GLI ASPETTI PENALI DELLA PRIVACY

(*Relazione dell'Avv. Luigi Tramontano al convegno dal titolo "PRIVACY. L'amministrazione condominiale e immobiliare quale responsabile del trattamento dei dati" tenutosi a Palermo, il giorno 15 giugno 2018, presso l'Astoria Palace Hotel)*

§ 1. *Riservatezza e tutela dei dati personali.* – Ritengo necessario premettere che *privacy* è un termine che può generare equivoci. In effetti, se si eccettua il modo con cui è chiamato il D.lgs. n. 196/2003 (*Codice della privacy*), il termine *privacy* non compare in nessuna norma nazionale, e neppure nel Regolamento UE n. 679/2016. Nel diritto inglese *privacy* significa "riservatezza", e il concetto si riferisce quindi, in senso proprio, a ciò che attiene alla sfera intima di ognuno di noi, ossia al significato naturale e più anticamente sentito dall'essere umano. In tale significato forte, la *privacy* è perciò un bene primario e ogni attacco alla stessa integra un reato (in gran prevalenza un delitto: sono quelli di cui agli artt. 614 e segg. c.p.). Invadere l'intimità altrui significa infatti, per ciò stesso, annullarla, e rivelare un aspetto della vita privata di altri può generare tragedie ([1]).

La nostra Costituzione garantisce la riservatezza definendo inviolabili (se non per motivato ordine dell'Autorità Giudiziaria) due suoi baluardi, ossia la "*La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione*" (art. 15), e il domicilio (art. 14). Dispone poi l'art. 8 della Convenzione per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali, che: "*Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza*", salve le possibili interferenze, purché previste dalla legge, da parte di una pubblica autorità.

Ora, l'aspetto preso in considerazione dal Regolamento UE n. 679/2016, e prima ancora dal nostro così detto codice della privacy, è affatto diverso. Non riguarda, se non in

[1] Fin dall'antichità la sfera intima dell'esser umano è ritenuta così inviolabile che ogni aggressione alla stessa merita sanzioni terribili. Mi viene in mente, ad esempio, il mito greco della metamorfosi del corvo, in origine un uccello della scorta del dio Apollo con bellissime piume bianche e d'argento, che, avendo assistito per caso al tradimento di Coronide, fidanzata del dio, glielo rivelò, e Apollo punì l'amata Coronide uccidendola. Subito dopo, però, sopraffatto dal dolore per la gravissima perdita subìta, punì anche il corvo, reo della delazione che aveva provocato una così immane tragedia, e lo trasformò nell'uccello dalle piume funeree che ci appare ancora oggi.

modo eventuale, la riservatezza. Attiene, piuttosto, in un senso molto più ampio, alla persona come individuo capace di scelte consapevoli. Oggetto di tutela di queste normative sono infatti i *dati personali*, intesi come ogni genere di notizie riferibili al nostro essere persone di questo mondo ([2]). L'indirizzo dove abitiamo, il nostro numero di telefono mobile, l'indirizzo della nostra posta elettronica, la targa dell'autoveicolo di cui siamo proprietari, e così via, sono tutti dati personali, ma evidentemente non hanno nulla a che vedere con la nostra sfera intima, o riservata.

Sono dati personali, naturalmente, anche quelli che denotano aspetti *sensibili* della nostra persona, come ad esempio la nostra vita sessuale, il nostro credo religioso, l'appartenenza ad un partito politico o ad una associazione sindacale, o le malattie genetiche e i difetti fisici di cui siamo affetti, i nostri precedenti giudiziari (condanne riportate, procedimenti pendenti, dichiarazioni di fallimento ecc.). Ma – va ribadito – non sono propriamente questi, tra tutti i dati che a vari livelli parlano di noi, quelli cui principalmente si riferisce la tutela apprestata dalla legislazione che stiamo considerando.

Oggetto della quale sono, piuttosto, quei dati che potremmo dire puramente personali, o identificativi, in ordine ai quali – all'opposto che per la riservatezza – vi è l'esigenza di contemperare due interessi contrapposti: da un lato, la necessità, imposta dalla globalizzazione, che i dati circolino liberamente all'interno dei paesi dell'Unione, che è esigenza irrinunciabile ([3]); dall'altro, la libertà dell'individuo di auto determinarsi liberamente.

Il contemperamento è operato in questi termini: la protezione della persona con riguardo al trattamento dei suoi dati non può e non deve limitare in alcun modo la libera circolazione dei dati all'interno dei Paesi dell'Unione. Le misure di protezione, dunque, devono funzionare come strumenti attraverso i quali l'interessato può lamentare che il trattamento di un suo dato non sia avvenuto in modo conforme alla legge, ma non potrà mai avvenire che s'impedisca che i suoi dati circolino nella maniera più ampia possibile (all'interno dell'Unione), ossia che la legge limiti o addirittura vieti tale circolazione.

([2]) L'art. 4 del D.lgs. 196/2003 definisce infatti "dato personale" "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*". La definizione che ne offre il Reg. UE n. 679/2016 è praticamente identica a quella della norma italiana.

([3]) Così, infatti, dispone l'art. 1, comma 3, del Reg. UE: "*La **libera circolazione** dei dati personali nell'Unione **non può essere limitata né vietata** per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*".

§ 2. *Lo scopo della tutela dei dati personali.* – L'argomento di cui ci dobbiamo occupare, dunque, è la tutela dei dati personali, non della *privacy*.

Si è istintivamente portati a pensare, se il tema è questo, al rischio che, facendo acquisti *on-line*, con una carta di credito, possano essere scoperti i nostri *pin* e svuotati i nostri conti correnti in un istante. Neppure questa prospettiva, però, è quella giusta da cui guardare. La pirateria informatica è certamente un pericolo concreto e sempre presente nell'era del commercio via internet. Ma non è tanto questo il pericolo considerato dalle norme di tutela che stiamo esaminando. Il dato personale viene infatti protetto in quanto aspetto della persona ([4]), non in quanto potenziale porta di accesso al suo patrimonio. In altri termini, oggetto di protezione sono gli individui, non i loro beni. Ed inoltre, se è vero che ognuno di noi tratta quotidianamente, soprattutto, propri dati personali (comunicandoli o lasciandoli imprudentemente accessibili ad altri), è altrettanto vero che gli obblighi che la normativa in esame impone di osservare non riguardano chi tratta dati *solo suoi*. Riguarda invece chi tratta dati di altri individui, e proprio per questo.

Ma perché? Perché i "corvi" che oggi dobbiamo temere sono più impalpabili e assai più subdoli degli uccelli in carne e piume cui si riferisce il mito di Apollo ricordato nella nota 1. Uno dei rischi che maggiormente corriamo nell'era digitale è infatti quello connesso al fatto di venire, inevitabilmente, "profilati". Il Regolamento UE definisce così la profilazione: "*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*" (art. 4).

Ed invero, tutte le caratteristiche che di noi, e degli altri, disseminiamo qua e là – i nostri gusti rivelati dai nostri acquisti, gli argomenti che ci interessano dalle nostre ricerche su *google*, ma anche i dati dei nostri clienti, dei nostri assistiti, dei nostri amministrati, e così via esemplificando – consentono a chi è in grado di raccoglierli, di "profilare" gli individui, ossia di farli corrispondere ad una tipologia di consumatore, di lavoratore, di acquirente, di professionista, ma anche di tifoso, di elettore, ecc. Questa attività di catalogare in gruppi omogenei ogni persona, può essere utilizzata – avverte il Regolamento UE n. 679/2016 – "*per adottare decisioni che la riguardano o analizzarne o prevederne le*

([4]) Proclama l'art. 1 del Reg. UE, invero, che "*Il presente regolamento stabilisce norme relative alla* ***protezione delle persone fisiche*** *con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati"*.

preferenze, i comportamenti e le posizioni personali" ([5]), giungendo fino al punto di monitorarne il comportamento ([6]).

Quindi, finché tali profili non possono essere riferiti a persone singolarmente identificabili, si rimane nell'ambito dei normali, e leciti, campionamenti di mercato. Laddove invece a tali profilazioni si accompagni la raccolta di dati che consentano un'identificazione sempre più precisa dell'individuo (dove abita, quanti anni ha, come si chiama, ecc.), allora questi meccanismi possono diventare estremamente pericolosi. Possono consentire di controllarci a distanza, di analizzare i nostri comportamenti, di indirizzare surrettiziamente le nostre scelte, anche non commerciali (ad esempio, a votare in un certo modo: il fatto si sarebbe già verificato, a quanto pare, negli Stati Uniti, in occasione delle ultime elezioni presidenziali) ([7]).

Ecco perché il trattamento negligente di un dato personale in sé e per sé apparentemente incolore, quale ad esempio il recapito telefonico, unito alle altre caratteristiche di chi ne sia l'intestatario, raccolte per altre vie, può diventare il punto debole attraverso il quale è possibile raggiungerci e colpirci. Ed ecco perché, quindi, ognuno di noi deve osservare la massima attenzione nel trattare i dati personali altrui.

§ 3. *I reati previsti dal codice della privacy. La tecnica legislativa.* – Una volta compreso questo, possiamo addentrarci nell'esame della tutela penale riservata al trattamento dei dati personali. In linea generale, va detto che la violazione dei diversi obblighi imposti al titolare del trattamento, o al responsabile, è sanzionata come illecito amministrativo o come reato, secondo la gravità. Tuttavia, in alcuni casi, la stessa condotta di base risulta essere sanzionata sia in via amministrativa che – se ricorrono altre condizioni – penalmente. È appunto questo il caso delle fattispecie di cui ci occuperemo.

La tecnica legislativa seguita per definire ogni figura di reato è infatti quella del rinvio ad altre norme dello stesso codice: ossia, la norma penale stabilisce i presupposti ulteriori per i quali la violazione di un dato obbligo, posto da altra norma cui si rinvia,

---

([5]) In questi termini il *Considerando* n. 24 del Reg. UE.

([6]) Se a qualcuno fosse venuta in mente la condizione in cui sono ridotti a vivere i membri del partito nel celebre romanzo di Orwell (*1984*), non direi che avrebbe sbagliato di molto. Il pericolo connesso alle attività di profilazione, in termini di annullamento delle libertà individuali, è in effetti in tutto identico, sia pur in scala ridotta, allo scenario che il grande scrittore inglese descrive nella sua opera.

([7]) Si teme, com'è noto, che possa essere accaduto quanto segue: uno dei *social network* più frequentati avrebbe venduto ad una società incaricata di organizzare la campagna elettorale di Donald Trump i dati da essa gestiti di milioni di individui, i quali poi sarebbero stati profilati secondo classi di opinioni personali (sulla misura delle tasse, nei confronti delle persone di colore, o degli stranieri, sui meriti e difetti del governo precedente, ecc.). In funzione delle lamentele o delle inclinazioni presentate dalla maggior parte delle persone così raggruppate, sarebbero stati poi indirizzati a ciascuno di loro appositi messaggi elettorali in cui il candidato presidente si impegnava a compiere giusto quelle azioni o prendere quelle decisioni idonee a incontrare il loro pensiero.

integra gli estremi di un reato. Va osservato, incidentalmente, che questa tecnica legislativa non è certamente la più indicata al fine di garantire l'effettiva conoscenza di ciò che è penalmente vietato e di ciò che non lo è, e quindi appare confliggere con il principio di trasparenza che, invece, dovrebbe permeare (almeno nella dichiarazione d'intenti che apre il testo normativo in esame) tutta la regolamentazione in materia. In realtà, la trasparenza è necessaria per rendere edotto il cittadino dei suoi diritti riguardo all'uso che si faccia dei suoi dati personali; laddove invece si tratti di un divieto sanzionato penalmente vale l'opposto principio – fissato dall'art. 5 del c.p. – per cui l'ignoranza della legge non scusa.

§ 4. *Le figure criminose di possibile interesse per un amministratore di condominio. A) Trattamento illecito dei dati.* – I reati previsti dal codice della privacy di cui un amministratore di condominio debba preoccuparsi sono essenzialmente quelli previsti dall'art. 167 (*Trattamento illecito dei dati*) e dall'art. 169 (*Omessa adozione di misure minime di sicurezza*) del D.lgs n. 196/2003. La prima norma configura dei delitti, la seconda una contravvenzione. Il che vuol dire, praticamente, che di quest'ultima si risponde anche se il fatto sia stato commesso per colpa (mentre dei delitti si risponde solo per dolo).

Dispone l'art. 167 del D.lgs. n. 196/2003:

"1. *Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19,* ***23****, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.*

2. *Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25,* ***26****,* ***27*** *e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni*".

Si tratta quindi di tre gruppi di delitti, se si guarda alle tre diverse sanzioni comminate dalla norma. Sono tutti reati comuni, dato che possono essere commessi da "*chiunque*". Perciò è irrilevante, sotto questo profilo, la soluzione che si voglia dare al quesito se l'amministratore di condominio debba considerarsi *titolare* oppure *responsabile* del trattamento.

Un trattamento illecito di dati, dunque, può realizzarsi in diversi modi, uno per ogni violazione di ciascun obbligo sancito dagli articoli cui il testo della norma in esame rinvia. Un amministratore di condominio, però, può effettivamente incorrere solo nelle violazioni degli obblighi sanciti nell'art. 23 (per quanto riguarda i delitti di cui al primo comma) e

dagli artt. 26 e 27 (per quanto riguarda il delitto di cui al secondo comma), perché tutte le altre norme richiamate nell'art. 167 stabiliscono obblighi che incombono su altre figure.

Le fattispecie di cui al primo comma consistono essenzialmente nel trattare un dato personale altrui in assenza di *consenso* dell'interessato. Se il trattamento senza consenso consiste in particolare nella "comunicazione" o nella "diffusione" di dati, il trattamento illecito è punito più gravemente. Per *comunicazione* s'intende il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, anche mediante la loro messa a disposizione o consultazione; per *diffusione*, invece, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Il reato previsto dal secondo comma consiste a sua volta nel trattare illecitamente (ossia in violazione degli obblighi stabiliti dagli artt. 26 e 27) *dati sensibili* o *giudiziari*, ossia quei dati il cui trattamento è soggetto a rigorosi limiti che vanno ben oltre il consenso dell'interessato. Proprio per la tipologia del dato che ne è oggetto, questo delitto è sanzionato più gravemente rispetto ai due precedenti.

Le tre categorie di ipotesi delittuose presentano per il resto elementi comuni che si possono esaminare congiuntamente. Innanzitutto, ogni reato si configura solo se il trattamento compiuto in violazione degli obblighi imposti dalle norme richiamate dall'art. 167 provochi un "nocumento" all'interessato: ossia, "*un pregiudizio giuridicamente rilevante di qualsiasi natura, patrimoniale o non patrimoniale*" (così Cass. pen., Sez. III, 23 novembre 2016, n. 15221).

Sotto il profilo soggettivo, oltre il dolo generico, ossia la volontà di violare l'obbligo riguardante il trattamento, è richiesto anche un dolo specifico: il trattamento illecito deve essere infatti effettuato (oltre che volontariamente, anche) al fine di trarre profitto, per sé o per altri, o di recare ad altri un danno. Una di queste due finalità deve animare, dunque, la volontà colpevole, ma per quanto riguarda il profitto è sufficiente che il comportamento sia posto in essere per tale scopo, non anche che un profitto in concreto si sia realizzato ([8]).

I reati di cui all'art. 167 si configurano solo se il fatto realizzato non integri un altro reato, "più grave" (cosiddetta clausola di *sussidiarietà*). In particolare, come abbiamo già detto, quando la violazione del dato personale integra un'offesa alla riservatezza della persona – nei due aspetti della libertà della corrispondenza o della inviolabilità del

[8] Non mi sento di concludere nello stesso modo per quanto riguarda il dolo di danno, dato che il reato si configura solo se il trattamento illecito abbia in effetti provocato un "nocumento" all'interessato, che è la stessa cosa di provocargli un danno; per la giurisprudenza più recente, del resto, il nocumento è ritenuto essere appunto l'evento del reato (non una condizione obiettiva di punibilità), dunque deve essere voluto dal reo. Si tratterebbe, quindi, più di un dolo intenzionale che di un dolo specifico, ove il reato si consumi provocando un danno ad altri. Se invece non si verifica alcun nocumento (e di conseguenza nessun danno), il reato non si consuma; rimane tuttavia punibile a titolo di tentativo se l'agente aveva comunque l'intenzione di danneggiare l'interessato.

domicilio – si applicheranno le norme previste dal codice penale, e non quella prevista dal codice della privacy.

Va infine segnalato che a norma dell'art. 5, comma 3, del D.Lgs. n. 196, il trattamento di dati personali effettuato da persone fisiche *per fini esclusivamente personali* è soggetto alla applicazione del codice solo se i dati sono destinati ad una comunicazione "sistematica" o alla diffusione. Il che significa che, ove il trattamento sia effettuato non per fini esclusivamente personali, qualsiasi privato può commettere il reato di cui all'art. 167, anche mediante la semplice comunicazione (ossia, con una comunicazione *una tantum*).

§ 5. Segue*: Il trattamento senza consenso.* – Per quanto riguarda le ipotesi di trattamento senza consenso (art. 167, comma 1), è sufficiente ricordare che l'art. 23 è appunto la norma che impone di trattare dati personali altrui solo dietro consenso "espresso" dell'interessato, e che stabilisce che tale consenso, oltre che poter riguardare l'intero trattamento o solo alcune operazioni di trattamento, per essere considerato *valido* deve essere liberamente prestato, documentato per iscritto, e informato (pertanto, l'adempimento degli obblighi di informativa sono un presupposto necessario della validità del consenso dell'interessato). Se il trattamento riguarda dati sensibili, poi, occorre che il consenso sia anche "manifestato" per iscritto (e non solo documentato in tale forma da chi lo raccoglie).

Pure va però ricordato che, ai sensi dell'art. 24 del codice, il consenso della persona cui si riferiscono i dati non è necessario in diversi casi, tra i quali merita segnalare – per i profili qui d'interesse – quello in cui il trattamento sia imposto da una legge (ad esempio, per l'amministratore di condominio gli è prescritto dall'art. 1130 c.c. di tenere il registro di anagrafe condominiale ([9]), nonché il registro dei verbali di assemblea ([10])), e quello in cui il trattamento sia necessario per eseguire obblighi derivanti da un contratto del quale l'interessato sia parte: è anche questo, ovviamente, il caso dell'amministratore di condominio, incaricato contrattualmente dall'assemblea dei condomini di svolgere i suoi compiti. I dati dei singoli condomini che servono all'amministratore per eseguire il suo mandato possono essere raccolti dunque senza necessità di consenso ([11]). È chiaro tuttavia

([9]) Com'è noto, tale registro deve contenere "*le generalità dei singoli proprietari e dei titolari di diritti reali e di diritti personali di godimento, comprensive del codice fiscale e della residenza o domicilio, i dati catastali di ciascuna unità immobiliare, nonché ogni dato relativo alle condizioni di sicurezza*", ossia tutti dati personali.

([10]) I quali possono contenere anche delle "*brevi dichiarazioni dei condomini che ne hanno fatto richiesta*", ossia delle posizioni o opinioni personali.

([11]) Ma si faccia attenzione in questo ambito: l'amministratore riceve l'incarico, e stipula quindi un contratto, con i proprietari delle singole unità immobiliari che compongono il condominio, non anche con i rispettivi familiari di questi. I dati dei quali, dunque, se occorre, devono essere acquisiti e trattati sempre con il loro esplicito consenso.

che, nei casi di che trattasi, il consenso non è necessario solo per l'uso dei dati che risponda alla finalità per cui il trattamento stesso è imposto dalla legge o reso necessario per l'esecuzione del contratto. L'uso del dato per fini diversi, quindi, ha di nuovo necessità del consenso dell'interessato.

ESEMPIO 1*: L'amministratore del condominio raccoglie i numeri telefonici di tutti i condomini. Successivamente fornisce il numero telefonico del condomino Tizio al condomino Caio, che ha necessità di contattarlo perché lamenta che dall'appartamento di Tizio proverrebbe acqua infiltratasi nel suo appartamento. In realtà Caio è uno scocciatore, che finisce per importunare inutilmente Tizio, dato che in seguito viene accertato che nell'appartamento di questi non si era verificata alcuna perdita d'acqua. Tuttavia Tizio aveva dovuto, a seguito della chiamata, rientrare in fretta in città (egli lavorava fuori e soleva rientrare nell'appartamento all'incirca una volta al mese), e perdere un giorno di lavoro.*

Abbiamo visto sopra in quali casi, ai sensi dell'art. 24, un dato sia trattabile senza necessità del consenso dell'interessato. Il numero del telefono portatile di Tizio non ricade in nessuno di questi casi, perché non si trovava inserito in alcun elenco conoscibile da chiunque, Tizio lo aveva individualmente fornito all'amministratore per essere raggiunto eventualmente da costui, e non da altri, non abitando stabilmente l'appartamento; né era necessario all'amministratore per eseguire le sue obbligazioni contrattuali, perché tra queste non rientra certo quella di raccogliere le lamentele di un condomino verso un altro riguardanti le proprietà singole. Pertanto, si trattava di un dato personale la cui "comunicazione" a terzi doveva essere espressamente consentita da Tizio, al momento in cui l'amministratore del condominio aveva raccolto il dato, costituendosi così "titolare" del suo trattamento. L'amministratore, pertanto, fornendo il numero telefonico di Tizio a Caio aveva in effetti trattato un dato personale di Tizio in violazione dell'art. 23, ossia in assenza di un consenso espresso specificamente con riguardo a quella forma di trattamento in concreto effettuata. Dal fatto, tuttavia, non era derivato un "nocumento" giuridicamente apprezzabile per Tizio, perché tale non può essere considerato il mero fastidio provato nel dover raccogliere la lamentela del vicino, posto che ogni cittadino è tenuto a rispondere dei danni cagionati dai propri beni, a prescindere dal fatto che la lamentela altrui sia fondata o meno. Inoltre, l'amministratore non ha di certo agito al fine di trarre un profitto (per sé o per altri), o di recare un danno a Tizio. Anzi, prestando fede alla richiesta di Caio, riteneva di contribuire a risolvere un problema.

§ 6. Segue: *Il trattamento illecito di dati sensibili o giudiziari*. – Quanto al delitto di cui al secondo comma dell'art. 167 vengono in rilievo, come visto, le violazioni degli obblighi stabiliti negli artt. 26 e 27, i quali riguardano le condizioni per il trattamento, rispettivamente, dei dati "sensibili" e di quelli "giudiziari". Sono entrambe eventualità che ben difficilmente dovrebbero interessare un amministratore di condominio, e in relazione alle quali basti qui dire che, fondamentalmente, il trattamento di tali dati è consentito solo

se autorizzato da un'espressa previsione di legge o provvedimento del Garante. Ma si guardino le vicende che seguono.

ESEMPIO 2: *Tizio, amministratore di condominio, deve eseguire la delibera assembleare che ha stabilito di affidare ad una persona qualificata il servizio di portierato, delegandolo a selezionare il più adatto dopo aver pubblicizzato in forme idonee la relativa offerta di lavoro. Alla selezione si presenta un solo candidato, e Tizio, nel colloquio preliminare, dopo avergli chiesto le referenze gli chiede di portargli il certificato del casellario giudiziale. Il candidato esegue, ma dal casellario risulta che egli ha riportato una condanna per il reato di rissa. Pertanto, il candidato non verrà assunto.*

L'amministratore non può chiedere il certificato penale all'aspirante portiere (né di nessun altro individuo). In quanto "*Il trattamento di dati giudiziari da parte di privati o di enti pubblici economici è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili*" (art. 27 D.lgs n. 196/2003). Com'è stato di recente chiarito dallo stesso Garante ([12]), cui il quesito era stato rivolto, non vi è nessuna norma di legge che consenta una richiesta del genere, perciò l'amministratore viola la privacy dell'interessato nell'acquisire il suo certificato del casellario, anche se questi ha acconsentito a portarglielo. Non è possibile proprio il trattamento, in questo caso, quindi anche la mera raccolta del dato in questione, a nulla rilevando il consenso dell'interessato. Tuttavia, anche qui, l'amministratore commette il reato di cui all'art. 167 comma 2, solo se abbia posto in essere tale violazione a scopo di profitto o di recare ad altri un danno. Il nocumento, dalla violazione commessa, è certamente derivato, perché l'interessato ha dovuto svelare una macchia del suo passato, al suo interlocutore. Ma il fine dell'amministratore di conseguirne un profitto (o di recare ad altri un danno) non c'è in questo caso. Infatti, egli non poteva sapere se il certificato giudiziale dell'aspirante portiere contenesse iscrizioni. Diverso sarebbe stato se, invece, l'amministratore sapeva, sia pur vagamente, che quel soggetto aveva un passato discusso, e avesse voluto sfruttare ciò per non assegnargli l'incarico di portiere. In una simile ipotesi avrebbe in effetti agito con il dolo richiesto dalla norma penale.

Al riguardo appare opportuno chiarire che, nel selezionare il portiere, non può neppure chiedersi ai candidati di rilasciare un'autocertificazione, sotto la loro responsabilità, circa l'assenza di condanne riportate o di procedimenti penali pendenti, perché anche per tale via la segretezza del dato giudiziario sarebbe evidentemente violata.

ESEMPIO 3: *Il condominio di cui è amministratore Tizio ha adottato un sistema di video sorveglianza. È previsto che le immagini registrate rimangano memorizzate al massimo per 48 ore, e che dopo siano automaticamente cancellate. Incaricato della visione delle immagini è lo stesso amministratore dello stabile, ed è stabilito che egli le può visionare solo se si verifica un fatto di danneggiamento ai beni di*

([12]) Vedi Garante Privacy, provv. n. 267 del 15 giugno 2017.

proprietà condominiale, oppure periodicamente, per effettuare la manutenzione ordinaria dell'impianto. Ebbene, in una di tali occasioni, nel rivedere le immagini, Tizio nota l'arrivo nell'androne della signora Sempronia – moglie del signor Sempronio, inquilini del secondo piano – accompagnata da un giovane, mano nella mano, e poi i due che si scambiano un bacio appassionato davanti la porta dell'ascensore. Essendo Tizio molto amico di Sempronio, decide di informarlo, e di conservare le immagini della condotta fedifraga. Perciò, estratte le immagini, le consegna a Sempronio, il quale, dopo qualche tempo, presenta un ricorso per separazione giudiziale dalla moglie, con addebito, e produce il detto filmato.

Non è chi non veda che Tizio si è comportato in questo caso esattamente come il corvo del mito ricordato nella nota 1. Tradotto nel linguaggio del codice della privacy, egli ha "trattato", comunicandolo a Sempronio, un dato sensibile di una persona (tali sono infatti, fra gli altri, "*i dati personali idonei a rivelare… la vita sessuale*"), non solo per un fine del tutto diverso da quello per cui il dato stesso era stato legittimamente raccolto, ma soprattutto in difetto del consenso scritto di questa. Ha dunque violato l'art. 26 D.lgs. n. 196/2003 (per il quale "*I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante*…"), e il trattamento illecito ha certamente prodotto un nocumento a Sempronia, la cui reputazione è stata compromessa. Tizio, infine, ha trattato illecitamente il detto dato non certo per un fine di profitto suo o dell'amico cui lo ha rivelato, ma comunque per produrre a Sempronia un danno, dacché egli ha consegnato l'immagine registrata a Sempronio affinché questi la potesse portare nel giudizio di separazione come prova che la causa della rottura del matrimonio andava addebitata alla moglie. Tizio, pertanto, verrà condannato per il reato di cui all'art. 167, comma 2, D.lgs n. 196/2003. Sempronio no, invece. Infatti, in soccorso di Tizio non può addursi la disposizione di cui all'art. 5, comma 3, del codice, perché se è vero che egli si è limitato a comunicare ad una sola persona il dato (non, dunque, una comunicazione sistematica, né una diffusione), tuttavia non lo ha fatto *per fini esclusivamente personali*, dacché certamente non era il suo matrimonio quello che veniva qui in discussione, ma quello di un'altra persona. Né può applicarsi a Tizio l'esimente prevista dall'art. 26, comma 4, lett *c*, del D.Lgs. n. 196/2003, il quale prevede che i dati sensibili possono essere oggetto di trattamento anche senza il consenso dell'interessato, ma previa autorizzazione del Garante, "*quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla L. 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile*". Il Garante periodicamente autorizza in via generale e provvisoria il trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale quando, appunto, sia necessario per lo svolgimento delle investigazioni difensive o comunque per far valere un diritto in qualsiasi sede (nel caso di specie vigeva l'autorizzazione n. 2 del 16/12/2009, pubblicata sulla G.U. n. 13 del 18 gennaio 2010, valida fino al 30/06/2011), ma Tizio non aveva nessun diritto da far valere, in una qualsiasi sede, rivelando a Sempronio la violazione dei doveri matrimoniali

di sua moglie. Sempronio si, all'opposto, e per questo motivo questi è stato assolto dall'identico reato per cui Tizio è stato invece condannato.

§ 7. *La video sorveglianza all'interno dei condomini.* – Il caso appena esaminato offre lo spunto per esplorare la disciplina della video sorveglianza all'interno di un edificio condominiale.

Un sistema di video sorveglianza comporta la raccolta, la registrazione, la conservazione e in generale, l'utilizzo di immagini, e perciò configura un trattamento di dati personali (art. 4, D.lgs. n. 196/2003), a volte – come abbiamo appena visto – perfino sensibili. È in effetti uno strumento altamente invasivo della nostra individualità, perché, data la capillare diffusione di telecamere, la nostra vita è continuamente ripresa da un occhio implacabile, come accade al protagonista del film *The Truman Show*, attore involontario della sua stessa vita.

La normativa sul trattamento dei dati personali, tuttavia, non scoraggia più di tanto l'adozione di tali sistemi. E il motivo è duplice: da un lato, come già ampiamente detto all'inizio, la tutela dei dati personali non si incentra affatto sulla tutela della riservatezza, a questa provvedendo piuttosto le norme del codice penale. Dall'altro, quello di essere tutti quanti sempre visibili si considera come un prezzo necessario da pagare al fine di scoraggiare azioni delittuose altrui. Assistiamo quotidianamente a casi in cui l'autorità di Pubblica Sicurezza riesce a risalire all'autore di un certo misfatto proprio esaminando le immagini raccolte dalle telecamere poste, a tutt'altri fini, da negozi, istituti di credito, condomini, ecc.

Un sistema di video sorveglianza, tuttavia, come ogni trattamento di dati personali, deve rispondere ai principi valevoli nella materia.

Viene in considerazione, innanzitutto, il principio così detto della "limitazione delle finalità", ossia quello per cui i dati personali devono essere "*raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi*" (art. 11, D.lgs. n. 196/2003) ([13]).

Nel caso del condominio in quanto tale, centro di imputazione distinto dai singoli condomini, il primo problema attiene proprio alla limitatezza dello scopo per cui può dirsi "*legittimo*" adottare un sistema di video sorveglianza. Si desume infatti dall'art. 1122-*ter* c.c. che la video sorveglianza sia legittima solo ove consenta di sorvegliare le "parti comuni" dell'edificio condominiale, quindi se la sua finalità sia esclusivamente quella di tutelare la proprietà comune. Non anche la sicurezza dei singoli condomini, la quale,

([13]) Negli stessi termini, l'art. 5, lett. *d*, del Reg. UE dispone che i dati personali siano "*raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità*".

invero, non è oggetto di condominio. L'esigenza di proteggersi dai ladri di appartamento, dunque, non legittima l'installazione di un sistema di video sorveglianza condominiale ([14]).

L'adozione all'interno del condominio di un sistema di video sorveglianza deve essere deliberata dall'assemblea con la maggioranza ordinaria di cui all'art. 1136, comma 2, c.c. (maggioranza degli intervenuti che rappresentino almeno la metà del valore dell'immobile). Una volta deliberata l'adozione del sistema, la sua concreta messa in opera deve soddisfare le condizioni stabilite dal d.lgs. n. 196/2003, come chiarite e specificate nel provvedimento dell'8 aprile 2010 del Garante per la privacy e nell'apposita guida "*Il condominio e la privacy*" pubblicata dal Garante stesso (e facilmente reperibile *on-line*).

In linea generale, prima di installare un sistema di video sorveglianza è necessario richiedere al Garante una "*verifica preliminare*", tutte le volte che detta installazione comporti "*rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare*" ([15]).

Né il provvedimento dell'8 aprile 2010, né la guida, dicono però nulla di specifico con riguardo al condominio. Ritengo quindi prudente consiglio quello che gli amministratori inoltrino la richiesta di verifica preventiva al Garante.

Senza bisogno di considerare casi particolarissimi (ad esempio, tra i condomini vi sia un collaboratore o un testimone di giustizia sottoposto a protezione, oppure una clinica privata che si occupi di procreazione assistita), va infatti rilevato che in un edificio condominiale le aree e gli spazi di proprietà individuale sono molto più estese di quelli comuni. E perciò, nell'installare una telecamera di video sorveglianza, sia pur destinata a riprendere solo ed esclusivamente le parti comuni (androne, portineria, scale, ascensore, area parcheggio, ecc.), di norma non sarà possibile escludere con certezza assoluta, *a priori*, che il raggio d'azione della telecamera non possa finire per cadere, anche in caso di spostamenti accidentali o fortuiti, su parti che invece non devono assolutamente potersi riprendere (uscio del singolo appartamento, box in uso esclusivo, ecc.). Sussiste quindi, in

---

([14]) Accadrà sovente che l'assemblea condominiale, pur dichiarando in sede di adozione dello strumento della video sorveglianza che la relativa finalità è quella indicata dall'art. 1122-ter c.c., di fatto la vorrà adottare proprio per proteggersi dai ladri di appartamento o da altri malintenzionati che possano attentare alla sicurezza dei singoli condomini. Ciò però non ha alcun rilievo. Si pensi, ad esempio, al caso che all'interno del condominio si verifichi effettivamente un'aggressione ai danni di un condomino. A stretto rigore, l'amministratore (o l'incaricato) non potrebbe utilizzare le immagini riprese dalla video camera per individuare e denunciare l'aggressore, perché un simile trattamento esulerebbe dalle finalità per cui la video sorveglianza è stata installata. Tuttavia, può senz'altro acquisire quelle immagini l'Autorità Giudiziaria, quindi è sufficiente che il condomino aggredito denunci l'aggressione ricevuta al più vicino posto di polizia, e rappresenti che l'area in cui egli è stato aggredito è sottoposta a video sorveglianza. Sarà in questo caso la stessa Autorità Giudiziaria a raccogliere le immagini che eventualmente riprendano l'aggressione, a fini di prova. Non violando la privacy di nessuno.

([15]) Punto 3.2.1 del Provvedimento del Garante dell'8 aprile 2010.

astratto, il *rischio* di violare un diritto fondamentale, qual è il domicilio privato, definito inviolabile, come abbiamo visto, dalla nostra Costituzione. E si tratta di un rischio *specifico*, appunto perché sorge proprio in ragione della normale contiguità tra aree comuni e spazi privati, in un edificio condominiale ([16]).

Del resto, il provvedimento in materia di video sorveglianza stabilisce espressamente che la richiesta di verifica preliminare non sia necessaria nei soli casi in cui: "*a) il Garante si sia già espresso con un provvedimento di verifica preliminare in relazione a determinate categorie di titolari o di trattamenti; b) la fattispecie concreta, le finalità del trattamento, la tipologia e le modalità d'impiego del sistema che si intende adottare, nonché le categorie dei titolari, corrispondano a quelle del trattamento approvato; c) si rispettino integralmente le misure e gli accorgimenti conosciuti o concretamente conoscibili prescritti nel provvedimento di cui alla lett. a) adottato dal Garante*" ([17]). Ora, non risulta che il Garante abbia ad oggi adottato un provvedimento di verifica preliminare riguardante la categoria degli edifici condominiali. Probabilmente sarà indotto a farlo, tra qualche tempo, proprio se le richieste di verifica preliminare da parte dei condomini aumentassero in modo considerevole ([18]).

Discorso ulteriore deve farsi riguardo ai condominii che abbiano un servizio di portierato (o comunque altre figure di lavoratori che operino al loro interno). Com'è noto, a seguito del D.lgs. n. 151/2015 (cosiddetto *jobs Act*), non esiste più il divieto esplicito per il datore di lavoro di utilizzare impianti di ripresa per finalità di controllo a distanza dei lavoratori, ma si ritiene comunque che il divieto sia implicitamente rimasto. Infatti, il nuovo art. 4 dello Statuto dei Lavoratori (L. n. 300/1970) prevede ora che è consentito al datore di lavoro di installare un sistema di video sorveglianza nella sua azienda dal quale possa derivare la possibilità di controllare a distanza il lavoratore, "*esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale*" (quest'ultima finalità è la novità introdotta dal *jobs Act*); il che viene comunemente inteso che, al di fuori di tali finalità consentite, detti sistemi non possano essere adottati.

Il punto è però che risulta arduo estendere questa norma al caso del condominio, perché il concetto giuridico di "*patrimonio aziendale*" non è facilmente sovrapponibile a

---

([16]) La richiesta di verifica preliminare, del resto, mette al sicuro l'amministratore da un altro rischio. Quello che la verifica sia condotta *d'ufficio* dal Garante, magari perché sollecitato in tal senso da uno o più condomini che avevano votato contro l'adozione della video sorveglianza, ritenendola inutilmente invasiva. La sola attivazione di un intervento simile espone il responsabile del trattamento almeno ad una sanzione amministrativa, proprio perché non ha chiesto la verifica preliminare, e salve le altre eventuali violazioni che l'ispettore del Garante dovesse rilevare a seguito dell'intervento.

([17]) Punto 3.2.2 del Provvedimento dell'8 aprile 2010 del Garante.

([18]) Per quanto è a mia diretta conoscenza, sono attualmente assai rare le richieste di verifica preliminare inoltrate da un condominio al Garante per la privacy.

quello di beni in proprietà comune, alla cui protezione la video sorveglianza in un condominio deve essere volta. In ogni caso, ove si seguisse l'art. 4 dello Statuto dei Lavoratori, il condominio dovrebbe richiedere apposita autorizzazione all'ufficio locale dell'Ispettorato del Lavoro per poter installare le video camere, perché questo prevede la norma in esame.

Se invece si programma la video sorveglianza in modo che essa si accenda solo nelle ore in cui non lavori il portiere, il problema si risolve alla base, perché in un caso del genere non è necessario richiedere e ottenere nessuna autorizzazione dato che l'impianto in effetti non riprenderà mai il lavoratore ([19]).

Per il resto, può rapidamente dirsi che le immagini registrate dal sistema di video sorveglianza devono essere conservate per poche ore (al massimo 24 o 48 negli intervalli festivi), e potranno essere visionate, da apposito "incaricato" (che può essere lo stesso amministratore), solo ove si verifichi un fatto di danneggiamento, oppure per effettuare le manutenzioni periodiche dell'impianto. Così come non deve essere puntata verso gli spazi in proprietà individuale, ogni telecamera non può nemmeno riprendere le aree esterne all'edificio condominiale (marciapiede antistante il portone, esercizi commerciali, altri edifici, ecc.). I dati raccolti devono essere poi protetti con idonee misure, tese ad evitare che possano essere carpiti da persone diverse da quelle espressamente autorizzate (misure di sicurezza). Infine il sistema di video sorveglianza deve rispettare gli obblighi di informativa prescritti dal codice.

A tale ultimo fine è sufficiente apporre un cartello che indichi che l'area è sottoposta a video sorveglianza, che la finalità consiste nella tutela della proprietà comune (non nel garantire la sicurezza dei condomini), e chi sia il titolare o il responsabile del trattamento dei dati. L'avviso va però posizionato prima del raggio di azione di ogni telecamera, e se queste funzionano anche di notte deve essere dotato di adeguata illuminazione per potere essere letto.

L'inosservanza dell'obbligo di adeguata informativa soggiace all'applicazione di una mera sanzione amministrativa (che può essere tuttavia molto salata), mentre la mancata adozione delle misure minime di sicurezza, come vedremo subito, configura il reato di cui all'art. 169 del codice ([20]).

([19]) Si consideri, del resto, che l'installazione di un sistema di video sorveglianza che rimanga in funzione anche durante le ore in cui vi sia il portiere potrebbe essere ritenuta non necessaria (e quindi violare il principio di proporzionalità) dagli ispettori del Garante della privacy, proprio perché tra le mansioni del portiere vi è proprio quella di custodire i beni comuni del condominio.

([20]) Tutte queste norme non deve invece osservare il singolo condomino che decida di installare una telecamera per proteggere la sua proprietà e, magari, anche per garantire la sicurezza dei suoi familiari. In questo caso, infatti, il trattamento dei dati è effettuato *per fini esclusivamente personali*, perciò, ai sensi dell'art. 5 del D.lgs. n. 196/2003, non è soggetto all'applicazione delle norme del codice della privacy. Né il resto del condominio ha il potere di vietarlo, sicché l'amministratore non si prenda mai carico di un problema

§ 8. *B) Omessa adozione di misure minime di sicurezza.* – Dispone l'art. 169, comma 1, D.lgs. n. 196/2003:

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

La contravvenzione consiste, dunque, nell'omettere di adottare le misure "minime" di sicurezza. Il reato non si configura nel caso siano state adottate misure di sicurezza rivelatesi *ex post* insufficienti o inidonee, ma solo nel caso di totale assenza di misure. Di questa contravvenzione, come già detto, si risponde anche per colpa, ossia anche se l'omessa adozione sia dovuta a mera negligenza, e non solo se frutto di scelta volontaria.

In linea con il principio dell'incentivo all'adeguamento tardivo valevole in genere per le contravvenzioni, anche per il caso di che trattasi è previsto un meccanismo che consente all'autore del reato di ottenere l'estinzione del reato stesso se adempie alle prescrizioni che gli verranno impartite al momento dell'accertamento, entro il termine fissatogli ([21]).

Cosa debba intendersi per "misure minime" di sicurezza varia ovviamente a seconda della categoria di dati che vengono in considerazione, ma fondamentalmente si tratta di tutti quelli accorgimenti di base da adottare per evitare che i dati possano andare persi o distrutti, oppure abusivamente carpiti da terzi. E quindi, esemplificando, se si tratta di dati raccolti in un supporto cartaceo, occorre quanto meno custodirli in appositi scomparti, possibilmente chiusi a chiave, e dotare l'immobile in cui sono custoditi di un impianto antincendio; se si tratta di dati raccolti in supporti informatici, occorre quanto meno installare un congruo antivirus, effettuare il backup periodicamente e salvare i dati in un supporto fisicamente separato, e così via ([22]).

---

del genere. Piuttosto è a dirsi che se una telecamera di questo tipo sia in grado di inquadrare anche parti dell'edificio condominiale in proprietà esclusiva di altri, allora il condomino che l'abbia installata commette il delitto di interferenze illecite nella vita privata (art. 615 c.p.), e chi subisce l'interferenza potrà chiedere all'Autorità Giudiziaria, previa denuncia, di disporre il sequestro dell'impianto di video sorveglianza illecito.

([21]) Dispone infatti il comma 2 dell'art. 169: "*All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili*".

([22]) Invero, l'art. 33 del codice, al quale come si è visto rimanda l'art. 169, non è affatto esaustivo perché rinvia a sua volta ad altre norme del codice. Dispone infatti l'art. 33 cit.: "*Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo (...) volte ad assicurare un livello minimo di protezione dei dati personali*". Si tratta del capo II del Titolo V del codice, e le misure minime di sicurezza sono dunque quelle stabilite negli articoli 34 (*Trattamento con strumenti elettronici*), e

Esempio 4: *Tizio, amministratore del condominio, inserisce mensilmente nelle buche delle lettere dei condomini, le note relative alle quote da versare. In ogni nota, oltre all'importo dovuto per quella corrente, compare, eventualmente, l'ammontare della mora del singolo condomino in ordine a quote arretrate. Poiché dette note vengono inserite in modo da poter essere sfilate dalla buca senza doverla necessariamente aprire con la chiave, qualunque condomino può vedere, aprendo una nota diretta ad un altro, se questi è moroso.*

Il condomino che effettuasse una simile azione commetterebbe il reato di cui all'art. 616 c.p., anche se si tratta di corrispondenza aperta (però, a lui non diretta), nella misura in cui la sottrae, sia pur temporaneamente, per leggerla. Ma anche a prescindere dal fatto che qualcuno apra la nota di altri, l'amministratore ha comunque omesso in un caso simile di adottare la misura minima di sicurezza per evitare che i dati personali contenuti in ogni singola nota potessero essere abusivamente carpiti (sarebbe bastato, ad esempio, mettere ciascuna nota in una busta chiusa), e quindi ha violato l'art 169 Dlgs. n. 196/2003.

---

35 (*Trattamento senza l'ausilio di strumenti elettronici*), sulle quali si sono soffermati in dettaglio i relatori che mi hanno preceduto. Di nuovo, può dirsi, che la tecnica legislativa non brilli esattamente per precisione e accuratezza.