A new field of research for Europe: developing an engineering for digital ethics

The need to anticipate the legislation and anticipate usage

Michel Riguidel, Paris

How do you think the internet will look like in 2025 and beyond?

Hybrid physical and virtual metasystem with high enthalpy (with autonomous, virtual entities and systems, acting and circulating throughout the infrastructure)

Digital usages are evolving so fast (The enthalpy[1] ΔH of usage is increasing so much), that it will be essential to constantly update models, tools and rules of digital ethics: personal data security, privacy compliance, ethics of contents, fight against the spread of violence, ethics of connected objects (robots, drones), ethics of digital prosthetics, ethical financial engineering with algorithms in real time, fair (with displayed finality) digital surveillance, right dosage of interferences of the internet oligarchs and telecom operators onto digital technique usage, ethics of collective actions, governance of virtual currencies, of security in obscurity, vigilance on censorship, on hacktivism, on dissemination of ideologies, etc.

Digital ethics which today targets only humans may spread soon to the ethics of autonomous systems (smart grid systems, robots, embedded system connected, remote control systems), however, managed by legal or virtual people. One has not been sufficiently prepared the inevitable emergence of a true responsible Internet of Things. This is a socio-technical design for all men and machines, a technical framework for the ethics of digital technologies, including hybrid physical systems (cars, drones, digital implants…).

Digital ethics affects digital identity management, network management (monitoring telecom operators' traffic) and service providers' management (content management of social networks and clouds' users).

It involves immediately the international facet since the digital world ignores geographic borders and undermined national courts.

What will be the essential functional building blocks of the Internet then?

An ethical building block inside the network is indispensable

The notions of accountability, responsibility and intentionality actions cling to digital ethics, since there is always a physical individual who triggers (knowingly causes or not) a computer action, to which can be attributed (directly or indirectly) the emergence of other IT events (failure in infrastructure, malfunction of a cloud, information leak, deployment of virus attacks, etc.). Today, safety, security and trust engineering are too narrow fields to stop conflicts, shorten disputes, and reduce vulnerabilities in networks.

Digital ethics encompasses the ethics field of communications, storage and computing. Mistrust essentially comes from the side of calculation, due to the opacity of software and asymmetry of service distribution.

Digital ethics cannot be implemented fully by technical measures, as the theoretical foundations of digital world (Turing machine, computer language) make it impossible to formally define the ethics of computer-digital activity (indecidability of software, etc.). Digital ethics is a subtle play of light and shadow to protect interests of the parties, and grow

[1] Today, enthalpy ΔH much better characterizes the ecosystem as its entropy ΔS or complexity.

the widespread interconnection in an anonymous world. Resilience, privacy, safety, security, confidence should be extended to philosophical principles, societal rules that must be instantiated into ecosystems as architecture, machines, services, software, framework, computational models, probes, questions and answers in real time ...).

Could you indicate where we should focus our activity research in the next 5-10 years to achieve? Are there new field of research to create/develop?

A new field of research: engineering in digital ethics

A whole engineering can be implemented to manage new technologies: IoT, future nanotechnologies, IT for health, etc.

There is a tendency (especially of legal origin) who would often hang up the rules for digital ethics to those of traditional ethics. Unfortunately, the notions of time, place and action (an action was perpetrated at such place and at such time) are no longer suitable in digital world, with the emergence of virtual IT entities[2]. Rules can be abstract and computerized (processed within computers at a rhythm of a billionth of a second and transmitted at the speed of light within networks). One may imagine their own digital laws that could move away from the classic rules of human behavior in the real world. The identification of numerical facts, digital evidence is a major issue, which is not completely resolved (forensics, audit, search, etc.). Engineering in IT ethics will affect the extension of existing computer languages, cryptographic protocols and methods of dissemination services (license agreement) and the trust models, and will allow a better deployment and acceptability of SDN-NFV.

Industry and research cannot leave this field as alone legal field: the weight of non-consideration of technical reality brings bad solutions. Ignorance of technical induced delays (hence the type of legal decisions made fait accompli), misunderstandings (hence technology development abort, following early hijackings usage). Technologies are often praised by marketing orchestration, or convicted by movements of opinions on social networks: peer-to-peer architecture and illegal downloading, blockchain technology and virtual currency managed in the dark (bitcoin), social networking and use of personal data.

It is difficult to specify in absolute virtuous ecosystem because censorship of use, software, content can be implemented only with respect to a context and in a well-defined socio-cultural environment. But it seems possible to design and implement formal models and questions (as software smart sensors) of digital ethics (running on a computing timescale).

Some simplistic universal models within a hybrid (physical and virtual) world involve too many risks: transparency (risk of totalitarianism), openness[3] (risk of developing a proprietary world), interoperability (risk of domino effects), and seamless world (risk of brutal attacks).

The obligation of reciprocity between actors (users, suppliers, etc.) for effective dialogue between stakeholders (commitment and response to some questions, in the form of computer probes) may be a way out of the rut in which the today's interconnected world has weakened.

A whole set of methodologies, models and tools could be developed to design and implement digital ethics as a new engineering domain, taking account European values: privacy, dignity and sovereignty of citizens.

[2] Neither the notions of data controller and data processor.

[3] There is always confusion with this computer notion of openness. The open system notion was created to build proprietary systems, which can be interconnected with a public interface.