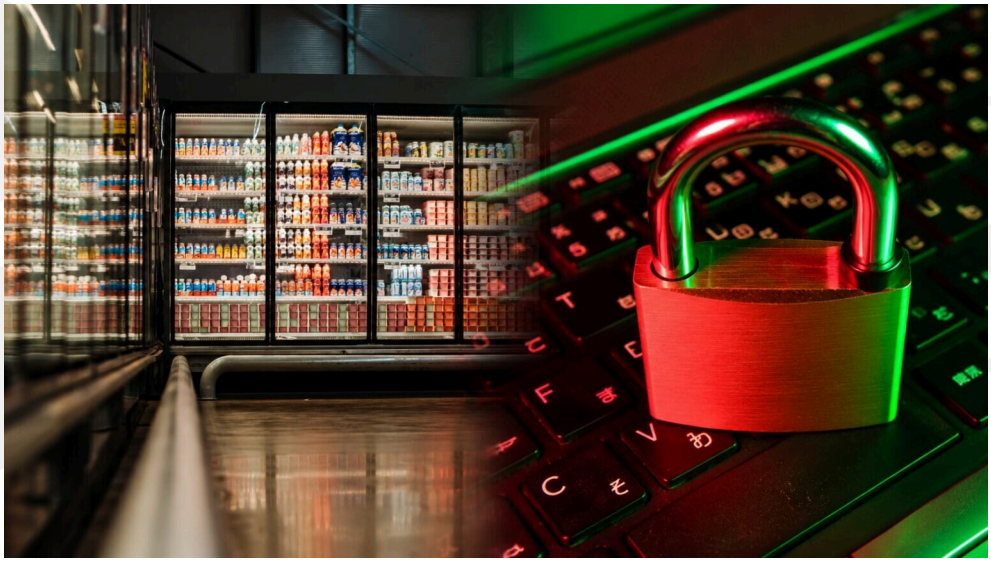
Cyberattack on French supermarkets exposes cross-border cybersecurity risks in Europe

14 OCTOBER 2026

Bruna De Carvalho Santos Pineschi



Illustrative composite image depicting cybersecurity threats to the European retail sector. Images adapted from photographs by Edu Schades Soares (Pexels) and flyD (Unsplash).

On 11–12 October 2026, hackers remotely seized Danfoss refrigeration controllers at hundreds of French supermarkets, causing defrost cycles and temperatures up to 50 °C. The Paris prosecutor called it a "large-scale" attack, causing food losses and fires in more than 400 stores. Prime Minister Lecornu tasked ANSSI with investigating. His office said France was coordinating with European counterparts. A Sekoia analyst told Reuters Spain, Portugal, Poland, Germany and Belgium were also affected. No one is responsible yet. Forbes said AI involvement remains unclear, though experts warn AI is increasing the "speed and scale" of cyberattacks.

This attack raises unanswered questions. Who was responsible for the attack? Did the attack come from outside France? What was the motivation? Why did the attack target supermarket fridges? Are more attacks coming?

The answers could help determine responsibility. If a foreign state or state-backed group is behind the attack, it raises issues of sovereignty and state responsibility under international law. If not, liability will depend on private law. Retailers could sue the Danish manufacturer in France, while claims against installers may be contractual. In this case, Danfoss's statement that most of the units hit had "*reached end of life and no longer receive software or security updates*" will likely help in deciding who bears the risk.

Looking ahead, the reporting obligations of the Cyber Resilience Act have been applied since September 2026. The core obligations will start only in December 2027. France has been referred to the Court of Justice for not transposing NIS2. Additionally, while there is nothing, until now, connecting this attack with AI, CrowdStrike recorded an 89% annual rise in operations by AI-enabled attackers. So, if AI tools continue to make cyberattacks cheaper and faster, the real test will be whether governments and businesses can continue protecting services and critical infrastructure before the next attack.

EPIS