MAGAZINE DI TECNOLOGIA, INNOVAZIONE, RICERCA E IMPRESA

eXL

Technology, Innovation, Research and Business Magazine

PRIVACY
Difendersi dall'IA

Privacy
Defence against AI

ARCHEOLOGIA
La mappa del sottosuolo

Archeology
Underground map

be smart, be safe.

Salute e sicurezza sono le nuove urgenze sociali mentre infervora il dibattito sull'apporto dell'Intelligenza Artificiale tra luci e ombre

Health and safety are new social urgencies while debate on Artificial Intelligence contribution heats up

Dicembre 2023 | Anno IV | n. 3 | Rivista quadrimestrale | Registr. Tribunale di Pisa n. 6/2020 del 4.11.20 | Direttore Responsabile: Eleonora Mancini
SF: € 6, Abb: € 10 | Poste Italiane S.p.A. - Spedizione in abbonamento postale - Aut. n. 2453/2020 del 01.11.2020 - Periodico R.O.C.

UNA INIZIATIVA DI CAMERA DI COMMERCIO TOSCANA NORD-OVEST E UNIONE INDUSTRIALE PISANA

Editore: Pacini Editore Srl, via Gherardesca 1, 56121 Pisa | Direttore Responsabile: Eleonora Mancini
Indirizzo della redazione: via Gherardesca 1, 56121 Pisa | Registrato Tribunale di Pisa n. 6/2020 del 4.11.20
Tipografia: Industrie Grafiche Pacini, via Gherardesca 1, 56121 Pisa

Patrizia Alma Pacini
direttore editoriale eXL

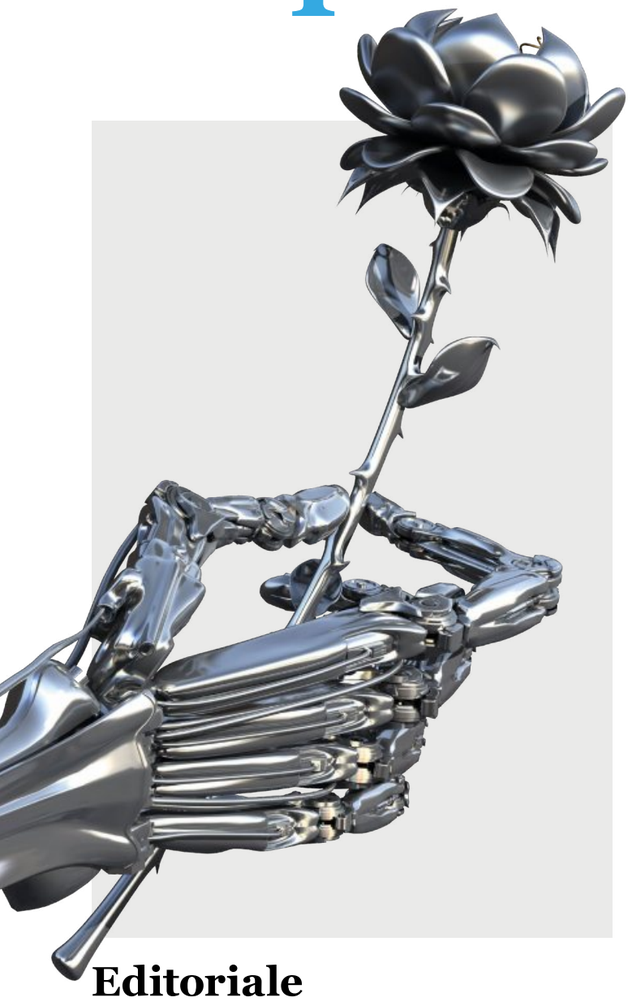
La legge suprema

The supreme law

Cosa significa ***Be Smart, Be Safe***? In questo nuovo numero di eXL abbiamo voluto aprire una finestra sulla interessante connessione tra sicurezza e nuove tecnologie, in particolare quelle digitali, che pervadono ogni campo anche in ragione del preponderante ingresso dell'Intelligenza Artificiale fino nella nostra quotidianità.
La pandemia ha come squarciato un velo, ci ha fatto conoscere la fragilità, ci ha fatti scoprire fragili proprio sotto il profilo della sicurezza, non solo quella sanitaria, rivelando in questo modo anche una certa presunzione del mondo moderno rispetto al progresso e ispirandoci dubbi e domande con un oneroso invito all'umiltà. In questo senso, nelle pagine di eXL, riflettiamo ad esempio sulla sicurezza dei dati personali, sul loro uso e i riflessi sui diritti fondamentali delle persone, affrontando in parallelo il tema della cybersecurity tra opportunità e rischi per le aziende.
Essere al sicuro significa sentirsi protetti ed essere reattivi, indipendentemente dall'ambiente o dalla situazione, con la capacità di usare strumenti e trovare soluzioni sempre, però, con la consapevolezza di limiti e confini sani.
La salute è la condizione imprescindibile per poter essere reattivi e, in questo senso, tecnologie digitali e Intelligenza Artificiale rivelano il loro potenziale positivo.
Salus populi suprema lex esto, *la salute del popolo sia la suprema delle leggi*, diceva Marco Tullio Cicerone. Salute e salvezza sono un tutt'uno con la sicurezza dei cittadini, come ci dimostrano del resto gli importanti progetti sviluppati dai nostri eccellenti centri di ricerca le cui innovazioni mirano sempre di più a monitoraggi, cure e terapie personalizzate per fronteggiare disturbi o malattie croniche e perfino rare.

What does ***Be Smart, Be safe*** mean?
In this new issue of eXL, we aim to shed light on the interesting connection between security and new technologies, in particular digital ones.
The pandemic lifted a veil, allowing us to glimpse the fragility of things and of ourselves, not only on the level of health but also from the point of view of security. Above all it showed us the presumption of the modern world with regard to progress, giving rise to doubts and questions and the painful realisation that we need to act with humility. It is in this sense that we wish to devote these pages of eXL to a reflection on matters of the safety of personal data, their uses and their repercussions on basic human rights, exploring these themes together with the parallel topics of cybersecurity and opportunities and risk s for businesses. Creating conditions of safety means feeling protected and being ready to react. Health is a prerequisite for reacting: it is in this sense that digital technologies and artificial intelligence reveal their positive potential.
Salus populi suprema lex esto – let the welfare of the people be the supreme law, said Cicero. Health and safety are one and the same, as we see, for example, in the important projects developed by our excellent research centres, whose innovations increasingly focus on monitoring, care and personalised therapies to meet the challenges of chronic and sometimes rare pathologies and diseases.

In questo numero



Editoriale

primo piano

DIGITALE

AZIENDE

RICERCA

SOCIALE

Edizione digitale, aggiornamenti e notizie su:

www.exlmagazine.it

Segui le news di eXL su facebook

Le firme eXL

Denise Amram

Francesca Anichini

Marco Laurino

Giuseppe Prencipe

Hanno collaborato a questo numero Federico Aromolo, Valentina Baldacci, Nicola Bellani, Niccolò Borgioli, Sara Profeti, Alina Sîrbu, Arianna Torelli

Direttore Editoriale
Patrizia Alma Pacini

Direttore Responsabile
Eleonora Mancini

Segreteria di Redazione
Laura Magli

Redazione
Luca Biagiotti, Francesco Ceccarelli, Margherita Cianchi, Luca Fracassi, Chiara Lazzaroni, Silvia Maculan, Nicola Maggi, Andrea Pantani, Alberto Susini, Carlo Venturini

Comitato Scientifico
Giuseppe Anastasi, Tiberio Daddi, Luigi Doveri, Manrico Ferrucci, Leonida Gizzi, Andrea Madonna, Stefano Marmi, Patrizia Alma Pacini, Andrea Piccaluga, Corrado Priami, Valter Tamburini, Patrizia Paoletti Tangheroni, Riccardo Toncelli

Progetto grafico e impaginazione
Margherita Cianchi

Realizzazione editoriale e stampa
Pacini Editore Srl, Pisa

MISTO
Carta da fonti gestite in maniera responsabile
FSC® C111769

Questa rivista utilizza vernice e plastificazione antibatteriche

Una iniziativa di Camera di Commercio Toscana Nord-Ovest e Unione Industriale Pisana

CAMERA DI COMMERCIO TOSCANA NORD-OVEST
UNIONE INDUSTRIALE PISANA

Con il contributo di

CRV CASSA DI RISPARMIO DI VOLTERRA

In collaborazione con

UNIVERSITÀ DI PISA
Sant'Anna
SCUOLA NORMALE SUPERIORE
Comune di Pisa
Consiglio Nazionale delle Ricerche

Partner

ACQUE
vitesco TECHNOLOGIES
TEATRO DI PISA
Confservizi Cispel Toscana

La medicina del futuro

Le nuove tecnologie e l'Intelligenza Artificiale stanno rivoluzionando la ricerca in campo medico

The medicine of future
New technologies and Artificial Intelligence are revolutionizing the medical field research

IL LABORATORIO IN UN CHIP

Analisi biomediche veloci e innovative con il progetto INTA di NEST e Scuola Normale

Laboratory on a chip

DI ANDREA PANTANI

Un laboratorio per analisi biomediche, in un chip. È nato a Pisa, presso il Laboratorio NEST della Scuola Normale Superiore. Il progetto è il primo spin-off del Consiglio Nazionale delle Ricerche Istituto Nanoscienze di Pisa (Crn-Nano) e della Scuola Normale Superiore di Pisa e si chiama **INTA Systems**.

Nato nel 2020, INTA sviluppa e produce **laboratori-on-chip ultrasensibili e portatili** per analisi rapide di fluidi. Le principali applicazioni sono biomedicali, di sicurezza, industria 4.0 e *food-analysis*. I dispositivi *lab-on-a-chip* brevettati di INTA sono in grado di rilevare in pochi minuti e in maniera semplice e decentralizzata una grande varietà di analisi (proteine, anticorpi, acidi nucleici, virus, batteri).

INTA integra conoscenze avanzate di fisica della materia, processi di fabbricazione di nanostrutture, tecniche innovative di coniugazione di biomolecole e analisi dati tramite algoritmi di intelligenza artificiale.

L'azienda, in cui adesso collaborano una ventina di persone, ha chiuso un secondo round di investimento di 2 milioni di euro a luglio scorso, partecipato da Eureka! Venture SGR, A11 Venture, Liftt e Deep Ocean Capital SGR, dopo il primo, da 350mila euro, di aprile 2021. Il chip che produce si trova in una cartuccia usa e getta del costo di appena 30/40 euro che può essere analizzata da un lettore ovunque.

#Matteo Agostini

«Il dispositivo è nato per rilevare biomarcatori neurologici, molecole presenti nel sangue di individui che hanno subito danni cerebrali», spiega **Matteo Agostini co-fondatore e ceo di INTA**. «Adesso è capace anche di misurare i livelli di batteri nelle acque di una rete idrica. Per le nostre analisi sfruttiamo la vibrazione delle onde acustiche che cambia di frequenza nel momento in cui gli anticorpi che attacchiamo sulla superficie dei sensori si "scontrano" con le molecole che intendiamo misurare».

Riguardo alla diagnostica, il dispositivo è in grado di **rilevare patologie come i traumi**

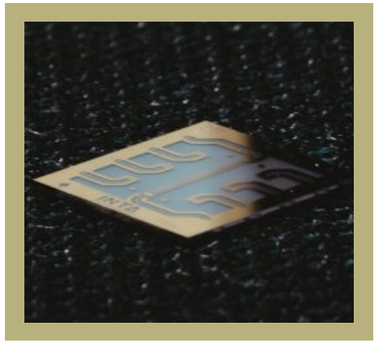
DA UNA SINGOLA GOCCIA DI SANGUE

rilevamento di biomarcatori: proteine e anticorpi, virus, batteri

diagnosi veloci e precise

riduzione di costi e tempo

cerebrali severi o lievi (TBI) **e il glioblastoma multiforme** (GBM), un tipo di tumore al cervello molto aggressivo. «Con il *lab-on-a-chip* è possibile rilevare TBI lievi o severi nei pazienti prima che siano sottoposti a tecniche diagnostiche lente e costose quali la tomografia assiale computerizzata (TAC) o la risonanza magnetica, oppure monitorare il GBM eseguendo **analisi del sangue molto veloci**.



Il dispositivo *lab-on-a-chip* brevettato da INTA

Questo permette di abbattere i costi diretti (analisi mediche) e indiretti (derivanti da mancata diagnosi) legati ai pazienti con traumi cerebrali e apre innovativi scenari nel monitoraggio delle recidive del glioblastoma».
Il principio di funzionamento su cui si basa il *lab-on-a-chip* è la **nano-acustica**, ovvero acustica realizzata in dispositivi nano-tecnologici, attraverso la generazione di onde acustiche controllate, una sorta di piccoli terremoti che si propagano all'interno del chip e che hanno effetti sulla sua superficie. Tramite nano-sensori acustici e micro-trasduttori acustici realizzati al NEST, è possibile interagire con molecole e fluidi ed eseguire le analisi sugli stessi.

Il progetto è stato realizzato all'interno del Laboratorio NEST (*National Enterprise for nanoScience and nanoTechnology*) durante il progetto di dottorato alla Scuola Normale Superiore che Matteo Agostini ha portato a termine sotto la supervisione e la guida scientifica di **Marco Cecchini** dell'**Istituto Nanoscienze del Cnr**, altro co-fondatore di INTA insieme a **Marco Calderisi** già **imprenditore nel ramo *data-science***.

The lab-on-a-chip devices patented by INTA Systems are able to perform a variety of analyses in a simple, decentralised manner: in just several minutes, they are able to reveal the presence of proteins, antibodies, nucleic acids, viruses and bacteria. The company was founded in 2020 as a spin-off of the Nanoscience Institute of Italy's National Research Council (CNR) in Pisa and the Scuola Normale Superiore of Pisa; today it is composed of approximately twenty collaborators. In July of this year it concluded a second investment round, amounting to € 2 million, in which Eureka! Venture SGR, A11 Venture, Liftt, and Deep Ocean Capital SGR took part. This follows its initial investment round of € 350,000 in April 2021. The chip produced by INTA Systems is contained in a single-use cartridge and costs only € 30-40; it can be analysed by a reader anywhere. "The device was created to detect neurological biomarkers, molecules present in the blood of subjects who have experienced cerebral damage", explained **Matteo Agostini**, *co-founder and CEO of INTA*. "Now it can also measure bacterial levels in a water system. For our analyses we take advantage of the vibration of acoustic waves, which change frequency when the antibodies that we attach to the surfaces of the sensors 'clash' with the molecules that we wish to measure".
With regard to diagnostics, the device is able to detect such pathologies as severe or mild cerebral traumas (TBI) and glioblastoma multiforme (GBM), a type of very aggressive brain cancer. "Our 'lab-on-a-chips' are able to detect mild or severe TBI in patients before resorting to slow and costly diagnostic techniques, such as computed tomography (CT) scans or magnetic resonance imaging; they can further monitor GBM in patients by means of a rapid, low-cost blood test. The chips allow operators to reduce expenses, whether direct (for medical analyses) or indirect (resulting from a lack of diagnosis), connected to patients with cerebral traumas. They thus open innovative monitoring possibilities in recurring GBM".

INTELLIGENZA “SENSORIALE”

Trattamenti precoci e personalizzati per pazienti con BPCO grazie ai Big Data raccolti da TOLIFE

TOLIFE, “sensory” intelligence

DI MARCO LAURINO*

Utilizzare **sensori indossabili** è oggi del tutto normale e lo facciamo senza rendercene conto. *Smartwatch* e *smartphone* sono i nostri amici inseparabili, che migliorano e velocizzano alcune delle nostre attività quotidiane. Ma come possono queste tecnologie costituire un valido aiuto per la salute?

Una risposta può darla **TOLIFE**, il progetto **HORIZON Europe** che ha l’obiettivo di sviluppare e validare clinicamente una piattaforma basata su **intelligenza artificiale e sensoristica non invasiva**, **per migliorare la gestione e la personalizzazione del trattamento di patologie croniche** ad elevata complessità.
In particolare, la piattaforma sviluppata nell’ambito del progetto, – avviato a settembre 2022 con una durata di 54 mesi – sarà ottimizzata e validata in condizioni di “vita reale” su pazienti affetti da broncopneumopatia cronica ostruttiva (**BPCO**), una malattia dell’apparato respiratorio che interessa bronchi e polmoni e provoca difficoltà a respirare. Si tratta di una condizione cronica con danni spesso irreversibili che possono essere solo monitorati.
In patologie complesse come la BPCO, anche i dati prelevati durante le attività quotidiane sono importanti. Possono essere utili per la previsione e il controllo delle riacutizzazioni, per valutare continuativamente lo stato di salute e migliorare la qualità della vita del paziente, ottimizzare i protocolli terapeutici e mitigare i costi sanitari.
Il progetto si propone di **raccogliere *Big Data* relativi alle attività quotidiane dei pazienti con BPCO**, come i dati sull’attività motoria e sulla condizione psicofisiologica, ma anche dati meteorologici e ambientali. I dati saranno raccolti da **strumenti *smart* indossabili** (*smartphone*, *smartwatch* e *smartshoes*) **o posti negli ambienti domestici** (coprimaterasso sensorizzato, unità di raccolta dati ambientale domestica e spirometro portatile). I dispositivi saranno prodotti commerciali o prototipi sperimentali sviluppati appositamente per essere “trasparenti” e non invasivi per il paziente.
I dati provenienti dai dispositivi saranno poi integrati attraverso una piattaforma *cloud* di raccolta e analisi dei dati. Gli algoritmi sviluppati hanno l’obiettivo di prevedere precocemente gli eventi di riacutizzazione della malattia e, parallelamente, di moni-

eXL | primo piano

torare lo stato di salute generale del paziente in modo continuativo e senza la necessità di particolari attività o azioni. Queste informazioni integrate potranno essere utilizzate dai medici con l'obiettivo di mettere in atto un trattamento precoce e personalizzato.
Sarà inoltre sviluppata un'interfaccia *software* per informare il paziente sul proprio stato di salute, sul piano di trattamento specifico e per fornire informazioni utili per un corretto stile di vita.
Il progetto, finanziato sui fondi del Programma quadro dell'Unione Europea per la ricerca e l'innovazione Horizon Europe nell'ambito della *call Tackling diseases*, è coordinato dal professore **Alessandro Tognetti** dell'**Università di Pisa** e vede coinvolto l'**Istituto di Fisiologia Clinica del Cnr** con l'ingegnere **Marco Laurino** come *Technical Manager*.
Il progetto *www.tolife-project.eu* è portato avanti da un **consorzio internazionale multidisciplinare**. Oltre all'Università di Pisa e Cnr-Ifc, il partenariato è composto da: Istituto Superiore di Sanità (Italia), *Adatec SRL* (Italia), *beWarrant* (Belgio), *Universidad Politecnica de Madrid* (Spagna), *Avvale España* (Spagna), *Fundacion Privada Instituto de Salud Global Barcelona* (Spagna), *Consorcio Mar Parc de Salut de Barcelona* (Spagna), *Time.Lex* (Belgio), *European Federation of Asthma&Allergy Associations* (Belgio) e *Pneumologisches Forschungsinstitut an der LungenClinic Grosshansdorf GmbH* (Germania).

** Cnr-Ifc, TOLIFE Technical Manager*

TOLIFE

Combining Artificial Intelligence and smart sensing TOward better management and improved quality of LIFE in chronic obstructive pulmonary disease

Today, wearable sensors are completely normal, to the point that we use them without being aware of it. Smartwatches and smartphones have become our inseparable friends, facilitating and speeding up some of our daily activities. Yet how can these technologies be employed to benefit our health? An answer might be provided by TOLIFE - *Combining Artificial Intelligence and smart sensing TOward better management and improved quality of LIFE in chronic obstructive pulmonary disease*: this is the **HORIZON Europe project** which aims to develop and clinically substantiate a platform based on artificial intelligence and non-invasive sensor technology, to the end of improving the management and personalisation of treatment of highly complex, chronic pathologies. In particular, the platform developed in the framework of the project – which was launched in September 2022 with a duration of 54 months – will be optimised and validated in "real life" conditions on patients suffering from chronic obstructive pulmonary disease. COPD is a pathology of the respiratory system that affects the bronchi and lungs and causes breathing difficulties. It is a chronic condition which often produces irreversible damage, which can only be monitored.

DIGITAL HEALTH un ecosistema

Telemedicina, app, robotica indossabile, i progetti di Unipi per migliorare la qualità della vita

Health ecosystem

DI GIUSEPPE PRENCIPE* E ALINA SÎRBU**

La ***Digital Health*** rappresenta l'intersezione tra la tecnologia digitale e l'assistenza sanitaria. Si tratta di un campo in rapida evoluzione che sfrutta le innovazioni tecnologiche per migliorare e personalizzare la cura del paziente, ottimizzare la ricerca clinica e potenziare l'efficienza dei sistemi sanitari. Attraverso strumenti come **telemedicina**, **app per la salute**, ***wearables*** e **Intelligenza Artificiale** (IA) applicata su vari tipi di dati, essa mira a trasformare il tradizionale paradigma dell'**assistenza**, rendendo questa più **accessibile**, **tempestiva** e **centrata** sul paziente. Questo cambiamento porta non solo a diagnosi e trattamenti più precisi, ma anche a una maggiore partecipazione del paziente nella gestione della propria salute.
Lo sviluppo della *Digital Health* ha come prerequisito la collaborazione tra gli specialisti della salute e quelli informatici. Negli ultimi anni a Pisa si è sviluppato un ecosistema di collaborazioni tra vari istituti, che includono l'Università di Pisa, il Sant'Anna, gli ospedali Santa Chiara e Cisanello e vari istituti del Cnr. Le attività dei gruppi di ricerca locali si espandono a livello nazionale e internazionale in vari progetti e finanziamenti.

Di seguito alcuni dei progetti attivi nel settore della *Digital Health* in cui l'Università di Pisa è attiva.

Il progetto PNRR ***Tuscany Health Ecosystem*** **- THE** (*www.tuscanyhealthecosystem.it*) mira a stimolare, sostenere e consolidare la crescita dell'ecosistema delle scienze della vita della Toscana. Ad esempio, una delle attività consiste nell'integrazione tra dispositivi e calcolo su misura per costruire strumenti basati su IA affidabili per diagnosi personalizzate, riabilitazione e trattamento domiciliare, democratizzando così l'accesso a modelli di assistenza sanitaria incentrati sulla persona.

Il progetto PNRR ***Fit for Medical Robotics*** (www.fit4medrob.it) affronta il tema della riabilitazione e assistenza personale di soggetti con funzioni motorie, sensoriali o cognitive ridotte o assenti a causa di lesioni o motivi congeniti mediante trattamento robotico, che rappresenta una straordinaria opportunità (fino a ora non sfruttata) per offrire un'assistenza sanitaria migliore e più efficiente.

eXL | primo piano

La *Digital Health* è protagonista anche nei programmi di finanziamento PRIN. Il progetto **MEDICA** – *Modelling and vErification of alkaptonuria and multiple sclerosis Driven by biomedICAl data* – si propone di integrare dati per costruire modelli computazionali di due malattie: la sclerosi multipla e l'alkaptonuria. Il progetto **FAVORITE**, invece, studia un nuovo gene associato allo spettro dell'Autismo utilizzando metodologie in vitro e in vivo, con il supporto dell'IA.

La *Digital Health* pisana è caratterizzata anche da numerose collaborazioni internazionali. **AInCP** – *clinical validation of Artificial INtelligence for providing a personalized motor clinical profile assessment and rehabilitation of upper limb in children with unilateral Cerebral Palsy* (*aincp.eu*) – è un pro-

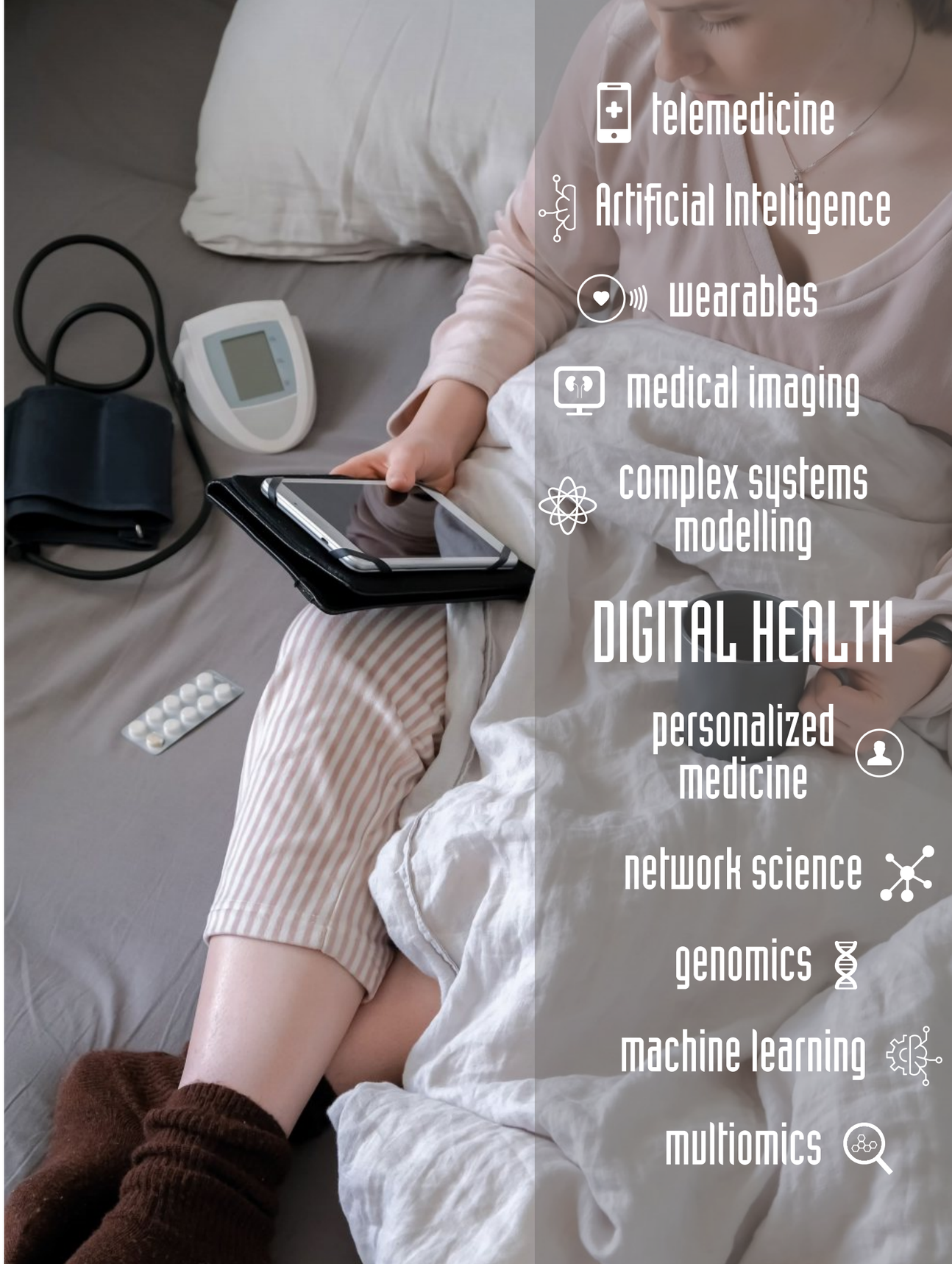
getto finanziato dalla Commissione Europea che ha lo scopo di sviluppare strumenti software basati su tecniche di IA per il supporto alla diagnosi e alla riabilitazione di bambini con paralisi cerebrale unilaterale.
Spark Pisa, invece, ha come missione la ricerca traslazionale, i.e. l'avanzamento della ricerca in medicina per produrre soluzioni reali e terapie utili per i pazienti. Nato all'Università di Stanford nel 2006, riunisce quasi 50 istituti a livello mondiale. Sotto l'ombrello Spark vengono finanziati progetti di ricerca UNIPI e portati avanti vari progetti in collaborazione con Stanford.

L'Università di Pisa e l'intero ecosistema pisano emergono quindi come un polo di eccellenza in questo settore, dimostrando come la collaborazione tra specialisti della salute e informatici possa portare a risultati straordinari e come la *Digital Health* sia non solo il futuro, ma già anche una realtà tangibile con profondi ed evidenti impatti socio-economici.

** Professore Associato, Dipartimento di Informatica, UNIPI. Si interessa di swarm robotics e IA applicata alla salute*

*** Professoressa Associata, Dipartimento di Informatica, UNIPI. Ricerca in machine learning e modellizzazione applicate alla salute*

Digital health stands at the crossroads of digital technology and healthcare. It is a rapidly evolving field which takes advantage of technological innovations to improve and personalise patient care, optimise clinical research and enhance the efficiency of healthcare systems. Using such tools as **telehealth**, **health apps**, **wearables** and **artificial intelligence** (AI) applied to various types of data, digital health aims to transform traditional assistance paradigms, making them more accessible, more rapid and more patient-centred. This innovation not only leads to more precise diagnoses and treatments but also to greater participation on the part of patients in managing their health.
The development of digital health requires collaboration between specialists in the fields of health and information technology. Over the last few years, a collaborative ecosystem has evolved in Pisa between various actors, including the University of Pisa, the Sant'Anna School of Advanced Studies, the Santa Chiara and Cisanello hospitals and several institutes of the National Research Council (CNR). The activities of local research groups have also expanded nationally and internationally in various projects and funding initiatives. The University of Pisa is involved in a number of current projects in the sector of digital health.
The *Tuscany Health Ecosystem project* (THE, www.tuscanyhealthecosystem.it), an initiative within the framework of the National Recovery and Resilience Plan (NRRP), aims to stimulate, support and consolidate the growth of Tuscany's life sciences ecosystem. Another NRRP project, *Fit for Medical Robotics* (www.fit4medrob.it), concerns rehabilitation and personal assistance for subjects with decreased or absent motor, sensorial or cognitive functions by means of robotic treatments. The *MEDICA project* (Modelling and vErification of alkaptonuria and multiple sclerosis Driven by biomedICAl data) has the objective of integrating data to construct computational models for two diseases: multiple sclerosis and alkaptonuria. The *FAVORITE project*, finally, studies a new gene associated with the spectre of autism with the aid of artificial intelligence.



ECCELLENZA NEL PHARMA

AOP Health: dal cuore della Toscana, l'avanguardia nelle malattie rare e in terapia intensiva

AOP, an excellence in Pharma

DI REDAZIONE

Sempre più soluzioni e terapie per i malati rari e per la terapia intensiva: questo è il lavoro concreto che **AOP Health Italy**, azienda biofarmaceutica di origine austriaca, porta avanti da sempre, e in Italia, in particolare, da quando ha scelto Pisa come sede centrale.

In questi anni, infatti, AOP Health ha reso disponibili nuove soluzioni per diverse patologie rare, ha attivato progetti di ricerca in partnership con Istituti di tutta Italia e ha realizzato un programma intenso di ampliamento dell'organico, dando vita a una fase di sviluppo che proseguirà anche nel prossimo futuro. "Da due anni a questa parte è iniziata per noi una fase importante", commenta **Nicola Zancan**, **General Manager di AOP Health in Italia**. "Abbiamo portato sul mercato italiano nuove terapie integrate potenzialmente in grado di fare una profonda differenza nella cura di persone affette da Policitemia Vera, un tumore raro e cronico del sangue, da Ipertensione Arteriosa Polmonare o Ipertensione Polmonare Cronica Tromboembolica, malattie polmonari che, se non adeguatamente trattate, causano un pericoloso scompenso cardiaco". Di grande impatto sulla sicurezza dei pazienti sono, poi, le soluzioni messe a punto da AOP Health nell'ambito della terapia intensiva per la gestione della sepsi e dello shock settico, condizioni altamente critiche che richiedono un intervento urgente. Va infatti ricordato che la sepsi, che colpisce fino a 50 milioni di persone nel mondo ogni anno, è anche la prima causa di decesso negli ospedali a livello globale.

AOP Health è attiva da oltre vent'anni nella ricerca, **sviluppo e distribuzione di soluzioni terapeutiche integrate per pazienti affetti da patologie rare e in condizioni critiche**. Sono quattro le aree terapeutiche nelle quali opera, con attività di ricerca particolarmente avanzate: **onco-ematologia**, **cardiologia** e **pneumologia**, **terapia intensiva e neurologia**.

Nel 2019, già attiva in Italia, ha deciso di stabilire la sua base italiana a Pisa e avviare una fase di consistente sviluppo. "Pisa per noi è un polo particolarmente interessante per la sua collocazione e logistica, grazie alla presenza di prestigiose università, ma anche per le attività di ricerca e la vitalità delle start up

eXL | primo piano

nel biotech e nelle nanotecnologie. Di fatto un territorio ideale per chi come noi si occupa di medicina e di ricerca scientifica e medica", osserva Zancan. Le attività realizzate in modo integrato e sinergico hanno un valore nazionale e spesso internazionale. "Un esempio recente è la **partnership con la Croce Rossa di Pisa**, nata per garantire assistenza e continuità terapeutica ai pazienti affetti da Ipertensione Arteriosa Polmonare, assicurando la tempestiva disponibilità delle pompe di somministrazione infusionale anche in situazioni di emergenza, attiva non solo in Toscana ma anche in altre regioni, e puntiamo all'Italia intera". Il Gruppo AOP Health, nel suo complesso, punta ad arrivare a 1 miliardo di euro di fatturato nel 2030 a livello mondiale e in questo contesto di crescita l'Italia sta giocando, e sempre di più giocherà, un ruolo di primo piano a livello internazionale. "Per raggiungere questi traguardi valutiamo costantemente nuovi progetti d'investimento in Italia, ulteriori ampliamenti dell'organico e collaborazioni con importanti realtà accademiche e del mondo scientifico per favorire il progresso delle cure e migliori possibilità per i pazienti" chiarisce Zancan.

More and more solutions and therapies for rare disease patients and for intensive care: this is the work that AOP Health Italy, biopharmaceutical company headquartered in Austria, has been carrying out in Italy, particularly in the past two years, since it set its base in Pisa.
"We brought to the Italian market new integrated therapies that have the potential to make a profound difference in the care of people with Polycythemia Vera, a rare and chronic blood cancer, from Pulmonary Arterial Hypertension or Chronic Thromboembolic Pulmonary Hypertension, pulmonary diseases that, if not adequately treated, cause dangerous heart failure" said **Nicola Zancan**, *General Manager at AOP Health Italy*.
Of great impact on patient safety are, then, the solutions developed by AOP Health within the ICU for the management of sepsis and septic shock.
AOP Health has been focused for over twenty years on the research, development and distribution of new therapeutic options for rare diseases and critical care. The company provides integrated solutions in four areas: hemato-oncology, cardiology and pulmonology, intensive care and neurology.
In 2019, already active in Italy, the company established its Italian base in Pisa and started a phase of substantial development, with new therapies available, research projects and an increase in its workforce. The AOP Health Group as a whole aims to reach 1 billion euros in sales by 2030 worldwide, and Italy is playing, and increasingly will play, a leading role internationally.
"To reach these goals we are constantly evaluating new investment projects in Italy, further staff expansions, and collaborations with important academic and scientific partners to promote the progress of treatments and better possibilities for patients," said Zancan.

di Denise Amram*

LA STRATEGIA DEI DATI

I valori dell'Unione Europea per una regolamentazione dei flussi di dati a tutela dei diritti fondamentali e per una migliore organizzazione delle strategie aziendali

European data strategy

L'effetto della dimensione digitale sui diritti fondamentali delle persone può essere generalmente descritto come l'analisi delle conseguenze derivanti dalla **mancanza di trasparenza o consapevolezza del soggetto riguardo alle operazioni di gestione dei dati**, come la profilazione delle abitudini o dei comportamenti, **e l'uso secondario dei dati**. La conseguente graduale perdita di controllo sul flusso di informazioni determina un aumento della probabilità di subire conseguenze negative, alcune delle quali potrebbero non essere prevedibili, a causa del trattamento di dati personali e non personali specialmente nell'ambiente digitale: si pensi all'accesso non autorizzato alle informazioni personali, alla profilazione che esponga a contenuti o decisioni automatizzate, spesso non strettamente legate agli scopi iniziali della raccolta dei dati.

L'interesse per questo argomento è suscitato dalle numerose iniziative legislative promosse nell'ambito della **strategia europea dei dati**, volte a stabilire ruoli e responsabilità dei vari attori coinvolti in un determinato flusso di dati, allo scopo di identificare e valutare in modo più accurato l'impatto che essi possono avere sulle rispettive attività, sia nei confronti degli utenti in generale che nei confronti di categorie specifiche di soggetti vulnerabili.

Questo processo mira a consentire l'implementazione di livelli di conformità diversificati per specifici obblighi al fine di proteggere gli utenti di servizi o di prodotti cosiddetti *data-driven*. Per esempio, la valutazione dell'impatto sulla **protezione dei dati** come definita nell'articolo 35 del Regolamento UE n. 2016/679, noto come GDPR, nonché la valutazione dell'**affidabilità dei sistemi basati su tecniche di intelligenza artificiale** e i requisiti di ***due diligence*** imposti dal Regolamento UE 2022/2025 (*Digital Services Act*) per i contenuti online disegnano nuovi scena-

#Denise Amram

ri per la *compliance* aziendale, sia pubblica che privata.
Il gioco vale senz'altro la candela: nella società orientata ai dati, il riuso delle informazioni costituisce il motore principale per il progresso in tutti i settori e facilita la transizione digitale nello sviluppo di beni e nell'erogazione di servizi. In questo contesto, il Regolamento UE 2022/868, *Data Governance Act*, introduce addirittura il meccanismo di "**altruismo dei dati**", attraverso il quale gli individui possono contribuire direttamente alle sfide della *data economy* mettendo a disposizione le loro informazioni personali a organizzazioni – i cosiddetti intermediari di dati – che si occupano di gestire in maniera sicura le informazioni da condividere *as open as possible* secondo condizioni e per finalità determinate, centralizzando di fatto il processo di *compliance* rispetto ai flussi in entrata e in uscita. Attraverso l'altruismo dei dati, il **controllo dell'individuo sulle informazioni che lo riguardano** non solo è mantenuto, ma addirittura è rafforzato grazie a un sistema di obblighi informativi rispetto agli usi e riusi da parte di terzi. Allo stesso tempo si incentiva il processo virtuoso di raccolta, gestione e condivisione in maniera sicura delle informazioni generate per una pluralità di scopi e di trattamenti.

** Ricercatrice in Diritto Privato Comparato, Scuola Superiore Sant'Anna*

Nuove sfide: il Data Governance Act
introduce l'*altruismo dei dati*

The European Union has developed a series of legislative initiatives to regulate data economy and its effects, included in the so-called EU Data Strategy. These regulations aim to establish **roles and responsibilities among the different stakeholders involved in a given (personal or non-personal) data flow**. The overall objective of the EU is to precisely identify and assess the impact that the digitalisation of services and products may have on users and their fundamental rights, as well as on the market and its rules in order to shape an inclusive data-driven society.
To this end, different compliance levels are envisaged through specific obligations for private and public organisations in order to protect and promote data subjects' fundamental rights while boosting data processing activities and the re-use of relevant information. In this context, the EU Regulation UE 2022/868, the Data Governance Act, introduced the mechanism of "**data altruism**", by means of which individuals can directly contribute to the challenges of the data economy by making their personal information "as open as possible", meaning available to specific organisations (namely the data intermediaries) which securely manage data in **robust infrastructures**, to be shared and reused by third parties for declared purposes. Such a bottom-up approach helps the data subjects to maintain and strengthen the control over their personal information and, at the same time, it encourages a virtuous and secure process of collecting, managing, and sharing the data generated to boost scientific progress and innovation.

eXL | digitale

di Arianna Torelli*

... Solo nella misura in cui si alimenta un rapporto di fiducia [...] immanente alle società, si può sperare di attingere alla soddisfazione del bisogno di sicurezza che in esse si manifesta.

DIRITTI E SICUREZZA

Il 2023 ha segnato il settantacinquesimo anniversario della Dichiarazione Universale dei diritti umani ma a distanza di anni sono ancora molte le violazioni

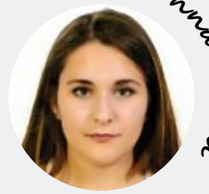
Right to security

Il 2023 è stato un anno particolarmente simbolico poiché ha segnato il settantacinquesimo anniversario della proclamazione della Dichiarazione Universale dei diritti umani, il venticinquesimo anniversario della *UN Declaration on Human Right Defenders* e il trentesimo anniversario della Dichiarazione di Vienna e Programma d'azione, eppure ha visto verificarsi molteplici violazioni dei diritti fondamentali, l'insorgere di conflitti e l'intensificarsi di altri in quasi ogni continente. Dimenticare l'importanza dei diritti, trascurarne la tutela per abdicare alla soddisfazione del bisogno di sicurezza che innerva le società contemporanee equivale a dimenticare la storia dell'uomo, poiché essa è la storia dei diritti e della loro lenta conquista, dell'opposizione all'irrazionalità umana e politica che nega differenza e dignità.

È sufficiente dare uno sguardo alle cronache recenti, per mettere in questione il tanto invocato **diritto alla sicurezza e alla difesa: il fatto stesso che nel discorso pubblico ci si continui ad appellare a esso è forse indice di uno stato di insicurezza più profondo, che nasce dal non vedere preservati i diritti fondamentali**. Inoltre, va considerato che parlare di diritti chiama in causa anche la categoria di *identità*, poiché proprio questi costituiscono un contraltare al potere scellerato, alla sovranità partigiana. Di quale sicurezza si può godere, se ovunque e ripetutamente intorno a noi si vedono violati i requisiti minimi per la preservazione dell'integrità fisica e morale, e in diverse circostanze della dignità umana?

È pressoché impossibile stabilire un confine rispetto a una minaccia non identificata: qualsiasi azione – o presupposta reazione – si rivela completamente inefficace perché non orientata, perché senza destinatario. Così un confine cessa di essere un dispositivo di difesa e diviene una mera divisione escludente, che sostituisce, tanto nella prassi linguistica quanto in quella etico-politica, la protezione con l'isolamento. Rimane a dir poco singolare, però, che si rinnovi ciclicamente l'impulso a tracciare confini profondi, destinati a diventare faglie irrimediabilmente divergenti che, ampliandosi, sottraggono spazio vitale al di qua e al di là del limite: la faglia si amplia, tutto ciò che vi è intorno a poco a poco finisce per essere consumato. Bisognerebbe forse chiedersi da dove provenga questa tensione a fissare un limite, anche quando non si scorgono definitamente i confini del pericolo percepito; soprattutto, quando una simile dinamica può avere come deriva la demonizzazione dell'altro da sé, l'esclusione, l'annientamento.

Non è difficile intravedere come il bisogno di sicurezza possa esorbitare dalla sfera della difesa e tramutarsi in un espediente d'offesa: se la difesa è legittima, così anche l'offesa può essere legittimata. Piuttosto che i confini e gli atti di forza – quegli stessi atti d'offesa celati dall'apparenza, pretestuosamente calata, di atti di difesa nei confronti dell'alterità politica, etnica o culturale – bisognerebbe invocare invece in primo luogo il rispetto dei diritti umani, civili e sociali. **Solo nella misura in cui si alimenta un rapporto di fiducia, orizzontalmente e verticalmente, immanente alle società, si può sperare di attingere alla soddisfazione del bisogno di sicurezza che in esse si manifesta**.



#Arianna Torelli

* *Studentessa in Filosofia, Scuola Normale Superiore*

The year 2023 has been a particularly symbolic one, as it marks the 75th anniversary of the proclamation of the Universal Declaration of Human Rights, the 25th anniversary of the UN Declaration on Human Right Defenders, and the 30th anniversary of the Vienna Declaration and Programme of Action. Nonetheless, the year has seen numerous violations of fundamental rights, the outbreak of some conflicts and the intensification of others on nearly every continent. Forgetting the importance of rights, neglecting to protect them in the name of those security needs which have become the obsession of contemporary societies is tantamount to forgetting human history: the development of civilisation is in fact the story of rights and the slow process of conquering them in the face of irrational social and political ideas which deny difference and dignity.

We need only take a look at recent news events to call into question the much-heralded right to security and defence: the fact that we continue to appeal to this right in public discourse in itself reveals the profound state of insecurity in which we find ourselves, which is caused by the perception that our fundamental rights are not being respected. At the same time, identity discourse is not completely unrelated to the notion of rights, given that the latter act as a bulwark against unbridled power and partisan affirmations of sovereignty. What kind of security can we expect when everywhere around us we repeatedly see violations of the minimum preconditions for preserving our physical and moral wellbeing and even our human dignity? Rather than borders and acts of force – those same aggressive acts masquerading as defence measures against political, ethnic or cultural otherness – we need first of all to invoke respect for human, civil and social rights. Only to the extent that we create **relations of trust** within societies, both horizontally and vertically, can we hope to enjoy the security which they are meant to provide.

di Niccolò Borgioli* e Federico Aromolo**

MAI TROPPO SICURI

L'importanza di difendere i nostri dispositivi in un mondo sempre più connesso

How to protect against cyberattacks

Con l'evoluzione tecnologica siamo sempre più connessi. Oggetti un tempo pensati per lavorare isolati dal resto del mondo sono stati prima informatizzati, divenendo sistemi ciberfisici, e poi interconnessi con il mondo per fornirci sempre più dati e funzionalità.

Le auto moderne e del futuro, tipici esempi di sistemi ciberfisici, sono costantemente connesse alla rete per fornirci contenuti, traffico in tempo reale e ulteriori funzionalità per rendere il viaggio più confortevole. Allo stesso tempo, i veicoli continuano ad evolvere integrando funzioni essenziali per la nostra sicurezza, come *cruise control adattivo*, sistemi anticollisione e guida autonoma.
Tuttavia, tutto questo ha un prezzo: una maggior esposizione al rischio di attacchi informatici. Uno studio recente pubblicato da SonicWall (importante società di sicurezza informatica statunitense) ha analizzato il trend di cyberattacchi degli ultimi anni evidenziando come solo nel corso del 2022 il numero di attacchi a sistemi ciberfisici sia quasi duplicato rispetto all'anno precedente, toccando quota 112 milioni. Questo è un chiaro segnale che **l'attenzione dei cybercriminali si stia sempre più spostando verso i sistemi ciberfisici, siano essi critici (come le auto) o non critici (come i termostati, i televisori e le lavatrici smart)**.
In questo contesto risulta cruciale la definizione e lo **sviluppo di tecnologie in grado di proteggerci** da tali minacce. I computer tradizionali possono essere protetti attraverso l'utilizzo di firewall e software antivirus. Tuttavia, tali strumenti richiedono continui aggiornamenti e non sono pensati per operare in un contesto dove le risorse computazionali a disposizione e la possibilità di intervento umano sono limitate (come potrebbe essere un'automobile).
Per poter fronteggiare queste crescenti minacce, il **laboratorio di Sistemi in Tempo Reale** (ReTiS) della Scuola Superiore Sant'Anna è all'avanguardia nella ricerca e nello sviluppo di tecnologie innovative in grado di proteggere i dispositivi digitali di oggi e di domani. In particolare, le ricerche svolte nell'ambito del progetto SPHERE, finanziato dal Ministero dell'Università e della Ricerca, hanno

Con il progetto SPHERE l'accesso alla rete diventa sicuro

consentito di sviluppare nuove metodologie mirate a garantire l'accesso alla rete in maniera sicura ai sistemi che svolgono funzioni critiche e individuare in tempo reale attacchi al sistema.
Vediamo in dettaglio di cosa si tratta. I sistemi tradizionali di individuazione degli attacchi si basano sull'identificazione di un insieme di caratteristiche che definiscono un attacco (firma) e sull'analisi del traffico di rete al fine di individuare comportamenti malevoli. Questo approccio, tuttavia, richiede una conoscenza puntuale dei possibili attacchi e un continuo aggiornamento delle firme per rimanere al passo con le nuove minacce.
I ricercatori del laboratorio ReTiS, invece, hanno sviluppato un **meccanismo di identificazione basato su Reti Neurali Artificiali** in grado di superare questi limiti mediante una **metodologia di apprendimento che consente di riconoscere i comportamenti buoni e conseguentemente di individuare gli attacchi come comportamenti anomali**.
Tale soluzione permette di individuare attacchi in tempo reale con una precisione del 99,9% anche in presenza di tecniche di attacco sconosciute. Per poter essere utilizzati in sistemi ciberfisici, questi meccanismi devono essere progettati per garantire una risposta in tempo reale e un utilizzo efficiente delle risorse computazionali a disposizione dei sistemi di bordo. Di conseguenza la ricerca del laboratorio ReTiS si sta focalizzando anche sull'ottimizzazione del meccanismo di difesa utilizzando le più recenti tecniche di accelerazione hardware.

** Allievo perfezionando, Istituto di Telecomunicazioni, Informatica e Fotonica, Scuola Superiore Sant'Anna*

*** Ricercatore, Istituto di Telecomunicazioni, Informatica e Fotonica, Scuola Superiore Sant'Anna*

Technological evolution means that we are increasingly connected. Products that were originally conceived to allow us to work in isolation from the rest of the world were first digitised (becoming cyber-physical systems) and then interconnected with the world, creating increasing amounts of data and functions. All of this has come at a price, namely increased exposure to the risk of cyber attacks. A recent study published by SonicWall analysed the trend of cyber attacks over the last few years, reporting that in 2022 the number of attacks on cyber-physical systems doubled with respect to the previous year, numbering 112 million. This is a clear sign that cyber criminals increasingly have their sights set on cyber-physical systems, whether critical (such as cars) or non-critical (thermostats, televisions and smart washing machines).
In this context it becomes crucial to design and develop technologies that can protect us from such threats. The Real Time Systems (ReTiS) laboratory of the Sant'Anna School of Advanced Studies is at the forefront in researching and developing innovative technologies able to protect present and future digital devices. Research carried out in the framework of the SPHERE project funded by the Ministry of Higher Education and Research has led to the development of new methods aimed at guaranteeing safe Internet access for systems that carry out critical functions and at identifying attacks to a system in real time.
In addition, researchers at the ReTiS laboratory have developed an identification mechanism based on artificial neural networks, which is able to overcome present limits: this technology uses a learning function that recognises proper behaviours, with the result that it is able to identify attacks as anomalous acts. The mechanism can spot attacks in real time with an accuracy of 99.9%, including when these are carried out with unknown methods.
In order to be used in cyber-physical systems, these mechanisms must be designed to ensure real-time response and efficient use of computational resources.
Consequently, ReTiS lab's research is also focusing on defense mechanism optimization using the latest hardware acceleration techniques.

CULTURA DI CANTIERE

di Valentina Baldacci* e Nicola Bellani**

Grazie agli Enti Bilaterali per l'Edilizia, le Scuole Edili e CPT sta crescendo l'attenzione alla tutela della salute e della sicurezza sui luoghi di lavoro

H&S culture in worksites

Il lavoro in quanto tale è un insieme di azioni e relazioni che si svolgono nei più svariati ambienti in cui sembra purtroppo impossibile affrancarsi dal fenomeno degli **infortuni** e delle **malattie professionali**.

Quando i fenomeni infortunistici si manifestano, siamo soliti pensare a come la **tutela della salute e** la **sicurezza** non siano affrontate da tutti gli attori coinvolti in modo efficace e adeguato.
Nel rapporto annuale regionale 2022, l'Inail indica che a livello nazionale le denunce di infortunio sono state 703.432 con un aumento del 22,89 % rispetto al 2020 e del 24,63% in più rispetto al 2021.
A livello regionale, nello stesso Rapporto e nello stesso anno, le denunce di infortunio sono state 53.128, in aumento rispetto al 2020 (+28,47%) e al 2021 (+21,93%).

Le denunce di infortunio con esito mortale, rilevate in Toscana nel 2022 sono state 81, 1 caso in più rispetto al 2020 e 6 in più rispetto al 2021. Di questi 81 casi di infortunio con esito mortale, 62 si sono verificati in occasione di lavoro (8 in meno del 2020, 4 in più del 2021) e gli altri 19 sono riferiti alle denunce di infortunio con esito mortale in itinere.
A livello nazionale, invece, le denunce di infortunio con esito mortale sono state 1.208, 501 casi in meno rispetto al 2020 e 217 in meno rispetto al 2021. In particolare, gli infortuni mortali in occasione di lavoro sono stati 875, 602 in meno rispetto al 2020, 272 in meno rispetto al 2021 e 333 quelli in itinere.
Esaminando questi dati verrebbe da pensare che i problemi inerenti alla sicurezza sui luoghi di lavoro siano ancora lontani dal dirsi risolti. Tuttavia, se ci lasciassimo vincere da questa interpretazione, non saremmo obiettivi. È importante prendere in considerazione, guardandoci indietro, anche le azioni correttive messe in campo da enti, istituzioni, associazioni di categoria, un caso dopo l'altro, un anno alla volta… Proprio perché si parla di "cultura", il processo in atto sarà ancora lungo e il risultato del lavoro e della prevenzione di oggi potranno essere apprezzati solo nel mondo del lavoro di domani.
In Toscana, nel 2022, la Direzione Regionale di Inail ha sottoscritto un protocollo d'intesa finalizzato alla promozione di attività congiunte di formazione, promozione e informazione nel settore edile, con il Coordinamento Regionale dei Comitati Paritetici Territoriali Toscani per la Sicurezza sui luoghi di lavoro. Attraverso il coinvolgimento degli Enti Bilaterali per l'Edilizia, in particolare Scuole Edili e CPT, sono state promosse svariate iniziative.
Ed è proprio questa una delle finalità cardine su cui si basa il lavoro degli Enti Bilaterali del Settore Edile.
A Pisa, dal 1961, gli Enti Bilaterali per le Costruzioni (costituiti da Gruppo Costruttori - Ance di Pisa e dalle OO.SS. Feneal Uil - Fillea, CGIL e FILCA, CISL), Cassa Edile, Scuola Edile e CPT si occupano nello specifico di:

1. assicurare ai lavoratori una parte importante del trattamento economico derivante dal contratto di lavoro, nonché significative prestazioni integrative sul piano previdenziale e assistenziale;

2. svolgere nei propri cantieri-laboratorio le attività di formazione e di addestramento professionale in rapporto ai fabbisogni del mercato del lavoro;
3. perseguire fini istituzionali sulla prevenzione infortuni, l'igiene e l'ambiente di lavoro per le attività edili e complementari.

L'Ente Unico Scuola Edile e CPT della Provincia di Pisa esercita ogni opportuno intervento attraverso le visite di cantiere, per favorire l'attuazione delle norme di legge sulle misure di prevenzione e sull'igiene del lavoro, nonché sulle condizioni ambientali in genere, avvalendosi di tecnici professionalmente qualificati. Suggerisce inoltre l'adozione di iniziative dirette allo svolgimento di corsi di formazione per il personale preposto alla attuazione delle norme antinfortunistiche (D.Lgs.81/2008).
Di particolare rilievo, in quanto "progetto pilota" a partire dal 2016 e ancora in essere, è il progetto **Vivere il Cantiere e Impararlo a Scuola**, promosso dagli Enti Bilaterali del settore delle Costruzioni di Pisa in collaborazione con Inail Pisa, Asl, Ance Pisa e rivolto agli studenti degli istituti tecnici per geometri della Provincia di Pisa. Si tratta di un corso "16 ore - formazione primo ingresso", una importante innovazione introdotta in tutti i Contratti Collettivi di Lavoro dell'edilizia, che dal primo gennaio 2009 prevede che ciascun lavoratore riceva, prima dell'assunzione in Impresa, una formazione orientata alla sicurezza di base. Dare la possibilità agli studenti della terza classe delle scuole superiori di formarsi in questo senso rappresenta un modo di promuovere la "cultura della salute e sicurezza" già durante gli anni di studio di un futuro lavoro.
Iniziative come quelle sopra descritte sono da implementare e rendere strutturali nel percorso formativo di tutti gli studenti degli istituti secondari di secondo grado, anche in un'ottica di formazione continua dei futuri lavoratori.
Non meno importante sarà cercare di intraprendere, nel prossimo futuro, attività specifiche di formazione alla sicurezza nei luoghi di lavoro, tenendo conto ad esempio anche delle nuove sfide culturali che ci pone ogni giorno il fenomeno immigratorio di massa, in cui la sicurezza dovrà passare dall'elemento più basilare: la comprensione della lingua italiana e della nostra cultura della sicurezza.

** Coordinatore di Ente Pisano Cassa Edile ed Ente Scuola Edile e CPT della Provincia di Pisa*
*** Tecnico di cantiere*

In its 2022 annual regional report, INAIL stated that nationally there were 703,432 workplace injury reports, an increase of 22.89% compared to 2020 and of 24.63% with respect to 2021.
At the regional level, the same report stated that in 2022 injury reports numbered 53,128, an increase of 28.47% and 21.93% compared to 2020 and 2021, respectively.
Injuries resulting in death amounted to 81 in Tuscany in 2022, 1 more than in 2020 and 6 more compared to 2021. Of the 81 cases, 62 were immediate deaths at the worksite (8 fewer than in 2020, 4 more with respect to 2021), while the other 19 victims died in the aftermath of the accident.
In 2022, the Tuscan Regional Direction of INAIL signed an agreement protocol aimed at organising joint onsite **activities of training, awareness raising and information about workplace safety in the construction sector**. A variety of initiatives were set in motion through the involvement of the *Enti Bilaterali per l'Edilizia* ("bilateral agencies for the construction sector"), in particular the *Scuole Edili e CPT*.
Of particular relevance – in its capacity as a "pilot programme" begun in 2016 and still ongoing – is the project "**Vivere il Cantiere e Impararlo a Scuola**", sponsored by the *Enti Bilaterali* of the Pisa Construction Sector and in collaboration with INAIL Pisa, ASL, and ANCE Pisa. The project is specifically directed at students of the Technical Institutes for Surveyors of the province of Pisa. The 16-hour beginner's course represents a significant innovation introduced into all collective work contracts in the construction sector, which since January 2009 require that workers complete a basic safety training programme before being hired by a company. Providing third-year high school students with the opportunity to gain understanding of workplace safety issues represents a way of promoting a "**culture of health and safety**" before entering the working world.
Initiatives such as this one should be incorporated as permanent features of the curricula of all secondary school technical institutes, as part of the lifelong training of tomorrow's workers.

RISCHI D'IMPRESA

di Alberto Susini

**Sono ancora poche le aziende che investono in tecnologie contro minacce e attacchi informatici.
La Camera di Commercio in campo per la cybersicurezza**

Cybersecurity, business risks

La ***cybersecurity***, da un po' di tempo, sta provando a entrare nel vocabolario degli **imprenditori**. Per sensibilizzare le PMI sul tema, il sistema delle **Camere di Commercio** ha attivato all'interno delle proprie strutture di servizio dedicate alla diffusione della cultura e della pratica della diffusione del digitale (i cosiddetti **Punti Impresa Digitale** - PID) una serie di servizi.

Data Transfer

I dati provenienti dai test di autovalutazione delle PMI della Provincia di Pisa relativi al biennio 2021-2022 svelano però un quadro allarmante: soltanto il 7% ha investito in tecnologie idonee alla sicurezza informatica. Parliamo di strumenti quali gli IDS (*Intrusion Detection System*), la crittazione dei dati e l'identificazione biometrica, fondamentali nell'ottica di difendersi da minacce digitali sempre più sofisticate. Al di là dei dati, emerge un segnale preoccupante: la *cybersecurity* non è ancora percepita come una priorità strategica da parte del management aziendale.
Per far luce sulla questione abbiamo chiesto ad **Antonio Romeo**, **Direttore di Dintec e Responsabile Nazionale dei Punti Impresa Digitale delle Camere di Commercio**, alcune riflessioni.

Direttore, quali sono le minacce più comuni che le PMI devono affrontare in termini di cybersecurity?

«Secondo i dati dei PID, il 79% delle imprese italiane si trova in una fascia di rischio medio-elevata sotto il profilo della *cybersecurity*. Questo è dovuto a una scarsa formazione delle risorse umane e all'assenza di *policy* e di procedure adeguate a contrastare il problema degli attacchi informatici. Attacchi informatici che riguardano almeno il 41% delle imprese italiane con il *malware* e il *phishing* che rappresentano le tipologie più frequenti».

Quali sono le principali azioni che le piccole e medie imprese possono intraprendere per proteggersi?

«La principale azione che le piccole e medie imprese devono intraprendere per proteggere i loro sistemi organizzativi da attacchi *cyber* è intervenire sul capitale umano mediante azioni di formazione, che tuttavia solo il 10% delle imprese effettuano in modo sostenuto. Bisogna poi agire sui processi e sulla *governance* aziendale, individuando responsabilità interne chiare con funzioni di riferimento a presidio della tematica della *cyber*. Bisogna infine puntare sulla strumentazione tecnologica, che solo nel 37% dei casi le imprese dichiarano di aver implementato.
La sicurezza informatica, lo dicono i numeri, è diventata un imperativo per le aziende: investire in formazione, adottare protocolli efficaci e implementare soluzioni tecnologiche adeguate sono azioni ormai non più rinviabili».

#Antonio Romeo

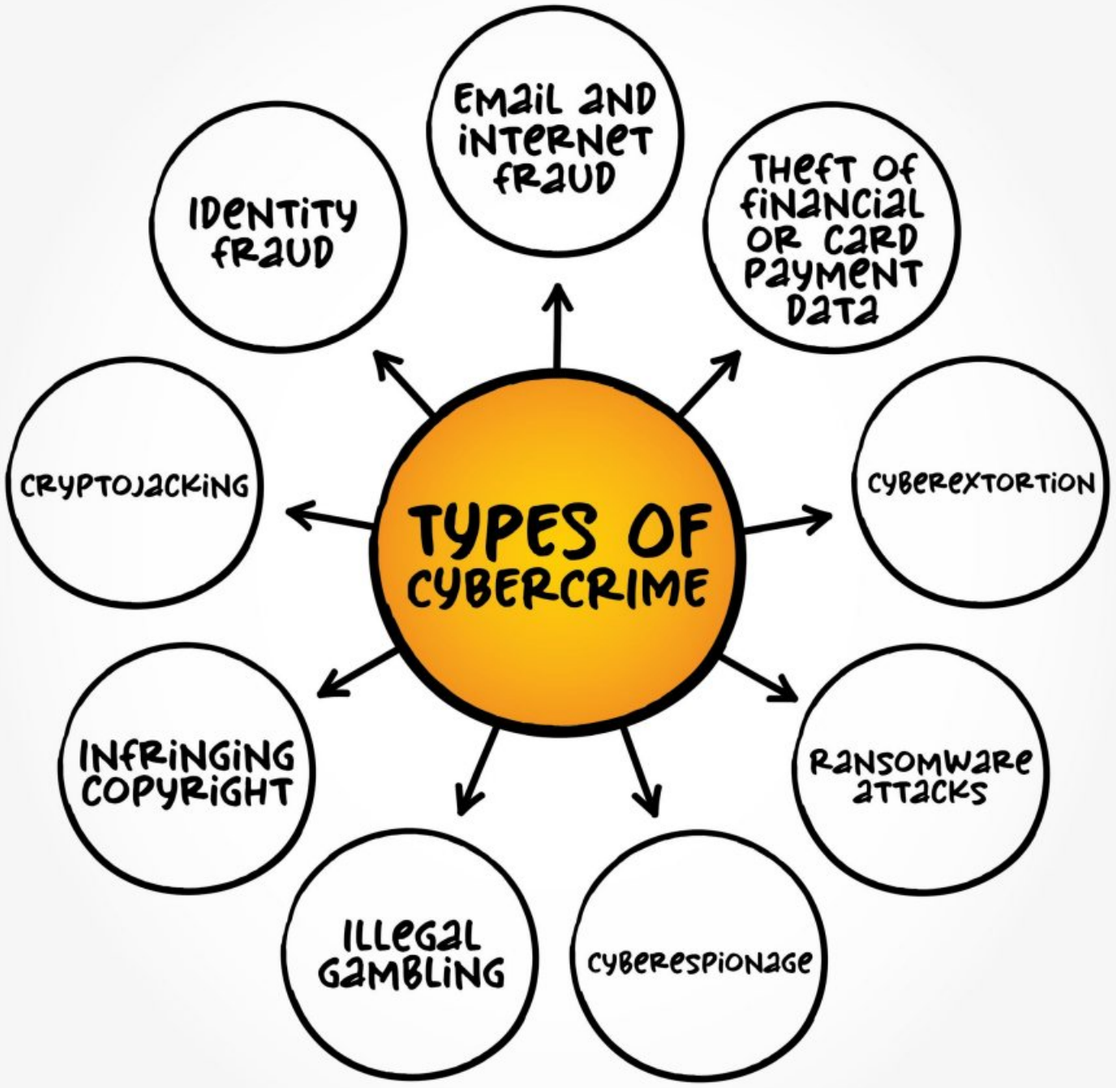
Cosa offre il sistema delle Camere di Commercio per supportare piccole e medie imprese nell'ambito della cybersecurity?

«Il sistema camerale mette a disposizione delle piccole e medie imprese una serie di strumenti per poter contrastare attacchi *cyber*. In prima analisi, un test gratuito (*PID Cyber Check*) che consente di effettuare un'autovalutazione del livello di rischio di attacchi informatici. A valle di questa attività viene generato un report che fornisce all'impresa una serie di suggerimenti per la cybersicurezza. Esiste poi un *assessment* più profondo (*Cyber Exposure Index*) che consente di avere una valutazione quantitativa dei servizi esposti, delle vulnerabilità presenti e delle fughe dei dati. Inoltre, il sistema delle Camere di Commercio offre, attraverso i PID, una serie di percorsi info-formativi per consentire alle imprese di avvicinarsi agli strumenti del sistema camerale e soprattutto colmare i gap in materia di cybersicurezza».

Statistics tell us that digital safety has become a major concern of companies, which have come to realise that they can no longer put off investing in training, adopting effective protocols and implementing adequate technological solutions. To gain insight into the phenomenon, we spoke with Antonio Romeo, director of Dintec and national coordinator of the *Punti Impresa Digitale* (PID, "digital business points") of Italy's Chambers of Commerce.

What are the most common threats that SMEs face in terms of cybersecurity?
«According to PID data, 79% of Italian businesses find themselves in a medium-to-high risk range with regard to cybersecurity. This is due to a lack of training on the part of personnel and to the absence of adequate policies which prevent cyber attacks. At least 41% of Italian companies have experienced attacks, with malware and phishing as the most frequent forms».

What are the most important actions that small and medium businesses can take to protect themselves?
«The primary action which small and medium busi-



nesses must take to protect their organisational systems from cyber attacks is to train their personnel; only 10% of companies carry out these initiatives regularly. Then, a business must review its procedures and governance model, assigning clear internal responsibilities and oversight functions with regard to cybersecurity. Finally, companies need to focus on the implementation of proper technological tools, which only 37% of businesses have undertaken».

What does the Chamber of Commerce system offer in the way of supporting small and medium businesses in the field of cybersecurity?
«The Chambers of Commerce are able to provide small and medium businesses with a series of tools to ward off cyber attacks. First of all, we offer a test free of charge (the PID Cyber Check) which allows companies to self-evaluate their risk level for digital attacks. Following this analysis, a report is produced which provides the business with a series of suggestions for protecting itself from cyber security dangers. Then, a more in-depth assessment can be performed (the Cyber Exposure Index): this gives companies a quantitative evaluation as to which of their services are exposed to risk and what their vulnerabilities are, including data leakage. In addition to these assessment tools, the PIDs offer a series of informational and training sessions to familiarise businesses with the tools of the Chamber of Commerce system, allowing them to address their cybersecurity concerns».

di Silvia Maculan e Sara Profeti

Difendersi DALLA RETE

Il doppio volto dell'Intelligenza Artificiale: se da un lato può essere utilizzata dai pirati informatici, dall'altro è un ottimo alleato per la sicurezza digitale

AI double face

L'**Intelligenza Artificiale** sta rapidamente diventando una tecnologia fondamentale in tantissimi settori e **sta rivoluzionando il modo in cui proteggiamo le nostre informazioni e i sistemi informatici**.

Nell'ambito della ***cybersecurity***, l'**Intelligenza Artificiale** (IA) è insieme arma e strumento di difesa. Da un lato, i "buoni" possono tenere il passo sfruttando meccanismi basati su *machine learning* e *deep learning*. Allo stesso tempo, l'IA potrebbe essere usata da *hacker* e criminali digitali per attaccare i sistemi informatici e le piattaforme di protezione dei dati personali degli utenti.
Per fronteggiare queste minacce emergenti, è importante, prima di tutto, formare dei professionisti sulla sicurezza, che siano educati non solo sull'IA ma anche nell'ambito della *cybersecurity*. Alcuni enti e università stanno già proponendo master e studi su questa tematica. A livello internazionale sarà anche importante sviluppare delle linee guida e degli standard a cui attenersi. L'IA, poi, dovrà essere usata in modo responsabile, ma anche sicuro.
Essa trova già applicazione nell'ambito della *cybersecurity*: riesce ad esempio a rilevare un attacco informatico, analizzando i dati di traffico, o per automatizzare le attività di sicurezza delle reti, o ancora per proteggere gli *end point*, come i computer e i dispositivi *mobile*.

Ci sono diversi modi in cui l'IA può dare supporto alla sicurezza digitale, anche indirettamente. Di seguito ne elenchiamo i principali.

Identificare e prevedere i rischi

I sistemi di AI possono essere utilizzati per analizzare grandi quantità di dati, in modo rapido ed efficiente, alla ricerca di attività anomale o sospette. Ciò può aiutare a identificare le minacce prima ancora che riescano a causare danni, ma soprattutto a individuare e risolvere vulnerabilità nei sistemi informatici.

Riconoscere nuove minacce e ridurre i tempi di risposta

La capacità di apprendimento dell'AI è uno dei suoi punti di forza più evidenti, ed è proprio questa caratteristica a permetterle di imparare a riconoscere nuove tipologie di attacchi e a rispondere in brevissimo tempo.

Riduzione dell'errore umano

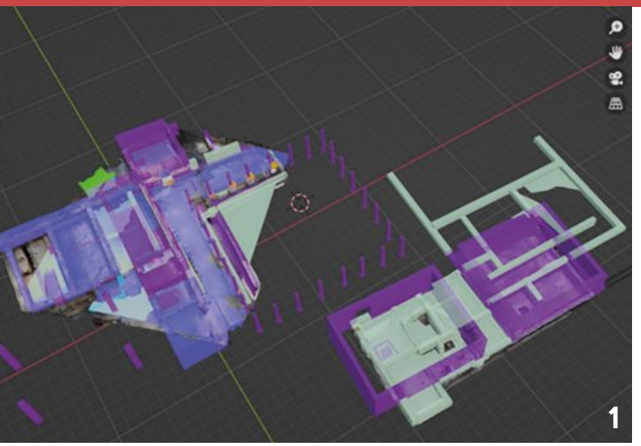
In situazioni di crisi dove sono richieste rapidità di risposta, freddezza e precisione, l'IA può dare supporto operando senza margine di errore. Un'altra applicazione interessante dei software basati sull'IA riguarda la formazione: il programma simula un attacco informatico e l'operatore si "allena" a difendere il sistema.

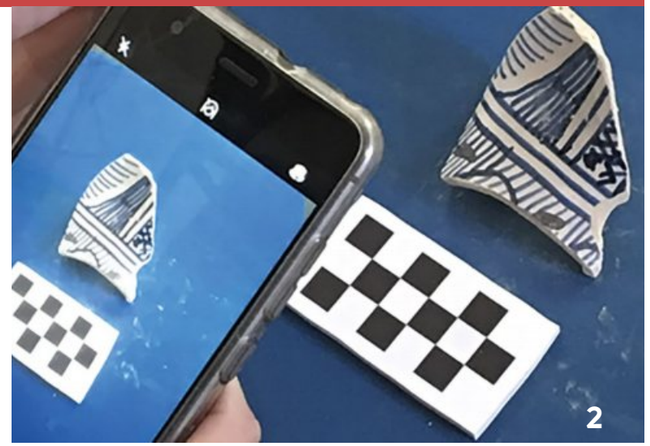
Sgravio del personale IT

È diffusa l'idea secondo cui l'IA è un sostituto che finirà col togliere lavoro al personale umano. In realtà questa ipotesi è ben lontana dalle possibilità delle attuali tecnologie, per quanto avanzate. È invece più probabile, e per alcune aziende già una realtà, che l'IA sia un supporto in grado di affiancare gli operatori permettendo loro di risparmiare tempo e così di dedicarsi ad attività per le quali sono necessarie competenze che essa non possiede, come il pensiero creativo.

È importante, sì, essere consapevoli dei rischi nel campo della *cybersecurity*. Tuttavia, i benefici offerti sono superiori. L'adozione dell'IA nella *cybersecurity*, infatti, può senz'altro migliorare la **sicurezza delle infrastrutture e dei dati sensibili**.

Artificial Intelligence is rapidly becoming a fundamental technology in many sectors, revolutionising the way we protect our information and data systems.
In the field of cybersecurity, AI is at the same time a weapon and a tool for defence.
On the one hand, the "good guys" are able to keep up with developments by taking advantage of mechanisms based on machine learning and deep learning. On the other hand, AI can be used by hackers and digital criminals, who have increasingly powerful means at their disposal to attack data systems and platforms that protect the personal data of users.
At the international level, developing binding guidelines and standards will be crucial. AI will have to be used responsibly and also securely. AI is already being used in the field of cybersecurity: it is able, for example, to detect a digital attack by analysing traffic data, to automate network security operations and to protect endpoints, such as computers and mobile devices.
AI can support **digital security** in many ways, sometimes indirectly: it is able to identify and predict risks, recognise new threats and reduce response times and human error, thus taking a burden off the shoulders of IT personnel.
While it is important to be aware of risks, the benefits it yields in the field of cybersecurity are greater. Adoption of AI in cybersecurity is in fact a positive tendency and can undoubtedly improve the safety of infrastructure and sensitive data.





1. Il complesso archeologico di Massaciuccoli Romana. *Elaborazione modello e immagine: Filippo Sala*

2. Riconoscimento automatico dei frammenti ceramici tramite la app di ArchAIDE. *Foto: Francesca Anichini*

3. Riconoscimento automatico dei frammenti ceramici tramite la app di ArchAIDE. *Elaborazione immagine: Miguel A. Hervas*

4. Il catalogo del progetto ArchAIDE e la ricostruzione 3D delle forme ceramiche. *Elaborazione immagine: team ArchAIDE*

di Francesca Anichini*

POTENZIALE ARCHEOLOGICO

Con MAPPALab l'Intelligenza Artificiale entra nel campo degli studi antichistici. Bastano una foto dal cellulare e una app per riconoscere i frammenti ceramici

MAPPALab, an innovative project

Il **Laboratorio MAPPA** (www.mappalab.eu) nasce nel 2012 dall'esperienza dell'omonimo progetto "MAPPA: Metodologie Applicate alla Predittività del Potenziale Archeologico", un progetto che sviluppò l'innovativa idea di **predire il potenziale archeologico sepolto in un contesto urbano**, utilizzando Pisa come *case study*, e creò il **primo archivio *open data* italiano** che raccoglie i dati grezzi provenienti dalle indagini e dalle ricerche archeologiche (MOD - https://digitallib.unipi.it/it/archivio/MOD-Mappa-Open-Data-archive).

In quell'esperienza furono gettate le basi degli elementi essenziali che caratterizzano il MAPPALab: la transdisciplinarietà dell'attività di ricerca metodologica con il coinvolgimento costante di professionalità differenti (archeologi, informatici, geologi, matematici, esperti di comunicazione); la centralità dello sviluppo e dell'utilizzo di strumenti digitali per gestire dati e rispondere a domande archeologiche; l'attenzione costante nei confronti di un riscontro applicativo dei prodotti della ricerca e, non da ultimo, la ferma volontà di rendere aperti i dati dell'archeologia italiana.
Negli anni il MAPPALab ha consolidato questi filoni di ricerca divenendo un punto di riferimento italiano e internazionale per quanti lavorano sui dati in ambito archeologico. Numerosi sono stati i progetti sviluppati che hanno sempre cercato di interconnettere i bisogni pratici

Il complesso archeologico di Massaciuccoli Romana. *Elaborazione modello e immagine: Filippo Sala*

degli operatori archeologici e le necessità di formazione degli studenti universitari, coniugando l'attività da campo con quella laboratoriale, attraverso la sperimentazione costante nell'innovazione digitale e in nuovi ambiti di ricerca, tra i quali l'archeologia dell'età contemporanea e quella ambientale. Tra il 2016 e il 2019, MAPPALab entra nel mondo dell'IA coordinando il progetto europeo **ArchAIDE** (*Archaeological Automatic Investigation and Documentation of cEramics*, www.archaide.eu) e sviluppando una **app capace di riconoscere i frammenti ceramici attraverso una foto da mobile**.

Contemporaneamente, il laboratorio continua l'attività sui dati e, ad aprile 2023, vara la nuova **piattaforma Magoh** (https://magoh.cfs.unipi.it) che gestisce e rende fruibili per professionisti, funzionari, ricercatori e cittadini un

Documentazione di reperti contemporanei.
Foto: Francesca Anichini

Nella piattaforma Magoh 20.000 evidenze archeologiche toscane

patrimonio di oltre 20.000 evidenze archeologiche in 107 comuni toscani.

Legati alla sperimentazione di nuove applicazioni sono inoltre attivi diversi progetti di ricerca che spaziano dalla **ricostruzione paleoambientale attraverso tecniche di IA**, alla definizione di **modelli virtuali ricostruttivi tramite BIM e *software open source***, all'applicazione di analisi spaziali e tecniche di ***data visualization*** in ambito archeologico, ai test con strumenti robotici per la catalogazione dei reperti.

Sono tra i punti di forza del MAPPALab il connubio con la matematica e la statistica e la promozione di numerose attività di formazione legate all'utilizzo di **linguaggi di programmazione**, come R e Pyton, su tematiche archeologiche.

Infine, MAPPALab continua a incentivare la condivisione aperta dei dati con l'implementazione costante dell'**archivio MOD** e con la gestione della rivista *open access* «**ArcheoLogicaData**» (www.mappalab.eu/archeologica-data-2).

** Insegna Archeologia Moderna e Contemporanea presso Unipi dove è tra i fondatori del MAPPALab*

The **MAPPA laboratory** (www.mappalab.eu) was founded in 2012 as a continuation of the initiative that went by the same name: *MAPPA: Metodologie Applicate alla Predittività del Potenziale Archeologico* (*MAPPA: Applied Methodologies for the Predictability of Archaeological Potential*). This project developed the innovative idea of predicting below-ground archaeological potential in urban areas, using Pisa as a case study. It created Italy's first open data archive, which collects raw data from archaeological investigations and research (MOD - https://digitallib.unipi.it/it/archivio/MOD-Mappa-Open-Data-archive/).

That experience laid the bases for the essential elements which characterise MAPPALab: the interdisciplinary character of methodological research operations, with the constant involvement of different professional figures (archaeologists, IT specialists, geologists, mathematicians and communication experts); the emphasis on developing and using digital tools to manage data and provide answers to archaeological questions; constant attention to the results of the application of research products; and, not least, the firm resolve to make Italian archaeological data open.

Over the years, MAPPALab has consolidated these lines of research, becoming a point of reference in Italy and abroad for those working on data in the field of archaeology. Between 2016 and 2019, MAPPALab entered the world of AI, coordinating the **European project ArchAIDE** (Archaeological Automatic Investigation and Documentation of cEramics - www.archaide.eu/) and developing apps able to recognise ceramic fragments by means of photos from mobile devices.

Today, the laboratory continues these data operations. In April 2023, it launched the new MAGOH platform (https://magoh.cfs.unipi.it), which manages a database of over 20,000 archaeological objects in 107 Tuscan cities and towns, making information available to professionals, operators, researchers and citizens.

Several other ongoing research projects are connected to this experimentation with new applications. These include paleoenvironmental reconstruction through AI techniques, the definition of reconstructive virtual models through BIM and open source software, the application of spatial analyses and data visualisation techniques in archaeological contexts, and tests with robotic instruments for cataloguing finds.

Il complesso archeologico di Massaciuccoli Romana.
Elaborazione modello e immagine: Filippo Sala

di Luca Fracassi

PROTETTI con un messaggio

Grande impulso è riservato all'informazione digitale in tema di allerta ed emergenze. Con AlertPisa, i cittadini ottengono notizie in tempo reale

Protected by a message

Si chiama **AlertPisa** il sistema del **Comune di Pisa** che permette di ricevere **messaggi di avviso sulle emergenze** che possono verificarsi nel territorio del Comune di Pisa. Ogni cittadino può iscriversi e ricevere informazioni immediate sul proprio *device*.

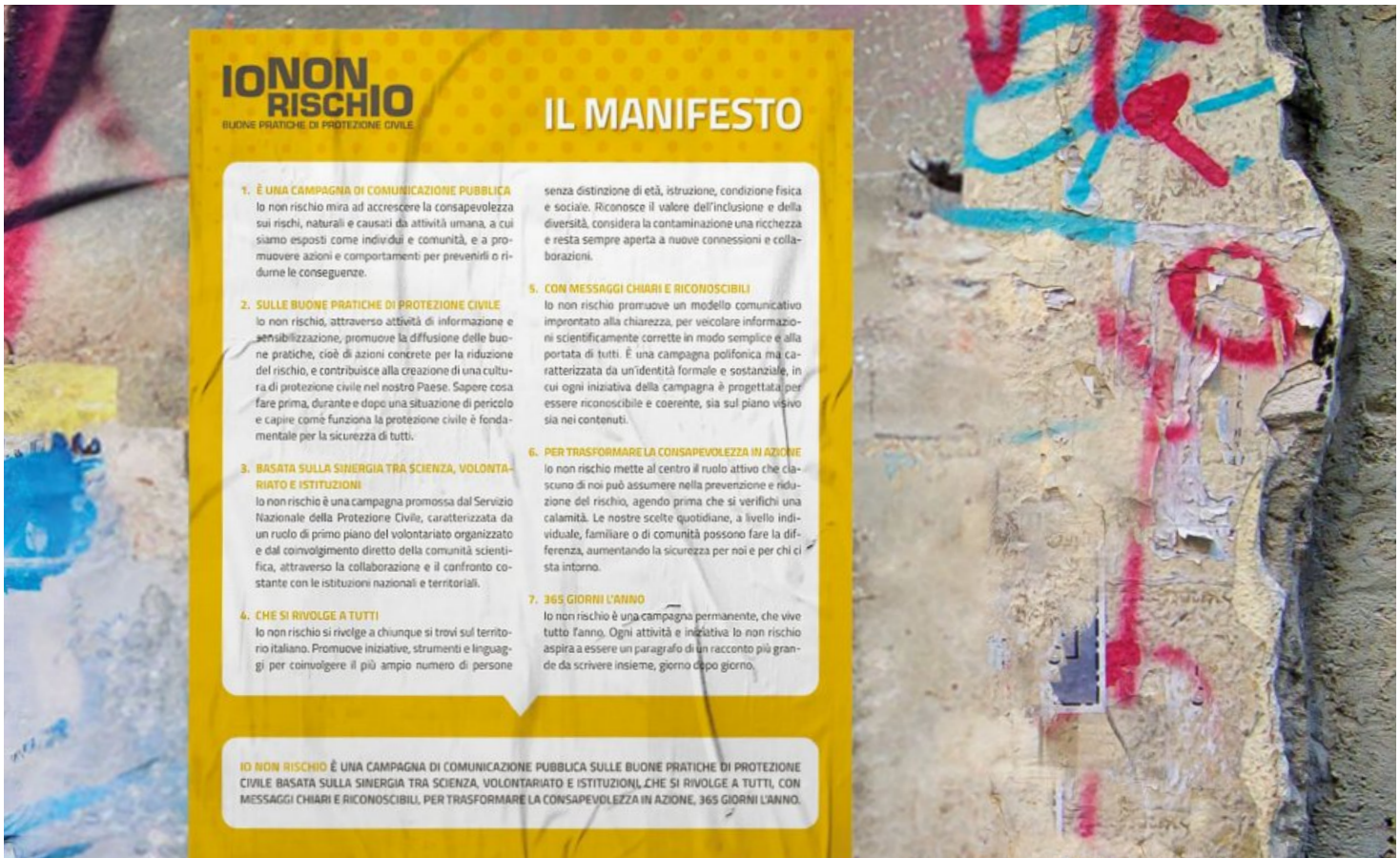
Negli ultimi anni stiamo assistendo al progressivo aumento di eventi meteorologici che un tempo potevano essere definiti straordinari per intensità e frequenza. Ci stiamo abituando alla diramazione di allerte meteo dal giallo all'arancione, per vento, mareggiate, pioggia e temporali, rischio idrogeologico. Se da un lato ci si interroga sulle politiche da introdurre per contrastare il cambiamento climatico, dall'altro chi ha la responsabilità di governare i territori deve mettere in campo un sistema efficiente in grado di intervenire in caso di bisogno. Perché le emergenze, non solo quelle legate al maltempo, possono verificarsi ovunque e in qualsiasi momento. Lo sanno bene i sindaci, che hanno grandi responsabilità in materia e che, coordinando il lavoro della **Protezione Civile comunale**, sono in prima linea per garantire incolumità e sicurezza alla popolazione, non soltanto nel corso di possibili emergenze ma anche quando il lavoro è meno visibile, nella fondamentale opera di prevenzione dei pericoli.

Di fronte a un evento inatteso, bisogna sapere cosa fare e quando, e questo richiede che ogni cittadino sia informato costantemente sulle varie fasi dell'emergenza: il Comune di Pisa ha lanciato sui suoi social una campagna per promuovere l'iscrizione dei cittadini al sistema di allertamento "AlertPisa", che permette di ricevere avvisi relativi alle allerte meteo ed emergenze che interessano il territorio comunale. Possono registrarsi tutti i residenti e domiciliati a Pisa o che hanno comunque un interesse a essere informati su criticità che possono verificarsi nel territorio comunale. La registrazione è gratuita e consente di scegliere se ricevere comunicazioni tramite sms ed email (sono obbligatori), notifiche su app, chiamata su linea fissa e linea cellulare. Attualmente sono 5.800 i cittadini iscritti al servizio AlertPisa.

Alla pagina **www.comune.pisa.italertpisa** il link per procedere alla registrazione al sistema di allertamento.

Sempre sul fronte della comunicazione, ogni anno, solitamente a inizio autunno, anche a Pisa si svolge "**Io non rischio**", la campagna di comunicazione pubblica sulle buone pratiche di protezione civile basata sulla sinergia tra scienza, volontariato e istituzioni, che si rivolge a tutti, con messaggi chiari e riconoscibili, per trasformare la consapevolezza in azione, 365 giorni l'anno. "Io non rischio" è promossa dal Dipartimento della Protezione Civile con Anpas (Associazione Nazionale Pubbliche Assistenze), Ingv (Istituto Nazionale di Geofisica e Vulcanologia), Reluis (Rete dei Laboratori Universitari di Ingegneria Sismica), Fondazione Cima (Centro Internazionale in Monitoraggio Ambientale), Conferenza delle Regioni e delle Province autonome e ANCI, Associazione Nazionale Comuni Italiani.

"**AlertPisa**" is the name of the system implemented by the Municipality of Pisa which allows citizens to receive warning messages for emergencies that may develop in the city and its environs. Each citizen can register to receive information in real time on his or her device.
When an unexpected event occurs, we need to know what to do and when. This requires constantly informing all citizens as to the various phases of the emergency. The Municipality of Pisa has launched a campaign on its social networks to encourage registration on the AlertPisa system so that citizens are able to receive warnings about weather alerts or emergencies that regard the city and surrounding areas. Both Pisa residents and others who wish to be informed about these types of events may register. Registration is free of charge; it allows participants to choose whether they wish to receive communication via text message and email (these are obligatory), via app, or via a call to a landline or mobile phone. At present, 5,800 citizens are registered on AlertPisa. Persons can register on the warning system by accessing the link www.comune.pisa.it/alertpisa.
Pisa also participates in the ***Io non rischio*** ("I don't take risks") initiative, which usually takes place at the beginning of autumn each year. This is a public communication campaign regarding good civil protection practices based on synergies between science, volunteer work and state agencies. The campaign is directed at everyone, using clear, recognisable messages to transform awareness into action, 365 days a year.
Io non rischio is promoted by the Department of Civil Protection as well as by the Conference of Regions and Autonomous Provinces and the National Association of Italian Municipalities (ANCI), among others.



DA 130 ANNI INSIEME

CRV
DA 130 ANNI INSIEME

CASSA DI RISPARMIO
DI VOLTERRA

www.crvolterra.it

www.exlmagazine.it – eXL social