Introduction

Côme Berbain,
director of Innovation and of the Autonomous Vehicle Program, RATP Group,
&
Bertrand Pailhès,
director of Technology and Innovation, CNIL

"Confidence!" "Trust!" During a period of apparently tenser social relations as the references inherited from industrial society are disappearing and as digital technology is becoming a major factor in the transformation of modern societies, these are two catchwords to which few political leaders or experts can stake out a claim. The rollout of the information society over the past thirty years has led to major progress, such as the composition of the Wikipedia encyclopedia by thousands of anonymous contributors without personal ties, the new forms of technology based on a global scientific consensus, and software "open" to anyone.[1]

In the digital realm, confidence or trust are poorly defined concepts referring to diverse interests, depending on whether we are talking about forms of technology, contents, or the persons contributing to them. In many cases, confidence is mainly a question of the rules, procedures and standards that everyone finds acceptable; and these, when upheld, lay the grounds for all parties to sincerely and safely take part in online activities. Some of these procedures rely on special techniques, like asymmetric cryptography; but others, on the practices of organizations and individuals. While "netiquette" was, at the end of the 20th century, intended to introduce civility in cyberspace, recent online developments are characterized by an increase in abuse and hate, and the spread of conspiracy theories, as the magic of instantaneous access has turned "truth" into something relative. This trend is evidence of the fragility of the means used to boost confidence and trust in digital technology. This polysemous topic evinces the very ambivalence of technology's impact.

Is it not time to take stock of the trends that are adding to, or on the contrary detracting from, our trust or confidence in digital technology? Before broaching the latest techniques, procedures, rules and regulations designed in response, it is worthwhile reviewing the psychological or legal interpretations of confidence and trust in order to gain a vantage point for glimpsing two key dimensions: the stability and transparency of relations based on confidence. Confidence on the Internet arises out of a patient construction, a process consolidated over time that no short-term action, however deliberate and legitimate, can match. It is built on the visibility of the processes, algorithms or entities in which it is to be placed. Opacity has never provided a stable approach to confidence-building, whether for information systems, state authorities, the social networks or encryption algorithms.

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France).

This issue of our journal explores the various ways to restore confidence among users, firms and institutions. Technological solutions will thus be brought under consideration along with the changes made in regulations and the roles of institutions.

The advance toward an "information society" mainly depends on the possibilities created by digital technology. It is, therefore, tempting to try to find a technical answer to the question of confidence. Such solutions might be based on technical assessments involving sophisticated methods of certification or on embedding confidence, partially or fully, in the technology itself. As shown by the cases of homomorphic encryption and artificial intelligence (AI), this approach, though promising, is not yet mature enough. A technical solution cannot, by itself, sustain confidence. Blockchains, too, attempt to generate confidence through technology alone, given their objective of replacing trusted third parties with a protocol.

Since it is often said that a computer system's principal vulnerability is located "between the chair and the keyboard", it is probably unrealistic in our digital age to base confidence on technology alone. Though indispensable, technology cannot by itself detect the full range of human factors, evidence of this being the phishing expeditions or bitcoin scams that repeatedly succeed by playing on the very familiar emotions of greed and gullibility without exploiting any vulnerability in the technology itself.

Besides, any technology that takes account of confidence will suffer from an actual disadvantage whenever simplicity for users and the speed of execution override safety. It will be bloated; and its operation, slower and more complicated. Who reads the fine print about a cyberproduct's security? Who pays attention to the details in the directions for installing an encryption messaging protocol? Nonetheless, these details, which claim end-to-end security, are what can build up, or tear down, confidence. Instead of being a technical reality, confidence turns out to be, in the real world, a presupposition made by users or a matter of marketing and branding.

Given these limitations of a purely technological approach, additional actions are needed to organize the development of information systems and their security. This issue was soon enough seen as being complicated. Already in the 1970s during discussions about computerization, legal guarantees related to the uses of these new machines were deemed appropriate. In France, the Informatics and Freedom Act and the CADA Act (which set up the Commission of Access to Administrative Documents), both in 1978, and, in 1979, a law about archives embodied the conclusions drawn from deliberations on this topic. These legal texts set the principles to be upheld in clear terms that everyone can understand: the purpose of data processing, the principle of proportionality, security, the storage of data, and the transparency of automated decisions, especially in the public sector. This set of ideas, worked out more than forty years ago, is still deemed relevant.

Obviously, the advent of the Internet and the uses of digital technology in all fields of activity have lent even more importance to the production of confidence and trust. They have spawned new practices and regulatory principles. The EU General Data Protection Regulation (GDPR) enshrines data protection in the law and provides for reinforcing it. The trend toward "open (public) data" is not just a principle about the access to data. It has fostered new approaches that rely on active, organized communities who want to apply the principles of the commons to the governance of essential digital resources. This line of thought is being extended to the regulation of algorithms, which, in an attempt to cope with complexity, involves a combination of mathematical proof, legal guarantees and multidisciplinary approaches.

Given the second-generation of online services, which are based on a multitude of contributors and on the key role of a limited number of platforms, the question of confidence in online information has come into the spotlight. While the example (which is not, however, above criticism) of Wikipedia has demonstrated the possibility for a reasonable governance of information, the current mixture of public authorities who are hard to believe, of businessmen who are spurred on by their economic interests (sales of advertising space) and of interest groups who have organized to support selected facts or theories is a potently dangerous combination that raises technical, institutional and legal questions. Recent developments in Europe and the United States respond to the need to strike a new balance in this very sensitive area.

Questions about governance — of the Internet and of information society — draw attention to the role of public authorities in building confidence during the digital age and to the form of confidence to be provided. Transposing in cyberspace a major facet of confidence — the identification of physical persons — is a problem that opens onto a wide range of possible actions for public authorities despite the stiff resistance they have encountered in France. Although several other countries have managed to roll out solutions for an “electronic identity”, very few have done so outside the public sphere. What we observe is that the management of online identities is now as much (if not more often) in the hands of a few private players (Google or Facebook) as under the control of officials. Governments are suspected of wanting to use digital technology to tighten their control over the population. In France, this dualism was evident in the case of StopCovid. On the one hand, state authorities supported this software program as an issue of sovereignty, but on the other hand, they had trouble rolling out this technical solution and politically following up on it so as to build confidence. Meanwhile, Google and Apple have deployed very effective technical systems from which any democratic control is missing. By the way, other European countries have not adopted the same viewpoint on this topic as France.

Since public authorities are unable to create the technical solutions for shoring up confidence and unable to stimulate confidence in the software applications they manage to develop, they should turn toward other fields of action. By making digital technology accessible for everyone, adopting an ambitious policy of “digital inclusion”, and regulating online forums and spaces so as to balance the freedom of speech with its limits (a role currently opposed by the big platforms), public authorities will be able to make room for building confidence and asserting a legitimacy based on democracy.