La protezione dei dati personali e il ruolo del Garante in ambito pubblico*

Licia Califano

Keywords: dati personali, privacy, GDPR, Garante Privacy, direttiva 95/46

Con l'occasione dell'approvazione e pubblicazione del cd. "pacchetto protezione dati" da parte dell'Unione europea, questo Volume intende ripercorrere i venti anni da quando il diritto alla protezione dei dati personali – per convenzione linguistica "diritto alla privacy" – ha fatto il suo significativo ingresso nella legislazione italiana. Un diritto di natura costituzionale, fondamentale, che oggi si costruisce sul concetto di autodeterminazione informativa quale potere del singolo di decidere quale parte di sé, sotto forma di informazioni, far conoscere agli altri, stabilendo altresì chi debbano essere i destinatari, per quali fini e con quali modalità e limiti. Un diritto che, nel nostro Paese, ha un grosso debito di riconoscenza nei confronti degli impulsi provenienti dall'esterno: dal sistema CEDU e dall'Unione europea, dalle loro Carte e Corti, dagli atti da essi derivati. Ma anche l'opera interpretativa svolta sul piano interno dai giudici ha avuto un ruolo importante nell'orientare il processo di codificazione normativa.

Tutto ciò ha quindi portato il legislatore a licenziare la cornice giuridica che, a partire dal 1996, garantisce e rende effettiva la tutela del diritto. Da qui la l. 675/1996 e, successivamente, il d.lgs. 196/2003, noto come "Codice privacy". E tra i principali strumenti di garanzia è prevista un'apposita Autorità amministrativa indipendente, il Garante per la protezione dei dati personali, il cui ruolo è ormai consacrato al livello massimo europeo dalla Carta dei diritti fondamentali dell'Ue (art. 8, c. 3) e dal Trattato sul funzionamento dell'UE (art. 16, c. 2), nonché valorizzato dal nuovo regolamento UE generale in materia (2016/679).

Fatta questa doverosa premessa, si tratta di capire come il diritto alla privacy sia stato fino ad oggi garantito nel sistema nazionale del potere pubblico, e quale sia stato il ruolo svolto dal Garante in questo processo di vigilanza e tutela. Nel fare ciò, non si può non partire da una breve sintesi del quadro giuridico che è stato disegnato.

Occorre in primo luogo ricordare che si parla della specificità dei trattamenti in ambito pubblico, essendo stata una precisa scelta del legislatore italiano normare questo settore in maniera unitaria, ponendo regole di carattere generale per tutti i trattamenti ivi svolti. La direttiva 95/46/CE aveva in proposito lasciato ampia discrezionalità agli Stati membri, limitandosi a fornire dei criteri trasversali (in particolare, cfr. gli artt. 7, par. 1, lett. *e)*, e 8, par. 4); e la l. 675/1996 aveva in qualche modo ripreso lo schema proposto dalla c.d. direttiva madre, dedicando ai trattamenti posti in essere da parte di soggetti pubblici una sola disposizione specifica (l'art. 27), salvo comunque prevedere singole clausole disseminate in tutto l'articolato.

Invece, il legislatore del 2003, proprio al fine di fornire un testo unico in materia di protezione dei dati personali che fosse il più sistematico, efficace e intellegibile possibile, ha dedicato interi contenitori alla disciplina esclusiva e specifica per i trattamenti posti in essere in ambito pubblico. In quest'ottica vanno pertanto collocati il capo dedicato alle regole generali proprie per i soggetti pubblici (artt. 18-22), il titolo dedicato a profili settoriali (artt. 59-74); per non parlare di quei settori del mondo pubblico soggetti a regole ancor più peculiari, come, per citarne alcuni, l'ambito giudiziario (artt. 46-49), securitario (artt. 53-57) o sanitario (artt. 75-94). Questa scelta di certo rende più facile

* Il presente contributo è precedentemente comparso come prefazione al volume G. Busia – L. Liguori – O. Pollicino (a cura di), Le nuove frontiere della privacy nelle tecnologie digitali: bilanci e prospettive, Roma, 2016, pubblicato in occasione del ventennale del Garante per la protezione dei dati personali. Il contributo non è stato, pertanto, sottoposto a referaggio.

per le pubbliche amministrazioni (intese in senso lato) districarsi in una normativa che nel nostro Paese è entrata in vigore più tardi che altrove, e in maniera anche più dirompente (ricordiamo che fino al 1996 l'Italia era infatti priva di una disciplina organica sulla protezione dei dati personali, si trovavano solo specifiche disposizioni disseminate in singoli settori, a partire dallo Statuto dei lavoratori del 1970).

Per quanto riguarda invece alcune delle specificità contenutistiche proprie della normativa privacy dedicata al settore pubblico, non si può non rilevare come essa si costruisca su una regola di base che funge da spartiacque rispetto alla parte dedicata invece all'ambito privato. Mentre in quest'ultimo mondo – cioè quello dei rapporti contrattuali, dei settori produttivi, dell'economia e del commercio, del nesso sinallagmatico tra prestazioni e profitto – il principale (ancorché non esclusivo) presupposto a legittimare il trattamento è il consenso dell'interessato (artt. 23 e 24), in quello delle pubbliche amministrazioni il perseguimento di finalità di carattere istituzionale rende cedevole predetto strumento (cfr., in particolare, l'art. 18, c. 2 e 4).

E il fondamento specifico di questi trattamenti non deve per forza risiedere in una disposizione normativa (art. 19, c. 1), salvo poi alcune significative eccezioni – a partire dalle operazioni di comunicazione e diffusione, per le quali la norma è imprescindibile: art. 19, c. 2 e 3. È d'altra parte evidente che i soggetti pubblici, per esistere e funzionare legittimamente, devono comunque avere alla base una legge che li istituisca e attribuisca loro funzioni di carattere pubblico.

Questa costruzione giuridica non contraddice affatto il concetto di autodeterminazione informativa, che si costruisce essenzialmente sull'istituto del consenso informato, per affidare all'individuo il potere di scelta sull'ambito di circolazione dei propri dati personali**,** e che attiene al tema del confine tra libertà e loro esercizio da parte di ciascuno. Al contrario, essa si innerva sulla forma di Stato stessa, intesa come il rapporto tra governati e governanti, all'interno di quel "contratto sociale" che sta alla base del vincolo di cittadinanza: se il potere pubblico, soprattutto nella sua forma di Stato democratico-sociale, è tenuto a fornire servizi alla collettività di riferimento, allora per farlo deve poter disporre delle informazioni necessarie (ed esponenzialmente crescenti) all'espletamento della propria missione, anche di carattere personale. In questa prospettiva vanno dunque inserite le recenti tendenze alla digitalizzazione della pubblica amministrazione, a partire, ad esempio, dal Sistema pubblico dell'identità digitale (Spid), in cui il flusso di dati personali tra cittadini ed enti, nonché tra enti stessi, costituisce (dovrebbe costituire) il presupposto per assicurare l'efficacia ed efficienza delle prestazioni, ma al contempo lo snellimento della burocrazia e la riduzione dei costi.

Ovviamente, proprio perché si sta parlando di un ordinamento costituzionale liberaldemocratico, gli apparati pubblici devono disporre di questi dati nel rispetto dei limiti generali di necessità, finalità, proporzionalità, a garanzia delle libertà individuali; e, in ultima analisi della dignità della persona, di cui il diritto alla privacy costituisce presidio irrinunciabile.

Tra le regole generali che governano i trattamenti di dati personali effettuati da parte di soggetti pubblici non possiamo tralasciare le garanzie specifiche con cui sono rivestiti i dati sensibili e giudiziari (artt. 20-21), cioè quelle informazioni dotate di un più elevato tasso di delicatezza in ragione del potenziale discriminatorio che possono dispiegare se

conosciuti e trattati in maniera inappropriata. Discende dunque da qui l'esigenza che tali dati siano trattati per finalità di rilevante interesse pubblico che trovino specifica base in una norma di legge; e laddove quest'ultima non sia sufficientemente dettagliata, allora si deve costruire un dialogo tra amministrazioni e Garante al fine di legittimare questi trattamenti. Il tutto, nella doverosa consapevolezza della loro indispensabilità per lo svolgimento delle attività istituzionali che si intende porre in essere, poiché in gioco ci sono le libertà fondamentali e la dignità della persona umana (art. 22).
Garanzie che si fanno ancora più robuste quando ad essere trattati sono i dati cd. "supersensibili", cioè quelli idonei a rivelare lo stato di salute (e, in parte, anche quelli idonei a rivelare la vita sessuale), legati a doppio filo con l'essenza più intima della persona. In questa prospettiva, pertanto, viene riproposta la necessità di acquisire il consenso dell'interessato (art. 18, c. 4) – salvo poi prevedere delle importanti semplificazioni a vantaggio delle strutture e dei professionisti della sanità (artt. 75 ss.) –, come anche viene imposto un divieto assoluto e insuperabile di diffusione (art. 22, c. 8).
Il quadro giuridico appena descritto, però, non può non fare i conti con la realtà fattuale, caratterizzata da tanti fattori che influenzano e indirizzano l'effettiva tutela del dato personale. Si deve pertanto considerare che l'imponente accelerazione del progresso tecnologico cui abbiamo assistito negli ultimi anni (e cui stiamo tuttora assistendo) ha inevitabilmente investito anche il settore pubblico: da qui, la proliferazione di banche dati pubbliche, la velocizzazione e moltiplicazione dei flussi informativi, l'interconnessione crescente tra gli archivi. A ciò si aggiunga la complessità della società odierna, con fenomeni economici e sociali di carattere globale che hanno reso il dato personale un bene preziosissimo (anche in termini monetari quantificabili), la cui condivisione è assurta al rango di attività umana privilegiata: la rete internet ha infatti consentito un vero e proprio accorciamento delle distanze fisiche, anche tra cittadini e amministratori. Inoltre, non dobbiamo dimenticare che ciclicamente si propongono "emergenze" che spingono il potere pubblico ad allargare i propri spazi di azione e quindi a comprimere le sfere di libertà individuale, attraverso massicce operazioni di controllo sui dati personali: si pensi, ad esempio, alla c.d. sorveglianza di massa avviata in risposta alla riaccesa recrudescenza del pericolo terroristico.
In questo snodo cruciale tra *Sein* e *Sollen*, tra essere e dover essere, un ruolo fondamentale lo svolge (e lo ha costantemente svolto) il Garante per la protezione dei dati personali. Come affermato anche dalla recente e fortemente garantistica giurisprudenza della Corte di giustizia, l'Autorità rappresenta infatti il custode dei principi che regolano il governo della privacy, coniati in sede europea ma ormai pienamente applicati in ciascuno dei suoi Stati membri. In questa sua veste di controllore della conformità dei trattamenti, e grazie al *know-how* e all'esperienza di cui dispone, essa rappresenta il punto di snodo in cui si rende possibile allineare quadro normativo e realtà empirica.
E questa sua collocazione si rende evidentemente ancor più strategica nel contesto pubblico. Infatti, se nel settore privato prevale la componente vigilante, quando i trattamenti sono svolti da parte di soggetti pubblici il Garante è anzitutto un interlocutore in grado di orientare le politiche dell'ente nella direzione più appropriata in termini di tutela della privacy. Questa natura consultiva è evidente nelle funzioni espressamente

affidate dal Codice (cfr. in via generale l'art. 154, c. 1, lett. *g)*, n. 4 e 5, ma, per aspetti specifici, anche gli artt. 19, c. 2 e 20, c. 2 e 3). Ma essa è ancor prima connaturata in una logica più sistematica di leale collaborazione: nella convinzione che agendo in via preventiva, con indicazioni puntuali e raccomandazioni sensibilizzanti, è possibile giungere a trattamenti leciti e proporzionati, e quindi evitare violazioni e conseguenti provvedimenti di carattere repressivo e/o punitivo.

Per chiarire meglio l'importanza di questa delicata funzione svolta dal Garante, si veda quanto fatto su due temi piuttosto centrali: sanità digitale e trasparenza delle pubbliche amministrazioni. Si tratta di due settori di intervento che rendono al meglio l'idea di quanto la cooperazione del Garante con le istituzioni pubbliche del Paese (Legislatore, Governo, dicasteri, enti territoriali, altre Autorità di controllo, strutture sanitarie, pubbliche amministrazioni di ogni ordine e grado) possa produrre dei risultati reali e tangibili in termini di aumento del livello di protezione dei dati personali degli individui.

Per quanto concerne l'ambito sanitario, anche qui lo sviluppo delle tecnologie dell'informazione e della comunicazione non ha tardato a far sentire il proprio decisivo apporto, soprattutto quando si discute di efficientamento delle prestazioni di cura offerte al paziente. Ma se la semplificazione degli adempimenti, l'incremento delle potenzialità di archiviazione e, al contempo, di comunicazione delle informazioni sul paziente, la velocizzazione delle procedure, lo snellimento dei processi organizzativi, la riduzione dei costi sono certamente obiettivi di politica pubblica legittimi, nell'ottica del bilanciamento tra diritti fondamentali occorre non compromettere la protezione dei dati personali. Nello scenario di una sanità sempre più digitale, sono inevitabilmente aumentate le banche dati contenenti informazioni sullo stato di salute dei pazienti in relazione ad eventi clinici presenti e trascorsi (come, ad esempio, i referti medici, la documentazione relativa a ricoveri, gli accessi al pronto soccorso, ecc.), accessibili da parte degli operatori sanitari, affinché sia consentito loro di conoscere immediatamente il quadro clinico dei pazienti che hanno in cura e, quindi, effettuare le migliori diagnosi e prognosi. La sanità elettronica ha pertanto ricevuto dal Garante una particolare attenzione e cautela, nella ferma convinzione che la tutela della privacy rappresenti, oltre ad un ineliminabile momento di salvaguardia della dignità della persona, un *quid pluris* nella prestazione dei servizi dovuti ai cittadini.

In questi anni si registrano tanti interventi decisivi dell'Autorità – mi limito qui a ricordare solo alcuni temi: referti online, servizi telematici di prenotazione delle prestazioni, telemedicina, interconnessione sanitaria, schede di dimissione ospedaliera, sistema tessera sanitaria –, ma quello che negli ultimi anni si è posto all'attenzione di tutta la comunità è il Fascicolo sanitario elettronico e il dossier sanitario aziendale, cioè i principali archivi in cui tende a confluire tutta la storia clinica degli assistiti dal servizio sanitario pubblico (il primo gestito dalle Regioni, il secondo formato da ciascuna struttura di cura). Il Garante, prima tra tutte le principali istituzioni, nel 2009 ha fornito un quadro di indicazioni tramite Linee guida, affinché questi due strumenti fossero creati e governati nel rispetto della volontà dei pazienti e di un quadro minimo di garanzie di tutela dei dati.

Poi le strade di Fse e dossier si sono divise, essenzialmente per la scelta del legislatore di

regolamentare solo il primo, probabilmente con l'obiettivo finale di superare la frammentazione dovuta alla presenza di raccolte operate autonomamente dai singoli istituti di cura. E così, sulla base dell'art. 12 del d.l. 179/2012, si è avviato il dialogo tra Garante, Ministeri interessati (Salute, Lavoro, Economia), Regioni (quali titolari dei servizi sanitari territoriali), Agid (per gli aspetti infrastrutturali), per la definizione del quadro regolamentare di dettaglio, nonché delle misure tecniche necessarie per l'implementazione del Fse: il parere reso dall'Autorità il 22 maggio 2014 sul regolamento attuativo (poi divenuto d.P.C.M. 178/2015) condensa perfettamente la sinergia di intenti e contenuti maturata in questo primo importante passaggio di un percorso ancora lungo.

Per quanto riguarda invece il dossier sanitario aziendale, la strada si è rivelata più faticosa e accidentata: in primo luogo perché è del tutto assente una cornice normativa di base; in secondo luogo perché i titolari del trattamento sono le strutture sanitarie, e quindi numerosissimi e sparsi su tutto il territorio nazionale, e soprattutto tutte scoordinate tra di loro. L'esito è stato che sono giunte all'Autorità numerose segnalazioni di violazioni del Codice privacy, che, a seguito di accertamenti anche ispettivi, hanno condotto il Garante ad adottare numerosi provvedimenti inibitori, prescrittivi e sanzionatori, al fine di riportare questi organismi in un quadro di conformità ai principi e alle regole della protezione dati. Alla luce di questa esperienza, il Garante ha compiuto uno sforzo ulteriore, adottando, il 4 giugno 2015, delle nuove Linee guida, questa volta dedicate al solo dossier sanitario elettronico, in modo da orientare le politiche di gestione del dato da parte degli organismi sanitari, e quindi prevenire fenomeni di accessi abusivi o trattamenti non autorizzati.

Anche il secondo tema che intendo toccare è indicativo del grande lavoro svolto dal Garante ai fini di una migliore garanzia di protezione del dato personale, attingendo alla varietà di compiti che costellano la sua architettura funzionale: ci si riferisce al sempre più influente aspetto della trasparenza della struttura e dell'attività delle pubbliche amministrazioni, il cui impatto sulla privacy dei cittadini tutti (dai vertici politici ai dirigenti amministrativi, dai dipendenti ai collaboratori a vario titolo, ai comuni cittadini) può essere estremamente invasivo. La trasparenza delle informazioni chiama inevitabilmente in causa anche gli individui: e non tutte le notizie che riguardano le tantissime persone coinvolte sono necessarie a soddisfare il bisogno della collettività di sapere come la macchina burocratica opera; e comunque ci sono categorie di informazioni che devono in ogni caso essere protette, poiché concernono strettamente, appunto, la dignità degli individui.

In questa prospettiva il Garante si è sempre mosso nella convinzione che individuare strumenti di pubblicità rispettosi della privacy degli individui significa modellare in maniera soddisfacente il potere pubblico nell'equilibrio tra conoscenza (dell'attività) e riservatezza (delle persone): è giusto consentire la circolazione delle informazioni necessarie affinché la pubblica opinione possa controllare l'operato dei pubblici poteri ma, al contempo, è doveroso garantire un elevato livello di protezione dei dati riguardanti le singole persone, in modo da evitare che vengano resi ostensibili dati personali inutili a fini di trasparenza, ma che abbiano implicazioni afflittive sulla dignità degli interessati; peraltro, in taluni casi le informazioni pubblicate sono così delicate da rivelare

aspetti anche intimi della vita privata delle persone, rispetto alle quali l'"accessibilità totale" diventa particolarmente invasiva.
Infatti, è proprio la cd. accessibilità totale la prospettiva su cui si è mosso il legislatore negli ultimi anni, in particolare con i due cruciali decreti legislativi che hanno riordinato il frastagliato panorama della pubblicità di atti e documenti per finalità di trasparenza. Il primo è il d.lgs. 33/2013, costruito esclusivamente sugli obblighi di pubblicazione di informazioni sui siti web istituzionali, ai fini di consentire il controllo sociale sull'utilizzo delle risorse pubbliche e in ottica di prevenzione dei fenomeni di corruzione e *maladministration*. Il secondo invece è il d.lgs. 97/2016, di modifica del testo unico precedentemente citato, il quale amplia gli obiettivi per giungere fino alla realizzazione della piena partecipazione dei cittadini alla vita democratica: e lo fa primariamente introducendo una forma di accesso generalizzato che ricorda nelle modalità l'accesso ai documenti amministrativi di cui alla l. 241/1990, ma con requisiti e limiti molto meno stringenti (come l'esonero dalla necessità di dimostrare sia un interesse qualificato che una motivazione).
Il Garante ha così potuto sollevare criticità e suggerire soluzioni che tenessero in maggiore considerazione le fondamentali esigenze di riservatezza dei cittadini interessati, muovendosi lungo le direttrici fornite dai suoi principi ispiratori: necessità, finalità, proporzionalità e liceità. Quindi, l'Autorità ha fornito pareri preventivi al Governo in occasione dell'emanazione dei due decreti legislativi (rispettivamente, datati 7 febbraio 2013 e 3 marzo 2016); ha emesso le proprie Linee guida (15 maggio 2014), un utile strumento rivolto alle pubbliche amministrazioni, per aiutarle nell'adempimento degli obblighi di pubblicazione online con un'attenzione alla massima tutela possibile del dato personale; ha prodotto una vasta mole di interventi censori (sotto forma di divieti, prescrizioni e sanzioni pecuniarie) nei confronti di amministrazioni che, nel diffondere documenti, hanno violato il Codice privacy. Nel momento in cui si sta scrivendo, il Garante è coinvolto in uno stretto dialogo con l'Autorità nazionale anticorruzione per disegnare assieme, sulla base di un preciso obbligo normativo, i limiti e le esclusioni al «diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni», introdotto nel 2016 e ispirato al modello del Freedom of information act.
Quanto detto finora riguarda il passato e il presente. Per il futuro, il regolamento (UE) 2016/679 pone l'Autorità di fronte a nuove sfide. Senza scendere nel dettaglio dei cambiamenti (per certi versi epocali) che il regolamento apporterà, mi limito solo a fornire uno spunto circa la nuova disciplina della protezione dei dati personali (e al ruolo dell'Autorità di vigilanza) rispetto all'ambito pubblico.
Anzitutto, da un punto di vista metodologico, il regolamento generale non distingue chiaramente tra trattamenti effettuati da titolari pubblici e titolari privati, trattando unitariamente i presupposti di liceità del trattamento (art. 6, par. 1), e quindi mettendo sullo stesso piano l'«esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri» con l'istituto consenso e con gli altri requisiti alternativi. In questo, il regolamento rappresenta la naturale continuazione dell'impostazione fatta propria dalla direttiva madre del 1995; tuttavia, ai fini di applicazione interna, dato che l'operatore del diritto dovrà fare i confronti con il Codice privacy, verrà avvertito lo

stacco netto rispetto al paradigma che ha retto fino ad oggi. Si tratterà di capire se questa novità, per la realtà italiana, avrà anche dei riflessi sulla sostanza del quadro di tutele. Venendo ai contenuti con riferimento allo specifico ambito pubblico, il regolamento lascia in effetti un certo margine di discrezionalità al legislatore interno, con riferimento sia ai dati personali cd. comuni (art. 6, parr. 2 e 3) che a quelli sensibili (art. 9, par. 2, in particolare lett. *g*), peraltro con particolare attenzione ai dati genetici, biometrici e sulla salute (art. 9, par. 4). Il che deve dunque spingere in prima battuta il legislatore stesso, avvalendosi anche dell'esperienza maturata dall'Autorità, a valutare: se mantenere in piedi il Codice, quanta parte di esso conservare, dove e come intervenire con una novazione; ciò sapendo che le elevate garanzie attualmente previste dal d.lgs. 196/2003 non risultano necessariamente incompatibili con il quadro regolamentare europeo. Si pensi, ad esempio, all'efficacia dimostrata dal meccanismo messo in piedi sul trattamento dei dati sensibili e giudiziari da parte degli enti pubblici (artt. 20 e 21 del Codice), con il proficuo dialogo tra: organizzazioni rappresentative (si pensi alla Conferenza delle Regioni o alla Conferenza dei Rettori), autrici degli schemi tipo di regolamenti; singole amministrazioni (dai Ministeri agli enti locali), competenti a redigere il proprio regolamento interno, conforme allo schema tipo laddove presente; Garante, in funzione consultiva a tutela delle esigenze di privacy.

Si presti infine attenzione a due novità di grande impatto, che potranno effettivamente imprimere una svolta rilevante in termini di accrescimento delle garanzie. In primo luogo, il legislatore nazionale, nel legiferare entro gli ambiti cui si faceva cenno, dovrà perseguire «un obiettivo di interesse pubblico» che sia «proporzionato all'obiettivo legittimo perseguito» (art. 6, c. 3, ultimo periodo): in altre parole, gli atti normativi interni dovranno rispettare il principio di proporzionalità, pena la sua non conformità al regolamento europeo; dopodiché, si tratterà di capire quale organo giustiziale sarà competente a sindacarne la legittimità: cioè se la Corte costituzione o la Corte di giustizia, o entrambe. In secondo luogo, il legislatore stesso, prima di approvare qualsiasi legge che comporti il trattamento di dati personali, dovrà consultare l'Autorità di vigilanza (art. 36, c. 4): finora, invece, la normativa coinvolgeva la funzione consultiva del Garante solo con riferimento agli atti di natura regolamentare o amministrativa, quindi, appare evidente il passo in avanti compiuto dal Garante, e delle tutele che esso può assicurare.

In conclusione, diventa inevitabile immaginare come la combinazione di queste due innovazioni rappresenti un sensibile rafforzamento della protezione dei dati personali, e quindi della tutela della dignità della persona, poiché fornisce un indirizzo univoco alle garanzie di carattere sostanziale, cioè quelle contenute nelle norme, che alle garanzie di natura istituzionale, ossia quelle connesse all'attività di controllo assicurata dal Garante.