The Contradiction of EU Tech Governance

27 MAY 2026

Giovanni De Pellegrini and Jorge Rey Higueras



The proliferation of technology companies, together with the establishment of stricter regulations governing them, has pushed States to develop new ways of ensuring that these enterprises operate within the limits of the law. Given the extensive processing of personal data carried out by these companies, and the importance of protecting such data, it is essential to strengthen the regulations applicable to them. One of the mechanisms adopted by the EU has been the protection of whistleblowers. Having become a controversial topic over the last decade, whistleblowers are individuals who report inappropriate or unlawful behaviour within a

company. Therefore, considering the significant data-processing activities conducted by technology companies, it is crucial to protect whistleblowers within these employment relationships so that any improper conduct can be effectively investigated and prosecuted.

1.1 The need for accountability

In recent decades, there have been notable developments in regard to how much power digital technologies have gained in Europe to provide people with certain information, allow them to communicate, and gather their data. Consequently, the European Union began attempting to position itself as a global leader in digital governance through regulations, with the aim of increasing transparency and accountability in the tech sector.

Digital platforms continue to increase their influence over societies and democratic life, and insufficient oversight can generate public concerns over transparency, the power possessed by tech companies, and the institutional effectiveness of regulatory oversight. This fact demonstrates that tech companies cannot be automatically seen as private businesses providing neutral services anymore. However, regulation by itself remains an insufficient policy and tool: independently from the expansion of the European regulatory framework, effective accountability can result as a difficult target to achieve due to the presence of opacity within digital platforms and the limited access regulators have to internal corporate practices.

1.2 The opacity in tech companies and the role of whistleblowers

Despite the expansion of European digital regulation, effective oversight of technology companies remains difficult because major digital platforms operate through highly opaque systems. Major examples of such systems include algorithms used for recommendation systems, targeted advertising, and content moderation usually proprietary, which means companies rarely disclose the full functioning of their digital infrastructures to the public and regulators. Frank Pasquale's *The Black Box Society* argues that the digital economy and other contemporary digital systems function as "black boxes", environments where decision-making processes remain inaccessible despite their significant impact on societies, politics, and policies. In addition, some of the most relevant activities in the contemporary technological world, such as AI training and data collection practices, are characterized by remaining frequently difficult to verify externally, particularly when commercial and industrial secrecy or intellectual property are invoked. In this context, whistleblowers become particularly important in providing internal information inaccessible to public authorities and society. Their exposure of hidden practices and malpractices, internal research, and failures in governance contribute to reducing information asymmetry between tech companies and the public. Kate Kenny's book *Whistleblow-*

ing: Toward a New Theory argues that whistleblowing should be understood not only as an individual act of dissent, but also as a mechanism capable of strengthening democratic accountability within opaque environments.

1.3 Public trust and democratic legitimacy in digital governance

Digital governance relies heavily on trust in the transparency of technologies as well as their governance being democratic. As observed by the OECD in its reports on digital trust and AI governance for the period 2021-2024, public trust in digital technologies depends strongly on such aspects as transparency and accountability. However, a lack of accountability may increase distrust in both tech firms and regulatory authorities. Concentrating informational power within major digital platforms, combined with limited access to internal corporate practices, may contribute to the creation of a public perception that sees tech companies operating beyond democratic control. Consequently, there is a danger that such covert activity, inadequate regulation, and ineffective systems of accountability may become part of wider problems of public mistrust and technological disfranchisement. Within this scenario, whistleblowing takes on special democratic importance, as it uncovers information which would otherwise be unavailable to both regulatory authorities and the public. This process of uncovering and increased transparency serves not only corporate accountability, but also democratic legitimacy.

2. The EU Whistleblower Protection Framework.

The European Union's framework regarding whistleblower protection is relatively recent, despite the different corruption scandals that have surrounded European countries over the last two decades.

Until 2019, EU members could only rely on the Recommendation of the Committee of Ministers to member States on the protection of whistleblowers, adopted by the Council of Europe. Even if Recommendation (2014)7 established some guidelines that helped States shape their internal regulations, the lack of binding force affected whistleblowers, as no protection was guaranteed to them.

According to Abazi (2020), different factors influenced the delay in the establishment of the primary EU framework on the subject. Firstly, the European Commission was uncertain about its capacity to enact regulation, as whistleblower protection affects some sensitive Member States' competences. In addition, the absence of the term "whistleblower" in multiple national languages was conceived as a barrier to this intended harmonization.

2.1. General Explanation of the Framework.

The European Union's framework for protecting whistleblowers consists of the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law. This Directive establishes a policy of minimum standards that EU members can expand should they wish to do so.

As explained by the Directive, "persons who work for a public or private organisation or are in contact with such an organisation in the context of their work-related activities are often the first to know about threats or harm to the public interest which arise in that context". In this way, their reports are highly beneficial for safeguarding society as a whole.

The Directive applies directly to workers, whether their labour relationship is on the verge of commencing, is currently ongoing, or has already ended. Furthermore, the Directive applies to whistleblowers reporting a closed list of breaches of Union law.

Important guidelines included in the Directive are the triangular system of reporting – internal, external, and public disclosures – as well as the need to safeguard the confidentiality of whistleblowers. Moreover, the regulation obliges States to adopt protective measures to prevent retaliation.

2.2 Uneven Implementation across EU Member States.

Considering the harmonization purpose of the Directive in ensuring minimum standards for the protection of whistleblowers across EU member States, it is pertinent to analyse the implementation by Member States and the transposition into national laws. Evidence has shown that implementation has varied between countries and, indeed, demonstrates that protecting whistleblowers was not truly a priority.

The Report from the Commission to the European Parliament and the Council on the implementation and application of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of law argues that only three countries were able to adopt legislation by the transposition deadline of 21st December 2021: Malta, Portugal, and Sweden. In contrast, eight countries did so in 2022 and thirteen in 2023. Meanwhile, the European Commission opened infringement proceedings in 2022 against those 24 members, and six of them were referred to the Court of Justice of the European Union. Belgium, Poland, and Estonia were the last countries to adopt proper regulations for whistleblower protection.

In the meantime, Transparency International has published an analytical report in 2026, *How effective is whistleblower protection in the EU? Trends, gaps, and emerging practices across member states*. The report argues that the key differences in European regulations protecting whistleblowers have been provoked by delayed and unequal transposition. Indeed, significant differences remain between EU members.

In this fashion, and as a matter of fact, while countries such as Greece, Ireland, Luxembourg, Slovakia, or Spain have channeled newly submitted reports through newly created bodies, other countries such as Belgium, Croatia, and France have relied on already existing Human Rights organisations, whereas Austria, Italy, and Romania have opted for anti-corruption agencies. Diverse policies are also present in the fight against retaliation. Some countries – such as Spain – prefer to guarantee full compensation for damages, whereas others provide only economic restitution.

2.3. Limits of practical enforcement and corporate pressure.

Despite the advances made in recent years, the situation for whistleblowers may not be as encouraging as presumed. A survey conducted by Transparency International in December 2021, days before the transposition deadline, showed that 45% of EU citizens were reluctant to report corruption due to fear of retaliation.

The information obtained by Transparency International is in line with the data provided by the Special Eurobarometer 534: Citizens' attitudes towards corruption in the EU in 2023. Even though this Eurobarometer analysed corruption in general, its data helps to assess the level of effectiveness of whistleblower regulations in European countries. According to the survey, 80% of the respondents who alleged having experienced corruption did not report it. Furthermore, 54% argued that they would not know where to report corruption. Finally, 47% identified the difficulty of proving anything as the main reason preventing them from reporting corruption. Whistleblower protection is essential to ensure that inappropriate acts and corrupt practices are properly reported. If citizens do not know where to report them, fear may become a barrier to uncovering such acts.

In addition, the aforementioned report from Transparency International shows that penalties for retaliation in European countries are highly diverse. Fines range between 15 and 8.000 euros in countries such as Bulgaria, Croatia, Latvia, or Romania, while Spain considers fines of up to 1.000.000 for corporate organisations. Besides, some countries have also established criminal offences for those engaging in retaliation against whistleblowers, but in practice, these legal provisions have rarely been utilised. While the EU Directive establishes examples of retaliation, in reality, workers may experience different forms of reprisals, as enterprises possess significant capacity to pressure them. Hence, it is essential to impose penalties against retaliation, as this could prevent possible corporate pressure.

3. The Contradiction of EU Tech Governance

3.1 How insufficient protection undermines accountability in the European tech sector

In another respect, technological companies customarily process large amounts of personal data, affecting thousands of European citizens. Therefore, as they manage highly sensitive issues, it is essential to ensure that misconduct is exposed.

3.2 Risks for democratic legitimacy and public trust

Whistleblower protection deficiencies can result in extensive risks related to the issue of corporate accountability and go beyond the problem of legitimization of digital governance at the EU level. Today, the European Union positions itself as a global regulator of digital technologies thanks to measures such as the Digital Services Act and the Artificial Intelligence Act. The validity of these regulatory acts relies on the ability to maintain transparency and effective oversight in relation to tech companies.

Whistleblowers are critical to making sure that the power imbalance between the companies, regulators, and citizens does not persist due to the lack of necessary information. Whistleblower protection deficiencies may discourage potential informants from exposing wrongdoings happening within the environment in which they operate. Whistleblowers become essential sources of information capable of reducing informational asymmetries between corporations, regulators, and citizens, and without adequate protection policies, employees will be afraid of possible retaliation and less likely to report wrongdoings or illegal activities. This might help to build a negative public opinion regarding the fact that tech companies act outside of the democratic process, and the regulations cannot be enforced effectively by any regulatory bodies.