fypl french yearbook *of* public law
Issue 2, 2024

Administering Truth[1]

Philippe Cossalter
Full professor of French public law, Saarland University

Abstract:

This article examines the State's role in administering truth within both the legal and digital spheres. Drawing on historical and philosophical reflection, it traces the distinction between reality and truth, the latter as a legal construct ascertained through evidence and proof. The State emerges as a *trusted third party* charged with both establishing and safeguarding truth — a function that the digital age has simultaneously reinforced and destabilised.
Analysing both French and European regulatory frameworks—the GDPR, the eIDAS Regulation and national cybersecurity directives—the paper first examines how truth is constituted through digital identity (§ I). Within these frameworks, the State certifies the reliability of identities and secures the integrity of transactions; digital identity accordingly becomes a new dimension of public order, sustained by an evolving regime of administrative policing.
The article then turns to measures to restore truth against content manipulation (§ II), examining successive French legislative responses alongside EU instruments including the AI Act, the Digital Services Act and the Digital Markets Act. Further analysis unveils the tension between ambitious regulatory objectives and the limited efficacy of enforcement mechanisms, particularly against State-sponsored disinformation campaigns and AI-generated synthetic content.
The contribution ultimately situates these developments within the broader divergence over the regulation of digital content, interrogating the capacity of French and European legal frameworks to sustain the State's truth-administering function in an era of systemic disinformation.

Keywords:

Administration of truth, Digital identity, Content manipulation, Administrative policing
The reliefs of the Abu Simbel temple depict the overwhelming victory of Egypt under

1 Article originally published in French in the Revue française de droit administratif.
Cossalter P., 'Administrer la vérité', *RFDA*, 2025, no. 2, p. 233. See also, published concurrently in French under the same title: Auby J.-B., 'Administrer la vérité. Les institutions publiques, garantes du vrai? ', PubliAdmin, 2025, no. 1.

Ramses II over the Hittite Empire of Muwatalli. Nearly 3300 years later, we know that the victory was on the whole a Hittite one.[2] Yet what matters is neither historical nor military truth; what endures amid the ageless marble of the Nile valley is the political message serving the State, conveyed by the monument itself. Military reality, swiftly swept away by desert sands, thus stands apart from historical truth.

According to Cornu's *Vocabulaire juridique*, truth is 'the intrinsic property of reality'.[3] When this reality is grasped by law, it is established through evidence. Evidence itself is defined as the 'demonstration of the existence of a fact or act in the forms recognised or prescribed by law'.[4] From a philosophical perspective, Thomas Aquinas stated that one must not equate truth with reality. The Scholastics argue that one must distinguish between the reality or truth of things (*veritas rei*) and perceived truth (*veritas intellectus or veritas in cognoscendo*).[5]

Our intention here is not to adopt a philosophical perspective. Regardless of the analytical standpoint we assume, we must acknowledge that *administering truth* consists in securing the integrity of a certain representation of reality, rather than of reality itself. A gap necessarily exists between reality and truth. We shall thus retain the idea that *truth is the legally recognised correlation between material truth—or reality—and perceived truth*. This correlation is established in law through evidence.

The gap between reality and truth runs through the entirety of law. At the judicial level,[6] the device of presumption exemplifies the idea that a measure of judicial truth is needed to ascertain the existence of a right, without there being any need—and often any possibility—to prove the reality of the facts. Therefore, judicial truth asserts itself within a given legal system by virtue of a previously accepted social convention. Examples of this inevitable gap between reality and truth abound: the determination of parentage,[7] the presumption of innocence, the principle that offences and penalties must be prescribed by law.

Taking this further, one may consider that reality has no legal standing unless it is in the interest of the social order to admit a given fact into the domain of truth.

If we accept that law is the body of rules of conduct socially prescribed and enforced by the coercive authority of the State, it becomes possible to draw a close link between truth and the State. The State administers truth insofar as it belongs to the legal order.

The State has historically played a major role in setting out the legal framework governing the relationship between reality and truth. The State—and before it, pre-state

2 Freu, J., Mazoyer, M., *L'apogée du nouvel empire hittite : Les Hittites et leur histoire*, 2008, Paris, L'Harmattan, p. 138 ff.

3 Cornu, G. (ed.), *Vocabulaire juridique*, 13th ed., Paris, PUF, *voce* Vérité.

4 Cornu, G. (ed.), *Vocabulaire juridique*, 13th ed., Paris, PUF, *voce* Preuve.

5 See Lalande, A., *Vocabulaire technique et critique de la philosophie*, 1968, Paris, PUF, *voce* Vérité.

6 Michel Foucault analysed, in terms that are too literary and too far removed from our subject to be reused here, the relationship between law and truth. See Foucault, M., 'La vérité et les formes juridiques', cycle of lectures delivered in 1973 at the Pontifical University of Rio de Janeiro, reproduced in *Dits et écrits*, 2004, Paris, Gallimard, vol. 1, nº 139, p. 1495, and Thirion, N., 'Des rapports entre droit et vérité selon Foucault : une illustration des interactions entre les pratiques juridiques et leur environnement', *Revue interdisciplinaire d'études juridiques*, vol. 70, no. 1, 2013, pp. 180-188.

7 In this regard, the recourse to genetics does not reduce the gap between the reality of the filiation link and its legal recognition. Kalogirou, M., 'Le lien génétique entre deux personnes en droit de la filiation : réalité factuelle, réalité juridique?', *La Revue des droits de l'homme* (Online), 18, 2020, published online 12 June 2020, accessed 20 May 2021. URL: http://journals.openedition.org/revdh/9763; DOI: https://doi.org/10.4000/revdh.9763.

forms of authority—prescribes standards for weights and measures and the computation of time. Currency, its accounting and the trust placed in its value are fundamental state functions. Sovereigns alone possessed the means to commission the first maps of the world; maps are themselves in many respects instruments of power, by virtue of the control they afford over a certain representation of the world.[8]

Before continuing our analysis, we must clarify the term 'administering'. *Administering truth* can bear at least two meanings. In conventional administrative law, the expression refers to the organs and functions through which the State secures an acceptable correlation between the reality of things and perceived truth—and it is this notion that we employ here. The term 'administering' also carries the meaning of 'giving, providing, conferring' (*Dictionnaire de l'Académie française*). From the State's perspective, 'administering truth' would amount to imposing a certain vision of reality. This performative dimension—'administering' as 'enunciating'—was explored in a recent issue of the literary journal *Nouveaux cahiers de marge*.[9] We shall proceed on the former, institutional basis, though the performative aspect is by no means foreign to administrative practice.

Beyond the judicial sphere, the State's intervention in administering truth is contested on political, philosophical, and indeed legal grounds. The debates surrounding memory laws are a case in point: the appropriation by law of a historical truth imposed upon the social order.[10] Where the legislator confines itself to acknowledging a historical fact and characterising it in law, the resulting enactment is non-normative and for that very reason unconstitutional.[11] If, on the other hand, the legislator couples such acknowledgment with a sanction for disputing the historical fact, it disproportionately interferes with freedom of expression and communication.[12] Constitutional case law has in substance denied the legislature—and thereby the State—the possibility of determining historical truth. The exceptions to this prohibition are few and relate essentially to the criminalisation of *Shoah* denial.[13]

Paradoxically, while historians have challenged any role for the State in determining historical truth, those very historians—chief among them Pierre Nora—have devoted a considerable part of their work to collecting and documenting the State's commemorative endeavours.[14] The crafting of the national narrative, so essential to the subjectivist conception of the Nation and to the principle of the indivisibility of the Republic, is an enduring concern of the State. Yet the construction of the national narrative is a proposition, not a compulsion: an ancient form of soft law, or indeed of *nudge*.

By the same token, the preservation of archives falls within the State's responsibilities:

8 Aguilera, T., Artioli, F., Barrault-Stella, L. et al., 'Introduction : Pour une approche pluridisciplinaire des usages politiques des cartes'. Aguilera, T., Artioli, F., Barrault-Stella, L. et al., *Les cartes de l'action publique. Pouvoirs, territoires, résistances*, Presses universitaires du Septentrion, 2021, pp. 9-38.

9 *Nouveaux Cahiers de Marge*, 2021 nº 3, 'Administrer la vérité'.

10 On the relationship between the historian and French law, see: Vivant, C., *L'historien saisi par le droit. Contribution à l'étude des droits de l'histoire*, Dalloz, Nouvelle Bibliothèque de Thèses, 2007, 525 pages.

11 *Conseil constitutionnel* (Constitutional Council), decision nº 2005-512 DC of 21 April 2005, *Loi d'orientation et de programme pour l'avenir de l'école*.

12 *Conseil constitutionnel* (Constitutional Council), decision nº 2012-647 DC of 28 February 2012, *Loi visant à réprimer la contestation de l'existence des génocides reconnus par la loi*.

13 *Loi du 29 juillet 1881, sur la liberté de la presse* (Press Freedom Act), Article 24 bis.

14 Nora, P. (ed.), *Les lieux de mémoire*, 1997, Paris, Gallimard.

source material essential both to the historian's work and to the State's mission of self-preservation through the notion of heritage.[15] Archives are paper-based but also, increasingly, photographic and audiovisual.

The State entertains a third relationship with truth: the comprehension of reality through statistics. The French State has created and still maintains the official body responsible for statistics (INSEE),[16] which operates within a regulatory framework set at European level.[17] The advent of big data appears to be transforming this relationship, or, to put it differently, the era of statistics is giving way to the era of data. The reality of natural and social facts, given the sheer volume of the data at stake and how they are disseminated, is now directly accessible to the general public.

The State has also traditionally shaped the perception of truth—historical, statistical, informational—through school curricula. The very setting of curricular content determines a relationship to history and to its narration that can never be neutral. The national education system is further tasked with educating citizens in critical analysis[18] 'in a society characterised by the proliferation and acceleration of information flows' because 'the development of critical thinking and the capacity of our students to act rationally to seek, receive, analyse and produce information is a matter of the utmost necessity'.[19]

A fifth—and arguably the most immediately relevant—relationship with truth concerns media law. It is in the media sphere that the disruption unleashed by artificial intelligence is most pronounced. Generative AI enables the production of realistic content across all digital platforms, from photographs to video and human voice; it further enables the circulation of such synthetic content through automated means, lending it far-reaching impact.[20] The war of disinformation, in itself nothing new, is becoming an ever more significant dimension of modern conflicts; theorised as information warfare—or *infowar*—it now forms an integral part of the new hybrid wars.[21]

The State will in all likelihood continue to serve as *trusted third party* in the years

15 Duclert, V. (2015), 'L'État et les archives. Question démocratique, réponse constitutionnelle', *Pouvoirs*, nº 153(2), pp. 37-48. https://doi.org/10.3917/pouv.153.0037.

16 *Loi nº 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques* (Law on the Obligation, Coordination and Secrecy of Statistics).

17 Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 on the transmission of data subject to statistical confidentiality, Regulation (EC) No 322/97 on Community statistics and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities.

18 See Article L. 312-9 of the *Code de l'éducation* (Education Code), as amended by Article 7 of *Loi nº 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique* (Law Aimed at Securing and Regulating the Digital Space), whose Article 3 provides for training in 'the risks associated with such tools and with content generated by artificial intelligence, as well as the fight against disinformation'.

19 Referral letter of 27 June 2023, addressed by the Minister of National Education and Youth to the President of the Conseil supérieur des programmes (CSP) requesting the reform of moral and civic education programmes from the first year of primary school to the final year of secondary school.

20 Klen, M., 'La nouvelle guerre de l'information', *Revue Défense Nationale*, 2024 nº 866(1), pp. 94-99. https://doi.org/10.3917/rdna.866.0094.

21 Marine, G., 'Un cyberespace de conflictualité', in Pelopidas, B., Ramel, F. (eds.), *Guerres et conflits armés au XXIe siècle*, 2018, Paris, Presses de Sciences Po.

ahead, but will not go unchallenged in doing so.[22] The term 'trusted third party' is borrowed from information technology, though the concept extends well beyond the digital sphere. In information technology, the *Encyclopedia of Cryptography and Security* defines the trusted third party as 'an entity within a given community that is trusted by all entities in that community to properly perform a particular service'.[23] The advantage of this broad definition is that it encompasses the entire world of electronic transactions in which the trusted third party plays a fundamental role.[24]

The concept of trusted third party also appears to have gained currency beyond information technology.[25] In French law the term surfaces on occasion, even beyond the digital sphere. In tax law, for example, a trusted third party is a member of a regulated profession (lawyer, notary, accountant) responsible for filing documents with the tax authorities on behalf of a taxpayer.[26]

The dematerialisation of transactions has effectively displaced the State from many of the functions through which it establishes truth: cryptocurrencies challenge the State's monopoly on currency;[27] online reviews render official hotel ratings superfluous;[28] identification systems on the Internet rival sovereign identity (see *infra*). The State has lost its role as intermediary in most electronic transactions, and not just commercial ones. This exclusion—or at the very least marginalisation—of the State from its intermediary function takes both direct and indirect forms.

The direct consequence of the State's withdrawal has been the rise of 'trusted third parties' (in a narrower sense), tasked with securing electronic transactions. The State's role was, for example, maintained through ICANN, the institution responsible for the assignment of Internet domain names,[29] which was *de jure* placed under the authority of the US Department of Commerce. The ICANN reform distanced this body from state influence, as a supposed token of neutrality.

A further example concerns freedom of expression, particularly on social networks, increasingly governed by private platforms that counter the State's regulatory claims with their own community standards. Competition from the private sector extends to

22 The *Conseil d'État* (Council of State) expresses this by stating that blockchain is 'the culmination of the disintermediation process' without mentioning the competition with the State's missions. See the report of the *Conseil d'État* (Council of State), *Puissance publique et plateformes numériques : accompagner l'«ubérisation»*, 2017.

23 van Tilborg, H.C.A., Jajodia, S. (eds.), *Encyclopedia of Cryptography and Security*, Springer, 2011, p. 637. DOI: https://doi.org/10.1007/978-1-4419-5906-5_98.

24 Froomkin, A. M., 'The Essential Role of Trusted Third Parties in Electronic Commerce', 75 *Or. L. Rev.* 49 (1996). Michel, A., 'Authentification, identification et tiers de confiance', *Hermès, La Revue*, 2009/1 (nº 53), pp. 127-136. DOI: 10.4267/2042/31488. URL: https://www.cairn.info/revue-hermes-la-revue-2009-1-page-127.htm.

25 '(Re)faire des journalistes des tiers de confiance', *Revue internationale et stratégique*, vol. 115, no. 3, 2019, pp. 7-16. Interview with Christophe Deloire, Interview conducted by Pascal Boniface.

26 See Article 68 of *Loi nº 2010-1658 du 29 décembre 2010 de finances rectificative pour 2010* (Supplementary Budget Act for 2010), which established the *tiers de confiance* (trusted third party) role. The duties of the *tiers de confiance* are defined in Article 170 ter of the *Code général des impôts* (General Tax Code, CGI).

27 Moron Puech, B., Cornaire, J., 'Cybermonnaies et protection de la souveraineté et de la propriété', in Cossalter, P., Guglielmi, G.J. (eds.), *Propriété, souveraineté, mondialisation*, Éditions Panthéon-Assas, 2024.

28 See Article L. 141-2 and L. 311-6 of the *Code du tourisme* (Tourism Code).

29 *Internet Corporation for Assigned Names and Numbers.*

domains as diverse as the identification of companies and even of individuals.[30]

The State's withdrawal also operates indirectly: in certain spheres, the State actually loses any possibility of effective control. Criminal response is a case in point. Minor offences committed online no longer elicit an adequate response. The security of transactions is instead maintained preventively, through community-based certification tools. Abuses of freedom of expression are moderated solely by social networks, which are subject to only the most indirect influence from States.

But States, having allowed unchecked competition to develop in the digital space, are now reclaiming the domain of truth by positioning themselves, in turn, as trusted third parties. Their role is to *establish* truth (I) and, where it appears compromised, to *restore* it (II).

I. Establishing truth

The protection of a 'digital public order'[31] far exceeds the question of truth. Cybersecurity, only tangentially relevant to our subject and therefore lying beyond the scope of the present analysis, is nonetheless one aspect of this new form of public order. The transposition of the NIS2 directive[32] is raising—and will continue to raise—difficult and fascinating questions for public administrations, both as a security actor and, above all, as a frequent target.[33]

But beyond security, truth is essential to the protection of public order in the digital age, first and foremost through the protection of digital identity, which is not merely an extension of identity in the physical world. Digital identity (A) is more broadly central to the trust that citizens may place in economic and non-economic transactions alike (B).

A. Digital identity

The first project in France, and perhaps worldwide, for the creation of a digital identity was the SAFARI project, devised in 1974.[34] Led by the *Institut national de la statistique et des études économiques* (INSEE), SAFARI would have enabled the cross-referencing of information held by the administration on all persons with a social security number, for the purpose of creating a digital identity. Devoid of safeguards and enabling a single author-

30 See among others Alamillo Domingo, I., 'El régimen jurídico de la Administración digital: aspectos tecnológicos, plataformas y servicios de intermediación', in Martín Delgado, I. (ed.), *El procedimiento administrativo y el regimen jurídico de la administración pública desde la perspectiva de la innovación tecnológica*, iustel, 2020, pp. 225-276.

31 See Mouron, P., Piccio, C., *L'ordre public numérique : libertés, propriétés, identités*, 2015, Aix-en-Provence, PUAM. More recently, see *Numérique et ordre public*, *Cahiers de la recherche sur les droits fondamentaux*, 2023 nº 21, https://doi.org/10.4000/crdf.8744.

32 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

33 See the special issue 'Collectivités territoriales et Cybersécurité' edited by Macilotti, G., Saunier, S. in *JCP Administrations et collectivités territoriales* 2024 nº 21.

34 Poulain, C., 'Le projet SAFARI (1970-1974)', *Terminal* (Online), 134-135 | 2022, published online 12 Oct. 2022. URL: http://journals.openedition.org/terminal/8787; DOI: https://doi.org/10.4000/terminal.8787.

ity to consolidate all information concerning individuals,[35] the project was abandoned and gave rise to the *loi informatique et libertés* (Data Protection Act)[36] and to the *Commission nationale de l'informatique et des libertés* (CNIL).

Fifty years later, digital identity has become a fully-fledged component of digital public order and a key safeguard for citizens, as it now benefits from a more developed regulatory framework and complies with the principles laid down by the GDPR.

Digital identity in its modernised version 'is the digital-age continuation of one of the oldest services the State renders to its citizens: securing the right to identity via civil registration and attesting it through the issuance of identity documents'.[37]

While some scholars have proposed granting legal personality and digital identity to AI robots,[38] digital identity is for the time being a means of defence against the potential effects of AI, which is now capable of generating realistic digital avatars of natural persons, or even of fabricating fictitious persons from scratch.

Legal identity is constituted by a number of particulars recorded and attributed at birth pursuant to Article 57 of the Civil Code:[39] the day, time and place of birth, sex, names and surname; these particulars are supplemented by the registration number in the *répertoire national d'identification des personnes physiques* (NIR).[40] Digital identity, for its part, appears to be no more than a projection of legal identity, 'digitalisation being merely a process that allows identity elements to be transcribed onto a digital medium, which in turn allows legal identity to be retrieved'.[41] This unidirectional link between legal identity and digital identity entails focusing on 'sovereign' (*régaliennes*) forms of identity, to the exclusion of identities created for use on private platforms.

Although the concept of digital identity did not feature in legislation until recently, it now stands at the centre of the *Service de garantie de l'identité numérique* (SGIN), introduced by *décret n° 2022-676 du 26 avril 2022* (Decree No. 2022-676 of 26 April 2022).[42] The SGIN enables individuals to obtain a certified digital identity, accessible through the *FranceConnect+* authentication platform. Identity certification is built around what legal scholarship terms 'pivot identity' (*identité pivot*), a minimum set of identifying particulars, no longer including facial recognition, since it was ruled out as an official means of

35 *Le Monde*, 21 mars 1974, Boucher, P., 'Une division de l'informatique est créée à la chancellerie "Safari" ou la chasse aux Français'.

36 *Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* (Data Protection Act).

37 Statement by Valérie Peneau reported in the information report filed pursuant to Article 145 of the *Règlement* (Rules of Procedure), concluding the work of the joint fact-finding mission on digital identity, nº 3190, filed on 8 July 2020.

38 Bensoussan, A., Bensoussan, J., *IA robots et droit*, 2019, Brussels, Bruylant.

39 *Code civil* (Civil Code), Article 57: 'The birth record will state the day, time and place of birth, the child's sex, the forenames to be given to him or her, the family name, followed, where applicable, by a mention of the parents' joint declaration as to the choice made, as well as the forenames, surnames, ages, occupations and residences of the father and mother and, where applicable, those of the declarant. If the child's father and mother, or one of them, are not designated to the civil registrar, no mention of this will be made in the registers'.

40 On all aspects of the identification of natural persons, see Coutort, S., Hennebert, C., Faher, M. (2020), *Livre blanc Blockchain et Identification numérique*, pp. 29 ff.

41 Coutort, S., Hennebert, C., Faher, M. (2020), *Livre blanc Blockchain et Identification numérique*, cited above, p. 31.

42 *Décret nº 2022-676 du 26 avril 2022* authorising the creation of an electronic identification means called 'Service de garantie de l'identité numérique' (SGIN) and repealing *Décret nº 2019-452 du 13 mai 2019* authorising the creation of an electronic identification means called 'Authentification en ligne certifiée sur mobile'.

identification.[43]

While digital identity may be, from the State's perspective, a mere extension of documentary identity into the virtual world, the broader question of identity in the digital sphere has now plainly outgrown this exclusive relationship with the State. The State may be regarded as one trusted third party among many that certify the reliability of an identity. Like numerous private operators, it provides what has been defined as a decentralised digital identity—that is, it acts as a trusted third party in certifying a user's identity.[44]

Contemporary developments in blockchain technology point to the emergence of an alternative means of securing a so-called 'sovereign' or 'self-sovereign' identity: a digital identity independent of any trusted third party.[45] The terminology bears no relation to State sovereignty; the identity the State provides is more aptly described as *régalienne*, pertaining to State prerogatives. These technologies equip individuals with an identity wallet enabling them to prove what they know (qualifications, certifications), what they hold (a bank account, citizenship), what they own (land, a residence), and who they are.[46]

Notably, Regulation (EU) 2024/1183,[47] amending the 2014 eIDAS Regulation[48] rests on this very concept: the European Digital Identity Wallet, which from 2026 will facilitate both cross-border mobility and the controlled use of the various components of identity, consistent with the principle of informational self-determination[49]—a principle that, curiously enough, the 2024 Regulation does not mention.

B. Security of transactions

The European eIDAS Regulation, which underpins the contemporary digital identity systems discussed above, seeks to 'enhance trust in electronic transactions in the internal market' (Recital 2), notably by ensuring identification in the digital sphere. It is supplemented by an implementing regulation.[50] At the European level, then, digital identity

43 See *Décret nº 2019-452 du 13 mai 2019* authorising the creation of an electronic identification means called 'Authentification en ligne certifiée sur mobile' (known as 'Décret Alicem'), repealed by *Décret nº 2022-676 du 26 avril 2022*, cited above.

44 Fines Schlumberger, J.-A., 'Identité décentralisée', *La Revue européenne des médias et du numérique*, nº 69-70, Spring–Summer 2024.

45 Fines Schlumberger, J.-A., 'Identité décentralisée', *La Revue européenne des médias et du numérique*, nº 69-70, Spring–Summer 2024.

46 Examples drawn from Fines Schlumberger, J.-A., 'Identité décentralisée', cited above.

47 Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

48 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

49 On this concept and its place in EU law, see Robustelli, L., *Le droit à l'autodétermination informationnelle en droit européen*, thesis, 2022, Université de Grenoble Alpes.

50 Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

was not conceived as a sovereign prerogative but rather as an instrument for protecting the internal market.

The *Agence nationale de la sécurité des systèmes d'information* (ANSSI) is the national guardian of digital security. The proliferation of threats to information systems security compels the State, through a specialised agency, to harmonise standards and protocols for protection across both the public and the private sector. ANSSI was established by *décret n° 2009-834 du 7 juillet 2009* (Decree No. 2009-834 of 7 July 2009) as a *service à compétence nationale* (a central government body with nationwide jurisdiction). As Article 3 of the decree provides, ANSSI is the national authority on information systems security, also for the purposes of the European cybersecurity regulation known as the *Cybersecurity Act*[51]. In that capacity it performs numerous functions set out in Articles 3 and 4 of the decree, which may be grouped into five broad categories: serving as the national authority for the protection of information systems; the design, implementation and deployment of secure inter-ministerial electronic communications; the inspection of the information systems of State services and of public and private operators; the operation of detection systems and the gathering of intelligence on events liable to affect the security of the information systems of the State, public authorities and public and private operators, and the coordination of the response to such events; and the granting of approvals for security devices and safeguards intended to protect, within information systems, information classified as national defence secrets.

A *prestataire de services de confiance* (trust service provider) may obtain a qualification certifying that its services comply with the security level defined by the *référentiel général de sécurité* (general security framework). Through ANSSI and its qualification functions, the State thus acts as a trusted third party in the broad sense of the term, thereby securing information systems.

On the vast subject of cybersecurity, the State can exert only limited leverage. On the one hand, it develops only an infinitesimal share of the tools and defence strategies; on the other, users themselves are the primary source of threats to their own security. The State's task, then, is to defend a fortress whose doors are all open and whose defenders are reckless children.

II. Restoring truth

Between what *freedom of speech* permits in the United States and the conception of freedom of expression prevailing in France, the gap has never been so wide.[52]

The *loi n° 2004-575 du 21 juin 2004, pour la confiance dans l'économie numérique* (Law for Confidence in the Digital Economy)[53] extended to the Internet the age-old principle of

51 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

52 On the relationship between the regulation of fake news and freedom of expression, see Pollicino, O. (ed.), *Freedom of Speech and the Regulation of Fake News*, Intersentia, 2023, and in particular the contribution by Türk, P., 'Liberté d'expression et régulation des fausses nouvelles en France', pp. 199-238.

53 *Loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique* (Act on Confidence in the Digital Economy).

freedom of expression (*Communication to the public by electronic means is free*), but nevertheless provided for a significant number of possible restrictions.[54]

Public authorities do not have the role of upholding truth as such, but only to the extent that it contributes to public order. The State therefore has no role in ascertaining truth except where its distortion would entail a breach of public order.

Where artificial intelligence is implicated, the means of preventing and punishing threats to public order in the digital sphere are likewise limited.

While the campaign against the manipulation of content in the digital sphere is essential, its effects appear minimal (A). States and European bodies will probably have to concentrate on the more unexciting effort to counter the uncontrolled proliferation of the means of producing synthetic content (B).

A. The illusory contest against content manipulation

Loi n° 2018-1202 du 22 décembre 2018, relative à la lutte contre la manipulation de l'information (Law relating to the fight against the manipulation of information) modifies the essentially remedial approach rooted in press law, by reinforcing the means of hindering large-scale manipulation of information.

Its central provision is the introduction of Article L. 163-2 into the Electoral Code, which institutes interim proceedings empowering the judge to order any measure necessary to halt, in the three months preceding the first day of the month in which general elections are held, the circulation of inaccurate or misleading allegations or claims liable to compromise the integrity of the election. Such allegations or claims, on an online public communication service, must further satisfy three conditions: their dissemination must be deliberate, artificial or automated; it must occur on a mass scale; and the allegations must be liable to compromise the integrity of the election. On *a priori* review, the *Constitutional Council*, having recalled the strict limits within which such interim proceedings were permissible, issued an interpretative reservation (*réserve d'interprétation*): only those allegations, claims or imputations whose 'inaccurate or misleading character is manifest' may be suppressed.[55] The reservation is more apparent than real, since it falls to the interim relief judge, under severe time constraints, to rule on the matters at hand, and the manifest-character requirement is inherent in the very same legal determinations the judge is called upon to make. The Council of State, in the advisory opinion delivered pursuant to Article 39, paragraph 5 of the Constitution,[56] underscored the particular difficulties of such scrutiny,[57] conducted under extreme urgency and in proceedings

54 Article 1 of *Loi nº 86-1067 du 30 septembre 1986*, as amended (Broadcasting Act) : 'The exercise of this freedom may be restricted only to the extent required, on the one hand, by respect for human dignity, for the freedom and property of others, and for the pluralist expression of currents of thought and opinion, and, on the other hand, by the preservation of public order, the requirements of national defence, the exigencies of public service, the technical constraints inherent in the means of communication, and the need for audiovisual services to develop audiovisual production'.

55 *Conseil constitutionnel* (Constitutional Council), decision nº 2018-773 DC of 20 December 2018, *Loi relative à la lutte contre la manipulation de l'information*, cons. 23.

56 Such advisory opinions are sufficiently rare to warrant emphasis.

57 *Conseil d'État* (Council of State), Ass., opinion nº 394641-394642 of 19 April 2018, on the bills on the fight against false information.

where the burden of proving the falsehood of the allegation rests on the applicant. In any event, the manifest-character requirement excludes allegations that are merely exaggerated, as the limited case law to date confirms.[58]

The fact that the 2018 law confines interim proceedings to allegations or claims whose inaccurate and misleading character is manifest raises two particularly sensitive and paradoxical questions. First, can the integrity of the election truly be compromised if the inaccuracy of the allegation is so manifest—who, after all, can be swayed by a manifestly false statement? Secondly, the 'manifest' character of the inaccuracy, an indeterminate legal concept, must be gauged by reference to the analytical capacity of the ordinary citizen, not that of the judge. A gap may well exist between the perception of reality and the critical faculties of any given individual.

However one may assess the merits and limitations of the 2018 law, it nonetheless became clear that the threat of manipulation extended well beyond the narrow framework of protecting electoral integrity.[59]

Loi n° 2024-850 du 25 juillet 2024, visant à prévenir les ingérences étrangères en France (Law Aimed at Preventing Foreign Interference in France) pursues a broader ambition, extending beyond the electoral framework to counter the effects of hybrid warfare—notably Russia's.

In doing so, it introduces, after Article L. 562-1 of the Monetary and Financial Code (*Code monétaire et financier*, CMF), a definition of interference as 'an act carried out directly or indirectly at the request or on behalf of a foreign power and having the purpose or effect, by any means, including the communication of false or inaccurate information, of harming the fundamental interests of the Nation, the functioning or integrity of its critical infrastructure or the proper functioning of its democratic institutions'.

Such a provision lays bare the near-total powerlessness of public authorities in the face of disinformation campaigns; the response provided by the 2024 Law, through the CMF, is the freezing of funds and economic resources of persons and entities responsible for such acts (Article L. 562-2-1 CMF) and, inevitably, largely ineffective criminal sanctions against the perpetrators.

B. The reasonable obligation to expose the distortion of reality

The primary risk that artificial intelligence poses to truth lies in 'deep fakes' produced by generative AI. Regulation (EU) 2024/1689 (AI Act)[60] addresses the phenomenon in relatively permissive terms. The AI Act distinguishes four tiers of risk: unacceptable, high, limited and minimal. The production of synthetic content falls within the limited-risk

58 *Tribunal de grande instance de Paris* (Paris Court of First Instance), 17 May 2019, nº 19/53935, concerning a misleading tweet about the storming of the Pitié-Salpêtrière hospital on 1 May 2019.

59 *Conseil constitutionnel* (Constitutional Council), decision nº 2018-773 DC of 20 December 2018, *Loi relative à la lutte contre la manipulation de l'information*, cited above, cons. 21: 'the legislator strictly delimited the information that may be the subject of the contested interim proceedings. On the one hand, such proceedings may target only inaccurate or misleading allegations or imputations of fact liable to undermine the integrity of the forthcoming ballot'.

60 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

category, which requires only that such content be marked and identifiable as AI-generated.[61]

Notably, the AI Act provides an adaptive mechanism empowering the European Commission, through its AI Office,[62] to adopt implementing acts. These will in turn enable the approval of codes of good practice to facilitate the application of obligations to detect and label content generated or manipulated by AI.[63]

The provisions of the AI Act must be read in conjunction with those of the Digital Services Act (DSA)[64] and of the Digital Markets Act (DMA).[65]

The DMA aims to impose specific competition obligations on the main providers of digital services (the 'gatekeepers'), designed for the proper functioning of the internal market. The regulation itself makes no mention of artificial intelligence, but some scholars argue that the constraints it lays down inevitably affect the deployment of AI; this is the case, for instance, with restrictions on the usage of user data (Article 5) or the transparency of advertising (Articles 5(9)-(10) and 6(8)).[66]

The DSA applies not to operators as such but to the services they provide; its purpose is to establish a framework of obligations for online intermediaries that permit the dissemination of illegal content. In its application, the Regulation must be read alongside the aforementioned LCEN[67] which governs illegal content on the Internet. More specifically, the DSA establishes a system for monitoring and sanctioning digital service providers with knowledge of 'illegal content', defined as 'any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law'. Illegal content within the meaning of the DSA thus encompasses the categories identified by the LCEN in Article 6, I, § 7, paragraph 3: the glorification, denial or trivialisation of crimes against humanity; incitement to commit terrorist acts and the glorification thereof, to racial hatred, to hatred against persons on the basis of their sex, sexual orientation, gender iden-

61 Article 50(2) of the AI Act: '2. Providers of AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content, shall ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated. Providers shall ensure their technical solutions are effective, interoperable, robust and reliable as far as this is technically feasible, taking into account the specificities and limitations of various types of content, the costs of implementation and the generally acknowledged state of the art, as may be reflected in relevant technical standards. This obligation shall not apply to the extent the AI systems perform an assistive function for standard editing or do not substantially alter the input data provided by the deployer or the semantics thereof, or where authorised by law to detect, prevent, investigate or prosecute criminal offences.'

62 The European AI Office was established within the European Commission by Commission Decision of 24 January 2024, 'establishing the European Artificial Intelligence Office' (C(2024) 390 final).

63 Article 50(7) of the AI Act.

64 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

65 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

66 Schwab, A., 'Digital Markets Act and artificial intelligence services', Sept. 2024, *Concurrences* N° 3-2024, Art. N° 119739, www.concurrences.com

67 *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique* (Act on Confidence in the Digital Economy), cited above.

tity or disability, and to violence, including sexual and gender-based violence; child sexual abuse material; violations of human dignity, of image rights, of privacy and of the security of persons; and all forms of blackmail and harassment. Such illegal content may plainly involve—and will increasingly involve—the use of artificial intelligence, notably in the form of synthetic images or sounds.[68]

Digital platforms, subject to the oversight of national administrative and judicial authorities and Union institutions, thus become—whether willingly or under compulsion—the auxiliaries of a new form of administrative policing.[69] Even where the object of such policing is not the protection of truth as such, truth will inevitably feature as an incidental concern; and more broadly still, so will the generation and dissemination of content through artificial intelligence.

What is now unfolding is a genuine clash of civilisations between the aspiration to regulate content, pursued by the European Union, and the *laissez-faire* policy championed by the United States.[70] European positions must hold firm, lest future generations inherit a *1984* in reverse.[71]

68 On the interplay between the DSA and the LCEN, see Besse, T., 'L'évanescente responsabilité pénale des fournisseurs de services intermédiaires dans le cadre de la mise en ligne de contenus illicites', *Cahiers de la recherche sur les droits fondamentaux*, 2023 nº 21, URL: http://journals.openedition.org/crdf/8804; DOI: https://doi.org/10.4000/crdf.8804.

69 Pénitot, M., 'Les modérateurs de plateformes en ligne : de nouveaux acteurs de police?', *Cahiers de la recherche sur les droits fondamentaux*, 2023 nº 21. URL: http://journals.openedition.org/crdf/8824; DOI: http://journals.openedition.org/crdf/8824.

70 Piquard, A., Rocard, P., 'Au sommet de Paris, la charge des États-Unis contre la "censure" de l'IA', *Le Monde*, 11 Feb. 2025. https://www.lemonde.fr/economie/article/2025/02/11/au-sommet-de-paris-la-charge-des-etats-unis-contre-la-censure-de-l-ia_6542711_3234.html.

71 The reader will probably have expected, from the article's very title, a reference to George Orwell's novel *1984* (*Nineteen Eighty-Four*). The reference was too obvious for us to yield to it. But it was also too obvious for us to overlook it. In the novel it is the super-State Oceania led by the *Big Brother* that exercises generalised surveillance through the Ministry of Truth and suppresses freedom of expression. In the reality we now live in, the *Big Brother* can be seen as the leaders of the GAFAM companies and Oceania as the reactionary international movement that is being built beyond States.