Associazione Italiana Information Systems Auditors

Cyber [In]Security = [De]Normazione

Collegio Universitario R. Einaudi
Torino, 25 maggio 2018
www.aiea.it

Carlo Muzzì
muzzi@acm.org
muzzi.org

Abstract: ***Cyber [In]Security = [De]Normazione***

« L'esistenza umana si svolge sempre più in un ecosistema digitale nel quale la cyber security riveste un ruolo sempre più significativo: per governarla è ormai improcrastinabile l'uso della leva normativa »

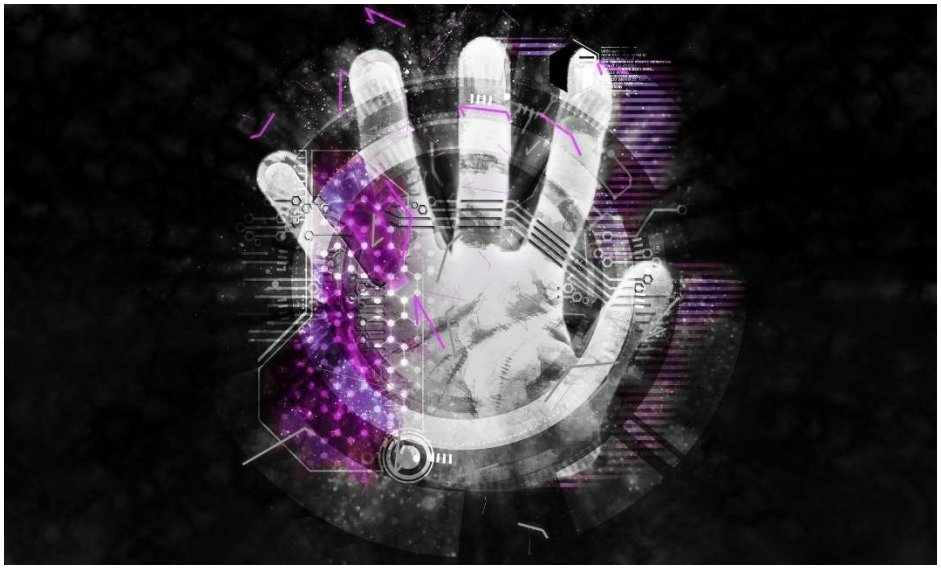
Cyber Security = Normazione

Cyber Insecurity = Denormazione

Il mondo in cui viviamo: l'era digitale

L'era digitale è il mondo in cui viviamo oggi.

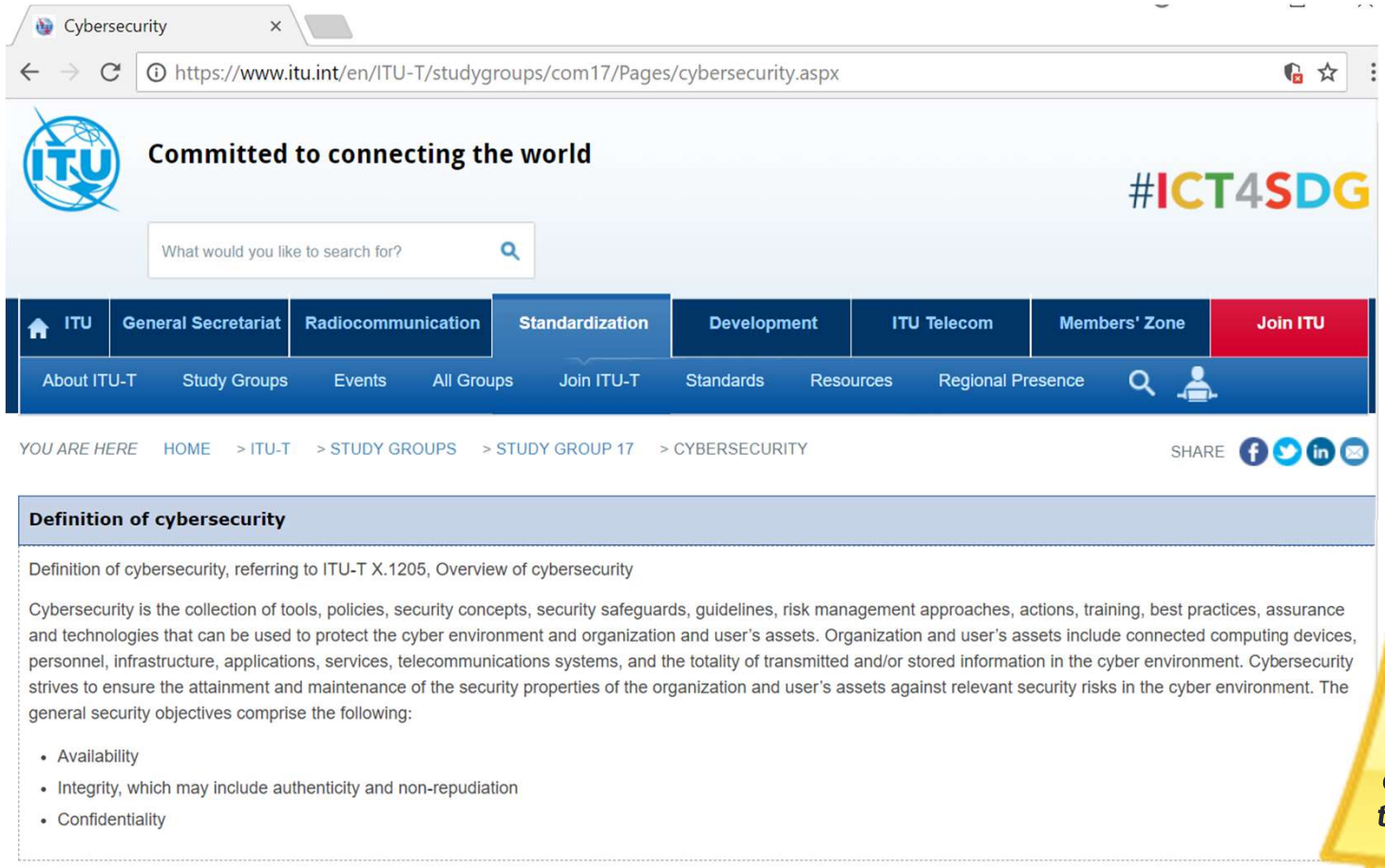
È il risultato della trasformazione della nostra realtà avvenuta grazie ad un repentino processo che, pur originatosi nel più circoscritto ambito scientifico e tecnologico, è giunto a pervadere ogni ambito della nostra esistenza.



«Siamo entrati nell'èra digitale. E l'èra digitale è entrata in noi. Non siamo piú gli stessi individui di un tempo. In meglio e in peggio».

[Ritchin, 2012]

Nell'era digitale la definizione di «Cyber Security» è ormai olisticamente incompleta



[ITU, 2018]

ITU is the United Nations specialized agency for information and communication technologies -ICTs.

ESTRATTO DA: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Cyber Insecurity and Cyber Libertarianism

COMMUNICATIONS OF THE ACM

HOME | CURRENT ISSUE | NEWS | BLOGS | OPINION | RESEARCH | PRA

Home / Magazine Archive / May 2017 (Vol. 60, No. 5) / Cyber Insecurity and Cyber Libertarianism / Full Text

DEPARTMENTS

Cyber Insecurity and Cyber Libertarianism

By Moshe Y. Vardi
Communications of the ACM, Vol. 60 No. 5, Page 5
10.1145/3073731
Comments (2)

VIEW AS: SHARE:

One can get a good picture of what is "hot" in technology by attending a Tech Summit. Such events are now held regularly in places trying to compete with Silicon Valley. I attended such a summit a few weeks ago. So what's hot? FinTech (financial technology), MedTech (medical technology), IoT (Internet of Things), and autonomous cars are all hot. These areas attract a high level of venture capital, and one can expect them to grow and reshape the financial, medical, and transportation industries. Underlying these technologies is, of course, the Internet—our "network of insecurity"—so we can expect cyber insecurity to spread across more and more aspects of our lives.

Cyber insecurity seems to be the normal state of affairs these days. In June 2015, the U.S. Office of Personnel Management announced it had been the target of a data breach targeting the records of as many as 18 million people. In late 2016, we learned about two data breaches at Yahoo! Inc., which compromised over one billion accounts. Lastly, during 2016, close to 20,000 email messages from the U.S. Democratic National Committee were

«… Cyber insecurity seems to be the normal state of affairs these days…

… Cyber libertarianism refers to the belief that individuals should be at liberty to pursue their own tastes and interests online. Cyber libertarianism is a common attitude in the tech community; "regulation stifles innovation" is the prevailing mantra…

… I believe, that the cybersecurity problem will not be resolved by the market. »

[Vardi, 2017]

ESTRATTO DA: https://cacm.acm.org/magazines/2017/5/216316-cyber-insecurity-and-cyber-libertarianism/fulltext

Cyber Insecurity and Cyber Libertarianism: Why is there no National Cyber Security Board ?

«… We can draw an analogy to car safety. Over the past 100 years, the amount of vehicle miles traveled has been steadily increasing, but fatalities with respect to vehicle miles traveled have been decreasing. Car safety has been increasing mostly due to government regulation. For example, the U.S. Congress established the National Transportation Safety Board in 1926. ***Why is there no National Cyber Security Board?*** *… »*

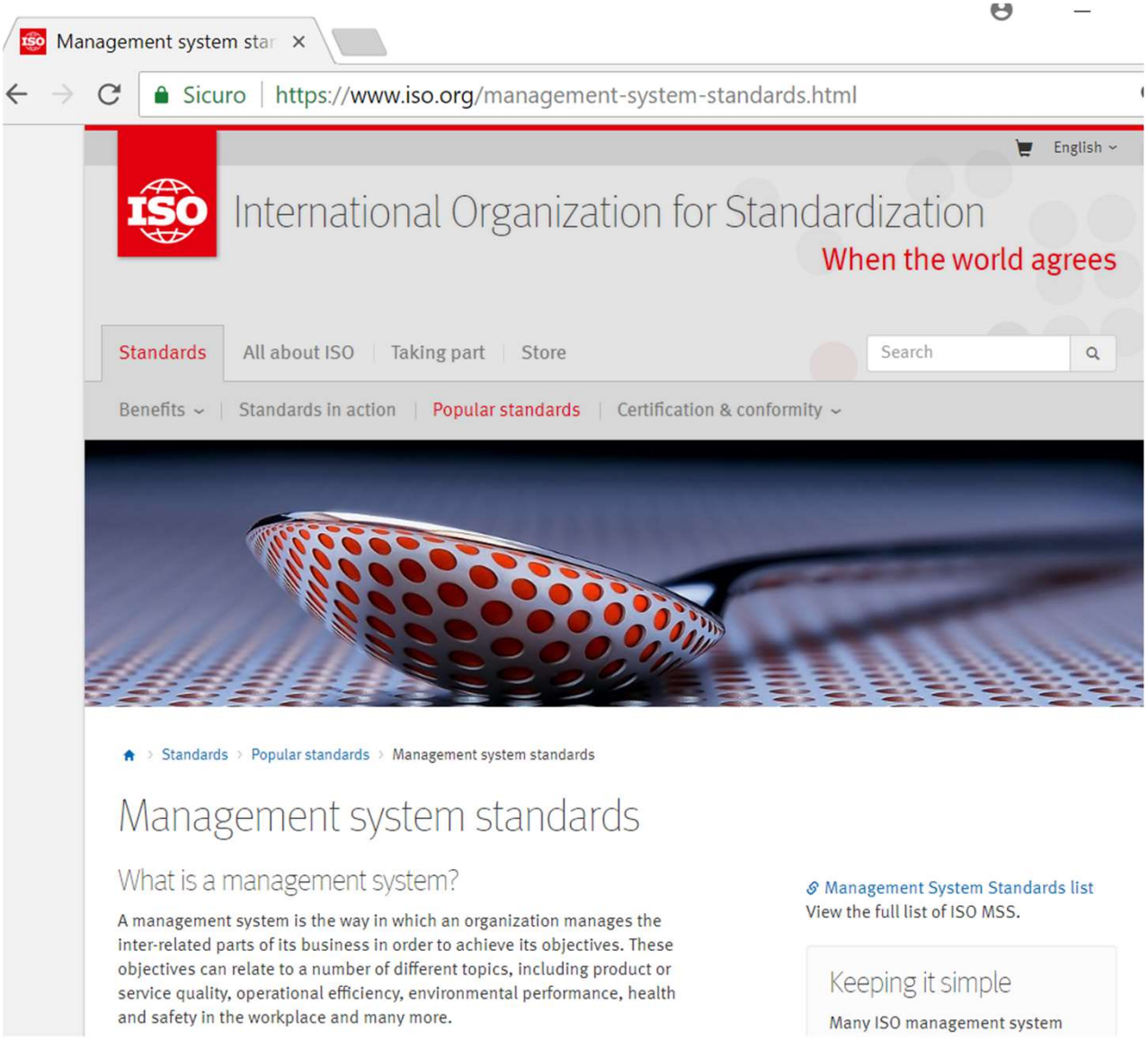
[Vardi, 2017]

ESTRATTO DA: https://cacm.acm.org/magazines/2017/5/216316-cyber-insecurity-and-cyber-libertarianism/fulltext

Fonti normative

Ma se l'assunto è «Cyber Security = Normazione», quali possono essere le fonti da cui può discenere una normazione?

La normazione dai “Sistemi di Gestione”



«Un sistema di gestione è il modo in cui un'organizzazione gestisce le parti correlate della propria attività al fine di raggiungere i propri obiettivi.».

[ISO, 2018]

ESTRATTO DA: https://www.iso.org/management-system-standards.html

ISO Management System Standards

Information Technology

Reference	Title
ISO/IEC 20000-2	Information technology -- Service management -- Part 2: Guidance on the application of service management systems
ISO/IEC 27003:2017	Information technology -- Security techniques -- Information security management systems -- Guidance
ISO/IEC 27552	Information technology -- Security techniques -- Enhancement to ISO/IEC 27001 for privacy management -- Requirements
ISO/IEC 20000-1	Information technology -- Service management -- Part 1: Service management system requirements
ISO/IEC 27001:2013	Information technology -- Security techniques -- Information security management systems -- Requirements
ISO/IEC 27010:2015	Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications
ISO/IEC 27013:2015	Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
ISO/IEC 90003:2014	Software engineering -- Guidelines for the application of ISO 9001:2008 to computer software
ISO/IEC DIS 19770-1	Information technology -- IT asset management -- Part 1: IT asset management systems -- Requirements

La **Cyber security**, pur potendo rientrare tra i temi trattati in diversi sistemi di gestione, assume indubbiamente un ruolo significativo all'interno delle norme di **Information Technology** della serie **27000.**

[ISO, 2018] ESTRATTO DA: https://www.iso.org/management-system-standards-list.html

In Italia: UNI CEI EN ISO/IEC 27001:2017

ENTE ITALIANO DI NORMAZIONE

Home | Chi siamo | Associazione | Normazione |

Home > Catalogo > Catalogo Norme > **UNI CEI EN ISO/IEC 27001:2017**

Norma numero : UNI CEI EN ISO/IEC 27001:2017
Titolo : Tecnologie Informatiche – Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione - Requisiti
ICS : [03.100.70] [35.030]
Stato : IN VIGORE
Commissioni Tecniche : [UNINFO Sicurezza Security] [UNINFO F12 - Sistemi di elaborazione delle informazioni]
Data entrata in vigore : 30 marzo 2017
Data ritiro :
Sommario : La norma specifica i requisiti per stabilire, attuare, mantenere e migliorare continuamente un sistema di gestione della sicurezza delle informazioni nel contesto dell'organizzazione. Inoltre essa include i requisiti per la valutazione e il trattamento dei rischi per la sicurezza dell'informazione adatti alle esigenze dell'organizzazione. I requisiti presenti nella norma sono generici e destinati ad essere applicati a tutte le organizzazioni, indipendentemente dal tipo, dalla dimensione o dalla loro natura.

Valida per «… **tutte le organizzazioni**…»

[UNI, 2018] ESTRATTO DA: http://store.uni.com/catalogo/index.php/uni-cei-en-iso-iec-27001-2017.html

ISO/IEC 27001

ISO/IEC 27001

Sistema di Gestione per la Sicurezza delle Informazioni (SGSI o ISMS).

- Applicabile a realtà di ogni dimensione
- Quasi 20 anni di esistenza sul mercato
- Ambito definibile a piacimento
- Approccio ciclico (PDCA)
- Costituisce un framework completo
- Dice cosa fare, non come farlo
- Rivolto al miglioramento continuo
- E' un riferimento universale e certificabile

UNINFO

[Guasconi, 2015]

Aziende certificate 27001 in Italia

Nonostante sia potenzialmente applicabile a tutte le organizzazioni, solo **660** aziende sono ISO 27001 su un totale di 83.447 aziende certificate: lo **0,79%**

Aziende Certificateal 02-2018	UNI EN 9100	UNI CEI EN ISO 13485	UNI EN ISO 3834	UNI EN ISO 9001	UNI EN 9110	UNI EN 9120	UNI ISO 29990	UNI ISO 20121	ISO 39001	ISO 22301	ISO 55001	UNI ISO 37001	UNI EN ISO 14001	UNI CEI EN ISO 50001	BS OHSAS 18001	UNI CEI ISO/IEC 27001
83.447	429	1.730	1.502	78.437	23	54	53	18	95	12	5	42	10.951	870	5.619	660

[ACCREDIA, 2018] ESTRATTO DA:
https://services.accredia.it/ppsearch/accredia_stats_reserved_2.jsp?ID_LINK=1755&area=310

Aziende in Italia (anno 2015)

Imprese attive nell'anno 2015:

- imprese attive in Italia: 4.338.085
- addetti: 16.289.875

[ISTAT, 2017]

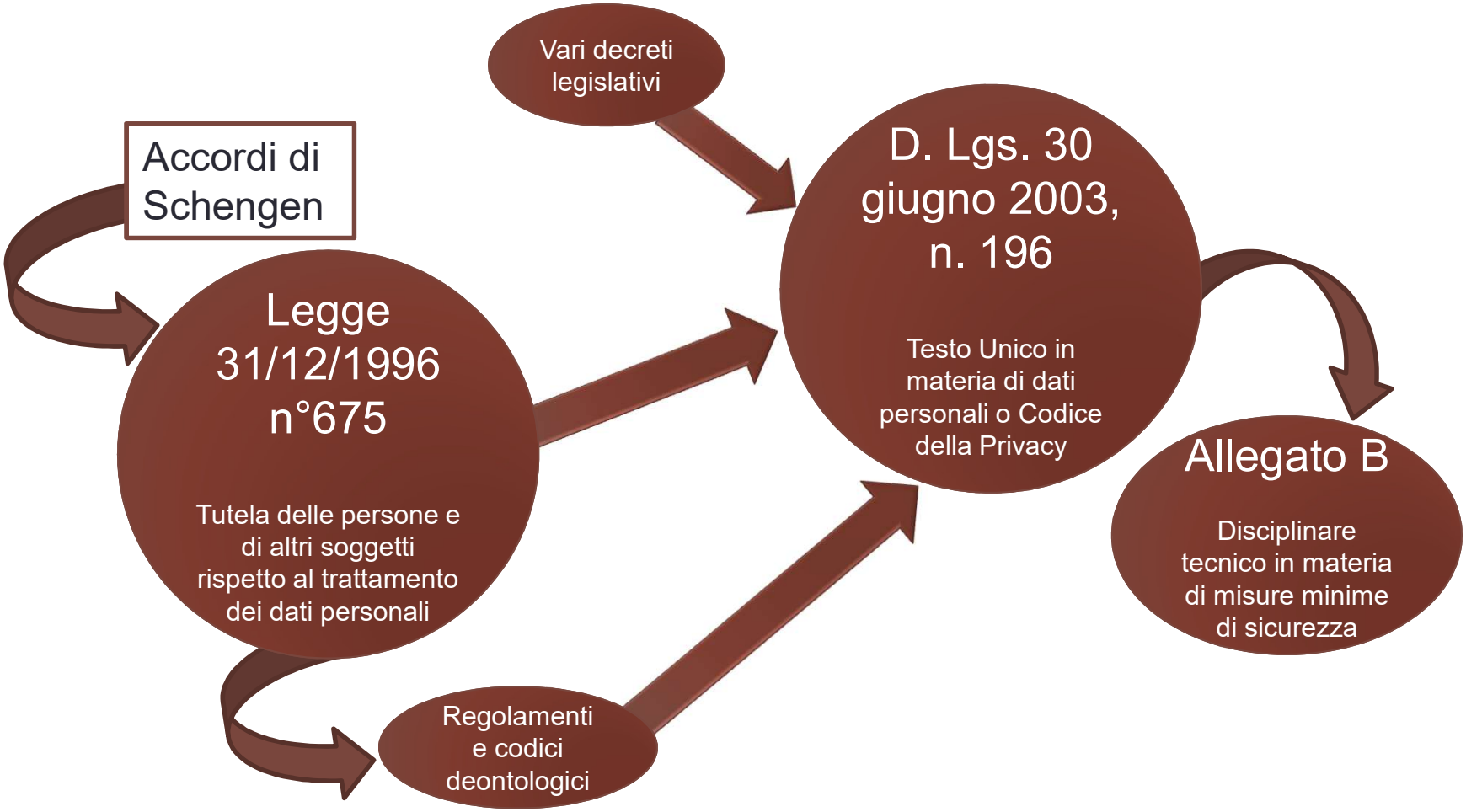
Alcune considerazioni

- Le % rappresentate in realtà sono ancora più basse per varie ragioni:
  - i soggetti certificati spesso hanno più di una certificazione
  - a certificarsi vi sono anche organizzazioni che non «propriamente» imprese.

- Il peso specifico delle certificazioni assume un valore usualmente più alto in quanto sono:
  - scelte individuali → maggiore motivazione
  - richieste dal mercato → ricadute diffuse

La normazione che proviene dalla “Privacy”

Nel panorama nazionale è indubbiamente la normazione più nota che ha spinto verso la Cyber Security di tipo aziendale.



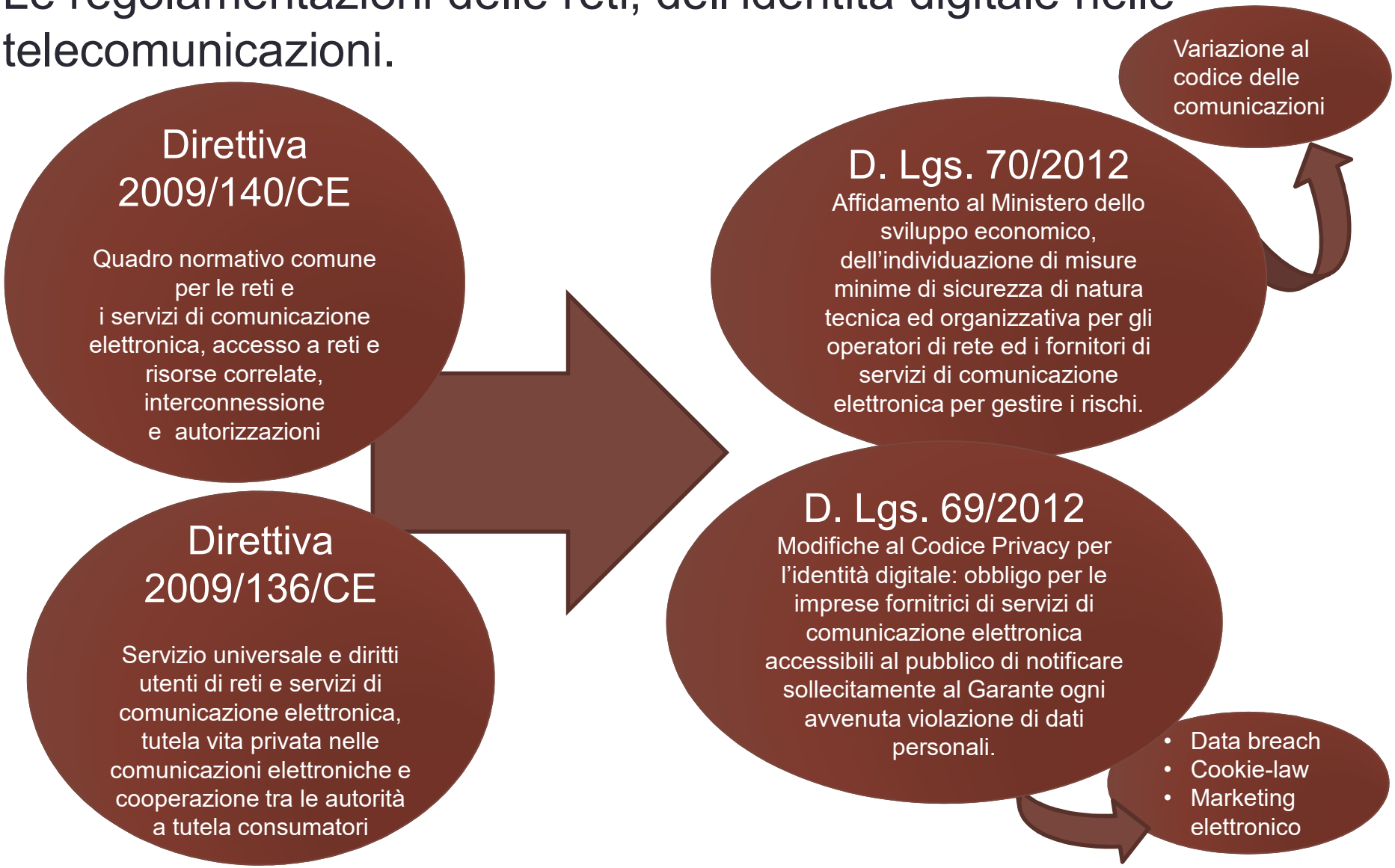
I “Provvedimenti” delle autorità con impatti sulla Cyber Security

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

- Amministratori di sistema
- Videosorveglianza
- GPS
- Dati biometrici
- Data breach
- Cookies
- …

“Privacy” e reti di comunicazione

Le regolamentazioni delle reti, dell’identità digitale nelle telecomunicazioni.



Naturalmente il GDPR: “General Data Protection Regulation”

Alcuni elementi con impatto sulla Cyber Security:

- DPO
- Valutazione del rischio
- Valutazione di impatto privacy
- Data Breach
- Privacy By Default
- Privacy By Design
- Profiling
- Data portability & Diritto All’Oblio
- Pseudoanomizzazione dei dati
- …

La normazione societaria

Nel contesto italiano è emerso che una buona gestione della compliance Privacy consente di soddisfare anche queste norme (spesso governate da procedure comuni)

Nel contesto USA questa norma ha avuto un forte impatto sugli aspetti informatici

La normazione a tutela di interessi geopolitici e geoeconomici

Diversi sono gli attori internazionali che emettono normazioni con impatto sulla Cyber Security per tutelare interessi geopolitici e geoeconomici.

Big Data: limitazioni e opportunità geopolitiche e geoeconomiche

Carlo Muzzì
AICA - Associazione Italiana per l'Informatica ed il Calcolo Automatico
muzzi@acm.org

Abstract. *The idea that Big Data can constitute a new frontier for innovation, competition and productivity in the global economy is now generally accepted; but there are many geo-political and geo-economic conditions that influence them in the global context. These conditions will be analyzed in this study, along with the opportunities offered.*

Keywords: Big Data, conditions, opportunities, geo-political, geo-economic.

Leve tramite le quali questi interessi sono influenzati:

- Storage
- Internet
- I grandi accumulatori di informazioni
- I giganti del calcolo
- Le influenze dei contesti giuridici

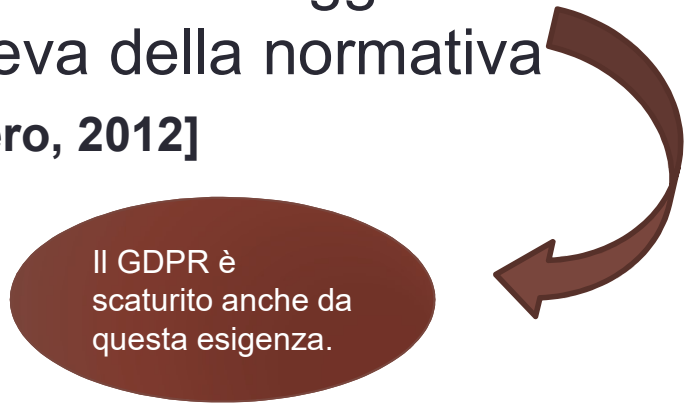
[Muzzì, 2013]

La normazione a tutela di interessi geopolitici e geoeconomici

La conclusione di questa ricerca del 2013 aveva evidenziato:

«… la prevalente superiorità dell'attore USA a livello mondiale e, in subordine, una significativa posizione degli attori asiatici. In generale l'Europa e il nostro paese [ITALIA] subiscono più che competere in questo mercato; per il nostro continente questa situazione non costituisce solo uno svantaggio economico, ma anche elemento di dipendenza strategica per certi versi assimilabile a quella esistente verso i paesi produttori di petrolio (lo scandalo del Datagate costituisce un chiaro esempio di tale subordinazione e dei rischi connessi…)»

Ma anche il quadro normativo costituiva uno svantaggio competitivo per l'Europa che non disponeva della normativa più armoniosa tipica degli USA. **[Mantelero, 2012]**



La normazione a tutela di interessi geopolitici e geoeconomici

theguardian

theguardian.com

Exclusive: how US and Britain unlock privacy on the internet

- Elaborate safeguards broken by NSA and GCHQ
- Encryption meant to protect emails, bank and medical records
- New Snowden revelations certain to cause political row

James Ball
Julian Borger
Glenn Greenwald

2013: il Datagate

R.it Social Network

Home | News | Speciali | Mobile | Social Network | Sicurezza | Prodotti | Interattivi | Video

602

Mark Zuckerberg al Senato Usa: "Cambridge Analytica non era l'unica ad avere i dati di 87 milioni di persone"

(reuters)

Il fondatore di Facebook compare a Washington davanti alle commissioni commercio e giustizia. "Sappiamo che quelle informazioni sono state vendute ad altre aziende. Ma stiamo lavorando perché non accada più". Attacco da parte di diversi senatori democratici: "Avete lasciato che i dati dei vostri utenti venissero saccheggiati". Ma intanto il titolo vola in borsa

di JAIME D'ALESSANDRO

2018: Facebook

Solo apparentemente non è mutato nulla.

La normazione a tutela di interessi geopolitici e geoeconomici

theguardian

theguardian.com

Exclusive: how US and Britain unlock privacy on the internet

- Elaborate safeguards broken by NSA and GCHQ
- Encryption meant to protect emails, bank and medical records
- New Snowden revelations certain to cause political row

2013: il Datagate

R.it Social Network

Home | News | Speciali | Mobile | Social Network | Sicurezza | Prodotti | Interattivi | Video

Mark Zuckerberg al Senato Usa: "Cambridge Analytica non era l'unica ad avere i dati di 87 milioni di persone"

(reuters)

Il fondatore di Facebook compare a Washington davanti alle commissioni commercio e giustizia. "Sappiamo che quelle informazioni sono state vendute ad altre aziende. Ma stiamo lavorando perché non accada più". Attacco da parte di diversi senatori democratici: "Avete lasciato che i dati dei vostri utenti venissero saccheggiati". Ma intanto il titolo vola in borsa

di JAIME D'ALESSANDRO

2018: Facebook

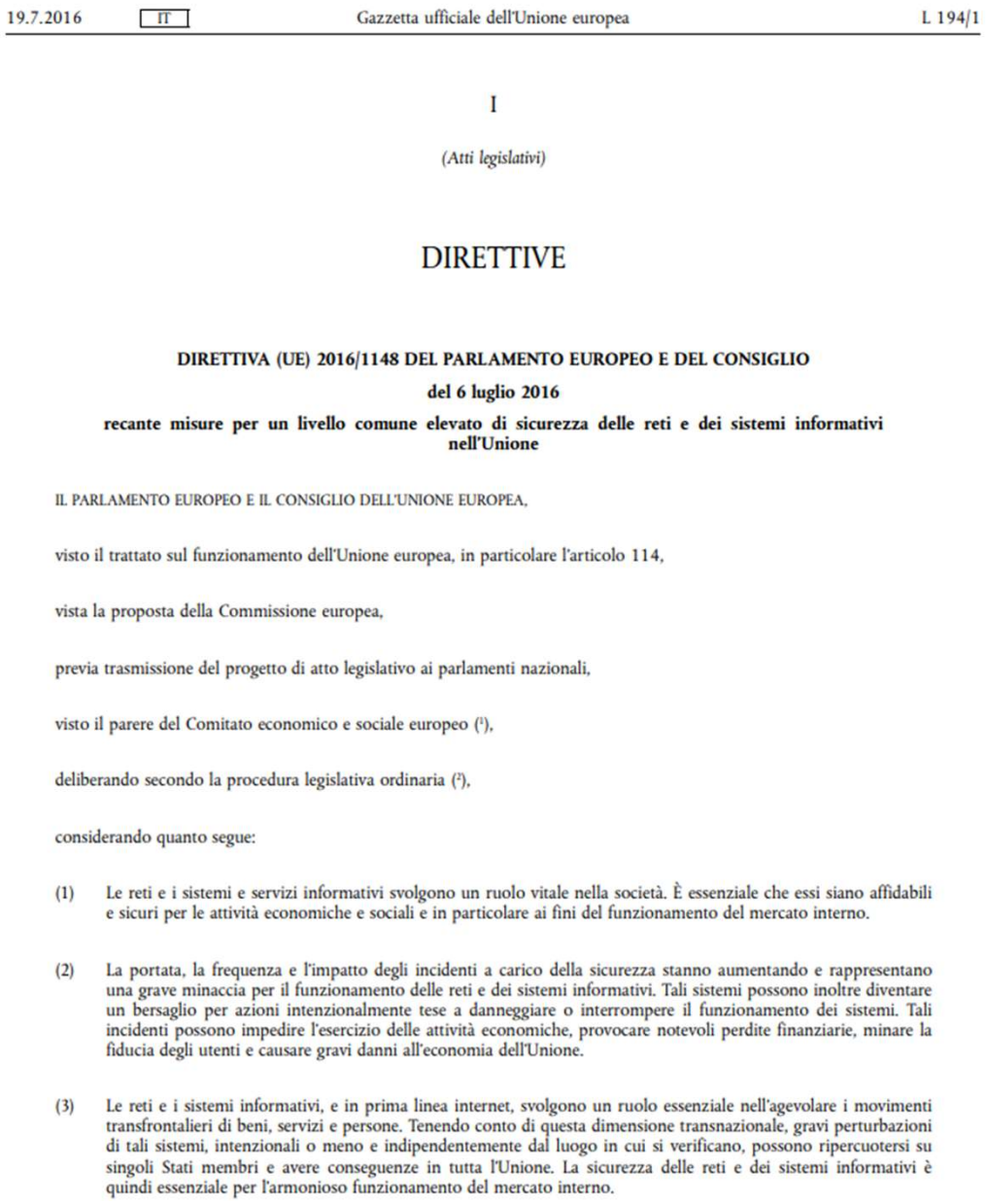
Solo apparentemente non è mutato nulla.

La normazione a tutela di interessi geopolitici e geoeconomici

DIRETTIVA (UE) 2016/1148

Costituisce un primo atto di armonizzazione europea della cybersecurity:

“Sicurezza delle reti e dei sistemi informativi”
“Network and Information Systems” (“NIS”).



19.7.2016 IT Gazzetta ufficiale dell'Unione europea L 194/1

I

(Atti legislativi)

DIRETTIVE

DIRETTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 6 luglio 2016

recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo (1),

deliberando secondo la procedura legislativa ordinaria (2),

considerando quanto segue:

(1) Le reti e i sistemi e servizi informativi svolgono un ruolo vitale nella società. È essenziale che essi siano affidabili e sicuri per le attività economiche e sociali e in particolare ai fini del funzionamento del mercato interno.

(2) La portata, la frequenza e l'impatto degli incidenti a carico della sicurezza stanno aumentando e rappresentano una grave minaccia per il funzionamento delle reti e dei sistemi informativi. Tali sistemi possono inoltre diventare un bersaglio per azioni intenzionalmente tese a danneggiare o interrompere il funzionamento dei sistemi. Tali incidenti possono impedire l'esercizio delle attività economiche, provocare notevoli perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia dell'Unione.

(3) Le reti e i sistemi informativi, e in prima linea internet, svolgono un ruolo essenziale nell'agevolare i movimenti transfrontalieri di beni, servizi e persone. Tenendo conto di questa dimensione transnazionale, gravi perturbazioni di tali sistemi, intenzionali o meno e indipendentemente dal luogo in cui si verificano, possono ripercuotersi su singoli Stati membri e avere conseguenze in tutta l'Unione. La sicurezza delle reti e dei sistemi informativi è quindi essenziale per l'armonioso funzionamento del mercato interno.

Bibliografia e sitografia

[ACCREDIA, 2018] Accredia-Ente Italiano di Accreditamento, Statistiche delle certificazioni di sistema di gestione, Statistiche relative a Aziende Certificate presenti in ogni Norma, Situazione al 02-2018, consultato il 20-05-2018.

[Guasconi, 2015] Guasconi F., La sicurezza nei sistemi di conservazione digitale, Security Summit, UNINFO, Roma, 2015.

[ISO, 2018] ISO-International Organization for Standardization, Management system standards-What is a management system?, consultato il 20-05-2018.

[ISTAT, 2017] ISTAT-Istituto Nazionale di Statistica, Annuario Statistico Italiano, Cap. 14, Imprese, 2017.

[ITU, 2018] ITU Telecommunication Standardization Sector, Definition of cybersecurity, referring to ITU-T X.1205, Overview of cybersecurity, consultato il 20-05-2018.

[Mantelero, 2012] Mantelero A., 2012, Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo, Il diritto dell'informazione e dell'informatica (Fasc. 1, 2012).

[Muzzì, 2013] Muzzì C., Big Data: limitazioni e opportunità geopolitiche e geoeconomiche, Atti del 50° Congresso Nazionale AICA, Salerno, 2013.

Bibliografia e sitografia

[Ritchin, 2012] Ritchin F., Dopo la fotografia, Piccola Biblioteca Einaudi, 2012.

[UNI, 2018] UNI-Ente Nazionale Italiano di Unificazione, Norma UNI - UNI CEI EN ISO/IEC 27001:2017, consultato il 20-05-2018.

[Vardi, 2017] Vardi M. Y., Cyber Insecurity and Cyber Libertarianism, Communications of the ACM, Vol. 60 No. 5, Page 5, 2017.