Provider of Data Integration Services for Fortune 100 Firms Exposed Sensitive Files

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/bj48tP5CLUc/provider-data-integration-services-fortune-100-firms-exposed-sensitive-files

---

Many Potential Backdoors Found in Huawei Equipment: Study

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/CBmxUm_OAlI/many-potential-backdoors-found-huawei-equipment-study

---

A Foggia la prima Laurea specialistica per formare professionisti della difesa



Il Dipartimento di **Giurisprudenza** dell'Università di **Foggia** ha ottenuto l'accreditamento del nuovo corso di laurea magistrale (della durata di due anni) in Scienze Giuridiche della Sicurezza, primo corso attivato in Italia per formare scientificamente i professionisti della protezione (delle persone, dei luoghi, dei dati e della rete).

"*Abbiamo pensato che fosse arrivato il momento per formare specialisti della sicurezza* – spiega **Donatella Curtotti**, direttore del Dipartimento di Giurisprudenza – *mancando in tutta Italia una laurea specialistica". Il corso di laurea punta così a preparare per il lavoro "nei settori della sicurezza, insegnandogli a prevedere, analizzare, studiare e isolare le più insidiose minacce che vengono ormai dappertutto, dalla rete come dalla nostra stessa società. Insomma* – aggiunge Curtotti – *abbiamo pensato a formare una figura fino ad oggi inesistente, che producesse professionisti indispensabili per la vita di tutti anche nei prossimi decenni".Il titolo di laurea permetterà di partecipare a tutti i concorsi nelle forze di polizia*.

Il nuovo corso di laurea avrà il primo anno comune per tutti gli studenti, improntato principalmente sulla sicurezza delle informazioni e della protezione dei dati (con approfondimenti

sui temi della privacy e i riflessi in ambito giuridico, economico, istituzionale e sociale); poi un secondo anno suddiviso in tre diverse aree alternative: sicurezza delle persone e sul lavoro, sicurezza dei dati aziendali, sicurezza del territorio e dello Stato.

https://www.key4biz.it/a-foggia-la-prima-laurea-specialistica-per-formare-professionisti-della-difesa/263301/

Libra, le Autorità vogliono vederci chiaro. Intanto a Ginevra non esiste (ancora) nessuna Association

Giovanni Buttarelli, Garante Europeo per la Protezione dei dati Personali e **Antonello Soro**, Garante privacy italiano, sono stati i primi a lanciare l'allarme. Adesso **Libra** non convince nemmeno le Autorità del resto del mondo.

Dal **Financial Stability Board** alla **Fed** passando per la **Financial Conduct Authority** è un coro di scetticismo e allerta sulla cripotvaluta di **Facebook** che, è il parere unanime, ha bisogno di un esame attento.

Il motivo è semplice. Una sua introduzione comporterebbe da subito un ampio e diffuso uso a differenza del Bitcoin, dato che Facebook conta quasi 2,4 miliardi di utenti.

In una lettera inviata al G20, il presidente dell'Fsb e vice presidente della Fed **Randal Quarles** mette in guardia sui rischi legati a un uso diffuso delle valute digitali. "*Anche*

se al momento i cryptoasset non rappresentano un rischio per la stabilità finanziaria" un uso diffuso di "nuovi tipi di criptoasset per i pagamenti merita un attento esame da parte delle autorità per assicurare siano soggette a elevati standard di regolamentazione" spiega Quarles, precisando che l'Fsb "*monitorerà i rischi da vicino e in coordinamento con altre autorità*".



Una posizione condivisa dal presidente della Fed, **Jerome Powell**, che ha ribadito l'impegno della banca centrale americana a valutare da vicino Libra. Gli fa eco il numero uno della Fca inglese, Andrew Bailey: "*Dobbiamo impegnarci a livello nazionale e internazionale con facebook e Libra. Non procederanno senza autorizzazione*" dice Bailey, secondo quanto riportato dal Financial Times. Le parole di Bailey sono in linea con quello del governatore della Bank of England, **Mark Carney,** e con quelle dell'Ue, secondo la quale la concentrazione di dati personali e finanziari di Facebook richiede molta attenzione.

Sul fronte politico Libra non convince neanche il Congresso americano, che ha convocato un'audizione sulla criptovaluta in luglio.

Insomma più ombre che luci sul nuovo progetto di **Mark Zuckerberg,** in attesa di ulteriori sviluppi, Facebook che si augura di poter operare Libra senza la rigida regolamentazione delle banche e delle altre società di pagamento, le autorità

rispondono con un secco no.

A Ginevra non c’è nessuno: la scoperta del Sole 24 Ore

E’ di oggi la notizia secondo cui la **Libra Association**, l’Associazione che dovrebbe finanziare e controllare il progetto di Facebook, al momento, non esiste.

Il **Sole 24 Ore** ha scoperto che al numero 13 di *Quai de l’Ile* di **Ginevra** in Svizzera – dove ha sede l’organizzazione – è interamente occupato da **Spaces**, una società di coworking che mette uffici e spazi a disposizione delle società. Non c’è traccia alcuna di Facebook e di Libra ma ci sono i nomi di oltre 30 aziende tra cui PayPal (tra i partner di Libra Association), Aig (compagnia assicurativa Usa) e diverse società tecnologiche.

Inoltre – spiega il quotidiano economico – nel registro del commercio di Ginevra non esiste Libra Association, che non è ancora stata iscritta.

Elka Looks, communications manager di Calibra, società di Facebook che investirà nel progetto, ha spiegato al Sole 24 Ore che “*Facebook avvierà la registrazione alla Camera di commercio di Ginevra nelle prossime settimane e il conferimento dei fondi sarà realizzato nei prossimi mesi e ci attendiamo che sarà completato nel 2020*“.

Per approfondire

https://www.key4biz.it/libra-le-autorita-vogliono-vederci-chiaro-intanto-a-ginevra-non-esiste-ancora-nessuna-association/263203/

French Consumer Group Launches Class Action Against Google

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/pTmrozAvrPs/french-consumer-group-launches-class-action-against-google

Captatori informatici (come i trojan), le osservazioni del Garante Privacy Antonello Soro



Antonello Soro conclude il suo mandato di Presidente dell'Autorità Garante per la protezione dei dati personali (giugno 2012 – giugno 2019).

In questa intervista a **Key4biz**, realizzata dal direttore **Raffaele Barberio,** che traccia il bilancio del Collegio durante il settennato, il Garante Privacy spiega l'utilizzo dei trojan e dei captori informatici durante le intercettazioni.

"*Sono favorevole ai captatori informatici quando davvero indispensabile, ma è un'arma così invasiva da usare con molto rigore e cautela. Per questo* – ha spiegato Soro – *abbiamo, anche di recente, chiesto a Governo e Parlamento di intervenire per regolare l'utilizzo dei trojan in maniera più determinata*".

Per approndire

https://www.key4biz.it/captatori-informatici-come-i-trojan-le-osservazioni-del-garante-privacy-antonello-soro/263052/

Con il trojan si può intercettare anche il cellulare dei parlamentari?

La legge **n. 3 del 9 gennaio 2019** (c.d. “spazza corrotti”), nel modificare gli artt. 266 e 267 del codice di procedura penale, ha ampliato l’utilizzo delle **intercettazioni** anche per i **delitti dei pubblici ufficiali contro la pubblica amministrazione** puniti con la pena della reclusione non inferiore nel massimo a cinque anni.

È noto che tra le diverse forme di intercettazione vi possono essere quelle c.d. “ambientali” cioè quelle in grado appunto di “intercettare” conversazioni tra presenti in un determinato ambiente.

Ultimamente, gli strumenti in uso sono diversi e tra questi grande risalto mediatico (dopo il caso del **CSM**) è stato rivolto ai *trojan*.

Grazie ai *trojan* qualsiasi apparato telefonico mobile può diventare uno strumento di intercettazione ambientale.



Tra le varie criticità dell'uso dei ***trojan*** **come intercettazione,** possiamo tenere in considerazione due temi principali.

Il primo, ovviamente, riguarda la tutela dei dati personali

Invero, già con deliberazione del luglio 2016 il CSM aveva recepito le migliori prassi da seguire in caso di compilazione dei "brogliacci" e cioè quello di evitare che venissero annotate "intercettazioni irrilevanti" (cioè intercettazioni palesemente estranee alle esigenze investigative e/o processuali, alla dimostrazione dei fatti costituenti reato e alla relativa responsabilità) capaci però di divulgare e quindi trattare dati personali senza alcuna valida base giuridica e talvolta a divulgare dati particolari (ex sensibili) irrilevanti ai fini delle indagini.

Sul punto il CSM, nella citata deliberazione, aveva stilato un protocollo virtuoso per effettuare quella attività di filtro per la connaturale esigenza di ricercare il giusto equilibrio tra valori costituzionali, nessuno dei quali è tanto prevalente da imporre automaticamente il sacrificio dell'altro.

Ultimamente, il ricorso ai *trojan* come strumento di intercettazione è stato ampiamente criticato dallo stesso Garante.

Nei vari interventi sul caso "**exodus**", Soro ha avuto modo di affermare che *"E' un fatto gravissimo. La notizia dell'avvenuta intercettazione di centinaia di cittadini del tutto estranei ad indagini giudiziarie, per un mero errore nel funzionamento di un captatore informatico utilizzato a fini investigativi, desta grande preoccupazione e sarà oggetto dei dovuti approfondimenti, anche da parte del Garante, per le proprie competenze. La vicenda presenta contorni ancora assai*

incerti ed è indispensabile chiarirne l'esatta dinamica…Ciò che, tuttavia, emerge con evidenza inequivocabile è la notevole pericolosità di strumenti, quali i captatori informatici, che per quanto utili a fini investigativi rischiano, se utilizzati in assenza delle necessarie garanzie anche soltanto sul piano tecnico, di determinare inaccettabili violazioni della libertà dei cittadini…Tali considerazioni erano state da noi rivolte al Governo, in sede di parere tanto sullo schema di decreto legislativo di riforma della disciplina intercettazioni che ha normato il ricorso ai trojan, quanto sullo schema di decreto attuativo che avrebbe, appunto, dovuto introdurre garanzie adeguate nella scelta dei software da utilizzare. E' indispensabile trarre, da questa vicenda, la determinazione necessaria per impedire ulteriori violazioni in futuro, nella consapevolezza di come non possano tollerarsi errori in un campo così sensibile, perché incrocia il potere investigativo e il potere, non meno forte, della tecnologia. Strumenti investigativi così delicati devono certamente essere disponibili gli organi inquirenti come prevede la legge, ma nel rispetto di garanzie elevate per tutelare la libertà dei cittadini"

Il secondo tema ha profili prettamente processuali di utilizzabilità delle intercettazioni da *trojan*

Invero, il richiamato caso del CSM ha evidentemente sottolineato che uno dei vari pericoli dell'**intercettazione** (diremmo "indiscriminata") è che questa **possa essere dichiarata inutilizzabile,** laddove ad esempio si verifichino intercettazioni di conversazioni di parlamentari.

Infatti, il regime previsto dalla Legge 20 giugno 2003, n. 140 in merito art. 68 Cost. distingue le **intercettazioni del**

parlamentare in “**dirette**“, “**indirette**“, “**casuali o fortuite**” (sulla distinzione fra intercettazioni “*dirette*”/”*indirette*”, da una parte, e “*casuali*” o “*fortuite*”, dall’altra, si possono citare le seguenti sentenze della Corte Costituzionale n. 114 e n. 113 del 2010, n. 390 del 2007; ordinanza n. 263 del 2010).

Sappiamo che per poter intercettare direttamente o indirettamente un parlamentare, deve essere richiesta **l’autorizzazione preventiva**, **a pena di inutilizzabilità**, alla Camera di appartenenza.

In quelle c.d. “casuali o fortuite”esse non andrebbero immediatamente trascritte, ma *meramente indicate* nel brogliaccio con la dicitura “***conversazione casualmente captata con parlamentare***”, dandone immediata informativa al pubblico ministero per le sue valutazioni, cioè per verificare se le intercettazioni siano in realtà indirette o dirette e quindi potenzialmente inutilizzabili ovvero sia necessaria **un’autorizzazione successiva**.

Invero, nel caso di intercettazioni casuali è prevista la possibilità di **autorizzazione successiva** a mente dell’art. 6 della Legge 20 giugno 2003, n. 140, laddove sia necessario utilizzare contro il parlamentare quelle intercettazioni già acquisite e rispetto alle quali, proprio per il carattere imprevisto dell’interlocuzione del parlamentare, l’autorità giudiziaria non avrebbe potuto, neanche volendo, munirsi preventivamente dell’autorizzazione della Camera d’appartenenza.

Incidentalmente, deve essere chiarito che le intercettazioni seppur inutilizzabili per il parlamentare sono perfettamente producibili nel processo riguardanti il terzo, cioè il soggetto intercettato insieme al parlamentare (sul tema si veda Corte di Cassazione Penale, Sez. II, ud. 16.11.2012, dep. 22.2.2013, n. 8739)

A questo punto è bene considerare che anche l'intercettazione da *trojan* deve rispettare le tutele di protezione delle comunicazioni e conversazioni del parlamentare.

Seguendo la lettura costituzionalmente orientata offerta dalla recente sentenza n. 38/2019 della Corte Costituzionale sull'art. 68, terzo comma, Cost. (sul tema dei tabulati telefonici riguardante un parlamentare); potremmo considerare applicabile tale impianto argomentativo anche all'utilizzo dei *trojan* (equiparabile in tutto e per tutto ad intercettazioni vecchio stile) e per la quale deve essere sempre richiesta alla Camera, alla quale il parlamentare appartiene o apparteneva, l'autorizzazione ad utilizzare le conversazioni o comunicazioni intercettate, anche frutto di procedimenti riguardanti terzi.

Sul punto osserviamo che l'art. 68 costituisce una maggiore garanzia della libertà e della segretezza di ogni forma di comunicazione, già assicurata dall'art. 15 Cost.

Invero, la *ratio* della garanzia prevista all'art. 68, terzo comma, Cost. non mira a tutelare un diritto individuale (la riservatezza del parlamentare), ma a proteggere la libertà della funzione che il parlamentare esercita, in conformità alla natura stessa delle immunità parlamentari, volte primariamente alla protezione dell'autonomia e dell'indipendenza decisionale delle Camere rispetto ad indebite invadenze di altri poteri, e solo strumentalmente destinate a riverberare i propri effetti a favore delle persone investite della funzione (sentenza Corte Costituzionale n. 9 del 1970).

Inoltre, l'art. 68, terzo comma, Cost. stabilisce chiaramente la necessità dell'autorizzazione della Camera d'appartenenza «per sottoporre i membri del Parlamento ad intercettazioni, in qualsiasi forma, di conversazioni o comunicazioni e a sequestro di corrispondenza».

Si tratta, in tal caso, di un'autorizzazione preventiva, che precede il compimento dell'atto d'indagine.

La Corte Costituzionale (nella sentenza n.38/2019) ha, poi, precisato che l'autorizzazione deve essere preventivamente richiesta non solo se l'atto d'indagine sia disposto direttamente nei confronti di utenze intestate al parlamentare o nella sua disponibilità (intercettazioni cosiddette "**dirette**"), ma anche tutte le volte in cui la captazione si riferisca a utenze di **interlocutori abituali del parlamentare**, **o sia effettuata in luoghi presumibilmente da questo frequentati**, al precipuo scopo di conoscere il contenuto delle conversazioni e delle comunicazioni del parlamentare stesso.

Ai fini della richiesta preventiva dell'autorizzazione, ciò che conta, in altre parole, non è la titolarità dell'utenza o del luogo, ma la direzione dell'atto d'indagine (sentenza Corte Costituzionale n. 390 del 2007).

Come ricordato dalla stessa Corte Costituzionale (sentenza n.38/2019) la tutela della corrispondenza di cui all'art. 15 Cost. riguarda tutti i soggetti dell'ordinamento, e deve riguardare anche i **dati "esterni"** di una comunicazione cioè quei dati ricavabili da qualsiasi strumento che consente, in virtù dell'evoluzione tecnologica, il tracciamento di localizzazioni e spostamenti dei titolari di apparati mobili.

Ancora, il significato da attribuire a «conversazioni o comunicazioni», induce a ritenere che al contenuto di una conversazione o di una comunicazione, siano accostabili, e risultino perciò protetti dalle garanzie costituzionali, anche i dati puramente storici ed esteriori, in quanto essi stessi "fatti comunicativi".

Del resto, il termine «comunicazioni» ha, tra i suoi comuni significati, quello di «contatto», «rapporto», «collegamento», evocando proprio i dati.

Pertanto, il *trojan* (come già argomentato per il "tabulato

telefonico” nella citata sentenza n.38/2019) può aprire squarci di conoscenza sui rapporti di un parlamentare, specialmente istituzionali, «di ampiezza ben maggiore rispetto alle esigenze di una specifica indagine e riguardanti altri soggetti (in specie, altri parlamentari) per i quali opera e deve operare la medesima tutela dell’indipendenza e della libertà della funzione» (sentenza Corte Costituzionale n. 188 del 2010).

https://www.key4biz.it/con-il-trojan-si-puo-intercettare-anche-il-cellulare-dei-parlamentari/262991/

Libra, William Nonnis (Ministero della Difesa): ‘Non chiamatela criptovaluta. Ci sarà una grossa svendita di dati personali’

Dopo il lancio di **Libra** da parte di **Facebook**, abbiamo chiesto a **William Nonnis,** Full Stack & Blockchain Developer del Ministero della Difesa, cosa ne pensa del progetto di **Mark Zuckerberg** che entrerà in funzione nel 2020.

In foto William Nonnis – Full Stack & Blockchain Developer – del Ministero della Difesa, fa parte dello staff tecnico di Italian Open Lab per lo studio, progettazione e sviluppo su Blockchain, AI, IoT e Applicazioni WEB sempre per il Ministero della Difesa. Inoltre è Member of Focus Group UNINFO

(CEN/CENELEC) Blockchain DLT, e del Consiglio Nazionale di Italia4Blockchain

Key4biz. ***Che cosa sarà "Libra?***

William Nonnis. Libra ha il merito di dare rilevanza ed attirare l'attenzione sull'argomento crypto, tanto da farlo notare a livello istituzionale. Ma, come redatto nella White Paper, ricordiamo che Libra non è una moneta, né una crypto, né una Blockchain.

Piuttosto é un sistema di pagamento estremamente comodo per acquistare, con il risparmio privato, il debito pubblico mondiale, quindi è sbagliato chiamarla moneta digitale o cryptovaluta. Anche perchè libra non sarà basata su blockchain pubblica (l'unica che garantisce assoluta trasparenza e tracciabilità di transazione) posto che le informazioni saranno visibili solo a chi appartiene alla rete stessa. I puristi di criptovaluta sostengono che il progetto della #Libra è l'antitesi del concetto di bitcoin, muovendo un'altro passo verso il controllo totale dei dati e degli utenti.

Key4biz*. Quali gli svantaggi e i rischi? Chi la controlla?*

William Nonnis. Svantaggi: secondo il mio punto di vista ci sarà una grossa svendita di dati personali, mettendo così fortemente a rischio privacy e tutela del cittadino. Gli sviluppatori sostengono che i dati personali non verranno tenuti sugli utilizzatori di Libra ed anche i vertici di Facebook hanno assicurato che la piattaforma non tratterà o farà affari né con i big data acquisiti, anche se solo momentaneamente, né con le transazioni avvenute sulla sua app Calibra. Ma, diversamente da ciò che avviene con il Bitcoin, identità e password degli utilizzatori della app saranno comunque registrate da terzi. Sostanziale è tale diversità rispetto al sistema Bitcoin, dove i dati sensibili degli utenti sono assolutamente anonimi e tali devono rimanere per

preservarli da sottrazioni illecite di criptovalute.

Su chi la controlla invece voci ancora non ufficiali sostengono sarà **Libra Association**, ma io ne dubito fortemente perché ritengo che tutti i partner vorranno acquisirne, e quindi controllarne, i contenuti che LIBRA conterrà, almeno in parte.

Key4biz*. Che cosa ha in comune con i bitcoin?*

William Nonnis. Nulla di nulla perché come già ribadito, bitcoin è una crypto basata su blockchain atta a favorire un'economia circolare e non è assolutamente controllata da nessuno. Libra, a differenza del Bitcoin, non viene "estratta" dalla rete attraverso i procedimenti informatici di mining ma viene "emessa" attraverso l'acquisto di titoli di Stato e l'uso di depositi bancari.

Key4biz*. Come sarà garantita la sicurezza delle transazioni?*

William Nonnis. I vertici di Facebook, avendo registrato **Calibra**, la nuova società sussidiaria di pagamenti e monetica, negli Usa, presso il **Financial Crimes Enforcement Network** (FinCEN), hanno potuto rendere il sistema operativo in tutti i suoi 50 stati Poiché la FinCEN è l'organo del Dipartimento del Tesoro degli Stati Uniti, dedito al controllo dei reati finanziari, che raccoglie dati e informazioni sulle transazioni economiche, per combattere riciclaggio di denaro, sovvenzionamento al terrorismo e altri crimini finanziari nazionali e internazionali, con tale registrazione Facebook si è resa garante de "la separazione tra dati sociali e finanziari" sostenendo che "costruirà e gestirà i propri servizi sulla rete Libra" nel rispetto delle norme antiriciclaggio.

Key4biz. E come saranno garantite le riserve di Libra?

William Nonnis. A quanto dicono gli ideatori, la Libra sarà garantita da una riserva di asset reali per assicurarne la

stabilità e per proteggerla dalla speculazione. Solo il tempo, comunque, potrà dimostrare la veridicità di tale asserzione.

Key4biz*. Come sarà garantita la privacy?*

William Nonnis. Zuckerberg sostiene che per ora l'interesse è dedicato ai dati di chi acquista piuttosto che alla gestione del denaro digitale.

Assolutamente vero, soprattutto perchè la reale fonte di guadagno oggi per tutte le grandi società sono proprio i dati. Ma, specificatamente su questo punto, ritengo che Libra (Facebook) debba prestare molta attenzione e muoversi con estrema cautela, dati i recenti scandali che hanno investito la **Cambridge Analitycs**. Gli esperti di privacy esprimono infatti molti dubbi sulle rassicurazioni di Facebook di non indirizzare gli annunci pubblicitari utilizzando informazioni finanziarie sensibili.

Key4biz*. Facebook può diventare così la superbanca 4.0? Cosa rischia il sistema bancario tradizionale?*

William Nonnis. Non ritengo, al momento, ci siano i presupposti per avallare tale ambizione, seppure già Facebook dispone della licenza in Europa per esercitare le funzioni di banca. Si dovrà attendere, infatti, la risposta dei singoli stati e la fiducia data dalle banche tradizionali, ma soprattutto desta interesse la replica delle aziende digitali come **Amazon, Google** e altri che, proprio come Facebook, hanno facoltà di esercizio in qualità di istituto bancario in europa. Non a caso per ora nell'associazione che gestirà lo sviluppo di Libra, non appare nessuna delle altre "temibili cinque" aziende.

Key4biz. *Cos'altro vuole aggiungere?*

William Nonnis. Personalmente ritengo che una reale, concreta e radicale novità per la collettività e, addirittura, un cambiamento di paradigma socio-culturale, potrà avvenire solo

adottando il modello stabilito da **Satoshi Nakamoto**, e cioè quello di una Blockchain pubblica con relativa economia circolare. Solo allora la rivoluzione tecnologica sarà veramente avvenuta e potrà dare il via a quello che a me piace definire il “buon futuro” che auguro a ciascuno di noi grazie al sussidio di una tecnologia pulita e trasparente.

https://www.key4biz.it/libra-william-nonnis-difesa-rischio-privacy-non-chiamatela-criptovaluta/262808/

Flaw in Outlook for Android Allows for Data Theft

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/bowJrPqhFxI/flaw-outlook-android-allows-data-theft

---

Gdpr & Privacy: consapevolezza e opportunità. Analisi ragionata della protezione dei dati personali tra etica e cybersecurity

La presentazione ufficiale è fissata per il 28 giugno 2019, nell’evento di Privacy Italia, organizzato in una *location*

prestigiosa, con la partecipazione di illustri relatori, invitati a disquisire sui temi esposti nel libro.
Di solito quando si nota la pubblicazione di un'opera scientifica non ci si interroga sui motivi che potrebbero renderla importante per il pubblico, tuttavia, in questo caso, l'eccezione conferma la regola.
Perché leggere questo libro, che si apre con la **Prefazione** di Giovanni Buttarelli, Garante Europeo per la protezione dei dati personali (EDPS).
Per interesse? per curiosità? E' probabile. E' sicuramente plausibile che la monografia venga apprezzata per lo stile, per i contenuti, per l'innovazione.

Val la pena di dire subito che è un libro per tutti, perché consente una lettura in cui gli esperti della materia ritrovano certezze, mentre i neofiti ricevono rassicurazioni.
L'Autore propone un'analisi ragionata delle novità normative. Dalle statistiche pubblicate in occasione del primo compleanno del GDPR si evince che in Italia solo il 17 % delle persone sa di che cosa si tratta e il 49 % ne ha sentito parlare. Bene, le osservazioni e informazioni di Nicola Fabiano sembrano voler raggiungere anche quel rimanente 34% di persone rimaste all'oscuro, ignare della normativa ed essenzialmente inconsapevoli del valore della propria identità.
E' una sorta di manuale che porta a trasformare l'ansia da prestazione per la *compliance* al GDPR nella sicurezza che ogni cambiamento genera opportunità e vantaggi.

LO STILE
Il nuovo lavoro monografico di Nicola Fabiano non si palesa, come si è soliti dire, come la sua ultima "fatica", anzi le parole mostrano una costante determinazione nel voler guidare il lettore nel "meraviglioso mondo" di servizi tecnologici, conoscendone, però, le regole, svelandone i segreti e trasmettendo le strategie vincenti.
E' un testo di alto livello scientifico, senza che il lettore ne avverta il peso sentendosi "inadeguato". Al contrario chi

legge viene attratto e coinvolto nella conoscenza oppure trova conferme del proprio sapere personale. Uno stile discorsivo che consente di assorbire con facilità anche le nozioni più tecniche.
E' un libro ricco di domande, ma soprattutto di risposte. Prima fra tutte, quella conclusiva DOVE STIAMO ANDANDO: "***c'è la necessità di parlare di ETICA.*** **Oggigiorno, ancora non c'è una matura coscienza etica che costituisca il fondamento per un approccio corretto e consapevole della dignità umana. È necessario, quindi, che si lavori per consolidare e accrescere una vera consapevolezza del valore della persona e dell'intera sfera di ciascun individuo in modo che non venga mai svilita la dignità umana."**

I CONTENUTI
Capitolo dopo capitolo, Nicola Fabiano accende la luce della consapevolezza sui diritti e doveri che abbiamo sotto gli occhi, dei quali, però, percepiamo solo alcuni profili.
Con estrema "leggerezza" ("che non è superficialità, ma planare sulle cose dall'alto" come ha insegnato Italo Calvino), l'Autore conduce la mente del lettore nel contesto europeo della tutela dei diritti, spaziando dalla Carta di Nizza e il Trattato di Lisbona, alla CEDU e la Convenzione 108/81, richiamando le diverse direttive (e-privacy) o proposte di direttive per poi contestualizzare i concetti nella cornice giuridica italiana.

Il libro si apre con la valutazione della rivoluzione culturale innescata dal Regolamento Europeo costruita sull'assioma per cui PRIVACY e DATA PROTECTION "**non sono sinonimi"** e contestualmente esiste una profonda differenza tra Privacy e SICUREZZA: ***"la protezione di dati personali include anche la sicurezza, ma non è vero il contrario."***
In uno dei paragrafi successivi viene evidenziata l'importanza del fatto che la protezione del dato si realizzi sin dalla

progettazione e con modalità di impostazione predefinita, come richiesto per tutti i Paesi menbri dell'Unione Europea.
Ed ancora, viene accuratamente illustrata l'essenza della c.d. *accountability*, perno sul quale poggia il sistema introdotto dal Regolamento Europeo; nozione che, invece, rappresenta una novità nel nostro ordinamento giuridico. Un concetto difficile da assimilare nella nostra società, dove sinora il singolo era abituato a muoversi secondo un modello che può essere parafrasato con lo *slogan* "dimmi cosa devo fare e io lo faccio".

Segue il delicato tema del trasferimento dei dati verso i paesi terzi, che sembrerebbe un concetto astratto, nella realtà è invece un'ipotesi semplice basti pensare alla scelta di un servizio cloud offerto da una azienda con sede fuori dall'Europa.
Il fulcro del lavoro scientifico va individuato nell' analisi tesa ad evidenziare il VALORE del DATO PERSONALE.

Come è possibile percepire il VALORE del dato? L'Autore parte dall'assioma che ***il dato personale costituisce un valore assoluto***, e di seguito offre un paragone che consente l'immediata percezione del concetto: "***quale valore attribuiamo alla vita umana? Riteniamo che la vita sia un valore assoluto e inviolabile perché è la sua stessa natura che ci permette di affermarlo. Si tratta di un elemento otologico, la vita è un valore. Allo stesso modo il dato si riferisce a informazioni personalissime di una persona fisica e va considerato un valore ontologicamente assoluto.***

Gli esempi per dimostrare il valore del dato personale sono numerosi, l'ultimo dei quali arriva proprio dal social network più famoso. Nella seconda metà di giugno, la cronaca ha riportato la notizia della diffusione negli USA della app *Facebook Study*. La proposta di Facebook di "profilare" gli utenti USA (chiedendo di condividere informazioni su come usano le app), ma questa volta a pagamento. L'applicazione *Study* serve per controllare cosa gli utenti fanno con il

proprio smartphone e in cambio ogni utente che aderisce verrà ricompensato. Ecco, probabilmente così è finalmente evidente per tutti: è proprio questo il VALORE (economico) dei DATI, collegato al consenso dell'utente chiamato ad essere consapevole del proprio diritto al controllo.

Il secondo capitolo del libro è riservato agli argomenti di *cybersecurity* e contiene una sorta di elenco di istruzioni per l'uso per muoversi in sicurezza su internet avendo consapevolezza dei rischi per i dati personali.
Gli smartphone, la posta elettronica, i social network, le varie modalità di messaggistica, il *cloud computing,* fanno parte del nostro modo di vivere e non possiamo, ma soprattutto non dobbiamo, farne a meno. E' necessario, però, conoscere i rischi e sapere come fare per proteggersi.
Questo messaggio emerge chiaramente nelle parole che vengono dedicate alla sfera di tutela da riservare ai minori. "***L'obiettivo di proteggere i minori non dal mondo digitale, ma all'interno dello stesso. Sarebbe impensabile e comunque anacronistico escludere i minori dal mondo digitale nell'era in cui viviamo che è basata quasi completamente sull'utilizzo di internet e delle tecnologie. I ragazzi devono imparare a conoscere la realtà digitale e a loro va insegnato con quale approccio avvicinarsi a queste risorse.".***
Nel terzo capitolo vengono esaminate le nuove frontiere tecnologiche (blockchain, big data, intelligenza artificiale, droni, robotica), che richiedono necessaria consapevolezza anche al fine di un corretto approccio etico al tema.
Ad esempio il mondo IoT (Internet of Things) dove la comodità o praticità del servizio ricevuto mette in ombra le domande sul trattamento dei dati personali. E' pur vero che "***sono sempre le azioni dell'utente attraverso cui si autorizza o non l'accesso a determinate informazioni e la comunicazione delle stesse" ma quanto è realmente consapevole il consenso dell'utente?***

L'INNOVAZIONE

L’Autore propone una chiave di lettura originale e innovativa del complesso contesto normativo, indicandola direttamente nel titolo dell’opera.
Sui piatti della bilancia ci sono due valori fondamentali: da un lato, la dignità dell’uomo e dall’altro, la tecnologia senza frontiere. Etica e Consapevolezza sono gli elementi essenziali per un corretto equilibrio.

1. *Awareness raising* è il must: “***la sensibilizzazione sui temi che riguardano la persona e conseguentemente la protezione dei dati personali e della privacy***”
2. ETICA è la parola d’ordine non solo con il preciso intento di prospettare alcune chiavi di lettura etiche delle norme del GDPR, ma anche per creare una coscienza etica.

Nei paragrafi finali dedicati all’analisi ragionata del tema dell’Intelligenza artificiale, l’Autore ricorda il momento in cui ha iniziato “***ad approfondire l’impatto e l’incidenza della ia e della robotica su privacy e protezione dei dati personali, focalizzando l’attenzione sull’etica e in particolare sulla identificazione di un approccio etico” (…) in considerazione dell’alto valore dei diritti fondamentali contenuti nella Carta europea.***

Il ragionamento viene quindi portato sino alla affermazione conclusiva per cui “***Non è necessaria soltanto l’attività di sensibilizzazione al tema dell’etica ma ancor più l’acquisizione di una concreta consapevolezza dell’etica che deve diventare una reale “coscienza etica”. Una coscienza etica implica il rispetto della legge sulla protezione dei dati personali (Gdpr e codice privacy), ma potrebbe non essere vero il contrario, ossi*****a rispettare la legge non significa necessariamente avere una “coscienza etica”.**
“Il tema è complesso, ma non è un percorso impossibile; la primazia dell’uomo sulle macchine consente di approfondire il tema dell’etica senza lasciare che le persone siano ridotte a meri dati, a bit, oggetto di elaborazioni algoritmiche e dati

in pasto ai sistemi di intelligenza artificiale.”

In conclusione, la lettura del libro di Nicola Fabiano regala l’opportunità di guardare il complesso mondo in cui viviamo con occhi consapevoli. Come ricorda una delle frasi più citate che girano sul web *È la luce della consapevolezza che rende le cose preziose e straordinarie. E allora le piccole cose non sono più piccole*.

Last but no least

Edito da GoWare l’altra editoria, nella collana TECNOLOGIA, il libro esiste in versione tradizionale per gli amanti della carta, ma anche *ebook*, decisamente *easy,* anche per la consultazione di tutti i documenti richiamati nel testo e immediatamente accessibile *on line*. Il libro assicura una prezioso patrimonio di documentazione e una imponente bibliografia normativa.
La TECNOLOGIA, proprio come “il trattamento dei dati personali”, è “al servizio dell’uomo” (come affermato nel Considerando n. 4 GDPR 679/16).
E’ una opportunità da non perdere, in modo consapevole.

Nicola Fabiano è avvocato cassazionista, specialista in Diritto civile. È Presidente dell’Autorità per la protezione dei dati personali di San Marino. Nel 2017 è stato incaricato dal Congresso di Stato (Governo) della Repubblica di San Marino della redazione di una specifica normativa in materia di protezione dei dati personali. Fa parte della Commissione privacy del Consiglio nazionale forense (cnf) e del gruppo di lavoro dell e del gruppo di lavoro della Fondazione italiana per l’innovazione forense (fiif). È autore di numerosi contributi scientifici presentati a conferenze internazionali e pubblicati. È stato insignito di numerosi awards.

https://www.key4biz.it/gdpr-privacy-consapevolezza-e-opportunita-analisi-ragionata-della-protezione-dei-dati-personali-tra-etica-e-cybersecurity/262699/