GDPR tra novità e falsi miti

Man mano che la scadenza del GDPR si avvicinava erano sempre di più le “leggende” che si consolidavano in ordine alla sua applicazione, e si diffondevano a macchia d’olio le interpretazioni più varie, il più delle volte instillando dubbi e timori francamente infondati, a volte proponendo letture decisamente pericolose.

Il Regolamento generale sulla protezione dei dati è una normativa complessa, che si colloca al crocevia con diverse altre fonti che ne intersecano e lambiscono l’ambito di applicazione; non sempre è semplice comprendere come questi ambiti possano essere regolati, e il legislatore nazionale, che avrebbe dovuto dettare le regole di coordinamento sul piano nazionale non è stato in grado di intervenire tempestivamente.

D’altra parte il Regolamento lascia ampi spazi di deroga al legislatore nazionale, e l’auspicio è che gli Stati membri se ne avvalgano il meno possibile, in modo da poter mantenere il quadro europeo quanto più uniforme.

In alcuni casi, tuttavia, è necessario che il legislatore intervenga: ad esempio in tema di consenso prestato dal minore per quanto riguarda l’offerta di servizi della società dell’informazione loro diretti; in questo caso il GDPR fissa un range (una età variabile tra i 13 e i 16 anni) e ogni Stato membro, autonomamente, dovrà stabilire l’età che ritiene più consona. L’Italia, nel momento in cui scrivo, non ha ancora pubblicato questa norma.

Questo articolo si propone di fare chiarezza su alcune interpretazioni fuorvianti che si stanno coagulando attorno alla lettera del Regolamento soprattutto tra chi non ha consuetudine con la normativa sulla protezione dei dati personali, in modo da scongiurare letture “pericolose”: come,

ad esempio, pericolose possono rivelarsi per chi ha poca dimestichezza con la normativa, le fantasiose interpretazioni relative al numero di dipendenti: taluni ritengono che l'obbligo di nominare il data protection officer riguardi solo le imprese con più di 250 dipendenti, altri addirittura che il Regolamento stesso trovi applicazione solo per le imprese con più di 250 dipendenti. Si tratta di interpretazioni di pura fantasia, il GDPR non commisura gli adempimenti a questo limite dimensionale e l'unico caso in cui si fa riferimento ai 250 dipendenti, nel testo, è relativamente all'obbligo di tenuta del registro delle attività di trattamento. Tuttavia anche in questo caso non è il numero dei dipendenti ad essere di per sé decisivo, ma l'occasionalità o il rischio del trattamento operato.

Preciso, infine, che questa analisi muove dalla mia personalissima esperienza, senza alcuna pretesa di completezza o sistematicità.

Obbligo o verità

L'articolato del Regolamento europeo è differente da quello delle norme nazionali: agli articoli veri e propri sono premesse alcune formulazioni (173, per la precisione) che sono indicate da un numero tra parentesi: si tratta dei "considerando".

I "considerando" sono la spiegazione del senso che il legislatore europeo voleva imprimere alla norma: per quello tendenzialmente non vengono utilizzati tempi verbali che indicano un precetto, ma viene usato per lo più il condizionale.

Il precetto vero e proprio è contenuto solo negli articoli. Avventurarsi in spiegazioni contorte sul perché una norma sarebbe o meno vincolante attaccandosi al testo del considerando (come ho visto fare in alcune discussioni sui social) è pericoloso: i considerando sono principalmente

rivolti ai Giudici della Corte di Giustizia, che hanno una approfondita conoscenza del diritto europeo e dell'ordinamento in cui il GDPR si inquadra.

La lettura dei considerando può essere utile, soprattutto per gli esempi che riportano: ma è sconsigliabile appellarsi ai cavilli che si crede di reperire nel testo; infatti, questi possono essere estremamente fuorvianti. Inoltre prima di avventurarsi in interpretazioni poggiate sulla lettera della legge, occorre tener presente che il Regolamento è una norma europea, e a differenza delle leggi italiane non è scritto in una lingua sola, ma in 24 lingue. In genere, se sorge un problema legato all'interpretazione letterale, va risolto nel senso prevalente che la norma ha nella maggioranza delle versioni ufficiali. L'inglese non è la versione predominante, e anche se a volte la versione in inglese appare più chiara di quella italiana e può essere di aiuto, non è di per sé dirimente.

Consensi, consensi ovunque

Il consenso è una delle basi giuridiche del trattamento elencate dall'articolo 6 del GDPR, non è prioritaria o prevalente rispetto ad altre. Questa impostazione, già seguita in Europa dai tempi della direttiva 95/46/CE, era stata ribaltata in Italia, dove il sistema era stato costruito attorno al consenso, elencando i casi tassativi in cui era possibile operare in via di eccezione al consenso stesso.

In estrema sintesi, il GDPR non obbliga ad avere il consenso per tutti i trattamenti, anzi: sono più i trattamenti che non impongono la richiesta di consenso che quelli che la impongono.

Se i dati che mi vengono forniti (conferiti, come si dice tecnicamente) al momento della stipula di un contratto mi serviranno per eseguire il contratto, non dovrò chiedere il consenso (ma attenzione: dovrò sempre rendere l'informativa),

e non mi servirà il consenso fintanto che utilizzerò i dati per eseguire il contratto e assolvere gli obblighi di legge connessi.

Attenzione anche al legittimo interesse, che è una diversa base giuridica: è una base che taluni considerano “pericolosa” o “rischiosa” e cercano di ricorrere al consenso invece che al legittimo interesse: ma consenso e legittimo interesse non sono due basi intercambiabili; il legittimo interessa opera spesso proprio dove il consenso non potrebbe essere validamente acquisito: infatti, il consenso che non è liberamente prestato non è valido, e il consenso non è valido perché non è libero ogni volta che è condizionato (dalla necessità di ricevere una prestazione o dal particolare rapporto che lega le parti, ad esempio).

Alcuni dei presupposti di invalidità del consenso (ad esempio la necessità di “coartarlo” per poter effettuare il trattamento connesso, o il particolare rapporto in essere tra le parti) sono proprio i presupposti su cui si fonda il legittimo interesse: si tratta di basi giuridiche alternative, nel senso che una esclude l’altra, nella maggioranza dei casi.

Resta il problema che il legittimo interesse non basta individuarlo: per impiegarlo validamente si deve anche fare il bilanciamento degli interessi (per iscritto, in ossequio al principio di accountability). Tuttavia se non sono in grado di ottenere un bilanciamento favorevole non posso limitarmi a inserire un modulo di consenso per superare il problema, devo valutare se in quel caso il consenso sarà valido o invece, invalido, perché condizionato. Ad esempio, nei rapporti di lavoro, il consenso, data la sperequazione nelle posizioni di forza di datore di lavoro e lavoratore non può essere impiegato se non in rari, marginalissimi, casi: il più delle volte il trattamento si baserà necessariamente sul legittimo interesse (cfr. WP opinion 2/2017).

Mi permetto anche una annotazione sinteticissima in ordine

all’informativa: è vero che la fortuna ha voluto che fosse sempre disciplinata dal medesimo articolo (il 13) nei due testi normativi, ma non basta sostituire la formula normativa per rendere una informativa conforme al GDPR: non solo perché è necessario rivedere il “tono” (il GDPR richiede un linguaggio semplice e chiaro, non legalese) e la forma (è preferibile dare un’informativa su più livelli) ma perché è diverso il contenuto. L’articolo 13 del GDPR richiede elementi prima non previsti, come l’indicazione della base giuridica, e sono elementi tassativi, non si possono omettere a piacimento. Scrivere “informativa resa ai sensi dell’articolo 13 del Regolamento UE 679/2016” su un testo risalente all’informativa “resa ai sensi dell’articolo 13 del D. Lgs. 196/03” è efficace come il nascondiglio dei bambini che credono di non essere visti se si coprono gli occhi coi palmi delle mani.

Le parole sono importanti

Come anticipato più sopra, il consenso può essere prestato da parte dei minori solo se essi hanno raggiunto il limite di età fissato dalle varie legislazioni nazionali.

Attenzione però perché la norma non tocca la capacità di agire del minore, che resta fissata dalle regole civilistiche, tocca solo i trattamenti la cui base giuridica è il consenso.

L’articolo 8 del Regolamento recita: “Qualora si applichi l’articolo 6, paragrafo 1, lettera a), per quanto riguarda l’offerta diretta di servizi della società dell’informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni.

Ove il minore abbia un’età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

Gli Stati membri possono stabilire per legge un’età inferiore

a tali fini purché non inferiore ai 13 anni.” La norma va letta così: *Qualora il trattamento sia basato sul consenso,* per quanto riguarda l’offerta diretta di servizi della società dell’informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni.

Eliminare il riferimento all’articolo 6 paragrafo 1 lettera a), e riportare solo l’inciso seguente: “per quanto riguarda l’offerta diretta di servizi della società dell’informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni” scompagina completamente il senso della norma, perché rivela una portata generale, che apparentemente incide anche sulla capacità di agire e che il legislatore non solo non si prefiggeva, ma proprio non ha scritto. “Le parole sono importanti” per dirla con Nanni Moretti, e negli articoli di legge sono imprescindibili anche quando sono hanno scarso *appeal* come “Qualora si applichi l’articolo 6, paragrafo 1, lettera a)”.

Cookie monster

Le interpretazioni più improbabili e gli adempimenti più strampalati si addensano come nubi attorno soprattutto al nodo del rapporto tra “cookie law” (qualunque cosa con questa espressione si intenda indicare) e GDPR.

La “cookie law”non abroga/ modifica o è abrogata/ modificata dal GDPR, come si paventa da più parti.

Innanzi tutto bisogna chiarire cosa sia la famigerata “cookie law”, dato che, a mio avviso, il punto critico è proprio la confusione intorno alla fonte normativa da cui discendono gli obblighi in ordine ai cookie (e non solo: sono obblighi che riguardano anche altri strumenti di remarketing). Parafrasando Goya, la confusione sulla “cookie law” genera mostri.

Innanzi tutto, generalmente quando parliamo di “cookie law”

spesso facciamo riferimento a più norme, che sgorgano a cascata dalla Direttiva e-privacy (Direttiva 2002/58/CE e s.m.i.).

Trattandosi di una direttiva, a differenza del Regolamento – che trova immediata applicazione nei singoli Stati -, la e-privacy aveva bisogno di essere attuata dalla normativa nazionale.

La parte che riguarda i cookie nella nostra normativa ha trovato compimento nell'articolo 122 del Codice della Privacy, il quale alla rubrica "**Informazioni raccolte nei riguardi del contraente o dell'utente"** dispone che "1. L'*archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con le modalità semplificate di cui all'articolo 13, comma 3. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso alle informazioni già archiviate se finalizzati unicamente ad effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio. Ai fini della determinazione delle modalità semplificate di cui al primo periodo il Garante tiene anche conto delle proposte formulate dalle associazioni maggiormente rappresentative a livello nazionale dei consumatori e delle categorie economiche coinvolte, anche allo scopo di garantire l'utilizzo di metodologie che assicurino l'effettiva consapevolezza del contraente o dell'utente. Ai fini dell'espressione del consenso di cui al comma 1, possono essere utilizzate specifiche configurazioni di programmi informatici o di dispositivi che siano di facile e chiara utilizzabilità per il contraente o l'utente (omissis)"*

In ragione del potere attribuito da questo articolo, il

Garante, nel 2014, emetteva il noto provvedimento "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie – 8 maggio 2014 [3118884]".

Discendono da questo provvedimento (che ha solo in parte valore prescrittivo generale) indicazioni sui cookie profilanti quali: usare il banner, inserire un testo idoneo nel banner e il link alla informativa estesa, bloccare il rilascio dei cookie da parte del sito sino a che il consenso non sia stato prestato, dare la possibilità di rifiutare l'uso dei cookie, anche attraverso le impostazioni di programmi, ovvero del browser. Non si tratta pertanto di obblighi che discendono dal GDPR, ma di indicazioni che consentono di non violare il dettato dell'articolo 122 del Codice Privacy che dispone che non si possono registrare cookie sul terminale dell'utente prima che questi abbia prestato il consenso informato.

Senza addentrarci in spiegazioni troppo complesse, ché non è lo scopo di questo scritto, mi limito a osservare che ciò che non discendente dalla direttiva madre (la 95/46/CE) abrogata dal Regolamento, non viene abrogato: quindi restano in piedi sia la direttiva e-privacy sia buona parte dell'articolo 122 del Codice privacy [indipendentemente dalla tecnica normativa che userà il legislatore, sia che abroghi il codice riproponendo (in pratica copiando e incollando) le norme "superstiti" in un nuovo decreto, sia che scriva un nuovo decreto solo per indicare le norme – o le parti di norme – del Codice privacy che dovranno essere abrogate (la comprensione di ciò che rimarrà vigente è più tortuosa, ma il risultato è identico)].

Il punto di intersezione tra la direttiva e-privacy e la direttiva madre (95/46/CE) verranno presidiati dal Regolamento generale sulla protezione dei dati: ciò che cambia in ordine all'informativa (oltre al linguaggio chiaro e ai contenuti), è che ora il titolare può scegliere le modalità semplificate per

rendere l'informativa e quindi può continuare a fare ciò che faceva prima indipendentemente dalla sopravvivenza del provvedimento del Garante (peraltro l'uso del banner era indicato come linea guida).

A ben guardare, la direttiva e-privacy aveva previsto un sistema in cui offrire la possibilità di rifiutare i cookie, richiamando espressamente la direttiva madre (e quindi, ora, il Regolamento), solo in ordine all'informativa: "*Gli Stati membri assicurano che l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente interessato sia stato informato in modo chiaro e completo, tra l'altro, sugli scopi del trattamento in conformità della direttiva 95/46/CE e che gli sia offerta la possibilità di rifiutare tale trattamento da parte del responsabile del trattamento. Ciò non impedisce l'eventuale memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente*".

Nel considerando connesso all'articolo 5 sopra riportato, si precisava che "*Tuttavia, tali dispositivi, per esempio i cosiddetti marcatori ("cookies"), possono rappresentare uno strumento legittimo e utile, per esempio per l'analisi dell'efficacia della progettazione di siti web e della pubblicità, nonché per verificare l'identità di utenti che effettuano transazioni "on-line". Allorché tali dispositivi, ad esempio i marcatori ("cookies"), sono destinati a scopi legittimi, come facilitare la fornitura di servizi della società dell'informazione, il loro uso dovrebbe essere consentito purché siano fornite agli utenti informazioni chiare e precise, a norma della direttiva 95/46/CE, sugli*

scopi dei marcatori o di dispositivi analoghi per assicurare che gli utenti siano a conoscenza delle informazioni registrate sull'apparecchiatura terminale che stanno utilizzando. Gli utenti dovrebbero avere la possibilità di rifiutare che un marcatore o un dispositivo analogo sia installato nella loro apparecchiatura terminale. Ciò riveste particolare importanza qualora utenti diversi dall'utente originario abbiano accesso alle apparecchiature terminali e quindi a dati contenenti informazioni sensibili in relazione alla vita privata che sono contenuti in tali apparecchiature. L'offerta di informazioni e del diritto di opporsi può essere fornita una sola volta per l'uso dei vari dispositivi da installare sull'attrezzatura terminale dell'utente durante la stessa connessione e applicarsi anche a tutti gli usi successivi, che possono essere fatti, di tali dispositivi durante successive connessioni. Le modalità di comunicazione delle informazioni, dell'offerta del diritto al rifiuto o della richiesta del consenso dovrebbero essere il più possibile chiare e comprensibili. L'accesso al contenuto di un sito Internet specifico può tuttavia continuare ad essere subordinato all'accettazione in conoscenza di causa di un marcatore o di un dispositivo analogo, se utilizzato per scopi legittimi."

Il nostro legislatore ha preferito ricorrere al consenso, piuttosto che ricorrere alla "possibilità di sottrarsi"; ad avviso di chi scrive, occorrerà fare maggiore attenzione alla prestazione del consenso che non deve essere meramente formalistica: occorre che il consenso si sostanzi in una azione positiva dell'utente, come ricordava anche il Garante nel già citato provvedimento: "*il superamento della presenza del banner al video deve essere possibile solo mediante un intervento attivo dell'utente (appunto attraverso la selezione di un elemento contenuto nella pagina sottostante il banner stesso)*".

C'è da domandarsi se, in assenza di un espresso richiamo, la

manifestazione di volontà che impone sia la direttiva e-privacy, sia il medesimo consenso disciplinato dal GDPR. Chi scrive propende per una risposta affermativa, in linea con l'orientamento espresso dal WP29 nelle linee guida sul consenso "*With regard to the existing e-Privacy Directive, WP29 notes that references to the repealed Directive 95/46/EC shall be construed as references to the GDPR. This also applies to references to consent in the current Directive 2002/58/EC*"

"*According to Article 95 GDPR, additional obligations in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks shall not be imposed insofar the e-Privacy Directive imposes specific obligations with the same objective.* ***WP29 notes that the requirements for consent under the GDPR are not considered to be an 'additional obligation', but rather as preconditions for lawful processing. Therefore, the GDPR conditions for obtaining valid consent are applicable in situations falling within the scope of the e-Privacy Directive***".

Secondo tale lettura è possibile procedere a fornire le informazioni su più livelli ma occorrerà fare attenzione se si utilizzano cookie profilanti che possono rivelare l'orientamento sessuale o lo stato di salute o le convinzioni politiche o filosofiche (o altri dati appartenenti alle particolari categorie individuate all'articolo 9 del GDPR): in questi casi (come peraltro anche secondo la Direttiva 95/46/CE) il consenso dovrà essere "esplicito" ovvero manifestato attraverso una dichiarazione espressa e non può essere "implicito".

Inoltre: quanti consensi andranno chiesti? Il GDPR ribadisce che il consenso deve essere granulare e non omnicomprensivo: sta a significare che viene ribadito il principio "un consenso / una finalità" e la finalità per cui si domanda il consenso per i cookie di profilazione è, come efficacemente

sintetizzato dal Garante nel fac simile di banner che aveva proposto: “inviarti pubblicità in linea con le tue preferenze”.

Comunque, in sintesi, il GDPR non pone nuove regole in tema di cookie, gli obblighi in ordine ai cookie nascevano da un’altra fonte che sopravvive al GDPR e il provvedimento del Garante mirava a facilitare alcuni adempimenti, lasciando per lo più il titolare libero di trovarne di diversi purché sostanzialmente equivalenti.

La direttiva e-privacy è comunque al momento in fase di revisione e presto sarà sostituita anch’essa da un Regolamento, il Regolamento e-privacy. Solo quando diverrà applicabile il regolamento e-privacy potremo attenderci modifiche significative anche alla “cookie law”.

Non fatevi prendere dal panico

“In molte delle civiltà meno formaliste dell’Orlo Esterno Est della Galassia, la *Guida galattica per gli autostoppisti* ha già soppiantato la grande *Enciclopedia galattica*, diventando la depositaria di tutto il sapere e di tutta la scienza, perché nonostante presenti alcune lacune e contenga molte notizie spurie, o se non altro alquanto imprecise, ha due importanti vantaggi rispetto alla più vecchia e più accademica *Enciclopedia*.

Uno, costa un po’ meno; due, ha stampate in copertina, a grandi caratteri che ispirano fiducia, le parole non fatevi prendere dal panico.” (Douglas Adams, Guida galattica per autostoppisti)

Dal 25 maggio 2018 il Regolamento è diventato applicabile. Nel momento in cui scrivo alla fatidica data manca ancora qualche giorno, e se state leggendo dopo il 25 maggio vuol dire che il mondo non è finito… Cosa è successo dal 25 maggio 2018? In soldoni, che il GDPR ha preso il posto della Direttiva

95/46/CE e della normativa nazionale che la attuava: nel nostro caso buona parte del Codice privacy.

Non è successo nulla di irreparabile il 25 maggio 2018: è una data che ha segnato un inizio, e se non siete ancora pronti, state tranquilli che siete in ottima e numerosa compagnia: il GDPR, in vigore ormai da due anni, giunto al momento della sua attuazione non ha trovato pronto nessuno, neppure il Working Party (che non ha ancora finalizzato tutte le linee guida promesse) né la Commissione (che non ha ancora pubblicato né le clausole standard per gli accordi sul trattamento, né le icone standardizzate per rendere le informative), né il legislatore nazionale, che, alla vigilia del 25 maggio, ancora lotta contro il tempo per riscrivere la normativa interna di coordinamento.

Il GDPR, dicevo, segna un nuovo inizio, un nuovo modo di approcciare la materia della protezione dei dati, più in linea con l'evoluzione tecnologica che ha reso obsoleta la direttiva che lo ha preceduto.

Per non farsi presto superare dalla tecnologia, il GDPR impone al titolare obblighi di documentazione che riflettono il suo potere discrezionale: il titolare stesso decide buona parte degli adempimenti in autonomia valutando i rischi e implementando le misure tecniche e organizzative che ritiene più idonee a proteggere i dati che tratta.

Il GDPR è pensato per evolversi al progredire della tecnica, e chi, meglio del titolare, conosce i trattamenti che opera e può proteggere i dati? Per quello occorre documentare le scelte che si fanno e non ci sono obblighi identici per tutti.

La corsa all'adempimento dell'ultimo minuto è un approccio fallimentare: il GDPR necessita di essere compreso, non a caso tanti autorevoli voci (primo tra tutti l'ICO) insistono sulla "consapevolezza", perché solo la consapevolezza in ordine alla gestione dei dati e alle esigenze di protezione che ne

discendono consentirà al titolare e ai responsabili di essere davvero “in regola”.

Il nuovo sistema è vero che prevede alte sanzioni, ma proprio perché è incentrato sulla valorizzazione della consapevolezza, considera la sanzione una *extrema ratio* e nessuno ha bussato alla nostra porta il 26 maggio 2018 per controllare a che punto fossimo con l’adeguamento. D’altra parte, è vero che questo non deve spingerci a restare inerti: buona parte del controllo passerà anche dal lato privatistico, prevedendosi sia il ristoro dei danni con connotazioni afflittive in caso di violazione della normativa, sia la class action.

Dire: “non mi interessa come funziona, voglio solo i documenti per mettermi a posto ed evitare le multe” è la spia di un approccio sbagliato; significa credere che l’adeguamento sia un adempimento una tantum e non un modo diverso di organizzarsi, e persino di pensare, che inizia ora. Nel corso del tempo abbiamo imparato molte cose che non interessavano a chi ci ha preceduto e che prima si pensava che non servissero: leggere e scrivere, usare i computer, leggere i valori nutrizionali sulle confezioni di cibo, le regole del codice della strada. Anche se non abbiamo la patente sappiamo che dobbiamo attraversare sulle strisce e camminare da una parte.

Non significa che dovranno tutti trasformarsi in legali o che tutti dovremo diventare esperti di informatica o ingegneri gestionali. Significa che dobbiamo però capire quello che stiamo facendo, e imparare a riconoscere e gestire le criticità.

Il GDPR ha un approccio molto meno burocratico del Codice della privacy, e anche se ci vorrà un po’ di tempo per scrollarci di dosso la polvere del sistema al quale siamo abituati, presto ci renderemo conto che molte cose sono più semplici di come le avevamo immaginate.

Meglio farsi trovare in alto mare con l’adeguamento adottando

un approccio consapevole, che sentirsi adeguati perché ci si è muniti di documentazione precompilata, destinata a restare chiusa in un cassetto (anche se il cassetto è una cartella elettronica) e che non ci servirà a nulla quando dovremo selezionare il fornitore di un servizio in outsourcing o dare riscontro a un interessato o valutare i rischi di un nuovo trattamento.

Come l'Enciclopedia Galattica, il nostro sistema concentrava "tutto il sapere e tutta la scienza" in tema di protezione dei dati personali nelle mani del Garante: ora con il GDPR il sistema muta, e il "sapere" e la "scienza" in fatto di protezione dei dati tornano nelle nostre mani; il Garante ci servirà come riferimento, ma non ci detterà più gli adempimenti in modo così dettagliato, come eravamo abituati. Come la guida Galattica, il GDPR ci pare avere lacune e notizie spurie, ma sul lungo termine, imponendo una seria riflessione su misure di sicurezza (informatiche, organizzative e persino contrattuali) imprescindibili in un mondo che evolve (con rischi che si evolvono e che le misure minime non potevano più presidiare) ci costerà meno del sistema precedente.

Il GDPR è la nostra Guida Galattica alla protezione dei dati personali: "non fatevi prendere dal panico"!

Bibliografia

1. F. di Resta, *La nuova privacy europea – I principali adempimenti del Regolamento UE 2016/679 e profili risarcitori* Torino, Giappichelli, 2018
2. Edoardo Pusillo, Divergenze linguistiche ed interpretazione uniforme delle norme europee http://www.farum.it/publifarum/ezine_articles.php?art_id=388
3. Gruppo di lavoro Articolo 29, WP 249 opinion 2/2017 on data processing at work
4. Garante Privacy – Individuazione delle modalità

semplificate per l’informativa e l’acquisizione del consenso per l’uso dei cookie – 8 maggio 2014 [3118884]
5. Gruppo di lavoro Articolo 29, wp259rev.01 Guidelines on consent under Regulation 2016/679
6. ICO Good and bad examples of privacy notices https://ico.org.uk/media/for-organisations/documents/1625136/good-and-bad-examples-of-privacy-notices.pdf

A cura di: **Cristina Vicarelli**

L’articolo GDPR tra novità e falsi miti proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/gdpr-tra-novita-e-falsi-miti/