Digressions on Ethics in the Internet of Things

By Gérald Santucci

"L'homme robot, l'homme termite, l'homme oscillant du travail à la chaîne système Bedeau, à la belote. L'homme châtré de tout son pouvoir créateur, et qui ne sait même plus, du fond de son village, créer une danse ni une chanson. L'homme que l'on alimente en culture de confection, en culture standard comme on alimente les bœufs en foin.

C'est cela l'homme d'aujourd'hui.

Si je suis descendu, je ne regretterai absolument rien. La termitière future m'épouvante. Et je hais leur vertu de robots. Moi, j'étais fait pour être jardinier."

(Antoine de SAINT-EXUPERY)

The 'Internet of Things' (IoT) is no longer a futuristic concept as it was when I was responsible for the IoT unit at European Commission DG CNECT between 2005 and 2012. It is an incredible economic force that is quickly developing even if today its thrust and impact are partly hidden by the boom and the hype of Artificial Intelligence.

Indeed, the IoT - the metaverse and Web3 likewise - has turned old-fashioned in the last few years in favor of generative artificial intelligence that has captured all the attention from media and professionals. Insofar as today generative IA seems to go around in circles with a stream of announcements of the launch of new models and technical benchmarks, time is ripe to remind the reality of industry by reintroducing IoT in the collective conversation.

I would like first of all to insist on the fact that IoT is no longer a term that can be claimed by any single organization, as it was often the case in the early 2000s, but, as Rob van KRANENBURG put it in a recent interview "One thing that has changed is the branding. In the past, we had terms such as RFID and 'ambient internet' which people associated with single companies... Now that the IoT term is generic, there is more willingness to embrace it without fear of being tied into a single provider." He could have mentioned as well ubiquitous networking, the disappearing computer, ambient intelligence, cyber physical systems, and a few more.

IoT uses a variety of technologies to connect the digital and physical worlds. Physical 'things' can be embedded with sensors that monitor them (e.g., temperature, motion) and actually any change in their environment and with actuators that receive signals from sensors and then react to the reported changes - it's a matter of 'sense and respond' as what was written in an old SAP report. Sensors and actuators communicate with computing systems via wired or wireless networks which in turn can 'smartly' manage the actions of connected objects. IoT combined with data and

analytics provides vast opportunities for organizations to innovate products and services and to increase operational efficiency.

IoT uses a variety of technologies to connect the digital and physical worlds. Physical objects can be embedded with sensors and actuators. Sensors monitor things like temperature or motion, or really any change in environment. Actuators receive signals from sensors and then react to the reported changes. Sensors and actuators communicate with computing systems via wired (for example, Ethernet) or wireless (for example, Wi-Fi or cellular) networks; these computers can monitor or manage the health and actions of connected objects and machines.

There are today more than 15 billion connected IoT devices around the world. This figure is expected to double by 2020, with 75% of all devices being IoT then. However, let's bear in mind that figures regarding the number of IoT devices are relatively meaningless since they depend on the definition of IoT. But according to McKinsey, "the total value potential for the IoT ecosystem could reach $12.6 trillion (€11.5 trillion) by 2020". This is a tremendous figure and the promise of an economic force fostering innovation in new products and services, shaping new ways of working, creating new job qualifications, setting new trends and, if properly oriented, being something 'good for all' i.e., as claimed by the IoT Council, part of the solution, not the problem (...) More important are the long term goals that we are setting to point the direction in which we want to go. These can be sustainability, mitigating climate change, tackling inequality and creating transparency in decision makingCommon IoT applications include Healthcare Transformation, IoT in Factories, Connected Cars, Smart Home Devices, Wearables, Smart Cities, and so on, assuming an IoT application is a collection of services and software that integrates the real-time data received from IoT devices."

IoT has begun to bring a dramatic change to the control that humans have over their environment by providing objects the ability to communicate with each other, and with humans, and take decisions on behalf of humans or without humans being involved in the process.

Therefore, like for Artificial Intelligence, it is imperative to hold and maintain a collective reflection on the ethical implications of IoT. For me, a key thinker of IoT Ethics is Jeroen VAN DEN HOVEN, Delft University of Technology, and a member of my IoT Expert Group at DG CNECT in 2010-2012, who highlighted a large number of IoT-specific ethical concerns, in particular the following:

- Ubiquity and pervasiveness - users should be able to opt-out of IoT without being forced to retreat into the pre-digital era.
- Miniaturization and invisibility - the design of future IoT devices should include making the technology visible and amenable to audit, quality control and accountability procedures.
- Ambiguity and ontology - as two evolutions are converging - humans to become 'augmented' and machines and systems to become 'intelligent' - the distinctions between natural objects, artefacts and human beings are gradually disappearing, which calls for a reconsideration of Human Identity in the IoT era.

- Identification - as objects will increasingly be endowed with unique identities, there is an urgent need to agree collectively the governance issue of who gets the authority to assign, administrate and manage these identities.

- Mediation and autonomous agency - as human beings act in IoT environments together and in concert with artefacts, devices and systems, human agency gets extended and augmented to a point where the course of human events may be impacted by spontaneous, unforeseen and unexpected interventions that are not directly caused by human beings.
- Embedded intelligence and 'extended mind' - IoT systems embed intelligence to a point where smart and dynamic objects with autonomous behavior become an extension to the human body and mind, which may eventually make individual human beings feel cognitively and socially handicapped.
- Distributed control - the locus of control and governance of IoT not being a central one because of the vast amount of nodes, hubs and data, an appropriate distributed governance of IoT represents a key challenge for the future.
- Unpredictability and uncertainty - as human beings are facing the risk of losing full control of the development of IoT, its is necessary, like for AI, to provide ethics guidelines for trustworthy IoT.

Therefore, following VAN DEN HOVEN advice, IoT policy should be designed, ideally at global level, but in any case at EU level, (i) to avoid the emergence of **social injustice** (fair access to IoT technology and qualification of the citizens to use it), (ii) to establish **trust** in IoT (data protection, privacy, security network and information management), (iii) to ensure the **adequateness** of IoT metaphors, (iv) to create a '**social contract**' between human beings and objects (by delegating actions to objects, human beings should have full confidence that these actions shall be those actually intended by them, (v) to allow for **informed consent** (invisible technology should be made visible to those interacting with it in order to fulfill privacy requirements).

In order to meet the requirements for ethical or trustworthy IoT, it is necessary to act on its main technological elements:

1) Sensors - To safeguard sensitive data and ensure their responsible usage, the ethical widespread deployment of all kinds of sensors is contingent on the full respect of existing legal measures about data protection, privacy, security, and product liability.

2) Networks - As human life is becoming increasingly intertwined with IoT networks of interconnected and mutually interacting devices, which are highly vulnerable to technical unreliability or intentional misuse, ethical questions arise in relation to the safety of these networks.

3) Data - The way IoT systems are designed to collect, store and process huge amounts of data is of fundamental ethical importance for privacy, in particular

regarding the profiling of individuals, the protection of personal data, and the informed consent of users.

4) Agency - Like for intelligent robots and autonomous systems, IoT systems interconnecting numerous devices and subsystems of devices can "make decisions" and act "autonomously", sometimes without "human in the loop", which raises serious concerns in terms of human agency and behavior due to the loss of transparency and the possibility of inexplicability or non-traceability of the decisions and their resulting actions.

IoT Ethics is as much important as AI Ethics, and actually the two are increasingly intertwined. Within a few years we have entered an era of hyperconnectivity where four 'tectonic mental shifts' are challenging our idea of human identity:

- Reality / virtuality, i.e. shaped things (cf. Bruce Sterling) from man-made artifacts to the current era of 'gizmos' and 'spimes' and the future 'biots' (both object and person).
- Human / Artefact: humans are expected to become 'augmented' by technology while at the same time artifacts are believed to evolve toward artificial general intelligence (AGI) machines endowed with capabilities that rival those of a human.
- Scarcity / Abundance: land, labor, capital and entrepreneurship are scarce factors of production whereas data is abundant, creating new business models, market structures and industry boundaries, indeed changing everything.
- Entities / Interactions: the IoT is changing the relationships between individual human beings and 'talking objects', provoking a metamorphosis of these objects and a new vision of living, human identity, and the very Idea of Man.

These 'tectonic mental shifts' are of course interdependent subparts of the whole phenomenon of hyperconnectivity - "the instant availability of people for communication anywhere and anytime" (Anabel QUAN-HAASE & Barry WELLMAN.). Such hyperconnectivity has major ethical implications as it may eventually lead to more loneliness or on the contrary more interdependence. I argued elsewhere that the recent COVID-19 pandemic had shown that the future of humanity lied in altruism and empathy, not in egoism and distance. This is even truer in the hyperconnectivity era where the very concept of humanness is questioned - the 'self' can remain the 'self' and the 'other' the 'other' or, in a new paradigm, as argued by Nicole DEWANDRE building on the work of Hannah ARENDT, the 'self' becomes plural (i.e. equal, unique and relational) and the 'other' is a self.

Therefore, what we should be aware of is that the ethics of IoT is not only a matter of compliance with and enforcement of existing regulations, or a problem of privacy and security, even if these elements are extremely important, it is primarily a collective reflection on the future of humanity and Sarah SPIEKERMANN's Idea of Man in a context where hyperconnectivity among human beings and with their artefacts raises a new challenge to the concept of human identity. After the Saint, the Hero, the Wise

Man, the *Honnête Homme*, and now the Hyperconnected Human, what role model of human is to emerge?

Is there anything between Clyne's Cyborg and Nietzsche's Superman?

This is probably the biggest challenge to which our generation shall have to respond.