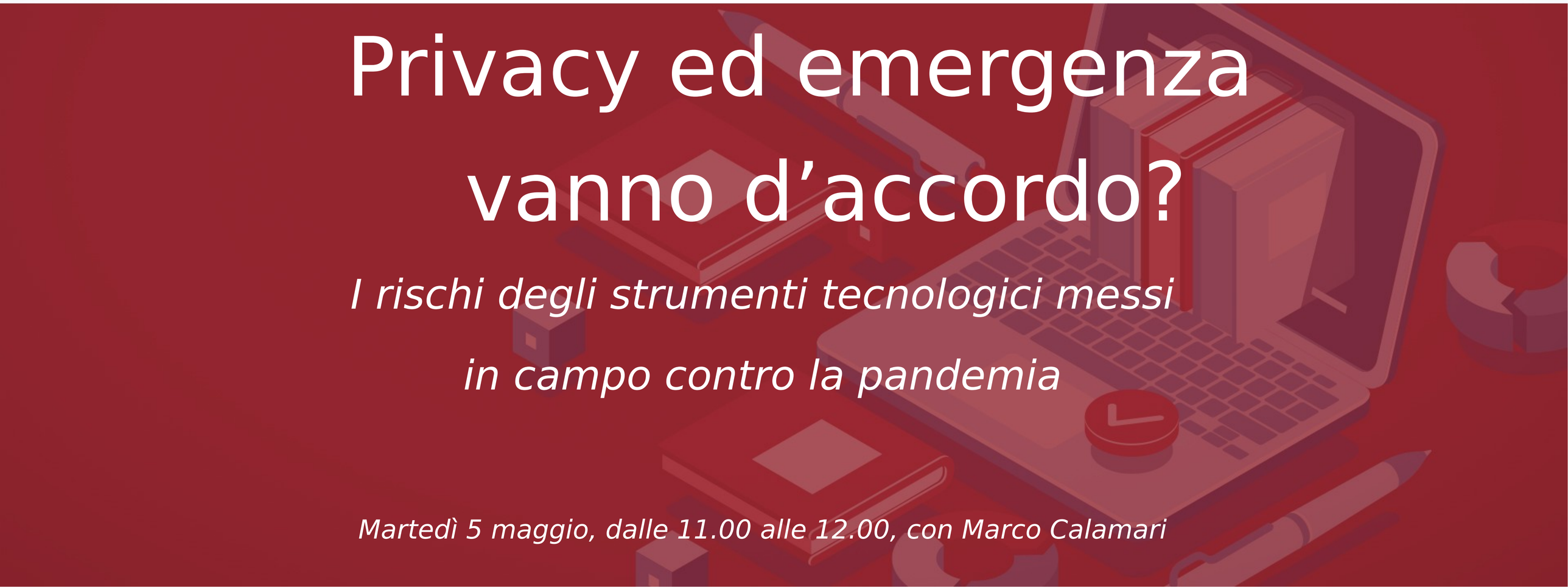
associazione stampa romana

L'UNICO SINDACATO CHE TUTELA I TUOI DIRITTI

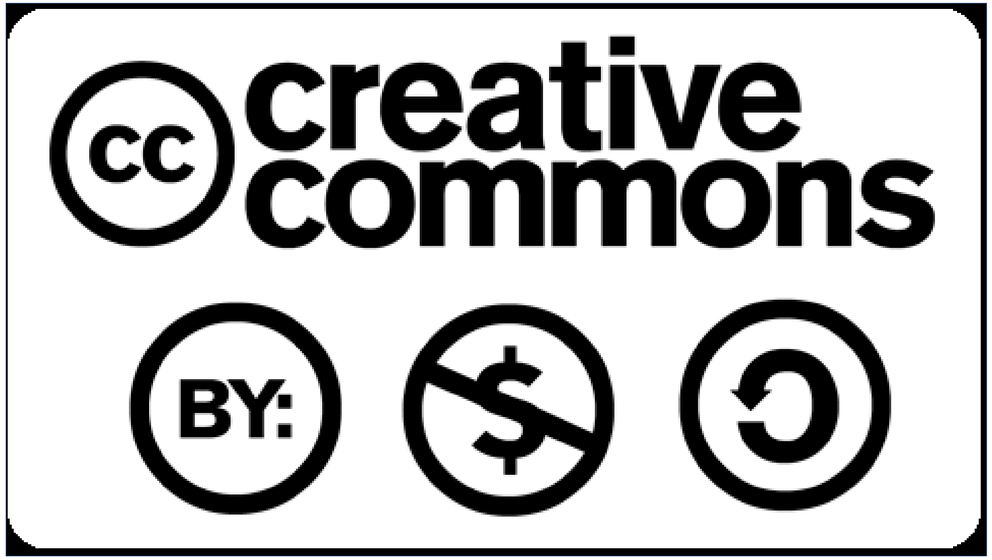
#FORMAZIONECONTINUA

Privacy ed emergenza vanno d’accordo?

I rischi degli strumenti tecnologici messi in campo contro la pandemia



Martedì 5 maggio, dalle 11.00 alle 12.00, con Marco Calamari



Marco A. L. CALAMARI – marco.calamari@ordineingegneripisa.it
ONIF *– Osservatorio Nazionale Informatica Forense*
PWS *– Progetto Winston Smith*

Short bio

Marco Calamari, classe 1955, ingegnere nucleare, ha operato fin dal 1986 nell'ITC in ambito multinazionale come architetto di applicazioni, specializzato in gestione di programmi legacy. Oggi si cimenta a rotazione in attivita' di Computer Forensics, editoriali e di formazione.

Attivista per i diritti civili digitali ed appassionato di privacy e crittografia, ha contribuito ai progetti FOSS Freenet, Mixmaster, Mixminion, Tor e Globaleaks.
Dal 2003 tiene su ZeusNews.it, Punto-Informatico.it ed altre riviste la rubrica Cassandra Crossing, che ha superato le 450 uscite. (www.cassandracrossing.org).

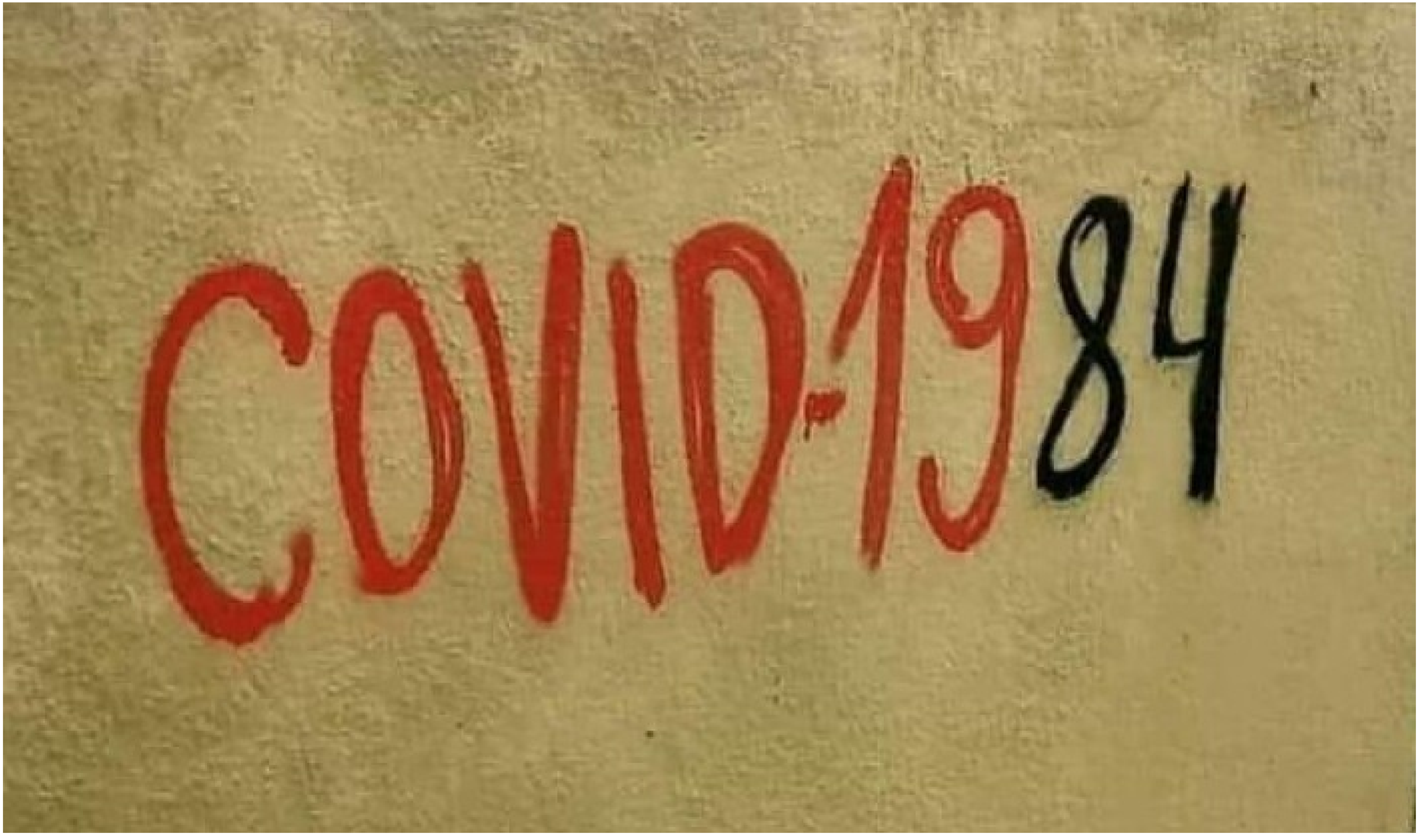
Piu' volte ospite e relatore al Festival Internazionale del Giornalismo, ha creato nel 2002 il convegno nazionale e-privacy, giunto quest'anno alla XXVII Edizione (15 e 16 maggio, online).

Fondatore del *Progetto Winston Smith*
Co-fondatore e fellow dell'*Hermes center for Transparency and Digital Human Right*.
Affiliazioni: IISFA, ONIF, AIP, Opsi, Hermes Center, PWS

Privacy ed emergenza vanno d'accordo?

NO!

Non possono andare d’accordo durante questa pandemia come non sono mai andati d’accordo durante tutte le “emergenze” del recente passato.
Dobbiamo noi farle andare d’accordo.


COVID-1984

Covid-1984

La risposta alla domanda che ci poniamo oggi, condensata in una sigla.
Ma si tratta di una visione Storica, Distopica, o semplicemente Paranoica?

Storica certamente
“Chi non conosce la storia è condannato a ripeterla."
(Jorge Agustín Nicolás Ruiz de Santayana y Borrás, non Tommaso Campanella)

Distopica anche, non solo perché è la realtà ad essere distopica, ma perché
“A pensar male degli altri si fa peccato ma spesso ci si indovina.”
(Giulio Andreotti, ma originariamente Pio XI)

Paranoica? Certamente, ma non per questo meno veritiera.
“La paranoia è una virtù ed i paranoici sono degli inguaribili ottimisti.”
(motto: Progetto Winston Smith)

Storia

1990 - ITAR applicata a PGP e tecnologie crittografiche.

2000 – Copyright imposto con misure tecnologiche.

2010 – 9/11 - contrasto al terrorismo con tecniche di intercettazione planetaria.

2020 – Pandemia – contrasto tramite contact tracing e tecnocontrollo sociale ?

199x - ITAR

Nel 1991 Phil Zimmermann scrive e pubblica in Rete PGP – Pretty Good Privacy, un programma di crittografia forte, che al tempo nemmeno la NSA - National Security Agency statunitense poteva violare.

Zimmermann fu indagato dall'FBI per 4 anni a causa dell'ITAR - International Traffic in Arms Regulations, per esportazione di tecnologie crittografiche, in essa considerate "munitions", cioè parificate ad armamenti.

Nel 1996 l'indagine ebbe termine dopo che il codice sorgente di PGP fu "esportato" legalmente come libro stampato con ISBN, e quindi protetto da *norma superiore*, cioè dal Primo Emendamento della Costituzione americana.

L'ITAR è stata modificata più volte riguardo l'export di tecnologie crittografiche; continua ad essere applicata ancora oggi nei confronti di certe nazioni.

200x - Copyright

A partire dall'inizio di questo millennio le tecnologie informatiche sono state utilizzate in maniera crescente, anche per imporre in maniera coercitiva il rispetto delle leggi riguardanti lo sfruttamento commerciale del diritto d'autore.

Spesso all'insaputa degli utenti-consumatori, le tecnologie DRM – Digital Rights Management systems sono state adottate per la distribuzione ed il commercio di testi, opere audiovisuali e software.

Oltre ad una riduzione della circolazione della conoscenza, ed al mantenimento di rendite di posizione di tipo finanziario, in campo legale ha rimosso, per gli utenti-consumatori, valori-diritti come il "*diritto di primo acquisto*".

In campo informatico ha reso in molti casi illegale il *reverse engineering* e l'analisi di software proprietario, non solo DRM ma firmware e sistemi operativi.

201x - 9/11

Pur essendo precedentemente praticate dalla NSA, e presumibilmente anche da agenzie governative di altri stati, come il GCHQ inglese, il GUOANBU cinese ed il GRU russo, l'11 settembre negli Stati Uniti ha provocato un aumento esplosivo delle operazioni di intercettazione e controllo degli abitanti dell'intero pianeta.

Come le rivelazioni di Edward Snowden nel 2013 hanno provato oltre ogni dubbio, in questo decennio la NSA ha realizzato infrastrutture tecnologiche e capacita' elaborative tali da poter intercettare l'intera Internet e tutti gli altri mezzi di comunicazione di massa. Ha anche acquisito la capacità di memorizzare, elaborare e ricercare le informazioni di tutti gli abitanti "*connessi*" del pianeta.

Malgrado le rivelazioni di Snowden, nella sostanza ben poco è stato fatto contro questi eccessi. Malgrado iniziative legali come il GDPR tutelino maggiormente la privacy delle persone, il trend di "*estrazione ed intercettazione*" di dati personali è tuttora in forte crescita, sia per operazioni *riservate* che per scopi commerciali.

202x - Pandemia

Ampiamente annunciata da un ventennio, e preceduta da una serie di "*pandemie minori*", due solo in questo millennio, SARS (2002) e MERS (2012), la pandemia CoViD-19 ha trovato impreparati i sistemi sanitari dei paesi sviluppati.

Previsioni precise sulla pandemia erano state diffuse negli ultimi venti anni da agenzie dell'ONU, da virologi ed epidemiologi di tutto il mondo, da scrittori, registi ed autori di serie televisive.
Ma invano. Sento molto a me vicine queste moderne "Cassandre"!

Nessuno credeva seriamente, od almeno era disposto ad investire soldi veri, nel contrasto ad un ipotetico nuovo virus che fosse stato allo stesso tempo mortale, senza immunità pregresse ed estremamente contagioso.

Ora, mentre le fosse si riempiono, la ricerca di nuovi strumenti funzionanti, od almeno di immediato impatto mediatico, per contrastare il virus è la priorità.

202x - Pandemia

Se la storia ci ha insegnato qualcosa è che gli eventi storici si ripetono, particolarmente quando i motivi pratici e gli interessi geopolitici che li hanno provocati sono ancora ben presenti.

Durante e dopo questa pandemia, le intercettazioni di massa ed il tecnocontrollo sociale, già largamente praticati sia nei paesi "*diversamente democratici*" che in quelli a "*democrazia compiuta*", certamente avranno un fortissimo sviluppo.

Dubitare di un evento così provato e prevedibile, come d'altra parte era l'arrivo della pandemia stessa, sarebbe così ingenuo da non essere etico.

La cosa più pericolosa di questa "ondata" di nuovo tecnocontrollo non è tecnologica ma sociale; come in passato rischia di essere accettata, anzi richiesta, anzi osannata da un'opinione pubblica terrorizzata ed allo sbando.

2020 - Immuni

Il primo esempio che ci toccherà come cittadini italiani è Immuni, un sistema informatico voluto e commissionato direttamente dal Governo italiano per il tracciamento dei contatti personali, per individuare i possibili contagiati prima che manifestino sintomi, permettendo di trattarli e/o isolarli preventivamente.

Nello storytelling di questo oggetto anzi sistema informatico, vengono utilizzati termini evocativi come *Volontario*, *Anonimo*, *Anonimizzato*, *Pseudonomizzato*.

Senza addentrarci in meandri socio-applicativo-legali, quali immaginare l'utilizzo "*volontario*" di un qualcosa destinato a controllare e dirigere la tua vita, occupiamoci invece dei concetti, molto ben definiti anche se spesso abusati, di anonimato, e di anonimizzazione dei dati.

Anonimato

L’anonimato tecnologico viene garantito con mezzi matematici ed informatici, crittografici, per essere esatti, ma riguarda solo un’informazione ben precisa, cioè l’identità di una persona o pseudo-persona.

E’ quindi una tecnica per celare una sola informazione ben precisa, non per renderla inaccessibile od inutilizzabile.

Possiamo paragonarla, usando la terminologia militare tanto cara allo storytelling della pandemia, ad una difesa perimetrale, ad un confine che si cerca di rendere invalicabile, superato od aggirato il quale non esiste difesa ulteriore che sbarri l’accesso ai dati personali relativi all’identità violata.

In questo modo l’identità viene difesa, ma i dati a cui essa è collegata no.

Anonimizzazione

Un discorso completamente diverso è quello della anonimizzazione dei dati.
In questo caso ciò che si vuole ottenere è l'impossibilità di dedurre, da un insieme di dati personali, l'identità della persona a cui essi appartengono.

Si tratta di un'impresa che è facile sottovalutare, e che al contrario è provatamente difficilissima quando non impossibile.

Facciamo un esempio: i dati di un censimento.

Qualitativamente essi comprendono nome e cognome della persona, indirizzo, dati anagrafici e fiscali, e tutti gli dati che vengono rilevati per scopi censuari. Anonimizzare questi dati sembrerebbe semplice, basta sostituire nome e cognome con un numero d'ordine, creare un secondo archivio dove scrivere a quale numero corrisponde ad un dato nome e cognome, e rendere inaccessibile, magari crittografandolo, questo secondo archivio.

Pseudonomizzazione

Problema risolto? In realtà no.

I dati non sono stati anonimizzati, e sono ancora personali. Sono stati pseudonimizzati, ma le informazioni sull'identita' sono ancora presenti, e possono essere perse, abusate, rubate, leakate …
La mera esistenza di queste informazioni impedisce nei fatti la completa anonimizzazione dei dati.

Un esempio? Ad un sistema di whistleblowing la legge italiana richiede di poter ottenere l'identità del whistleblower. Lo si realizza chiedendogli di rivelare l'identità e poi pseudonimizzandola in un archivio crittografato, accessibile solo ad una terza persona indipendente, che risponde solo alla magistratura.

Esercizio per i discenti:
quale è il punto debole che invalida questo "*whistleblowing pseudononimo*"?

Deanonimizzazione

Per ottenere un reale anonimato dobbiamo quindi rassegnarci a conservare i dati del nostro censimento cancellando del tutto i nomi?
Questo, pur distruggendo il censimento, non renderebbe completamente inutili i dati, che potrebbero essere ancora utilizzati, ad esempio a fini epidemiologici.

Nemmeno questo basta, l'intrinseco dettaglio esistente in questi dati ne permette, in maniera semplice la deanonimizzazione. Ma in quale maniera?
Lo ha esposto per la prima volta Paul Ohm nella sua paper del 2009 "*Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization***".**

In essa, tra l'altro, riferisce come sia addirittura banale deanonimizzare i dati del censimento statunitense del 1990, reidentificando con certezza l'87,1% dei cittadini, utilizzando la combinazione di: codice di avviamento postale, data di nascita e sesso, e confrontandoli con quelli dell'anagrafe pubblica.

Deanonimizzazione

Ma certamente si potrà fare di meglio!

Bene, la corposa ricerca in tema dell'ultimo decennio ci dice di no.

Per rendere un dato personale non anonimo, ma non-deanonimizzabile, lo si deve rendere praticamente inutile, se non per un singolo scopo particolare.

Un esempio? Li si deve aggregare.

Un dato aggregato è, nella maggior parte dei casi, realmente anonimo.
Sapere quanti maschi e quante femmine ci sono in un censimento, buttando via i dati originali, rende il dato aggregato realmente anonimo.

Ma anche inutile per qualsiasi altro scopo.

Contact tracing

E torniamo alla nostra applicazione di contact tracing. E' anonimizzabile?

No.

Quindi, se la realizzazione non è indispensabile, non dovrebbe essere realizzata.

Nel caso essa sia indispensabile, perché la sua efficacia, inserita in un sistema di prevenzione dei contagi che, almeno come progetto e risorse, possa funzionare in pratica, deve essere realizzata sulla base dei principi di necessità e di minimizzazione del trattamento dati.

Non a caso sono i principi alla base del GDPR.

… e quindi ?

I dati non indispensabili non devono essere raccolti.
Quindi niente geolocalizzazione, niente contatti della rubrica e dai social, niente identificativi univoci della persone o IMEI del cellulare (si, niente!).

I dati raccolti non devono essere centralizzati, se non nella misura minima strettamente necessaria, ma lasciati sui dispositivi degli utenti.

I dati raccolti, particolarmente quelli centralizzati, non devono essere trattati in nessun altro modo se non quello previsto dal funzionamento della applicazione.

I dati devono essere cancellati appena possibile, non appena verrà deciso di cancellarli od entro una certa data. Lo deve fare automaticamente l'applicazione.

I dati devono essere custoditi con cura, con precise responsabilità, proprio, non anche, perché sappiamo che questo non sarà comunque sufficiente.

Per concludere

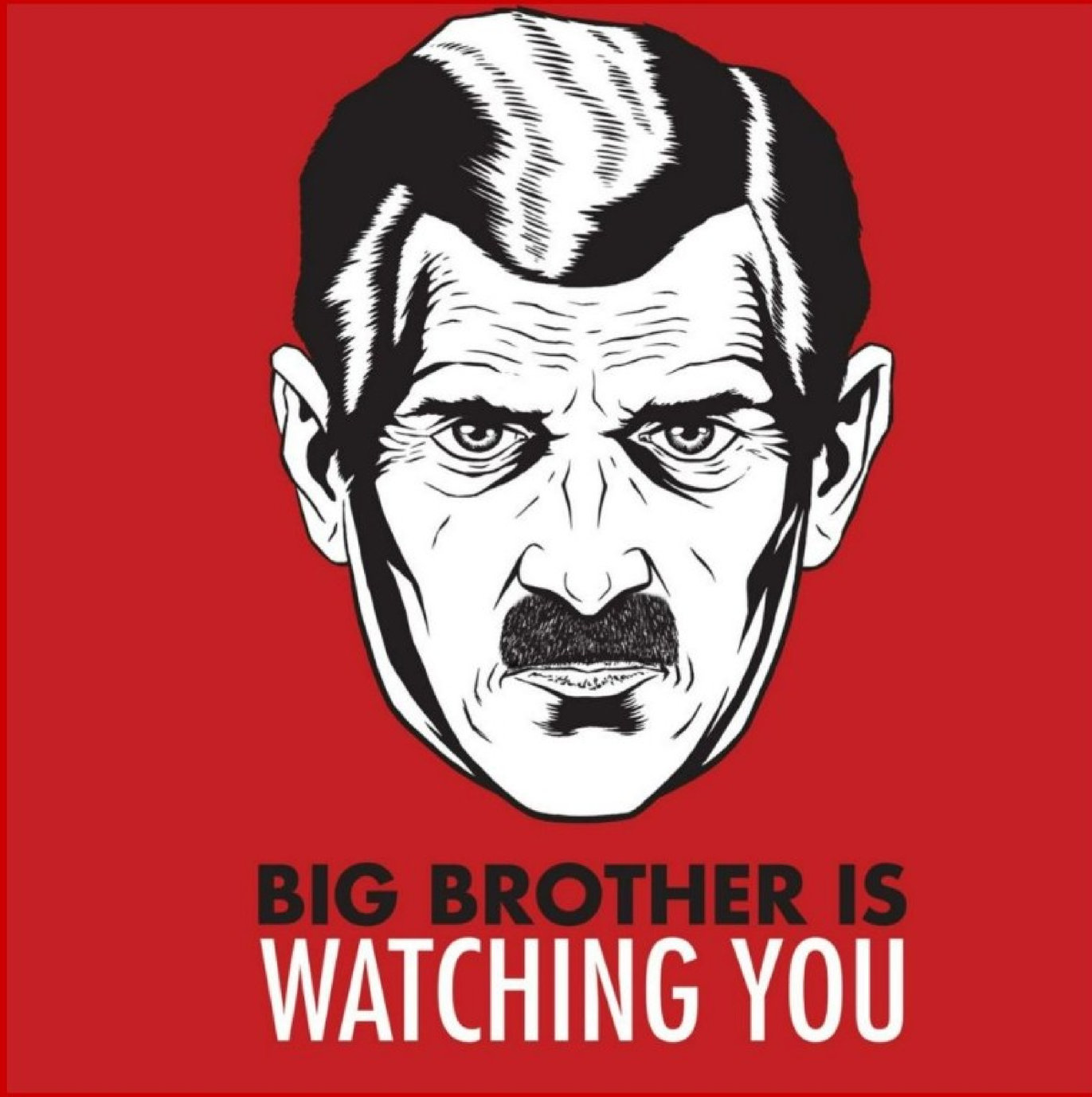
Privacy, anonimato, emergenza e contact tracing possono, anzi devono essere compatibili. Ma è necessario applicare i principi di realismo e di necessità.

Lasciando perdere quello che i poteri esecutivo, legislativo giudiziario ed informatico potranno, vorranno, dovranno e sapranno fare, noi, in quanto "quinto potere", dobbiamo pre-occuparci dello storytelling della pandemia, ed in particolare dei suoi dettagli (il demonio, come sempre, sta nei dettagli).

Quindi dobbiamo non solo evitare ma contrastare la :

- **banalizzazione delle soluzioni tecnologiche e dei problemi di privacy;**
- **descrizione delle soluzioni in termini certi o peggio salvifici;**
- **sottostima od omissione delle possibili conseguenze.**

E fare una lotta senza quartiere alle false dicotomie quali "salute o privacy".


BIG BROTHER IS
WATCHING YOU

Grazie per l'attenzione

+ Marco A. Calamari marco.calamari@ordineingegneripisa.it --+
| |
| PGP RSA: ED84 3839 6C4D 3FFE 389F 209E 3128 5698 |
| DSS/DH: 8F3E 5BAE 906F B416 9242 1C10 8661 24A9 BFCE 822B |
| Tel: (+39) 050 576031 Cell: (+39) 347 8530279 |
| Fax: (+39) 050 7849817 Skype-Twitter: calamarim |
| |
+ P.E.C.: marcoanselmoluca.calamari@ingpec.eu ------------+

associazione stampa romana

L'UNICO SINDACATO CHE TUTELA I TUOI DIRITTI

#FORMAZIONECONTINUA

FINE