

IN PRIMO PIANO

L'associazione "Circolo dei Giuristi Telematici", è la più "antica" del web giuridico, Fondata il 21 maggio 1998 dal Dott. Francesco Brugaletta (attualmente magistrato del TAR di Catania), dal Dott. Luca Ramacci (oggi Consigliere di Cassazione) e dall'Avv. Giorgio Rognetta del Foro di Reggio Calabria, prematuramente scomparso, si prefiggeva già all'epoca lo scopo di introdurre il processo telematico, oggi divenuta realtà.

La storica mailing list conta oggi quasi 300 iscritti tra avvocati, magistrati, giuristi d'impresa, universitari e tecnici specializzati di tutta Italia

Per informazioni:

info@giuristitelematici.net

<http://www.giuristitelematici.it>

@CircoloGT



NEWS

CONVEGNO "LE COMUNICAZIONI ELETTRONICHE" DI ANDIG



NEWS

LA FIRMA GRAFOMETRICA È UNA FIRMA ELETTRONICA O UNA FIRMA AUTOGRAFA? (MARCO CUNIBERTI)

NEWS

MASTER COURSE ANORC

NEWS

PETIZIONE PER LE REGOLE TECNICHE: GLI STATI GENERALI INVIANO LE FIRME ALLE AUTORITÀ

NEWS

E-PRIVACY AUTUMN EDITION A CAGLIARI IL 17 E 18 OTTOBRE 2014: ONLINE IL PROGRAMMA

NEWS

CONVEGNO IN MEMORIA DI GIORGIO ROGNETTA

Tweet

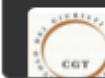
 Segui



Giuristi Telematici @CircoloGT 4h
A Marzo Master Course @_ANORC: per il Circolo sconto del 10% sul percorso formativo! Per maggiori informazioni anorc.it/evento/342_A_m...



Giuristi Telematici @CircoloGT 15 Gen
SAVE THE DATE: assemblea dei soci del Circolo il 23/01/2015. Per i dettagli relativi alla partecipazione: giuristitelematici.it



Giuristi Telematici @CircoloGT 6 Gen
Iscrizioni anno 2015 all'associazione



Il Circolo ha partecipato alle audizioni informali durante l'approvazione della L. 48/2008, di recepimento della Convenzione di Budapest sul Cybercrime

**COMMENTO ALLA LEGGE DI RATIFICA
DELLA CONVENZIONE DI BUDAPEST
del 23 NOVEMBRE 2001**

avv. Marco Cuniberti
avv. Giovanni Battista Gallus
avv. Francesco Paolo Micozzi
avv. Stefano Aterno

CAMERA DEI DEPUTATI N. 2807

DISEGNO DI LEGGE

PRESENTATO DAL MINISTRO DEGLI AFFARI ESTERI
(D'ALEMA)

DAL MINISTRO DELLA GIUSTIZIA
(MASTELLA)

DAL MINISTRO DELLE COMUNICAZIONI
(GENTILONI SILVERI)

E DAL MINISTRO PER LE RIFORME E LE INNOVAZIONI NELLA
PUBBLICA AMMINISTRAZIONE
(NICOLAIS)

DI CONCERTO CON IL MINISTRO DELL'INTERNO
(AMATO)

CON IL MINISTRO DELLA DIFESA
(PARISI)

E CON IL MINISTRO DELL'ECONOMIA E DELLE FINANZE
(PADOA SCHIOPPA)

Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno

Presentato il 19 giugno 2007

ONOREVOLI DEPUTATI! — La criminalità informatica nei suoi aspetti sociali e giuridici attira, ormai da molti anni, oltre che l'attenzione dei mezzi d'informazione, quella dei criminologi e della dottrina

giuridica, in particolare dei cultori del cosiddetto diritto penale dell'informatica.

In prosieguo di tempo, sulla scia dell'espandersi della società dell'informazione, anche le organizzazioni internazio-

DICHIARAZIONE DEI DIRITTI IN INTERNET: IL CIRCOLO PARTECIPA ALLE CONSULTAZIONI



Il 23 febbraio alle 10:30, nell'ambito delle consultazioni sulla Dichiarazione dei diritti in Internet, la Commissione per i diritti e i doveri relativi ad Internet terrà un'audizione ove un rappresentante del Circolo avrà l'opportunità di esprimere le considerazioni dell'associazione in merito ai principi contenuti nella dichiarazione.

L'audizione verrà trasmessa in diretta sulla web-tv della Camera dei deputati.

HOME PAGE

CHI SIAMO

ATTIVITÀ CGT

#FOIA4ITALY: INCONTRO DELLE ASSOCIAZIONI CON I PARLAMENTARI E CONFERENZA STAMPA



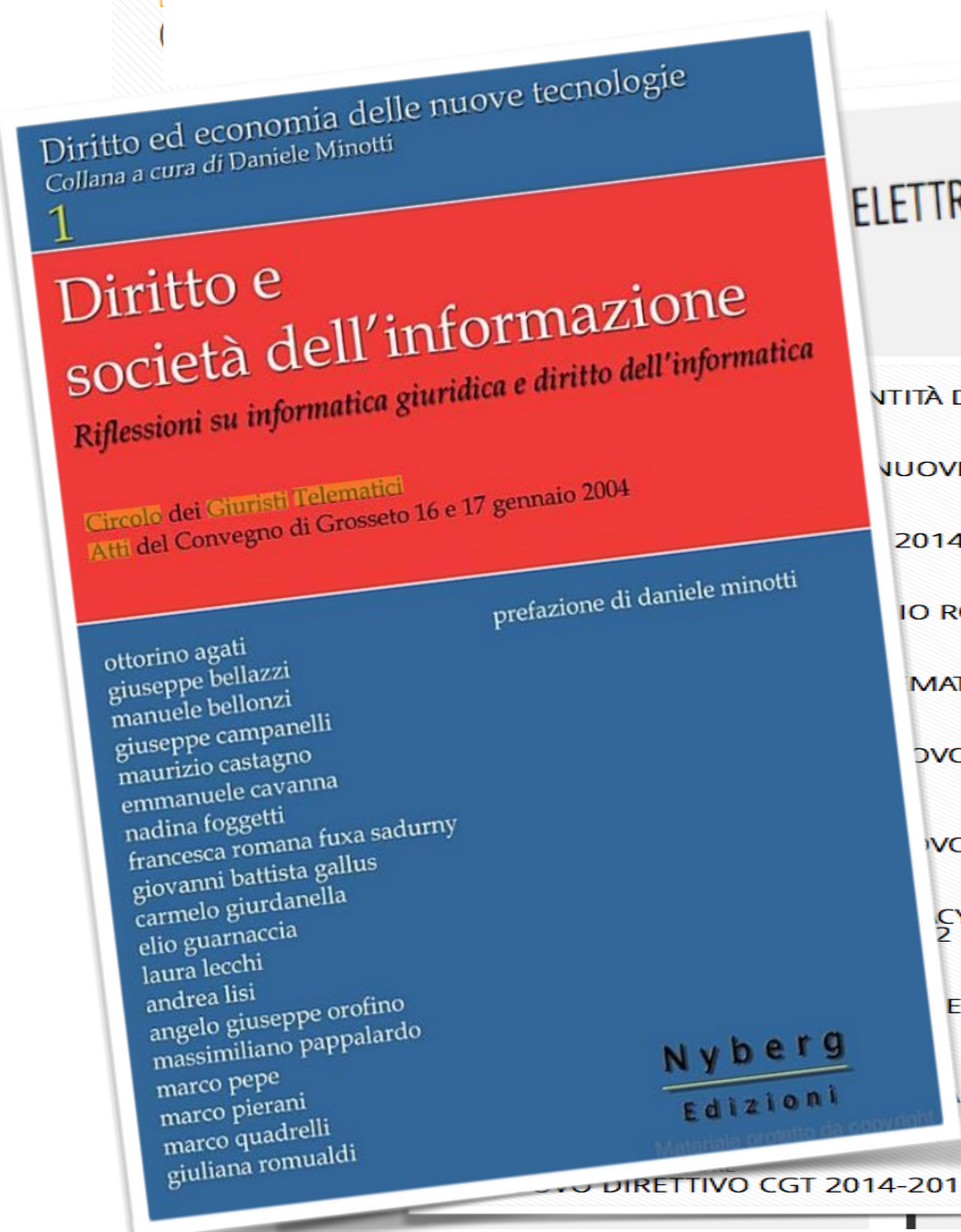
#Foia4Italy

Il Freedom of Information Act per l'Italia

presentato ai parlamentari italiani

30 associazioni della società civile: "Matteo Renzi l'aveva promesso, noi l'abbiamo scritto. Non resta che approvarlo"

Il Circolo si è fatto promotore di svariati convegni e seminari giuridici, oltre che di alcune pubblicazioni cartacee



ELETRONICHE"

NEWS

PETIZIONE PER LE REGOLE
GENERALI INVIANO LE FIR

QUE GLI STATI

Diritto ed economia delle nuove tecnologie
Collana a cura di Daniele Minotti
4

ITC Disabilità e Diritto

Atti del Convegno del Circolo dei Giuristi Telematici
Roma, 28 e 29 ottobre 2005

a cura di
Antonio Antonello

presentazione di Antonio A. Martinelli

con i contributi di
Ottorino Agati
Antonio Antonello
Carlo Baccantini
Carlo De Rosa
Maria Concetta De Vito
Silvia Dieli
Nicola Diopoli
Nadine Fagotti
Pierluigi Fagotti
Antonio A. Martinelli
Carlo Magliaro
Silvia Mori

SSERVATORI.NET
digital innovation

/ HOME

/ ACCEDI

DATI &
PUBBLICAZIONI

BUSINESS CASE

CONVEGNI

WORKSHOP &
WEBINAR

VIDEO

/ Enterprise Solutions / Digital Markets / Mobile Economy / Industry / PA / PMI / Startup

CONVEGNO: 26/02/2015

**PROFESSIONISTI IN DIGITALE? UN VALORE PER LE IMPRESE
CLIENTI!**

LA VERA FORZA È NEL SISTEMA

OSSERVATORIO: ICT & Professionisti

PRESSO: Aula Carlo De Carli – Campus Bovisa – Via Durando 1

**international
open data day
cagliari 2014**



CAGLIARI OPEN DATA DAY
2015

E-Privacy 2014
Autumn Edition

INTERNET *è delle* **COSE**
e non più delle **PERSONE?**



**international
open data day
italia 2013**

Cagliari



Studying the Internet, exploring its potential & experimenting new ideas

lunch seminar



29 ° Nexa Lunch Seminar - Trademark law and Free/Open Source Systems

25 marzo 2015
Carmine Antonio Perri, già studente del LL.M in
Intellectual Property
[more >](#)

events



Internet e Democrazia: il Centro Nexa su Internet & Società a Biennale Democrazia 2015

L'edizione 2015 di Biennale Democrazia, che si
svolgerà a Torino dal 25 al 29 marzo, dedica
ampio spazio al tema "Internet e Democrazia",
proponendo una serie di incontri che anche
quest'anno sono co-organizzati, in parte o
interamente, dal Centro Nexa su Internet e
Società del Politecnico di Torino.
[more >](#)

events

upcoming events

March
25
2015

Via Boggio
65/a Torino
(primo piano)

29 ° Nexa Lunch Seminar - Trademark law and Free/Open Source Systems

Mercoledì 25 marzo 2015, ore 13-14
Via Boggio 65/a, Torino (primo
piano) Ingresso libero Webcast live
Come raggiungerci: scarica la
mappa in PDF (464...

■ [apri il calendario eventi](#)

recent publications

Lorenzo Canova, Raimondo
Iemma e Federico Morando
**#WikiTrasparenza - Chi apre
davvero i dati sulle risorse
pubbliche**
Raimondo Iemma, Federico

search

join our community

Iscriviti alle nostre **mailing lists**,
contattaci, esplora i nostri **corsi**,
controlla le nostre **offerte di lavoro**,
compila il nostro **form** per essere
aggiornato su future opportunità
(come bandi per assegni o borse di
ricerca).

nexa planet

Unification of copyright law -
European Copyright Society. Tra gli
autori del testo della lettera inviata al
Commissario per la "Digital Economy
and Society" anche il Prof. Marco
Ricolfi, co-direttore del Centro Nexa.

**Peer production and the
opportunities and struggles of
constructing a more humane
production system.** Yochai Benkler,
faculty co-director presso il Berkman



"GlobaLeaks (...) won't have any central point of failure"

Forbes

"Their project aims to make a suite of software (...) to (...) maintain a whistle-blowing platform"



"Tor2web is a positive step for those who want to publish anonymously without sacrificing the exposure"

ars technica

WHISTLEBLOWING TECHNOLOGIES

Empowering Truth as a Human Right



ABOUT & MISSION

Hermes Center for Transparency and Digital Human Rights develop and promote Transparency and Freedom-Enabling Technologies...

[Read More »](#)

PROJECTS & TECHNOLOGIES

Transparency and Anonymity are not just ideas, they are technologies that we develop and promote...

[Read More »](#)

PAPERS & RESEARCH

Our Research and Studies Center establishing the State-Of-The-Art for Scholars, Professionals and Public Institutions...

[Read More »](#)

NEWS & PRESS

Stay updated about Hermes activities, initiatives, publications and events...

[Read More »](#)

Trattamento dei dati personali

Il D.lgs 196/2003 (parte generale)
Introduzione al “Codice della Privacy”

La “mappa” del Codice e degli allegati

I principi generali

Diritti e libertà fondamentali

Principio di necessità

Le definizioni

I dati personali

I dati identificativi

I dati sensibili e “supersensibili”

I dati giudiziari

Altre tipologie di dati

Il concetto di “trattamento”
Onnicomprensività del trattamento

Comunicazione

Diffusione

L' ambito di applicazione

Il trattamento per fini esclusivamente personali

I Soggetti

Titolare

Responsabile

Trattamento dei dati personali

Incaricato
Interessato
L'informativa
Forma e contenuto
Eccezioni
Il consenso
I diritti dell'interessato
Le misure di sicurezza
Misure minime e misure idonee

Il Disciplinare tecnico in materia di
misure minime di sicurezza (Allegato
B del Codice)
Misure per i trattamenti effettuati
senza strumenti elettronici
Outsourcing dei servizi
Responsabilità civile e penale e
sanzioni amministrative
Privacy e dipendenti
Videosorveglianza
Amministratore di sistema

Introduzione

Il “right to be let alone”

“La solitudine e la privacy sono divenute ancor più essenziali per l'individuo, ma le moderne tecnologie e le invenzioni, hanno, attraverso invasioni sulla vita privata, sottoposto a stress mentale ed a disagio, di gran lunga maggiore di quello che potrebbe essere inflitto dalle mere lesioni fisiche”



Vi faccio una domanda.

Quando è stata scritta la frase che avete appena letto?

Il “right to be let alone”

**The right “to be let alone”
(diritto ad essere lasciati soli)**

*Warren and Brandeis - “The Right to
Privacy”*

Harvard Law Review, Vol. IV

December 15, 1890

<http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm>



Dal “right to be let alone” alla regolamentazione del trattamento dei dati

- Dal right to privacy al corretto trattamento dei dati personali
 - Sviluppo tecnologico e avvento dell'informatica
 - Possibilità di elaborazione dei grandi quantità di dati
 - Creazione di banche dati pubbliche



Convenzione europea dei diritti dell'Uomo

Art.8

Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza.

Carta dei Diritti fondamentali dell'Unione Europea

Art.8 comma 1

Protezione dei dati di carattere personale

Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano

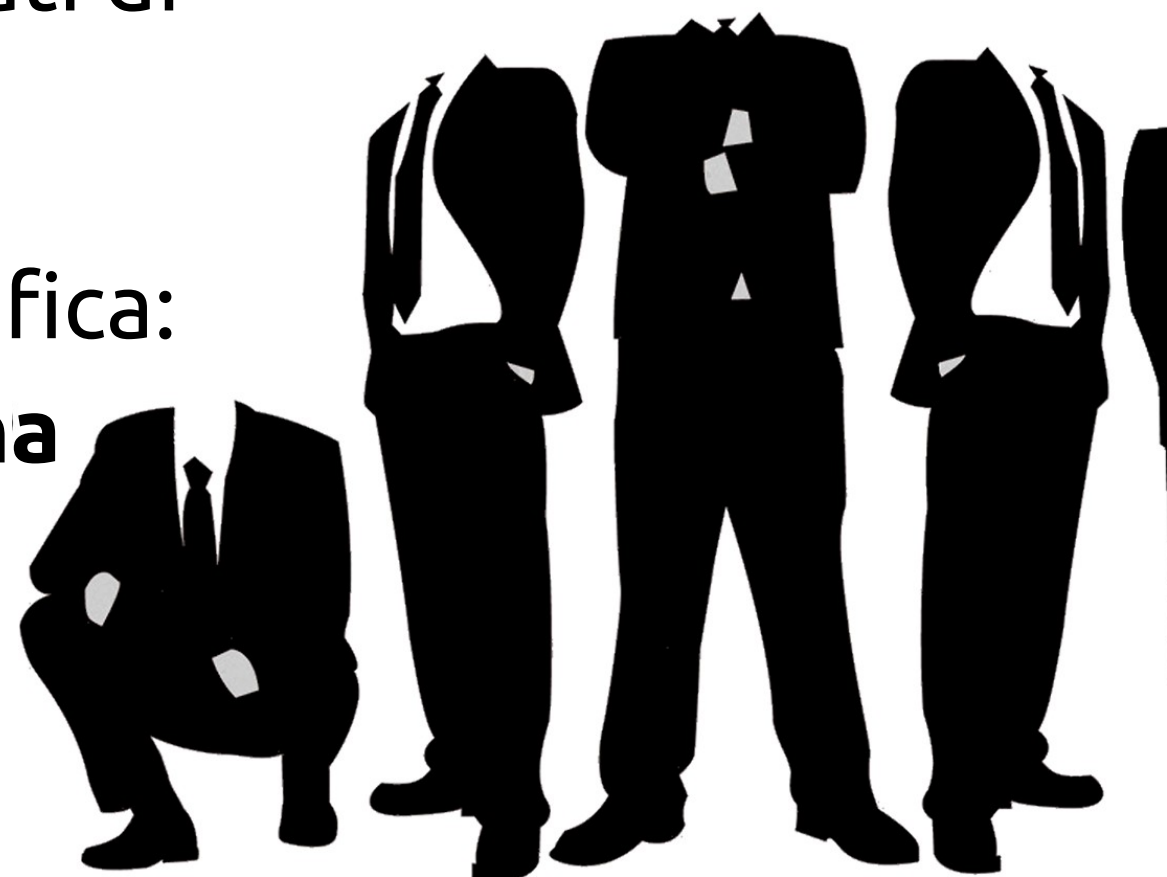
Convenzione di Strasburgo (1981)

Convenzione n. 108 sulla protezione
delle persone rispetto al
trattamento automatizzato di dati di
carattere personale, adottata a
Strasburgo il 28 gennaio 1981

“dati di carattere personale” significa:

**ogni informazione relativa ad una
persona fisica identificata o
identificabile**

(persona interessata)



Convenzione di Strasburgo (1981)

Si applica:

- ai casellari ed alle elaborazioni automatizzate di dati a carattere personale;
- nei settori pubblici e privati



DIRETTIVA N. 95/46/CE
DEL PARLAMENTO EUROPEO
E DEL CONSIGLIO del 24 ottobre
1995



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

Non è formalmente una legge di recepimento della direttiva 95/46, ma nella sostanza ne attua i principi, fornendo una tutela addirittura più pervasiva

- ☑ E' stata modificata e integrata da una pluralità di decreti legislativi
- ☑ Disciplina assai rigida, via via attenuata dalle successive integrazioni



IL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Decreto Legislativo 30 giugno 2003, n. 196
“Codice in Materia di Protezione dei Dati Personali”



- Dovrebbe coordinare la disciplina contenuta nella L. 675/96, nei decreti legislativi successivi, nella disciplina regolamentare, con le opportune modifiche ed integrazioni;
- Entrato in vigore quasi integralmente il primo gennaio del 2004

LA STRUTTURA DEL CODICE

Tre parti e tre allegati

- Parte I (disposizioni generali)
 - Principi fondamentali, adempimenti e regole di carattere generale
 - Regole ulteriori per i soggetti pubblici
 - Regole ulteriori per i privati e gli enti pubblici economici
- Parte II – Disposizioni relative a settori specifici
- Parte III (tutela dei diritti e sanzioni)
 - Tutela amministrativa e giurisdizionale
 - Ufficio del Garante
 - Sanzioni amministrative e penali
 - Norme transitorie

Allegati

- Allegato A
 - CODICI DI DEONTOLOGIA
- Allegato B
 - DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA
- Allegato C
 - TRATTAMENTI NON OCCASIONALI EFFETTUATI IN AMBITO GIUDIZIARIO O PER FINI DI POLIZIA

IL FUTURO: LA PROPOSTA DI REGOLAMENTO EU

Proposta presentata il 25/1/2012

- Regolamento, non più direttiva
 - Immediatamente esecutivo (quando verrà approvato)
- Principali novità
 - Estensione a alcuni trattamenti, anche non effettuati nell'UE
 - Diritto alla “portabilità del dato” e “diritto all'oblio”
 - Introduzione del Data protection officer
 - Valutazione d'impatto privacy e privacy by design
 - Obbligo di notificazione delle violazioni dei dati personali
 - Revisione dei poteri delle Autorità Nazionali di controllo

http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm



DISPOSIZIONI E PRINCIPI GENERALI

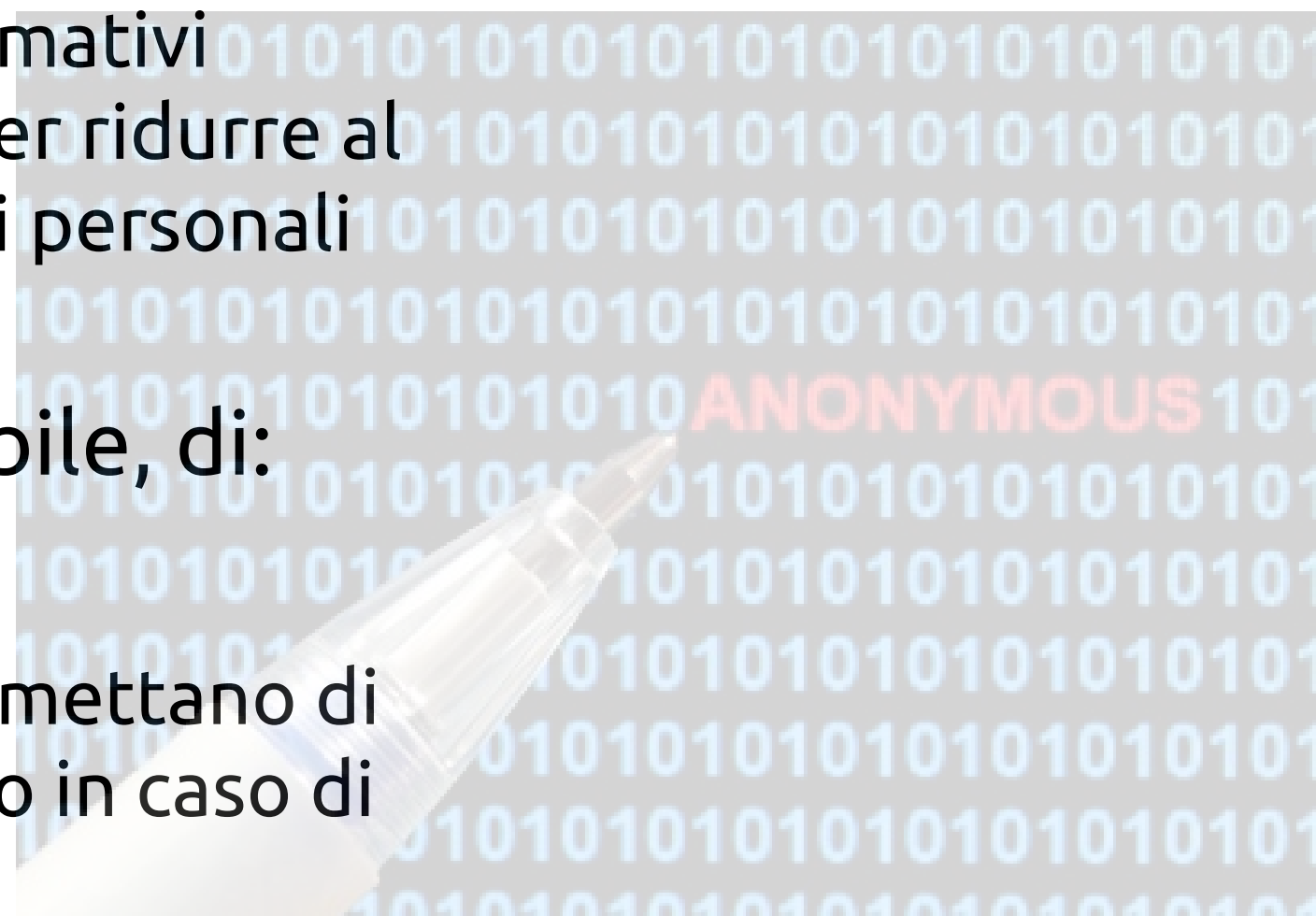
- Art. 1
 - “Chiunque ha diritto alla protezione dei dati personali che lo riguardano”
 - Enunciazione “con gran vigore” (Raffaele Zallone) del diritto alla protezione dei propri dati personali

- Art. 2
 - Le norme del Codice sono volte a garantire che il trattamento dei dati personali si svolga nel **rispetto dei diritti e delle libertà fondamentali**, nonché della **dignità dell'interessato**, con particolare riferimento alla **riservatezza**, all'**identità personale** e al **diritto alla protezione dei dati personali**

- Diritti e libertà fondamentali di tutti i soggetti coinvolti (interessati, titolari e terzi)
 - Dignità dell'interessato
 - diritto alla riservatezza
 - diritto alla identità personale
 - Il diritto alla protezione dei dati personali

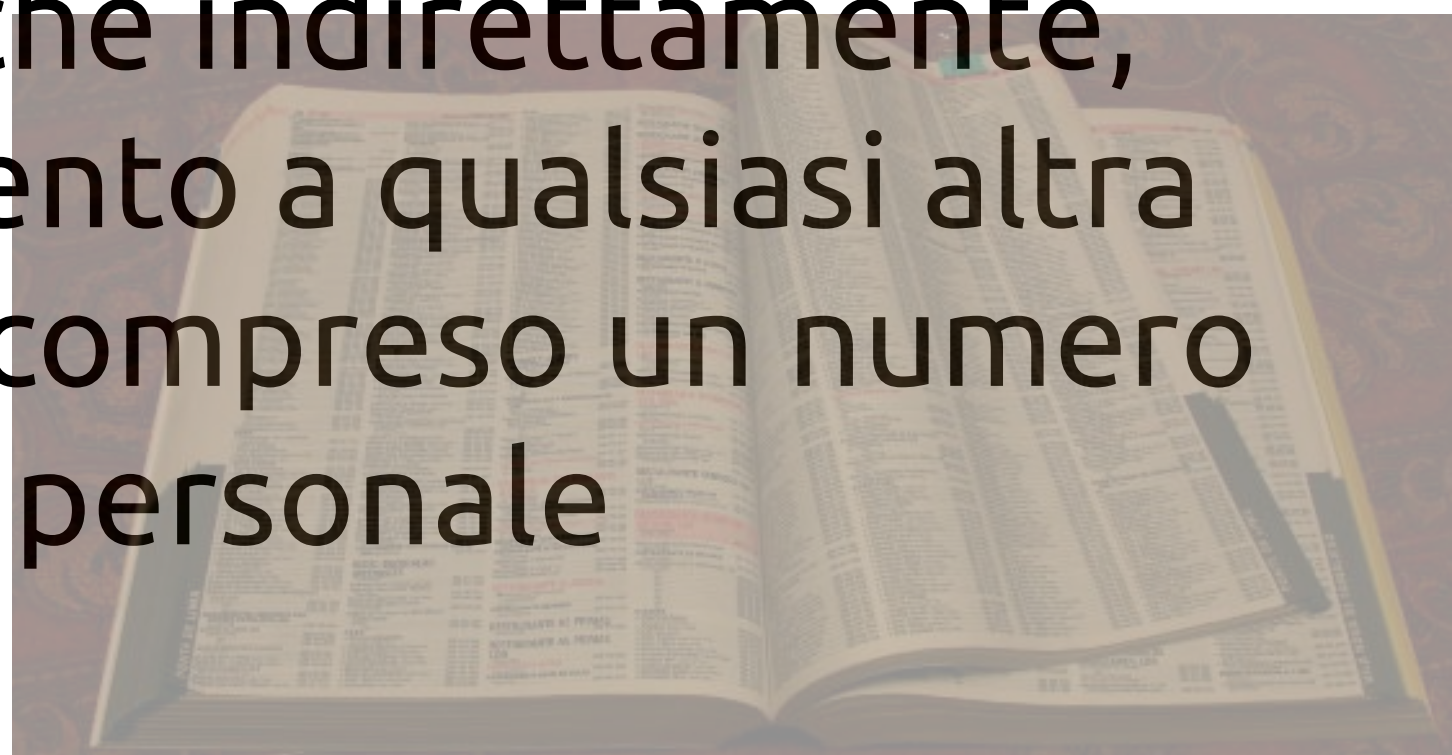
Art. 3

- Principio di necessità nel trattamento dei dati
 - I programmi e i sistemi informativi devono essere configurati per ridurre al minimo l'utilizzazione di dati personali e di dati identificativi
- Utilizzo, per quanto possibile, di:
 - **dati anonimi;**
 - opportune modalità che permettano di identificare l'interessato solo in caso di necessità



I DATI PERSONALI

- "dato personale", qualunque informazione relativa a persona fisica, ~~persona giuridica, ente od associazione,~~ identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale



- Dato = informazione.
 - qualsiasi elemento che abbia un contenuto informativo (Giovanni Ziccardi)
 - Parole, suoni, immagini, filmati etc.
- Categoria generale: dato personale
- Sotto-categorie: dati genetici, dati identificativi, dati giudiziari, dati sensibili, dati relativi a malattie contagiose di particolare gravità, dati anonimi, dati biometrici

Dati personali ≠ Dati anonimi

“DATO ANONIMO”, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile



A N O N Y M O U S



- Dati identificativi
 - dati personali che permettono l'identificazione diretta dell'interessato.

- **Dati sensibili**

- **Dati idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati idonei a rivelare lo stato di salute e la vita sessuale.**



- Dati giudiziari
 - Dati in materia di casellario giudiziale, anagrafe delle sanzioni amm.ve, riguardanti la qualità di indagato o imputato[...].



- Dati “super-sensibili”
 - Dati genetici: protezione estesa al massimo livello; necessità di notificazione; pressanti requisiti per la sicurezza e la separazione dei trattamenti
 - Dati relativi a malattie contagiose di particolare gravità
 - Legge 5 giugno 1990, n. 135 (infezione da HIV)
 - Art. 5: rilevazione statistica della infezione da HIV deve essere comunque effettuata con modalità che non consentano l'identificazione della persona
 - Art. 6: divieto assoluto di indagini da parte del datore di lavoro



- Dati “super-sensibili”

- Dati relativi all'interruzione di gravidanza

- Art. 11 L. 194/1978
 - L'ente ospedaliero, la casa di cura o il poliambulatorio nei quali l'intervento è stato effettuato sono tenuti ad inviare al medico provinciale competente per territorio una dichiarazione con la quale il medico che lo ha eseguito dà notizia dell'intervento stesso e della documentazione sulla base della quale è avvenuto, **senza fare menzione dell'identità della donna**

- Dati relativi a persone offese da atti di violenza sessuale

- art. 734-bis del codice penale
 - vietata la divulgazione non consensuale delle generalità o dell'immagine della persona offesa

Per fortuna queste tipologie di dati ben difficilmente vengono trattate dagli Ingegneri...

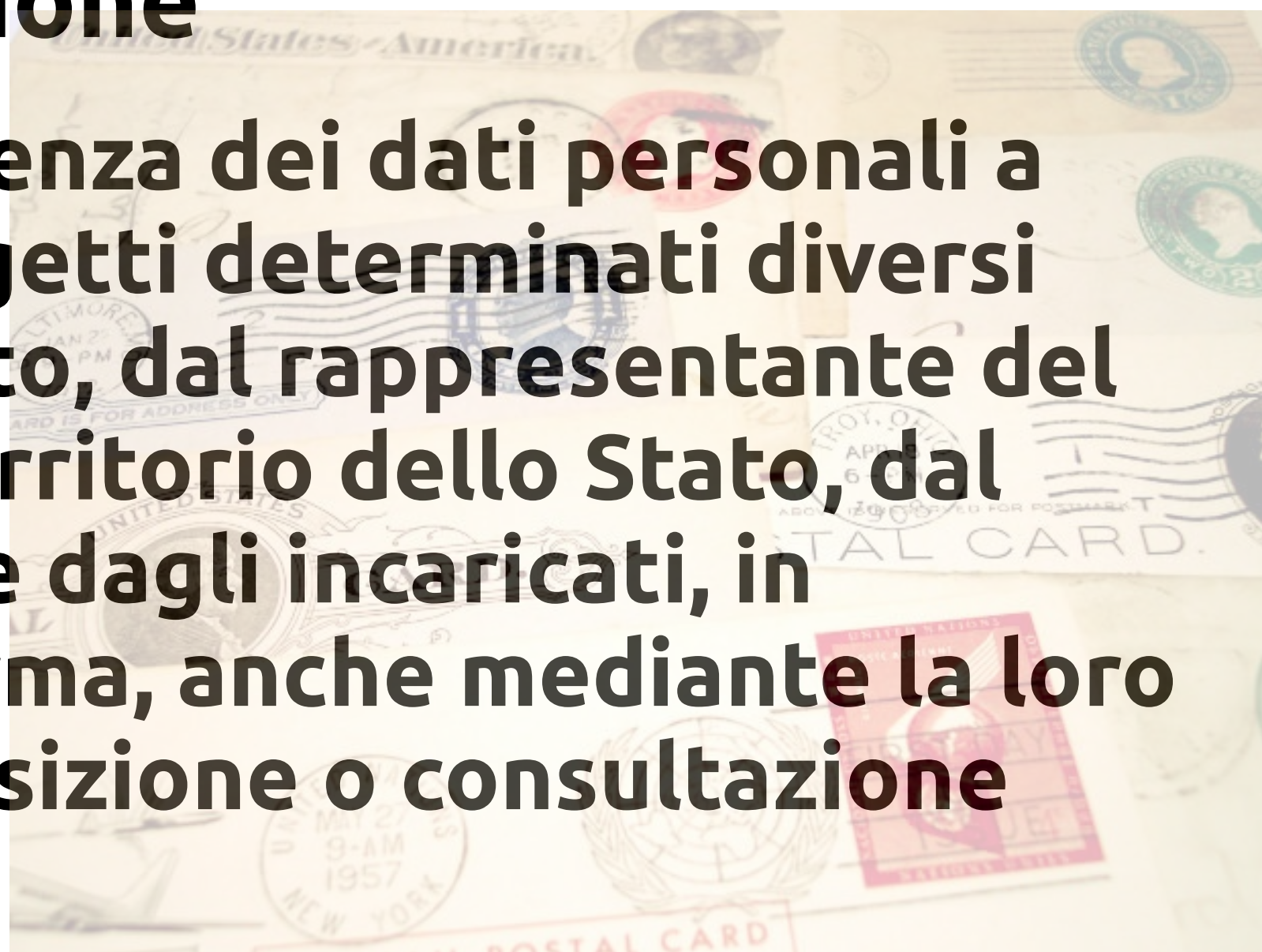
- TOP TEN DEI DATI PERSONALI (Giovanni Ziccardi)
 - Dati genetici
 - Dati relativi a malattie contagiose di particolare gravità
 - Dati idonei a rivelare lo stato di salute e la vita sessuale
 - Dati giudiziari
 - Altri dati sensibili
 - Dati biometrici
 - Dati di ubicazione o di traffico
 - Dati comuni
 - Dati quasi anonimi (identificazione solo per via mediata)
 - Dati anonimi



IL TRATTAMENTO

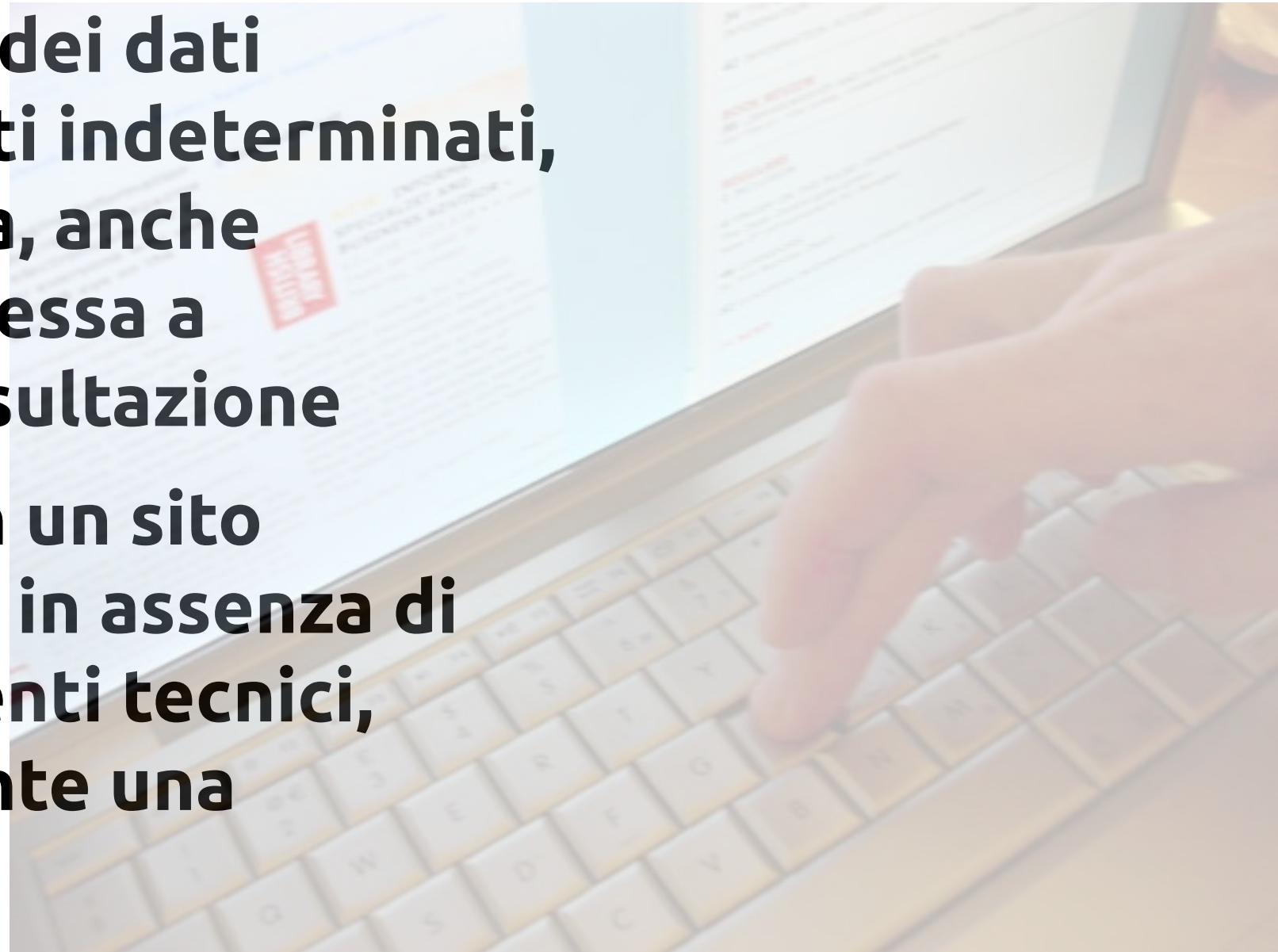
- Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, **la consultazione**, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati

- **La comunicazione**
 - **il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione**



- **La diffusione**

- **il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione**
- **La pubblicazione in un sito Internet configura, in assenza di specifici accorgimenti tecnici, quasi invariabilmente una “diffusione”**



QUALI TRATTAMENTI DI DATI NELLA PROFESSIONE DELL'INGEGNERE?

Dati personali

Clienti (persone fisiche)

Dipendenti e collaboratori

Terzi
(es. Perizie e consulenze)

Contatti online
(sito web, social)

Tipi di dati personali

Comuni

Sensibili (es. dipendenti)

Giudiziari
(perizie e consulenze,
soprattutto in ambito
penale)

Biometrici
(autenticazione)

Marketing

OGGETTO E AMBITO DI APPLICAZIONE

- Principio di stabilimento
- La disciplina si applica:
 - al trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato
- Ovvero
 - Qualora vengano impiegati strumenti situati nel territorio dello Stato (anche diversi da quelli elettronici) salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea



- Il trattamento per fini esclusivamente personali
- Tendenzialmente esentato dall'applicazione della disciplina
 - A condizione che i dati non siano destinati ad una comunicazione sistematica o alla diffusione



- Il trattamento per fini esclusivamente personali
 - Una comunicazione occasionale è compatibile con il trattamento a fini esclusivamente personali
 - Si applicano in ogni caso i principi riguardanti la responsabilità civile (art. 15) e gli obblighi di sicurezza (art. 31)



LE MODALITA' DEL TRATTAMENTO

Art. 11 del Codice

Principio generale di buona fede

- Il trattamento di dati personali personali deve avvenire:
 - in modo lecito
 - secondo correttezza;

Centralità delle regole generali di buona condotta, e delle regole deontologiche, per individuare la “correttezza” dei trattamenti

- **Principio di finalizzazione**
 - I dati devono essere raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- **Principio di esattezza**
 - I dati devono essere esatti e, se necessario, aggiornati;
- **Principio di pertinenza e di non eccedenza**
 - I dati devono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

I dati personali trattati
illecitamente
non possono essere
utilizzati



LA PAROLA ALL'AVV. MICOZZI (PER INFORMATIVA E CONSENSO)

D.lgs. 196/2003

Misure Minime

Misure Idonee



Alcuni punti fermi sulla sicurezza

La sicurezza è un processo dinamico

Non esistono soluzioni preconfezionate, o applicabili a tutti

E' impossibile raggiungere la sicurezza "assoluta", in quanto non esistono sistemi sicuri

Occorre puntare a un grado ragionevole e adeguato di sicurezza

Alcuni punti fermi sulla sicurezza

Il grado di insicurezza di un sistema è direttamente proporzionale alla sua complessità

Come sottolinea Giovanni Ziccardi, non bisogna mai dimenticare che ogni sistema sia composto da tre fattori:

Hardware

Software

Wetware (il fattore umano)

Alcuni punti fermi sulla sicurezza

Wetware (il fattore umano)

Da Wikipedia:

Wetware is used in conversation, notably USENET and in hacker culture. Also known as liveware, meatware or the abbreviation PEBKAC (Problem Exists Between Keyboard And Chair), is a term generally used to refer to a person operating a computer. It refers to human beings (programmers, operators, administrators) attached to a computer system.

Lo scopo della sicurezza è garantire

C Confidentiality

L'accesso ai dati
è riservato a chi ne
ha diritto

I Integrity

I dati non devono
essere danneggiati
manipolati
perduti

A Availability

I dati devono essere
sempre disponibili
continuità dei sistemi
continuità della connettività

L'obbligo di sicurezza

L'obbligo di sicurezza

Art. 31. Obblighi di sicurezza

*I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di **distruzione o perdita**, anche accidentale, dei dati stessi, di **accesso non autorizzato** o di **trattamento non consentito o non conforme** alle finalità della raccolta.*

L'obbligo di sicurezza

Art. 31. Obblighi di sicurezza

Custodia;

Controllo;

Idoneità;

Adeguatezza

- Con riguardo alle conoscenze acquisite in base al progresso tecnico
- Con riguardo alla natura dei dati
- Con riguardo alle specifiche caratteristiche del trattamento

L'obbligo di sicurezza

L'introduzione di un sistema integrato dovrebbe consentire di:

- mantenersi aggiornati su nuove minacce e vulnerabilità,
- trattare incidenti e perdite, in ottica di prevenzione e di miglioramento del sistema
- verificare la mancata implementazione di policy e procedure di sicurezza
- intervenire in tempo per prevenire danni
- implementare politiche e procedure conformi alle best practices internazionali

LA PAROLA ALL'AVV. MICOZZI (PER LE MISURE MINIME DI SICUREZZA)

LA RESPONSABILITA'

LA RESPONSABILITA' CIVILE

La responsabilità civile

Art. 15

Danni cagionati per effetto del trattamento

- 1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.
- 2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

La responsabilità civile

Attività pericolose:

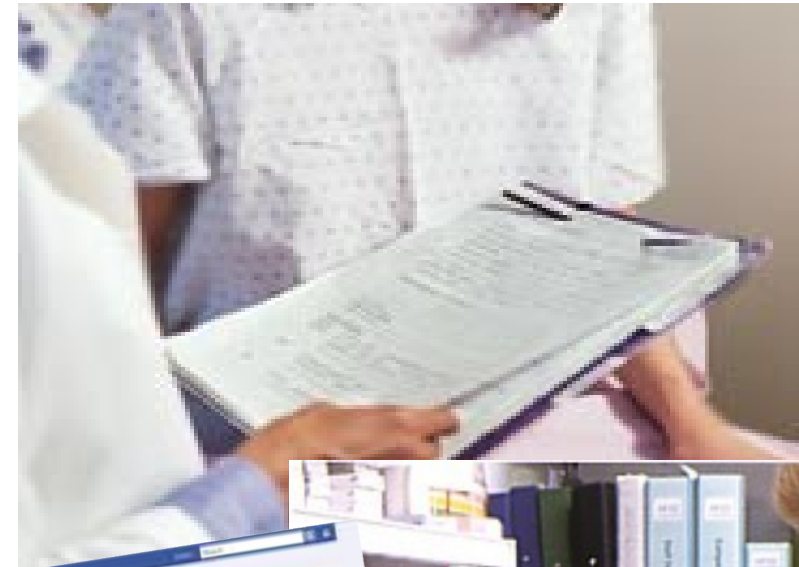
Art. 2050 cod. civ.

Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, **se non prova di avere adottato tutte le misure idonee a evitare il danno**



La responsabilità civile

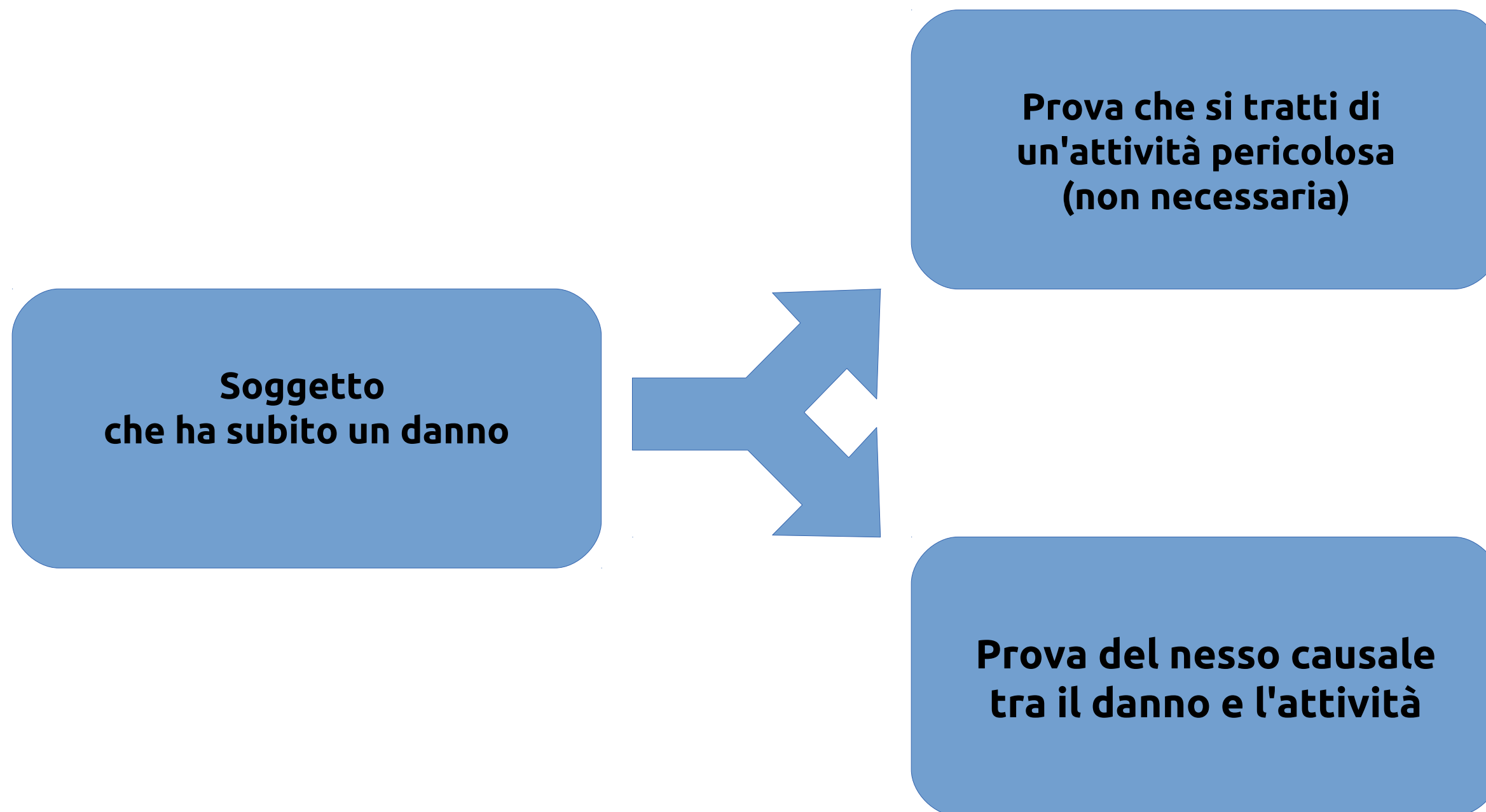
Attività pericolosissime



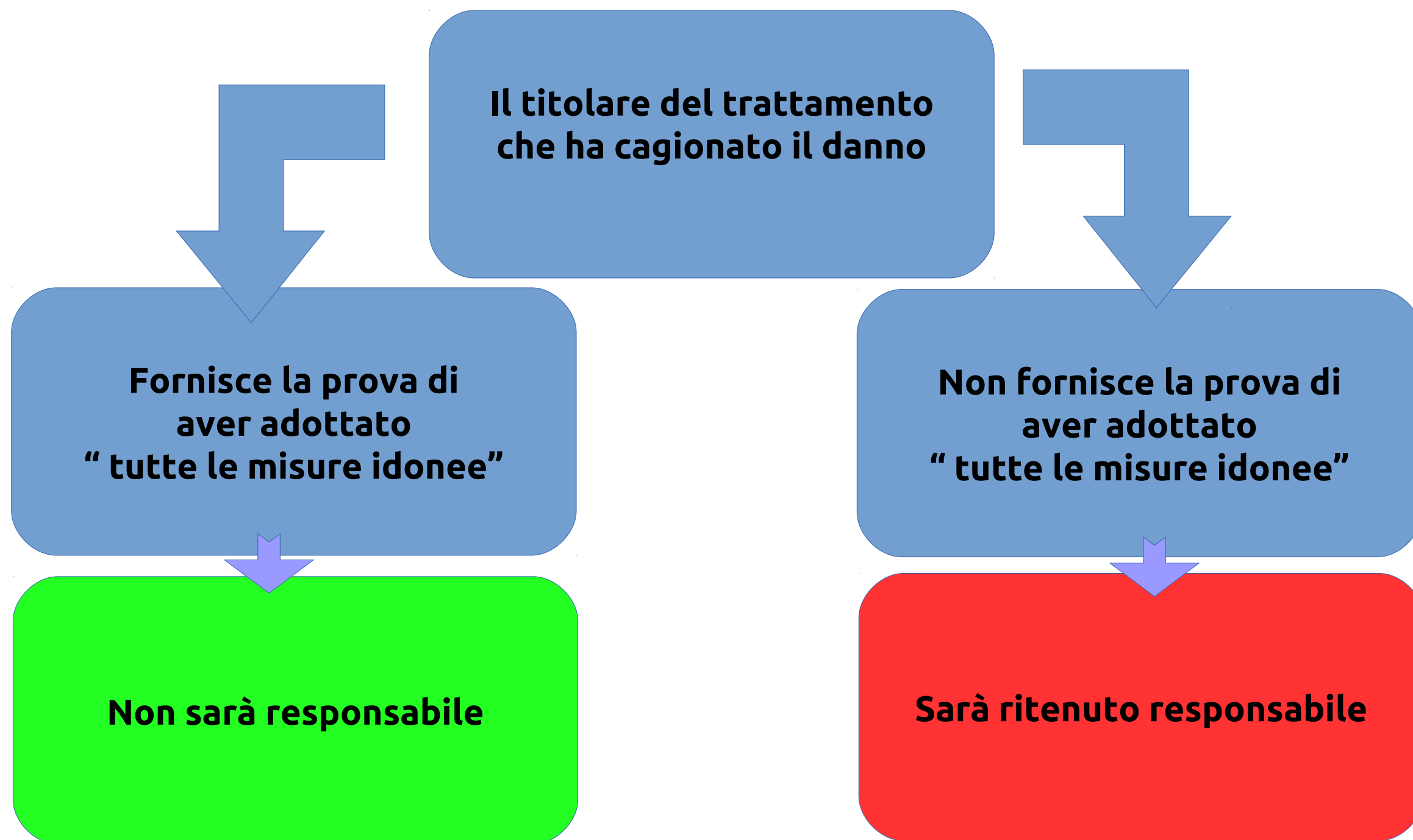
La responsabilità civile

- Nessun trattamento è escluso
- Anche il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è espressamente soggetto all'applicabilità della disciplina in tema di responsabilità (oltre che a quella in tema di sicurezza) – art. 5

La responsabilità civile



La responsabilità civile



La responsabilità civile

- Quali sono “tutte le misure idonee”?
 - Non sono le misure minime
 - La piena adozione delle misure minime evita soltanto di incorrere in responsabilità penali
 - E allora quali sono queste misure?
- Occorre fare riferimento all'obbligo di sicurezza dei trattamenti

- Prova particolarmente rigorosa
 - Non basta la prova di non aver commesso alcuna violazione di legge
 - Non basta la prova di aver adottato le regole di comune prudenza
- Occorre la prova positiva di aver impiegato ogni misura atta a impedire l'evento dannoso

- Nella pratica:
 - Prova di aver (preventivamente) adottato tutte le misure previste dai migliori standard sulla sicurezza dei dati personali
- Non basta neanche la prova della negligenza del danneggiato

- Danni patrimoniali e non patrimoniali
- In particolare, **il danno morale**
 - **Il danno morale è risarcibile quando è violato l'art. 11**



LE SANZIONI AMMINISTRATIVE

Le singole violazioni amministrative omessa o inidonea informativa

- Omessa o inidonea informativa all'interessato

Tale violazione - per comprendere la quale occorre far riferimento all'art. 13 del Codice che disciplina l'informativa – è punita con la sanzione amm.va del pagamento di una somma da € 6.000,00 ad € 36.000,00.

La L. legge 27 febbraio 2009, n. 41 di conversione del d.l. n. 207 del 30 dicembre 2008 ha inasprito le sanzioni, e introdotto svariate altre modifiche

E' punita con la sanzione amm.va da € 10.000,00 ad € 60.000,00:

- la cessione dei dati ad altro titolare perchè vengano trattati in termini incompatibili con quelli per i quali sono stati raccolti
- la violazione di qualsiasi altra disposizione in tema di trattamento dei dati

Le singole violazioni amministrative: altre fattispecie

E' punito con la sanzione amm.va da € 20.000,00 ad € 120.000,00, in aggiunta alla responsabilità penale (“in ogni caso”):

- Il trattamento di dati personali effettuato in violazione delle misure minime di sicurezza (art. 33)
- Il trattamento illecito di dati personali ai sensi dell'art. 167
 - Nei casi di cui all'articolo 33 è escluso il pagamento in misura ridotta

E' punita con la sanzione amm.va da € 30.000,00 ad € 180.000,00, in aggiunta alla responsabilità penale:

- L'inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto emanati dal Garante (ed in particolare, quelli di cui all'articolo 154, comma 1, lettere c) e d)

Le singole violazioni amministrative:
omessa informazione o esibizione al Garante

La mancata informazione o
esibizione di documenti al Garante
che li richieda sottopone alla
sanzione amm.va del pagamento di
una somma che va da € 10.000,00 ad
€ 60.000,00

“Aggravanti e attenuanti”

Per le ipotesi di minore gravità, avuto riguardo alla natura anche economica o sociale dell'attività svolta, i limiti minimi e massimi stabiliti sono applicati in misura pari a due quinti

In caso di più violazioni (salve alcune ipotesi), commesse anche in tempi diversi in relazione a banche di dati di particolare rilevanza o dimensioni, si applica la sanzione amministrativa del pagamento di una somma da 50.000 euro a 300.000 euro, e non è ammesso il pagamento in misura ridotta

“Aggravanti e attenuanti”

In altri casi di maggiore gravità e, in particolare, di maggiore rilevanza del pregiudizio per uno o più interessati, ovvero quando la violazione coinvolge numerosi interessati, i limiti minimo e massimo delle sanzioni sono applicati in misura pari al doppio.

Come se non bastasse, le sanzioni possono essere aumentate fino al quadruplo quando possono risultare inefficaci in ragione delle condizioni economiche del contravventore

La pubblicazione del provvedimento

- In tutti i casi di violazione amministrativa può essere disposta la pubblicazione del provvedimento del Garante in uno o più giornali indicati nel provvedimento stesso.
- La pubblicazione avviene, ovviamente, a spese del contravventore

LE SANZIONI PENALI

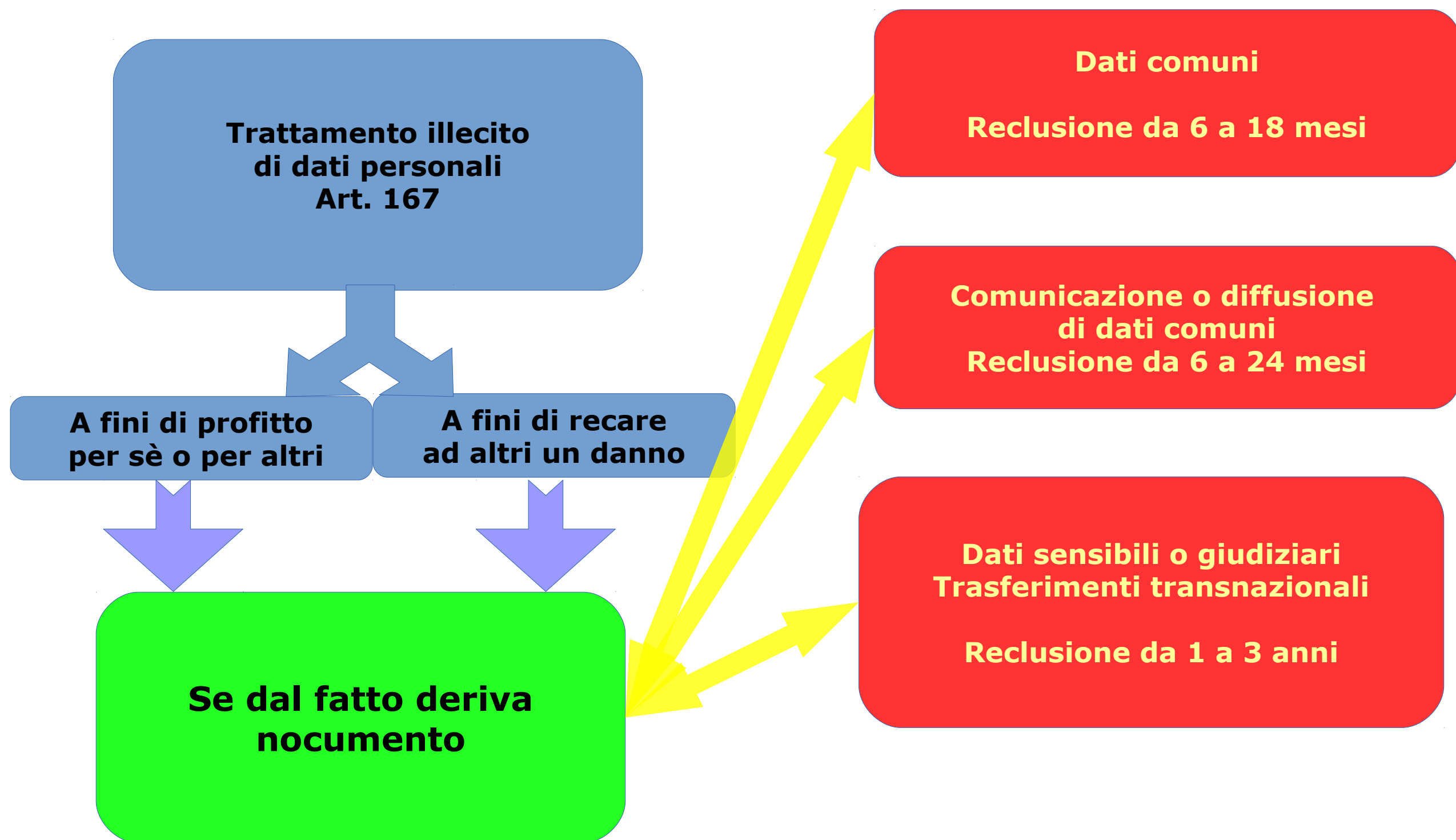
Illeciti penali

Costituiscono fonte di responsabilità penale:

- Trattamento illecito dei dati al fine di trarre per se o per altri un profitto o di recare ad altri un danno
- Falsità nelle dichiarazioni e notificazioni al Garante
- Omissione nell'adozione delle misure minime di sicurezza di cui all'allegato B
- Inosservanza dei provvedimenti del Garante

E' prevista la pena accessoria della pubblicazione della sentenza.

La responsabilità penale



Art. 171 Altre fattispecie

1. La violazione delle disposizioni di cui agli articoli 113, comma 1, e 114 è punita con le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300 (Statuto dei lavoratori)

Espletamento di indagini sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore;

Uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori



Sanzioni penali e misure minime

Art. 169

Misure di sicurezza

Primo Comma

Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 e' punito con l'arresto sino a due anni



Una forma di oblazione specialissima

- Il secondo comma dell'art. 169 prevede una sorta di oblazione specialissima subordinata ad un ravvedimento operoso.
- Si prevede, infatti, che all'atto dell'accertamento del reato (o nei casi più complessi per mezzo di un atto del Garante) all'autore del reato venga impartita una prescrizione per la regolarizzazione, e quindi per la adozione di tutte le misure minime previste.

Una forma di oblazione specialissima

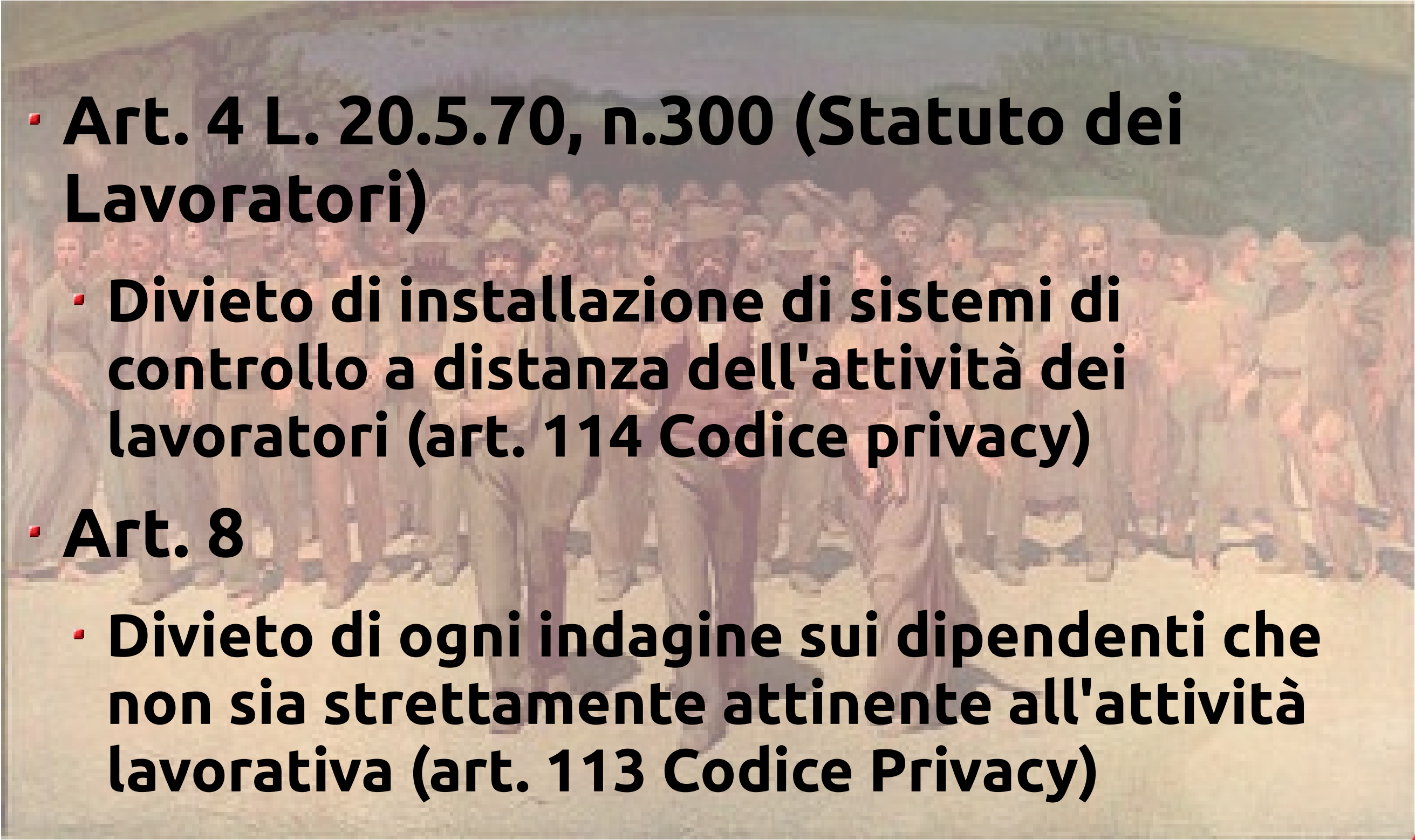
Tale adeguamento deve avvenire entro il termine fissato al momento dell'accertamento. Questo termine è quello strettamente necessario ad apprestare tutte le misure minime previste dall'all. B.

Nel caso in cui sorgano difficoltà per l'adozione delle misure minime può essere concessa una proroga non superiore a sei mesi

Una forma di oblazione specialissima

- Una volta apprestate le misure minime di sicurezza, come impartito dalla prescrizione all'atto dell'accertamento, l'autore del reato avrà 60 giorni di tempo per ottenere dal Garante l'ammissione al pagamento di una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa (€ 30.000,00).
- Il pagamento di tale “modesta” somma e l'effettivo adeguamento alle misure minime estinguono il reato. Si incide, in tal modo, sulla “punibilità astratta, estinguendo la possibilità statale di applicare la pena”.

Il controllo a distanza dei lavoratori

- 
- **Art. 4 L. 20.5.70, n.300 (Statuto dei Lavoratori)**
 - **Divieto di installazione di sistemi di controllo a distanza dell'attività dei lavoratori (art. 114 Codice privacy)**
 - **Art. 8**
 - **Divieto di ogni indagine sui dipendenti che non sia strettamente attinente all'attività lavorativa (art. 113 Codice Privacy)**

Statuto dei Lavoratori

- ART. 4 - Impianti audiovisivi.
- È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori



Statuto dei Lavoratori

- ART. 4 - Impianti audiovisivi.

Gli impianti e le apparecchiature di controllo che siano richiesti da **esigenze organizzative e produttive** ovvero dalla **sicurezza del lavoro**, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna



Statuto dei Lavoratori

- ART. 8. - Divieto di indagini sulle opinioni.
 - E' fatto divieto al datore di lavoro, al fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoro
 - Espressamente fatto salvo dall'art. 113 Codice Privacy
- Garante dati personali - Decisione 2 febbraio 2006
 - Proporzionalità nei controlli effettuati dal datore di lavoro
 - Artt. 3 - 11 Cod. Privacy

Controllo a distanza e videosorveglianza

Garante Privacy, 4/10/12

<http://bit.ly/VtPFLu>

Call center

4 telecamere brandeggiabili
e con zoom

Rilevato anche l'audio

Immagini non registrate, ma
visualizzabili da un tecnico
manutentore, non incaricato



Controllo a distanza e videosorveglianza

L'azienda:

“le finalità del trattamento sono da ricondursi esclusivamente a motivazioni di deterrenza di eventuali fatti illeciti ed alla tutela del patrimonio aziendale”

Nessun accordo sindacale

Nessuna idonea informativa



Controllo a distanza e videosorveglianza

Il Garante

E' un controllo a distanza

Non sono state provate le esigenze organizzative e produttive, e comunque manca l'accordo sindacale

In ogni caso, è un trattamento non conforme ai principi di liceità, pertinenza e non eccedenza



Privacy, controlli a distanza e Statuto dei lavoratori

Provvedimento del Garante 2 febbraio 2006

- <http://www.garanteprivacy.it/garante/doc.jsp?ID=1229854>
- Riguarda una casa di cura
 - Contestazione di addebito disciplinare per navigazione internet non attinente al lavoro



Sarebbe stato sufficiente verificare gli avvenuti accessi a Internet e i tempi di connessione senza indagare sui contenuti dei siti

Altri tipi di controlli sarebbero stati proporzionati rispetto alla verifica del comportamento del dipendente

Massima attenzione ai dati sensibili



Privacy Policies

Documento non previsto nè
obbligatorio

Può assumere
un'importanza
fondamentale



Contenuto

- Descrizione dei trattamenti;
- Descrizione delle mansioni e degli obblighi;
- Elencazione analitica delle misure e degli obblighi di sicurezza (non soltanto delle misure minime...);
- Elencazione analitica delle norme di comportamento per i trattamenti, anche con sistemi informatici;
- Policies particolareggiate e netiquette;



Contenuto

Utilizzo dei beni di proprietà dell'ente, con particolare riguardo ai personal computer e alle altre apparecchiature elettroniche

Navigazione web e utilizzo della posta elettronica "ufficiale"

Explicitazione dei divieti e delle possibilità di controllo, anche ai fini dell'acquisizione del consenso del dipendente;



Le linee guida del Garante per posta elettronica e internet

Le linee guida del Garante per posta elettronica e internet

- Pubblicata in G.U. n. 58 del 10 marzo 2007
- Indicazioni in ordine all'uso del computer sul luogo di lavoro

<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1387522>

Le linee guida del Garante

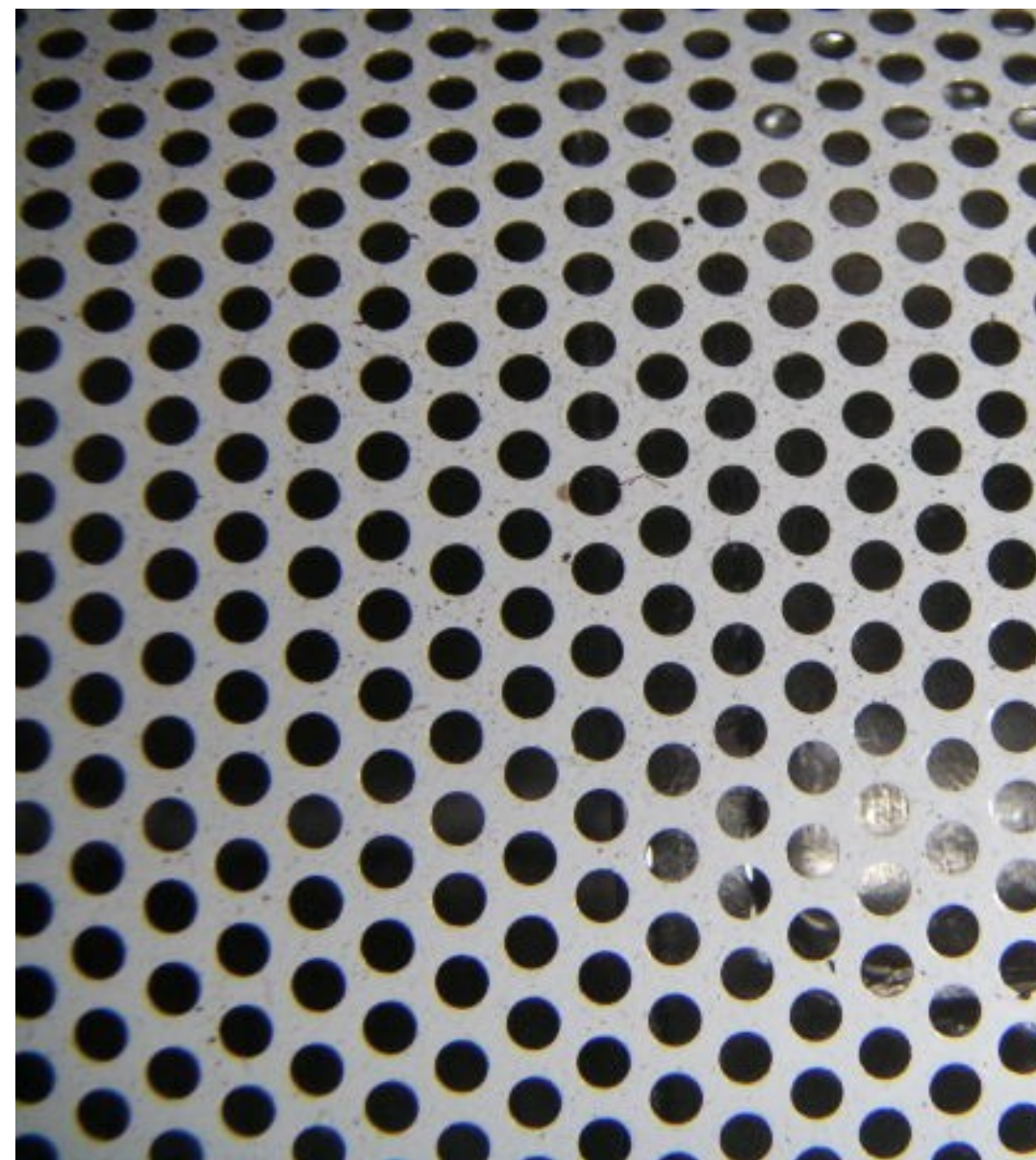
- Due esigenze (a volte) contrapposte
 - Trattamento di dati (anche sensibili) dei dipendenti
 - Prevenzione degli usi arbitrari degli strumenti informatici

Le linee guida del Garante

- Adozione (caldamente raccomandata) di un disciplinare interno (coinvolgendo le R.S.A.) nel quale siano chiaramente indicate le regole per l'uso di Internet e della posta elettronica
- Finalità:
 - Informare preventivamente, con chiarezza e in modo dettagliato i lavoratori sulle modalità di utilizzo di Internet e della posta elettronica
 - Informare sulla possibilità che vengano effettuati controlli (e sulle eventuali modalità)
- Pubblicizzazione del disciplinare



- Il datore di lavoro deve adottare ogni misura per prevenire usi impropri:
 - Individuazione dei siti correlati all'attività lavorativa
 - Adozione di filtri
- Prevenzione piuttosto che repressione e controllo a posteriori

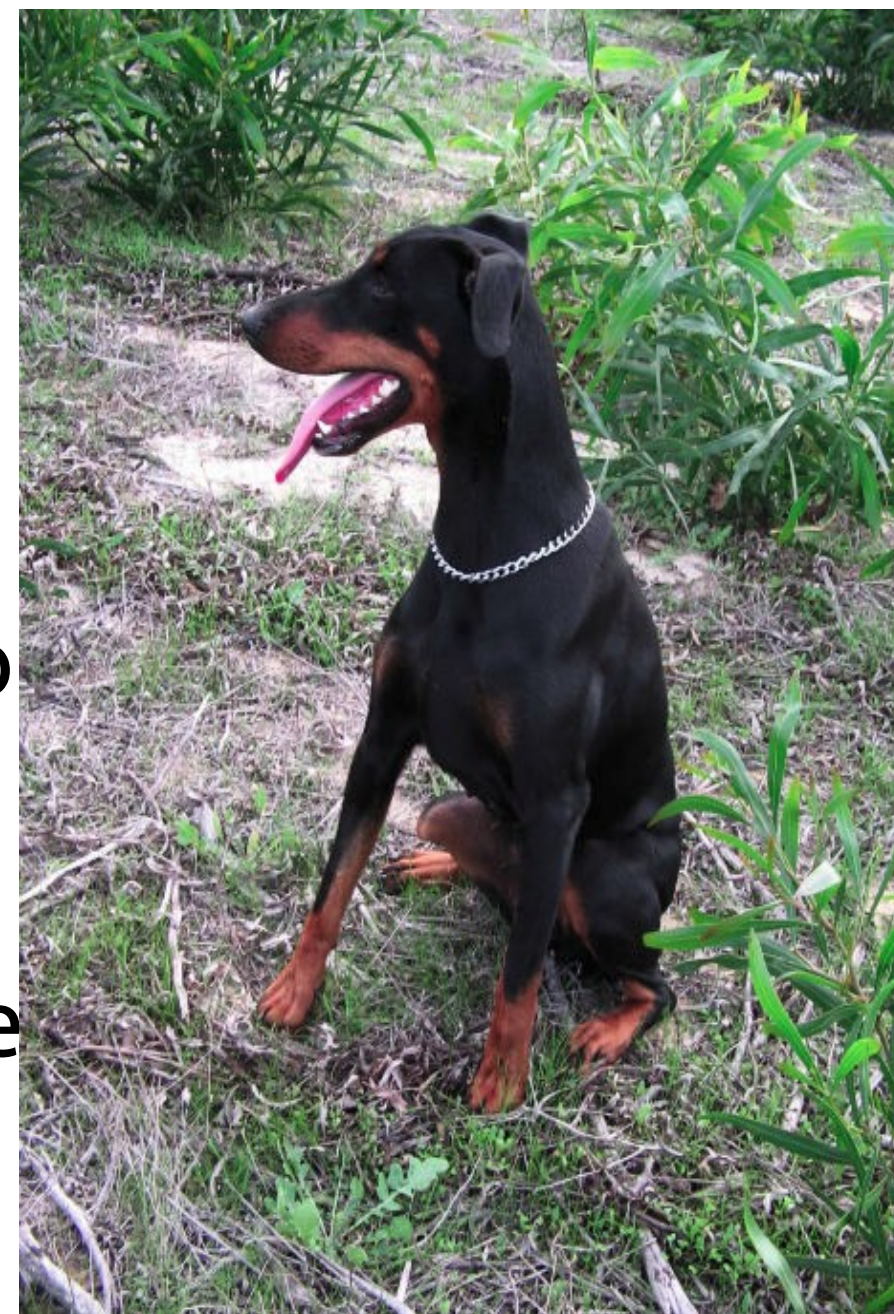


- Indirizzi condivisi (di natura non privata)
commerciale@società.it
- Attribuzione (facoltativa) di un'e-mail personale
- Policy per le risposte automatiche
- Individuazione di un "fiduciario" che verifichi il contenuto delle mail in caso di assenza prolungata o non prevista del lavoratore interessato e di improrogabili necessità legate all'attività lavorativa



I controlli datoriali

- Considerati come *extrema ratio*
 - Da adottare con gradualità
 - Devono essere preceduti da verifiche a livello di gruppi di lavoro reparto etc.
 - Devono essere preceduti da un richiamo all'osservanza delle regole
 - I controlli individuali costituiscono l'eccezione



I controlli datoriali

- E' sempre illecito il trattamento effettuato mediante sistemi hardware e software preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire l'attività di lavoratori



Controlli e biometria

Il Garante non ama i controlli biometrici

Garante Privacy , verifica preliminare
17.11.2010

<http://goo.gl/Cbt10>

Le imprese che intendono adottare sistemi di lettura delle impronte digitali per verificare la presenza in servizio dei dipendenti devono prima dimostrare che le finalità di controllo non possano essere realizzate con sistemi meno invasivi



E i social network?

Social network e recruitment

La maggior parte degli HeadHunter ricerca dati ed informazioni sul candidato prima di decidere in merito alla sua assunzione (LinkedIn, Facebook 123people, etc)

...ma pochi lavoratori hanno consapevolezza del fatto che ciò che si pubblica in rete può avere influenza sulle sue prospettive di lavoro



Signs of the social networking times.

Social network e recruitment

Le informazioni sono potenzialmente “utili” ai fini disciplinari e, anche, penali

E' possibile, infatti, comprendere se un lavoratore si trova effettivamente a lavoro (geotag) o se stia semplicemente perdendo tempo, o se stia diffondendo informazioni riservate dell'azienda, o se stia diffamando il suo datore di lavoro...

Social network e limiti...

I dati e le informazioni inserite dal lavoratore sul social network rappresentano “dati di cui è vietata l'indagine”?

Evidentemente sì... se si tratta di opinioni politiche, religiose o sindacali del lavoratore, nonché di informazioni relative a fatti non rilevanti ai fini della valutazione dell'attitudine professionale



Privacy e lavoro



Le regole per il corretto trattamento dei dati personali dei lavoratori da parte di soggetti pubblici e privati



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

La videosorveglianza

Provvedimento del Garante

Il Garante ha emanato il 29 aprile 2004 un primo provvedimento in tema di videosorveglianza.

Il Garante, in considerazione sia dei numerosi interventi legislativi in materia, sia dell'ingente quantità di quesiti, segnalazioni, reclami e richieste di verifica preliminare in materia sottoposti a questa Autorità, ed anche avuto riguardo alle disposizioni di legge hanno attribuito ai sindaci e ai comuni specifiche competenze volte a garantire l'incolumità pubblica e la sicurezza urbana, ha emanato un nuovo Provvedimento in materia di videosorveglianza, dell' 8 aprile 2010, sostitutivo del precedente

<http://www.garanteprivacy.it/garante/doc.jsp?ID=1712680>

Principi generali

- Principio di liceità

- «I soggetti pubblici, in qualità di titolari del trattamento (art. 4, comma 1, lett. f), del Codice), possono trattare dati personali nel rispetto del principio di finalità, perseguendo scopi determinati, espliciti e legittimi (art. 11, comma 1, lett. b), del Codice), **soltanto per lo svolgimento delle proprie funzioni istituzionali**. Ciò vale ovviamente anche in relazione a rilevazioni di immagini mediante sistemi di videosorveglianza»

Principi generali

- Principio di liceità

- «l'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili, quali ad es. le **vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, sul controllo a distanza dei lavoratori, in materia di sicurezza presso stadi e impianti sportivi...**»

Principi generali

- Principio di necessità
 - « ciascun sistema informativo ed il relativo programma informatico vengano conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi (es., configurando il programma informatico in modo da consentire, per monitorare il traffico, solo riprese generali che escludano la possibilità di ingrandire le immagini e rendere identificabili le persone)»

Principi generali

- Principio di proporzionalità
 - L'attività di videosorveglianza deve essere effettuata «nel rispetto del c.d. principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite (art. 11, comma 1, lett. d) del Codice)»

Principi generali

- Principio di finalità
 - « Gli scopi perseguiti devono essere determinati, espliciti e legittimi. Ciò comporta che il titolare possa perseguire solo finalità di sua pertinenza. ».
 - « possono essere perseguite solo finalità determinate e rese trasparenti, ossia direttamente conoscibili attraverso adeguate comunicazioni e/o cartelli di avvertimento al pubblico. Le finalità così individuate devono essere correttamente riportate nell'informativa. »

Informativa e videosorveglianza

- Gli interessati devono essere informati che stanno per accedere o che si trovano in una zona videosorvegliata e dell'eventuale registrazione, anche nei casi di eventi e in occasione di spettacoli pubblici (es. concerti, manifestazioni sportive)
- In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, vanno installati più cartelli.



Modello di cartello informativo



Modello di cartello informativo per sistemi privati collegati alle Forze di Polizia



Verifica preliminare

Il provvedimento generale in tema di videosorveglianza prescrive a tutti i titolari di sottoporre alla verifica preliminare del Garante i sistemi di videosorveglianza che prevedono una raccolta delle immagini collegata e/o incrociata e/o confrontata con altri particolari dati personali (ad es. biometrici), ovvero i sistemi c.d. intelligenti, che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli.

Anche l'allungamento dei tempi di conservazione oltre i sette giorni deve essere sottoposto a verifica preliminare (a meno che non derivi da una specifica richiesta dell'autorità giudiziaria o di polizia giudiziaria in relazione a un'attività investigativa in corso)

Durata della conservazione delle immagini

L'eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario - e predeterminato - a raggiungere la finalità perseguita

La conservazione deve essere limitata a poche ore (al massimo 24) salve specifiche esigenze di ulteriore conservazione, in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

Le registrazioni effettuate dai Comuni per finalità di tutela della sicurezza urbana, come vedremo, possono essere conservate per sette giorni

Nei casi in cui si voglia procedere alla conservazione delle immagini per un periodo superiore alla settimana, occorre richiedere la verifica preliminare al Garante (salvo che l'esigenza non derivi da specifica richiesta dell'Autorità giudiziaria)



Videosorveglianza e droni



Droni & controllo a distanza dei lavoratori



Mancata osservanza del provvedimento del Garante

- Al mancato rispetto delle disposizioni del Garante in tema di videosorveglianza può conseguire:
 - l'inutilizzabilità dei dati personali trattati in violazione della relativa disciplina;
 - blocco o di divieto del trattamento disposti dal Garante;
 - applicazione delle pertinenti sanzioni amministrative o penali

LA PAROLA ALL'AVV. MICOZZI (PER L'AMMINISTRATORE DI SISTEMA)



DOMANDE??

Grazie per l'attenzione



Salvo dove diversamente indicato, quest'opera è distribuita con licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo 3.0 Unported.

Per ottenere la versione in formato modificabile
contattare l'autore
Avv. Giovanni Battista Gallus

gallus@gm-lex.eu



[@gbgallus](https://twitter.com/gbgallus)

