은 사업자는 운영 권고를 고려하여 필요한 조치를 취하고, 권고 수령 후 1개월 이내에 그 조치를 담은 감사이행보고서를 채택해야 한다. 사업자들이 권고를 반드시 따라야 하는 것은 아니다. 그러나 이행하지 않는 경우 그 이유와 대안적 조치를 명시해야 한다. 제7항은 EC가 감사 수행을 위한 필요한 규칙을 정하여 위임 입법(delegated acts)을 채택할 수 있도록 규정하고 있는데, 2024년 2월 22일 감사에 대한 위임 입법이 발효되었다.¹³⁾

5) 문서의 공개(제42조)

DSA 제42조 제4항은 사업자로 하여금 제34조에 따른 위험평가 결과 보고서, 제35조 제1항에 따른 구체적인 위험 완화조치, 제37조 제4항에서 규정하는 감사 보고서, 제37조 제6항에서 규정하는 감사 이행 보고서를 모두 대중에게 공개하도록 함으로써, 시민사회, 연구자, 언론인

13) European Commission. (2024, 2, 23).

등 외부 이해관계자의 감독 가능성을 확보한다.¹⁴⁾ VLOP 및 VLOSE 사업자는 보고서가 완료되는 즉시 설립국의 DSC와 EC에 송부하고, 감사 보고서를 수령한 후 3개월 이내에 이 보고서들을 공개해야 한다. 해당하는 경우, 위험평가 및 완화조치 설계를 지원하기 위해 사업자가 수행한 협의에 관한 정보도 공개해야 한다.

이들 문서의 공개 시에 VLOP/VLOSE 사업자는 다음과 같은 이유로 공개된 보고서에서 정보의 일부를 비공개할 수 있다. 즉, 이 공개가 해당 사업자나 서비스 이용자의 기밀정보를 공개하게 하거나, 서비스의 보안에 심각한 취약성을 초래하거나, 공공의 안전을 해치거나 이용자에게 해를 끼칠 수 있다고 판단하는 경우이다. 유럽사법재판소의 판례(예: T-198/03 사건, Bank Austria Creditanstalt)에 따르면, 정보가 기밀로 인정되기 위해서는 해당 정보가 소수의 사람들에게만 알려져 있고, 그 공개가 정보를 제공한 사람이나 제3자에게 중대한 피해를 초래할 가능성이 있으며, 정보 공개로 인해 침해될 수 있는 이익이 객관적으로 보호할 가치가 있어야 한다. 이때 해당 이익의 보호 필요성은 비공개를 통해 보호되는 이익과 정보 공개에 대한 공익을 비교·형량하여 판단하여야 한다. 또한 공개 의무 예외는 엄격하게 해석되어야 한다. 정보 삭제에 대한 정당성이 각 사례별로 명확하고 충분히 설명되어야 하며, 위험평가 보고서 전체에 대해서는 기밀 유지를 주장할 수 없다. 사업자는 비공개에 근거를 DSC와 EC에 제출하는 사유서에 명시해야 한다.¹⁵⁾

14) 제42조 제1항~3항은 VLOP 및 VLOSE의 추가적인 투명성 보고서 작성 의무에 대해 규정하고 있다.

15) European Commission. “Q&A on risk assessment reports, audit reports and audit implementation reports under DSA”.

6) DSA의 전반적인 작동 구조

앞서의 준수 사항을 시기별로 정리하면 다음과 같다. VLOP/VLOSE 사업자는 지정 통보 후 4개월이 경과한 시점부터 의무가 적용된다. 지정 후 4개월 이내에 첫 위험평가를 완료하고, 이를 근거로 완화조치를 도입해야 한다. 이후 1년에 1회 이상 또는 위험에 중대한 영향을 미칠 가능성이 있는 기능을 배치하기 전에 위험평가를 수행해야 한다. 첫 감사는 의무가 적용된 이후 1년에 1회 이상 시행해야 한다. 감사 완료 후 1개월 이내에 감사 이행 보고서를 채택해야 하며, 감사 수령 후 3개월 이내에 위험평가 및 감사와 관련된 모든 문서를 공개해야 한다. EBDS는 1년에 1회 위험평가 및 완화에 대한 종합보고서를 발표해야 한다.

이러한 절차에 따라, 2023년 4월 25일에 처음으로 지정된 사업자의 경우, 2023년 8월 25일까지 위험평가 및 완화조치를 수행해야 했고, 1차 감사가 2024년 8월 말~9월 초에 완료된 이후 2024년 11월 말경부터 위험평가와 관련된 문서들이 공개되었다. 2025년 11월 말~ 12월 초경에 2차로 공개가 되었다.¹⁶⁾ EBDS의 첫 보고서는 2025년 11월 18일에 공개되었는데, 이 보고서는 2024년 2월 17일부터 2025년 2월 16일까지의 보고 기간을 다루고 있다.

16) 각 VLOP 및 VLOSE의 위험평가 보고서, 감사보고서, 감사이행 보고서는 다음 사이트에서 접근할 수 있다.

DSA database의 경우, <<https://tremau.com/resources/dsa-database/>> 참조.

DSA: Risk Assessment & Audit Database의 경우, <<https://docs.google.com/spreadsheets/d/12hJWpCFmHJMQQlzl1qkd6OGsMW82YcsWgJHxD7BHVps/edit?gid=0#gid=0>> 참조.

나. 시스템적 위험평가의 실효성과 한계

2023년 4월 25일에 지정된 사업자의 경우 첫 위험평가는 2023년 8~9월에 완료되었어야 했다. 그러나 위험평가 보고서가 일반 대중에게 처음으로 공개된 것은 2024년 11월 22일 경이다.¹⁷⁾ 이는 제42조 제4항의 공개 의무가 감사 사이클과 연계되어 있어, 감사가 완료된 후 3개월 이내에 공개하는 구조이기 때문이다. 첫 감사는 지정 후 1년 시점인 2024년 8월 말 경에 완료되어야 했으므로, 실제 공개가 2024년 11월 말에 이루어진 것이다. 이에 대해 EC는 Q&A에서 감사가 완료되지 않았더라도 2023년의 위험평가 보고서를 공개할 것을 권고하였다. 그러나 위험평가 보고서가 처음 공개된 것은 2024년 11월이고, 이때 부킹닷컴(booking.com), 잘란도(Zalando), 핀터레스트(Pinterest)는 2023년(2022~2023) 및 2024년(2023~2024) 보고서를 모두 공개한 반면, 메타(페이스북 및 인스타그램), 알리바바는 2024년도 보고서만을 공개하였다. DSA 시행 초기에 언제, 어떤 보고서를 발표해야 하는지에 대한 혼란이 있었던 것으로 보인다.¹⁸⁾

1) 첫 번째 위험평가 보고서에 대한 평가

DSA에 따른 첫 번째 시스템적 위험평가 보고서는 플랫폼에 대한 규제 역사에서 중요한 전환점이 될 수 있다. 무엇보다, 그동안 빅테크 기업

17) 정보법연구소(Institute for Information Law, IViR)와 암스테르담 대학이 운영하는 ‘DSA 관측소(Observatory)’ 프로젝트의 기사에 따르면, 이 당시에 지정된 25개 사업자 중 초기에 지정된 19개 사업자의 위험평가 보고서가 2024년 11월 22일에서 12월 4일 사이에 공개되었다. Albert, J. (2024, December 9) 참조. EC도 2024년 11월 26일에 이에 대한 보도자료를 배포하였다. European Commission. (2024, 11, 26) 참조.

18) Albert, J. (2024, December 9).

내부에서만 존재하던 위험평가와 정책적 고려가 공식 문서 형태로 외부에 공개되기 시작했다는 점은 중요한 진전이다. 플랫폼들은 이번 보고서를 통해 내부 정책, 절차, 위험 완화조치 등 그동안 알려지지 않았던 운영 정보를 비교적 체계적으로 제시했고, 이는 규제기관, 연구자, 시민사회가 빅테크의 운영 실태를 분석하고 규제 방향을 설계하는 데 실질적 단서를 제공할 수 있다.¹⁹⁾ 다만 거대 플랫폼의 시스템적 위험을 식별하고 완화조치를 취하도록 한다는 보고서의 목적에 비추어보면, 첫 번째 보고서들이 매우 미흡했던 것이 사실이다. 시스템적 위험평가 자체가 플랫폼이 자체적으로 수행하는 평가라는 점에서, 그 보고서가 일정하게 방어적이고 피상적인 수준에 머무를 가능성이 있었다.

시민사회의 공동 평가 의견은 2025년 3월에 발표된 <첫 번째 위험평가 보고서에 대한 초기 분석> 보고서에 담겨 있다.²⁰⁾ 이 보고서는 ‘DSA 시민사회 조정 그룹’이 ‘추천시스템 작업반’ 및 ‘민중 vs 빅테크 (People vs Big Tech)’와 협력하여 작성하였는데, 이들은 모두 유럽의 DSA 관련 시민사회 논의기구들이다. 이 보고서와 여러 다른 평가들²¹⁾에서는 공통적으로 첫 번째 위험평가 보고서의 주요 문제점이 다음과 같다고 지적하였다.

첫째, 플랫폼들의 보고서 대부분이 콘텐츠 및 이용자가 생성하는 위험 문제에 초점을 둔 반면, 플랫폼 자체의 설계 위험에 대해서는 간과하였다. 즉, 플랫폼들은 보고서가 다루어야 할 ‘시스템적 위험’을, 자사의 추천 알고리즘, 콘텐츠 관리 정책, 참여 유도형 순위 메커니즘에 내재된

19) 페이스북, 인스타그램, 유튜브, 틱톡, X 등 주요 플랫폼의 위험평가 보고서에 대한 분석은 신뢰·안전 전문가 팀 버나드(Tim Bernard)의 TechPolicy.press 기고글 참조. Bernard, T. (2024, December 21).

20) DSA Civil Society Coordination Group. (2025, March).

21) 예를 들어, Albert, J. (2024, December 9); Chapman, P. (2025, January 9).

위험이라기보다 악의적인 행위자가 초래하는 외부적 위협으로 규정하는 경향이 있었다. 플랫폼의 설계 자체가 위험을 내재하고 있다면 플랫폼의 설계를 변경해야 하는데, 이는 이윤 극대화라는 플랫폼의 목표와 상충될 수 있기 때문이다.

그러나 시민사회 보고서는 독립적이고 권위 있는 연구들에서 나온 여러 증거들에 따르면 플랫폼의 설계 기능이 어떻게 다양한 종류의 위험을 야기할 수 있는지 계속 드러나고 있다고 지적한다. 예를 들어, 참여도에 기반하여 콘텐츠 순위를 매기는 추천시스템은 다양한 시스템적 위험에 기여하는 방식으로 문제적 콘텐츠를 증폭시킨다. 한 연구에서는 틱톡의 추천 피드(For You Feed)가 이용자를 특정 유형의 콘텐츠에 반복적으로 노출시키는 ‘토끼굴(rabbit holes)’ 효과를 통해 시스템적인 정신 건강 위험을 초래할 수 있음을 밝혀낸 바 있는데,²²⁾ 틱톡은 자사 보고서에서 이 문제를 전혀 다루지 않았다. 심지어 틱톡은 보고서에서 “미성년자를 특별히 겨냥하지 않았으며 이들에 의해 주로 이용되지도 않는다”고 주장하였는데, 많은 연구들에 따르면 틱톡은 미성년자가 가장 많이 이용하는 플랫폼 중 하나이며, 틱톡 내부 문서에서도 틱톡은 13세 미만 이용자를 ‘핵심 연령층(critical demographic)’으로 간주하고 있었다.

다른 플랫폼의 보고서들 역시 악의적인 행위자의 행동과 위반 콘텐츠의 확산 방지 문제에 초점을 맞춘 반면, 추천 콘텐츠의 초개인화로 인해 발생하는 위험의 문제는 다루지 않았다. 시스템적 위험을 진단할 때 설

22) Hobbs, T. D., Barry, B., & Koh, Y. (2021). 'The corpse bride diet': How TikTok inundates teens with eating-disorder videos. The Wall Street Journal; Center for Countering Digital Hate (CCDH). (2025). Deadly by design; Eko. (2023). Suicide, incels, and drugs: How TikTok's deadly algorithm harms kids. DSA Civil Society Coordination Group. (2025, March)에서 재인용.

게 위험의 문제에 초점을 맞추지 않았기 때문에, 이어지는 완화조치에 대한 초점 역시 콘텐츠 및 콘텐츠 관리에 머물러 있었고, 문제를 식별하고 보고하는 책임 역시 이용자에게 전가되었다.

둘째, 위험평가 보고서에서 제시한 완화조치와 그 효과가 검증가능하지 않았다. 주장을 검증할 수 있는 구체적인 데이터를 플랫폼들이 제공하지 않았기 때문이다. 플랫폼들은 이렇게 추상적으로 제시할 수밖에 없는 이유에 대하여, 데이터가 영업비밀에 해당한다거나, 의도치 않게 악의적인 행위자에게 이용될 수 있기 때문에 민감한 경우가 있을 수 있다는 점을 들었다. 또한 DSA가 플랫폼에 완화조치의 선택 근거와 그 효과에 관한 주장을 뒷받침할 추가적인 맥락 정보와 데이터를 제출하도록 명시적으로 요구하지 않았다고 주장한다. 그러나 시민사회는 충분한 데이터가 제공되지 않는 한 보고서의 내용을 신뢰하기 어려우며, 특히 독립적인 연구와 유출된 문서들에서 보고서의 주장과 상충되는 사실이 드러나고 있다는 점에서 보고서의 주장들이 의심스럽다고 비판하였다.

나이트-조지타운연구소(Knight-Georgetown Institute, KGI)도 초기 위험평가 및 감사가 플랫폼 설계와 위험 간의 관계를 충분히 고려하지 못했다고 지적하였으며, 위험 및 완화 효과 평가에 사용된 데이터, 지표, 방법론에 대한 구체성이 부족하고, 데이터 접근성 부족으로 인해 외부에서 그 내용을 분석하는 데 어려움이 있다고 평가하였다.²³⁾

셋째, 위험평가 보고서 작성 과정에서 이해관계자와의 협의가 부재하였다. DSA 시민사회 조정 그룹에 속한 단체 가운데 위험평가 과정에서 자문 요청을 받은 곳은 단 한곳도 없었던 것으로 나타났다.

DSA는 전문(recital) 90에서 “VLOP 및 VLOSE 제공자는 위험평가 및 완화 방식이 최신의 신뢰할 수 있는 정보와 과학적 통찰에 기반하도록

23) Knight-Georgetown Institute (KGI). (2025, May 15).

해야 하며, 자신들이 취하는 위험과 조치에 의해 가장 큰 영향을 받는 집단을 대상으로 자체 가정을 검증해야 한다. 이를 위해 제공자는, 적절한 경우, 서비스 수신자(이용자)의 대표, 자사 서비스로 인해 영향을 받을 수 있는 집단의 대표, 독립적인 전문가 및 시민사회단체의 참여를 바탕으로 위험평가를 실시하고 위험 완화조치를 설계해야 한다. 또한 설문조사, 표적집단 면접(포커스 그룹), 라운드테이블 및 기타 자문·설계 방법을 적절히 활용하여 이러한 의견 수렴 과정을 위험평가 및 완화조치 설계 방법론에 내재화하도록 노력해야 한다. 특정 조치가 합리적이고 균형적이며 유효한지 평가할 때에는 표현의 자유에 대한 권리를 특별히 고려해야 한다”고 명시하고 있다. 그러나 대부분의 위험평가 보고서는 이해관계자와의 협의가 어떻게 이루어졌는지는 명확하게 밝히지 않았다.

넷째, 시민사회 평가보고서는 향후 위험평가 및 보고서 작성 과정에서 개선이 필요한 사항에 대해서도 제안하고 있는데, 보고서 형식의 개선도 그 중 하나이다. 각 플랫폼 보고서의 범위와 내용은 서비스 유형 및 관련 위험, 그리고 기업 간 문화적 및 조직적 차이에 따라 매우 다양하였다. 그런데 위험평가 보고서가 투명성을 위한 의미 있는 도구 역할을 하기 위해서는 이해하기 쉽고 비교 가능한 형식으로 발표되어야 한다. 물론 서비스의 성격과 기능에 따라 일정한 차이가 존재하겠지만, 공통의 포맷을 만드는 것이 불가능한 일은 아닐 것이다. 시민사회 평가보고서에서 제안하는 내용은 다음과 같은 것들이다.

- 분량 단축 및 내용의 구체화: 기존 자료를 재활용해 일반적인 정보가 과도하게 담긴 경향이 있음. DSA 법안에 직접적으로 부합하는 구체적인 내용 위주로 작성하여 전체적인 분량을 줄이고 가독성을 높여야 함.
- 시각화 및 구조화: 표나 시각 자료를 활용하여 구조를 일관되게

구성하는 것이 중요함 (예: 틱톡의 경우처럼 위험 요소와 이에 대응하는 완화조치를 대조하여 제시하는 표의 활용을 권장함).

- 하이퍼링크 및 참고문헌 명확화: 관련 연구나 투명성 보고서를 링크할 때 단순히 출처만 첨부해서는 안 되며, 주장을 뒷받침하는 정확한 자료 위치를 명시하여 링크를 제공해야 함.
- 평가 기준 및 수치화된 지표 공개: 유해 콘텐츠 노출도 및 완화조치 효과성을 측정 가능한 지표로 구체화해야 함. 이 지표들을 대중에게 공개하고, 명확한 시각 자료로 제시해야 함.
- 기계 판독 가능 데이터(Machine-Readable Data)의 제공: 데이터 추출 및 분석이 용이하도록 기계 판독 가능한 형식의 문서(JSON, CSV 등)를 함께 제공할 것을 권장함.

보고서의 개선 방안들은 이러한 문제점들로부터 자연스럽게 도출할 수 있다. 첫째, 위험평가 보고서는 콘텐츠 추천시스템을 비롯하여, 플랫폼의 설계가 미치는 위험을 보다 철저하게 다루어야 한다. 둘째, 완화조치의 효과성을 입증할 수 있는 정량적, 정성적 데이터를 공개해야 한다. 셋째, 위험평가 및 보고서 작성 과정에 이해관계자의 의미 있는 참여를 보장해야 한다. 넷째, 보고서의 내용을 쉽게 이해하고 상호 비교할 수 있도록 보고서의 형식을 개선해야 한다.

2) 첫 번째 라운드 이후의 상황

첫 번째 위험평가 보고서가 공개된 이후, 차기 라운드에서는 첫 공개에서 제기되었던 문제들이 어느 정도 개선되었을까.

유럽비영리법센터(ECNL)은 2년 차와 3년 차 보고서가 구조와 가독성 측면에서 개선되었으나, 내용적 측면에서는 의미 있는 진전을 보이지 못했다고 평가했다.²⁴⁾ 이 단체는 정책 보고서에서 현재까지 발표된 위

험평가 보고서의 5가지 문제점을 지적하였는데, 그 내용들은 앞서 살펴본 첫 번째 보고서에 대한 평가와 크게 다르지 않았다. 첫째, 실제 평가에 대한 세부 정보가 부족하다. 즉, 위험이 어떻게 개념화되고 식별되었는지, 그리고 각 위험의 심각성과 발생 가능성이 어떻게 평가되었는지에 대한 구체적인 설명이 부족하다. 시스템적 위험이 어떻게 식별되고 평가되었는지에 대한 일반적인 서술은 포함되어 있으나, 이를 입증할 수 있는 증거는 공개되지 않았다. 둘째, 특히 플랫폼의 제품과 서비스가 기본권에 미치는 위험과 완화조치의 효과에 대한 평가는 다른 시스템적 위험에 대한 분석에 비해 깊이와 충실도가 떨어진다. EU 기본권 헌장이 보장하는 권리를 포괄적으로 다루지 못한 채, 대체로 가장 가시적이거나 논란의 여지가 적은 권리에 초점을 맞추어 일부 권리만을 제한적으로 평가했다. 또한 자동화된 콘텐츠 관리 시스템과 같은 플랫폼의 완화조치가 기본권에 미치는 효과에 대해서도 충분한 평가가 이루어지지 않았다. 셋째, 의미 있는 면밀한 검토를 위해서는 플랫폼의 주장을 뒷받침하는 정보가 필요하지만, 대부분의 경우 관련 데이터나 충분한 정보를 제공하지 않았다. 또한 플랫폼은 자동화된 콘텐츠 관리 이외의 목적으로 사용되는 알고리즘에 대한 정보도 공개하지 않고 있다. 그러나 DSA 제34조 제2항은 광고나 콘텐츠 추천에 사용되는 시스템이 시스템적 위험에 어떠한 영향을 미치는지를 고려하도록 요구하고 있다. 넷째, 플랫폼은 세 차례의 위험평가 라운드 모두에서 시민사회를 비롯한 이해관계자와 충분한 소통과 협의를 거치지 않았다. 다섯째, 플랫폼은 일부 EU 국가의 특정 사례에만 초점을 맞추는 등 파편적으로 접근하고 있으며, 위험 및 완화조치에 대한 평가가 지리적, 언어적 맥락에 따라 어떻게 달라지는지 설명하지 못했다. 플랫폼은 EU 회원국 전반의 다양한 언어적, 지리적 맥락을 보다 일관되게 고려할 필요가 있다. ECNL은 향

24) European Center for Not-for-Profit Law (ECNL). (2026, March 3).

후 위험평가가 실질적으로 유용한 제도로 기능하기 위해서는 상당한 개선이 필요하다고 지적했다. 이를 위해서는 EC가 위험평가 보고서의 표준과 기대사항, 그리고 위험평가에서 공개해야 할 데이터의 범위에 대해서 구체적인 지침을 마련해야 한다고 촉구했다.

유럽시민자유연맹(Civil Liberties Union for Europe)도 유럽민주주의연합(European Partnership for Democracy)과 함께 2025년 11월 공개된 위험평가 보고서들을 분석한 공동보고서를 발표하였다. 이들 역시 이전 보고서와 비교해볼 때 의미 있는 진전을 찾아보기 어렵다고 비판했다.²⁵⁾ 특히 시민 담론과 선거 절차에 미치는 시스템적 위험에 초점을 맞추어, 플랫폼이 자체 설계에서 비롯되는 위험을 충분히 설명하지 못하고 있다고 지적했다. 이런 방식의 접근에 따르면, 시민 담론과 선거의 공정성을 위협하는 요인이 플랫폼의 설계에 있기 보다는 주로 허위정보나 외국의 개입과 같은 외부적 요인에서 비롯되는 것으로 간주된다. 또한 플랫폼이 여전히 시민 담론의 중요성을 주로 선거와 관련된 맥락으로만 인식하고 있다는 점도 비판하였다. 이러한 제한적인 관점은 시민 담론이 선거 시기에만 중요한 것이 아니라, 소수자의 목소리를 보호하고 다원주의를 촉진하는 등 민주주의의 일상적인 작동을 지탱하는 지속적이고 일관된 요소라는 점을 충분히 반영하지 못한다는 것이다. 주요 지표들이 공개되지 않았기 때문에, 외부 기관이 플랫폼의 위험 완화조치가 실제로 효과가 있었는지 검증하기 어렵고, 개선을 위해 내외 부적으로 어떤 이해관계자와 협의하였는지 불투명하다는 지적은 앞서 살펴본 다른 평가들과 유사하다. 이들은 이러한 문제를 개선하기 위해 EC가 위험평가 방법론에 관한 명확한 지침을 제시하고 감독 권한을 행사해야 한다고 제안하였다. DSA 제35조는 EC가 특정 위험과 관련하여 모범 사례를 제시하고 가능한 완화조치를 권고하기 위한 지침을 발표할

25) Liberties. (2026, March 10).

수 있다고 규정하고 있다. 또한 이들은 EBDS에 대해서도 향후 위험평가 보고서에서 플랫폼의 구조(설계)로 인한 위험을 명확히 밝히고, 이해관계자와의 협의가 이루어질 수 있도록 지침을 제시해야 한다고 제안하였다.

3) 유럽디지털서비스사회의 보고서

이처럼 위험평가 보고서의 내용 면에서 뚜렷한 진전이 없었던 원인으로 는 규제기관이 아직 구체적인 지침을 제공하지 않았다는 점이 꼽힌다. 플랫폼들의 위험평가 보고서를 유럽연합 차원에서 종합적으로 검토한 의견은 EBDS의 보고서를 통해 살펴볼 수 있다. DSA 제35조 제2항은 EBDS가 집행위원회와 협력하여 1년에 한번 위험평가 및 위험 완화 관행에 대한 종합보고서를 발행하고, 이를 통해 EU 및 회원국에서 두드러지고 반복적으로 나타나는 시스템적 위험을 식별하는 한편, 위험 완화를 위한 모범 관행을 제시하도록 하였다.

그러나 EBDS의 첫 번째 종합보고서는 2025년 11월 18일해야 처음 공개되었는데, 그 내용은 구체적인 지침을 제시하기보다는 현재 활용되고 있거나 제안된 위험 완화 관행을 열거하는데 초점을 맞추고 있었다. EBDS는 이 보고서의 어떤 내용도 DSA 제34조 또는 제35조의 준수를 위한 지침으로 해석되어서는 안 되며, VLOP 및 VLOSE의 규정 준수 여부에 대한 평가나 지침으로 해석되어서도 안 된다고 명시하였다. 또한 이 보고서는 DSA에 따라 현재 진행 중이거나 향후 이루어질 조사, 집행 조치 또는 공식적인 조사 결과에 어떠한 영향도 미치지 않는다고 밝혔다. 다만 이러한 방식이 향후 발간할 보고서에서도 유지되는 것은 아니며, EBDS는 향후 보고서에서 시스템적 위험 완화와 관련하여 발전하는 모범 관행을 식별하는 것을 목표로 한다고 말했다. 따라서 2026년 말에 발간될 두 번째 종합보고서에 담길 내용에 계속 주목할

필요가 있다. 첫 번째 보고서는 2024년 2월 17일부터 2025년 2월 16일까지를 보고 기간으로 하며, 사업자뿐만 아니라 다양한 이해관계자로부터 수집한 정보를 바탕으로 시스템적 위험에 대한 개요와 특정 위험 완화 관행에 대한 개요를 제시하는데 초점을 두고 있다. 보고서 작성에는 우선 VLOP 및 VLOSE 제공자가 2023년과 2024년에 EC와 각 회원국 DSC에 제출한 위험평가 보고서의 공개본,²⁶⁾ 제37조에 따른 감사보고서의 공개본이 활용되었다. 이 밖에도 제39조에 따른 DSA 광고 저장소, 제37조에 따른 DSA 감사이행 보고서, 투명성 보고서, 제17조에 따른 사유 진술서(statements of reasons)를 대중에게 공개하는 DSA 투명성 데이터베이스 등 VLOP 및 VLOSE 제공자가 작성한 여러 DSA 투명성 자료가 활용되었다. 아울러 EC와 DSC가 발주한 연구를 통해 수집된 의견, 연구자 및 시민사회단체가 제출하거나 발표한 자료와 연구 등도 보고서 작성에 반영되었다. 한편 보고서는 향후 DSA 제40조에 따른 연구자 데이터 접근 메커니즘을 통해 확보된 데이터를 활용함으로써 시스템적 위험에 관한 보다 발전된 과학적 분석이 가능해질 것이라고 전망하고 있다. 첫 번째 보고서가 작성될 당시에는 제40조에 따른 연구자 데이터 접근 메커니즘이 아직 작동하지 않았기 때문이다.

이 보고서는 VLOP 및 VLOSE 제공자의 자체 평가와 시민사회단체 및 연구자들의 분석을 종합하여, 현재 EU 내에서 식별된 가장 두드러지고 반복되는 시스템적 위험을, DSA 제34조 제1항의 구분에 따른 네 가지 범주로 나누어 제시하고 있다.

첫째, 불법 콘텐츠의 확산 위험으로 다음과 같은 행위들을 포함한다.

26) 2023년 4월 이후에 지정된 VLOP 및 VLOSE의 경우, 위험평가 보고서가 EC 및 DSC에 제출되기는 하였으나 아직 대중에게 공개되지는 않았던 시점이기 때문에 2025년 11월 18일 공개된 EBDS 보고서에는 포함되지 않았다.

- 불법 제품, 서비스 및 활동: 온라인 마켓플레이스를 통한 유해·위조 상품 및 미승인 의약품 등 불법제품의 유통, 인신매매 및 성착취 등 불법 활동 알선, 사이버 공격 도구 판매 등.
- 아동 성착취물(CSAM): 소셜 미디어 및 검색엔진을 통한 CSAM 유포, 온라인 그루밍.
- 테러리즘 콘텐츠: 테러 선전·모집 및 극단주의 콘텐츠 확산.
- 불법 증오표현 및 증오범죄 선동
- 지식재산권 침해: 위조품 및 불법 스트리밍을 통한 저작권, 상표권 침해, 불법 복제 콘텐츠 접근을 제공하는 앱.
- 은어, 암호화 언어를 통한 탐지 회피, 백업 계정/콘텐츠, 오디오·라이브스트림 포맷의 감시 사각지대.

둘째, 기본권에 미치는 부정적 영향이다. 이와 관련된 위험은 다음과 같다.

- 표현의 자유 및 정보 접근권 위축: 과도한 콘텐츠 삭제(합법적 콘텐츠 삭제), 과소한 콘텐츠 관리(콘텐츠 방치로 인한 소수자에 대한 위축 효과), 신고 시스템 남용, 불투명한 추천 시스템으로 인한 의견 다양성 저해.
- 차별금지 : 광고 및 알고리즘의 편향으로 인한 차별적 노출
- 소비자 보호: 허위광고, 가짜후기, 금융사기, AI를 이용한 유명인 사칭 사기.
- 사생활 및 개인정보 보호: 스토킹 앱, 동의 없는 성적 촬영물 유포(NCII), 신상 털기(doxing).

셋째, 시민 담론, 선거 과정 및 공공 안녕에 미치는 위험이다.

- 허위정보·조작정보, 외국 세력의 정보 조작(FIMI) 및 조직적 비

진정 행동(coordinated inauthentic behaviour, CIB).

- 선거과정의 허위조작정보: 선거 일정, 후보자격, 선거 절차에 대한 거짓 정보, 선거 정당성 훼손.
- 공인 대상 표적 공격: 정치인·언론인 등 공인을 대상으로 한 허위 정보, 명예훼손, 딥페이크 유포.
- 위기 및 재난시 공공 안녕 저해: 자연재해, 폭력 사태 시 조작된 영상 확산으로 사회적 혼란 유발, 폭력·소요 행위 조장.

넷째, 젠더 기반 폭력과 공중보건, 미성년자 보호 및 신체·정신적 웰빙에 미치는 부정적 영향이다.

- 젠더 기반 폭력(Gender-based violence, GBV): 여성·소수자 대상 디지털 성폭력, AI 생성 딥페이크 음란물 유포, 여성 공인에 대한 공격.
- 공중보건 : 백신·질병 관련 허위정보, 불법·위조 의약품 판매, 극단적 다이어트 조장.
- 미성년자 보호: 아동 성착취물(CSAM), 사이버 괴롭힘, 나이 인증 우회, AI 생성 아동 성착취물.
- 신체·정신적 웰빙 : 무한 스크롤 등 중독 유발 설계로 인한 수면 장애 및 신체·정신적 폐해, ‘토끼굴(Rabbit hole) 효과’로 인한 유해 콘텐츠(자해·섭식장애 등)의 반복 노출.

또한 이러한 위험들은 공통적으로 추천 시스템, 인터페이스 설계, 광고 시스템, 콘텐츠 관리(moderation) 시스템, 생성형 AI 오남용, 서비스의 의도적인 조작 등을 통해 나타났다.

이러한 시스템적 위험에 대응하여 보고서의 제4장에서는 플랫폼 사업자들이 도입하거나 제안한 위험 완화 관행들을 다음과 같이 소개하고 있다. 우선 온라인 인터페이스를 포함한 서비스 설계 측면에서는 총동적인 유해 행위를 억제하기 위한 ‘마찰(friction)’ 설계가 활용되고 있다. 예를 들어 이용자가 공격적이거나 유해한 콘텐츠를 게시하기 전에 경고창을 띄워 재고를 유도하는 팝업(circuit breakers)이나 넛지(nudge) 기법이 도입되었다. 미성년자 보호를 위해서는 미성년자 계정의 기본 비공개 설정, 모르는 이용자와의 다이렉트 메시지 차단, 야간 시간대 알림 제한 및 무한 스크롤 비활성화, 강화된 보호자 통제 도구 등이 대표적 조치로 제시되었으며, 민감한 콘텐츠에 대한 블러 처리와 경고 배너 적용도 활용되고 있다.

약관 및 집행과 관련해서는 딥페이크 등 새로운 위험을 반영하여 정기적으로 약관을 개정하고, 미성년자의 서비스 접근을 제한하며, 나이 인증을 강화하는 등의 조치가 활용되고 있다. 콘텐츠 조정 시스템에서는 인공지능 기반의 자동 탐지 기술과 인간 검토자의 역할을 결합한 운영체계가 활용된다. 텍스트, 이미지, 오디오 전반에 걸친 머신러닝 모델과 해시 매칭 기술(CSAM 및 테러 콘텐츠 탐지용)을 적용하는 한편, 특정 국가의 언어적·문화적 맥락과 은어를 파악할 수 있는 현지 전문 인력을 배치하는 노력이 병행되고 있다. 아울러 위반 계정에 대한 단순 경고부터 기능 제한, 수익화 차단, 영구 정지에 이르는 단계적 제재 메커니즘이 운영되고 있다. 팩트체커와의 협력이나 커뮤니티 노트(community notes)의 사용도 언급되었다.

알고리즘 및 추천 시스템과 관련해서는 유해하거나 검증되지 않은 콘텐츠의 노출 순위를 낮추는 강등(demotion) 조치와 함께, 공신력 있는 출처(authoritative sources)의 정보를 우선 노출하는 방식이 사용되고 있다. 나아가 이용자의 자율성을 보장하기 위해 프로파일링에 기반

하지 않은 추천 피드 선택권(opt-out)을 부여하거나 ‘관심없음’, 추천 초기화 기능을 제공하고, 대립되는 집단 간의 공통점을 넓히는 ‘브리징(bridging)’도 잠재적 완화조치로 제안되었다.

광고시스템과 관련해서는 광고주의 신원 사전 검증, 광고 콘텐츠에 대한 사전 심사, 선거와 같은 민감한 이슈 광고에서의 생성형 AI 사용 금지, AI 생성 광고에 대한 표시 의무, 미성년자 대상 표적광고의 제한 등이 제안되었다. 서비스의 악용 방지, 콘텐츠 및 계정의 진정성과 관련된 위험 탐지와 관련되어서는 딥페이크에 대한 투명한 라벨링 부착 의무화, 허위 계정에 대한 목록화, 위험 탐지팀의 운영, 2단계 인증 등의 조치가 시행되고 있다.

또한 법적으로 지정된 ‘신뢰할 수 있는 신고자(trusted flaggers)’의 통지에 대해 별도의 전용 접수 창구를 마련해 우선적으로 신속 처리하고 처리 결과를 피드백하는 협력 모델을 운영하고 있으며, 허위정보 대응을 위한 자율규약 준수, 선거 및 재난 대응을 위한 24시간 신속 대응 태스크포스(TF) 가동, 이용자 미디어 리터러시 캠페인 등도 주요 완화조치로 제시되었다. 이 외에도 허위정보 및 혐오표현 행동강령과 같은 업계 공동기준의 활용, 미디어 리터러시 캠페인이나 부모 가이드와 같은 인식제고 조치 등이 활용되고 있다.

그러나 보고서는 이러한 조치들이 현재 각 사업자에 의해 시행되거나 제안된 관행을 초기 단계에서 정리한 것일 뿐, 그 자체로 DSA 법적 준수 여부를 최종 평가하거나 공인된 ‘모범 사례(best practices)’로 확정된 것은 아니며, 향후 축적되는 실무 경험과 연구자들의 데이터 기반 연구를 통해 지속적으로 정교화될 것임을 덧붙이고 있다. 여러 시민사회단체에서 지적한 바와 같이, 이사회와 감사보고서를 비롯하여 EC 지침 등을 통해 위험평가 및 완화조치에 대한 보다 구체적인 실행 지침을 제공해야 위험평가가 보다 실효성을 가질 수 있을 것으로 보인다.

4) 미국 소송 자료와의 비교에서 드러난 한계

나이트-조지타운연구소(KGI)는 DSA 위험평가 보고서와 미국에서 메타 및 틱톡을 상대로 제기된 소송 과정에서 공개된 자료를 비교·분석하여, DSA 위험평가가 얼마나 형식적으로 이루어지고 있는지를 보여주었다.²⁷⁾ 미국에는 EU DSA와 같은 규제 절차가 존재하지 않지만, 소송 과정의 증거개시(Discovery) 절차를 통해 플랫폼의 내부 자료에 접근할 수 있는 제도가 마련되어 있다. 이처럼 미국과 유럽의 서로 다른 제도를 통해 공개된 증거와 자료들을 비교하는 것은 상호 학습의 기회가 될 수 있다.

DSA에 따른 플랫폼의 위험평가와 미국에서 진행된 소송은 모두 플랫폼이 미성년자에 미치는 잠재적 위험을 다루고 있다. 양자에서 공통적으로 강박적 이용 및 중독과 유사한 행동, 수면 부족, 자해, 섭식 장애를 비롯한 미성년자의 정신적·신체적 건강에 대한 우려가 확인되었다. 그러나 앞서 살펴본 시민사회 보고서에서도 지적했듯이, DSA에 따른 플랫폼의 자체적인 위험평가 보고서는 여전히 서술적인 수준에 머물러 있으며 플랫폼 설계에서 비롯된 위험이나 완화조치의 효과를 검증할 수 있는 데이터를 제공하지 않았다. 반면, 미국 소송 과정에서 공개된 자료는 플랫폼의 설계 위험에 대해 훨씬 더 상세한 정보를 제공하고 있다.

예를 들어, 틱톡은 2024년 위험평가 보고서에서 스크린타임(화면 이용 시간) 관리도구와 기본 프라이버시 설정을, 2025년 보고서에서는 청소년 안전 센터, 웰빙 및 보호자 가이드, 미성년자 대상 기본 설정 등 다양한 안전 기능에 대해 강조하였다. 그러나 이러한 완화조치의 효과에 관한 구체적인 정보는 거의 제공하지 않았다. 틱톡은 위험평가 보고서

27) Chapman, P., & Steinberg, M. (2026, February).

에서는 누가 자사 앱을 이용하는지 세부 정보를 거의 밝히지 않았지만, 미국 소송에서 밝혀진 내부 문서에 따르면 미성년자를 적극적으로 타겟팅해 왔다는 사실이 드러났다. 내부 문서에 따르면, 미국 미성년 이용자의 약 13%인 900만 명이 하루 3.5시간 이상 틱톡을 이용했으며, 약 10%는 하루 4시간 이상 이용했다. 또 다른 내부 문서에 따르면, 미성년 이용자 1,000만 명이 하루 6시간 이상 틱톡을 이용했으며, 틱톡은 이를 내부적으로 “객관적으로 해로운 이용(Objective harmful usage)”으로 분류했던 것으로 드러났다. 틱톡은 이러한 강박적 이용이 플랫폼에 “만연(rampant)”해 있으며, “보상의 가변성” 등 앱의 중독적 이용을 유발할 수 있는 요소를 통해 이용자가 “몰입(flow) 상태, 즉 극도의 참여감과 시간 감각 상실, 나아가 자아 상실에 이르는 심리 상태”에 이를 수 있는 것으로 나타났다고 자인했다. 즉, 틱톡은 대외적으로 스크린타임 관리도구가 이용자의 시간 관리를 돕는다고 강조했지만, 내부적으로는 미성년자가 스스로 스크린타임을 통제하는 데 필요한 ‘실행 기능(executive function)’이나 ‘자기 조절 능력’이 부족하다는 점을 인지하고 있었다. 또한 경영진은 스크린타임 관리도구가 매출에 미치는 영향을 제한하기 위해 “미성년자 및 과도한 이용자와 같은 특별 그룹에 대해서는 체류 시간 감소를 최대 5%까지 허용한다”는 가드레일을 설정했던 것으로 나타났다. 이용자가 직접 활성화해야 하는(opt-in) ‘스크린타임 휴식 알림’의 경우 채택률이 1.4%~1.5%에 머물렀으며, ‘수면 알림’은 0.7%~1.8%에 불과했다. 이들 도구를 활성화기 위해서는 무려 7단계의 복잡한 과정을 거쳐야 했기 때문이다.

메타는 청소년들이 11-12세에 인스타그램을 이용하기 시작하며 13세 미만 아동들이 연령을 허위로 기재하며 가입한다는 사실을 명확히 인지하고 있었다. 내부적으로는 이미 2015년에 13세 미만 인스타그램 이용자가 400만 명에 달하는 것으로 추정했다. 내부 문서에서는 ‘트윈

(Tweens, 10-12세 아동)’을 페이스북 가입 이후 장기 잔존율(retention)이 가장 높은 ‘특별하고 가치 있는’ 이용자 집단으로 묘사했다. 내부 분석에 따르면, 하루 동안 인스타그램 일일 활성 이용자가운데 이용시간 상위 0.1%는 6.83시간 이상을 이용했으며, 월간 활성 이용자의 상위 0.1%는 한 달에 127시간, 즉 하루 평균 4.5시간 이상을 앱에서 보냈다. 심야 시간대(0시~오전 4시)에 이용하는 청소년 가운데 11.7%인 약 150만 명이 잦은 알림 확인이나 짧은 이용 세션의 반복적인 재개 등 중독적 행동을 보였다. 이 심야 이용 세션의 33%는 메타가 보낸 푸시 알림에 의해 촉발된 것이었다. 이러한 자료들은 메타가 미성년자가 플랫폼을 언제, 얼마나 오래 이용하는지뿐만 아니라, 이러한 이용 패턴이 연령에 따라 어떻게 달라지는지까지 세밀하게 추적하고 있었음을 보여준다. 메타는 DSA 위험평가 보고서에서는 ‘알 수도 있는 사람(People You May Know, PYMK)’이나 ‘추천할 만한 계정(Accounts You May Find, AYMF)’ 기능을 통해 미성년자와 유해한 의도를 가진 성인이 연결되는 것을 방지하는 시스템을 갖췄다고 기술했다. 그러나 미국 소송 과정에서 공개된 2023년 내부 통계에 따르면, 인스타그램의 AYMF 기능은 불과 3개월 동안 성인 그루머(아동 성착취가 의심되는 성인) 계정을 약 200만 명의 청소년에게 선제적으로 추천한 것으로 나타났다. 이러한 추천의 약 22%가 실제 청소년의 팔로우 요청으로 이어져, 메타의 추천시스템을 매개로 약 50만 건의 성인 그루머-청소년 간 연결 요청이 발생했다.

이처럼 미국 소송 과정에서 공개된 내부 자료들은 플랫폼이 자체 설계에서 비롯되는 위험과 완화조치의 효과를 평가할 수 있는 구체적인 데이터를 이미 보유하고 있음을 보여준다. 그러나 이러한 데이터는 플랫폼의 DSA 위험평가 보고서나 미국의 안전 조치 관련 정보 공개에서 대부분 찾아보기 어려웠다. 이는 현재의 DSA 위험평가 제도가 가진 한계

를 보여주는 동시에, DSA 시스템적 위험평가 제도의 실효성을 높이기 위해서는 플랫폼이 보유한 내부 지표와 데이터를 충실하게 공개하는 일이 얼마나 중요한지를 보여준다.

5) 집행 조치를 통한 자체 위험평가의 한계 보완

아직까지는 플랫폼의 자체적인 위험평가 및 완화조치의 실효성을 높이기 위한 EC의 구체적인 실행지침이 제시되지 않았다. 그러나 EC의 집행 조치에서 위험평가 보고서가 활용되는 방식을 고려해 볼 때, 보다 강력한 집행이 이루어진다면 플랫폼이 보다 충실하게 위험을 평가하고 완화조치를 마련하도록 촉진할 수 있을 것이다. EC의 집행 조치 관련 보도자료를 살펴보면, EC는 위험평가 보고서를 기본적인 조사자료로 활용하고 있으며, 위험평가나 완화조치가 부실하게 이루어진 경우 이를 DSA 규정 위반의 근거로 삼고 있기 때문이다. 이에 대해서는 제4장에서 구체적으로 살펴본다.

다. 감사 제도의 실효성과 한계

독립적 감사는 플랫폼의 자체적인 위험평가가 갖는 자의성을 보완할 수 있는 절차이다. 첫 번째 감사 주기에서는 이른바 ‘빅4’ 컨설팅 회사 가운데 3개가 총 19건의 DSA 감사 중 17건을 담당했다.²⁸⁾ 페이스북, 인스타그램, 유튜브, 핀터레스트, 스냅챗 등은 언스트앤영(Ernst & Young,EY)이 감사를 수행했고, KPMG가 틱톡과 알리바바를, 딜로이트(Deloitte)는 Bing, 부킹닷컴, 링크드인을 감사했다. 이 3개사는 6개 감사법인들의 네트워크인 ECG(European Contact Group)에 소속되어

28) Albert, J. (2025, December 19).

있다.²⁹⁾ X는 예외적으로 FTI 컨설팅의 감사를 받았다.

현재까지 2024년과 2025년 두 차례에 걸쳐 감사가 진행되었는데, 감사의 절차와 실효성을 둘러싸고 여러 비판이 제기되고 있다.

첫째, 감사인이 따라야 할 표준적인 절차나 정의가 없다. 공통된 정의와 감사 방법론이 부재하기 때문에, 플랫폼과 감사인이 감사에 필요한 주요 개념을 스스로 해석해야 하는 문제가 발생한다. 예를 들어, DSA는 플랫폼에 추천시스템의 “주요 매개변수”를 “쉽고 이해하기 쉬운 언어”로 설명하고, 이용자에게 정보를 추천하는 데 있어 “가장 중요한” 기준과 “해당 매개변수의 상대적 중요도에 대한 이유”를 제시하도록 요구한다. 따라서 추천시스템에 대하여 의미 있는 감사를 수행하기 위해서는 우선 “주요 매개변수”, “쉽고 이해하기 쉬운 언어” 등의 용어에 대한 정의가 필요하다. 이들 개념의 정의가 DSA 준수에 대한 평가 기준이 될 수 있기 때문이다. 그러나 DSA에서 이들 용어를 구체적으로 정의하고 있지 않기 때문에, 각 플랫폼은 이를 서로 다른 방식으로 해석하였고, 감사에서도 플랫폼이 규정한 정의가 그대로 사용되었다.³⁰⁾ 그러나 감사인이 DSA를 독립적으로 해석하기보다 피감사 플랫폼의 정의를 그대로 수용하는 것은 문제가 있다. 감사 절차가 DSA 자체에 대한 준수 여부를 감사하는 것이 아니라, 제공자가 스스로 설정한 DSA 해석에 대한 준수 여부를 감사하는 것으로 제한되기 때문이다.³¹⁾

둘째, 감사인이 감사를 수행할 때 사용하는 절차와 방법론도 명확하지 않다. 감사에 관한 위임규정(delegated regulation)이 있기는 하지만 제한적인 지침만을 제공하고 있어서, 감사인마다 서로 다른 방법론을

29) <<https://www.europeancontactgroup.eu/>>.

30) Chapman, P. (2025, March 1).

31) Holznagel, D. (2025, June 11).

사용하였다. 예를 들어, 이용자가 추천시스템의 매개변수를 변경하였을 때 실제 결과에 영향을 미치는지를 감사할 때 감사인들은 서로 다른 방법을 사용한 것으로 나타났다. 페이스북 감사인의 경우에는 서면 기반 감사에 그친 반면, 핀터레스트의 감사인은 모델 관련 문서와 코드를 검토하여 추천시스템에 사용되는 주요 매개변수가 이용자의 프로파일링 거부 결정에 따라 영향을 받는다는 점을 확인했다. 유튜브의 감사인은 보다 심층적이고 견고한 방법을 통해 추천 결과를 평가한 것으로 보인다.³²⁾

셋째, DSA 제34조에 따른 위험평가 역시 독립적 감사의 대상이지만, 이에 대한 감사는 매우 제한적으로 이루어졌다. 제34조의 위험평가는 플랫폼 사업자 스스로 수행하는 일종의 자체 감사이다. 그러나 이러한 ‘감사 의무에 대한 감사’가 어떻게 처리되어야 하는가와 관련하여, 감사인들은 절차적 측면을 검토하는데 그친 것으로 보인다. 즉, 대개의 경우 제34조에 따른 플랫폼의 위험평가가 제대로 이루어졌는지 실질적인 내용을 검토하기 보다는 위험평가 및 완화의 절차를 중심으로 감사가 이루어졌는데 이는 충분하다고 보기 어렵다. DSA 제37조는 감사인의 임무에 대하여 플랫폼이 법률 준수를 위해 취한 조치만을 평가하는 것이 아니라 DSA의 준수 여부 자체를 평가하는 것임을 명확히 하였기 때문이다. DSA는 플랫폼으로 하여금 감사기관에 필요한 협력과 지원을 제공하고 감사 수행에 필요한 모든 데이터와 시설에 접근할 수 있도록 허용할 것을 요구하였다. 필요한 경우 알고리즘 시스템과 관련된 데이터에 대한 접근도 포함된다. 따라서 감사인들은 추천시스템의 알고리즘을 살펴보는데 유리한 위치에 있었지만, 실제로는 알고리즘 시스템에 대한 실질적인 감사가 수행되지 않았다.³³⁾

32) Chapman, P. (2025, March 1).

33) Holznagel, D. (2025, June 11).

【표 1】 DSA에 따른 첫 번째 감사 결과 요약

Platform	Auditor	34(1)	34(2)	34(3)	35(1)
AliExpress	KPMG	Disclaimer of Opinion (+ 'observations')	Disclaimer of Opinion	Positive	Disclaimer of Opinion
Amazon	KPMG	Positive w / comments	Positive w / comments	Positive	Positive
Apple App Store	EY	Positive	Positive	Positive	Positive
Bing	Deloitte	Positive w / comments	Positive w / comments	Positive w / comments	Positive w / comments
Booking	Deloitte	Positive w / comments	Positive w / comments	Positive w / comments	Positive w / comments
Facebook	EY	Disclaimer of Opinion	Disclaimer of Opinion	Positive	Disclaimer of Opinion
Google Maps	EY	Positive w / comments	Positive w / comments	Positive	Positive
Google Play	EY	Positive w / comments	Positive w / comments	Positive	Positive

Google Search	EY	Positive w / comments	Positive w / comments	Positive	Positive
Google Shopping	EY	Positive w / comments	Positive w / comments	Positive	Positive
Instagram	EY	Disclaimer of Opinion	Disclaimer of Opinion	Positive	Disclaimer of Opinion
LinkedIn	Deloitte	Positive	Positive	Positive	Positive w / comments
Pinterest	EY	Positive	Positive	Positive	Positive
Snapchat	EY	Positive w / comments	Positive	Positive	Positive
TikTok	KPMG	Disclaimer of opinion	Disclaimer of opinion	Positive	Disclaimer of opinion
Wikipedia	Holistic AI	Positive w / comments	Positive w / comments	Positive w / comments	Positive w / comments
X	FTI Consulting	Positive w / comments	Negative	No Conclusion	Negative
YouTube	EY	Positive w / comments	Positive w / comments	Positive	Positive
Zalando	Deloitte	Positive	Positive	Positive	Positive

【표 1】³⁴⁾은 DSA 제34조 및 제35조 의무에 대한 첫 번째 감사주기의 감사의견을 요약한 것이다. 대부분의 플랫폼이 “적정(positive)” 또는 “의견제시가 있는 적정(positive with comments)” 의견을 받았다. 앞서 살펴보았듯이, 이러한 결과는 플랫폼의 위험평가에 대한 감사를 수행할 때 위험평가가 제대로 이루어졌는지 내용적으로 평가를 하기보다는 절차적으로 점검하는 데 한정되었기 때문인 것으로 보인다.

한편, 플랫폼 알고리즘에 대한 감사의 경우 전통적인 감사 방법론만으로는 한계가 있으며, 알고리즘 시스템의 특성에 적합한 새로운 감사 방법론이 필요하다는 지적도 제기되고 있다. 전통적인 ‘체크박스’식 감사는 실시간으로 변경되고 학습하는 동적 알고리즘 시스템을 평가하는 데 적합하지 않다는 것이다. 또한 이러한 방법론은 플랫폼을 정적인 기술적 산물로 취급하는 경향이 있어 사용자 행동과 인터페이스 설계가 알고리즘과 상호작용하며 발생하는 실제 위험을 포착하지 못할 수 있다. 따라서 이러한 한계를 극복하기 위하여 새로운 알고리즘 감사 방법론이 개발될 필요가 있다.³⁵⁾

넷째, 대다수 감사인들은 EC가 플랫폼의 DSA 의무 위반에 대하여 조사를 진행하고 있는 경우, 해당 사안에 대한 평가를 수행하지 않고 건너뛰었다. 앞의 표에서 “의견 거절(Disclaimer of opinion)”로 표시되어 있는 부분이 여기에 해당한다. 그러나 DSA 제37조에는 EC의 조사 대상이라는 이유만으로 감사를 건너뛸 수 있도록 명시적으로 허용하는 규정이 없다.³⁶⁾ 이러한 입장을 취한 감사인은 EY, 딜로이트, KPMG로, 모두 ECG에 소속되어 있다. ECG는 입장문을 통해 EC가 특정 의무와 관련하여 플랫폼에 대한 조사를 이미 진행하고 있는 경우, 감사인은 해당 의무에 대한 결론을

34) Albert, J. (2025, December 19).

35) Solarova, S., Mesarčík, M., Pecher, B., & Srba, I. (2026).

36) Holznagel, D. (2025, June 11).

내리는 것을 자제해야 한다는 지침을 발표했다. 표면적인 근거는 EC가 감사인이 접근하지 못한 관련 증거를 확보하고 있을 가능성이 있으며, 이 정보가 감사인의 판단에 중대한 영향을 미칠 수 있다는 것이다.³⁷⁾ 이러한 입장은 감사인이 EC의 조사결과와 충돌되는 결론을 내릴 경우 발생할 수 있는 법적 책임을 고려한 것으로 보인다. 그러나 이러한 감사 관행은 정작 가장 엄격한 검토가 필요한 사안에 대해 독립적인 감사인이 책임을 회피하고 있다는 비판을 받을 수 있다.

반면 X에 대한 첫 번째 감사를 수행한 FTI 컨설팅의 경우, 감사기간 중 EC가 DSA 제34조 및 제35조와 관련한 절차를 개시했음에도 감사를 생략하지 않고 문제점을 지적하였다. 위 표에서 볼 수 있듯이 X는 ‘부정적(negative)’ 평가를 받았다. 그러나 X는 FTI 컨설팅의 감사 권고 사항을 무시하고 이행을 거부했다. 그 이유로 X는 EC의 관련 조사가 진행 중이라는 점, 시스템적 위험 관리 의무의 범위와 해석을 둘러싼 규제적 불확실성이 계속되고 있다는 점, 그리고 FTI 컨설팅의 감사 결과가 향후 EC의 결정과 상충될 가능성이 있다는 점을 들었다. 이후 X는 감사인을 FTI 컨설팅에서 BDO로 교체하였다. BDO 역시 ECG의 회원사이며, BDO는 2025년 감사에서 EC가 X의 위반 가능성을 조사하고 있는 의무에 대해서는 판단을 유보하였다.³⁸⁾ 물론 DSA는 감사인의 연속성을 요구하지 않으며, 알리바바는 오히려 X와 반대로 KPMG에서 FTI 컨설팅으로 감사인을 교체하기도 하였다. 그러나 플랫폼이 불편한 감사인을 더 순종적인 감사인으로 변경할 수 있다면, 독립적 감사의 의미가 무색해질 것이다. 더불어 EC가 조사 중인 사안에 대하여 감사인들이 입장을 거절해도 되는 것인지 EC가 서둘러 입장을 정리해야 할 것으로 보인다.

37) Albert, J. (2025, December 19).

38) Albert, J. (2025, December 19).

이와 같은 여러 문제점에도 불구하고 독립적 감사가 전혀 의미가 없었던 것은 아니다. 공개된 감사 보고서를 통해서 플랫폼 제공자의 내부 기준에 대한 여러 유용한 정보들이 드러나는 장점도 있었다.³⁹⁾ 그러나 독립적 감사가 보다 실효성을 갖기 위해서는 앞서 지적했던 문제에 대한 개선이 이루어질 필요가 있다.

라. 소결

2026년 7월 현재, VLOP 및 VLOSE에 대하여 사실상 두 차례의 위험평가와 감사가 이루어졌다. 위험평가와 감사 보고서를 통해 주요 플랫폼의 설계, 정책 및 관행에 관한 정보가 어느 정도 공개된 것은 중요한 성과이다. 그러나 미국에서 소송을 통해 드러난 자료들과 비교해 보면, 플랫폼의 자율적인 보고에서는 중요한 정보를 감추거나 의미를 왜곡하는 경우가 많았다. 따라서 DSA 위험평가 및 감사 제도가 애초에 목표로 삼은 효과를 달성하기 위해서는 다음과 같은 문제점들이 보완될 필요가 있다.

첫째, 위험평가 및 감사에 적용되는 정의, 절차, 규범 등이 좀 더 구체화될 필요가 있다. 그렇지 않으면 각 플랫폼과 감사인이 자의적으로 판단할 수밖에 없으며, 이는 객관적인 평가나 상호 비교를 어렵게 만든다. 둘째, 플랫폼은 주요 위험을 악의적인 행위자나 콘텐츠의 문제로 돌리고 있으며, 설계로부터 야기되는 위험에 대한 평가를 제대로 수행하고 있지 않다. 감사인들도 설계 위험평가의 적절성을 제대로 평가하지 않았다. 셋째, 완화 조치의 효과를 검증할 수 있는 데이터와 증거가 제공되지 않았다. 넷째, 위험평가 및 감사 과정에서 이해관계자와의 협의가 제대로 이루어지고 있지 않다. 다섯째, 감사인이 중요한 사항에 대해 EC의 조사가 진행되고 있

39) Holznagel, D. (2025, June 11).

다는 이유로 ‘의견 거절’을 하는 등 감사에 한계가 있었다.

현재까지는 이러한 문제들에 대한 감독 당국의 지침이 부족한 상황이다. 2025년 말에 발표된 EBDS 종합보고서는 식별된 시스템적 위험과 완화조치를 열거하고 있을 뿐 모범 관행을 제시하지 않았으며, EC 역시 효과적인 위험평가 및 감사를 위한 추가적인 지침을 제시하지 않았다. 2026년 말 종합보고서를 포함하여 감독 당국이 어떠한 지침을 제시할지 지켜볼 필요가 있다. 더불어 다음 장에서 살펴보듯이, 플랫폼의 투명성을 강화하기 위한 방안으로 도입된 제3자 데이터 접근 제도가 활성화되어야 할 것이다.

3/ 플랫폼 데이터에 대한 연구자 접근 제도의 현황

가. 연구자 접근 제도 개요

플랫폼 규제와 관련된 가장 큰 걸림돌 중 하나는 불투명성이다. 플랫폼의 알고리즘과 데이터는 기업의 영업비밀로 보호되고 있기 때문에 외부에서 그 작동 메커니즘을 알기 어렵다. 이를 보완하기 위해 DSA 제40조는 검증된 연구자들이 EU 내에서 시스템적 위험에 대한 연구를 수행하기 위해 VLOP 및 VLOSE의 데이터에 대한 접근을 요청할 수 있도록 하였다.⁴⁰⁾ 이는 플랫폼의 시스템적 위험을 더 잘 이해하고 DSA 준수에 대한 효과적인 감독을 지원하기 위한 것이다.⁴¹⁾ 또한 제34조~제35조에 따른 위험평가 및 완화조치가 플랫폼 사업자의 자의적, 형식적인 절차로 전락할 가능성과 제37조에 따른 독립적 감사가 플랫폼 사업자에 의해 사실상 ‘포획’될 위험을 보완할 수 있다.

제40조는 관할 당국 및 연구자의 데이터 접근 절차에 대해 규정하고 있다. 제40조 제1항은 DSC 또는 EC의 합리적 요청이 있을 경우, VLOP 및

40) DSA는 데이터 접근 제도 외에도 연구자가 활용할 수 있는 다양한 투명성 메커니즘을 도입하고 있다. DSA는 호스팅 서비스 제공자가 콘텐츠를 제한하는 결정 사항을 이용자에게 알리고 ‘이유 진술서(statements of reasons)’를 통해 이유를 설명하도록 하였는데, 이 이유 진술서는 DSA 투명성 데이터베이스에 축적된다. 이 데이터베이스를 통해 플랫폼가 콘텐츠를 제한하는 결정을 취한 현황을 추적할 수 있다. DSA 투명성 데이터베이스 사이트는 연구자들이 정보에 접근, 분석, 다운로드할 수 있도록 다양한 도구를 제공하고 있다.

<<https://transparency.dsa.ec.europa.eu/>>.

41) European Commission. (2025, 7, 3).

VLOSE가 본 규정의 준수 여부를 모니터링하고 평가하는 데 필요한 데이터에 대한 접근 권한을 제공하도록 하고 있다. 그런데 지금까지 실제로 이 조항이 규제기관에 의해 얼마나 활용되고 있는지는 의문이다. EC가 조사 대상 사안에 대한 정보를 얻기 위해 제67조에 따른 정보 요청(Request for Information, RFI)을 한 사실은 종종 보도자료를 통해 공개되지만, 제40조에 따른 데이터 접근 요청을 한 사실은 거의 찾아보기 어렵다. 다만 EC는 2025년 1월 17일 보도자료에서 플랫폼의 추천시스템과 관련하여 X에 세 가지 추가적인 기술 조사 조치를 통보했는데, 그 중 하나가 ‘X의 특정 상업용 API에 대한 접근 권한 요청’이다. 이것이 제 40조 제1항에 따른 요청인 것으로 보인다.⁴²⁾

EU 내 시스템적 위험을 탐지, 식별 및 이해하는 데 기여하는 연구를 수행하고자 하는 연구자들은 제40조에 따라 두 가지 방식으로 플랫폼에 대한 접근 권한을 제공받을 수 있다. 첫째 제40조 제12항에 따라, 관련 조건을 충족하는 연구자는 VLOP 및 VLOSE의 온라인 인터페이스에서 공개적으로 데이터에 접근할 수 있다. 둘째, 제40조 제4항에 따라 추가적인 조건을 충족하는 연구자는 DSC에 데이터 접근 신청서를 제출함으로써 VLOP 및 VLOSE의 비공개 데이터에 대한 접근을 신청할 수 있다.

제40조 제12항에 따라 공개적으로 이용 가능한 데이터에 접근하기 위해 연구자는 다음의 조건을 충족해야 한다.

- 상업적 이익과 무관해야 한다.
- 신청서에 연구 자금의 출처를 공개해야 한다.
- 데이터 보안 및 기밀성 요구사항을 충족하고 개인정보를 보호할 수 있어야 한다.
- 연구를 수행하는 데 필요하고 비례적인 범위의 데이터에만 접근할

42) European Commission. (2025, 1, 17).

수 있으며, 해당 데이터가 연구 목적에 기여한다는 점을 입증해야 한다.

‘검증된 연구자(vetted researcher)’로서 제40조 제4항에 따라 비공개 데이터에 접근하기 위해서는 연구자가 추가적으로 다음의 사항을 충족해야 한다. 이러한 조건의 충족 여부는 해당 플랫폼이 설립된 국가의 DSC가 판단한다.

- 연구 기관(지침 2019/790 제2조 제1항에 정의됨)에 소속되어 (affiliated) 있어야 한다.
- 계획된 연구 활동은 DSA 제34조 제1항에 명시된 시스템적 위협의 탐지, 식별 및 이해를 목적으로 하거나 DSA 제35조에 명시된 위험 완화조치를 평가하기 위한 것이어야 한다.
- 연구 완료 후 합리적 기간 내에 연구 결과를 무료로 공개할 것을 약속해야 한다.

2025년 7월, EC는 제40조 제4항에 따라 데이터 접근을 가능하게 하는 절차 및 기술적 조건을 명시한 위임규정을 채택했다. 이 규정은 VLOP와 VLOSE가 검증된 연구자들과 데이터를 공유하기 위한 절차, 데이터 형식, 데이터 문서화 요건 등을 규정하고 있다. 또한 검증된 연구자들의 데이터 세트에 접근 신청을 용이하게 하기 위해 DSC, VLOP, VLOSE 등이 공개해야 하는 정보에 대해서도 규정하고 있다.⁴³⁾

그런데 연구자들이 플랫폼 데이터에 대한 접근을 신청하기 위해서는 우선 어떤 데이터가 있는지 알 수 있어야 한다. 데이터 접근에 관한 위임규정 제6조 제4항은 연구자들이 어떤 데이터를 요청할 수 있는지 알 수 있도록 VLOP 및 VLOSE로 하여금 DSA 데이터 목록(Data catalogues)을 제공

43) European Commission. (2025, 7, 2).

하도록 하였다. VLOP 및 VLOSE는 온라인 인터페이스에서 DSA 데이터 목록을 쉽게 찾고 접근할 수 있도록 해야 한다. 또한 DSA 데이터 목록을 구축할 때 이러한 데이터의 공개로 인해 발생할 수 있는 기밀성, 데이터 보안 또는 개인정보 보호에 대한 잠재적 위험을 평가하고 최소화해야 한다.

DSA 데이터 목록에는 VLOP 또는 VLOSE가 위험평가에서 확인한 시스템적 위험과 관련된 데이터 및 관련 위험 완화조치에 대한 데이터가 포함되어야 하며, 새롭게 확인된 위험 및 완화조치를 고려하여 정기적으로 업데이트해야 한다. 데이터 목록에 모든 데이터가 포함될 필요는 없지만, 연구자의 데이터 접근 신청의 범위를 제한해서는 안 된다. VLOP 및 VLOSE는 검증된 연구자들에게 코드북, 변경로그, 아키텍처 문서 등 제공되는 데이터를 설명하는 관련 메타데이터 및 문서를 제공해야 한다.

검증된 연구자들이 데이터 접근 신청서를 제출하면, 80영업일 이내에 DSC는 타당한 근거를 제시한 요청서를 작성하여 데이터 제공자에게 제출하고 그 사실을 연구자에게 통보하거나, 해당 신청을 수용할 수 없는 경우 연구 책임자에게 그 이유를 통보해야 한다. 각 신청의 개요와 그에 대한 수정 및 업데이트 내역은 해당 요청을 제출한 DSC가 데이터 접근 포털을 통해 공개할 예정이다.

VLOP 및 VLOSE는 데이터 접근 요청을 접수한 후 15일 이내에 다음 두 가지 이유 중 하나를 근거로 DSC에 수정 요청을 제출할 수 있다(제40조 제5항).

- 요청된 데이터에 접근할 수 없는 경우
- 데이터에 대한 접근 권한을 부여하면 서비스의 보안이나 기밀 정보, 특히 영업비밀 보호에 심각한 취약점이 발생할 수 있는 경우

수정 요청에는, 요청된 데이터 또는 요청 목적에 적합하고 충분한 여타의 데이터에 접근할 수 있는 하나 이상의 대체 수단에 대한 제안이 포함되어야 한다. DSC는 15일 이내에 결정을 내리고 VLOP 및 VLOSE에 그 결정과, 필요한 경우 수정된 요청 내용 및 요청 준수 기한을 통보해야 한다(제 40조 제6항). 상업적 고려사항은 요청된 데이터에 대한 접근을 자동으로 거부하는 근거가 되어서는 안 되며, 데이터 접근 방식을 변경하거나 추가적인 데이터 보안 및 기밀 유지 요건을 부과하는 것을 고려하여야 한다.

분쟁이 상호 수용 가능한 방식으로 해결될 수 있도록 VLOP 및 VLOSE는 DSC에 중재 참여를 요청할 수 있다. 그러나 DSC의 중재 참여는 자발적인 것으로서 중재 결과가 DSC를 구속하지 않는다. 수정 요청에 대한 최종 결정 권한은 여전히 DSC에 있다. 중재 과정에 참여하는 모든 당사자는 성실하게 임하고 공정하고 상호 수용 가능한 합의에 도달하기 위해 노력해야 한다.

나. 연구자 접근 제도 활용 현황과 문제점

위임규정은 2025년 10월 29일부터 발효되었다. 이와 함께 연구자들의 데이터 접근을 지원하고 향후 DSA 데이터 접근을 통해 얻은 연구 결과물을 공개할 ‘DSA 데이터 접근 포털’도 개통되었다.⁴⁴⁾ 연구자들은 데이터 접근 포털을 통해 데이터 접근 신청서를 제출할 수 있다.

앞서 설명했듯이, 연구자들이 플랫폼에 데이터 접근을 신청하기 위해서는 우선 어떤 데이터가 있는지 알 수 있어야 한다. DSA 데이터 접근 포털은 각 플랫폼의 데이터 목록에 접근할 수 있는 링크를 모아서 제공하고 있

44) <<https://data-access.dsa.ec.europa.eu/home>>.

다.⁴⁵⁾ 그런데 제40조 제12항에 따라 공개적으로 접근 가능한 데이터에 접근할 수 있는 각 플랫폼의 링크 목록은 제공하고 있지 않다. 대신 다음과 같이 학계나 시민사회가 운영하는 프로젝트에서 관련 정보를 제공하고 있다.

- DSA 40 Collaboratory⁴⁶⁾
- 디지털 민주주의 모니터(Digital Democracy Monitor)⁴⁷⁾
- 플랫폼 투명성 도구 트래커(Platform Transparency Tools Tracker, George Washington University IDDP)⁴⁸⁾

데이터 접근 위임규정이 2025년 10월 29일 발효되었음에도 불구하고, 2026년 7월 현재 DSA 제40조 제4항에 근거하여 승인된 ‘검증된 연구자’ 데이터 접근 사례는 확인되지 않는다. DSA Observatory에 게재된 한 기고글에서 제40조 제4항에 근거한 데이터 접근 신청이 거부된 사례가 공유되었다. 다만 이 신청은 DSA 데이터 접근 포털이 공개되기 하루 전인 2025년 10월 28일에 제출되었고, 당시에는 데이터 접근 요청 대상 플랫폼인 틱톡의 본사가 있는 아일랜드의 DSC인 미디어위원회(Coimisiún na Meán, CNAM)의 안내문도 발표되지 않은 상태였다. CNAM은 2026년 2월 26일에야 신청자 가이드를 발표했다. 데이터 접근 요청이 거부된 이 연구자는 제40조 제4항에 근거한 데이터 접근 신청이 연구자들에게 익숙한 연구비 신청과 달리 법률적 행정 절차에 가깝고, 개인 연구자 수준이 아니라 기관 차원의 참여가 필요하다는 점을 비판하였다.

2026년 5월 19일, EC와 DSC, 그리고 VLOP 및 VLOSE는 공동으로 연구

45) <<https://data-access.dsa.ec.europa.eu/public/dc/data-catalogues>>.

46) <<https://dsa40collaboratory.eu/faq/>>.

47) <<https://digitalmonitor.democracy-reporting.org/data-access/>>.

48) <<https://iddp.gwu.edu/platform-transparency-tools-brussels-effect>>.

자의 데이터 접근을 지원하기 위해 첫 원탁회의를 개최하였다. 당시 DSC는 49건의 신청서를 접수했는데, 주로 소셜미디어 플랫폼의 데이터에 대한 접근을 신청하고 있었고, 불법 콘텐츠 확산, 광고 투명성, AI 기능 등의 위험 요소에 초점을 맞추었다고 한다. 2026년 7월 현재 DSC가 신청서를 평가 중이라고 전해지며, 승인된 신청서가 있는지는 확인되지 않는다. DSA 데이터 접근 포털에 승인된 프로젝트와 결과 보고서에 접근할 수 있는 메뉴가 마련되어 있기는 하지만, 아직 아무런 데이터가 등록되어 있지 않다. 즉, 제40조 제4항에 따른 연구자 데이터 접근은 제도적으로 준비가 되었지만, 8개월이 넘는 시점에도 실질적인 활성화에는 이르지 못한 것으로 보인다. 2026년 말까지 승인된 사례들이 나올지 지켜볼 필요가 있다.

이러한 상황에서 제40조 제12항에 따른 공개 인터페이스를 통하여 데이터에 접근하는 것이 대안적인 경로가 될 수 있다. 학계가 독립적으로 구축한 ‘DSA 40 Collaboratory’ 사이트는 각 플랫폼의 공개 인터페이스를 통하여 데이터에 접근할 수 있는 방법에 대한 정보와 신청, 승인, 기각 건수 등의 현황을 공개하고 있다.⁴⁹⁾ 각 플랫폼이 데이터 요청을 항상 수용하는 것은 아니다. 이 사이트의 통계에 따르면 틱톡은 승인이나 거절 결정까지 평균 약 32.58일, X는 69.17일이 소요되었고, 데이터가 3건에 불과하지만 유튜브는 승인까지 평균 13일이 소요되었다. 가장 흔한 거절 사유는 “귀하의 신청서를 검토한 결과, 귀하가 제안한 데이터의 사용 목적이 DSA 제34조에 명시된 바와 같이 EU 내 시스템적 위험을 탐지, 식별 및 이해하는 데 기여하는 연구 수행에만 국한된 것으로 보이지 않습니다”라는 것이다.

연구자에게 공개적으로 접근 가능한 데이터를 제공하는 것은 VLOP와 VLOSE의 의무임에도 불구하고, 이들은 그다지 적극적이지 않다. VLOP와

49) <<https://dsa40collaboratory.eu/tracker-insights/>>.

VLOSE가 연구자에게 공개적으로 접근 가능한 데이터를 제공하지 않아 EC가 의무 위반으로 결정한 사례들도 있었다. 2024년 7월, EC는 X에 대한 예비 조사 결과를 발표하였는데, X가 연구자들에게 공개 데이터에 대한 접근을 제공하지 않았다는 내용이 포함되어 있었다.⁵⁰⁾ 2025년 6월에는 알리익스프레스(AliExpress)에 대한 조사 절차에서 연구자의 데이터 접근 문제를 포함한 여러 쟁점에 대해 이행약정을 수용하였다.⁵¹⁾ 2025년 10월에는 틱톡과 메타가 공개 데이터 접근 의무를 위반했다는 예비 판단을 받았다.⁵²⁾

공식적인 DSA 데이터 접근 포털은 제40조 제12항에 따른 각 플랫폼의 공개 인터페이스와 관련하여 구체적인 정보나 지원을 제공하고 있지 않다. 다만 DSA 40 Collaboratory 등 학계와 시민사회의 자발적인 활동을 통해 접근이 이루어지고 있을 뿐이다. 학계와 시민사회의 자발적인 이니셔티브는 환영할만한 것이지만, 지속가능성에 한계가 있을 수 있다. 또한 EC 등 감독 당국이 공개 인터페이스를 통한 데이터 접근이 실효성 있게 이루어질 수 있도록 감독해야 한다는 점에서 공적 지원이 공백 상태라는 점은 문제라고 볼 수 있다.

공개 인터페이스를 통한 데이터 접근이 플랫폼의 시스템적 위험을 파악할 수 있는 의미 있는 데이터를 제공하는지에 대한 의문도 제기된다. 한 연구는 틱톡과 메타를 대상으로 가짜 계정을 만들어 실제 이용자에게 보이는 공개 정보 환경(PIE)을 구성하고, 이를 각 플랫폼의 연구 API가 제공하는 데이터와 비교하였다.⁵³⁾ 그 결과 플랫폼의 연구 API가 제공하는 데이터는 세 가지 측면에서 체계적인 데이터 손실이 존재한다는 사실이 발견되었

50) European Commission. (2024, 7, 12).

51) European Commission. (2025, 6, 18).

52) European Commission. (2025, 10, 24).

53) Bekavac, L., & Mayer, S. (2026).

다. 첫째, 접근할 수 있는 정보의 범위가 축소되었고(게시물의 최대 약 50%만 API를 통해 접근 가능), 필수적인 맥락적 메타데이터가 제거되었으며(최대 약 83%), 연구자에게 심각한 기술적 제약이 적용되었다(하루 약 1,000건의 요청으로 제한). 해당 연구는 메타와 틱톡에서 현재와 같은 형태의 연구 API로는 DSA에서 구상하는 시스템적 위험에 대하여 의미있고 독립적인 감사를 수행하는 것이 어렵다고 결론지었다. 이러한 측면들도 당국의 감독 대상으로서 검토될 필요가 있다.

4/ 시스템적 위험에 대한 DSA의 집행 현황

가. DSA 집행절차 개요

DSA에 따른 집행절차는 다음과 같은 일련의 단계를 거쳐 이루어진다.

- **모니터링, 정보요청(Request for Information, RFI): 제67조**
EC는 위험평가 보고서, 투명성 보고서, 시민사회단체 등 제3자 정보 등을 토대로 DSA 위반 여부에 대한 정보를 수집한다. VLOP 및 VLOSE, 감사인, 그 밖의 사람들에게 관련 정보를 제공하도록 요구할 수 있다. 정보 요청에 대해서 부정확하거나 불완전하거나 오해의 소지가 있는 정보를 제공하는 경우 제74조에 따른 과징금을 부과할 수 있다.
- **공식절차 개시(Opening of formal proceeding): 제66조**
EC는 VLOP 및 VLOSE가 DSA를 위반했다고 의심되는 경우 본 조사를 위한 공식절차를 개시할 수 있다. 이때 해당 혐의에 대한 감독관할이 회원국의 DSC에서 EC로 이관된다. EC는 DSC에 지원을 요청할 수 있다.
- **심층 조사: 제67조~69조, 제72조**
EC는 DSA 위반 여부를 판단하기 위해 추가 조사를 실시한다. EC는 제67조에 따른 정보 요청 외에도 강력한 정보 수집 권한을 가지고 있다. 제68조에 따라 정보 수집을 목적으로 자연인이나 법인을 인터뷰할 수 있으며, 제69조에 따라 VLOP, VLOSE, 기타 필요한 사업장에 대한 검사(inspection)를 실시할 수 있다. 검사를 위해 사업장

건물 등에 출입하거나, 관련 장부 및 기록을 검사할 수 있고, 책이나 기타 기록의 사본을 얻을 수 있다. 또한 제72조에 따라 DSA의 효과적인 이행 및 준수 여부를 감독하기 위해 필요한 조치를 취할 수 있는데, 여기에는 VLOP 및 VLOSE에게 데이터베이스 및 알고리즘에 대한 접근 권한 및 관련 설명을 제공하도록 명령하거나, 문서를 보관하도록 의무를 부과하는 것이 포함된다. 독립적인 외부 전문가나 감사인의 지원을 받을 수도 있다.

▪ **잠정 조치(Interim measures): 제70조**

서비스 이용자에게 심각한 손해가 발생할 위험이 있는 경우, EC는 VLOP 등에 잠정 조치를 명령할 수 있다.

▪ **예비판단(preliminary findings): 제73조**

EC는 조사 결과 위반으로 판단되는 경우, 최종 결정을 채택하기 전에 예비판단(예비 조사결과)을 통지한다(제73조 제2항). 이 예비판단에서 문제를 해결하기 위해 취해야 하는 조치를 설명해야 한다. VLOP 등은 이에 대해 의견을 진술할 기회를 갖는다(제79조).

▪ **이행약정(Commitments): 제71조**

VLOP 등은 시정조치를 이행약정의 형태로 자발적으로 제안할 수 있으며, EC는 이 이행약정을 VLOP 등에게 구속력 있게 적용하고 더 이상 조치 사유가 없음을 선언하는 결정을 할 수 있다. 기업은 위반을 인정하지 않고도 절차를 종결할 수 있고, EC는 신속하게 VLOP 등의 DSA 준수를 유도할 수 있다. 이후에 이행약정을 위반하는 것은 DSA를 위반하는 것으로서 과징금 부과 대상이 된다(제74조 제1항 제c호).

▪ **불이행(Non-compliance) 결정 및 과징금: 제73조, 제74조**

EC는 VLOP 등이 DSA 조항, 제70조에 따른 잠정 조치, 제71조의

이행약정을 준수하지 않는다고 판단하는 경우 불이행 결정을 채택한다(제73조). 이 경우 해당 사업자는 최대 직전 회계연도 기준 전 세계 연간 매출액의 6%에 해당하는 과징금을 부과 받는다.

▪ **시정 실행계획(action plan): 제75조**

EC는 VLOP 등에 대한 불이행 결정에서 침해를 종식시키거나 시정하는 데 충분한 조치를 포함하는 실행계획을 수립하고 일정 기간 내에 제출하도록 요구한다. 실행계획이 접수되면 EBDS가 1개월 내에 의견을 제시해야 하며, EC는 이 의견을 접수한 후 1개월 이내에 승인 여부를 최종 결정한다.

▪ **이행강제금(Periodic penalty payments): 제76조**

불이행결정이나 이행약정 등이 이행되지 않는 경우 EC는 이행을 강제하기 위해 반복적으로 벌금을 부과할 수 있다. 최대 벌금 규모는 직전 회계연도 기준 전세계 연간 매출액 또는 수입을 기준으로 한 평균 일일 매출액(또는 수입)의 5%에 해당하는 금액이다.

나. 시스템적 위험별 주요 집행 현황

EC는 VLOP와 VLOSE에 대하여 이루어지고 있는 모든 집행 조치와 진행 상황을 공개하고 있다.⁵⁴⁾ 각 플랫폼별로 지정된 날짜부터 시작하여 어떠한 혐의로 공식 절차가 개시되었는지, 지금까지 어떤 내용의 정보요청(RFI)이 발송되었는지, 최종 제재 결정이나 이행약정이 어떻게 확정되었는지 등 모든 이력과 공식 보도자료의 링크를 볼 수 있다.⁵⁵⁾ 이하에서는

54) European Commission. Supervision of the designated very large online platforms and search engines under DSA.

55) 시민사회 등 제3자가 별도의 사이트를 구축하여 EC의 DSA 집행 현황을 제공하기도 한다. 예를 들어,

주요 시스템적 위험별로 2026년 7월 현재까지 EC의 집행 현황을 정리하였다. 각 사례에는 시스템적 위험과 직접 관련되지 않은 위반 사항도 포함되어 있다.

1) 미성년자 보호, 정신적·신체적 웰빙

미성년자 보호 및 정신적, 신체적 웰빙과 관련된 위험은 가장 많은 공식 절차가 개시된 영역이다. 무한스크롤, 자동재생 등 중독성 설계와 연령확인 시스템의 문제 등이 지적되고 있다.

틱톡(TikTok)

EC는 틱톡에 대해 2024년 2월 19일에 1차 공식절차를 개시했다.⁵⁶⁾ 미성년자 보호, 광고 투명성, 연구자의 데이터 접근, 중독성 설계 및 유해 콘텐츠의 위험 관리와 관련된 이슈들이 쟁점이 되었다.

이와 별개로 2024년 4월 22일에는 틱톡 라이트(TikTok Lite) 출시와 관련하여 두 번째 공식 절차가 개시되었다.⁵⁷⁾ EC는 틱톡 라이트의 “작업 및 보상 프로그램(Task and Reward Program)”이 특히 플랫폼의 중독성과 관련된 위험에 대한 충분한 사전 평가와 효과적인 위험 완화조치 없이 출시되었다는 점에 우려를 표명했다. 또한 EC는 틱톡에 안전성 평가가 완료될 때까지 EU 내에서 틱톡 라이트 보상 프로그램을 일시적으로 중단하는 잠정 조치를 부과할 의사를 통보했다. 같은 해 8월 5일에 틱톡은 이

The Future of Free Speech (FoFS) – DSA Enforcement Tracker:

<<https://futurefreespeech.org/tracker-of-dsa-enforcement/>>.

SocialMediaTransparency.org – DSA Enforcement Tracker:

<<https://socialmediatransparency.org/dsa-tracker>>

Tremau – DSA Database: <<http://tremau.com/resources/dsa-database>>.

56) European Commission. (2024, 2, 19).

57) European Commission. (2024, 4, 22).

프로그램을 EU 내에서 영구적으로 철수하고, 이를 우회하는 다른 프로그램을 시작하지 않겠다는 이행약정을 제출했다. 이는 EC가 DSA에 따라 공식 절차를 개시한 온라인 플랫폼으로부터 이행약정을 수락한 첫 번째 사례이다.⁵⁸⁾

2년간의 조사 끝에 2026년 2월 6일, EC는 틱톡이 중독성 설계, 특히 무한 스크롤, 자동재생, 푸시 알림, 고도로 개인화된 추천시스템 등의 기능으로 인해 DSA를 위반했을 가능성이 있다는 예비판단을 내렸다.⁵⁹⁾ EC는 틱톡이 이러한 중독적 기능이 미성년자 및 취약한 성인을 포함한 이용자들의 신체적, 정신적 건강에 미칠 수 있는 해로운 영향을 제대로 평가하지 않았다고 보았다. EC는 “틱톡은 새로운 콘텐츠로 이용자들에게 지속적으로 ‘보상’을 제공함으로써 계속 화면을 내리게 만드는 충동을 부추기고 이용자의 뇌를 ‘자동 조종 모드(autopilot mode)’로 전환시킨다”고 비판하며, 과학적 연구에 따르면 이는 강박적 행동으로 이어지고 이용자의 자제력을 저하시킬 수 있다고 지적했다. 또한 EC는 틱톡이 위험평가 과정에서 미성년자가 밤에 틱톡을 이용하는 시간, 이용자가 앱을 여는 빈도 및 기타 앱의 강박적 이용을 나타내는 중요한 잠재적 지표들을 간과했으며, 이러한 위험을 완화하기 위한 합리적, 비례적, 효과적인 조치를 시행하는 데도 실패했다고 지적했다. EC는 스크린타임 관리도구와 자녀 보호 도구 등 현재 틱톡이 시행하고 있는 조치들이 효과적이지 못하다고 판단했다. 이러한 문제를 해결하기 위해 EC는 틱톡이 서비스의 기본 설계를 변경해야 한다고 보았는데, 예를 들어 ‘무한 스크롤’과 같은 주요 중독성 기능을 일정 시간 후에 비활성화하고, 야간을 포함하여 효과적인 ‘화면 이용시간 단축’ 조치를 시행하며, 추천시스템을 개선할 필요가 있다고 보았다. 한편, 연구자의 데이터 접근에 대한 예비판단은 2025년 10월에 채택되었고,⁶⁰⁾ 광고

58) European Commission. (2024, 8, 5).

59) European Commission. (2026, 2, 6).

투명성에 관한 사안은 이행약정을 통해 2025년 12월에 마무리되었다.

이어 EC는 2026년 7월 24일, 틱톡의 미성년자 계정이 DSA의 안전 기준을 충족하지 못한다며 다시 예비판단을 내렸다.⁶¹⁾ 틱톡에서는 미성년자 계정도 ‘공개’로 설정할 수 있어, 틱톡 계정이 없는 이용자를 포함한 모든 이용자가 미성년자의 콘텐츠를 볼 수 있으며, 이 설정을 통해 16~17세 미성년자의 콘텐츠가 ‘추천 피드’를 통해 다른 틱톡 이용자에게 추천될 수 있다. EC는 이러한 노출이 잠재적 가해자로부터 원치 않는 접촉을 초래할 수 있으며, 콘텐츠가 사이버 괴롭힘에 악용될 위험을 내포하고 있다고 보았다. 또한 미성년자가 게시한 콘텐츠가 온라인에 영구적으로 남아 평생에 걸쳐 부정적인 결과를 초래할 위험도 있다. 미성년자가 비공개 계정을 선택하더라도 다른 이용자의 ‘팔로잉’ 및 ‘팔로워’ 목록을 통해 계정을 쉽게 찾을 수 있으며, 프로필 사진은 틱톡 계정이 없는 이용자를 포함한 누구에게나 공개되어 원치 않는 접촉 등의 위험에 노출될 수 있다. EC는 틱톡이 미성년자의 ‘공개’ 계정 기본 설정을 조정하여 해당 미성년자가 수락한 틱톡 이용자에게만 콘텐츠가 기본적으로 표시되도록 해야 한다고 잠정적으로 판단했다.

2026년 2월 6일의 예비판단 직후, 틱톡은 이에 대해 강력하게 반발했다. 틱톡 대변인은 예비판단이 플랫폼에 대해 “전면적으로 허위이며 전혀 근거 없는 묘사를 하고 있다”며, “가용한 모든 수단을 동원해 이 조사 결과에 이의를 제기하기 위해 필요한 모든 조치를 취할 것”이라고 밝혔다.⁶²⁾ 2026년 7월 현재 예비판단 이후 최종 결정은 아직 나오지 않은 상황이며, 틱톡이 예비판단에 대해 제79조에 따른 의견진술을 하고 있는 것으로 보인다. 2025년 12월 5일 내려진 X에 대한 최종 결정이 2024년 7월 12일

60) European Commission. (2025, 10, 24).

61) European Commission. (2026, 7, 24).

62) Daher, N. (2026, February 9).

의 예비판단 이후 거의 17개월이 소요된 점을 고려해 보면, 틱톡에 대한 최종 결정도 수개월 이상 상당한 시간이 소요될 것으로 보인다.⁶³⁾ 유럽의 회조사처(EPRS)는 “이번 조치는 불법 콘텐츠, 데이터 보호 또는 경쟁 문제가 아닌, 특히 미성년자와 취약한 성인에게 유해한 플랫폼 구조 자체에 초점을 맞춘 최초의 사례”라고 의미를 부여했다.⁶⁴⁾

메타(Meta)

2024년 5월 16일, EC는 페이스북과 인스타그램의 알고리즘이 아동의 행동 중독을 촉발하고 특정 콘텐츠에서 벗어나지 못하는 소위 ‘토끼굴 효과’를 초래할 수 있다고 우려하며, 메타를 상대로 공식절차를 개시했다. EC는 메타가 도입한 연령 확인 및 검증 방식에 대해서도 우려를 제기했다.⁶⁵⁾

2026년 4월 29일, EC는 약 2년의 조사 끝에 메타의 인스타그램과 페이스북이 13세 미만 미성년자의 서비스 접근 위험을 성실히 파악, 평가 및 완화하지 못해 DSA를 위반하였다는 예비판단을 내렸다.⁶⁶⁾ 메타는 이용약관에서 최소 연령을 13세로 정하고 있지만, 13세 미만의 아동이 계정을 만들 때 허위의 생년월일을 입력할 수 있었던 반면, 생년월일의 정확성을 확인할 수 있는 효과적인 통제 장치는 마련되어 있지 않았다. 또한 메타 플랫폼에서 13세 미만 아동을 신고하는 기능이 사용하기 어렵고 효과적이지 않았으며, 신고가 이루어지더라도 적절한 후속조치가 이루어지지 않는 경우가 많았다. 메타는 13세 미만 아동이 인스타그램과 페이스북에 접속해 부적절한 콘텐츠에 노출될 위험을 제대로 파악하지 못하는 등 위험평가가 불완전했다. EC는 메타가 위험평가 방법론을 변경하고, 13세 미만 아동의

63) Slaughter and May. (2026, March 6).

64) Negreiro, M., & Anaç, Ö. D. (2026, May 6).

65) European Commission. (2024, 5, 16).

66) European Commission. (2026, 4, 29).

서비스 이용을 예방, 감지 및 차단하는 조치를 강화해야 한다고 보았다.

2026년 7월 10일, EC는 틱톡과 마찬가지로 메타에 대해서도 중독성 설계가 DSA를 위반하였다고 예비판단을 내렸다.⁶⁷⁾ 메타는 중독성 설계가 미성년자 및 취약한 성인을 포함한 이용자들의 신체적, 정신적 건강에 미치는 위험성을 제대로 평가하지 않았다. EC는 인스타그램과 페이스북의 고도로 개인화된 추천, 자동 재생, 무한 스크롤과 같은 설계 특징이 이용자의 뇌를 ‘자동 조종 모드’로 전환시켜 강박적 이용으로 이어질 수 있다는 점을 메타가 위험평가 과정에서 충분히 고려하지 않았다고 지적했는데, 이러한 표현은 2026년 2월 6일에 틱톡에 대한 예비판단과 거의 유사하다. 또한 EC는 메타의 현재 완화조치가 중독성 설계에서 비롯되는 위험을 효과적으로 해결하지 못했다고 판단했다.

스냅챗(Snapchat)

2026년 3월 26일, EC는 스냅챗에 대해 공식절차를 개시했다.⁶⁸⁾ 스냅챗 이용약관은 이용자의 연령을 만 13세 이상으로 규정하고 있지만, 연령 확인이 이용자의 자가 신고에만 의존하고 있어 불충분하다고 판단했다. 또한 스냅챗이 성적 착취나 범죄 활동 모집처럼 유해한 의도를 가진 이용자들의 접촉으로부터 미성년자를 적절히 보호하지 못하고 있으며, 기본 설정 역시 미성년자의 개인정보 보호, 안전 및 보안을 충분히 보장하지 못하고 있다고 의심했다. 또한 스냅챗이 마약, 전자담배, 주류 등 불법 또는 연령 제한 품목의 판매에 관한 정보의 유통을 통제하는데 효과적이지 않으며, 불법 콘텐츠 신고 시스템의 접근성도 떨어지고 다크패턴을 사용하고 있을 가능성도 있다고 보았다.

67) European Commission. (2026, 7, 10).

68) European Commission. (2026, 3, 26a).

성인 콘텐츠

2025년 5월 27일, EC는 Pornhub, Stripchat, XNXX, XVideos 등 4개의 성인 콘텐츠 VLOP를 대상으로 공식절차를 개시했다.⁶⁹⁾ 미성년자의 접근을 제한하기 위한 효과적인 연령확인 도구, 아동의 권리, 이용자의 정신적 및 신체적 건강에 미치는 부정적인 영향에 대한 위험평가와 완화조치 등이 조사 대상에 포함되었다. 이후 Stripchat은 VLOP에서 지정 해제되었다. 이에 대한 예비판단은 2026년 3월 26일에 나왔다.⁷⁰⁾ EC는 이들 사이트들이 위험평가를 성실히 수행하지 않았으며, 미성년자의 서비스 접근을 막기 위한 실효성 있는 조치를 이행하지 못했다고 판단했다. 이들 사이트는 성인 전용 사이트이지만, 만 18세 이상임을 확인하는 단순 클릭만으로 미성년자가 플랫폼에 접속할 수 있도록 허용하고 있다. EC는 이러한 ‘자기선언(self-declaration)’ 방식이 실효성 있는 조치가 아니며, 이들 플랫폼 전반에 걸쳐 도입된 페이지 블러 처리, 콘텐츠 경고, ‘성인 전용’ 표지 등의 추가적인 완화조치 역시 미성년자 접근을 제한하는 데 효과적이지 않다고 판단했다.

2) 불법 콘텐츠 유포

불법 콘텐츠 확산 위험과 관련해서는 주로 전자상거래 플랫폼들이 집행 대상이 되었다.

알리익스프레스(AliExpress)

EC는 2024년 3월 14일, 알리익스프레스에 대해 공식절차를 개시했는데, 불법 콘텐츠 유포의 시스템적 위험평가 및 완화, 신고 및 조치

69) European Commission. (2025, 5, 27).

70) European Commission. (2026, 3, 26b).

(notice-and-action), 내부 이의제기 메커니즘, 광고 및 추천시스템의 투명성, 판매자 추적성, 연구자의 데이터 접근 의무 위반이 쟁점이었다.⁷¹⁾ 1년여의 조사 끝에 EC는 알리익스프레스가 불법상품 유통과 관련된 위험을 평가하고 완화해야 할 의무를 위반했다는 예비판단을 내렸다. 다른 쟁점에 대해서는 알리익스프레스의 이행약정을 수용했다.⁷²⁾ 이행약정을 통해 숨겨진 링크와 제휴 프로그램을 통한 불법상품 확산, 신고 및 조치 메커니즘, 내부 이의제기 시스템, 광고 및 추천시스템 투명성(광고 저장소와 추천시스템 개인화 옵션 포함), 판매자 추적성, 연구자를 위한 공공 데이터 접근과 관련된 우려 사항을 해소하기로 했다.

2026년 7월 20일, EC는 알리익스프레스가 불법상품 판매와 관련된 위험을 성실히 평가하고 완화해야 할 의무를 위반한 것을 이유로 5억 5천만 유로의 과징금을 부과하고 시정조치를 명령했다.⁷³⁾ 이는 DSA 시행 이후 최대 규모의 과징금이다. EC는 알리익스프레스가 잠재적 불법 제품을 검토할 충분한 인력이 있는지 제대로 평가하지 못했고, 자사의 추천 및 광고 시스템이 불법 제품 확산에 미치는 영향을 제대로 평가하지 못했으며, 평가에 정량적 지표가 부족했다고 판단했다. 완화조치에 있어서도 불법상품 탐지 시스템이 제대로 작동하지 않았고, 불법상품 판매자에 대한 제재 정책이 제대로 시행되지 않았으며, 제품 규정 준수 검사는 제품 분류 오류를 통해 쉽게 우회될 수 있었고, 위조품 확산을 효과적으로 막지 못하는 등 여러 가지로 미흡했다고 지적했다. 알리익스프레스는 2026년 10월 20일까지 EC에 개선 계획을 제출해야 한다.

71) European Commission. (2024, 3, 14).

72) European Commission. (2025, 6, 18).

73) European Commission. (2026, 7, 20).

테무(Temu)

2024년 10월 31일, EC는 테무가 불법 제품 판매, 서비스의 중독성 설계, 이용자에게 구매를 추천하는 데 사용되는 시스템, 그리고 연구자를 위한 데이터 접근과 관련된 영역에서 DSA를 위반했는지 평가하기 위한 공식절차를 개시했다.⁷⁴⁾ 그리고 2025년 7월 28일, 불법 제품이 유통될 위험을 성실히 평가해야 할 의무를 위반했다는 예비판단을 내렸다.⁷⁵⁾ 다만, 완화 조치의 효과성, 중독성 있는 설계 기능의 사용, 추천시스템의 투명성, 연구자를 위한 데이터 접근성 등 다른 의혹에 대해서는 계속 조사를 진행할 예정이라고 밝혔다.

2026년 5월 28일, EC는 테무가 불법 제품 유통 위험에 대해 성실히 평가할 의무를 위반한 데 대해 2억 유로의 과징금을 부과했다.⁷⁶⁾ 테무는 위험 평가에서 자체 서비스에 관한 구체적인 증거가 아니라 전자상거래 부문 전체에 대한 일반 정보에 기반하여 평가하였고, EU 소비자들이 불법상품을 접할 가능성을 과소평가했다. 조사 과정에서 EC는 일반 소비자로서 가장하여 구매 테스트를 하는 ‘미스터리 쇼핑 기법’을 사용했다. 그 결과, 충전기 중 상당수가 기본적인 안전 테스트를 통과하지 못했으며, 테스트 대상 유아용 장난감 중 상당수는 법적 안전 기준치를 초과하는 화학물질을 함유하였거나 분리되는 부품으로 인해 질식 위험을 초래하는 등 중상급 수준의 안전 위험을 내포하는 것으로 나타났다. 또한 추천시스템과 제휴 인플루언서를 활용한 제품 홍보 프로그램 등 자사 서비스의 설계가 불법 제품 확산 위험을 어떻게 증폭시킬 수 있는지 제대로 평가하지 못했다. 테무는 2026년 8월 28일까지 시정 실행계획을 제출해야 한다.

74) European Commission. (2024, 10, 31).

75) European Commission. (2025, 7, 28).

76) European Commission. (2026, 5, 28).

쉬인(Shein)

2026년 2월 17일, EC는 중독성 설계, 추천시스템의 투명성 부족, 아동 성착취물 등의 불법상품 판매를 이유로 쉬인에 대한 공식절차에 들어갔다.⁷⁷⁾ 아동 모양의 섹스 인형 등 아동 성착취물로 간주될 수 있는 콘텐츠를 비롯해 불법상품 판매를 제한하기 위한 시스템, 서비스 이용에 따른 포인트나 보상 제공 등 중독성 있는 설계와 관련된 위험 및 완화조치, 추천시스템의 투명성 등이 조사 대상이다. 쉬인이 설립된 국가인 아일랜드 DSC인 CNAM도 조사에 참여한다.

3) 시민 담론, 선거 절차, 공공안보 위험

X (구 Twitter)

2023년 12월 18일, EC는 X사가 위험 관리, 콘텐츠 조정, 광고 투명성 및 연구자를 위한 데이터 접근과 관련된 영역에서 DSA를 위반했는지 평가하기 위한 공식절차를 개시했다.⁷⁸⁾ 이스라엘에 대한 하마스의 공격 시점에 불법 콘텐츠가 확산된 것이 조사의 계기가 되었다. 2024년 7월 12일, EC는 X사가 다크패턴, 광고 투명성 및 연구자의 데이터 접근과 관련된 영역에서 DSA를 위반했을 가능성이 있다는 예비판단을 내렸다.⁷⁹⁾ 그러나 시스템적 위험과 관련된 불법 콘텐츠 및 정보조작 대응에 관한 조사는 예비판단에 포함되지 않았고, 계속 진행 중이다.

2025년 12월 5일, EC는 예비판단 사안에 대해 DSA 위반 결정을 내리고 1억 2천만 유로의 과징금을 부과하였다.⁸⁰⁾ 이는 DSA에 따른 첫 번째 규

77) European Commission. (2026, 2, 17).

78) European Commission. (2023, 12, 18).

79) European Commission. (2024, 7, 12).

정 위반 결정이었다. EC는 X 플랫폼이 ‘인증된 계정’에 ‘파란색 체크 표시’를 사용하는 것을 이용자 기만 행위로 보았다. X 플랫폼에서는 누구나 비용을 지불하고 ‘인증됨’ 상태를 얻을 수 있지만, 회사는 계정 소유자가 누구인지 실질적으로 검증하지 않기 때문이다. 따라서 마치 인증된 계정인 것처럼 표시하는 것은 이용자 기만행위이며, 이는 이용자를 사기나 악의적 행위자의 조작에 노출시킬 위험이 있다. 또한 EC는 X의 광고 저장소가 DSA의 투명성 및 접근성 요건을 충족시키지 못한다고 판단했다. X사는 연구자에게 플랫폼의 공개 데이터에 대한 접근 권한을 제공해야 하는 의무도 이행하지 못했다. 예를 들어, X사의 약관은 연구자들이 스크래핑을 포함한 어떤 방식으로든 공개 데이터에 독립적으로 접근하는 것을 금지하고 있으며, X사의 공개 데이터 접근 절차에 불필요한 장벽을 두고 있었다.

X사는 DSA 위반 사항을 시정하기 위한 실행계획을 제출했고, EC는 이를 승인했다.⁸⁰⁾ 실행계획에서 X사는 검색 기능 개선 및 응답 속도 향상 등 광고 데이터베이스의 개선, 더 많은 광고 관련 데이터의 공개와 API를 통한 접근의 제공, 적격 연구자에게 무료로 신속한 데이터 접근을 제공할 수 있도록 심사절차의 간소화, 공개데이터 스크래핑을 계약상 금지하던 조항의 삭제, 이러한 변경 사항에 대하여 독립 감사가 평가하고 그 결과를 위원회에 제출할 것 등을 약속하였다. EBDS는 6월 15일 제시한 의견에서 X의 실행계획이 불충분하다고 판단했지만, EC는 X가 실행계획을 이행하는 과정에서 고려해야 할 사항 몇 가지를 명확히 한 후에 승인하였다.

그런데 이와 동시에 X는 2025년 12월 5일, 과징금 부과 결정에 대해 적법절차의 권리가 침해되었다고 주장하며 EU 일반법원에 소를 제기했다. 이는 DSA 과징금에 대한 최초의 사법심사 사건이다. X사는 국제자유수호

80) European Commission. (2025, 12, 5).

81) European Commission. (2026, 7, 16).

연맹(Alliance Defending Freedom International)이라는 단체의 지원을 받고 있는데, 이들은 X가 전면적인 온라인 검열을 시행하지 않기 때문에 표적이 되고 있다고 본다.⁸²⁾ 이 단체는 표현의 자유를 내세우는 기독교 법률 옹호단체이다.⁸³⁾ 반면 EDRi 등 유럽의 디지털 권리 단체들은 EC의 과징금 결정을 환영하고 있다. EDRi는 이번 결정이 검열에 관한 것이 아니라 투명성과 소비자 공정성에 관한 것이라고 본다.⁸⁴⁾

메타

2024년 4월 30일, EC는 메타를 상대로 공식절차를 개시하였다.⁸⁵⁾ 유럽 의회 선거를 앞두고, 서비스 내 기만적인 광고 및 정치 콘텐츠와 관련된 정책과 관행, 메타가 적절한 대체 도구 없이 실시간 여론 분석 도구인 ‘클라우드탱글(CrowdTangle)’ 서비스를 중단한 상황에서 실시간 시민 담론 및 선거 모니터링 도구의 부재, 불법 콘텐츠 신고 메커니즘 등이 DSA를 위반했는지 여부가 쟁점이었다. 클라우드탱글은 연구자, 언론인, 시민사회 단체가 실시간 시각 대시보드를 통해 선거를 감시할 수 있도록 지원하는 공개 분석 도구인데, 메타는 이 서비스의 종료를 추진하고 있었다. EC는 2024년 6월 유럽의회 선거와 여러 회원국 선거를 고려할 때, 이 서비스의 중단이 오정보 및 허위조작정보의 추적, 유권자 개입 및 투표 방해 행위의 식별, 그리고 팩트체크 담당자, 언론인 및 기타 관련 선거 이해관계자에게 제공되는 실시간 투명성 측면에서 시민 담론과 선거 과정에 피해를 줄 수 있다고 우려하였다. 공식절차 개시 이후 2026년 7월 현재 EC의 후속 조치는 아직 없는 상황이다.

82) Alliance Defending Freedom International. (2026, February 20).

83) <<https://adfinternational.org/about-us/>>.

84) EDRi. (2025, December 8).

85) European Commission. (2024, 4, 30).

틱톡

2024년 12월 17일, EC는 선거 위험성과 관련하여 틱톡에 대한 공식절차를 개시했다.⁸⁶⁾ 틱톡이 2024년 11월 24일에 실시된 루마니아 대선과 관련하여 선거의 공정성과 연관된 시스템적 위험을 적절히 평가하고 완화해야 할 의무를 제대로 이행하지 않았다는 의혹에 대해 DSA 위반 여부를 조사하기 위한 것이었다. EC는 이 조사에서 틱톡의 추천시스템과 틱톡의 정치 광고 및 유료 정치 콘텐츠 관련 정책이 선거 또는 시민 담론에 미치는 위험 관리 문제를 다룰 것이라고 밝혔다. 만일 EC의 의심이 사실로 입증된다면, 이는 DSA 제34조 제1항, 제34조 제2항 및 제35조 제1항 위반에 해당하게 된다. 아일랜드 DSC인 CNAM도 이 조사에 참여한다. 공식절차 개시 이후 2026년 7월 현재까지 EC의 후속 조치는 없는 상황이다.

4) 젠더기반폭력

X (구 Twitter)

2026년 1월 26일, EC는 X사가 EU 내 X 시스템에 Grok 기능을 배포하는 과정에서 위험을 적절히 평가하고 완화했는지를 조사하는 공식절차를 개시했다.⁸⁷⁾ 더불어 2023년 12월에 시작된 X사의 추천시스템에 대한 기존 조사도 확대하겠다고 밝혔다. 생성형 AI인 Grok과 관련한 위험은 조작된 성적 이미지, 아동 성학대 자료에 해당할 수 있는 콘텐츠 등 EU 내 불법 콘텐츠의 유포와 관련된 위험이 포함된다. CNAM도 설립국가의 DSC로서 이 조사에 참여한다.

86) European Commission. (2024, 12, 17).

87) European Commission. (2026, 1, 26).

다. DSA 집행 현황에 대한 분석

1) 집행 조치를 통해 자율적 위험평가의 실효성 촉진

2024년 2월 19일, 틱톡에 대한 EC의 공식절차 개시 보도자료를 보면, “지금까지 진행된 예비 조사, 특히 2023년 9월 틱톡이 제출한 위험평가 보고서 분석 및 불법 콘텐츠, 미성년자 보호, 데이터 접근과 관련하여 틱톡이 위원회의 공식 정보 요청에 답변한 내용을 바탕으로, 위원회는 틱톡에 대한 공식절차를 개시하기로 결정했다”라고 언급하고 있다. 비단 틱톡에 대해서만이 아니라, EC는 공식절차 개시 단계에서 거의 예외 없이 “OO년 O월에 제출된 위험평가 보고서 분석에 기초해”라는 문구를 사용한다. 즉, 플랫폼이 제출한 위험평가 보고서가 해당 플랫폼에 대한 가장 기본적인 조사자료라는 점을 알 수 있다. 플랫폼의 내부 시스템과 정책에 대한 설명을 담고 있기 때문에 조사의 쟁점과 방향을 제시해주는 출발점이 될 수 있는 것이다.

나아가 EC는 위험평가 보고서를 “자율적인 평가가 불충분했다”고 지적하는 근거로도 활용하고 있다. 예를 들어, 틱톡에 대한 예비판단에서 EC는 “틱톡은 평가 과정에서 미성년자가 밤에 틱톡을 이용하는 시간, 이용자가 앱을 여는 빈도 및 기타 잠재적 지표와 같은 앱의 강박적 이용을 나타내는 중요한 지표들을 간과했다”고 지적했다. 메타에 대해서도 EC는 “위험평가 방법론 자체를 바꿔야 한다”고 권고했다. 즉, 자율적인 위험평가 보고서의 허점이 곧 위반의 증거가 될 수 있는 것이다. 테무에 대한 DSA 위반 결정과 관련하여, 헤나 비르쿠넨 EC 기술 주권, 보안 및 민주주의 담당 부위원장은 “위험평가는 형식적인 절차가 아니라 DSA의 핵심이다. 테무의 위험평가는 구체적인 위험을 과소평가하고, 구체성이 부족하며, 확실한 증거에 기반하지 않았고, 포괄적이지 않았다”고 말했다.⁸⁸⁾ 이처럼 DSA

집행에서 위험평가의 진정성을 따지는 것은 플랫폼의 자율적인 위험평가가 성실하게 이루어질 수 있도록 촉진하는 요인이 될 수 있다.

2) 집행 대상 이슈 및 소요기간

아래 표에서 볼 수 있는 바와 같이, DSA 위반 혐의로 조사에 들어간 이슈는 광고 투명성, 연구자에 대한 데이터 접근, 중독성 설계, 미성년자 연령 확인, 추천시스템 위험(토끼굴 효과), 불법상품 확산의 시스템적 위험 등 매우 다양하다. 여러 이슈가 한 번에 공식절차에 포함되더라도, 조사가 먼저 완료된 쟁점에 대해서는 예비판단과 최종 결정이 내려지고 있다.

공식절차 개시로부터 예비판단까지 소요된 기간을 보면, 미성년자 연령확인, 불법상품 확산의 시스템적 위험, 광고 투명성, 연구자 데이터접근 등의 이슈에 대해서는 1년 내외의 기간이 소요된 반면, 중독성 설계와 관련된 쟁점은 2년 이상 소요되었고, 추천시스템의 위험이나 시민 담론 및 선거절차와 관련된 조사는 아직 예비판결이 나오지 않은 상황이다. 상대적으로 판단이 용이한지 여부에 따라 조사에 소요되는 시간이 달라지는 것은 당연하다. 주제 측면에서도 초기에는 상대적으로 판단이 용이하다고 볼 수 있는 미성년자 보호와 전자상거래 분야에 초점을 맞추다가 점차 소셜미디어 분야로 확대되어 가는 것을 볼 수 있다.

과징금 규모는 첫 번째 대상이었던 X가 1억 2,000만 유로, 테무가 2억 유로, 알리익스프레스가 5억 5000만 유로로 순차적으로 증가하고 있다. 사안의 중대성에 따라 달라지기도 하겠지만, DSA 제도의 시행 초기라는 점을 감안하여 낮게 책정한 측면도 있을 것이다. 향후 다른 플랫폼이라도 유사한 위반이 반복되면 과징금 규모가 더 커질 가능성이 있다.

【표 2】플랫폼별 집행 절차 일자 및 쟁점

플랫폼	쟁점	공식절차 개시	예비판단	결정
X	다크패턴, 광고투명성, 연구자 데이터접근	2023.12.18.	2024.7.12.	2025.12.5.
틱톡	광고투명성	2024.2.19.	2025.12.5. (이행약정)	
틱톡	연구자 데이터접근	2024.2.19.	2025.10.24.	
틱톡	중독성 설계	2024.2.19.	2026.2.6.	
틱톡	미성년자 계정 안전	2024.2.19.	2026.7.24.	
틱톡 라이트	사전위험평가 누락	2024.4.22.	2024.8.5. (이행약정)	
메타	13세 미만 접근 방지(연령확인)	2024.5.16.	2026.4.29.	
메타	중독성 설계	2024.5.16.	2026.7.10.	
메타	연구자 데이터접근	2024.5.16.	2025.10.24.	
알리익스프레스	불법상품 확산 시스템적 위험	2024.3.14.	2025.6.18.	2026.7.20.
알리익스프레스	통지조치,이의제기,광고추천투명성,판매자추적성,연구자접근	2024.3.14.	2025.6.18. (이행약정)	
테무	불법상품 확산 시스템적 위험	2024.10.31.	2025.7.28.	2026.5.28.
성인 사이트들	미성년자 연령확인 미비	2025.5.27.	2026.3.26.	

【표 3】 아직 예비판단이 없는 플랫폼별 쟁점

플랫폼	쟁점	공식절차 개시	비고
X	불법콘텐츠 확산, 정보조작 대응	2023.12.18.	2025.12. 결정에서 제외되고 별도 진행
X	생성형AI 딥페이크, 아동성착취물 위험, 추천시스템 확대조사	2026.1.26.	
틱톡	유해콘텐츠 위험관리 (추천시스템)	2024.2.19.	
메타	추천시스템의 토끼굴 효과	2024.5.16.	
메타	기만적 광고, 정치콘텐츠, CrowdTangle 대체도구 부재	2024.4.30.	
테무	중독성 설계, 추천시스템 투명성, 연구자 데이터접근	2024.10.31.	2026.5.28. 불이행결정에서 제외, 별도 진행
쉬인	불법상품, 중독성 설계, 추천투명성	2026.2.17.	
틱톡	루마니아 선거개입 의혹, 추천시스템 조작	2024.12.17.	
스냅챗	그루밍, 불법상품 노출, 연령확인 미비	2026.3.26.	

3) 이행약정을 통한 빠른 집행

공식절차 개시를 통해 심층 조사가 시작된 이슈 중 일부에 대해서는 플랫폼이 이행약정을 제안하고 EC가 이를 수용하면서 절차가 마무리되었다. 틱톡은 틱톡 라이트에 대해 2024년 4월 22일 공식절차가 개시되자마자, 같은 해 8월 5일 서비스를 철회하는 것으로 이행약정을 하였고, 2025년 12월에는 광고 투명성 조치에 대해 이행약정을 하였다. 알리익스프레스는 결국 불법상품 확산의 시스템적 위험에 대해서 DSA 위반 제재를 받았지만, 같은 날 공식절차가 개시된 다른 이슈들에 대해서는 이행약정을 제안하여 절차를 마무리했다. EC의 입장에서 이행약정은 플랫폼이 DSA 규정을 준수하도록 간편하게 유도하는 수단이 된다. 플랫폼 입장에서는 규정 위반 결정을 받지 않고 집행절차를 끝낼 수 있는 방법이기도 하지만, 불법상품 확산의 시스템적 위험이나 중독성 설계 등은 해당 플랫폼의 핵심적인 수익 모델을 변경해야 하기 때문에 이행약정 절차를 채택하지 않은 것으로 보인다. 그러나 핵심 수익 모델이 아닌 부수적인 정책과 관련해서는 이행약정 제도가 빠른 결과를 이끌어내는 역할을 하는 측면이 있다.

4) 불법정보 규제에서 중독성 설계 규제로의 전환

플랫폼의 자율적인 위험평가에서는 서비스 설계에서 비롯되는 위험에 대해서 제대로 분석하지 않았다. 그럼에도 불구하고 EC가 무한 스크롤, 자동 재생, 푸시 알림, 고도로 개인화된 추천시스템 등 중독성 설계에 대해 DSA 위반으로 예비판단을 내리고 있다는 사실이 주목할 만하다. 이는 플랫폼의 핵심적인 수익 모델과 관련된 조치이기 때문이다. 2026년 2월 6일에 틱톡의 중독성 설계에 대해 첫 예비판단이 있었고, 7월 10일에는 메타에 대해서도 유사한 판단이 내려졌다. 정부의 감독 권한을 통해 시스템의 재설계를 이끌어낼 수 있을지 최종 결정을 지켜볼 필요가 있다.

5) 집행에 있어서 지정학적 영향

2025년까지 주로 틱톡이나 중국의 전자상거래 사이트들이 DSA의 제재 대상이 되었다. 그런데 최근 DSA 집행이 X, 메타와 같은 미국 기반 빅테크로까지 확대되면서 미국과 유럽 사이의 지정학적 긴장이 높아지고 있다. 특히 미국에서 트럼프 대통령이 재선된 이후, X와 메타 등 빅테크 기업들은 노골적으로 기업 정책을 변경하였다. 메타 CEO인 저커버그는 2025년, 페이스북에 동영상⁸⁹⁾을 올려 트럼프에 대한 지지를 표명하며 “우리는 트럼프 대통령과 협력하여 전 세계 정부에 맞설 것입니다. 그들은 미국 기업들을 공격하고 더 많은 검열을 강요하고 있습니다”라고 말했다. 또한 미국 내 팩트체커를 없애고 커뮤니티 노트로 대체하겠다고 밝혔으며, 기존의 LGBTQ 커뮤니티 보호 규칙도 폐지하는 조치를 취했다. 미국 부통령 JD 밴스는 2025년 원헬안보회의 연설에서 “유럽이 가장 근본적인 가치들로부터 후퇴하고 있다”고 경고했다. 2025년에 나온 미 하원 직원 보고서에 DSA가 검열을 하고 표현의 자유를 침해한다고 비판했다.⁹⁰⁾ 이러한 정세 속에서 2025년 말까지 X에 대한 제재가 지연되자, 미국의 정치적인 압력으로 DSA 집행이 미뤄지거나 아예 폐기되는 것이 아닌지에 대한 우려도 불거졌다.⁹¹⁾

다행히 EC는 X에 대해 과징금을 부과했고, 틱톡과 메타의 중독성 설계에 대해서도 DSA 위반 예비판결을 내렸다. 그러나 X는 이에 대해 소송을 제기했으며, 다른 기업들도 유사한 대응을 할 것으로 예상된다. 미국의 압력이 DSA 집행에 향후 어떠한 영향을 미칠지 주시할 필요가 있다.

89) <<https://www.facebook.com/watch/?v=1525382954801931&vanity=zuck>>.

90) Committee on the Judiciary, U.S. House of Representatives. (2025, July 25).

91) Józwiak, M. (2025, November 26).

5/ 한국에 대한 시사점

가. ‘개별 콘텐츠 규제’에서 ‘시스템적 위험 규제’로 패러다임 전환의 필요성

2026년 7월 시행된 개정 정보통신망법은 EU DSA의 신고 및 조치(notice-and-action) 제도를 부분적으로 도입하였다⁹²⁾. 그러나 신고 및 조치 제도가 한국과 유럽에서 갖는 의미는 상당히 다르다. 유럽에서는 신고 및 조치 제도, 그리고 이어지는 이의신청, 분쟁조정 제도가 플랫폼의 자율규제로서 불법정보 처리를 위한 기본 메커니즘이다. 반면, 한국에서는 여전히 방송미디어통신심의위원회를 통한 행정심 의가 불법정보 처리를 위한 기본 메커니즘이다. 이러한 상황에서 정보통신서비스제공자가 이용자의 신고를 받고 처리하는 관행이 부분적으로 존재하는데, 신고 및 조치 제도는 이러한 관행을 공식화한 측면이 있다. 따라서 개정 정보통신망법이 기존의 내용 규제 체제에 변화를 가져왔다고 보기는 어렵다. 그간 논란이 되어 온 정부기관의 내용 규제 권한, 즉 콘텐츠의 ‘불법’ 여부뿐만 아니라 ‘유해’ 여부까지 판단할 수 있는 권한 역시 크게 달라지지 않았다. 이러한 규제 구조가 유지되는 한, 사업자가 적극적으로 자율적인 조치에 나설 유인 역시 크지 않다.

92) 개정 정보통신망법 제44조의12는 누구든지 대규모 정보통신서비스 제공자의 정보통신망에서 유통되는 불법정보와 허위조작정보를 대규모 정보통신서비스 제공자에게 신고할 수 있도록 하였다. 신고를 받은 대규모 정보통신서비스 제공자는 신고를 접수한 후 신고자에게 그 사실을 통지해야 하며, 해당 정보의 삭제 또는 접근차단, 정보노출 제한, 게재자 계정의 정지 또는 해지, 광고 수익 등 수익화 제한 등의 조치를 취하고 해당 조치를 한 정당한 이유와 이의신청 절차 등을 신고자 및 게재자에게 통지해야 한다. 신고가 근거가 없을 경우 기각할 수도 있다.

정보통신망법 개정의 가장 큰 명분 중 하나는 ‘허위조작정보의 유통 통제’였지만, 시민들의 팩트체크 참여 없이 이것이 얼마나 실효성을 가질 수 있을지는 의문이다. 팩트체크가 활성화된다고 해서 오정보(misinformation) 또는 허위조작정보(disinformation)가 완전히 사라지는 것은 아니지만, 팩트체크 관행의 활성화 없이 허위조작정보를 효과적으로 통제하는 것 역시 어렵다⁹³⁾. 2020년을 전후하여 한국에서도 자율적인 팩트체크 문화가 형성되었지만, 정치적 편향성 논란이 지속되면서⁹⁴⁾ 현재 한국의 팩트체크 공동체는 사실상 사라진 상태라고 볼 수 있다.⁹⁵⁾

오정보이든 허위조작정보이든, 허위정보의 유통은 사회적 해악을 야기할 수 있고 플랫폼은 자신의 서비스를 통해 허위정보가 쉽게 확산되는 것을 통제할 책임이 있다. 그러나 개정 정보통신망법이 의도적으로 조작된 거짓정보인 ‘허위조작정보’에 초점을 맞추면서, 한국 정보통신서비스제공자의 자율규제기구인 <한국인터넷자율정책기구> 역시 넓은 의미에서 허위정보 일반이 아니라 ‘허위조작정보’에만 초점을 맞추어 기준과 절차를 수립하고 있다.⁹⁶⁾ 그런데 이를 위해서는 허위조작정보인지 여부, 즉 이를 배포하는 이용자가 허위임을 인식하고 손해를 끼칠 의도로 배포했는지 사업자가 판단할 수 있어야 하고, 나아가 타인의 인격권이나 재산권 또는 공공의 이익을 침해하는지 판단할 수 있어야 하는데 이러한 판단을 사업자가 공정하고 실효성 있게 수행할 수 있을지 의문이다. 반면, 실제 허위정보의

93) 통상적으로 허위정보는 해악을 끼칠 의도는 없는 거짓정보인 오정보(misinformation)와 악의적인 의도를 갖고 조작된 거짓정보인 허위조작정보(disinformation)로 구분된다.

94) 오마이뉴스. (2024, 8, 19).

95) 2026년 현재 국제팩트체킹네트워크(IFCN)의 인증을 받은 한국 기관은 JTBC와 단비뉴스, 단 2곳이며, 그 외에 사회적협동조합 빠띠가 시민 중심의 팩트체크 활동을 이어가고 있다. IFCN Signatories 참조.
<<https://ifcncodeofprinciples.poynter.org/signatories>>.

96) KISO(한국인터넷자율정책기구). (2026, 6, 19).

유통은 악의적인 의도가 없는 수많은 이용자의 공유와 참여를 기반으로 이루어지는데, 이때 정보의 허위 여부에 대한 판별, 즉 팩트체크 활동은 훨씬 명확한 대응이 될 수 있으며, 팩트체크가 시민 참여적으로 이루어진다면 더욱 효과가 있을 것이다. 따라서 ‘허위조작정보’에만 초점을 맞추는 현행 법률은 실제 허위조작정보의 유통 구조에 효과적으로 대응하는 데 한계가 있을 수 있다.

지금까지 살펴보았듯이, 유럽은 개별 불법정보에 대한 통제를 넘어 추천 알고리즘을 통한 콘텐츠 증폭과 유통 구조에 초점을 맞추고 있다. 또한 불법정보로 인해 야기되는 해악을 넘어, 중독성 설계와 같이 플랫폼의 환경 요인이 야기하는 위험에도 주목하고 있다. 개별적인 신고 및 조치만으로는 플랫폼의 구조적인 책임을 포착하기 어렵기 때문이다.

한국에서도 대규모 정보통신서비스 제공자에 대해 단순 신고 및 조치 의무를 넘어, 자사의 알고리즘 설계와 서비스 운영이 초래하는 시스템적 위험을 정기적으로 평가하고 이에 대한 완화조치를 취하도록 하는 별도의 제도적 틀을 도입할 필요가 있다. 이를 위한 첫 걸음은 행정심의회와 국가규제 중심의 인터넷 내용규제 체제를 ‘규제된 자율규제’ 체제로, 플랫폼의 시스템적 위험에 대한 규제로 전환하는 것이다.

나. 중독성 설계에 대한 대응

방송미디어통신위원회는 “14세 미만은 서비스 가입을 제한하고 14세 이상 19세 이하 청소년에게는 과몰입을 유도하는 중독성 설계와 추천 알고리즘 노출을 제한하는 방안을 단계적으로 검토하고 있다”고 밝힌 바 있다. 현재 한국 정부는 특정 연령 이하 아동의 서비스 접근을 제한하는 방식과 중독성 설계를 규제하는 방식을 모두 검토하고 있는 것으로 보인다. 그런

데 서비스 접근 제한 방식은 아동 보호를 명분으로 하지만, 아동의 정보 접근권과 소셜미디어가 갖는 긍정적 기능으로부터 아동을 배제한다는 문제점이 있다. 중독성 설계의 경우 무엇을 중독성 설계로 볼 것인지, 그 폐해를 어떻게 입증할 것인지 등의 난점이 있지만, 전 세계적으로 대응이 이루어지고 있는 문제인 만큼 국제적인 정보 공유와 협력을 통해 해결해 나갈 필요가 있다.

전술한 바와 같이 한국의 플랫폼 규제가 개별 불법콘텐츠에 대한 규제에 치우친 반면 시스템적 위험에 대한 규제는 매우 미흡한 상황에서, 아동의 안전이라는 측면에서 플랫폼의 중독성 설계에 대한 책임 문제를 검토할 필요도 있다. 아동의 안전은 국제인권규범이 인정하는 아동 인권의 주요한 부분일뿐더러 한국 사회에서도 수용성이 높은 의제이다. 나아가 플랫폼의 중독성 설계는 아동에게만 부정적 영향을 미치는 것이 아니라 특정한 취약성을 가진 성인은 물론 플랫폼과 종속적인 관계를 맺고 있는 플랫폼 노동자에게도 정신적, 신체적 위험을 야기하는 문제로 논란이 되고 있다. 따라서 아동 뿐 아니라 모든 이용자의 취약성을 표적으로 삼는 플랫폼 설계에 대한 책임과 규제에 대한 제도가 발전할 필요가 있다. 유럽에서는 중독성 설계로부터 소비자를 보호하기 위해 국가 차원의 알고리즘 규제를 모색하는 디지털 공정성법이 추진되고 있다.⁹⁷⁾

다. EU DSA의 성과와 한계에 대한 연구

한국에서 EU DSA와 유사한 시스템을 도입할 경우, EU의 성과와 한계에 대한 면밀한 분석을 통해 시행착오를 줄일 필요가 있다. EU DSA를 통해 이미 주요 플랫폼의 위험평가 보고서와 감사 보고서 등이 공개되어 있으

97) Albert, J., Sax, M., & Helberger, N. (2026, May 19).

며, 이는 한국의 규제기관이나 연구자들이 새로운 규제체제를 도입하기 전이라도 참고할 수 있는 자료이다. 규제기관의 경우 유럽 규제기관과의 소통과 협력을 통해 추가적인 정보를 수집할 수도 있을 것이다.

앞서 살펴본 DSA 제도의 한계를 되풀이하지 않기 위한 대비도 필요하다. 예를 들어, 자율적인 시스템적 위험평가의 실효성을 높이기 위해 보다 구체적인 절차와 기준을 마련할 수 있을 것이다. 완화조치의 효과를 뒷받침하는 지표나 데이터의 공개를 의무화하는 방안도 고려할 수 있다. 감사와 관련해서도 감사기준과 방법론의 불명확성으로 인해 감사인이 사실상 피감사 플랫폼이 정의한 개념을 그대로 수용하거나, 국가 당국의 조사가 진행 중인 사안에 대해 의견을 회피하는 관행을 어떻게 개선할 것인지 검토해야 한다. 감사인의 독립성과 전문성을 어떻게 보장할 수 있을지, 한국에서 이를 감당할만한 감사인이 얼마나 확보될 수 있을지도 고민해야 할 과제이다. 더불어 지역적인 맥락에 따라 위험의 종류나 정도, 완화조치의 효과성이 달라질 수 있다는 점도 고려할 필요가 있다.

데이터 접근과 관련해서는 유럽에서 나타난 병목 지점을 검토해볼 필요가 있지만, ‘검증된 연구자’ 제도와 같은 요건을 갖추는 관행이 한국에 매우 미흡하다는 점도 문제이다. 한국은 EU와 유사한 개인정보 보호 법제를 갖추고 있고 개인정보보호법에 ‘과학적 연구’ 목적의 예외 규정을 두고 있지만, 이를 기업 내부의 비공개 영리 연구에도 폭넓게 적용하며 방만하게 운영되고 있다. 그 결과 개인정보 보호를 위한 연구자의 훈련이나 규범적 관행이 충분히 발전할 수 있는 환경이 조성되지 못했다. 따라서 데이터 접근 제도를 도입하기 전이라도 프라이버시 보호와 데이터 기반 연구를 조화시킬 수 있는 모범 관행과 제도를 발전시킬 필요가 있다.

라. 학계 및 시민사회 참여의 활성화

DSA 위험평가 및 감사 과정에서는 시민사회와의 협의 부족이 계속 지적되었다. 위험평가의 객관성을 높이고 이용자의 관점을 반영하기 위해서는 다양한 시민사회의 참여가 필수적이기 때문이다. 국내 제도 설계에서도 이러한 참여를 보장할 수 있는 방안을 고려할 필요가 있다.

플랫폼 데이터에 대한 연구자의 접근과 연구도 활성화될 필요가 있다. 현재 일부 플랫폼의 데이터에는 제한적이거나 유럽 외 지역의 연구자들도 접근할 수 있다.⁹⁸⁾ 그러나 한국에서는 플랫폼 데이터에 기반한 연구 관행이 거의 형성되어 있지 않다. 주요 빅테크 플랫폼의 위험평가 보고서나 감사 보고서가 공개되어 있지만, 이에 대한 연구도 거의 이루어지고 있지 않다. 이는 독립적인 학술 연구에 대한 공적 지원이나 민간 재단의 지원이 부족한 한국의 열악한 연구 환경에서 기인한 문제이기도 할 것이다. 그러나 DSA와 유사한 데이터 접근 제도가 한국에 도입되기 전이라도 제한적인 범위에서나마 한국적 맥락에서 필요한 주제에 대해 플랫폼 데이터를 활용하는 연구 관행을 촉진할 필요가 있다. 연구 인프라와 관련된 문제를 단기간에 해결하기는 어렵겠지만, 한국에서 플랫폼 데이터에 대한 접근이 보다 용이해지면 관련 학술 연구도 활성화될 것으로 기대할 수 있다.

물론 유럽의 제도를 무조건 수입하자는 것은 아니다. 중요한 것은 제도의 도입 취지와 운영의 맥락을 이해하고 한국의 상황에 맞게 제도를 설계하고 적용하는 것이다. 한국에는 오래된 국내 플랫폼이 존재해 왔으나, 이용자 환경에서는 이미 글로벌 플랫폼의 영향력이 확대되고 있다. 플랫폼이

98) 디지털 민주주의 모니터에서는 주요 플랫폼들의 데이터 접근 정책을 비교한 자료를 공개하고 있다. 이 자료를 보면, YouTube(데이터 API v3), Telegram, Bluesky는 별도의 검증 절차 없이 표준 이용자 계정을 통해 간편하게 접근할 수 있도록 지원하고 있다.

<<https://digitalmonitor.democracy-reporting.org/data-access/>>.

불법 상품, 아동권리, 젠더 폭력, 시민 담론은 물론 민주주의에 이르기까지 사회 전반에 시스템적 위험을 미치는 상황에서 한국도 크게 예외는 아니다. 전 세계 이용자들이 플랫폼이 야기하는 시스템적 위험을 함께 경험하고 있는 만큼, 이러한 위험의 식별과 완화를 모색하는 EU DSA 사례는 한국의 플랫폼 규제 체제를 개선하는 데 유용한 지침이 될 수 있을 것이다. □

참고문헌

국내 자료

- 이권일. (2024). EU 디지털서비스법(DSA)에 나타난 자율규제 (이슈페이퍼 24-17-⑩). 한국법제연구원.
- 연합뉴스. (2026, 7, 16). 14세 미만 SNS 가입 제한 검토...청소년 알고리즘 규제 추진.
- 오마이뉴스. (2024, 8, 19). SNU팩트체크 7년 만에 중단... "한국 언론자유 퇴보".
- 포춘코리아. (2026, 3, 26). "SNS 중독 설계, 빅테크 책임" 알고리즘 탐욕 저격한 美 법원.
- KISO(한국인터넷자율정책기구). (2026, 6, 19). [보도자료]KISO, 허위조작정보 자율정책 가이드라인 최종 발표 .
<<https://www.kiso.or.kr/notice/press-detail?no=622>>.

유럽 집행위원회(EC) 보도자료·공식문서 (발행일순)

- European Commission. (2023, 12, 18). Commission opens formal proceedings against X under the Digital Services Act [Press release].
- European Commission. (2024, 2, 19). Commission opens formal proceedings against TikTok under the Digital Services Act [Press release].
- European Commission. (2024, 2, 23). Delegated Act on Independent Audits under the Digital Services Act.
- European Commission. (2024, 3, 14). Commission opens formal proceedings against AliExpress under the Digital Services Act [Press release].
- European Commission. (2024, 3, 26). Commission publishes guidelines under the DSA for the mitigation of systemic risks online for elections [Press release].
- European Commission. (2024, 4, 22). Commission opens proceedings against TikTok under the DSA regarding the launch of TikTok Lite in France and Spain, and communicates its intention to suspend the reward programme in the EU [Press release].
- European Commission. (2024, 4, 30). Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act [Press release].
- European Commission. (2024, 5, 16). Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram [Press release].
- European Commission. (2024, 7, 12). Commission sends preliminary findings

- to X for breach of the Digital Services Act [Press release].
- European Commission. (2024, 8, 5). TikTok commits to permanently withdraw TikTok Lite Rewards programme from the EU to comply with the Digital Services Act [Press release].
- European Commission. (2024, 10, 31). Commission opens formal proceedings against Temu under the Digital Services Act [Press release].
- European Commission. (2024, 11, 26). Very large online platforms and search engines to publish first risk assessment and audit reports under the Digital Services Act [Press release].
- European Commission. (2024, 12, 17). Commission opens formal proceedings against TikTok on election risks under the Digital Services Act [Press release].
- European Commission. (2025, 1, 17). Commission addresses additional investigatory measures to X in the ongoing proceedings under the Digital Services Act [Press release].
- European Commission. (2025, 5, 27). Commission opens investigations to safeguard minors from pornographic content under the Digital Services Act [Press release].
- European Commission. (2025, 6, 18). Commission accepts commitments offered by AliExpress under the Digital Services Act and takes further action on illegal products [Press release].
- European Commission. (2025, 7, 2). Commission adopts delegated act on data access under the Digital Services Act [Press release].
- European Commission. (2025, 7, 3). FAQs: DSA data access for researchers.
- European Commission. (2025, 7, 14). Commission publishes guidelines on the protection of minors [Press release].
- European Commission. (2025, 7, 28). Commission preliminarily finds Temu in breach of the Digital Services Act in relation to illegal products on its platform [Press release].
- European Commission. (2025, 10, 24). Commission preliminarily finds TikTok and Meta in breach of their transparency obligations under the Digital Services Act [Press release].
- European Commission. (2025, 11, 20). Digital Services Act report lays out landscape of systemic risks online [Press release].
- European Commission. (2025, 12, 5). Commission fines X €120 million under the Digital Services Act [Press release].
- European Commission. (2026, 1, 26). Commission investigates Grok and X's recommender systems under the Digital Services Act [Press release].
- European Commission. (2026, 2, 6). Commission preliminarily finds TikTok's

- addictive design in breach of the Digital Services Act [Press release].
- European Commission. (2026, 2, 17). Commission launches investigation into Shein under the Digital Services Act [Press release].
- European Commission. (2026, 3, 26a). Commission investigates Snapchat's compliance with child protection rules under the Digital Services Act [Press release].
- European Commission. (2026, 3, 26b). Commission preliminarily finds Pornhub, Stripchat, XNXX and XVideos in breach of the Digital Services Act for allowing minors to access their services [Press release].
- European Commission. (2026, 4, 29). Commission preliminarily finds Meta in breach of Digital Services Act for failing to prevent minors under 13 from using Instagram and Facebook [Press release].
- European Commission. (2026, 5, 28). Commission fines Temu €200 million for breaching the Digital Services Act [Press release].
- European Commission. (2026, 7, 10). Commission preliminarily finds the addictive design of Instagram and Facebook in breach of the Digital Services Act [Press release].
- European Commission. (2026, 7, 16). Commission accepts X's action plan to comply with Digital Services Act [Press release].
- European Commission. (2026, 7, 20). Commission fines AliExpress €550 million for breaching the Digital Services Act [Press release].
- European Commission. (2026, 7, 24). Commission preliminarily finds TikTok in breach of Digital Services Act for failing to ensure safe accounts for minors [Press release].

학술 논문·연구보고서

- Bekavac, L., & Mayer, S. (2026). Auditing Meta and TikTok Research API Data Access under Article 40(12) of the Digital Services Act. arXiv preprint arXiv:2601.12390. <<https://doi.org/10.48550/arXiv.2601.12390>>.
- Chapman, P. (2025, March 1). From ambiguity to accountability: Analyzing recommender system audits under the DSA. TechPolicy.press.
- Chapman, P., & Steinberg, M. (2026, February). Measuring risk: What EU risk assessments and US litigation reveal about Meta and TikTok. Knight-Georgetown Institute.
- Committee on the Judiciary, U.S. House of Representatives. (2025, July 25). The foreign censorship threat: How the European Union's Digital Services Act compels global censorship and infringes on American free speech (Interim Staff Report).

- DSA Civil Society Coordination Group. (2025, March). Initial analysis on the first round of risk assessments reports under the EU Digital Services Act. European Center for Not-for-Profit Law (ECNL). (2026, March 3). Five critical lessons from three years of DSA risk assessments.
- Knight-Georgetown Institute (KGI). (2025, May 15). Systemic risk assessment under the Digital Services Act.
- Solarova, S., Mesarčík, M., Pecher, B., & Srba, I. (2026). Beyond the checkbox: Strengthening DSA compliance through social media algorithmic auditing. <<https://arxiv.org/html/2601.18405v1>>.

언론 기사, 단체 블로그

- Albert, J. (2024, December 9). DSA risk assessment reports: A guide to the first rollout and what's next. DSA Observatory.
- Albert, J. (2025, December 19). What are DSA audits doing for systemic risk enforcement? The case of X. DSA Observatory.
- Albert, J., Sax, M., & Helberger, N. (2026, May 19). Digital Fairness Act: Why we need an ambitious DFA to protect digital consumers from manipulative and addictive design practices. DSA Observatory.
- Alliance Defending Freedom International. (2026, February 20). X challenges €120m fine under EU censorship law at top European court.
- Bernard, T. (2024, December 21). Reading the systemic risk assessments for major speech platforms: Notes and observations. TechPolicy.press.
- Chapman, P. (2025, January 9). Advancing platform accountability: The promise and perils of DSA risk assessments. TechPolicy.press.
- Daher, N. (2026, February 9). TikTok to challenge "categorically false" DSA addictive design findings. Lexology.
- EDRi. (2025, December 8). Press release: EU stands up to Big Tech with €120 million fine to X.
- Holznagel, D. (2025, June 11). Shortcomings of the first DSA audits — and how to do better. DSA Observatory.
- Jahangir, R. (2026, May 28). EU tests limits of platform 'risk assessments' with €200 million Temu fine. TechPolicy.press.
- Jóźwiak, M. (2025, November 26). Waiting for the DSA's big enforcement moment. DSA Observatory.
- Liberties. (2026, March 10). Latest DSA risk assessment reports are 'copy & paste' of weak democratic safeguards on Big Tech.
- Negreiro, M., & Anaç, Ö. D. (2026, May 6). Addictive design on online platforms. European Parliamentary Research Service (EPRS).

Slaughter and May. (2026, March 6). TikTok's "addictive design" provisionally found to be a breach of the DSA: Where is the line between engagement and addiction?

웹사이트

European Commission. "Q&A on risk assessment reports, audit reports and audit implementation reports under DSA".

<<https://digital-strategy.ec.europa.eu/en/faqs/qa-risk-assessment-reports-audit-reports-and-audit-implementation-reports-under-dsa>>.

European Commission. Supervision of the designated very large online platforms and search engines under DSA.

<<https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>>.

European Commission. DSA Transparency Database.

<<https://transparency.dsa.ec.europa.eu/>>.

European Commission. DSA Data Access Portal.

<<https://data-access.dsa.ec.europa.eu/home>>.

Alliance Defending Freedom International. About us.

<<https://adfinternational.org/about-us/>>.

DSA 40 Collaboratory. FAQ / Tracker insights.

<<https://dsa40collaboratory.eu/>>.

Democracy Reporting International. Digital Democracy Monitor: Data access.

<<https://digitalmonitor.democracy-reporting.org/data-access/>>.

European Contact Group. <<https://www.europeancontactgroup.eu/>>.

George Washington University Institute for Data, Democracy & Politics (IDDP). Platform Transparency Tools Tracker.

<<https://iddp.gwu.edu/platform-transparency-tools-brussels-effect>>.

International Fact-Checking Network (IFCN). Signatories.

<<https://ifcncodeofprinciples.poynter.org/signatories>>.

The Future of Free Speech. DSA Enforcement Tracker.

<<https://futurefreespeech.org/tracker-of-dsa-enforcement/>>.

SocialMediaTransparency.org. DSA Enforcement Tracker.

<<https://socialmediatransparency.org/dsa-tracker>>.

Tremau. DSA database. <<https://tremau.com/resources/dsa-database/>>.

Meta / Zuckerberg, M. (2025). [Facebook video statement].

<<https://www.facebook.com/watch/?v=1525382954801931>>.