NEWS LETTER

2025-11-28

Legal Issue

- 버그바운티, 더 이상 선택이 아닌 필수 생존 전략
- AI와 개인정보 보호의 새로운 지평: CJEU의 CK v. Dun & Bradstreet Austria 판결 분석

MINWHO News

- 김경환 대표변호사, ALB Korea Law Awards 2025에서 Managing partner of the Year (Boutique Firm) 수상
- 양진영 변호사, 법제처 세미나에서 AI 시대에 맞춘 법령정보 서비스 혁신 방향 논의

Business CASE

법무법인 민후

법무법인 민후

Legal Issue

버그바운티, 더 이상 선택이 아닌 필수 생존 전략

김경환 대표변호사

애플이 10월 10일 자사 버그바운티 프로그램을 대폭 확장했다. iOS뿐 아니라 macOS, watchOS, visionOS까지 범위를 넓히고, 최고 보상금도 100만달러 이상으로 상향했고 특정조건을 만족할 경우 최대 500만달러도 초과할 수 있다. 단순한 보안 취약점 신고 제도를 넘어, 애플 내부 보안팀과 외부 연구자 간의 협업 플랫폼으로 진화하고 있다.

버그 바운티의 개념 자체는 1995년 넷스케이프에서 처음 시작했지만, 2010년대 초반 구글과 페이스북이 본격적으로 도입하면서 확산됐다. 초기에는 화이트해커를 제도권 안으로 끌어들이는 데 초점이 있었다. 한국에서도 2015년경부터 금융보안원, 한국인터넷진흥원, 일부 대기업이 시범 운영을 시작했지만, 대부분은 폐쇄형 테스트 수준에 그쳤다.

글로벌에서는 '보안계의 에어비앤비'라 할 수 있는 해커원(HackerOne), 버그크라우드(Bugcrowd) 같은 전문 플랫폼이 등장해 보안 연구자와 기업을 매칭하는 생태계로 발전했다. 이들은 단순한 보상 시스템이 아니라, 취약점 리포트 검증, CVSS(Common Vulnerability Scoring System) 기반 평가, 보상금 산정까지 체계적으로 관리한다. 반면 한국의 많은 기관과 기업은 여전히 이메일 제보나 자체 게시판을 통해 수동적으로 제보를 받고 있다.

버그바운티의 핵심은 '외부 참여를 통한 지속적 검증'이다. 전통적인 보안 점검은 계약 시점의 정적 테스트에 불과하지만, 버그바운티는 실시간으로 시스템의 안전성을 시험한다. 더 나아가, 이 제도는 해커를 적이 아니라 파트너로 대우하는 문화적 전환을 상징한다.

국내에서는 세 가지 구조적 문제가 있다. 첫째, 법적 불확실성이다. 정보통신망법상 '무단 접근' 개념이 모호해, 의도치 않게 제보자가 법적 리스크를 떠안을 수 있다. 둘째, 예산 문제다. 보안팀 예산은 대부분 장비와 점검 비용에 쓰이기 때문에, 버그바운티 보상금은 후순위로 밀린다. 셋째, 조직문화다. '취약점 제보=실수 노출'로 인식하는 경향이 여전히 강하다. 또 일부 기관은 '인증된 참여자만 참여 가능' 같은 제한을 두어 사실상 커뮤니티 기반 검증의 장점을 잃는다.

버그바운티가 다음 단계로 나아가기 위해서는 법·제도적, 기술적, 문화적 세 축의 정비가 필요하다. 법적으로는 '선의의 취약점 제보자 보호조항(legal safe harbor)'이 반드시 필요하다. 이는 미국의 DMCA §1201 예외조항이나 EU의 NIS2 Directive가 이미 규정하고 있는 부분이다. 한국에서도 정보통신망법에 '정당한 목적의 취약점 탐지 및 제보는 위법이 아니다'라는 명문화가 필요하다. 기술적으로는 보상 기준의 투명화가 필요하다. CVSS 점수에 따른 등급별 보상, 중복 리포트 처리 기준, 공개 시점 정책 등을 명확히 해야 한다. 또 인공지능(AI) 모델, 사물인터넷(IoT), 서비스형소프트웨어(SaaS) 등 신흥 영역에 대한 버그바운티 가이드라인도 새로 마련돼야 한다. 문화적으로는 보안팀이 제보자와 '같은 팀'이라는 인식이 자리 잡아야 한다. 기업은 버그바운티 결과를 부끄러운 리스크가 아니라 '투명성과 개선의 증거'로 공개해야 한다.

버그바운티는 단순한 보안 프로그램이 아니라, 디지털 사회의 신뢰를 재구성하는 장치다. 시스템의 완벽함을 전제로 하지 않고, 불완전함을 관리 가능한 상태로 만드는 구조이기 때문이다. 한국이 지금처럼 폐쇄적인 보안 프레임에 머무른다면, 글로벌 수준의 보안 경쟁력은 결코 따라잡을 수 없는 바, '공유된 안전'을 추구하는 인터넷의 미래로 가는 가장 현실적인 경로다.

김경환 대표변호사, 변리사

프로필 보기

02-532-3425
oalmephaga@minwho.kr

Legal Issue

AI와 개인정보 보호의 새로운 지평: CJEU의 CK v.Dun & Bradstreet Austria 판결 분석

현수진 변호사

2025년 2월 27일, 유럽사법재판소(CJEU)는 CK v. Dun & Bradstreet Austria 사건(C-203/22)에서 GDPR 제15조(1)(h) 및 제22조와 관련한 중대한 판결을 선고했다. 본 판결은 자동화된 의사결정 프로세스에서의 투명성 의무와 영업비밀 보호 간 균형에 관한 법적 기준을 제시하였다.

1. 사건의 배경 및 개요

오스트리아 시민 CK는 Dun & Bradstreet Austria GmbH(이하 D&B)가 수행한 자동화된 신용평가 결과, "신용도가 불충분하다"는 판단을 받았다. 이에 따라 이동통신사가 CK와의 신규 또는 연장 계약 체결을 거부하였다. CK는 이 결정의 근거와 자동화 평가의 논리를 알고자 GDPR 제15조(1)(h)에 따라 정보 제공을 요청했으나, D&B는 알고리즘이 영업비밀에 해당한다며 상세 정보 제공을 거부했다.

CK는 오스트리아 개인정보보호기관(DPA)에 이의를 제기했고, DPA는 D&B에 의미 있는 정보제공을 명령했다. D&B는 이에 불복해 오스트리아 연방행정법원에 소송을 제기했으나, 법원 역시 D&B가 CK에게 충분한 정보를 제공하지 않았다고 판단했다. 하지만 집행기관(비엔나 시의회)은 D&B가 이미 의무를 이행했다고 보고 집행을 거부했고, 이에 CK는 다시 행정법원에 이의를 제기했다. 행정법원은 GDPR 해석에 관한 쟁점이 있다고 판단해 CJEU에 예비적 판단을 요청하게 되었다.

2. CJEU 판결의 법리적 쟁점

CJEU는 해당 사건에 대하여 다음과 같은 쟁점을 검토했다.

(1) GDPR 제15조 1항 (h)호의 해석

설명의무의 구체성: GDPR 제15조 1항 (h)호에서는 자동화된 의사결정(프로파일링 포함)과 관련된 정보공개 의무를 규정하고 있다. 정보주체는 ① 자동화된 의사결정의 존재 여부, ② 관련 논리의 의미 있는 설명, ③ 의미 및 예상 결과에 대한 정보를 제공받을 권리가 있다.

프로파일링과 자동화 결정의 구분: 본 판결에서 CJEU는 GDPR 제15조 1항 (h)호에서 말하는 "의미 있는 정보"란 개인이 해당 결정을 이해하고 이의를 제기할 수 있을 정도로 구체적이어야 한다고 판단하였다. 단순히 알고리즘이나 수학적 공식, 기술적 세부사항을 제공하는 것이 아니라, 실제로 어떤 개인 데이터가 어떻게 사용되어 결과가 도출되었는지, 그리고 데이터가 달라졌을 때 결과가 어떻게 달라질 수 있는지에 대해 명확하고 이해하기 쉬운 설명이 필요하다는 것이다.

(2) 영업비밀과 개인정보 보호 권리의 충돌

영업비밀 주장의 한계: D&B는 알고리즘은 기업의 영업비밀이므로 상세 공개가 불가하다고 주장했으나, CJEU는 영업비밀 보호가 데이터주체의 기본권(정보접근권)을 절대적으로 제한할 수 없다고 판시하였다. 영업비밀이 문제될 경우, 해당 정보를 정보주체에 제공하는 대신 감독기관이나 법원에 제출하여 비례성 원칙에 따라 권리 균형을 판단받아야 하며, 일률적 배제는 허용되지 않는다고 보았다.

(3) GDPR 제22조와 인간 개입 의무

자동화된 의사결정과 보호조치: GDPR 제22조는 "프로파일링 등 자동화된 개별 의사결정"에 관한 조항으로, 정보주체가 전적으로 자동화된 처리(프로파일링 포함)에 근거한 결정의 대상이 되지 않을 권리를 명시하고 있으며, 개인정보처리자는 정보주체의 권리를 보호하기 위하여 ① 인간의 개입을 요구할 권리, ② 자신의 관점을 표명할 권리, ③ 결정에 이의를 제기할 권리를 보장하여야 한다.

완전 자동화 결정의 엄격한 기준: CJEU는 "기계적 추천의 단순 승인"은 유효한 인간 개입으로 인정되지 않으며, 결정 프로세스 전반에 걸친 실질적 평가가 필요하다고 보았다. 특히 알고리즘이 완전 자동화된 경우 설명 의무(투명성)가 강화되며, "블랙박스" 방식의 시스템 운영은 위법으로 간주될 수 있다.

자동화 결정의 책임 소재: 해당 사건에서는 D&B와 같은 신용평가 기관이 제공하는 점수 자체가 자동화된 결정에 해당하는지, 아니면 실제 계약 거부를 결정한 이동통신사가 책임을 지는지에 대한 논의도 있었다. CJEU는 신용점수가 계약 체결 여부에 결정적 영향을 미친다면, 점수 제공 행위 자체도 GDPR 제22조의 자동화 결정에 해당할 수 있으므로, 신용평가 기관도 GDPR 제22조에 따른 자동화된 의사결정의 책임을 질 수 있다는 점이 명확해졌다.

3. 한국 기업 입장에서 주목할 사항

현행 개인정보 보호법에는 GDPR 제22조에 상응하는 자동화 결정 관련 규정이 미비하다. 다만, 제35조(열람청구권)에서 유사한 접근권을 인정하고 있어 CJEU 판결이 국내 감독기관의 해석에 영향을 줄 가능성이 있다.

CJEU 판결은 인공지능 기반 신용평가 시스템을 운영하는 금융기관 등에 중대한 영향을 미칠 것으로 예상된다. 특히 "이해 가능성" 기준의 구체화와 "실질적 설명" 요건 강화로 인해 알고리즘 투명성 관리가 새로운 규정준수 과제로 부상하였다. 향후 개인정보 영향평가 과정에서도 자동화 결정 설명 체계에 대한 검증이 강화될 것이다.

이를 고려하면, AI 알고리즘을 활용하여 자동화된 의사결정을 내리는 한국 기업은 다음 측면에서 준비가 필요하다.

(1) 자동화 결정 설명 체계 개선: AI 모델 개발 단계부터 Explainable AI(XAI) 도입을 검토해야 한다. 특히 정보주체가 열람청구권을 행사할 경우에 대비하여, 자동화 결정 프로세스 매핑 및 문서화 등 결정 로직 시각화 도구를 개발하는 등, 알고리즘 투명성 강화를 위해 체계를 개선할 필요가 있다.

(2) 분쟁 대응 매뉴얼 정비: 본 판결을 통해 알고리즘이 영업비밀에 해당할 경우에도, 감독기관과의 사전 협의가 필수 절차로 자리잡을 것으로 보인다. 이에 따라, 영업비밀 주장 시 감독기관에 해당 정보를 제출한 후 부분적 공개 방안을 모색하는 등, 분쟁 대응을 위한 내부 매뉴얼 마련이 절실하다.

이번 판결은 단순히 유럽의 사례를 넘어 "AI의 책임 있는 사용" 을 위한 글로벌 표준을 제시했다. 한국 기업은 알고리즘 투명성 강화와 인간 개입 프로세스의 실질적 운영을 통해 EU 시장에서의 규정준수 리스크를 선제적으로 관리할 필요가 있다.

현수진 변호사

프로필 보기

02-532-3424
hyunsj@minwho.kr

법무법인 민후

MINWHO NEWS

김경환 변호사, ALB Korea Law Awards 2025 수상

김경환 변호사, Managing partner of the Year (Boutique Firm) Finalist

법무법인 민후의 김경환 대표변호사가 ALB(Asian Legal Business) 톰슨로이터가 주최한 ALB Korea Law Awards 2025에서 'Managing Partner of the Year (Boutique Firm)' 부문을 수상했습니다.

올해 시상식에서 김경환 대표변호사는 탁월한 리더십과 지속적인 성과 창출 능력을 높게 평가받아 파이널리스트 명단에 오른 데 이어, 'Managing Partner of the Year (Boutique Firm)' 부문에서 최종 수상의 영예를 안게 되었습니다. 이는 개인의 전문성뿐 아니라 법무법인 민후의 성장 및 발전을 견인해 온 리더십을 인정받은 결과로 평가됩니다.

ALB Korea Law Awards는 국내외 유수 로펌과 변호사들의 업적을 종합적으로 심사해 각 분야의 뛰어난 법률 전문가를 선정하는 권위 있는 시상식으로, 김경환 대표는 지난해에도 동일 부문 파이널리스트로 이름을 올리며 국내 부티크 로펌 가운데서도 독보적인 위상을 이어가고 있습니다.

법무법인 민후는 개인정보·AI 등 신기술 분야와 더불어 특허, 상표, 저작권, 디자인 등 지식재산권 전반에 걸쳐 전문성을 강화해 왔습니다. 더불어 잡코리아–사람인 웹크롤링 분쟁, 야놀자 DB 크롤링 사건, 핑크퐁 상어가족 저작권 침해 사건, 메타–개인정보보호위원회 과징금 취소 소송 등 주요 사건을 성공적으로 수행하며 의미 있는 성과를 축적해 왔습니다.

김경환 대표변호사는 IT·IP 전문 로펌으로서 민후를 이끌며 기술 발전에 따른 새로운 법률 수요를 신속하게 반영해 왔으며, 이러한 성과가 이번 개인 부문 최고상인 'Managing Partner of the Year (Boutique Firm)' 수상으로 이어졌습니다.

김경환 변호사는 "급변하는 기술 환경 속에서도 전문 법률 서비스를 한층 정교화하고, 국내외 고객에게 최적의 해결책을 제공하는 로펌으로 계속 성장해 나가겠다"며 "혁신과 전문성 강화에 기반한 신뢰받는 파트너로 자리매김하겠다"고 수상 소감을 전했습니다.

MINWHO NEWS

양진영 변호사,법제처 세미나에서 AI 시대에 맞춘 법령정보 서비스 혁신 방향 논의

양진영 변호사 법제처 세미나에서 AI 시대에 맞춘 법령정보 서비스 혁신 방향 논의

법제처는 지난 10월 28일 '2025년 찾기쉬운 생활법령정보 세미나'를 개최하며, 인공지능(AI) 기술 환경에 적합한 생활법령정보 서비스 개선책을 적극적으로 검토했습니다.

이번 행사에서는 AI 시대에 필요한 법령정보 서비스의 방향성이 주요 의제로 다뤄졌으며, 법률·기술 분야의 다양한 전문가들이 참여해 관련 논의를 이어갔습니다. 이 자리에서 법무법인 민후의 양진영 변호사는 법률전문가의 시각에서 AI 기술이 생활법령정보 서비스에 도입될 때 기대되는 효과와 고려해야 할 과제들을 제시하며 주목을 받았습니다.

양진영 변호사는 "AI 기반 법령정보 서비스가 확대되기 위해서는 정확성과 신뢰성 확보가 무엇보다 중요하며, 국민이 실제로 활용할 수 있는 정보 품질을 높이는 것이 핵심"이라고 강조했으며, AI가 국민의 법률 접근성을 높이는 도구로 자리 잡기 위해 필요한 제언도 함께 제시했습니다.

마지막으로 참석자들은 AI 기반 생활법령정보 서비스가 앞으로 국민의 법률 접근성을 보다 향상시키는 방향으로 발전할 필요가 있다는 데 의견을 모으며, 향후 서비스 혁신을 위한 다양한 아이디어를 공유했습니다.

Business CASE

이달의 주요 업무사례

1. 소프트웨어 저작권 침해 손해배상 소송, 억대 금액 청구받은 의뢰인 대리해 약 85% 감액 화해권고 결정 도출

2. 상속재산분할 관련 상속인을 대리해 다른 상속인들과의 공유에서 단독 소유로 권리관계 명확히 한 사례

3. 정보통신망법 비밀침해죄 피의자를 대리하여 무혐의 받아 승소

4. 클라우드 서비스 사용료 청구소송에서 원고를 대리하여 사용료 지급 판결 이끌어 승소

5. 부정경쟁방지법 위반으로 모조품 제조·판매 금지 및 손해배상청구소송에서 원고를 대리하여 부정경쟁행위 인정 및 금지명령 판결 이끌어 승소

6. IT 용역계약 자문 - 시스템 개발 sw용역계약 상 소스코드 제공 의무 여부에 관한 검토 자문 제공

7. 경쟁사 직원 채용 시 해당 직원들의 경업금지약정 유효성 및 법적 리스크 사전 검토 자문

8. 상표 무단 사용 및 불법 데이터 크롤링에 대한 경고장 작성 법률자문

9. 외국인 대상 기명식 선불전자지급수단 발급을 위한 신원확인 서비스의 법적 유효성 법률자문

10. AI 교육 콘텐츠 서비스 기업에 AI디지털교과서 서비스 이용약관 검토 법률자문

법무법인 민후

서울특별시 강남구 테헤란로 134, 포스코 타워 역삼 11층

Tel. +82-2-532-3483 **Fax.** +82-2-532-3486

www.minwho.kr

[변호사 소개 바로가기] [주요 업무사례 바로가기]

[전화 상담 바로가기] [카톡 상담 바로가기] [홈페이지 상담 바로가기] [이메일 상담 바로가기]

본 뉴스레터의 내용 또는 기타 법률 문의가 필요하신 경우
법무법인 민후로 연락주시면 담당 변호사님의 답변을 받으실 수 있습니다.