이슈와 논점 Issues and Perspectives

국회입법조사처 | 2026. 02. 02. | 제2469호

nars.go.kr 국회입법조사처

쿠팡 국정조사에서의 개인정보 침해 관련 쟁점

박 소 영 · 김 형 진

2025년 대규모 개인정보 침해사고가 잇따른 가운데, 11월 국내 대표 플랫폼인 쿠팡에서 발생한 개인정보 침해사고는 플랫폼 기업의 내부 보안 관리 및 사고 대응 체계 전반의 문제점을 부각하며 사회적으로 큰 파장을 야기하였다. 기존의 행정조사·제재 및 국회 청문회만으로는 사회적 의혹과 불신을 해소하기 어렵다는 지적이 이어지면서 국정조사 논의가 진행되고 있다. 본 보고서는 쿠팡의 내부보안체계 상황, 개인정보 데이터베이스 관리 방식, 통지 내용과 방식에 대한 의사결정 과정, 자체 조사의 이유와 방식, 피해자 배상 방식 등 국정조사 과정에서 중점으로 점검해야 할 주요 쟁점을 정리한다.

1. 쿠팡 개인정보 유출의 경위

2025년 11월 국내 최대 전자상거래 업체인 쿠팡에서 약 3,370만 계정[1]에 대한 대규모 개인정보 유출이 발생하였다. 2025년 6월 24일경 해외에서 쿠팡 시스템에 대한 비정상적 접근이 시작되었고, 이후 고객정보에 대한 유출이 일어난 것으로 추정되고 있다. 2025년 12월 2일 국회 과학기술정보방송통신위원회 현안질의에서 쿠팡 최고정보보호책임자(CISO)는 퇴사자인 용의자가 내부자 전용 토큰(token) 인증 서명키[2]를 외부로 유출하였고, 이를 이용해 가짜 토큰을 만든 후 API[3]를 통해 시스템에 접근한 것으로 보인다는 취지로 답변하였다.

쿠팡은 2025년 11월 18일 유출 사실을 인지하고, 11월 19일·20일에 약 4,500여 개 계정의 피해가 발생한 것으로 관련 신고·통지를 하였다. 하지만 약 열흘이 지난 11월 29일 쿠팡은 피해 규모를 약 3,370만 개 계정으로 확대 발표하였다.

1) 다만, 현재 쿠팡측은 개인정보가 유출된 계정 수가 약 3,000개 수준으로 제한적이라고 주장하고 있다.

2) 이용자가 ID, 비밀번호 등을 이용하여 로그인하면, 인증서버가 서명키로 서명하여 상기 로그인 정보에 기반한 인증된 토큰을 만든다. 인증된 토큰은 해당 이용자가 이미 인증되었음을 증명하는 증표이고, 로그인 없이도 인증 토큰을 통해 이용자 본인임을 증명할 수 있다. Token의 구조와 이에 사용되는 아이디 정보를 알고 서명키를 가지고 있으면 해당 아이디 정보에 해당되는 허위의 인증된 토큰을 만들 수 있다. 이에 대해서 현안질의 당시 김승주 고려대학교 교수는 호텔에 들어갈 때 신원확인을 한 뒤 방 열쇠를 발급받는데, 그 방 열쇠를 발급하는 비밀번호를 가져간 상황으로 이해하면 된다고 비유하여 설명하였다.

3) Application Programming Interface의 약자로, 소프트웨어 시스템 간에 서로 데이터를 주고받을 수 있게 하는 인터페이스이다.

2. 그간 제기된 주요 논란

1. 내부보안체계의 미비

쿠팡은 2020년, 2021년, 2023년 등 여러 차례 개인정보 침해 사고를 경험하였음에도 불구하고, 이번에 재차 대규모 침해가 발생하였다. 반복되는 사고를 볼 때 내부 보안 관리와 대응 체계가 근본적으로 개선되지 않았다는 점이 지적되고 있다.

특히 토큰 서명키는 회사 외부로 반출되어서는 안 되는 핵심 보안 자산으로, 퇴사 등 인사 변동 시 즉시 폐기하거나 재발급하는 것이 일반적인 보안 관리 기준에 해당한다. 그럼에도 불구하고 토큰 서명키가 장기간 외부에 노출된 정황이 있었고, 외부에서 API를 통해 시스템 접근이 가능하였다. 이러한 행위가 상당 기간 지속되었음에도 이를 이상 징후로 탐지하지 못하였고, 인지한 이후 11일이 경과한 시점에서야 약 3,370만 개 계정에 대한 접근이 이루어진 사실을 확인하였다면, 권한 관리, 접근 기록 분석, 사고 대응 프로세스 등 쿠팡의 보안 체계 전반에 구조적 취약점이 존재했을 가능성을 시사한다.

NARS www.nars.go.kr

발행처 | 국회입법조사처 **발행인** | **이관후** 국회입법조사처장
저 자 | **박소영** 사회문화조사실 과학방송통신팀 입법조사관, 변호사
02-6788-4713 sypark@assembly.go.kr
김형진 정치행정조사실 행정안전팀 입법조사관, 변호사
02-6788-3842 hjkim6984@assembly.go.kr

국회입법조사처 NATIONAL ASSEMBLY RESEARCH SERVICE

2. 유출 정보의 광범성과 민감성

이번 사고에서 특히 논란이 된 부분은 유출된 개인정보의 규모와 유형이 매우 광범위하고 다양했다는 점이다. 유출자는 개인정보 침해 사고로서는 역대 최대 규모인 3,370만 개 고객 계정의 개인정보에 접근한 것으로 알려졌다. 또한 유출된 정보에는 이용자의 이름, 이메일, 주소뿐만 아니라 배송지 주소록, 일부 주문정보 등 민감한 정보도 포함되었다. 특히 배송지 주소록이 유출됨에 따라 이용자 본인뿐만 아니라 제3자의 정보까지도 함께 노출된 것으로 전해진다. 이는 기존의 다른 개인정보 침해 사건에서, 유출 정보의 유형이 이용자 본인의 인적사항 등으로 한정되었던 점과 대비되는 부분이다.

또한, 활성 회원의 정보뿐만 아니라 탈퇴 회원의 정보도 유출된 것으로 전해진다. 특히 탈퇴 후 사후 처리와 관련성이 크지 않아 보이는 배송지 주소록 정보(공동현관 비밀번호 등)까지 유출된 것으로 알려져 논란이 일었다. 이처럼 광범위하고 다양한 유형의 개인정보가 유출된 점을 두고, 쿠팡의 개인정보 데이터베이스 관리 방식의 적절성에 대한 논란이 이어졌다.

3. 유출 사실 통지의 부적절성

쿠팡의 정보주체에 대한 통지가 매우 형식적이고 소극적인 방식으로 이루어졌다는 비판이 제기되고 있다. 쿠팡은 사고 초기에 팝업창이 아닌 웹페이지 상단의 다른 배너 광고 옆에 "고객 여러분께 심려와 걱정을 끼쳐드려 진심으로 사과드립니다"라는 작은 배너를 게시하여 유출 사실을 명확히 알기 어려운 표현으로 안내하였고, 그마저도 단기간(1~2일) 노출한 후 삭제하였다. 피해를 최소화하기 위해 정보주체가 취할 수 있는 방법에 대한 안내도 부족하였고, 유출 항목 일부(공동현관 비밀번호)를 누락하였으며, 담당부처 및 연락처 정보도 직접 기재하지 않고 URL 링크 형태로 제공하여 스미싱 등 2차 피해 발생 가능성을 높였다. 또한 통지 내용에 '유출'이라는 표현 대신 '노출', '무단 접근' 이라는 표현을 사용하여, 쿠팡이 대규모 개인정보 침해 가능성을 인지한 이후 정보주체 보호를 최우선으로 두고 의사결정을 하였는지에 대한 논란이 제기되었다.

개인정보보호위원회가 2025년 12월 3일 개인정보 '노출'이 아닌 '유출'로 변경할 것, 팝업창 등을 통해 공지할 것 등을 쿠팡에 촉구한 이후에야,[4] 쿠팡은 "개인정보 유출사고에 관해 재안내 드립니다"라는 제목으로 재통지를 하였다.

4) 개인정보보호위원회 보도자료, 「개인정보위, "쿠팡에 ①유출로 수정·보완해 재통지, ②이용자 대상 피해 최소화 방법 적극 안내, ③2차 피해 방지 자체 대응 강화" 촉구 의결」, 2025. 12. 3.

4. 수사 중 사안에 대한 자체조사의 불법성 여부

2025년 11월 말부터 민관합동조사단 조사와 경찰 수사가 진행 중인 상황에서, 쿠팡이 유출자로 지목된 전직 직원을 자체 접촉하고 그를 통해 얻은 증거를 외부업체에 맡겨 포렌식한 결과를 12월 25일 공지하여 논란이 일고 있다. 쿠팡은 특정된 유출자가 사용한 모든 장치와 하드드라이브를 회수하여 자체 포렌식한 결과 그 내용이 유출자의 진술 내용과 부합하다고 자사 앱·웹에 공지하였다. 유출자가 탈취한 보안키를 사용하여 3,300만 고객 계정의 기본적인 고객정보에 접근했으나 약 3,000개 계정의 고객정보(이름, 이메일, 전화번호, 주소, 일부 주문정보)[5]만 저장했고, 사태에 대한 언론보도를 접한 후 저장한 정보를 모두 삭제하였으며 고객정보 중 제3자에게 전송된 데이터는 일체없다는 것이다.

쿠팡의 공지에 대해 과학기술정보통신부, 경찰, 개인정보보호위원회는 모두 반박하고 있다. 과학기술정보통신부는 2025년 12월 25일 민관합동조사단이 조사 중인 사항을 쿠팡이 일방적으로 알린 것에 대해 강력히 항의하였고,[6] 경찰은 2026년 1월 12일 쿠팡의 개인정보 유출 규모가 자체 발표한 3,000개보다 훨씬 큰 것으로 보고 있다고 언급하였다.[7] 개인정보보호위원회 또한 2026년 1월 14일 쿠팡이 자체 조사 결과를 공식 조사에서 확인된 것처럼 공지하는 행위는 국민들이 상황을 오인하고 정확한 유출 내용과 피해 범위를 파악하기 어렵게 하는 등 개인정보보호위원회 조사 방해에 해당할 수 있으므로 즉각 중단할 것을 촉구하였다. 또한 조사 과정에서 자료제출 요구에 응하지 않거나 지연 제출을 반복하는 행위는 제재 처분 시 가중요건이 될 수 있음을 엄중 경고하였다.[8] 하지만 쿠팡은 2026년 1월 27일 기준으로 이 공지를 유지하고 있다.

5. 배상 방식의 적절성 논란

2025년 12월 29일에는 쿠팡 홈페이지를 통해 개인정보 유출 고객에 대한 보상안이 발표되었다.[9] 개인정보 유출을 통지받은 3,370만 개 계정의 고객을 대상으로 1인당 5만 원 상당의

5) 이에 공동현관 출입번호는 2,609개라고 밝히고 있다.
6) 과학기술정보통신부 보도 설명자료, 「쿠팡의 개인정보 유출 조사 관련 배포자료는 민관합동조사단의 확인이 필요한 사항입니다」, 2025. 12. 25.
7) 보안뉴스, "[쿠팡 해킹] 경찰 '쿠팡 개인정보 유출 3000건 훨씬 넘어'... 로저스 대표 1차 소환 불응", 2026. 1. 12.
8) 개인정보보호위원회 보도자료, 「개인정보위, 쿠팡의 자체조사 결과 홈페이지 공지 중단 등 촉구」, 2026. 1. 14.
9) 쿠팡 보도자료, 「쿠팡, 고객 신뢰 복원 위한 보상안 발표…1조6850억원 규모 구매이용권 지급」, 2025.12.29.

구매이용권을 지급한다는 내용이었다.

그러나 배상 방식을 둘러싸고 여러 논란이 제기되었다. 우선, 위법 행위에 대한 책임을 전제로 한 '배상'이 아니라, 적법한 행위로 인한 손실에 관계되는 '보상'이라는 표현이 사용되었다. 또한 배상의 내용은 금전 지급이 아니라 '구매이용권'을 지급하는 방식이었으며, 해당 이용권을 쿠팡의 여러 계열사에서 일부씩을 사용하도록 구성된 형태였다.[10] 아울러 이용권 사용기간도 3개월로 한정되었으며, 일부만 사용한 경우 잔액이 환불되지 않는다는 제한도 두었다.

이와 같은 보상 방안에 대하여, 지급된 구매이용권을 모두 사용하기 위해서는 쿠팡 계열사의 서비스에 가입·이용이 요구된다는 점에서 실질적인 배상이라기보다는 마케팅 수단에 가깝다는 지적이 제기되었다. 특히 사고 이후 쿠팡 서비스를 탈퇴한 고객의 경우, 보상을 받기 위해 재가입해야 한다는 점에서 보상을 계기로 소비자를 재차 거래관계로 유인하려 한 것이 아니냐는 논란이 이어졌다.

3. 향후 중점적으로 검토해야 할 쟁점

1. 내부보안체계 상황

엄격하게 관리해야 하는 내부자 전용 토큰 서명키가 퇴직 이후에도 유효하게 작동하였다는 점은 단순한 실수를 넘어 전사적 내부 통제 프로세스에 구조적 결함이 있을 가능성을 시사한다. 또한 이를 통해 대규모 개인정보에 접근하는 것이 가능했다면, '내부자 위협'을 방어하기 위한 최소 권한 원칙과 이상 징후 탐지 설계가 제대로 작동하지 않는 것일 수 있다. **퇴사자에 대한 접근권한 회수 절차, 실시간 탐지·차단의 운영방식, 유사한 접근이 추가로 발생했을 가능성은 없는지에 대한 확인이 요구된다.**

2. 개인정보 데이터베이스 관리 방식

현행 「개인정보 보호법」 제21조에 따르면, 탈퇴 등으로 이용자의 개인정보가 불필요하게 되었을 경우, 원칙적으로 해당 개인정보는 ① 지체 없이 파기되어야 한다.[11] 물론 사후 정산이나 제품 보증 등을 위하여 예외적으로 개인정보를 계속 보유하는 것은 가능하나,[12] 이 경우에도 ② 다른 개인정보와 분리 보관해야 하며, ③ 예외 사유와 직접적으로 관련된 정보에 한하여 보유하여야 한다. 이는 비활성정보에 대한 접근 가능성을 제한함으로써, 내부 직원의 무단 조회·활용을 방지하고 해킹 등 사고 발생 시에도 피해 범위를 국소화하려는 데 그 목적이 있다고 할 수 있다.

그런데 이번 유출사건에서는 활성 회원의 정보뿐만 아니라 탈퇴 회원의 정보까지도 일괄 유출된 것으로 알려졌다. 이는 유출자가 활성 정보뿐만 아니라 비활성 정보에도 별다른 제약 없이 접근할 수 있었을 가능성을 시사한다. 나아가 이는 ① 비활성 정보에 대한 파기 의무 또는 ② 분리 보관 의무가 제대로 이행되지 않았을 가능성에 대한 점검 필요성을 제기한다. 아울러 사후 정산, 소비자 피해 구제, 제품 보증 등 법에서 정한 예외 사유와 관련성이 크지 않아 보이는 정보까지도 유출되었다는 의혹도 제기되고 있는바, ③ 예외 사유를 기준으로 계속 보유할 개인정보를 구체적으로 선별하는 절차가 적정하게 이루어졌는지 여부에 대한 확인도 요구된다. **향후 국정조사 과정에서 쿠팡의 개인정보 데이터베이스 관리 방식, 특히 탈퇴 회원 정보 등 비활성 정보의 관리가 적정하게 이루어졌는지 여부를 중점적으로 점검해볼 필요가 있다.**

3. 통지 내용과 방식에 대한 의사결정 과정

개인정보 유출 통지의 목적 중 하나는 정보주체가 자기 보호 조치를 취할 수 있도록 하는 것이다. 그러나 쿠팡은 침해 사실을 늦게 인지하고 피해 규모 산정에도 상당한 시간이 소요될 만큼 내부 보안 역량의 부족을 드러내면서, '유출'에 대해서는 부정적인 태도를 유지하고 통지의 시기와 방식을 소극적으로 운영하였다. 그 결과 정보주체 보호 측면에서 통지 제도의 취지가 충분히 구현되었는지에 대한 문제 제기가 가능하다.

향후 조사 과정에서는 쿠팡이 유출 사실을 명확히 인지하기 전에도 유출 정황을 파악하고 있었던 것은 아닌지, 그럼에도 불구하고 법이 정한 형식적 기준에 맞춰 통지의무를 뒤늦게 이행하였던 것은 아닌지 확인해 볼 필요가 있다. 또한 소극적으로 통지에 이르게 된 경위에 관해서도 확인이 필요하다. 3,370만 개 계정에 대한 비정상적 접근이 확인된 상황에서 '유출' 표현을 회피하는 판단은 누구에 의해 어떠한 기준과 책임 하에 결정되었는지에 대한 설명이 요구된다.

10) 쿠팡 상품 5천원 구매이용권, 쿠팡이츠 배달 주문 상품 5천원 구매이용권, R.LUX 뷰티 &패션 상품 2만원 구매 이용권, 쿠팡트래블 국내 숙박 & 국내 티켓 상품 2만원 구매이용권.

11) 이 경우 개인정보가 복구되거나 재생되지 않도록 조치해야 한다.

12) 다른 법령에 따라 개인정보를 계속 보존하여야 하는 경우(동법 제21조제1항 단서). 예컨대, 전자상거래법상 계약 또는 청약철회 등에 관한 기록(5년), 대금결제 및 재화등의 공급에 관한 기록(5년), 소비자의 불만 또는 분쟁처리에 관한 기록(3년) 등.

4. 자체 조사의 이유와 방식

쿠팡은 정부와 협력하여 자체 조사를 하였다고 주장하나, 수사기관은 사전에 관련 내용을 협의한 바 없다는 입장이다. 만약 쿠팡이 민관합동조사단 및 수사기관과의 사전 협의 없이 독자적으로 유출자를 특정하고 자신들이 선정한 외부업체에 증거를 전달하여 포렌식을 수행하는 과정에서 유출자와의 부적절한 합의, 증거의 은닉·변형 등 증거의 효용을 해하는 행위를 하였거나, 조사·수사 과정에서 사실과 다르거나 수사기관의 판단을 오인·혼동케 할 정도의 허위·과장된 진술을 하였다면, 경우에 따라 형사책임도 문제될 수 있다.

미국에서도 유사한 사례가 존재한다. Uber는 2016년 해커에 의해 약 5,700만 명의 개인정보가 유출되는 사건을 겪었는데, 당시 회사는 해커들에게 데이터를 삭제하고 외부에 유출 사실을 알리지 않는 조건으로 10만 달러를 지급하면서 이를 버그바운티(Bug Bounty)[13]에 따른 보상인 것처럼 처리하였다. 미국 법원은 당시 해당 사안을 담당하였던 Uber 수석 보안 책임자에 대해, 연방거래위원회(FTC)의 조사 절차를 방해하고 중대한 범죄 사실을 은폐하였다는 이유로 사법방해(Obstruction of Justice)와 중범죄 은폐(Misprision of a Felony) 혐의를 인정하여 유죄를 선고하였다.[14]

수사 중에 쿠팡이 스스로 유출자를 특정하고 신고·자료 제출에 앞서 자체적으로 포렌식을 실시한 이유는 무엇인지, 포렌식이 진술을 전제로 범위를 한정하여 이루어진 것은 아닌지, 정부 및 수사기관의 조사 결과가 나오기 전에 이를 대외적으로 공지한 필요성과 정당성은 무엇이었는지, 이러한 의사결정은 누구에 의해 이루어졌는지, 그리고 정부·수사기관이 쿠팡이 자체 포렌식한 원본 자료를 동일한 상태로 확보하고 있는지에 대한 확인이 요구된다.

5. 피해자 배상 방식

현행 「개인정보 보호법」은 개인정보 유출 등 법령 위반에 대해 손해배상 책임을 규정하고 있다. 그리고 손해배상의 원칙적인 방식은 '금전'을 통한 배상이다. 물론 예외적으로 금전이 아닌 수단에 의한 배상도 가능하나, 어디까지나 피해자의 자유로운 의사에 기초한 선택을 전제로 한다.

그런데 이번 사고에서는 보상이라는 명목하에 금전이 아닌 구매이용권이 지급되었으며, 이러한 방식에 관하여 피해자의 의사를 확인하는 절차는 없었다. 이는 쿠팡이 금전을 통한 배상책임을 사실상 회피하면서, 피해자로 하여금 원치 않는 방식으로 배상을 수용하도록 유도한 것은 아닌지, 나아가 보상을 계기로 소비자를 다시 거래관계로 유인하려 한 것인지 의혹을 불러왔다.

향후 국정조사 과정에서는 배상 방식의 적절성에 대한 검토와 함께, 구매이용권 지급 방식을 원치 않는 피해자, 혹은 사고 이후 서비스를 탈퇴한 피해자에 대한 별도 배상 가능성이나 그 계획에 대해 점검해볼 필요가 있다.

4. 개인정보 위험에 익숙해지는 한국

쿠팡 사태는 권한 없는 자가 국민의 약 65%에 해당하는 개인정보에 실제로 접근하였다는 사실만으로도 중대한 사안이며, 그 자체로 국가 안보와 사회 안전에 연쇄적 영향을 미칠 수 있는 위험을 내포하고 있다. 특히 국가 차원의 조사와 수사가 진행 중인 상황에서 기업이 자체 조사를 실시하고 그 결과를 대외적으로 공표한 행위는 사건의 성격과 책임 구조를 고려할 때 엄중한 평가의 대상이 된다. 그럼에도 불구하고 쿠팡이 상장된 미국 자본시장에서는 이번 사태가 기업 가치에 미치는 영향이 제한적일 것이라고 분석하며, 한국 소비자들이 개인정보 유출 사고에 상대적으로 익숙하다는 점을 언급하였다.[15] 이러한 시각이 고착화될 경우 반복되는 대규모 유출과 규제의 틈새를 이용하는 행위가 사실상 용인되는 구조로 이어질 우려가 있으므로 이를 방지하기 위한 대응이 필요하다.

「이슈와 논점」은 국회의원의 입법활동을 지원하기 위해 최신 국내외 동향 및 현안에 대해 수시로 발간하는 보고서입니다.

13) 윤리적 해커가 기업의 보안 취약점을 제보하고 보상받는 제도를 말한다.

14) U.S. Department of Justice. Northern District of California, Former Chief Security Officer Of Uber Convicted Of Federal Charges For Covering Up Data Breach Involving Millions Of Uber User Records, 2022. 10. 5.

15) KBS뉴스, "JP모건, 개인정보 유출 '쿠팡' 잠재적 고객이탈 제한적일 것", 2025. 12. 2.

07233 서울시 영등포구 의사당대로 1 국회입법조사처
Tel. 02-6788-4510
발간등록번호 31-9735044-001340-14
ISSN 2005-744X