

쿠팡 사태와 규제 신뢰의 시험대

쿠팡을 둘러싼 개인정보 유출과 규제 논란은 이제 한 기업의 위법 여부나 과징금 규모만의 문제가 아니다. 이 사건은 한국의 디지털 규제체계가 소비자에게는 충분한 보호를 제공하면서, 기업과 투자자에게는 공정하고 예측 가능한 제도로 인식되는지 묻는 시험대가 됐다.

8 월 31 일 CNBC 보도는 사태의 성격이 달라졌음을 보여준다¹. 보도에 따르면 미국 의회와 쿠팡 투자자들은 한국 정부의 조치가 미국계 기업에 대한 차별적 규제일 수 있다는 문제를 제기하고 있으며, 미국무역대표부(USTR)의 Section 301 조사와 추가 관세 가능성까지 거론하고 있다. 아직 공식 조사가 시작되거나 관세 조치가 결정된 것은 아니다. 그러나 국내 규제 사건이 한미 통상 현안의 언어로 번역되기 시작했다는 사실만으로도 한국은 이를 가볍게 볼 수 없다.

물론 개인정보 보호는 통상 마찰을 우려해 양보할 영역이 아니다. 플랫폼 기업이 수천만 이용자의 데이터를 다루는 만큼 보안 의무를 소홀히 하거나 사고를 은폐했다면 엄정한 책임을 물어야 한다. 외국계 기업이라고 해서 한국 법의 예외가 될 수도 없다. 소비자 보호는 정부의 가장 기본적인 책무다. 그러나 강한 규제와 좋은 규제는 다르다. 좋은 규제는 처벌의 크기로 평가되지 않고, 실제 피해와 기업 책임에 맞는 억제 효과를 만들었는지로 평가된다. 데이터 유출 사건에서 중요한 것은 단순히 영향 가능 인원이 몇 명인가가 아니다. 어떤 개인정보가 노출됐는지, 실제 외부 반출과 보관·악용이 있었는지, 기업이 사전에 합리적인 보안조치를 했는지, 사고를 발견한 뒤 얼마나 신속히 통지·통제·보상·재발방지에 나섰는지를 함께 따져야 한다.

쿠팡 사건에서 한국 정부와 미국 의회 측의 설명이 크게 엇갈리는 것도 이 때문이다. 한국 정부는 약 3,755 만 명의 이용자가 영향을 받았다고 본 반면, 미국 하원 법사위원회 공화당 측 보고서는 전직 직원이 실제로 보관한 정보가 약 3,000 개 계정 수준이었다고

¹ Papp, J. (2026, August 31). *Coupang dispute fuels new U.S. tariff pressure on South Korea*. CNBC. <https://www.cnbc.com/2026/08/31/coupang-south-korea-us-tariffs.html>cnbc

주장했다. 이 차이는 누가 옳으냐는 정치적 공방에 앞서, ‘접근 가능성이 있었던 데이터’, ‘실제로 반출된 데이터’, ‘제 3 자가 보관하거나 악용한 데이터’를 규제기관이 명확히 구분하고 설명해야 한다는 과제를 제기한다.

제재는 예방을 유도해야지, 기업의 존속을 위협하는 방식의 응징이 되어서는 안 된다. 기업이 기본 보안의무를 무시하거나 침해를 은폐했거나 조사에 비협조적이었다면 강한 제재가 정당하다. 그러나 충분한 예방 노력에도 불구하고 고도화된 공격이나 내부자 일탈이 발생했고, 기업이 신속한 통지와 피해 구제, 재발방지 조치를 취했다면 제재 역시 달라져야 한다. 모든 유출을 동일한 중과실로 간주하면 기업은 보안투자보다 법적 위험 회피에 더 많은 자원을 쓰고, 침해 사실의 신속한 공개도 위축될 수 있다. 이는 결국 소비자 보호라는 규제의 본래 목적을 약화시킨다.

문제는 제재의 비례성에 그치지 않는다. 기업과 투자자, 외국 정부가 조사와 처분의 과정이 불투명하거나 선택적으로 적용됐다고 의심하는 순간, 법집행은 통상 분쟁의 소재가 된다. 한국은 과거 공정거래 사건에서도 이 문제를 경험했다. 미국은 2019 년 한미 자유무역협정에 따라 한국의 경쟁법 행정절차를 놓고 협의를 요청했고, 한국은 이후 피심사인의 증거 접근과 처분 사유 고지 등을 보완했다. 이 경험은 절차적 공정성이 국가의 규제주권을 약화시키는 것이 아니라, 오히려 정당한 법집행을 외부 압력으로부터 지키는 장치임을 보여준다.

최근 한미 통상협의를 반도체, 조선, 대미 투자, 공급망 재편 및 관세 문제와 긴밀히 연결돼 있다는 점에서 쿠팡 사태의 파장은 더 클 수 있다. 2026 년 9 월 현재 양국은 한국의 대미 반도체 투자와 관세 대우를 둘러싼 협의를 이어가고 있으며, 한국은 경쟁국보다 불리하지 않은 조건을 확보하려 하고 있다. 이런 상황에서 특정 미국계 기업을 둘러싼 규제 분쟁은 단지 개인정보 사건으로만 읽히지 않는다. 한국 시장의 개방성, 규제 예측 가능성, 그리고 한미 경제협력의 신뢰를 가늠하는 상징적 사건으로 해석될 가능성이 있다.

한국이 택해야 할 길은 분명하다. 미국의 통상 압박에 밀려 규제를 완화할 필요는 없다. 그러나 정부는 쿠팡 사건의 사실관계와 과징금 산정 근거, 기업의 방어권 보장 여부,

유사 사례와의 비교 기준을 국내외에 투명하게 설명해야 한다. 영향 가능 인원과 실제 피해를 구별하고, 제재가 억제를 위한 것인지 응징을 위한 것인지 분명히 해야 한다.

규제 주권은 외부 비판을 무시하는 데서 나오지 않는다. 누구에게나 같은 기준을 적용하고, 그 기준을 증거와 절차로 입증할 수 있을 때 비로소 규제 주권은 설득력을 얻는다. 쿠팡 사태는 한국이 개인정보 보호와 투자 신뢰 사이에서 선택해야 한다는 뜻이 아니다. 소비자를 보호하면서도 공정하고 예측 가능한 규제국가가 될 수 있는지, 바로 그 역량을 보여줄 시험대다.

The Coupang Controversy and the Stress Test of Regulatory Credibility

The controversy surrounding Coupang's alleged personal-data breach and the ensuing regulatory response has evolved beyond an inquiry into the legality of a single company's conduct or the size of a potential administrative penalty. It has become a broader test of whether South Korea's digital regulatory framework can provide effective protection for consumers while remaining fair, predictable, and credible in the eyes of businesses and investors.

A CNBC report published on August 31 indicates that the matter has acquired a new dimension². According to the report, members of the U.S. Congress and Coupang investors have raised concerns that the South Korean government's actions may constitute discriminatory regulation of a U.S.-affiliated company. The possibility of a Section 301 investigation by the Office of the United States Trade Representative (USTR), as well as the imposition of additional tariffs, has also been raised. No formal investigation has been initiated, nor has any tariff measure been determined. Nevertheless, the fact that a domestic regulatory dispute is beginning to be framed in the language of U.S.–Korea trade relations are significant and should not be treated lightly by Seoul.

Personal-data protection, of course, is not an area in which regulatory standards should be relaxed merely to avoid trade friction. A platform company entrusted with the data of tens of millions of users must be held accountable if it fails to meet fundamental security obligations or attempts to conceal a breach. Foreign-affiliated companies cannot be exempt from Korean law. Protecting consumers remains one of the government's most basic responsibilities.

At the same time, regulatory severity should not be conflated with regulatory quality. Sound regulation is not measured by the magnitude of punishment alone, but by whether it produces deterrence proportionate to the actual harm suffered and to the company's degree of responsibility. In a data-breach case, the critical issue is not simply the number of individuals who may have been affected. Regulators must assess the nature of the personal information exposed; whether data were in fact extracted, retained, or misused by outside parties; whether the company

² Papp, J. (2026, August 31). *Coupang dispute fuels new U.S. tariff pressure on South Korea*. CNBC. <https://www.cnbc.com/2026/08/31/coupang-south-korea-us-tariffs.html>cnbc

had implemented reasonable security safeguards in advance; and how promptly it notified affected individuals, contained the incident, provided remedies, and adopted measures to prevent recurrence.

This is also why the accounts offered by the South Korean government and by U.S. congressional Republicans diverge so substantially in the Coupang matter. The Korean government has stated that approximately 37.55 million users may have been affected. By contrast, a report issued by Republicans on the U.S. House Judiciary Committee has asserted that the information retained by a former employee involved only approximately 3,000 accounts. Before this discrepancy becomes the subject of a political contest over which account is correct, it raises a more fundamental regulatory question. Authorities must clearly distinguish among data to which access may have been possible, data that were exfiltrated, and data that were subsequently retained or misused by third parties.

Sanctions should promote prevention rather than become punitive measures that threaten a company's continued viability. Strong penalties are warranted where a company has disregarded basic security obligations, concealed an incident, or failed to cooperate with an investigation. However, the regulatory response should differ where a sophisticated cyberattack or employee misconduct occurred despite substantial preventive efforts, and where the company acted expeditiously to notify affected individuals, mitigate harm, provide relief, and prevent recurrence. If every breach is treated as equivalent evidence of gross negligence, companies may divert resources from security investment toward the management of legal risk. Prompt disclosure of incidents may also be discouraged. Such an outcome would ultimately undermine, rather than advance, the purpose of consumer protection.

The concern extends beyond the proportionality of penalties. Once companies, investors, or foreign governments conclude that investigations and enforcement actions are opaque or selectively applied, domestic law enforcement can become a source of international trade conflict. South Korea has encountered a comparable issue in the area of competition law. In 2019, the United States requested consultations under the Korea–U.S. Free Trade Agreement concerning administrative procedures in Korean competition-law enforcement. South Korea subsequently enhanced procedural safeguards, including respondents' access to evidence and notice of the

grounds for administrative dispositions. That experience demonstrates that procedural fairness does not erode regulatory sovereignty. Rather, it strengthens the legitimacy of enforcement and helps insulate lawful regulatory action from external pressure.

The implications of the Coupang controversy may be particularly consequential because recent U.S.–Korea trade consultations are closely linked to semiconductors, shipbuilding, investment in the United States, supply-chain restructuring, and tariff policy. As of September 2026, the two governments remain engaged in discussions concerning Korean semiconductor investment in the United States and the tariff treatment associated with it, while Seoul seeks to secure terms no less favorable than those available to competing countries. In this context, a regulatory dispute involving a particular U.S.-affiliated company is unlikely to be viewed solely as a personal-data matter. It may also be interpreted as a symbolic measure of the openness of the Korean market, the predictability of its regulatory environment, and the durability of trust in U.S.–Korea economic cooperation.

The appropriate course for South Korea is therefore clear. It need not dilute its regulatory standards in response to trade pressure from the United States. However, the government should provide a transparent explanation, both domestically and internationally, of the factual basis of the Coupang case; the methodology used to calculate any administrative penalty; the extent to which the company's rights of defense were protected; and the criteria used to compare analogous cases. It should distinguish clearly between the number of individuals potentially affected and the scope of actual harm, and it should articulate whether the purpose of any sanction is deterrence or retribution.

Regulatory sovereignty is not secured by disregarding external criticism. It acquires legitimacy only when the same standards are applied consistently to all parties and when those standards can be substantiated through evidence and fair procedure. The Coupang controversy does not require South Korea to choose between the protection of personal data and the preservation of investor confidence. Rather, it presents a test of whether the country can demonstrate its capacity to achieve both: to protect consumers while maintaining a regulatory system that is fair, predictable, and worthy of trust.