In particolare, l'Autorità, che in materia ha adottato già un provvedimento il 15 dicembre 2011 [doc. web n. 1883880] inibitorio e prescrittivo nei confronti di una nota società operante nel settore dei giochi e servizi resi tramite ricevitorie, ha monitorato il trattamento dati effettuato da alcune società afferenti ad un altro noto gruppo del medesimo settore. Al riguardo, pur non essendo stati ravvisati i presupposti per l'adozione di un provvedimento del Collegio, è emerso che le dette società, prima dell'adozione di nuovi contratti-tipo, utilizzavano, in contrasto con l'art. 23 del Codice, una formula di consenso unico al trattamento dei dati personali dei punti vendita per la finalità contrattuale e per quella promozionale e si limitavano ad avvisare punti vendita e ricevitorie che "*il conferimento dei dati era necessario*", senza alcuna distinzione per tipologia di dati o finalità perseguita.

Inoltre, è risultato che le società in questione avevano effettuato campagne di incentivazione per la vendita dei propri servizi nei confronti dei punti vendita, senza il necessario consenso distinto e specifico. Pertanto l'Ufficio ha avviato un procedimento sanzionatorio nei confronti di tutte le società del gruppo coinvolte in tale trattamento dati (nota 20 luglio 2012).

11.8. CESSIONI DI DATI PERSONALI A FINI DI *TELEMARKETING*

Con provvedimento del 5 aprile 2012 [doc. web n. 1891156], il Garante ha ribadito che l'acquirente di liste di dati personali da utilizzare per attività di *telemarketing* deve verificare che gli interessati abbiano espresso il proprio preventivo consenso ai contatti di natura commerciale. Il caso riguardava un interessato i cui dati erano stati tratti da un questionario *online* che, a seguito degli accertamenti effettuati dall'Autorità, non è risultato conforme alla disciplina di legge, dal momento che prevedeva come obbligatoria la prestazione del consenso dell'interessato a fini promozionali (v. art. 23 del Codice).

Nel contratto di fornitura delle liste dei potenziali clienti, inoltre, i rapporti tra le parti erano regolati in modo da ricondurre la formale qualifica di titolare del trattamento alla sola società fornitrice dei dati personali degli interessati, nonostante diverse pattuizioni evidenziassero un ruolo sostanziale di titolare anche della società acquirente i dati, potendo questa determinare le finalità e modalità dei contatti promozionali effettuati per proprio conto e nel proprio interesse.

Per queste ragioni, il Garante ha ritenuto che anche l'acquirente dovesse essere considerato titolare dell'attività di *telemarketing* in questione, ed ha dichiarato illecito e vietato il trattamento effettuato in assenza del prescritto consenso dei singoli interessati al trattamento per finalità promozionali (provv. 5 aprile 2012 [doc. web n. 1891156].

11.9. *MOBILE PAYMENT*

Nel 2012 in merito ai nuovi servizi di pagamento attraverso il telefono cellulare, noti come *mobile remote payment* e *mobile proximity payment,* l'Autorità ha acquisito presso i diversi soggetti interessati (oltre agli operatori telefonici, gli istituti bancari, i circuiti delle carte di credito, i *merchant* ed i cd. "*hub* tecnologici"), una serie di informazioni. In particolare, con riguardo ai servizi che consentono di attivare "in remoto" il pagamento di un bene o di un servizio, l'Autorità ha analizzato i sistemi e le modalità con le quali gli operatori telefonici, gli *hub* tecnologici incaricati della gestione tecnica del servizio e diversi *merchant,* consentono ai propri clienti di effettuare micropagamenti per l'acquisito di servizi e prodotti digitali fruibili tramite *smartphone,* PC e *tablet,* con conseguente addebito del relativo costo sul conto telefonico dell'utente, o attraverso decurtazione dell'importo dal credito telefonico nel caso di carte ricaricabili.

Con riguardo, invece, ai servizi che includono pagamenti elettronici di "prossimità", per i quali è necessaria una vicinanza fisica tra il dispositivo mobile ed il prodotto o servizio acquistato (attraverso il ricorso alla tecnologia *NFC* (*Near Field Communication*), il Garante ha svolto la suddetta attività anche presso alcuni istituti bancari ed alcuni dei circuiti delle carte di credito.

Le indagini dell'Autorità sono state estese anche ad un noto motore di ricerca.

Questa attività conoscitiva costituisce la base per predisporre una regolamentazione di tali servizi che consenta, favorendo l'uso delle descritte tecnologie, un utilizzo corretto dei dati personali degli utenti da parte dei soggetti coinvolti.

11.10. LA DISCIPLINA DEI *DATA BREACH*

In attuazione della direttiva comunitaria in materia di sicurezza e *privacy* nel settore delle comunicazioni elettroniche (Direttiva n. 2009/136/CE, di recente recepita con il d.lgs. 28

maggio 2012, n. 69, in G.U. 31 maggio 2012, n. 126), il nuovo art. 32-*bis* del Codice prevede che i fornitori di servizi di comunicazione elettronica accessibili al pubblico (quali telefonia, accesso a internet, *account* di posta elettronica) sono obbligati a comunicare senza indebiti ritardi al Garante e, in alcuni casi, al contraente o ad altre persone interessate, il verificarsi di eventi, qualificati come "*violazioni di dati personali*", riguardanti i dati personali contenuti nei *database* di tali soggetti.

Alla base di tale normativa vi è la consapevolezza che un evento che coinvolga i dati personali trattati dai suindicati soggetti, se non gestito in modo adeguato e tempestivo, può provocare un grave danno economico e sociale al contraente (o alle altre persone interessate), tra cui l'usurpazione d'identità (cfr. considerando 61, Direttiva n. 2009/136/CE).

Al riguardo, il 26 luglio 2012 il Garante ha adottato le "Linee-guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali" (in G.U. 7 agosto 2012, n. 183 [doc. web n. 1915485]) recanti prescrizioni nei confronti dei fornitori, con particolare riguardo: all'individuazione dei soggetti tenuti a comunicare la violazione; alle circostanze in cui la comunicazione dev'essere effettuata; all'obbligo di avvisare anche gli utenti; alle misure di sicurezza tecniche e organizzative da adottare.

In sostanza, è stato chiarito che l'obbligo di comunicare i *data breach* spetta esclusivamente ai fornitori di servizi telefonici e di accesso a internet, non riguardando viceversa le reti aziendali, gli internet *point* (che si limitano a mettere a disposizione dei clienti i terminali per la navigazione), i motori di ricerca, i siti internet che diffondono contenuti.

La comunicazione, anche sommaria, deve avvenire entro ventiquattro ore dalla scoperta dell'evento: i fornitori devono dare le informazioni utili ad una prima valutazione dell'entità della violazione ed hanno tre giorni di tempo per una descrizione più dettagliata. All'esito delle verifiche, i medesimi soggetti devono comunicare al Garante le modalità con le quali hanno posto rimedio alla violazione e le misure adottate per prevenirne di nuove. Al fine di agevolare l'adempimento, il Garante ha predisposto anche un modello di comunicazione, disponibile *online* in formato pdf [doc. web n. 1915835].

Nei casi più gravi, i fornitori hanno l'obbligo di informare anche gli interessati considerando, tra l'altro, il pregiudizio che la perdita, la distruzione o l'accesso non

autorizzato ai dati può comportare (furto di identità, danno fisico, danno alla reputazione), l'"attualità" dei dati (dati più recenti possono rivelarsi più interessanti per i malintenzionati), e la loro qualità (finanziari, sanitari, giudiziari).

Con la citata delibera 26 luglio 2012 è stata contestualmente avviata una consultazione pubblica per acquisire osservazioni in merito ad alcune, specifiche modalità applicative della nuova disciplina, contenuta nell'art. 32-*bis* del Codice.

Dal 1° giugno 2012, data di entrata in vigore della disciplina in materia di *data breach*, sono pervenute all'Autorità diverse comunicazioni di violazioni, da parte di fornitori di servizi di comunicazione elettronica di grandi dimensioni.

Nei casi la cui trattazione è stata conclusa, l'Autorità ha verificato che fossero state adottate misure idonee a porre rimedio alle violazioni subite e a prevenirne di analoghe e non ha ritenuto necessario adottare provvedimenti specifici.

Relativamente ad altre comunicazioni di *data breach* gli accertamenti sono ancora in corso.

11.11. L'UTILIZZO DEI *COOKIE*. FAQ

La disciplina relativa all'uso dei cd. *"cookie"* (i piccoli *file* di testo che i siti visitati dall'utente inviano al suo *browser* per essere poi ritrasmessi agli stessi siti alla successiva visita del medesimo utente) e degli altri strumenti analoghi (quali web *beacon/web bug, clear GIF*) è stata modificata, a seguito dell'attuazione della Direttiva n. 2009/136/CE (che è intervenuta sulla Direttiva n. 2002/58/CE, la cd. "Direttiva *e-Privacy*"), ad opera del d.lgs 28 maggio 2012, n. 69.

In sostanza, il nuovo art. 122 del Codice consente l'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate a condizione che tali soggetti abbiano espresso il proprio consenso sulla base di un'informativa semplificata (art. 13, comma 3, del Codice). La disciplina dei *cookie* si basa pertanto sul principio del cd. "*opt-in*", eccezion fatta per i dispositivi di natura tecnica, ossia quelli strettamente necessari ad effettuare la trasmissione della comunicazione o alla fornitura del servizio esplicitamente richiesto dall'abbonato o dall'utente. Per questi ultimi, la legge prevede ora il libero utilizzo, ferma restando la necessità che contraenti e utenti vengano sempre adeguatamente informati.

Al riguardo, il Garante ha avviato una consultazione pubblica volta a individuare le modalità semplificate per l'informativa di cui all'art. 13, comma 3, del Codice, da rendere *online* sull'utilizzo dei suindicati dispositivi (provv. 22 novembre 2012, in G.U. 19 dicembre 2012, n. 295 [doc. web n. 2139697]).

Al fine di fornire comunque prime indicazioni sul tema il 18 dicembre 2012 l'Autorità ha anche pubblicato sul proprio sito internet apposite *FAQ* [doc. web n. 2142939].

11.12. LA LOTTA ALLO *SPAM*

Anche nel 2012 il Garante ha ricevuto numerose richieste d'intervento relative ad attività di *spam* realizzata mediante diversi mezzi (posta elettronica, fax, chiamate telefoniche preregistrate, sms); rispetto agli anni precedenti, appaiono diminuite le segnalazioni riguardanti fax indesiderati, anche in ragione dei numerosi provvedimenti inibitori e prescrittivi adottati dall'Autorità, che hanno in taluni casi comportato l'applicazione di sanzioni amministrative di notevole importo.

Fax e e-mail risultano comunque più utilizzati per le attività di *spam* rispetto agli sms.

In un'occasione, l'Autorità, considerato il numero degli interessati e le affermazioni rese dal titolare riguardo alle modalità del trattamento dati, ha adottato un provvedimento inibitorio e prescrittivo (provv. 21 marzo 2012 [doc. web n. 1895176]), di seguito sinterizzato, ed avviato autonomi procedimenti sanzionatori per la contestazione delle sanzioni amministrative previste dagli artt. 161 e 162, comma 2-*bis*, del Codice (note 27 febbraio, 27 e 31 agosto 2012).

Più spesso, quando l'invio di comunicazioni promozionali automatizzate è risultato occasionale, oppure frutto di un mero errore, l'Autorità ha inviato ai titolari del trattamento apposite note di richiamo al pieno rispetto della disciplina in materia (*ex multis* nota 24 maggio 2012).

Anche in materia di *spam* rileva la questione dell'applicabilità del Codice alle persone giuridiche ed agli enti assimilati, poiché il decreto "salva Italia" (d.l. n. 201/2011 convertito con l. 22 dicembre 2011 n. 214) ora include nel concetto di "interessato" di cui all'art. 4 del Codice le sole persone fisiche (v. *supra* par. 2.1.1.).

Fax indesiderati

Il 21 marzo 2012 l'Autorità ha adottato un provvedimento inibitorio e prescrittivo nei confronti di una società italiana svolgente attività di *tour operator* appartenente ad un gruppo spagnolo [doc. web n. 1895176], la quale aveva inviato comunicazioni promozionali indesiderate via fax, talora nonostante l'interessato avesse comunicato più volte alla medesima società il diniego al trattamento dei propri dati personali. Il Garante ha vietato il trattamento dati in essere, prescrivendo altresì di rilasciare un'idonea informativa e di acquisire il consenso degli interessati, specifico, espresso e documentato per iscritto, da ottenere anche qualora i dati siano tratti da elenchi pubblici o da siti web (cfr. provv. 14 luglio 2005 [doc. web n. 1151640] e provv. 2 marzo 2011 [doc. web n. 1802423]).

Invio di fax per l'iscrizione in banche dati a pagamento

Un'associazione, che a sua volta aveva raccolto le lamentele di varie imprese, ha segnalato l'invio a vari destinatari di moduli contrattuali con i quali una società insediata in Slovacchia, affermando di gestire un cd. "registro del mercato nazionale" invitava i destinatari, iscritti a loro insaputa nel registro stesso, a confermare l'esattezza dei dati riportati sui moduli inviati o a fornire quelli corretti.

L'attività è apparsa, in particolare, in possibile contrasto con gli obblighi in materia di informativa e consenso per il trattamento di dati personali, relativi all'invio di comunicazioni promozionali (v. artt. 13 e 23 del Codice). Pertanto, il Garante ha avviato un'apposita cooperazione con l'Autorità slovacca, le cui verifiche hanno evidenziato che i dati erano stati tratti da fonte pubbliche e i destinatari iscritti nel registro *de quo* a loro insaputa.

L'Autorità slovacca ha pertanto impartito precise prescrizioni alla società, con particolare riferimento all'obbligo di rilasciare ai soggetti iscritti nel registro un'informativa idonea indicante i tipi di dati trattati, la loro origine e la possibilità di decidere riguardo al trattamento dati, specialmente quando quest'ultimo sia associato ad eventuali pagamenti.

Mail Spamming

Rimangono numerose le violazioni via e-mail, per le quali talvolta risulta difficile individuare i titolari del trattamento, per le modalità con cui si può operare in rete, sia perché talora i siti mittenti risultano intestati a soggetti fantasiosi o comunque privi di recapiti utilmente contattabili, sia perché spesso essi hanno sede in Paesi *extra*-europei, ove l'Autorità non ha competenza (art. 5 del Codice).

In diversi casi, invece a seguito di istruttorie talvolta anche complesse, L'Autorità ha

verificato che l'invio di fax e, ancor più di e-mail, promozionali indesiderati è stato effettuato da società localizzate in Paesi europei (in particolare, Francia, Svizzera, Regno Unito) ed ha richiesto la collaborazione delle Autorità dei rispettivi Paesi per far cessare gli invii indesiderati.

Talora, queste Autorità hanno richiesto chiarimenti direttamente alle società mittenti, invitandole al rispetto dei diritti degli interessati, sanciti, pur con qualche peculiarità, anche dai rispettivi ordinamenti (nota 19 settembre 2012).

Va però considerato che l'attività di contrasto al fenomeno dello *spam* proveniente dall'estero incontra ancora ostacoli a causa di alcune differenze tra le legislazioni degli Stati europei, non solo in termini di disciplina sostanziale ma anche per quanto attiene alla tutela e ai rimedi azionabili.

In un particolare caso, l'accertamento relativo all'invio di alcune e-mail indesiderate è stata l'occasione per l'adozione di un provvedimento inibitorio e prescrittivo in materia di acquisizione di dati personali *online* per finalità eterogenee (provv. 20 dicembre 2012 [doc. web n. 2223607]). In tale occasione, coerentemente con l'ottica semplificatoria prevalente nella più recente legislazione nazionale, il Garante -oltre a inibire il trattamento dati posto in essere e a dare apposite prescrizioni- ha ricordato, tuttavia, l'eccezione del cd. "*soft spam*", in base al quale, se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso (v. art. 130, comma 4).

Da alcune segnalazioni è emerso che chiunque, accedendo al sito di una nota compagnia di assicurazioni, poteva richiedere preventivi Rca inserendo indirizzi di posta elettronica di altri soggetti ad insaputa di questi ultimi e della stessa compagnia assicuratrice. Il fenomeno ha comportato l'invio massivo ed incontrollato, sulle caselle di posta elettronica di ignari soggetti, di e-mail contenenti preventivi mai richiesti.

Al fine di arginare tale fenomeno l'Autorità, dopo una ampia ed articolata attività istruttoria, da un lato ha verificato l'adozione di misure organizzative e tecniche volte ad

impedire che soggetti ignoti anche alla stessa compagnia, continuassero a sollecitare preventivi non richiesti dagli interessati, dall'altro ha dettato ulteriori accorgimenti a tutela dei dati personali degli ignari titolari di indirizzi di posta elettronica.

In particolare le misure di sicurezza adottate dalla compagnia assicuratrice hanno riguardato:

1) l'attivazione di un apposito elenco di esclusione che consente di bloccare l'invio di e-mail ad utenti che abbiano già lamentato la ricezione di comunicazioni indesiderate;

2) la previsione di un sistema automatizzato di *alert* (nello specifico l'invio di una e-mail di avvertenza) qualora la richiesta di invio di preventivi al medesimo indirizzo di posta elettronica superi una determina soglia nell'arco di una giornata.

A tali misure si è aggiunta la specifica indicazione dell'Autorità di contrassegnare l'e-mail di avvertenza con caratteri, anche grafici, di chiarezza ed immediatezza tali da consentire all'utente sia di distinguerla da altre e-mail ricevute, sia di fornire un più semplice riscontro.

Dopo questi interventi non risultano all'Autorità, ulteriori segnalazioni in merito.

11.13. L'ISTRUTTORIA RELATIVA AD UN SERVIZIO DI TELEFONIA *IP* (INTERNET *PROTOCOL*)

Un utente dei servizi di messaggistica, condivisione *file* e comunicazione vocale offerti dalla società Skype S.a.r.l. ha lamentato l'impossibilità di eliminare definitivamente il proprio *account.*

Come verificato dall'Autorità, le indicazioni contenute nella guida *online* disponibile sul sito internet della società, alla sezione *FAQ*, chiariscono in effetti che "*una volta creato, non è possibile eliminare un account Skype o cambiare un nome Skype. Tuttavia, puoi rimuovere tutti i dati personali contenuti nel tuo profilo*"; con l'avvertenza che, a seguito di tale operazione, "*sarà ancora possibile cercarti tramite il tuo nome Skype*".

Alla richiesta di cancellazione rivoltale dal segnalante la società aveva replicato, invece, che tale operazione è possibile, ma che per consentire una puntuale verifica circa l'identità del richiedente, questi deve indicare mese ed anno di creazione del proprio *account.* Tale adempimento era stato ritenuto dal segnalante troppo oneroso, trattandosi di *account* creato molto tempo prima ed in relazione al quale non aveva tale memoria di dettaglio.

La società, pur sottolineando di essere soggetta alla normativa lussemburghese in materia di protezione dei dati personali (oltre che, ovviamente, alle previsioni della Direttiva n. 95/46/CE) e riconoscendo, pertanto, la competenza esclusiva dell'Autorità Garante del Lussemburgo, ha comunque rappresentato che:

1) le procedure per la verifica dell'identità di chi chiede la cancellazione del proprio *account* sono adottate per minimizzare il rischio che l'istanza provenga da soggetti non autorizzati ovvero abbia carattere fraudolento; inoltre, Skype ha dichiarato di detenere una quantità minima di dati per poter associare un determinato soggetto ad uno specifico *account*, specie se quest'ultimo è gratuito. Né, al riguardo, i documenti di identità sarebbero idonei a comprovare con certezza la riconducibilità di quella persona all'*account* in questione;

2) con riferimento alle *FAQ* del proprio sito, Skype, a seguito dell'intervento dell'Autorità, si è ripromessa di aggiornarle ed eventualmente modificare le procedure atte a consentire agli utenti di chiudere, in autonomia, il proprio *account*. In realtà, le procedure adottabili in modo autonomo dagli utenti possono portare non alla chiusura dell'*account*, ma solo alla cancellazione di una o più delle informazioni presenti sul profilo dell'utente (quali il nome utente o *username*, i dati anagrafici, l'indirizzo e-mail, il numero di telefono). In tale evenienza, lo *username* comunque rimarrebbe, in modo che altri utenti che già ne fossero a conoscenza, sarebbero comunque in grado di contattare quello specifico utente;

3) Skype ha riconosciuto che le *FAQ*, allo stato, non chiariscono che il servizio di supporto tecnico clienti può bloccare permanentemente (non dunque cancellare) l'*account*, rimuovendo lo *username* dalle *directories* pubbliche, in modo che non sia più visibile dagli altri utenti, con la medesima procedura prevista in caso di frodi o abusi.

L'*username* resta in tal caso archiviato dai sistemi della società, per evitare che in futuro altri soggetti possano utilizzare il medesimo nome e indurre confusione negli utenti del servizio. Anche in questa ipotesi, l'utente può comunque rimuovere le proprie informazioni personali dal profilo prima che l'*account* sia bloccato.

Questi chiarimenti hanno evidenziato che, a fronte di una richiesta di cancellazione, Skype si limita in realtà a fornire un servizio di mera deindicizzazione continuando a detenere alcuni dati personali degli utenti.

Permane pertanto la necessità di verificare la tipologia dei dati conservati dopo la chiusura dell'*account*, i tempi e le modalità di tale conservazione, della quale peraltro l'utente potrebbe non essere ben informato.

Per tali motivi, il Garante ha deciso di avviare ulteriori approfondimenti e, data la rilevanza del fenomeno (Skype conta milioni di utenti in tutto il mondo), di ampliare il contesto di riferimento, sottoponendo la tematica all'esame del Gruppo di lavoro *ex* Art. 29.

12. LA PROPAGANDA ELETTORALE E LE ASSOCIAZIONI

In prossimità delle consultazioni elettorali amministrative del 2012 e politiche del 2013, l'Autorità ha approvato due provvedimenti che confermano le regole già stabilite in materia dal provvedimento generale del 7 settembre 2005 ([doc. web n. 1165613], in G.U. 12 settembre 2005, n. 212 Relazione 2005 p. 65), prevedendo speciali casi di esonero temporaneo dall'informativa per partiti, movimenti politici, sostenitori e singoli candidati ed individuando le corrette modalità in base alle quali tali soggetti possono utilizzare a fini di propaganda elettorale i dati personali dei cittadini (es. indirizzo, telefono, e-mail) (provv. 5 aprile 2012 [doc. web n. 1885765], in G.U. 16 aprile 2012, n. 89 e provv. 10 gennaio 2013, in G.U. 14 gennaio 2013, n.11 [doc. web n. 2181429]).

È stato in particolare evidenziato che per contattare gli elettori ed inviare materiale di propaganda possono essere usati, senza il consenso degli interessati, i dati contenuti nelle liste elettorali detenute dai comuni, ovvero nell'elenco degli elettori italiani residenti all'estero, in altre fonti documentali detenute da soggetti pubblici accessibili a chiunque, nonché i dati personali di aderenti ed iscritti e quelli raccolti nel quadro delle relazioni interpersonali avute con cittadini ed elettori.

È invece necessario il consenso qualora si utilizzino dati presenti sul web per altre finalità, ovvero per particolari modalità di comunicazione elettronica quali sms, e-mail, mms, telefonate preregistrate e fax.

Il consenso è altresì obbligatorio per usare sia i dati degli abbonati presenti negli elenchi telefonici, sia i dati relativi a simpatizzanti o ad altre persone già contattate per singole iniziative politiche (ad es., *referendum*, proposte di legge, raccolte di firme).

Non sono invece in alcun modo utilizzabili gli archivi dello stato civile, l'Anagrafe dei residenti, indirizzi raccolti per svolgere attività e compiti istituzionali dei soggetti pubblici o per prestazioni di servizi, anche di cura, liste elettorali di sezione già utilizzate nei seggi, dati annotati privatamente nei seggi da scrutatori e rappresentanti di lista durante operazioni elettorali.

I soggetti che utilizzano i dati per esclusivi fini di selezione di candidati alle elezioni, di propaganda elettorale e di connessa comunicazione politica, vengono esonerati dall'obbligo

di rendere l'informativa, sino alle date indicate nei suddetti provvedimenti, solo nelle ipotesi in cui i dati stessi siano raccolti direttamente dalle predette fonti, oppure il materiale propagandistico sia di dimensioni così ridotte che, a differenza di una lettera o di un messaggio di posta elettronica, non sia possibile inserirvi un'idonea informativa, anche sintetica. Decorso il termine indicato, partiti, movimenti politici, sostenitori e singoli candidati possono continuare a trattare (anche mediante mera conservazione) i dati personali raccolti lecitamente solo informando gli interessati entro il termine indicato nei provvedimenti, nei modi previsti dall'art. 13 del Codice.

Presenta, invece, caratteri di novità il caso postosi nell'ambito delle consultazioni tenutesi in data 25 novembre e 2 dicembre 2012 per l'individuazione del candidato della coalizione di centro-sinistra alla Presidenza del Consiglio dei ministri (cd. "primarie"). Al riguardo l'Autorità (provv. 31 ottobre 2012 [doc. web n. 2079275]) ha esaminato alcuni profili problematici sollevati da un comitato e da alcuni privati cittadini in merito al trattamento dei dati personali dei partecipanti alle operazioni di voto. Tali perplessità traevano origine da alcune disposizioni del relativo regolamento, che prevedeva la necessaria sottoscrizione di un "pubblico appello" e l'iscrizione in un apposito "albo" ai fini della partecipazione alle consultazioni, con connessa possibile diffusione dei dati personali, anche sensibili, degli interessati.

Il Garante, richiamata la natura "sensibile" dei dati trattati e il connesso regime normativo, ha ribadito la necessità di attenersi ai princìpi posti dagli artt. 3 e 11 del Codice, invitando altresì il Comitato della Coalizione (nella dichiarata veste di titolare del trattamento) a stabilire modalità idonee ad evitare forme di diffusione dei dati e ad adottare adeguate misure di sicurezza a tutela dei medesimi. L'Autorità, infine, ha evidenziato la necessità di rendere un'idonea informativa preventiva agli interessati, rinviando, per la disciplina degli ulteriori profili non espressamente considerati, alle disposizioni dell'autorizzazione generale n. 3/2011.

13. LA PROTEZIONE DEI DATI PERSONALI E IL RAPPORTO DI LAVORO PUBBLICO E PRIVATO

Il trattamento di dati personali riferiti a lavoratori, operanti sia nel settore pubblico che privato, continua a interessare le aree già individuate nella precedente edizione (e di seguito menzionate), nelle quali è costantemente richiesto l'intervento dell'Autorità, anche di natura ispettiva (v. *infra* par. 20.).

Segnalazioni e reclami hanno evidenziato profili in parte già trattati in passato (in particolare nel provv. 23 novembre 2006, linee-guida per il trattamento di dati dei dipendenti privati [doc. web n. 1364099], e nel provv. 14 giugno 2007, linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico [doc. web n. 1417809]), con riguardo alle modalità di consegna della documentazione indirizzata al singolo lavoratore (contenente, ad es., contestazioni disciplinari, notizie di carattere valutativo o sanitario), ma pure innovativi, quali la corretta configurazione del protocollo informatico e il conseguente regime (o, semplicemente, la possibilità) di accesso alle informazioni inerenti i singoli lavoratori da parte di altri colleghi.

L'utilizzo delle tecnologie "vecchie" (anzitutto i sistemi di videosorveglianza) e "nuove" (ad es., la geolocalizzazione dei veicoli aziendali e, quindi, indirettamente, dei lavoratori che ne fanno uso) continua a rappresentare una delle principali aree di intervento dell'Autorità.

Diverse segnalazioni, connesse al regime di pubblicità di documenti ed informazioni relativi ai dipendenti pubblici -in larga misura già affrontate nelle menzionate linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico nonché nelle linee-guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web del 2 marzo 2011 [doc. web n. 1793203]- continuano a pervenire all'Autorità ed evidenziano carenze nella puntuale applicazione della disciplina di settore.

A seguito della promulgazione della l. 6 novembre 2012, n. 190 (Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione)

-che solo in parte ha tenuto in considerazione il contenuto della segnalazione al Parlamento e al Governo ai sensi dell'art. 154, comma 1, lett. *f)*, del Codice da parte dell'Autorità (cfr. segnalazione 10 dicembre 2009 [doc. web n. 1693019])- e considerando i quesiti e le richieste che continuano a pervenire, in particolare da parte di società (di regola multinazionali), concernenti le modalità del trattamento di dati personali in relazione alle procedure di segnalazione interna (cd. "*whistleblowing*"), il Garante ha avviato nuovi approfondimenti in materia.

Merita infine segnalare che, senza significative variazioni, è stata rinnovata l'autorizzazione generale n. 1/2012 per il trattamento dei dati sensibili nell'ambito del rapporto di lavoro (provv. 13 dicembre 2012 [doc. web n. 2158817]).

13.1. "CIRCOLAZIONE" DI INFORMAZIONI ALL'INTERNO DEL CONTESTO LAVORATIVO

Numerose sono le segnalazioni e i reclami che lamentano, all'interno del contesto lavorativo, illeciti trattamenti di dati personali ed in particolare informazioni personali rese note ad altri lavoratori (per lo più colleghi) che non ne avrebbero titolo. La fattispecie più segnalata è quella relativa alle modalità di consegna di comunicazioni individuali destinate al lavoratore (aventi il più vario contenuto) cui, con l'introduzione di sistemi di protocollazione elettronica, si sono aggiunte segnalazioni relative alla impropria configurazione di tali sistemi (che consentirebbe l'indebita acquisizione di informazione da parte di colleghi).

Notifica a mano di determinazioni

In più di una circostanza l'Autorità è stata chiamata a pronunciarsi in relazione alla notifica a mano del lavoratore di comunicazioni contenenti dati personali: tali sono stati considerati anche i dati numerici, riassunti in *report* ed elaborati al fine di monitorare l'andamento produttivo di unità organizzative.

È stato in particolare affermato, conformemente a quanto valutato in termini generali dal Gruppo Art. 29 nel Parere n. 4/2007 - WP 136, adottato il 20 giugno 2007, che i dati quantitativi e qualitativi riferiti allo svolgimento dell'attività professionale di un'unità organizzativa di un istituto previdenziale rientrano nell'ampia nozione di dato personale di cui all'art. 4 comma 1, lett. *b)* del Codice, ma non in quello di dato sensibile (provv. 18 ottobre 2012 [doc. web n. 2174351]).

Nel caso di specie, tuttavia, l'Autorità non ha ritenuto violata la disciplina sulla protezione dei dati personali in quanto la consegna nelle mani della reclamante di alcune note dirigenziali contenenti i dati in parola è risultata essere effettuata legittimamente da un'incaricata alla segreteria della dirigente firmataria delle medesime note. È stato infatti accertato, che tra i compiti degli incaricati di segreteria, uno specifico ordine di servizio prevedeva espressamente le attività oggetto di reclamo.

Ove, invece, il personale incaricato non solo della consegna, ma anche di operazioni di trattamento che comportano la conoscenza del contenuto degli atti in parola dovesse "*spillare*" o consegnare "*in busta chiusa*" un documento di cui, in ragione delle mansioni svolte, può legittimamente aver preso conoscenza, si determinerebbe un ingiustificato aggravio di adempimenti in capo al titolare del trattamento.

L'opportunità di siffatte misure è stata invece ribadita nel diverso caso in cui -con particolare riguardo al trattamento di dati sensibili- il titolare si avvalga di personale incaricato del solo recapito (si pensi, ad esempio, ai commessi; cfr. in tal senso, le indicazioni, richiamate anche nel reclamo, fornite in termini generali dal Garante al punto 5.3. delle linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, cit.; non diversamente il punto 5.5. della deliberazione 23 novembre 2006 [doc. web n. 1364939], linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati).

Il Garante ha altresì posto a fondamento della propria decisione il fatto che, anche in relazione alla consegna di documentazione contenente informazioni particolari (e comunque non sensibili) -qual è il caso delle contestazioni disciplinari- l'ordinamento ammette la consegna "*a mano*" del primo atto del procedimento disciplinare contenente la contestazione degli addebiti (cfr. art. 55-*bis*, comma 5, d.lgs. n. 165/2001), contemperando così l'esigenza di speditezza del procedimento e di certezza in capo al datore di lavoro quanto all'avvenuta notificazione della comunicazione all'interessato con la necessità di assicurare la riservatezza del lavoratore. Più in generale, peraltro, il titolare del trattamento può avere un legittimo interesse, specie in relazione a particolari tipologie di atti (ad es., atti

per i quali è stabilito un termine o dalla cui ricezione decorrono particolari effetti), ad acquisire prova dell'avvenuta ricezione degli stessi, che ben può essere precostituita salva l'adozione delle menzionate cautele nell'individuazione dell'incaricato mediante l'apposizione di una sottoscrizione ad opera del destinatario su copia della comunicazione allo stesso diretta (cfr., con riguardo, ad es., alle modalità di consegna di atti contenenti contestazioni disciplinari ovvero dell'atto di recesso, Cass. civ., sez. lav., 1 giugno 1988, n. 3716, e Cass. civ., sez. lav., 4 febbraio 1997, n. 1024).

Analoghe considerazioni sono state svolte in una fattispecie similare (provv. 18 ottobre 2012 [doc. web n. 2174582]), concernente la notifica di determinazioni aventi ad oggetto l'irrogazione di sanzioni disciplinari ad un lavoratore da parte del proprio superiore gerarchico (ancorché *ad interim*).

Protocollo informatico

Come anticipato, il Garante ha chiarito che l'accesso alle informazioni relative ai dipendenti acquisite nel protocollo informatico -il sistema informativo in cui si registrano i documenti in entrata e in uscita di un'azienda o di una pubblica amministrazione- deve essere limitato al solo personale specificamente incaricato di tali trattamenti e non può essere consentito alla generalità indifferenziata degli utenti dei servizi di protocollazione (provv. 11 ottobre 2012 [doc. web n. 2097560]). Nella vicenda oggetto di segnalazione è emerso invece che, presso un'importante sede periferica di un ente pubblico, un ampio numero di dipendenti, indipendentemente dalle mansioni svolte, poteva venire a conoscenza di dati personali, anche relativi all'esecuzione della prestazione lavorativa da parte dei colleghi (quali permessi accordati in base alla l. n. 104/1992, permessi studio, documentazione riguardante sussidi per l'accesso a mense scolastiche o borse di studio ovvero contestazioni disciplinari).

L'Autorità ha accertato la violazione delle disposizioni relative alle misure minime di sicurezza del sistema di protocollazione e gestione documentale, poiché non erano stati individuati e configurati i profili di autorizzazione dei diversi incaricati, così da limitare l'accesso ai dati relativi ai dipendenti al solo personale assegnato a questo compito. Di qui le prescrizioni impartite, per segmentare la visibilità dei documenti e dei fascicoli relativi al personale ai soli dipendenti incaricati del trattamento dei dati; è stato altresì prescritto lo