La sicurezza dei dati e delle informazioni nell'era del GDPR, dei Big Data e dell'intelligenza artificiale

Ing. Enrico Venuto
venuto@polito.it

POLITECNICO DI TORINO

Privacy

675/1996

Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali

196/2003

Codice per la Protezione dei Dati Personali

(UE) 679/2016

Regolamento Generale sulla protezione dei dati

(General Data Protection Regulation – GDPR)

POLITECNICO DI TORINO

La sicurezza ai tempi della privacy

Nel 2004 la compliance era facile: c'era un disciplinare

Allegato B – Disciplinare tecnico in materia di misure minime

- Password personali segrete di almeno 8 caratteri cambiate almeno 2 volte all'anno
- Ogni 6 mesi disattivare le utenze non più attive
- Verifica annuale delle autorizzazioni
- Aggiornamento dei sistemi di sicurezza e patch dei programmi almeno 2 volte all'anno
- Backup almeno una volta a settimana
- DPS
- Cifratura dati sensibili e giudiziari

POLITECNICO DI TORINO

La sicurezza ai tempi del GDPR

Sicurezza e valutazione dei rischi

La valutazione dei rischi e l’adozione di misure di sicurezza è rimessa, caso per caso, al Titolare e al Responsabile in rapporto ai rischi specificamente individuati.

POLITECNICO DI TORINO

Misure minime per la sicurezza ICT delle PA

- AgID ha predisposto un documento che contiene l'elenco ufficiale delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" fornire alle pubbliche amministrazioni un riferimento pratico per valutare e migliorare il proprio livello di sicurezza informatica.

- Le Misure, che si articolano sull'attuazione di controlli di natura tecnologica, organizzativa e procedurale, prevedono tre livelli di attuazione (minimo M, Standard S e Alto A). Prende le mosse dall'insieme di controlli noto come SANS 20, oggi pubblicato dal Center for Internet Security come CCSC «CIS Critical Security Controls for Effective Cyber Defense» nella versione 6.0 di ottobre 2015

- L'obiettivo del documento è quello di fornire tempestivamente alle PA un riferimento normativo e consentire loro di intraprendere un percorso di progressiva verifica e adeguamento in termini di sicurezza informatica.

POLITECNICO DI TORINO

Misure minime per la sicurezza ICT delle PA

Modulo di implementazione

- Inventario dei dispositivi autorizzati e non
- Inventario dei software autorizzati e no autorizzati
- Proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstatione e server
- Valutazione e correzione continua delle vulnerabilità
- Uso approriato dei privilegi di amministratore
- Difese contro i malaware
- Copie di sicurezza
- Protezione dei dati

POLITECNICO DI TORINO

Modulo di implementazione del Politecnico di Torino

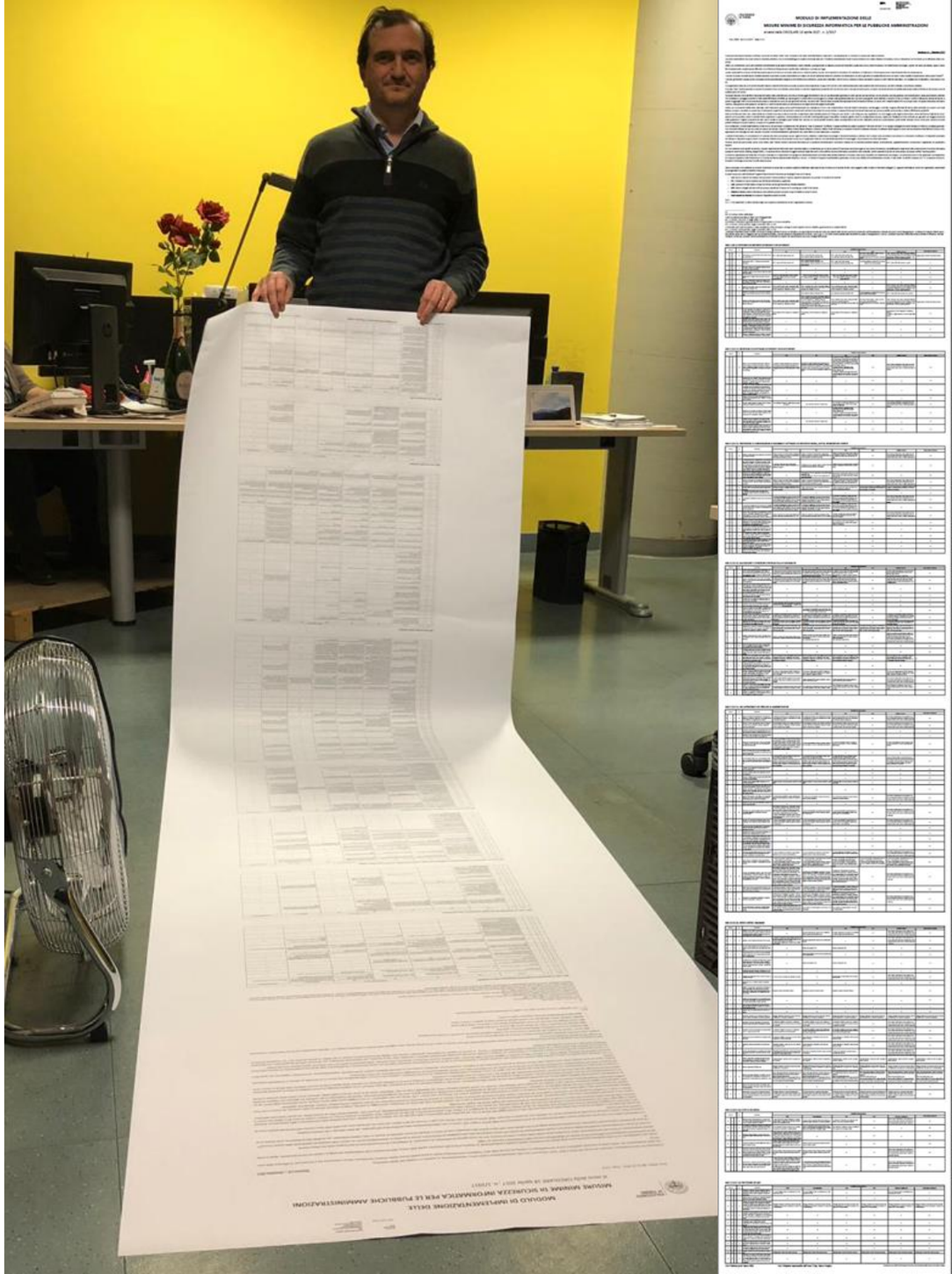
4 metri quadri

di testo corpo 13

di elenco di misure

organizzate

per perimetri e per ambiti



POLITECNICO DI TORINO

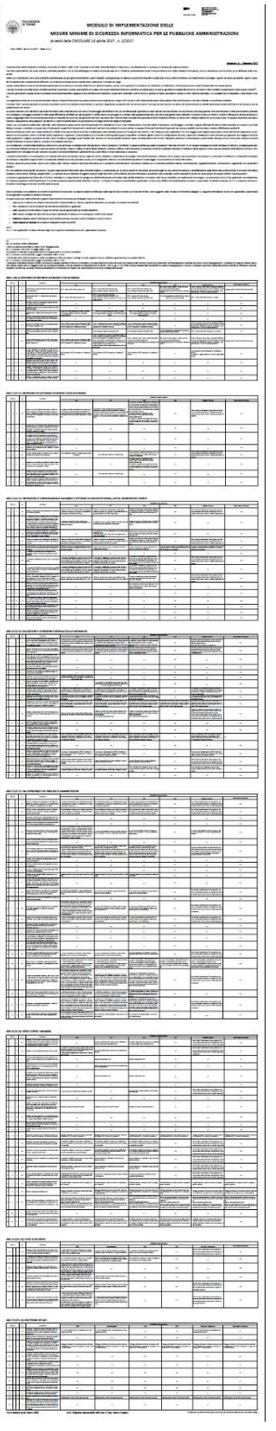
Norme Minime per la sicurezza ICT delle PA

Modulo di implementazione del Politecnico di Torino

Il termine "Rete" sembra associato al concetto di perimetro sicuro che delimita cosa sta dentro e cosa fuori.

… ma qualcosa è cambiato!

Negli atenei pressoché tutti i servizi sono web e l'accesso ad essi è aperto, nel senso che tali servizi sono accessibili nella stessa maniera dall'interno del campus come da qualsiasi parte del mondo.
Gli utenti svolgono la loro attività anche dall'estero, ed hanno necessità di operare su tutti i sistemi universitari, con qualsiasi tipo di dispositivo, anche di loro proprietà, come fossero in sede.



POLITECNICO DI TORINO

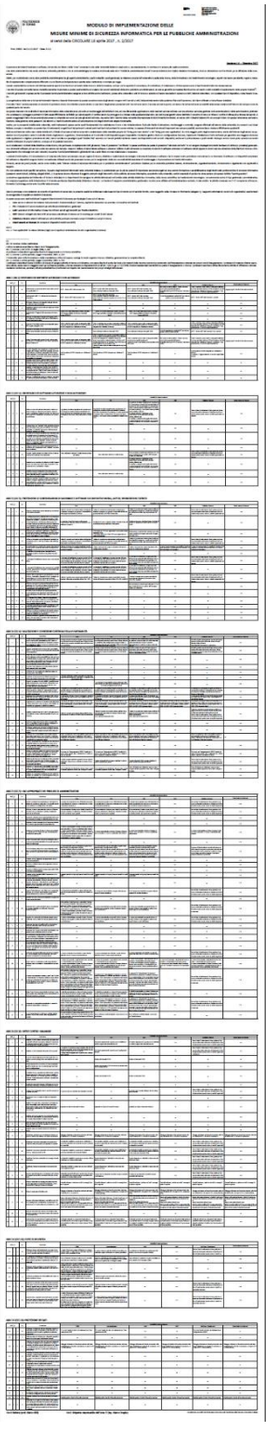
Norme Minime per la sicurezza ICT delle PA

Modulo di implementazione del Politecnico di Torino

Il termine "Rete" sembra associato al concetto di perimetro sicuro che delimita cosa sta dentro e cosa fuori.

… ma qualcosa è cambiato!

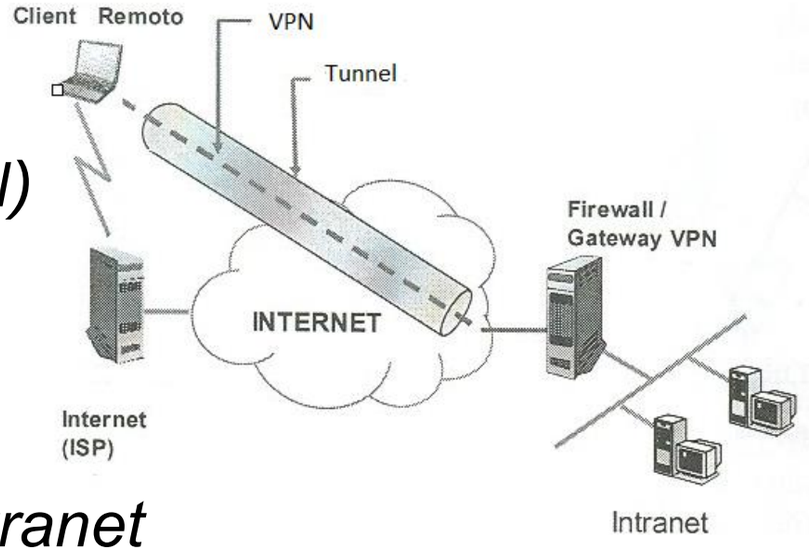
Molti trattamenti, spesso quelli fondamentali, che richiederebbero il più alto livello di attenzione, monitoraggio e controllo, vengono effettuati all'esterno, da consorzi o sul Cloud italiano, europeo o mondiale: su questo tipo di trattamenti, erogati fuori dai perimetri a utenti anch'essi fuori dai perimetri le norme minime, in assenza di interventi strutturali importanti non sempre possibili, sembrerebbero risultare difficilmente applicabili.



Dove è il nemico?

Fuori dall'azienda – Difesa del perimetro (firewall)

Fuori dell'azienda e dei suoi partner (VPN)



Dentro l'azienda: protezione dell'intranet

Dappertutto: protezione delle applicazioni, dei dati, dei dispositivi

POLITECNICO DI TORINO

Zero Trust Security

Zero trust security è un modello di sicurezza informatica che richiede una verifica sicura dell'identificazione per ogni persona e dispositivo che tenta di accedere ad una rete privata, indipendentemente da dove si trovi, dentro o fuori che sia del perimetro della rete. E' un approccio olistico alla network security che utilizza diversi principi e tecnologie.

La IT network security tradizionale è basata sul concetto di dentro o fuori del perimetro sicuro. In questo scenario è molto difficile ottenere l'accesso da fuori della rete sicura, ma una volta dentro, chiunque è considerate "amico" (anche un hacker) ed ha pieno accesso a tutta la rete.

POLITECNICO DI TORINO

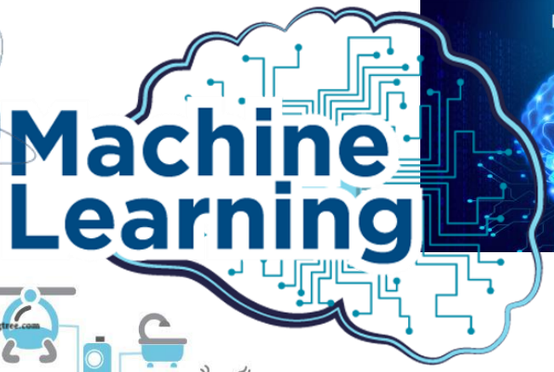
Sicurezza

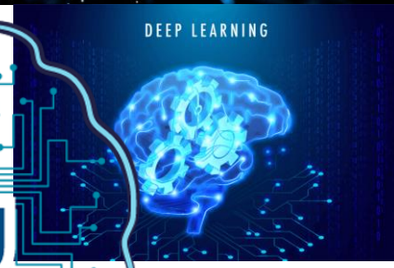
La sicurezza della rete, dei servizi e dei dati/documenti non dipende più solo dalle proprie infrastrutture interne aziendali.

Va considerato che ci si trova in un mondo ed in un mercato interconnesso

E’ primariamente un fatto culturale e richiede un approccio nuovo e multidimensionale

Big Data
+ Analytics
= Smart Data



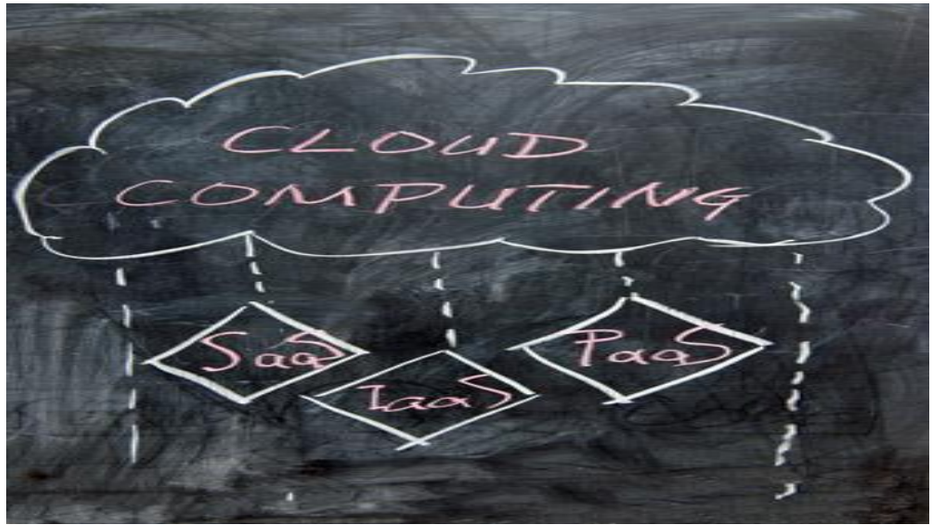


INDUSTRY 4.0

IGF Internet Governance Forum

POLITECNICO DI TORINO

XaaS
La nuova era del Cloud



Infrastructure as a Service – BUILD
Platform as a Service – DEPLOY
Software as a Service – BUY & USE

XaaS – Anything as a Service

Service	Abbr.
Analytics as a service	AnaaS
API as a service	AaaS
Artificial intelligence as a service	AIaaS
Backend as a service	BaaS
Banking as a service	BaaS
Blockchain as a service	BaaS
Business process as a service	BPaaS
Contact information as a service	CIaaS
Containers as a service	CaaS
Construction as a service	CaaS
Container as a service	CaaS
Crane as a service	CaaS
Communications as a Service	CPaaS
Data as a service	DaaS
Desktop as a service	DaaS
Drone as a service	DaaS
Database as a service	DBaaS
Distribution as a service	DaaS
Energy storage as a service	ESaaS
Electric vehicle as a service R	EVaaS
Function as a service	FaaS
Farming as a service	FaaS
Games as a service	GaaS
Hadoop as a service	HaaS
Housing as a service	HaaS
Infrastructure as a service	IaaS
Identity as a service	IDaaS
IT as a service	ITaaS
Logging as a service	LaaS
Management as a service	MaaS
Microgrid as a service	MaaS
Mobility as a service	MaaS
Monitoring as a service	MaaS
Metal as a service	MaaS
Mobile backend as a service	MBaaS
Machine Learning as a service	MLaaS
Network as a service	NaaS
Network Defense as a service	NDaaS
Payments as a service	PaaS
Platform as a service	PaaS
Push notification as a service	PaaS
Recovery as a service	RaaS
Roboras a service	RaaS
Search as a service	SaaS
Security as a service	SaaS
Software as a service	SaaS
Storage as a service	SaaS
Transportation as a service	TaaS
Testing as a service	TaaS
Unified Communications as a Service	UCaaS

XaaS
Cloud Computing

Analytics, API, Artificial intelligence, Backend, Banking, Blockchain, Business process, Contact Information, Content as a service, Construction, Container, Crane, Communications, Data, Desktop, Drone, Database, Distribution, Energy storage, Electric vehicle, Function, Farming, Games, Hadoop, Housing, Infrastructure, Identity, IT, Logging, Management, Microgrid, Mobility, Monitoring, Metal, Mobile backend, Machine Learning, Network, Network Defense, Payments, Platform, Push notification, Recovery, Robot, Search, Security, Software, Storage, Transportation, Testing, Unified Communications

…human as a service??

POLITECNICO DI TORINO

CLOUD Act

Clarifyng Lawfull Overseas Use of Data Act (USA 23/3/18)

Una legge federale che permette, tra l'altro, alle autorità giudiziarie statunitensi di ottenere dai fornitori di servizi cloud di diritto USA dati e informazioni sensibili, anche quando sono depositati fuori dal perimetro statunitense.

Il Cloud act, come ha notato anche il Garante europeo per la privacy, rema in direzione opposta, consentendo (anzi, incentivando) le multinazionali del settore a prelevare informazioni a prescindere dalla collocazione geografica dei server o degli utenti interessati.

POLITECNICO DI TORINO

Gaia-X:

Un progetto di Cloud Europeo pensato da Berlino per la sovranità sui dati - 29/10/2019

"L'economia europea ha urgente bisogno di sovranità su dati"

[Peter Altmaier - ministro dell'Economia tedesco]

European data infrastructure as an alternative to services of American Internet giants.

The Gaia-X cloud network is intended to pave the way for European business models to digital business models and also to help combat diseases such as cancer by means of data analysis.

To implement the data infrastructure is "a central, European-supported organization" is necessary.

POLITECNICO DI TORINO

Big Data, Smart Data, AI

- Big Data: Enormi moli di dati strutturati e destrutturati, eterogenei, provenienti da varie fonti, non più analizzabili e gestibili con gli strumenti tradizionali (relazionali)
- Big Data Analytics: l'analisi di grandi moli di dati permette di individuare informazioni «nascoste» e di generare conoscenza
- L'intelligenza artificiale si nutre di dati; i dati servono ad «addestrare» i modelli; i dati hanno un valore inestimabile

Nuovi mestieri

- Data Scientist
- Data Engineer
- Data Analyst
- Chief Data Officer
- Data Steward
- …
- Demiurgo dei Big Data

GOOGLE...

SA TUTTO!

https://www.youtube.com/watch?v=LIfgbkrrCrU

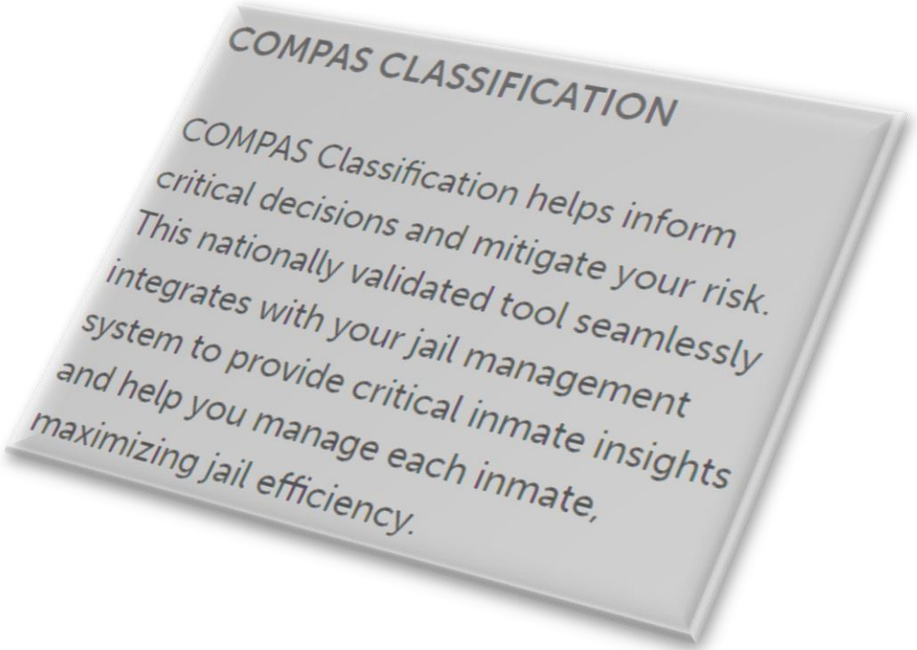
Big Data, Smart Data, AI

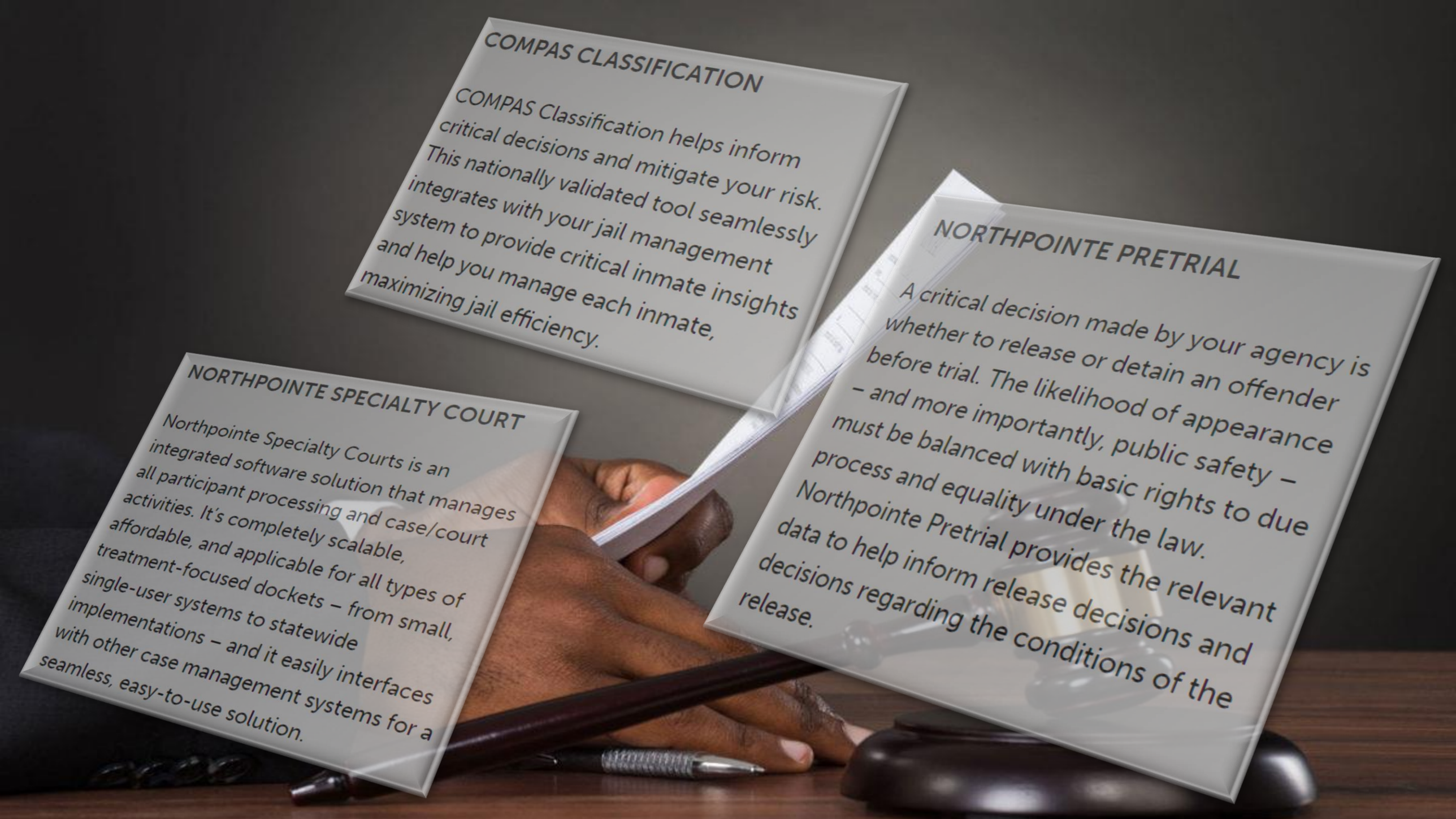
Predictive justice

Le pene negli Stati Uniti incominciano a basarsi su previsioni elaborate da sistemi AI.

Dopo il suo arresto nel 2013, Eric Loomis è stato condannato a sei anni di prigione in base a una previsione algoritmica opaca (Compas) secondo cui avrebbe commesso più crimini.

I modelli di apprendimento automatico sono affidabili tanto quanto i dati su cui vengono formati. Se i dati sottostanti sono distorti in qualsiasi forma, esiste il rischio che le disuguaglianze strutturali e i pregiudizi non vengano semplicemente replicati, ma amplificati.




COMPAS CLASSIFICATION
COMPAS Classification helps inform critical decisions and mitigate your risk. This nationally validated tool seamlessly integrates with your jail management system to provide critical inmate insights and help you manage each inmate, maximizing jail efficiency.
NORTHPOINTE SPECIALTY COURT
Northpointe Specialty Courts is an integrated software solution that manages all participant processing and case/court activities. It's completely scalable, affordable, and applicable for all types of treatment-focused dockets – from small, single-user systems to statewide implementations – and it easily interfaces with other case management systems for a seamless, easy-to-use solution.
NORTHPOINTE PRETRIAL
A critical decision made by your agency is whether to release or detain an offender before trial. The likelihood of appearance – and more importantly, public safety – must be balanced with basic rights to due process and equality under the law. Northpointe Pretrial provides the relevant data to help inform release decisions and decisions regarding the conditions of the release.

POLITECNICO DI TORINO

Big Data, Smart Data, AI

Il Sistema di Credito Sociale (社会信用体系)

è un'iniziativa creata dal governo cinese al fine di sviluppare un sistema nazionale per classificare la reputazione dei propri cittadini. Sarà utilizzato per assegnare ad ogni cittadino un punteggio rappresentante il suo "credito sociale", sulla base di informazioni possedute dal governo, riguardanti la condizione economica e sociale. Funzionerà come un sistema di sorveglianza di massa e sarà basato su tecnologie per l'analisi di Big Data. Inoltre, avrà la funzione di attribuire un punteggio alle imprese che operano nel mercato cinese e quindi di classificarle.

European Parliament

Need for ethical principles concerning the development of robotics and artificial intelligence for civil use

C'è più dell'Art.22

"*warns that […] maximum caution is required in order to prevent unlawful discrimination and the targeting of certain individuals or groups of people defined by reference to race, colour, ethnic or social origin, genetic features, language, gender expression or identity, sexual orientation, residence status, health or membership of a national minority which is often the subject of ethnic profiling or more intense law enforcement policing, as well as individuals who happen to be defined by particular characteristics*". [2017]

Il Codice Etico dell'Unione Europea

Linee guida su utilizzo e sviluppo di sistemi di Intelligenza Artificiale
Aprile 2019

Predisposto da un gruppo di 52 esperti (informatici, ingegneri, giuristi, filosofi, industriali, matematici).

l'Intelligenza Artificiale deve avere l'uomo al centro e deve essere al servizio del bene comune per migliorare il benessere e garantire la libertà.

- Rispetto per la dignità dell'uomo
- Libertà dell'individuo
- Rispetto per la democrazia e per la giustizia
- Eguaglianza e non discriminazione
- Diritti dei cittadini

Il Codice Etico dell'Unione Europea

Linee guida su utilizzo e sviluppo di sistemi di Intelligenza Artificiale
Aprile 2019

LINEE GUIDA

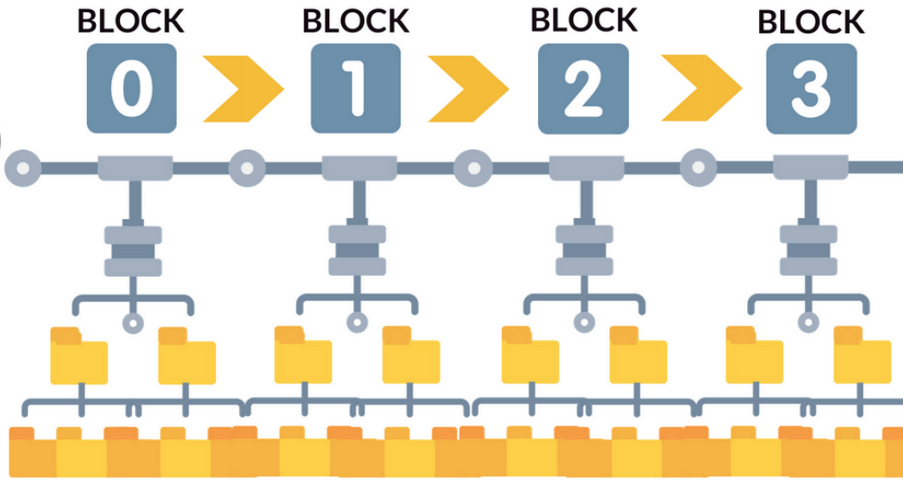
- Supervisione umana
- Solidità tecnica e Sicurezza
- Privacy e Governance dei dati
- Trasparenza
- Diversità, assenza di discriminazione, correttezza
- Benessere sociale e ambientale
- Responsabilità

Blockchain

"A blockchain is a chronologically sorted, distributed, digital ledger which contains an irreversible archive of transaction records that are stored and chained together in batches called blocks".

Fu ideata nel 2008 da Satoshi Nakamoto (pseudonimo) per realizzare il libro mastro (Ledger) della Cryptomoneta Bitcoin.

Consente alle persone di conservare, ritrovare e spendere crypomonete ovunque nel mondo superando tutte le frontiere e senza avere la necessità dell'intermediazione di nessuna terza parte (peer-to-peer).



AccruBit Academy

POLITECNICO DI TORINO

Blockchain

La Blockchain (Nakamoto Consensus) è un algoritmo distribuito che consente di mantenere sincronizzati grandi quantità di nodi (senza aver grandi informazioni sulla loro potenza di calcolo, rete, tempi di poropagazione, entrata nella rete o loro abbandono).

La sua natura peer-to peer è la forza del sistema, ma anche un suo problema.

Poiché ogni partecipante mantiene un copia completa e funzionale della blockchain, ogni volta che viene aggiunto un dato, questo deve venire aggiunto sugli hard disk di ogni partecipante alla rete.

POLITECNICO DI TORINO

Se ci sono 1000 dipendenti ognuno dei quali condivide 1 imagine di 2 MB al giorno per un intero anno, allora ognuno di loro avrà sulla sua macchina una blockchain che occupa 730 GB di storage, per un totale complessivo nell'azienda di 730 TB.
Non va però considerate la sola questione della quantità di storage necessario, ma anche il collo di bottiglia sulla rete per tenere allineati in tempo reale 24/7 tutti quei dati su tutti quei computer.

Le blockchains non sono adatte per conservare e trasferire dati "voluminosi", anche se la cosa non è impossibile.

POLITECNICO DI TORINO

Blockchain

Blockchain permissionless (DLT Consortium - pubblica)

Non esiste nessun attore pre-selezionato che fa da validatore, ma chiunque nel sistema è un validatore.

Chiunque può entrarne a fare parte o a uscirne liberamente.

Il processo di consenso è controllato da un numero predefinito di nodi: almeno il 50%+1 deve confermare la validità di ogni blocco che viene processato.

Blockchain permissioned (DLT privata)

Esiste uno o più attori pre-selezionati che svolgono la funzione di validatore nel network

Il Processo di consenso, ovvero il permesso di scrivere i blocchi nella catena è centralizzato da una unica organizzazione, quindi solo 1 nodo crea il consenso.
Una piattaforma privata è essenzialmente un tradizionale database centralizzata con l'aggiunta della crittografia come strumento di sicurezza e verifica

POLITECNICO DI TORINO

Blockchain e Smart Contract

https://www.paradigma.it/2019/09/04/smart-contract-prime-riflessioni-del-notariato/

Il Decreto Semplificazioni (D.L. n. 135/2018 convertito dalla Legge n. 12/2019 definisce lo smart contract “Un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse”. Attribuendogli il valore della forma scritta “previa identificazione delle parti interessate”.

L’AGID ha il compito di preparare le linee guida sulle procedure di identificazione informatica delle parti, ma anche gli standard tecnici che le blockchain dovranno rispettare per produrre gli effetti giuridici della validazione temporale elettronica, in coerenza con la normativa europea e nazionale. Su linee guida e standard tecnici – che sarebbero dovuti arrivare entro metà maggio

Blockchain e Smart Contract

https://www.paradigma.it/2019/09/04/smart-contract-prime-riflessioni-del-notariato/

“Il legislatore pare pensare implicitamente alle blockchain permissionless, aperte, e in particolare a quelle più diffuse, come Ethereum. Perché quelle permissioned, centralizzate, prevedono il controllo di un’“autorità” o di una ristretta cerchia di soggetti”.

Nelle blockchain permissionless, a rendere difficili i cosiddetti “attacchi del 51%” (portati cioè con il consenso della maggioranza dei nodi) è proprio il livello di diffusione della catena dei nodi. Ma quanto dev’essere distribuito un registro affinché sia considerato affidabile? “È una delle tante domande a cui la norma non dà risposta”.

Blockchain e incompatibilità col GDPR

https://www.agendadigitale.eu/documenti/certificati-di-laurea-su-blockchain-e-gdpr-i-problemi-di-conformita-privacy/

L'inserimento da parte delle istituzioni universitarie dell'hash crittografico dei diploma di laurea (o del Diploma Supplement) in una rete blockchain ha l'obiettivo di creare una prova immutabile dell'integrità e dell'autenticità degli attestati conservati fuori catena, consentendone la verifica e la portabilità a livello globale e limitando i rischi di eventuali frodi o manomissioni illecite.

L'inclusione di dati personali in forma cifrata e di hash in blockchain pubbliche, qualora effettuata da terze parti, comporta però una generale incompatibilità con le disposizioni del GDPR.

… e il diritto all'oblio?

“La blockchain non è affatto la prima tecnologia emergente ad essere etichettata come incompatibile con la privacy e gli altri principi giuridici fondamentali. Le applicazioni blockchain potrebbero essere dirompenti, ma ciò non significa che non possano essere progettate e implementate in modo conforme alla legge”.

Prof. Christopher Millard, Queen Mary University di Londra

Blockchain e incompatibilità col GDPR

https://www.agendadigitale.eu/documenti/certificati-di-laurea-su-blockchain-la-soluzione-diplome/

Diplome si appoggia a una rete blockchain permissioned fondandosi sul principio della sovranità del dato (self- sovereignty).

All'utente viene assegnato un wallet attraverso cui conservare e gestire direttamente le proprie qualifiche, senza ricorrere a intermediari fiduciari – quale ad esempio l'Università stessa.

Attualmente l'indirizzo pubblico del wallet non è associato a un'identità certificata dell'utente, di cui si dovrà dare prova separatamente al di fuori dell'ecosistema.

Il wallet, a cui è associata una coppia di chiavi, pubblica e privata, è strutturato in modo tale da poter contenere uno o più smart contract, che fungeranno da archivio per qualsiasi certificato di studio o qualifica professionale

Blockchain e incompatibilità col GDPR

https://www.corrierecomunicazioni.it/digital-economy/certificazioni-di-laurea-4-0-con-la-bockchain/

BlockChain Degree è un sistema per la certificazione su blockchain dei titoli conseguiti dagli studenti della Link Campus University, ed è basato su blockchain pubblica Ethereum e sullo standard Blockcerts sviluppato dal MIT Media Lab.

Al conseguimento della laurea, gli studenti ricevono un file contenente le informazioni relative al titolo di studio, all'ateneo e alla carriera universitaria che potrà essere verificato su un portale messo a disposizione dall'università, dallo studente o da qualsiasi entità con cui lo studente lo voglia condividere, per accertare la veridicità delle informazioni riportate.

L'adozione dello standard Blockcerts permette, inoltre, di provare l'autenticità di un documento certificato anche nei casi in cui il portale web per la verifica non sia disponibile.

“Not your keys, not your crypto”

https://hackernoon.com/tech-explained-top-24-blockchain-hacks-in-history-first-half-40c390dc4a96

- [Mt.Gox hack] In February 2014, the exchange revealed that a hacker had stolen approximately 850,000 BTC (~$473 million) from the platform. Affected users were left out cold.
- [51% attack] In 2018, several notable cryptocurrencies such as ZenCash, Verge, and Ethereum Classic fell victim to 51% attacks. Overall, attackers walked away with over $20 million last year due to this blockchain security issue.
- [Bitfinexex] In August 2016, was the second largest Bitcoin hack ever made after Mt.Gox. The breach claimed 120,000 BTCs (worth $72 million).

Last year, exchanges lost over $900 million to hackers.

La sicurezza dei dati e delle informazioni nell'era del GDPR, dei Big Data e dell'Intelligenza artificiale

THANK YOU

Ing. Enrico Venuto

venuto@polito.it