IRSEM
INSTITUT DE RECHERCHE STRATÉGIQUE DE L'ÉCOLE MILITAIRE

www.irsem.fr

Strategic Brief - 70

June 3, 2024

Extension of the FISA Law

European "digital sovereignty" far from American concerns

CLOTILDE BÔMONT

The extraterritorial scope of certain US laws allows intelligence agencies to access the data of European citizens and organizations without their consent, disregarding EU regulations and running counter to European "digital sovereignty". Sharply criticized on both sides of the Atlantic, the extension of the FISA law passed at the end of April 2024 is an impediment to EU-US cooperation in the digital domain just before the European and US elections.

The boom in generative AI, disinformation campaigns, the increase in government-backed cyberattacks from Russia (APT28, APT29) and China (APT31), content regulation, and platforms accountability... In light of these current issues, the renewal of the US FISA law at the end of April 2024 went relatively unnoticed in France. Yet, on the eve of European and American elections, this measure concerning the gathering of digital data raises broader questions about transatlantic cooperation in a context of reassertion of European "digital sovereignty."

Enacted by the US Congress in 1978, the Foreign Intelligence Surveillance Act (FISA) governs the physical and electronic surveillance of foreign individuals and corporations, both on US soil and abroad. Following numerous breaches of privacy and data security of American citizens, particularly under the mass surveillance program Stellar Winds, and in order to legalize the actions of the US intelligence services, the law was amended in 2008. Section 702 of the amendment states that US intelligence agencies can require communications and digital services operators to provide them with any data they deem useful, without necessarily needing a warrant. It specifies that this measure cannot target US nationals. While FISA was set to expire in December 2023, its validity was extended by a few months by US President Joe Biden before the Senate voted for its two-year renewal on April 20, 2024.

Defended by the Biden administration, the bill sparked heated debates in the United States, crossing divisions between Republicans and Democrats. While some argued the law's usefulness for national security and the fight against terrorism, especially in the context of Sino-American rivalry and conflicts in Ukraine and the Middle East, others denounced serious infringements on individual freedoms. The repeated violations of the law by the Federal Bureau of Investigation (FBI) were particularly criticized, with the Foreign Intelligence Surveillance Court (FISC) – the federal court overseeing compliance with FISA – itself denouncing numerous abuses of the law. Analysts reportedly used Section 702 to access the data of US citizens without a warrant during the Black Lives Matter movements in 2020 and the Capitol riot on January 6, 2021. Former US President Donald Trump himself vehemently accused the NSA and the FBI of abusing the law during the 2016 presidential election to harm his campaign, and harangued his supporters on his social network Truth Social on April 10, 2024, calling to "kill FISA."

The rejection of proposals to better regulate data seizure also angered the law's opponents. In mid-April, the House of Representatives narrowly rejected a provision requiring a warrant for investigations indirectly involving US nationals (such as in an exchange between a surveilled foreign person and an American citizen).

Finally, the law's tightening was another point of contention. Two amendments extend Section 702 to foreign travelers on US soil and to international drug traffickers. A third, more controversial, amendment updates the definition of communications and services operators.

Although the FISC emphasized the need to adapt this definition to technological changes, the new definition is considered too broad by various stakeholders, including major digital industries. It now includes any entity "with access to equipment that is or can be used to transmit or store wired or electronic communications." This significantly broadens the range of companies, organizations, or even individuals falling within the scope of the law, as simply providing a Wi-Fi connection theoretically meets this definition. However, dwellings, public establishments, and commercial catering and accommodation establishments are excluded.

In Europe, the renewal of FISA has not been well received either. Alongside the Patriot Act passed in 2001 and the CLOUD Act adopted in 2018, it is one of the US laws directly threatening the security of European data. Their extraterritorial reach allows the US government to compel American digital services companies to provide their costumers' data, even if it never leaves European soil. Given the oligopolistic state of the market, the major US digital companies almost inevitably intervene in the value chains of digital services, thus exposing a large portion of European data to US intelligence agencies. These provisions not only limit Europeans' control over their data but also conflict with EU regulations, starting with the General Data Protection Regulation (GDPR). While measures have been proposed within the EU to limit the impact of such laws, they do not always achieve consensus. This was demonstrated by the debates on the European cloud service certification scheme (EUCS), the second version of which included a clause guaranteeing that offers certified to the highest security level would not be subject to non-European jurisdictions. Although this clause was removed from the latest version of the text, FISA's renewal may reignite discussions.

Moreover, FISA's renewal highlights the ambivalence of the Euro-American relationship on digital matters. It comes shortly after the signature on July 10, 2023 of a new data transfer agreement between the US and the EU (the Data Privacy Framework, DPF). This agreement is the third of its kind, the Safe Harbor and the Privacy Shield having been invalidated by the Court of Justice of the European Union (CJEU) in 2015 and 2020 on the grounds that they insufficiently ensured the protection of Europeans' personal data. The European Commission had already faced heavy criticism in March 2022, when the agreement in principle on the DPF was announced. In particular, Commission President Ursula von der Leyen was accused of yielding to US pressure, as the US leveraged the argument of the war in Ukraine and European security to push for the adoption of the DPF when the EU had been standing firm against Washington for nearly two years. By signing the DPF without obtaining solid guarantees on European data security while FISA was nearing its end, the EU seems to have lost its leverage to demand a revision of the American law.

The US decision on FISA also bodes ill for the future of the EU-US Trade and Technology Council (TTC), whose effectiveness is increasingly questioned. Established in 2021, the TTC helped revive transatlantic dialogue after Donald Trump's presidency, attesting to the will for bilateral cooperation and the many shared economic and strategic interests. However, the defense of its national interests sometimes leads Washington to neglect its European partner. By unilaterally adopting measures such as the Inflation Reduction Act (IRA), controls on semiconductor exports to China, sanctions against the telecoms company Huawei and the tightening of the FISA law, without considering the impact on the EU, the US shows that the US-EU relationship is not a priority on its agenda.

Thus, although the opposition to FISA's renewal in the US seems to converge with European interests, it should be borne in mind that it is primarily driven by domestic concerns. FISA's tightening is a powerful reminder of the need for the EU to assert itself vis-à-vis its American ally and to reduce its structural dependence on the US. Despite real progress in European "digital sovereignty" over the last five years, the EU still needs to accelerate the development of its industrial and R&D capacities and make the preservation of its market a priority. The June 2024 elections are an opportunity to (re)define the ambitions of European digital policy. ■

Clotilde Bômont *is a researcher in digital geopolitics (IRSEM).*

Contact : clotilde.bomont@irsem.fr