Aspen Institute Italia

INTERNATIONAL CONFERENCE

Tel Aviv, November 24–25, 2019

The Aspen Initiative in Israel

International Conference

The Aspen Initiative in Israel

The tech revolution and the future of business

Tel Aviv, 24-25 novembre 2019

Organizzato in collaborazione con
The Frenkel-Zuckerman Institute for Global Economics, Coller School of Management, Tel Aviv University
Peres Center for Peace and Innovation

Con il contributo di
Ministero degli Affari Esteri e della Cooperazione Internazionale
AVM Gestioni SGR
Oliver Wyman – TASC
Telecom Italia Sparkle
UBI Banca

The Aspen Initiative in Israel

The tech revolution and the future of business

Tel Aviv, 24-25 novembre 2019

INDICE DEI DOCUMENTI

The Aspen Initiative in Israel

The tech revolution and the future of business

The Aspen Initiative in Israel è una importante iniziativa internazionale che l'Istituto svilupperà in continuità negli anni. Israele è certamente un interlocutore indispensabile per una riflessione sulla *disruption* tecnologica e i suoi effetti sul business. Grazie alla collaborazione con la Tel Aviv University e il Peres Center for Peace and Innovation e avvalendoci del supporto dell'Ambasciata italiana a Tel Aviv, abbiamo riunito un gruppo di circa 50 persone composto da rappresentanti del business ed esperti italiani e israeliani allo scopo di discutere aspetti cruciali che si stanno imponendo con determinazione nella realtà quotidiana, dalle aziende alla società, mettendo in discussione gli assetti attuali e spingendo verso la ricerca di nuove politiche industriali, della formazione/istruzione, del lavoro. I temi al centro del dibattito sono stati le biotecnologie e la bioingegneria; l'efficienza energetica (risorse rinnovabili, energia pulita e "smart grids"); le città intelligenti e la qualità della vita; le biotecnologie nell'agricoltura. La convergenza di interessi tra Italia e Israele su questi temi è peraltro importante per le relazioni in termini di "business": Israele, piccolo paese decisamente all'avanguardia nell'innovazione tecnologica, può offrire interessanti prospettive di confronto e collaborazione.

Si è anche discusso sugli scenari geopolitici in cui le tecnologie innovative si collocano e ne sono sempre più parte integrante. La sfida per le democrazie occidentali è dunque al contempo concettuale, politica, economico-sociale, tecnologica (vista l'importanza delle nuove tecnologie digitali in tutte le dimensioni), in un contesto internazionale fortemente connesso che può produrre rapidi "effetti-contagio".

Aspen Institute Italia intende seguire e analizzare queste tematiche nell'ambito di un filone di attività articolato su 1 conferenza annuale, preceduta da un lavoro preparatorio di raccolta di materiali e riunioni con esperti: ***The tech revolution and the future of business*** è una conferenza internazionale dedicata a un'analisi comparata delle esperienze di innovazione tecnologica in alcune delle economie più avanzate e dinamiche, tra la competizione globale crescente e delicate scelte e l'esigenza di combinare efficacemente risorse pubbliche e private.

In questo dossier vengono riportati i documenti che offrono un quadro il più possibile esaustivo di quanto emerso dal dibattito tra i partecipanti, corredato da articoli apparsi sulla stampa e da una selezione di articoli pubblicati sulla rivista *Aspenia* e *Aspenia Online* (Aspeniaonline.it).

As of November 24, 2019

Aspen Institute Italia

The Frenkel-Zuckerman Institute for Global Economics
Coller School of Management
Tel Aviv University

Ministry of Foreign Affairs and International Cooperation

The Aspen Initiative in Israel

In cooperation with
Peres Center for Peace and Innovation

International Conference

The tech revolution and the future of business

Tel Aviv, November 24 – 25, 2019

With a contribution by
AVM Gestioni SGR
Oliver Wyman - TASC
Telecom Italia Sparkle
UBI Banca

AGENDA

SUNDAY, NOVEMBER 24

Location: Peres Center for Peace and Innovation – Opening of the conference and panel discussion (*132 Kedem St., Tel Aviv-Jaffa*)

4:45pm	Meeting point in the hotel lobby and departure for the *Peres Center for Peace and Innovation*
5:30pm-5:45pm	Arrival of participants
5:45pm-6:40pm	Tour of the Peres Center
6:45pm-7:00pm	Opening and welcome remarks *(Lobby)*
7:00pm-8:00pm	Panel discussion

SETTING THE STAGE
The innovation ecosystem in Israel and Italy: how innovation can assist making the world a better place?

Q&A

8:00pm Buffet dinner *(Lobby)*

MONDAY, NOVEMBER 25

Location: Tel Aviv University, Coller School of Management *(Room 430)*
(Ramat Aviv)

8:30am — Meeting point in the hotel lobby and departure for *Tel Aviv University*

9:15am — Arrival of participants and opening of the conference

9:30pm-11:00am — **SESSION I**
The geopolitics and economics of technological revolution

- The "technology cold war" between China and the US and the security of 5G networks
- Trade conflicts and global supply chains: is the world de-globalizing?
- Cybersecurity: the challenges ahead
- The need for global governance in the AI: sharing common rules to better manage risk
- Technology and democracy: what post 4.0 capitalism in a changing world?

Discussion

11:00pm-11:30am — Coffee break

11:30am–1:00pm — **SESSION II**
The "open innovation system" and the Israeli experience

- The start-up nation model: why is the EU lagging behind?
- Sharing assets and competences: the eco-system and the imperative of brain circulation
- Alternative business models: open innovation – where a firm's boundary meets the outside world
- Overcoming the fear of failure: value-creation and the appetite for risk
- A new cultural model: lessons from Israel for the EU and Italy
- Smart cities, human mobility and quality of life: comparing experiences

Discussion

1:00pm-2:30pm — Buffet lunch

2:30pm-4:00pm — **SESSION III**
Digital transformation and the post 4.0 business: looking at specific sectors

- Investing in innovation: fintech as an opportunity for the financial ecosystem
- Biotechnologies and bioengineering in medicine as strategic technologies
- The new frontiers of energy efficiency: clean energy and the future of agriculture

Discussion

4:00pm-4:30pm — **Closing remarks**

7:30pm	Reception *hosted by the Italian Ambassador to Israel* (Alonim 6, Ramat Gan)	*by invitation only*
	Transfer to the Hotel	

TUESDAY, NOVEMBER 26

am	Departures

The schedule is flexible except for opening and closing hours. No simultaneous translation is provided

The Aspen Initiative in Israel

International Conference

The tech revolution and the future of business

Tel Aviv, 24-25 novembre 2019

In collaborazione con *The Frenkel-Zuckerman Institute for Global Economics, Coller School of Management, Tel Aviv University,Peres Center for Peace and Innovation*

Con il contributo di *Ministero degli Affari Esteri e della Cooperazione Internazionale*
AVM Gestioni SGR, Oliver Wyman – TASC, Telecom Italia Sparkle, UBI Banca

Sintesi della discussione a cura di *Ivan Jevtovic*

In uno scenario globale caratterizzato da forte interdipendenza tra i paesi, qualsiasi interruzione negli scambi commerciali o nelle infrastrutture tecnologiche può avere un impatto di portata globale. Le attuali tensioni a livello geopolitico dimostrano che tali interruzioni possono derivare da azioni convenzionali, come l'imposizione di tariffe bilaterali, o da azioni non convenzionali, come ad esempio gli attacchi informatici. Le misure adottate da governi e regolatori per prevenire questi rischi possono avere effetti a lungo termine sulle imprese e sulla società - e risultano non facilmente reversibili.

È pertanto necessaria una ridefinizione delle competenze dei *policy makers*, sostenuta da un quadro normativo coordinato e omogeneo a livello internazionale, al fine di governare sviluppi tecnologici e scenari in rapida evoluzione. La rivoluzione tecnologica in atto sta definendo nuove regole del gioco tra attori tradizionali e nuovi entranti digitali in diversi settori fondamentali: dall'ambito medico alla finanza, dalla bioingegneria all'efficienza energetica nelle città, fino alle biotecnologie per l'agricoltura.

In questo panorama internazionale sempre più complesso, Israele rappresenta uno dei migliori esempi al mondo di ecosistema a innovazione aperta. I tratti caratteristici della "nazione start-up" israeliana derivano in gran parte dalla sua storia e dall'esigenza costante di "innovare per necessità", in agricoltura, nel settore della difesa così come nelle tecnologie avanzate. L'intelligenza artificiale è ormai applicata con successo a sicurezza, sanità e servizi finanziari, ed il sistema-paese offre numerosi spunti per un proficuo scambio di esperienze. Israele, piccolo paese all'avanguardia nell'innovazione tecnologica, può offrire interessanti prospettive di confronto e collaborazione con l'Italia, in una convergenza di interessi in termini di "business" e grazie ad una complementarietà in diversi settori, dall'arte all'agricoltura.

La geopolitica e l'economia della rivoluzione tecnologica

L'esponenziale crescita della Cina nel commercio internazionale dal 1999 ad oggi, passando dal 4% al 25% dell'output globale, ha profondamente cambiato gli equilibri mondiali ed il suo rapporto con il partner americano – e non solo. Oggi la Cina rappresenta il primo o secondo partner commerciale di molti paesi, avendo completato un'evoluzione significativa da paese-produttore e consumatore - fino a diventare un attore primario anche nell'ambito delle tecnologie avanzate. Le tensioni commerciali tra Cina e Stati Uniti hanno, tuttavia, portato alla luce un profondo disallineamento tra le due super-potenze su questioni fondamentali, fino ad ipotizzare la fine della globalizzazione nella versione a cui abbiamo assistito negli ultimi venti anni.

La risposta dell'amministrazione americana alla crescente influenza della Cina si è basata finora su misure bilaterali, come ad esempio le tariffe doganali e divieti motivati da "sicurezza nazionale", nonostante i fattori in gioco siano ormai multilaterali e su scala globale. Ne è esempio la sensibilità del governo statunitense alle infrastrutture 5G fornite da Huawei, anche nel contesto di commesse ai partner europei, come emblema della mancanza di fiducia verso aziende cinesi (definite da Trump come un "dipartimento dell'intelligence di Pechino") e dei rischi connessi alla cybersecurity.

Tuttavia, l'antagonismo tra Stati Uniti e Cina non può essere definito come una nuova "Guerra Fredda" in quanto l'interazione tra di loro è tuttora - ed è destinata a rimanere ancora a lungo - molto profonda e diversificata in numerosi settori. Piuttosto, sarà la modalità con cui le due potenze sceglieranno di collaborare a definire in modo decisivo gli scenari globali dei prossimi anni. In tale contesto, l'attuale dominio tecnologico della Cina in ambito 5G rappresenta il suo "momento-Sputnik": un considerevole vantaggio competitivo a cui gli Stati Uniti sono chiamati a rispondere. Un possibile *de-coupling* tra i due Paesi nelle forniture di alcuni settori particolarmente sensibili, come ad esempio i semiconduttori e le infrastrutture tecnologiche, è destinato a ridefinire gli equilibri a livello globale. Stretta tra gli interessi contrapposti delle due potenze, l'Europa si trova a bilanciare tra il ruolo di alleato leale al partner transatlantico, e la necessità di approvvigionarsi delle migliori tecnologie per le nuove reti 5G, dove il leader asiatico offre soluzioni all'avanguardia.

Il tasso di crescita del traffico dati, infatti, cresce esponenzialmente: i volumi che viaggiano sulle infrastrutture digitali raddoppiano ogni tre anni, e sulle reti mobili addirittura si decuplicano ogni cinque. È interessante notare come alcune aziende risultano i principali drivers del traffico dati, creando dei veri e propri oligopoli: Youtube rappresenta il 37% del traffico dati internet su reti *mobile*, seguita dai principali social media come Facebook (8.4%), Snapchat (8.3%) e Instagram (5.7%); nel segmento dei motori di ricerca Google domina con il 93% di quota di mercato. Con l'introduzione del 5G, che renderà qualsiasi oggetto

potenzialmente connesso ("*internet of things*"), si prevede che nel 2025 si potranno contare nel mondo un trilione di dispositivi (oggi sono circa 50 miliardi) rispetto a otto miliardi di abitanti. La potenza delle attrezzature per telecomunicazioni, come ad esempio i *routers*, dovranno sostenere il traffico di 1 terabyte al secondo, un multiplo del traffico attuale. Al contempo il ruolo di campioni nazionali del settore telecomunicazioni nella posa e gestione dell'infrastruttura 'pesante', tra cui i cavi sottomarini, va ridefinendo una nuova "geopolitica digitale". Tali network diventano pertanto un elemento cruciale anche nei rapporti tra paesi, alla stregua di reti elettriche e di connessioni stradali e ferroviarie.

L'innovazione diffusa, grazie alle interconnessioni tecnologiche, sta alla base della Quarta Rivoluzione Industriale in atto - con sconvolgimenti sociali, politici e culturali ed un impatto epocale sulle istituzioni, l'industria e gli individui. La capacità di gestire questo cambiamento senza alzare barriere, bensì tutelando la sicurezza collettiva con un approccio coordinato e regole univoche tra paesi, rappresenta una delle maggiori sfide per i *policy makers* globali.

La *Cyber-security*, infatti, ha assunto rilevanza sistemica a seguito del proliferare di attacchi informatici che hanno causato gravi danni ad aziende e governi. Come per la criminalità tradizionale, l'obiettivo non deve essere azzerare i casi di minacce cibernetiche, bensì ridurle ad un livello minimo con cui si possa convivere - ovvero preservare i benefici delle nuove tecnologie per la società, contenendone il lato oscuro rappresentato da soggetti malevoli e dei *malware* con cui agiscono. Questi hanno ormai raggiunto un livello di sofisticazione tale per cui affrontano l'intelligenza artificiale dei computer con gli stessi meccanismi di *machine-learning*, in una guerra tra pari. Così come i criminali ordinari si riconoscono spesso per un comportamento anomalo, così il *malware* può solo essere intercettato e riconosciuto osservando trend anomali nel traffico dati, senza necessariamente cercare di individuare i singoli soggetti. Sono numerosi i casi in cui soggetti criminali riescono a penetrare il sistema, deviare i flussi e appropriarsi dei fondi o anche solo dati personali dei clienti, minacciandone la diffusione dietro richiesta di ricompensa – alla stregua dei terroristi. In tali casi i responsabili del business ed esperti legali sono chiamati a reazioni immediate, con le dovute competenze in nuovi ambiti tecnologici che hanno dato vita a nuove specializzazioni e professioni, sconosciute fino a pochi anni fa.

Da questa necessità di gestire e proteggere il traffico dei dati, scaturisce la nuova sfida per i soggetti preposti alla sicurezza (agenzie governative, nello specifico) ed un potenziale conflitto tra la tutela degli individui e la loro privacy, come uno dei pilastri della democrazia moderna. La fiducia dei cittadini nei loro governi diventa pertanto cruciale, e l'introduzione di specifiche leggi in ambito cyber-security e protezione dei dati diventa sempre più attuale: nel caso dell'Unione Europea la tutela dei diritti del cittadino (vedi la stringente normativa GDPR) rappresenta il fulcro - mentre in Cina lo è la stabilità del sistema, e quindi del potere centrale, a scapito della privacy dell'individuo.

Nel caso della Russia, il *cyber-space* è uno strumento per espandere la propria influenza all'estero, mentre per gli Stati Uniti lo è soprattutto a beneficio dell'economia, oltre che di influenza internazionale. La regolamentazione dello spazio digitale globale rappresenta, dunque, la ricerca di un equilibrio sensibile tra interessi spesso divergenti tra democrazie liberali e "regimi digitali" autocratici. La definizione di un quadro normativo condiviso e omogeneo a livello internazionale, nella misura realisticamente possibile, è ormai una priorità.

Il "sistema a innovazione aperta" e l'esperienza israeliana

In un contesto internazionale sempre più complesso, Israele rappresenta un esempio virtuoso di ecosistema a innovazione aperta. Lo spirito di innovazione diffuso in tutta la società, conosciuta nel mondo come "nazione start-up", deriva in gran parte dalla sua storia contemporanea e dall'esigenza di innovare per necessità, a partire dall'agricoltura e dal settore della difesa. Agli albori dello Stato Israeliano, in mancanza di risorse naturali, è stato infatti il capitale umano la risorsa più importante per creare le basi della prosperità nazionale. A partire dal 2010, il Governo ha avviato un programma di condivisione del know-how in ambito militare, accumulato in oltre 30 anni di investimenti, a beneficio della sperimentazione in altri segmenti del settore privato.

Oggi, Israele rappresenta un centro di eccellenza mondiale nelle tecnologie avanzate: l'intelligenza artificiale è ormai applicata con successo ai settori della sicurezza, sanità, biotecnologie e servizi finanziari, ed il numero di start-up (6.600 in base a dati OECD e 20.000 brevetti, per 8,8 milioni di abitanti) rappresenta un primato mondiale.
Le fondamenta di questo modello si basano su tre componenti che si integrano con successo, come in pochi altri paesi: ricerca accademica di base, partecipazione attiva dello Stato e capitali privati. L'università svolge un ruolo primario con ricerche ad alto tasso di insuccesso; lo Stato partecipa con fondi pubblici a numerose iniziative e ricerche; il mercato apporta capitali privati da fondi di Venture Capital, *business angels* e aziende internazionali (da capitali privati esteri deriva oggi l'85% degli investimenti). Esempi di questo sistema di innovazione aperta sono professori universitari che al contempo svolgono il ruolo di CEO in aziende tecnologiche, oltre ad un ruolo di *Chief Scientist* in organismi governativi. Una certa flessibilità legislativa è pertanto indispensabile per consentire la disseminazione delle competenze, a beneficio dell'ecosistema.

Le sinergie tra mondo accademico, governo e settore privato hanno favorito lo sviluppo di un ambiente unico, favorevole all'innovazione e all'imprenditoria giovanile, che ha portato alla nascita di migliaia di start-up e ha fatto registrare investimenti pro capite record, in gran parte coperti da capitali privati stranieri. Il governo, forze armate incluse, è in grado di attrarre i migliori talenti accademici in progetti di ricerca in tutti i settori, compresi quelli dell'IT e della sicurezza informatica. L'azione di stimolo incrociato che ne risulta, assieme

alla capacità di attrarre capitale privato, sono rappresentate al meglio nel cluster ad alta tecnologia "Silicon Wadi", situato nei pressi di Tel Aviv, che è diventato uno dei migliori incubatori di start-up del mondo.

In confronto, l'Unione Europea è attanagliata da legislazione sempre più articolata e invasiva, con l'obiettivo primario di tutelare gli interessi dei consumatori, la concorrenza e la protezione dei dati. Inoltre, vincoli di budget a livello governativo hanno ridotto gli investimenti a favore della ricerca a livelli minimi, se raffrontati agli Stati Uniti e la Cina, oltre che all'esempio israeliano. In Italia, inoltre, la ricerca universitaria continua a non trovare sinergie ed un *modus operandi* continuativo con le grandi aziende e le loro esigenze di innovazione e sviluppo. Una condivisione continuativa di esperienze tra *stakeholders* israeliani, pionieri del suddetto modello virtuoso, e controparti italiane ed europee avrebbe pertanto un grande impatto a livello di fertilizzazione e apprendimento delle migliori pratiche e casi di successo.

La trasformazione digitale ed il business post 4.0

L'impatto delle nuove tecnologie e la digitalizzazione sta radicalmente trasformando interi settori economici, dove modelli tradizionali sono costretti (e incentivati) ad evolversi rapidamente per stare al passo con il mondo del business "post 4.0". Ne sono impattati alcuni settori fondamentali, come le biotecnologie e la bioingegneria in campo medico; l'efficienza energetica (risorse rinnovabili, energia pulita e *smart grids*); il fintech; le città intelligenti e la qualità della vita; le nuove tecnologie nell'agricoltura.

In particolare, settori come la finanza vedono le aziende tradizionali, in passato leader nei rispettivi ambiti, sotto attacco da nuovi attori ad alto contenuto tecnologico. Agevolati anche da nuova legislazione alquanto favorevole ai nuovi entranti (vedi la direttiva PSD2 in Europa), società fintech possono disporre di enormi basi-dati sui clienti, sia visualizzando i loro rapporti bancari che dall'interazione con numerose applicazioni "allodola" sugli smartphone rielaborate da algoritmi, che permettono di tracciare profili comportamentali di ogni consumatore.

La struttura dei costi delle banche tradizionali, ancora basata su reti di sportelli fisici, e soprattutto la stringente regolamentazione (sia su livelli di capitale e liquidità, che sulla gestione dei dati dei clienti), rende la competizione del tutto squilibrata. Tuttavia, il patrimonio di conoscenza reale tra le banche ed i loro clienti, accumulata in anni di interazione anche a livello famigliare, sarà molto difficile da conseguire dai nuovi entranti, che basano le analisi dei loro *data scientists* su comportamenti degli individui nel mondo virtuale - ad esempio i social media - che spesso lasciano volutamente tracce fuorvianti del proprio profilo. Inoltre, gli stessi algoritmi che stanno alla base del *machine learning* e analisi comportamentali basati su dati di massa, sono spesso contaminati da cosiddetti *bias* insiti nelle serie storiche o nella cultura di chi la progettati: ne sono un esempio la considerazione

della popolazione afro-americana negli Stati Uniti e correlazione con livello di istruzione e tasso di criminalità, non sempre attendibile in prospettiva futura.
Pertanto, la concorrenza introdotta dal fintech in alcuni segmenti della catena del valore delle banche (come i pagamenti istantanei, ad esempio, o soluzioni di risparmio) non necessariamente devono portare alla distruzione di valore – o addirittura all'estinzione del modello tradizionale, anche considerando la esigua profittabilità finora dimostrata dalla grande maggioranza dei *disruptors* digitali. I due modelli possono, invece, coesistere e cercare sinergie nell'ambito dell'intelligenza artificiale per l'analisi comportamentale e predittiva dei clienti, dei pagamenti basati su nuove tecnologie - blockchain ad esempio - e di efficienza e rapidità nella gestione delle richieste dei clienti - in particolare delle piccole e medie imprese, il cui accesso al credito è uno dei fattori principali per la crescita dell'economia, degli investimenti e dell'occupazione in Europa.

Diversi altri settori, oltre alla finanza, possono beneficiare dalla convergenza tra aziende tradizionali e nuovi attori tecnologici. Ne è un esempio il settore farmaceutico, nell'ambito più ampio di *life sciences*: grazie alle nuove tecnologie ed all'intelligenza artificiale, la nuova frontiera è rappresentata da cure basate su farmaci personalizzati, adattate a ciascuno individuo - in base all'analisi del suo genoma e dei trenta miliardi di cellule di ogni organismo umano (oltre a quaranta miliardi di batteri e virus che lo popolano). I benefici del *machine learning* si estendono anche alla ricerca e sviluppo di nuovi farmaci, il cui costo è tradizionalmente oberato (in alcuni casi per l'80% del totale) da fattori regolamentari e test necessari su un campione sufficientemente ampio; tali costi possono essere drasticamente abbattuti grazie ad analisi delle serie storiche e algoritmi incentrati sull'A.I, a beneficio di una diffusione molto più ampia di nuovi medicinali.

Simili sviluppi sono già in atto in ambito medico, dove robot comandati a distanza risultano più affidabili per interventi di microchirurgia, e nel campo della nutrizione, dove gravi lacune culturali - ad esempio il diabete diffuso tra le donne arabe - sono state affrontate con successo da start-up israeliane, volte a migliorare l'educazione alimentare nelle popolazioni mediorientali – abbattendo anche barriere culturali e religiose.
Questa visione a lungo termine, al di là dei benefici che apporta alle industrie tecnologiche, può evolvere ulteriormente a vantaggio di tutta la società, considerando che la parte maggioritaria della popolazione israeliana (circa il 90%) non lavora direttamente nel dinamico mondo dell'high tech, bensì in settori tradizionali. L'applicazione dell'intelligenza artificiale ai campi più disparati può infatti innescare un ciclo virtuoso di ricadute su tutti gli altri settori, come quello dell'arte.

Uno scambio di esperienze continuativo può offrire interessanti prospettive di confronto e collaborazione tra i due paesi: il patrimonio culturale italiano, la creatività diffusa e la complementarità con Israele in molti settori industriali e agricoli, così come il turismo,

offrono opportunità significative per superare le tradizionali inefficienze, grazie a tecnologie e innovazioni all'avanguardia.

Selezione di articoli da
Aspenia e Aspenia Online

DIGITAL GEOPOLITICS - SPECIAL ISSUE IN COOPERATION WI...

ECONOMY & FINANCE | SOCIETY & CULTURE | TECHNOLOGY & SCIENCE

A business model for digital integration

By **Hal Varian** On **Dec 3, 2019**

Though all businesses depend on economies of scale (whether on the supply side or the demand side), learning-by-doing is crucial, particularly to high-tech enterprises. Learning is indeed essential and requires investments in data collection, analysis and testing. And this is where competition between the high tech giants is now taking place, also involving start-ups, as long as they are willing to invest in expertise.

The term "network economies" has a precise and clear economic meaning, yet neoeconomists tend to confuse it with other concepts, such as incremental returns to scale and "learning-by-doing". This article seeks to clarify the matter.

THE IMPORTANCE OF LEARNING-BY-DOING. Let us consider the following definitions.

Economies of scale – demand-side. The benefit that each subsequent user derives from the enjoyment of a service is greater the more users have already enjoyed it (network economies, network externalities).

Economies of scale – supply side. The incremental production cost of an output (or of an incremental improvement in quality) diminishes as output increases (growing returns to scale).

Learning-by-doing. The unit production cost (or incremental improvement in quality) decreases as output increases (learning curve, or experience curve).

I consider the "demand-side" and "supply-side" definitions of economies of scale extremely useful, because they immediately highlight the virtuous mechanism that generates the phenomenon. Network economies depend on enhanced value based on the number of units sold, whereas returns to scale are based on cost reductions or improvements in quality in relation to the number of units produced.

The difference between economies of scale on the supply side and learning-by-doing has to do with timing: learning-by-doing is usually defined in relation to output or cumulative investments, whereas economies of scale relate to production levels during a certain period of time.

These kinds of increasing returns to scale are driven by different forces. Network economies cannot be separated from market shares. They are indeed included as a premise of the model: the value of a product to consumers depends on its market share. By contrast, it is the dimension, or the level of production (not the market share itself) that is the decisive factor in returns to scale. When it comes to learning-by-doing it is experience that counts.

In the economic literature, experience is often measured by cumulative output. Though it is a useful simplification of the model, this approach may be somewhat misleading inasmuch as it suggests that "learning" is a passive activity that occurs automatically when a greater quantity of output is produced. Nothing could be further from the truth. Learning-by-doing necessarily requires investments in data gathering, analysis and testing.

Learning is crucially important to economic progress. However, it does not occur "simply"; it requires investments both at the individual level and at the organizational level as well as at the level of society as a whole. Data gathering is only the first step. To be useful, data needs to be turned into information, knowledge and understanding.

Economies of scale on the supply and demand sides are certainly major economic forces. However, they lose much of their significance in relation to learning-by-doing, which I consider the main source of competitive advantage in technological industries.

SEARCH ENGINES AND ECONOMIES OF SCALE. In view of the above, we may wonder whether or not search engines such as Google, Bing, Yandex and Baidu represent network economies. Do we need to know how many other people use the same search engine as us? Of course not. The important thing is the performance of the search engine itself, not the number of people using it. This means that traditional economies of scale do not apply to search engines.

In the early 2000s there were several general-purpose search engines: Alta Vista, Lycos, Inktomi, Yahoo, Microsoft Live and Google (Lycos, Inktomi and Google stemmed from the NSF/DARPA digital library research program – an initial example of how the funding of government research can contribute to innovation and increase productivity). In those days, people commonly used several search engines.

As time went by, some search engines were able to improve their performance, while others lagged behind. There was no apparent advantage due to scale. Indeed, it was often the newest and smallest engine that seemed to work best and to improve most rapidly. This resulted in a consolidation of the sector marked by the presence of a small number of general-purpose search engines.

During this same period of consolidation, we witnessed the emergence of several "special-purpose" search engines for local searches, shopping, travel and so forth. Such search engines tend to focus on commercial considerations – for example, on which areas the most money is in circulation. If we consider commercial searches rather than general purpose searches, the structure of the sector is very different. Some 44% of searches for products start on Amazon, 34% on a search engine and 31% on a specific vendor's website. This observation is particularly important because the searches most economically advantageous to general purpose search engines are commercial ones, mostly because they attract more advertising. General purpose searches are a particularly difficult area of business because they permit the sale of 6% of what is actually produced (that is, from pay clicks alone). There is fierce competition here, but, as may easily be deduced, they fall short when it comes to producing free clicks.

Though traditional economies of scale on the demand side do not apply to searches, can economies of scale apply on the supply side? Internet multinationals such as Amazon, Google, Facebook, Microsoft and IBM have data centers throughout the world. Many of these companies lease part of their computer and networking infrastructure. This cloud computing technology has the advantage of allowing new players to increase their calculation infrastructure requirements as their operational scale increases. Data centers, which in the past represented a fixed cost, have now become a variable cost, thus generating a considerable increase in income for technological start-ups.

The hardware component of IT now represents a constant return with a view to industrial growth. Clients can order computational power on demand. Providers operating data centers can offer greater power by enhancing the CPU's core, by increasing the number of CPUs on the motherboard, increasing the number of motherboards on the rack in the data center or even increasing the number of data centers. Each level of increase corresponds to an increase in performance more or less in line with demand.

It is a different matter when it comes to software. Once an investment has been made to develop a piece of software, it can be replicated at almost zero marginal cost. In this regard, software is a perfect example of the learning concept.

INDIRECT NETWORK ECONOMIES. Some observers have said that search engines demonstrate two kinds of network economies, since advertisers want to be where the most users are, and users want to be where the most advertisers are. However, this latter assertion is difficult to confirm in practice, in view of the fact that users generally do not choose a search engine on the basis of the number of advertisements. If anything, given the choice between two search engines, consumers would probably prefer the one with fewer advertisements.

If traditional network economies do not work with search engines, what can indirect economies of scale achieve? This concept implies a somewhat more complex virtuous circle. Let us consider an operating system involving three parts: the vendor of the operating system, the developers of applications for the operating system and the clients that purchase both the operating system and the applications.

Let us assume that two vendors of operating systems are in competition. Application developers may consider this beneficial with a view to creating applications for whatever system has the largest number of users; users, in turn, may consider such an operating system advantageous because it includes a variety of applications. This situation could entail a virtuous cycle: more users means more developers and more developers means more users. The result is a winner-takes-all market, in which the best can capture a very large market share, thereby reducing – if not eliminating – the competition.

Such a model may be attractive, but it does not necessarily correspond to the facts. After all, there are three operating systems for the pc (Linux, Windows and Mac OS), and two main operating systems for mobile devices (iOS and Android). There seems to be room for more than one operating system for both desktops and mobile devices. There appear to be fewer indirect network economies than is commonly thought. Indeed, application developers are involved on several platforms and can offer applications for both main operating systems for mobile devices.

THE VALUE OF KNOWLEDGE. One variation on the theme that we have been considering concerns so-called “data entry barriers”. The idea is that a major player already working in the sector (an incumbent) has a larger quantity of data from its users, which enables it to develop better products than its potential competitors, thus granting it an unbeatable competitive edge.

The first and most obvious point is that if there is a data barrier to entry, it applies to all industries. After all, players already involved in the sector do indeed produce a good or a service, unlike newcomers. So by definition incumbents must have more

data than new players. Thousands of new companies are formed every year and the fact that they have less data than their established competitors does not seem to discourage them in the least.

But is starting a new business a matter of data or knowledge? For instance, if I wanted to enter the car manufacturing industry but knew absolutely nothing about how to build a car, should this be regarded as a barrier to entry?

Knowledge is a crucial part of production. In economic models, knowledge is embodied in the production function, but in the real world it is embodied in people. If you want to launch a car company but know nothing about how to build a car, the first thing you would have to do is to hire car engineers having the necessary expertise.

In the search engines sector, new competitors – who may have started trading without any data – have often successfully competed with players already established in the market. Google was not the first search engine, but it had a better algorithm than other existing players. Furthermore, it succeeded in building a learning system that constantly improves on the basis of the initial algorithm.

When they entered the market, the companies that are now successful did not have the same data that they have now, but they were still able to acquire sufficient initial expertise and to gather sufficient data, information and expertise to gain a competitive advantage over players already in the market.

It is enough to consider, for instance, the way in which Google gained experience in the voice recognition sector in 2006. The first thing it did was to hire top researchers in the field, who are the ones that supplied Google with its knowledge. These researchers developed GOOG-411, a service that used voice recognition for phone directory services. The team's key intuition was to implement the voice recognition algorithm in the cloud rather than on individual devices; and this enabled the algorithm to learn – literally – from millions of verbal requests. Within the space of a few months, the algorithm became very good, and by the end of the year it was one of the best voice recognition systems available. Some years later, the Google Brain teams were able to apply neural networks to criticalities relating to voice recognition and thus to improve performance further.

Table 1 – Competition between internet providers

Table 1 • Competition between internet providers

Product	AMAZON	APPLE	GOOGLE	FB	MICROSOFT
advertising platforms	X		X	X	X
artificial intelligence	X	X	X	X	X
browsers	X	X	X		X
cloud services	X		X		X
digital assistants	X	X	X	X	X
ebooks	X	X	X		
email and messaging		X	X	X	X
general purpose search engines			X		X
home delivery services	X		X		
maps		X	X		X
office tools		X	X		X
operating systems	X	X	X		X
smartphones	X	X	X		X
social networks			X	X	
special purpose search engines	X	X	X	X	X
streaming video	X		X	X	
video and music distribution	X	X	X		
video conferencing		X	X	X	X

However, other companies, too, are implementing similar improvements. Amazon has developed Echo and has set itself the target of recognizing and answering voice requests more quickly than has been possible hitherto. When Echo was first developed, the average response time was about 2.5-3 seconds. The working team set itself a target of 2 seconds. But that was not good enough for Jeff Bezos, who called for a latency of just 1 second. This target has yet to be achieved, but they have managed a latency of as little as 1.5 seconds, which is better than any other technology available at the present time.

INVESTING IN EXPERTISE AND KNOWLEDGE. I have described three concepts: network economies, returns on scale and learning-by-doing. Network economies are a demand-side phenomenon (the value depends on sharing), whereas the other two effects are supply-side phenomena (the cost depends on current or cumulative output).

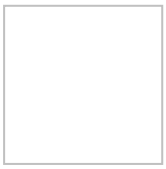
If we consider the leading high-tech companies of today, we see strong competition. As the table shows, they are all competing in several different sectors. This competition is the reason why we can see such rapid innovation and such low costs

in the technology industries.

All these companies invest heavily in expertise. At any particular moment, they may have different capabilities, but they can overcome shortcomings by learning quickly. At one time, Google did not know much about operating systems or voice recognition, Facebook knew little about video streaming and image searches and Amazon knew little about selling cloud computing. But they learned fast and the knowledge that they accumulated is the key reason for their competitive advantage in online industries.

The opinions expressed are exclusively those of the author and do not necessarily reflect Google's opinions.

economy world technology digital social media



Hal Varian

Hal Varian is Chief Economist with Google. He is a professor emeritus at the University of California and the Berkeley School of Information, specializing in microeconomics and information economics.

Niccolò Serri

Democracy and digital authoritarianism

The technology of artificial intelligence is foreshadowing a monumental step for the world. Machine learning techniques have increased the analytic and reasoning capabilities of algorithms enormously, while deep learning promises to create software that works in ways similar to the human brain. This change affects every aspect of our economy and society, and is having a major impact on global geopolitics.

It is interesting to analyze the paradigm shift produced by artificial intelligence, taking into consideration how the major powers are addressing the technological challenge of AI in their national security strategies. While the United States and China vie for sector hegemony in a Cold War-style scenario, the European Union lags behind. The Old World is lacking in dynamism as well as major high tech companies and, above all, it invests very little in AI. In order to pull itself up, Brussels is going to have to invest more decisively in the ethical development of new technologies that are culturally compatible with their values.

Niccolò Serri is a researcher at the Fondazione Leonardo Civiltà delle Macchine.

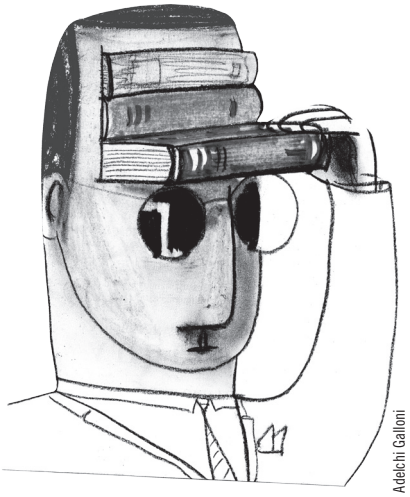
In the specific field of defense, the effects of AI promise to be groundbreaking and to revolutionize the way in which military conflicts are fought and won. The application of algorithms, along with developments in advanced robotics, are already having an effect on battlefields, improving the decision-making independence of war machinery. These developments are evident in everything from aircraft to ground vehicles, moving the human element to the margins of the combat zone. It is therefore no accident that intellectuals and entrepreneurs – from Stephen Hawking to Elon Musk – have opposed the use of lethal autonomous weapons. Not only that, but AI has opened new fronts for confrontation between world powers by shifting the theme of national security to the cyber realm of man/machine relations, where it is data that counts. The interconnectivity associated with the Internet of Things is allowing for new and advanced forms of espionage, and the moment is not far off when it will be possible for hackers to pre-emptively attack and dismantle an adversary's defenses.

In early 2018, the Trump administration launched a collaboration with Google to improve its drones' visual recognition capability. (Following the protests of its employees, the Mountain View colossus announced that it had decided not to renew the project, known as Maven, for this year.) Still, from Russia to Israel, and even including governments with fewer actual military units (such as Singapore), countries are seizing the opportunity to automate war.

THE TRANSFORMATION OF NATIONAL POWER. In reality, the transformation is much broader: the development of AI is going to influence international geopolitics at a level much deeper than mere military structures.

As Michael Horowitz points out, rather than a specific-use technology, AI is a "general enabler" comparable to a combustion engine or electricity, with equal benefits for various sectors of the economy. According to estimates by

McKinsey, automation will lead to the replacement of over one third of existing jobs by the year 2030, resulting in major gains in industrial productivity and in the services sector. The economic transformation is not going to be simple, with the inevitable computerization of government and the social reorganization that will involve.



Adelchi Galloni

The implementation of a rising number of technologies associated with AI and its direct impact on growth is sure to alter the economic underpinning of national power, thereby increasing inequality among countries capable of embracing innovation and those that lag behind. By its very nature, AI is a sector that offers considerable advantages of position – strategically speaking, the first-mover advantage. Indeed, the industrialization of intelligence has not only immediate economic effects, but also tends to accelerate the development of the entire national technological ecosystem by triggering a virtuous development circle likely to open inroads for other less technologically advanced countries. Thanks to innovations such as 5G, the increased connection range and speed of many devices will give an exponential boost to data collection and analysis capacity. The question that remains, however, is who will control the new connection infrastructures.

THE HI-TECH COLD WAR. Given the geopolitical importance of technology, fierce competition between the major powers was to be expected. As in the years of the space race during the Cold War, the technological challenge of AI was destined to assume an immediate nationalistic tone. By September 2017, Russian president Vladimir Putin was already predicting that whoever became the leader in this sector would "rule the world". The United States of America, cradle of the internet civilization and robotics research, still maintains global primacy in terms of total computational capacity and business-oriented technological applications.

The AI sector attracted over 10 billion dollars in venture capital in 2017 alone, in addition to government funding and strategic investments in major Silicon Valley firms such as Apple and Facebook. Nevertheless, this development is not being driven within a strategic public policy framework, but is guided by an essentially laissez-faire innovation model in which the sector remains largely unregulated and private enterprise is given considerable decision-making autonomy. This ensures a dynamic economic system, but it also has the negative aspects identified in a study commissioned by Barack Obama from the White House Science and Technology Policy Office in 2016, which highlighted the administration's difficulty channeling AI research toward sectors considered strategic, such as the military, despite its numerous potential dual applications.

Challenging the United States for leadership is China, which in July 2017 began investing heavily in a ten year AI development plan, mobilizing its massive resources in an effort to secure a dominant position in the new technologies. The Asian giant has no lack of structural problems holding it back, starting with an economic development model that invested little in the past in the technological content of its exports. Nevertheless, the approach by the centralized government of the People's Republic has produced immedi-

ate results, utilizing large sector companies – Weibo, Tencent and Alibaba – as no less than an extension of its industrial policy. China already has the largest number of the world's top 500 super computers and excels in the number of scientific articles published in the field of deep learning. Beijing aims to become the top sector superpower by 2030, with an increasingly valuable AI industry.

China's rapid technological advancement has rekindled a geopolitical competition with the United States that was already being stoked by Donald Trump's neoprotectionist promises. The skirmish recently centered on the Chinese telecommunications company Huawei, accused of industrial espionage and banned by the nation members of the intelligence alliance established by the UKUSA multilateral accord.

DIGITAL AUTHORITARIANISM. Naturally, this competition also has ideological aspects. Referring precisely to China's technological development model, the non-governmental organization Freedom House has spoken of "digital authoritarianism", of how AI and Big Data analysis have allowed the People's Republic of China to slash the costs of repression.

Since 1994, the Great Firewall of China has been preventively censoring internet content considered socially dangerous. The development of automatic analysis and facial recognition algorithms has extended surveillance to many areas of the physical and digital lives of Chinese citizens, transforming the Weibo social network and WeChat messaging app into a means for the pre-emptive control of dissent. In 2015, the authorities also began to introduce a social credit system that ranks each individual citizen's conduct by cross-referencing the data of various devices. In essence, the political use of AI has transformed the internet from a tool for individual freedom into a panopticon for use by the government. This undermines the argument of

those who have always considered technological development as synonymous with individual freedom; it undoubtedly clashes with the fundamentals of a liberal political model based on the democratic centrality of privacy and property rights.

The international technopolitical panorama is therefore being redefined in terms of a new bipolarism, with the US and China waging the battle for international influence along the lines of their respective commercial expansion. China's New Silk Road project across Eurasia calls for major infrastructure investments in cabling and mobile radio networks, while the technologies being developed by Chinese firms are already being exported to other authoritarian contexts in the Middle East and Africa. Russia's role is, for now, a secondary one, concerned mainly with more aggressive forms of AI for military use and for disrupting the political processes of its adversaries. The European Union risks seeing its strategic position in this sector compromised. According to a study by PricewaterhouseCoopers, to date, 70% of global AI economic impact will be concentrated in North America and China.

EUROPE LAGS BEHIND. Europe remains the largest AI and robotics research hub, producing a larger number of scientific articles than the US or China. However, it is having difficulty transforming this pre-eminence into economic power and practical technology.

This is due, first, to its lack of a coordinated industrial policy framework at central level, with member states continuing to act for the most part independently of Brussels. France, for example, has made AI a strategic priority, placing mathematician Cedric Villani at the head of a parliamentary task force to draw up the development guidelines that were published in March 2018 in the "AI for Humanity" report. Germany, on the other hand, still lacks a national AI plan, operating mainly at regional level (for example,

funding a Baden-Württemberg "cyber valley"). A series of minor states, such as Estonia and Finland, are working on integrating algorithms into their public administrations – in anticipation of the impact that technologies are going to have on government functions – but remain too marginal to act as a sector development driver for the whole of Europe.

The lack of an integrated AI industrial policy at European level has impeded the rise of national champions capable of meeting the Sino-American competition and promoting the interests of the Old World. According to Stratfor, SAP SE is the only European hi-tech company worth more than 100 billion dollars. The inability to foster the development of large-scale enterprise in technologically advanced sectors is also reflected in a less innovative ecosystem for start-ups. Again, according to Stratfor, Europe has no more than a couple of dozen "unicorns" – new firms valued at a billion dollars or more – while the United States has over a hundred. Most importantly, approximately half of European start-ups currently engaged in AI are located in the United Kingdom. Thus, Brexit is going to have some major repercussions, not only geopolitically but also for European technology policies.

The lack of investments is surely a decisive factor in this. The public and private resources that Europe has made available fall well below the self-financing abilities of Silicon Valley and those of the PRC. Aware of the shortfall, in April 2018 the European Commission allotted 1.5 billion euro for investments in AI within the framework of the Horizon 2020 program. Brussels will seek to invest a total of 20 billion euro in the sector by that date through private partnerships within the strategy of the Single Digital Market launched in May of 2015.

But increased investments in artificial intelligence may not be enough. Uniformity of data is an essential requirement for making algorithms more efficient and capable of operating in the real world of decision-making. In this

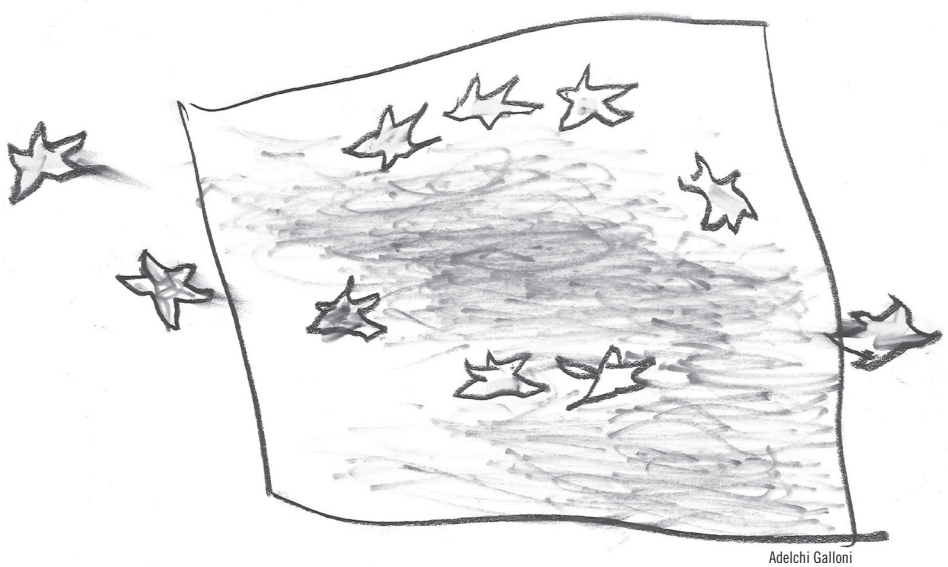
regard, the EU's regulatory fragmentation poses a considerable obstacle to development on the scale necessary to compete on the global market. European Union members have strict rules on the dissemination and licensed use of data – to the point of obliging their physical storage on servers located within national borders – while linguistic differences render the development of continent-wide integrated software complex.

From the digital point of view, and despite a potential pool of more than half a billion users, the European market is still scarce, compared with the United States and China. Indeed, these two sovereign states have the benefit of a homogeneous administration and a broader user-base, especially in the case of Beijing. If data will soon become the oil of the future economy, as *The Economist* recently predicted, then China is tomorrow's Saudi Arabia.

IN SEARCH OF A MODEL. In order to get into the global AI race, the EU is not only going to have to develop its own industrial model, balancing state intervention and market so as to foster an efficient approach to innovation; it must also, and above all, offer new quality standards. Neither the American deregulation model nor Chinese authoritarianism offers guarantees regarding the shared rules by which to address the social impact of the new technologies. Europe, on the other hand, has the opportunity to make a difference through ethically sound and transparent technological development, strict rules on the protection of personal data and the development of an innovative legal framework capable of regulating artificial intelligence in terms of legal liability. This would make possible the development of a technological "soft power" to ensure common rights. At the same time, an ethical European AI model would foster a sort of informal protectionism for the continent's businesses by exploiting the cultural differences with America and the Asian giants.

The EU General Data Protection Regulation – in force since May 2018 – has already increased costs for some major American firms, forcing them to review their own personal data rules. In December, Brussels presented a coordinated AI plan in which it urges – in addition to the goals of increasing investments through public/private partnerships and creating common data repositories – the moral and reliable development of new technologies. That same month, a committee of EU experts published a first draft of the ethical guidelines that the Commission intends to adopt in matters of new technologies.

In order to seize the opportunities offered by the technology challenge and be a player in the geopolitical game of the future, Europe is going to have to embrace the values of a new digital humanism: guiding research, opening new areas for investment and offering a cultural bulwark against authoritarian and materialistic models that threaten to transform the promise of artificial intelligence into a new dystopia.



Adelchi Galloni

Luca Dal Fabbro

The energy internet revolution

Artificial intelligence looks set to become a formidable accelerator in the transition to a more sustainable world. The energy industry is unquestionably one of the many areas likely to be affected by this revolution. The introduction of smart networks and devices will lead to an "energy internet" capable of radically transforming the industry. Both opportunities and challenges abound, and Italy is rising to the occasion.

Artificial intelligence (AI) is going to be the next game changer in many areas of the global economy, from transportation and the manufacturing industry to energy and domotics (information technology in the home). A recent study conducted by the International Data Corp shows that annual global investment in AI is going to double by 2022, hitting the $80 billion mark. As far as the energy industry is concerned, it would not be far-fetched to state that it is going to experience a new industrial revolution, thanks precisely to AI. This might be called the "energy internet revolution".

Addressing a post to twenty-year-old students on his

Luca Dal Fabbro is Chairman of Snam, Europe's leading gas utility.

blog, Microsoft founder Bill Gates wrote that artificial intelligence and energy are two of the three areas of industry (the third is biotechnology) that are going to have a huge impact on the world in the near future – an impact akin to that of the digital revolution back in the 1980s. According to Gates, AI is going to make our lives "more productive and more creative", while making energy "cleaner, cheaper and more reliable"; it is going to help fight climate change and poverty.

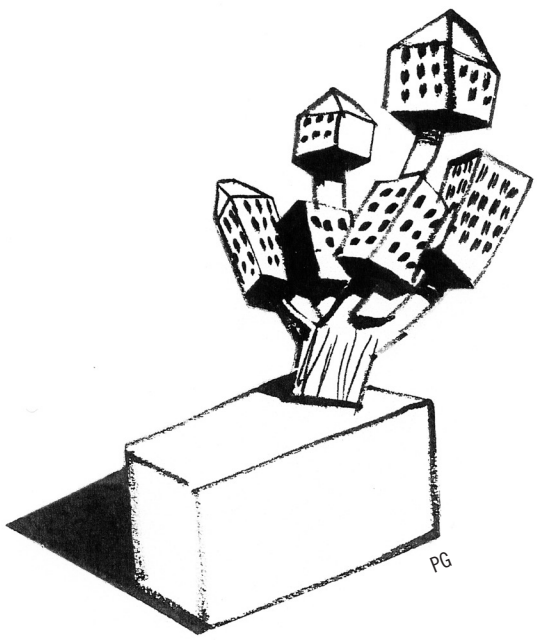
The International Energy Agency (IEA) has predicted that in the energy sphere AI is going to play a crucial role over the coming years, and that it is going to radically transform our systems, making them more interconnected, more reliable and more sustainable.

AI projects and applications in the energy industry, the growing amount of information and data available and the ability to analyze that data are going to boost energy security and efficiency, reduce greenhouse gas emissions, mitigate climate change and help to develop a more rational approach to consumption.

At the end of the day, artificial intelligence is going to be the tool that helps the industry transform the huge mass of data available into new solutions for the challenges facing us, starting with the so-called "three Ds of energy transition": decarbonization, decentralization and digitalization.

As early as the next decade, widespread infrastructure interconnection, the systematic use of advanced monitoring instruments and sensors, the development of innovative methodologies and technologies for extracting and processing Big Data and recourse to integrated tools for analysis and forecast models are all going to bring radical change to every aspect of the industry's profile. In the context of renewable energy production and of the consumption of energy in general, there are many complex issues for which AI can find solutions. Indeed, numerous projects have already been set in motion on the basis of this technology.

AI FOR EFFICIENCY AND RENEWABLE ENERGY. The first radical transformation is going to concern energy efficiency. Google, for example, has succeeded in reducing its data center's consumption, and thus its emissions, by 15% thanks to automatic learning systems. But it is not only the giant corporations that have access to AI. Small and medium-sized enterprises are also going to benefit from it. The home environment is one of the areas with the greatest potential. It has been estimated that by 2040 there will be 1 billion smart homes and 11 billion smart household appliances in the world. Their optimization, made possible by artificial intelligence, will slash energy consumption in the home by more than 10%. These interconnected networks are going to generate a huge mass of data that can be used by energy companies to provide consumers with tailor-made solutions.



The revolution is going to impact cities primarily, where it has been estimated that 60% of the world's population will be living by 2030. Smarter cities will consume less energy per inhabitant thanks to new technologies. But AI

solutions are also going to impact rural areas and, in general, less developed countries, thus paving the way for major opportunities in the struggle against inequality and energy poverty.

Where the production of energy from renewable sources is concerned, predictive systems will be able to help resolve the problems occasioned by uncertain weather conditions and to optimize production. By integrating their own weather data with weather data from satellites in real time, AI systems are capable of identifying recurring patterns, of maximizing efficiency and of minimizing the risks for the supply of electric energy. With its Digital Wind Farm project, GE Energy has successfully managed to optimize the output of its wind-energy turbines, boosting that output by 20%.

NEW SMART NETWORKS. The development of an energy internet is also going to have a considerable impact on large energy networks; these will become an increasingly strategic asset in that they will be increasingly smart and capable of combining their traditional function with the ability to send and to process a growing mass of data. Kevin Ashton, the English engineer who invented the expression "Internet of Things" (IoT) twenty years ago, defined it as a computer's ability to see, sense and smell the world. Well, that is exactly what is happening and is going to happen more and more to large energy networks in the coming years.

The growing use of AI techniques and of machine learning to monitor networks can bring major benefits in terms of optimization, maintenance and emission reduction. In the gas industry, for example, recourse to increasingly advanced monitoring technologies can help to combat methane leakage and thus boost our efficiency in the transition from carbon to methane in an effort to contain CO_2 emissions.

With machine learning systems it is possible to predict peak demand for

electricity in real time and thus optimize dispatching. Google reckons that with its machine learning systems it can maximize the use of renewable sources in the grids and optimize energy use by 10% without needing new infrastructures. Open Energi has estimated that in the United Kingdom alone there is a 6 GW flexibility on the demand side on which it can count at peak evening times without any repercussions for the end consumer. There may also be significant benefits to be gained thanks to AI on the Operation & Maintenance front. According to the IEA's figures, it is going to be possible to save approximately 20 billion dollars at the global level in 2040 thanks to predictive systems and network maintenance.

CYBERSECURITY: CHALLENGES AND OPPORTUNITIES. Every momentous, historic change inevitably entails critical issues, and the AI revolution is no exception. The main problem concerns the greater likelihood of physical and virtual attacks on these increasingly smart and interconnected systems. In a recent book, journalist Ted Koppel postulates an attack on one of the three electric power transmission networks in the United States. The author concludes that you could bring the world's greatest power to its knees with a laptop as your only weapon.

At the same time, however, a virtuous use of artificial intelligence can make it increasingly easy to protect strategic assets, with particular reference to large telecommunications, electric power and gas networks. A cybersecurity strategy capable of combining AI techniques' ability to process a huge mass of data – to identify potential threats as they form and rapidly distinguish what is important from what is not – can represent added value in the defense of our strategic infrastructures.

The transformation under way also goes hand in hand with the need for increasing safeguards for our privacy and personal data protection. Thus, it is

necessary – as of right now – that we debate new initiatives and strategies for the surveillance, monitoring and disconnection of assets. We also need a new rules system. A farsighted and ethical approach can certainly make it possible to reduce the problematic areas while seizing all the opportunities offered by this new industrial revolution.

THE CASE OF SNAM. Artificial intelligence in Italy's major energy networks is a revolution that is already on our doorstep and in which Italy can and must be out in the forefront, thanks to its most strategic corporations. Snam is an example. In its industrial plan through 2022, Snam has launched a project known as Snamtec which consists of new investments worth 850 million euro and which is designed to lay the groundwork for the energy company of the future. It is a program of investments in energy transition and innovation that shows how the two issues go hand in hand.

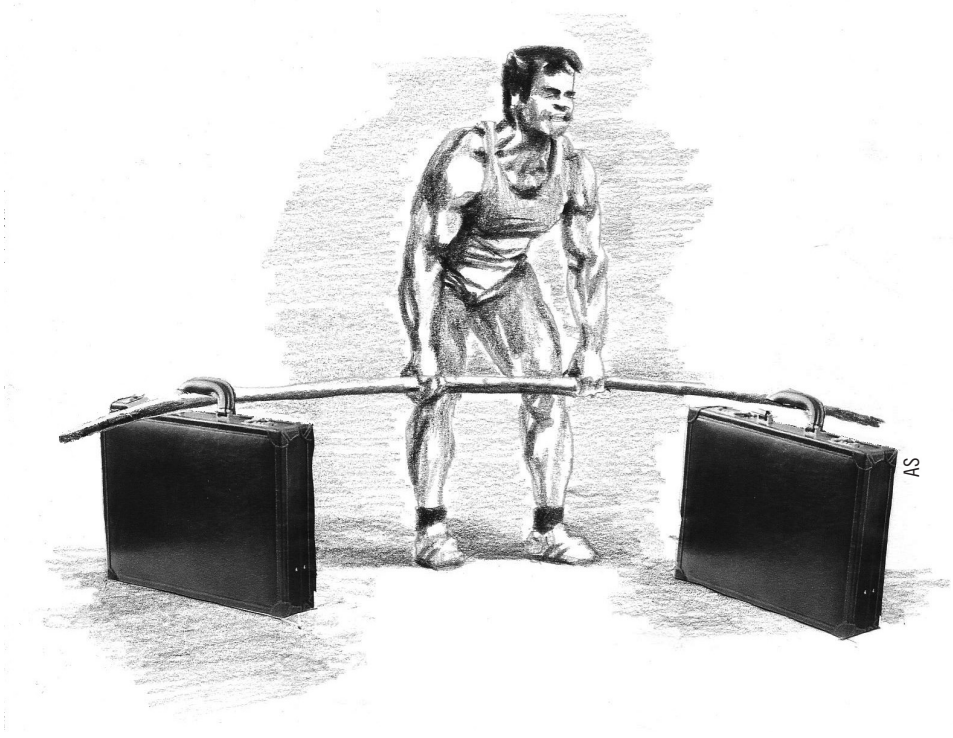
One of the first projects to have been launched was called Dafne. It is a system for predicting future demand for gas that uses sophisticated algorithms based on neutral networks. This advanced machine learning solution allows the company to predict the flows in its network with increasing accuracy, thus reducing consumption and emissions.

AI is also used for asset maintenance: with the use of cognitive computing technologies it is possible to analyze maintenance reports, to interpret them, to identify potential causes of failure or faults, and to formulate suggestions and indications useful for technicians to manage the network with increasing efficiency, guaranteeing greater reliability and security.

In addition to the above, Snam is launching a plan for designing and implementing an IoT platform for concentrating data detected by sensors in the field. This is a method that has already been tried and tested in remote diagnostic and command fields. It will allow the company to optimize network

performance and, in due course, to make the network increasingly independent in terms of control and management. The availability of machine learning technologies together with the technical staff's management skills and data scientists' analytical skills will make it possible to create analysis models that will make the network increasingly smart and automated.

The Snam case study shows the extent to which the energy internet is already a reality in Italy, and how it is radically transforming the industry. Artificial intelligence is set to become a formidable accelerator in the transition towards a more sustainable world – a transformation that we need to monitor with an eagle eye and to govern with great care, but that can offer huge benefits to society and to the environment while also offering new opportunities for development and competitiveness.



DIGITAL GEOPOLITICS - SPECIAL ISSUE IN COOPERATION WI…

TECHNOLOGY & SCIENCE EU & EUROPE

Data protection, Europe's head start

By **Niccolo Serri** On **Dec 3, 2019**

The new European regulation on the protection of data is poised to launch a new global regulatory system. It will serve to protect the rights of the individual in the information society and allow Europe to have a dominant voice in the international debate on ethics and law in the digital ecosystem. It is now up to the businesses on the continent to adapt quickly and effectively to the dictates of the new regulation.

The General Data Protection Regulation (GDPR) was approved by the European Parliament and Council in late April 2016, and it officially went into effect on May 25, 2018. In contrast with previous undertakings, the regulatory nature of the GDPR offers a legal framework that is both formal and binding for member states, thereby harmonizing at European level the fundamental principles underlying the control and protection of personal data, and creating a new category of rights within the post-Lisbon treaties system.

Today, however, data privacy reform has yet to be completed. Despite the all-inclusive nature of the GDPR, some of its 99 articles leave the possibility open for individual countries to legislate independently in such a way as to further define the regulation's instructions – in the case of some clinical or biometric categories for example. While some eu member states have already issued special laws by which to comply with the dictates of Brussels, others are still in the implementation phase. Alignment proceeds, but there is still confusion, which is creating problems for the private sector and for many companies that missed the deadline and are now furiously restructuring in order to embrace the new European rules.

THE REGULATION'S POTENTIAL. The GDPR has ushered in numerous benefits as much for consumers as for businesses operating in the digital economy. The new European regulation is based on the dual pillar of "privacy by design and default", a concept formalized in 2010 by Ann Cavoukian, then-commissioner for privacy of the Canadian province of Ontario. According to this approach, the privacy of individual data must always be considered the default position by businesses; it must also be

taken into account in the design of algorithms and digital services from the earliest stages of their development. Instead of indiscriminately amassing data, businesses are obliged to treat personal data solely in the manner necessary for their immediate ends. For European citizens, the new regulation facilitates access to and management of their data by introducing the right to individual portability (the ability to request the transfer of their data from one platform to another), and the right to cancellation (to be able to oblige companies to delete their data, thereby undermining the creation of monopolies in the digital economy).

The need to modernize European policy is being spurred, on the one hand, by rapid developments in digital technology that have made the 1995 Commission data protection directive obsolete. On the other, the globalization of communications networks and the consequent flow of personal data – with the growing danger of cyberespionage, not least by foreign security agencies – have increased public sensibility to the issue of digital privacy. Indeed, the European Commission had already proposed an initial legislative draft of the GDPR back in January 2012, and the Council of Europe itself undertook the reform of its Convention no. 108 on the automated treatment of data approved in Strasbourg in 1981.

As regards European businesses, the GDPR introduces immediate organizational costs, but promises to strengthen competitiveness, especially at international level. Indeed, the strict nature of the EU regulation has the potential to facilitate innovation through protected digital services and consumer-friendly products, thereby turning European firms into "champions" of an ethical approach to the digital ecosystem.

The GDPR applies in the strict sense of the term not only to European companies but, more in general, to all those operating on the digital market. That means Google, Amazon and Facebook, who are all being forced to review their data management practices so as not to lose certain slices of the market. This could facilitate a sort of European technological "soft power" that could counterbalance the lack of investment in digital by strengthening the international ethical/legal framework. Thus, European firms better positioned to adapt the pillars of the gdpr could draw advantages from it.

Add to that the informal protection that could be ensured by the new system of sanctions introduced by the EU regulation. Article 83 of the new code, for example, provides that a company that violates user or employee data can be fined up to 20 million euro or 4% of annual global turnover, whichever is the higher amount. This provision offers a powerful disincentive for the worst transgressions – especially for the giants of Silicon Valley and the Far East – and could benefit those European enterprises that are first to comply with the directive. In the first year of the GDPR's

application, sanction levying was little more than nominal: In 2018, for instance, the data protection authority of the German *Länder* Baden-Württenberg imposed a sanction on an online chat for violating Article 32 on the security of data treatment. Prior to that, Portugal's Comissão Nacional de Proteção de Dados fined the Barriero Hospital of Lisbon 400,000 euro for having allowed unauthorized access to patient data. The watershed came in January 2019, when the French Commission Nationale de l'Informatique et des Libertés (CNIL), decided in favor of the La Quadrature du Net association's claim, slapping a 50 million euro fine on Google for lack of transparency in its informed consent to the personalization of online ads.

CHALLENGES TO ENTERPRISE. Despite the competitive opportunities created by the GDPR and the onerous price of transgressing, European enterprises have been slow off the mark. According to a McKinsey survey at the beginning of 2018, almost no senior European manager considered his/her firm ready for the regulation's entry into effect, and expected its application would be postponed beyond the May 2018 deadline. The majority of firms then sought to address the problem by adopting temporary solutions, resorting to the manual control of their databases, starting with the hiring of adjunct personnel. Indeed, the GDPR makes it obligatory for all government ministries and major firms that handle sensitive data to hire a data protection officer to oversee compliance.

Companies operating in digital business-to-business sectors have had to comply with the provisions of GDPR Article 28 on data treatment responsibilities, which imposes stricter measures on the transfer of data along production chains. Companies are obliged to ensure that none of their supplier chain is processing personal data while providing their services, even when that is not immediately visible. Business-to-consumer companies, on the other hand, have another hurdle to face: that of obtaining users' informed consent to the treatment of personal data. Databases compiled outside the transparency and regulatory criteria of the GDPR risk becoming useless as a commercial asset. In both cases, the arsenal of it instruments available to businesses need to be modernized so they can automatically oversee their data gathering mechanisms, maintain their tangible traceability and meet multiple user requests.

The situation is made more difficult by the fact that member states have a degree of discretion in implementing the GDPR, and can decide to tighten some of the provisions at national level. Indeed, more than 30% of the regulation's articles contain clauses that allow national legislatures to choose from various options (concerning the minimum age for consent of personal data treatment, for example) and to more specifically define the rules for data protection in government

administrations, labor relations and social policy. The risks associated with legislative non-homogeneity are only in part offset by the creation of The European Data Protection Committee (edpc), a new independent institution made up of representatives from the various national authorities, and of a European Data Protection Supervisor. The role of the new entity is precisely to stabilize compliance with GDPR norms through the publication of guidelines and codes of conduct. The edpc differs from a steering committee in that it can issue binding decisions on specific cases when those cases involve more than one European country.

THE INTERNATIONAL PANORAMA. Germany is an interesting case: it has a long tradition of personal data protection, and was the first to pass a special law for implementation of the GDPR. The law on the protection of data for the Hesse Lander, approved in 1970, is the first example of data protection legislation in the world. In addition to the federal commissioner for data protection – which is located in Bonn and acts in a supervisory capacity – every *Länder* has its own data protection authority, and this necessitates continuous interface.

Implementation of the GDPR in Germany has two main features: first, the German legislature departs from the neutrality of European law – which avoids citing specific technologies and devices – to make explicit reference to the problems associated with video surveillance; secondly, it limits some individual rights linked with control and transparency.

In the case of France, the new GDPR regulations had to accommodate the country's cultural specificity. The first French legislation on data privacy dates back to 1978, and that remained substantially unchanged until the first European directive was issued. Thus, the GDPR has triggered an institutional transformation with stronger supervisory powers than those of the CNIL.

The broadest features of France's application of the European regulation concern the workings of an administrative machine traditionally infused with a strong government centrism. French legislation provides that a national government performing its public functions need not request the prior consent of its citizens on the treatment of data except when those regard health or genetics.

In Italy, the protection of personal data is not explicitly acknowledged in the Constitution, and for a long time these issues were ignored by national legislation. Only when a code for the protection of personal data was approved in 2003 – on the heels of the 1995 European Directive – did Italy become aligned with the other member states. With the arrival of the GDPR, the Italian government decided to update but not replace the earlier code, in favor of a change in perspective from a

model based on the sole anticipatory authorization of the treatment of personal data by the authority to a risk-based approach that incorporates the European regulation's concept of responsibility.

Italy's adaptation of the GDPR consents, for example, to its onerous administrative sanctions, but it also maintains criminal sanctions of up to three years in prison for the illegal treatment of personal data. Moreover, Italian legislation is very detailed with regard to the treatment of healthcare data, obliging all public providers to employ a data protection officer and to keep a detailed register of how patients' data are utilized. Italy has – at least so far – also been the only European case in which the personal data of the deceased are regulated.

Finally, another special case deserving of mention is Japan. With a view to ensuring its businesses' continuity of access to the European market, the Land of the Rising Sun has decided to align itself with the obligations of the gdpr: its binding regulations guarantee European citizens access to their data. Furthermore, the country has established a claims management system and offers assurances that its government will not utilize the data for any purpose except those strictly to do with national security, also stringently regulating any data's eventual transfer to third countries. Brussels and Tokyo reached an accord in late 2018 within the framework of the European Union/Japan free trade partnership on recognition of the reciprocal equivalence of their data protection systems.

Based on the values of a new technological humanism, the European regulation is poised to become the basis for a new global regulatory system. Thanks to the GDPR, Europe stands to have a dominant voice in the international debate on ethics and law in the digital ecosystem, thereby helping to steer its development in a direction that coincides with its political and economic interests. In order to fully exploit this potential, however, businesses on the continent are going to have to adapt quickly and effectively to the dictates of the new regulation. Another trick will be to ensure homogeneity in the regulation's application in the various member states and to keep the GDPR's common rules from becoming mired in the morass of each country's national legislation.

Europe technology EU digital

Niccolo Serri

Niccolò Serri is a PhD student in economic and social history at the University of Cambridge, Magdalene College, working on the comparative dimension of Southern Mediterranean welfare states. He previously collaborated with the Italian Ministry of Foreign Affairs and the Lelio and Lesli Basso Foundation.

Roberto Cingolani

Roboethics

The relationship between people, robots and artificial intelligence is changing all the time, raising pressing legal, ethical and philosophical questions. Whereas the United States seems to regard the phenomenon with a business-oriented approach, Europe favors a regulatory strategy. However, the best starting point seems to be the concept of "roboethics", promoted by the scientific community some twenty years ago with the aim of examining the social consequences of the use of autonomous and intelligent systems.

The day when robots can be as intelligent as human beings still seems remote (and may perhaps never come, at least as long as we continue to use silicon), but the ethical, social and human issues raised by their large and widespread presence in society deserve attention already. A thorough examination of these arguments is under way, combining purely technical aspects with the legal, ethical and philosophical aspects necessary to formulate the guidelines for future coexistence between human beings

Roberto Cingolani is Chief Scientific Officer of the Italian Institute of Technology in Genoa.

and autonomous/intelligent systems (A/IS). These considerations are a matter for all those involved in the design, development and use of these new and revolutionary technological products. To create A/IS capable of acting in the interests of mankind and of the community is an objective shared by experts from many different disciplines: electronic and mechanical engineers, computer scientists, psychologists, neurologists, cognitive scientists, artificial intelligence specialists, logicians, mathematicians, philosophers, jurists, economists, designers and artists.

HOW TO EDUCATE MACHINES. We must remember the distinction between "stupid" and "intelligent" machines. The former are human artifacts which, though often extremely sophisticated, do not raise any particular or new ethical problems (the criteria and standards already used for technological products apply). The situation with "smart" machines is different. Once a robot develops the capacity to decide and act autonomously, to learn and to acquire experience with algorithmic decision-making processes (albeit without emotion or spirituality), entirely new and important ethical and regulatory issues arise.

A cognitive machine capable of learning raises the issue of how to teach it: what educational strategies should be used? How can a machine be rewarded for good behavior (or the "right" answer)? The key question becomes: "How to punish a robot when it makes a mistake?"[1]

People break rules out of necessity, by mistake, for revenge or out of spite. In most cases the motives behind such violations are due to psychological and existential changes or conditions of particular necessity or hardship. Re-education involves punishment, which usually entails limiting freedom – some kind of privation or the payment of a fine. More generally, all educational processes are based on a balance between punishment and reward.

Punishment is based on the fact that all human beings, and even the more intelligent animals, fear being deprived of something that they value: whether freedom in the case of a prison term, or a toy in the punishment of a mischievous child. Fear of losing something of value is part of human psychology but also a consequence of the principle of self-preservation that influences all living beings. Fear of punishment normally causes us to behave better so as not to suffer a deterioration in our quality of life.

In the case of a machine, the violation of a rule could simply result from the assessment that this transgression is necessary in order to reduce a number of negative collateral effects of a particular action. The violation would simply be the result of an algorithm which, by minimizing collateral risks and damage, seeks to achieve a particular aim under certain conditions. The most classic instance involves an autonomous car with faulty brakes: it must choose whether to sacrifice its passenger by crashing into a wall or to sacrifice pedestrians by continuing in the same direction. On the basis of the same violation, the car can only choose the solution involving the probability of less harm, whatever that may be. Different cars in the same situation and with the same ambient conditions would all reach the same conclusion. Different people, however, in the same situation and conditions, would not all do the same. Their decisions would be affected by imponderable subjective factors that would inevitably lead to different individual decisions (for instance, if one of the pedestrians were a relative, the final decision could be different, irrespective of the absolute risk calculation).

The diversity of human behavior stems from the non-algorithmic nature of our intelligence, from the ever-present element of irrationality, emotion and the intrinsic imponderability of our logical mechanisms. Human irrationality or non-rationality, the result of the hormonal component of our species,

gives rise to creativity, imagination and feelings, which in turn lead to variability and a lack of predictability in our behavior.

It would be very difficult to punish a machine that breaks a rule. It could not be deprived of food or liberty, inasmuch as neither is of crucial importance to its species. Nor could it be deprived of its life, because by disconnecting

CO

its batteries we would be doing nothing different from what we do when we shut down a computer. The machine may be able to understand and to decide, but that is not enough to have an awareness of itself and the consequent instinct of protection, survival and preservation of the species. Whatever code may be developed to regulate coexistence between human beings and intelligent machines, it will have to take account of the fact that machines obey laws different from those of biology.

UNRESOLVED QUESTIONS AND CURRENT PROPOSALS. Of course, all this will depend on how quickly the identity and personality of autonomous intelligent machines evolve. In the remote event of their truly

becoming a separate species, they will require a specific legal and ethical framework to set them within society and establish their rights and duties. This would not necessarily involve a subordinate role with respect to mankind – like the animal under the responsibility of its master or the artifact under the responsibility of the builder – but something new and profoundly different from what we have formulated hitherto.

A/IS can be remote-controlled by human beings: such machines exist in several areas of work and human activity and are an important aid to the security, efficiency, and productivity of certain processes. They inevitably require the involvement of human beings to steer and control them; it is the humans who make the decisions.

Other kinds of more highly evolved A/IS can be programmed to carry out certain tasks entirely autonomously. They are equipped with AI, are capable of "thinking" for themselves, and have no need for human input. Scientists and scholars all over the world have suddenly realized that machines of this kind raise security, ethical and legal problems and have promptly embarked on intensive cultural and anthropological deliberations, which are still very much in progress.

There is a growing debate on these matters in Europe and in other technologically advanced countries. Every new robotic product raises problems prompting ethical and political deliberations, for the protection of the common good and of the community. The sustainability of progress in A/IS, the impact on individuals and on the various sectors of society and the dangers and damage that they may entail are issues that require the development of new dedicated cultural and regulatory instruments. Indeed, this is starting to happen at the political and institutional level.

In 2016, two important documents on robotics were published: in October, the White House's Office of Science and Technology Policy published *Arti-*

ficial intelligence, automation, and the economy, and in May the European Parliament's Legal Affairs Committee published its *Recommendations to the Commission on Civil Law Rules on Robotics*. The White House document focuses on artificial intelligence: the core is not robotics but AI; the focus is particularly on how to organize a "Good AI Society", in which artificial intelligence plays a predominant role. Probably influenced by Silicon Valley representatives, it is a very optimistic document: AI will help to improve everything and the dangers are confined to cyberwarfare and autonomous weapons; ethical considerations are limited to efforts to ensure the transparency of everything relating to machinery and research into it.

The document published by the European Parliament's Legal Affairs Committee, however, focuses mainly on robotics – on the "Good Robotic Society". To achieve a Good Robotic Society we need to assess how many job positions will be lost when large numbers of robots are introduced into society. Both soft and hard legislation will also need to be introduced to regulate potential offenses in this field and their gravity; to this end it will be necessary to establish a law committee and legal framework on robotics and artificial intelligence.

These are two antithetical approaches, which reflect the Americans' business-oriented approach and the Europeans' regulation-oriented approach and which separate AI and robotics.

Last, we must remember that, also in 2016, the study group of the UK's Convention of the Society for the Study of Artificial Intelligence and Simulation of Behaviour drew up five rules for the management of intelligent machines. The committee confirmed – at least partly – the principle that artificial intelligence and robotics go hand-in-hand.

Rule one: Robots are multi-use tools. Robots should not be designed solely or even primarily to kill or to harm human beings, except in the interests of national security.

Rule two: Humans, not robots, are responsible agents. Robots should be designed and operated as far as is practicable to comply with existing laws and fundamental rights and freedoms, including privacy.

Rule three: Robots are products. They should be designed using processes which assure their safety and security.

Rule four: Robots are manufactured artifacts. They should not be designed in a deceptive way to exploit vulnerable users; instead their machine nature should be transparent.

Rule five: The person with legal responsibility for a robot should be attributed.

This is a simple and pragmatic approach, more effective than the lengthy studies presented by the United States and Europe, and one which provides definitions and defines criteria. However, the building of a regulatory system remains a remote prospect.

PROCEEDING FROM "ROBOETHICS". The aforementioned documents (published in 2016) stem from international deliberations involving the entire scientific community, which had begun some five years previously. In 2017, the IEEE (Institute of Electrical and Electronics Engineers) engaged in a major interdisciplinary debate focused on common technical, legal and ethical factors, which produced an interesting program document: *Ethically aligned design, version 1*. Further joint research is currently under way with a view to a "Version 2" by the end of 2019. Furthermore, eleven IEEE P7000™ Standards Working Groups have been established to steer and guide research work in the coming years.

It is important to remember that all this has emerged within the space of a few years – the concept of roboethics was only postulated in around the year 2000. At that time, and for the first time, roboethics proposed objectives and committed deliberations by scientists, philosophers, jurists, sociologists

and anthropologists to lay the ethical foundations for the design, development and use of robots.

A visionary definition was recently proposed by Spyros G. Tzafestas, who defined roboethics as "a branch of applied ethics, that is, philosophical and therefore systematic and informed deliberations, examining the positive and negative consequences of robots in society with the aim of promoting the ethical design, development and use of robots, and particularly of smart and autonomous robots."[2]

The term "roboethics" has now become partly obsolete, replaced by the generic term "ethics of A/IS"; however, the questions raised by roboethics from the outset remain topical: can a robot do good or evil? Can a robot be dangerous to the human race? The ethical values defined in Gianmarco Veruggio's *Roboethics Roadmap* of 2006 are also still topical:

- to observe the values of human dignity and human rights;
- to promote criteria of equity, justice and equality in access to new technologies;
- to correctly assess harm and benefits;
- to protect cultural diversity and legitimate pluralism;
- not to discriminate or stigmatize;
- to encourage solidarity and cooperation;
- to respect privacy and the need for informed consent;
- to accept responsibility for the biosphere.

Last, in the specific case of A/IS, it is also necessary to develop an inclusive and participative strategy vis-à-vis citizens in order to prevent, on the one hand, utopian hopes and, on the other, irrational fears. Emotive or ideological attitudes can divert attention away from the real problems and ultimately prompt unrealistic enthusiasm or wholesale indiscriminate rejection. The latter can be very harmful if it pointlessly obstructs the development of

technology that really could be an important tool for economic development and social progress, inasmuch as it helps human beings without harming them or replaces them in a positive way.

[1] Wendell Wallach and Colin Allen, *Moral machines. Teaching robots right from wrong*, Oxford University Press 2010.
[2] Spyros G. Tzafestas, *Roboethics. A navigating overview*, Springer 2016.