Ciò, comporta l'improrogabile esigenza di assicurare che almeno alcuni tra gli accorgimenti e le misure di cui al precedente punto 7, limitatamente a quelli adattabili al caso di specie, siano applicati comunque dai predetti fornitori nell'ambito di analoghi trattamenti di dati di traffico telefonico e telematico effettuati per finalità non di giustizia, ma di fatturazione, pagamento in caso di interconnessione e commercializzazione di servizi, nel più breve periodo temporale indicato nel menzionato art. 123.

Per tali ragioni il Garante, contestualmente e distintamente da quanto va disposto ai sensi dell'art. 132, comma 5, del Codice, prescrive ai fornitori di cui al paragrafo 3, ai sensi dell'art. 17 del medesimo Codice, di adottare nel termine e con la modalità di cui al paragrafo 7.10. le misure e gli accorgimenti indicati nella lettera c) del seguente dispositivo.

Copia del presente provvedimento verrà trasmessa al Ministero della giustizia, anche ai fini della sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana a cura dell'Ufficio pubblicazione leggi e decreti, nonché, per opportuna conoscenza, all'Autorità per le garanzie nelle comunicazioni.

TUTTO CIÒ PREMESSO IL GARANTE:

a) ai sensi degli artt. 17, 123 e 132, comma 5, del Codice, prescrive ai fornitori di servizi di comunicazione elettronica individuati nel paragrafo 3 di adottare nel trattamento dei dati di traffico telefonico e telematico di cui al paragrafo 4 le misure e gli accorgimenti a garanzia degli interessati individuate nel presente provvedimento, provvedendo a (par. 7):

   1. adottare specifici sistemi di autenticazione informatica basati su tecniche di strong authentication, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione, che si applichino agli accessi ai sistemi di elaborazione da parte di tutti gli incaricati di trattamento, nonché di tutti gli addetti tecnici (amministratori di sistema, di rete, di data base) che possano accedere ai dati di traffico custoditi nelle banche dati del fornitore, qualunque sia la modalità, locale o remota, con cui si realizzi l'accesso al sistema di elaborazione utilizzato per il trattamento, evitando che questo possa aver luogo senza che l'incaricato abbia comunque superato una fase di autenticazione informatica nei termini anzidetti. Per i dati di traffico trattati per esclusive finalità di accertamento e repressione dei reati, una di tali tec-

nologie deve essere basata sull'elaborazione di caratteristiche biometriche dell'incaricato, in modo tale da assicurare la presenza fisica di quest'ultimo presso la postazione di lavoro utilizzata per il trattamento. Tali modalità di autenticazione devono essere applicate anche a tutti gli addetti tecnici (amministratori di sistema, di rete, di data base) che possano accedere ai dati di traffico custoditi nelle banche dati del fornitore. Relativamente ai soli addetti tecnici indicati al presente punto 1, qualora circostanze legate a indifferibili interventi per malfunzionamenti, guasti, installazioni hardware e software, aggiornamento e riconfigurazione dei sistemi, determinino la necessità di accesso informatico a sistemi di elaborazione che trattano dati di traffico in assenza di strong authentication, fermo restando l'obbligo di assicurare le misure minime in tema di credenziali di autenticazione previste dall'Allegato B. al Codice, deve essere tenuta traccia dell'evento in un apposito "registro degli accessi", nonché delle motivazioni che li hanno determinati, con una successiva descrizione sintetica delle operazioni svolte, anche mediante l'utilizzo di sistemi elettronici. Tale registro deve essere custodito dal fornitore presso le sedi di elaborazione e messo a disposizione del Garante nel caso di ispezioni o controlli, unitamente a un elenco nominativo dei soggetti abilitati all'accesso ai diversi sistemi di elaborazione con funzioni di amministratore di sistema, che deve essere formato e aggiornato costantemente dal fornitore.

2. adottare specifiche procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati. Il fornitore deve definire e attribuire agli incaricati specifici profili di autorizzazione differenziando le funzioni di trattamento dei dati di traffico per finalità di ordinaria gestione da quelle per finalità di accertamento e repressione dei reati e, infine, dalle funzioni di trattamento dei dati in caso di esercizio dei diritti dell'interessato (art. 7 del Codice);
3. adottare, per la conservazione dei dati di traffico per esclusive finalità di accertamento e repressione di reati, sistemi informatici distinti fisicamente da quelli utiliz-

zati per gestire dati di traffico anche per altre finalità, sia nelle componenti di elaborazione, sia di immagazzinamento dei dati (storage). I dati di traffico conservati per un periodo non superiore ai sei mesi dalla loro generazione possono, invece, essere trattati per le finalità di giustizia sia prevedendone il trattamento con i medesimi sistemi di elaborazione e di immagazzinamento utilizzati per la generalità dei trattamenti, sia provvedendo alla loro duplicazione, con conservazione separata rispetto ai dati di traffico trattati per le ordinarie finalità. Le attrezzature informatiche utilizzate per i trattamenti di dati di traffico per le esclusive finalità di giustizia di cui sopra devono essere collocate all'interno di aree ad accesso selezionato (ovvero riservato ai soli soggetti legittimati ad accedervi per l'espletamento di specifiche mansioni) e munite di dispositivi elettronici di controllo o di procedure di vigilanza che comportino la registrazione dei dati identificativi delle persone ammesse, con indicazione dei relativi riferimenti temporali. Nel caso di trattamenti di dati di traffico telefonico per esclusive finalità di giustizia, il controllo degli accessi deve comprendere una procedura di riconoscimento biometrico. Infine, il fornitore deve adottare misure idonee a garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici in tempi compatibili con i diritti degli interessati e comunque non superiori a sette giorni;

4. designare specificamente gli incaricati che possono accedere ai dati di traffico conservati per le finalità di cui all'art. 132 del Codice, anche per consentire l'esercizio dei diritti di cui all'art. 7 del Codice medesimo. Il processo di designazione deve prevedere la documentata frequenza di una periodica attività formativa concernente l'illustrazione delle istruzioni, il rispetto delle misure di sicurezza e le relative responsabilità. Per quanto riguarda le richieste per l'esercizio dei diritti di cui all'art. 7 del Codice che comportano l'estrazione dei dati di traffico, nei limiti in cui ciò è consentito ai sensi dell'art. 8, comma 2, lettera f) del Codice, il fornitore deve conservare in forma specifica la documentazione comprovante l'idonea verifica dell'identità del richiedente ai sensi dell'art. 9 del Codice stesso, e adottare opportune cautele per comunicare i dati al solo soggetto legittimato in base al medesimo articolo;

5. rendere i dati di traffico immediatamente non disponibili per le elaborazioni dei sistemi informativi allo scadere dei termini previsti dalle disposizioni vigenti. Il fornitore deve cancellare o rendere anonimi senza ritardo tali dati, in tempi tecnicamente compatibili con l'esercizio delle relative procedure informatiche, nei data base e nei sistemi di elaborazione utilizzati per i trattamenti nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza (backup e disaster recovery) effettuate dal titolare anche in applicazione di misure previste dalla normativa vigente e, al più tardi, documentando tale operazione entro i trenta giorni successivi alla scadenza dei termini di cui all'art. 132 del Codice;
6. adottare soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti sui diversi database utilizzati. Tali soluzioni comprendono la registrazione, in un apposito audit log, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici. I sistemi di audit log devono garantire la completezza, l'immodificabilità, l'autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad auditing. A tali scopi il fornitore deve adottare, per la registrazione dei dati di auditing, anche in forma centralizzata per ogni impianto di elaborazione o per datacenter, sistemi di memorizzazione su dispositivi non alterabili. Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche;
7. svolgere, con cadenza almeno annuale, un'attività di controllo interno per verificare costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati di traffico previste dalle norme vigenti e dal prov-

vedimento del Garante, anche per ciò che riguarda la verifica della particolare selettività degli incaricati legittimati. Tale attività di controllo deve essere demandata a un'unità organizzativa o, comunque, a personale diverso rispetto a quelli cui è affidato il trattamento dei dati per la finalità di accertamento e repressione dei reati. I controlli devono comprendere anche verifiche a posteriori, a campione o su eventuale allarme derivante da sistemi di Alerting e di Anomaly Detection, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento. Sono svolte, altresì, verifiche periodiche sull'effettiva cancellazione dei dati decorsi i periodi di conservazione. L'attività di controllo deve essere adeguatamente documentata in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate. L'esito dell'attività di controllo deve essere: comunicato alle persone e agli organi legittimati ad adottare decisioni e ad esprimere, a vari livelli in base al proprio ordinamento interno, la volontà della società; richiamato nell'ambito del documento programmatico sulla sicurezza nel quale devono essere indicati gli interventi eventualmente necessari per adeguare le misure di sicurezza; messo, a richiesta, a disposizione del Garante o dell'autorità giudiziaria;

8. documentare i sistemi informativi utilizzati per il trattamento dei dati di traffico in modo idoneo secondo i princìpi dell'ingegneria del software, evitando soluzioni documentali non corrispondenti a metodi descrittivi standard o di ampia accettazione. La descrizione deve comprendere, per ciascun sistema applicativo, l'architettura logico-funzionale, l'architettura complessiva e la struttura dei sistemi utilizzati per il trattamento, i flussi di input/output dei dati di traffico da e verso altri sistemi, l'architettura della rete di comunicazione, l'indicazione dei soggetti o classi di soggetti aventi legittimo accesso al sistema. La documentazione va corredata con diagrammi di dislocazione delle applicazioni e dei sistemi, da cui deve risultare anche l'esatta ubicazione dei sistemi nei quali vengono trattati i dati per le finalità di accertamento e repressione di reati. La documentazione tecnica deve essere aggiornata e

messa a disposizione dell'Autorità su sua eventuale richiesta, unitamente a informazioni di dettaglio sui soggetti aventi legittimo accesso ai sistemi per il trattamento dei dati di traffico;

9. proteggere i dati di traffico trattati per esclusive finalità di giustizia con tecniche crittografiche, in particolare contro rischi di acquisizione fortuita o di alterazione accidentale derivanti da operazioni di manutenzione sugli apparati informatici o da ordinarie operazioni di amministrazione di sistema. Il fornitore deve adottare soluzioni che rendano le informazioni residenti nelle basi di dati a servizio delle applicazioni informatiche utilizzate per i trattamenti, non intelligibili a chi non disponga di diritti di accesso e profili di autorizzazione idonei, ricorrendo a forme di cifratura od offuscamento di porzioni dei data base o degli indici o ad altri accorgimenti tecnici basati su tecnologie crittografiche. Tale misura deve essere efficace per ridurre al minimo il rischio che incaricati di mansioni tecniche accessorie ai trattamenti (amministratori di sistema, data-base administrator e manutentori hardware e software) possano accedere indebitamente alle informazioni registrate, anche fortuitamente, acquisendone conoscenza nel corso di operazioni di accesso ai sistemi o di manutenzione di altro genere, oppure che possano intenzionalmente o fortuitamente alterare le informazioni registrate. Eventuali flussi di trasmissione dei dati di traffico tra sistemi informatici del fornitore devono aver luogo tramite protocolli di comunicazione sicuri, basati su tecniche crittografiche, o comunque evitando il ricorso alla trasmissione in chiaro dei dati. Protocolli di comunicazione sicuri devono essere adottati anche per garantire più in generale la sicurezza dei sistemi evitando di esporli a vulnerabilità e a rischio di intrusione;

b) ai sensi dei medesimi artt. 17, 123 e 132, comma 5 del Codice, nonché dell'art. 157 del Codice, prescrive ai predetti fornitori titolari del trattamento di effettuare tutti gli adempimenti di cui alla precedente lett. a) al più presto e, comunque, entro e non oltre il termine del 30 aprile 2009, dandone conferma al Garante attestando entro lo stesso termine l'integrale adempimento;

c) ai sensi dell'art. 17 del Codice prescrive ai medesimi fornitori titolari del trattamento di adottare, rispetto ai dati di traffico trattati per le finalità di cui all'art. 123 del Codice,

entro e non oltre il termine del 30 aprile 2009, ovvero per quanto riguarda la strong authentication riferita agli incaricati che accedono ai dati di traffico nell'ambito dell'attività di call center, 30 giugno 2009, dandone ai sensi dell'art. 157 del Codice conferma al Garante e attestando entro lo stesso termine l'integrale adempimento, i seguenti accorgimenti e misure (par. 8):

1. adottare specifici sistemi di autenticazione informatica basati su tecniche di strong authentication, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione, che si applichino agli accessi ai sistemi di elaborazione da parte di tutti gli incaricati di trattamento nonché di tutti gli addetti tecnici (amministratori di sistema, di rete, di data base) che abbiano la possibilità concreta di accedere ai dati di traffico custoditi nelle banche dati del fornitore, qualunque sia la modalità, locale o remota, con cui si realizzi l'accesso al sistema di elaborazione utilizzato per il trattamento, evitando che questo possa aver luogo senza che l'incaricato abbia comunque superato una fase di autenticazione informatica nei termini anzidetti. Qualora circostanze eccezionali, legate a indifferibili interventi per malfunzionamenti, guasti, installazione hardware e software, aggiornamento e riconfigurazione dei sistemi, determinino la necessità di accesso a sistemi di elaborazione che trattano dati di traffico da parte di addetti tecnici in assenza di strong authentication, fermo restando l'obbligo di assicurare le misure minime in tema di credenziali di autenticazione previste dall'Allegato B. al Codice in materia di protezione dei dati personali, deve essere tenuta traccia in un apposito "registro degli accessi" dell'eventuale accesso fisico ai locali in cui sono installati i sistemi di elaborazione oggetto di intervento e dell'accesso logico ai sistemi, nonché delle motivazioni che li hanno determinati, con una descrizione sintetica delle operazioni svolte, anche mediante l'utilizzo di sistemi elettronici. Tale registro deve essere custodito dal fornitore presso le sedi di elaborazione e messo a disposizione del Garante nel caso di ispezioni o controlli, unitamente a un elenco nominativo dei soggetti abilitati all'accesso ai diversi sistemi di elaborazione con funzioni di amministratore di sistema, che deve essere formato e aggiornato costantemente dal fornitore;

2. adottare procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati;
3. rendere i dati di traffico immediatamente non disponibili per le elaborazioni dei sistemi informativi allo scadere dei termini previsti dalle disposizioni vigenti, provvedendo alla loro cancellazione o trasformazione in forma anonima, in tempi tecnicamente compatibili con l'esercizio delle relative procedure informatiche, nei data base e nei sistemi di elaborazione utilizzati per i trattamenti nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza (backup e disaster recovery) effettuate dal titolare anche in applicazione di misure previste dalla normativa vigente e, al più tardi, documentando tale operazione entro i trenta giorni successivi alla scadenza dei termini di conservazione (art. 123 del Codice);
4. adottare soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti sui diversi database utilizzati. Tali soluzioni comprendono la registrazione, in un apposito audit log, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici. I sistemi di audit log devono garantire la completezza, l'immodificabilità, l'autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad auditing. A tali scopi il fornitore deve adottare, per la registrazione dei dati di auditing, anche in forma centralizzata per ogni impianto di elaborazione o per datacenter, sistemi di memorizzazione su dispositivi non alterabili. Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche;

5. documentare i sistemi informativi utilizzati per il trattamento dei dati di traffico in modo idoneo secondo i princìpi dell'ingegneria del software, evitando soluzioni documentali non corrispondenti a metodi descrittivi standard o di ampia accettazione. La descrizione deve comprendere, per ciascun sistema applicativo, l'architettura logico-funzionale, l'architettura complessiva e la struttura dei sistemi utilizzati per il trattamento, i flussi di input/output dei dati di traffico da e verso altri sistemi, l'architettura della rete di comunicazione, l'indicazione dei soggetti o classi di soggetti aventi legittimo accesso al sistema. La documentazione va corredata con diagrammi di dislocazione delle applicazioni e dei sistemi, da cui deve risultare anche l'esatta ubicazione dei sistemi nei quali vengono trattati i dati per le finalità di accertamento e repressione di reati. La documentazione tecnica deve essere aggiornata e messa a disposizione dell'Autorità su sua eventuale richiesta, unitamente a informazioni di dettaglio sui soggetti aventi legittimo accesso ai sistemi per il trattamento dei dati di traffico;

d) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia anche ai fini della sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana a cura dell'Ufficio pubblicazione leggi e decreti, nonché, per opportuna conoscenza, all'Autorità per le garanzie nelle comunicazioni.

Roma, 17 gennaio 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

28. ANAGRAFE TRIBUTARIA: SICUREZZA E ACCESSI (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Francesco Pizzetti;

PREMESSO

Sulla base di un'analisi preliminare del sistema informativo della fiscalità, il 14 dicembre 2007 il Garante ha deliberato l'avvio di accertamenti volti a verificare, in più fasi, i trattamenti di dati personali effettuati presso l'anagrafe tributaria, rilevando che elementi di maggior criticità e urgenza erano da ravvisarsi nelle misure di sicurezza adottate per gli accessi da parte di enti esterni, pubblici e privati, all'amministrazione finanziaria.

La prima fase di accertamenti attinente a tali accessi è stata completata. Il Garante svolgerà nel prosieguo le altre verifiche programmate sul trattamento dei dati effettuato dalle articolazioni dell'amministrazione finanziaria, con particolare riguardo alla struttura degli archivi, alle modalità di accesso, alle applicazioni utilizzate, alle tipologie di informazioni, alle misure di sicurezza, alle abilitazioni e alle autorizzazioni degli utenti.

Le attività ispettive completate hanno invece riguardato, in particolare:

1) il controllo degli applicativi che consentono l'accesso all'anagrafe tributaria a soggetti esterni all'amministrazione finanziaria (loro funzionalità; tipologie di dati visualizzabili con i differenti profili di autorizzazione previsti);
2) la designazione di responsabili e di incaricati, i sistemi di autenticazione (ad es., modalità di formazione e gestione delle password; controlli degli accessi ai sistemi applicativi)

(*) [doc. *web* n. 1549548]

e i sistemi di autorizzazione;

3) le procedure di audit interno ed esterno sull'accesso alle informazioni contenute nell'anagrafe tributaria (ad es., controlli sulle abilitazioni e sulle autorizzazioni degli utenti abilitati all'utilizzo degli applicativi, modalità di raccolta dei logfile e loro analisi automatizzata).

Gli accertamenti ispettivi hanno avuto luogo presso l'Agenzia delle entrate, Sogei S.p.A. (Società generale d'informatica, responsabile del trattamento dei dati contenuti nell'anagrafe tributaria), regioni, province, comuni e altri enti che accedono a tale anagrafe, con la piena collaborazione degli enti coinvolti. Le verifiche hanno consentito di evidenziare criticità, in ambito sia informatico, sia organizzativo, documentate nei verbali in atti.

Dalle risultanze emerge che i sistemi di collegamento all'anagrafe tributaria utilizzati dai soggetti esterni all'amministrazione finanziaria sono i seguenti:

- "Siatel", applicazione web utilizzata principalmente da comuni, province, regioni, università, asl e consorzi di bonifica, per un totale di circa 9.400 enti e 60.000 utenze, che consente di visualizzare dati anagrafici completi, dati fiscali e atti del registro relativi alla totalità dei contribuenti;
- "Puntofisco", applicazione web di recente realizzazione e attualmente in dotazione a enti previdenziali, tribunali, camere di commercio e società varie, per un totale di circa 180 enti e 18.000 utenze. Puntofisco consente di visualizzare dati anagrafici, fiscali e atti del registro relativi alla totalità dei contribuenti, più aggiornati e con maggiore segmentazione delle informazioni rispetto a Siatel (ad es., differenziando tra dati anagrafici attuali o completi dello storico), ma permette anche di accedere a dati sensibili (presenti nel dettaglio degli oneri deducibili);
- "3270 enti esterni", collegamento diretto, tramite terminali fisici o emulatori di terminale, ai sistemi centrali dell'anagrafe tributaria, in corso di dismissione per esigenze di aggiornamento tecnologico, che tuttora consente a soggetti anche privati (Telecom Italia S.p.A., Enel, Inail, Inps, camere di commercio, Ministero delle politiche agricole, "interforze") di collegarsi a informazioni anagrafiche e fiscali relative alla totalità dei contribuenti; la struttura dell'applicativo non consente all'Agenzia delle entrate di conoscere il numero di utenti;
- "Entratel", applicativo utilizzato dagli enti principalmente ai fini della trasmissione delle

dichiarazioni, con flussi di dati solo in entrata verso l'Agenzia delle entrate; le credenziali di autenticazione fornite dall'Agenzia permettono altresì all'operatore di visualizzare la posizione fiscale dell'ente attraverso l'apposita web application ("Fisconline"/"Cassetto fiscale");

- "web services", strumenti realizzati sulla base di specifiche tecniche definite caso per caso dall'Agenzia delle entrate, che consentono di accedere a dati anagrafici anche completi relativi alla totalità dei contribuenti. Tali collegamenti sono utilizzati da 21 enti, ma la configurazione del collegamento non consente all'Agenzia di conoscere il numero di utenti;
- "file transfer", collegamenti per la gestione di flussi di dati per la gran parte in entrata (principalmente provenienti da banche), ma alcuni anche in uscita (ad es., verso concessionari della riscossione), utilizzati da circa 200 enti.

OSSERVA

Nel corso dei menzionati accertamenti ispettivi, sulla base della documentazione in atti, sono state riscontrate alcune criticità di seguito descritte, già in parte riconosciute dall'Agenzia, relative agli accessi all'anagrafe tributaria da parte degli enti esterni all'amministrazione finanziaria, riferibili in particolare alle autenticazioni e alle autorizzazioni degli utenti, ai controlli da parte dell'Agenzia e alle estese possibilità di accesso alle banche dati. Accanto a diverse problematiche attinenti alla sicurezza, sono emersi e vengono affrontati connessi profili concernenti aspetti sostanziali del trattamento.

Il Garante, ai sensi dell'art. 154, comma 1, lett. c) del Codice, ritiene necessario prescrivere una serie di misure e accorgimenti che devono essere adottati dall'Agenzia delle entrate, anche in riferimento ai soggetti esterni che accedono all'anagrafe tributaria, di seguito indicati. Tali misure e accorgimenti, principalmente di carattere tecnico e organizzativo, sono necessari al fine di porre rimedio alle carenze riscontrate e a incrementare, in particolare, i livelli di sicurezza degli accessi all'anagrafe tributaria, rendendo il trattamento conforme alle disposizioni vigenti.

1. ACCESSI ALL'ANAGRAFE TRIBUTARIA DA PARTE DI SOGGETTI ESTERNI ALL'AMMINISTRAZIONE FINANZIARIA: PROFILI GENERALI

Criticità

Alcuni accertamenti in proposito sono risultati meno agevoli in considerazione del fatto che l'Agenzia non aveva immediatamente disponibile, come richiesto dall'Autorità, una completa documentazione relativa sia ai soggetti esterni collegati, sia ai sistemi di accesso utilizzati da questi ultimi (numero e categorie di soggetti, finalità degli accessi e tipologie di collegamenti e di dati comunicati).

Dagli atti emerge ora che l'Agenzia autorizza gli accessi all'anagrafe tributaria solo in seguito alla stipula di apposite convenzioni, anche standard, a livello centrale e regionale. Tuttavia, l'assenza di una documentazione di insieme sui collegamenti in essere non agevola un monitoraggio costante sulla sussistenza dei presupposti che hanno consentito l'attivazione del canale informativo, nonché i dovuti controlli sulla correttezza della gestione degli accessi e della consultazione delle informazioni. La periodica ricognizione degli enti che accedono all'anagrafe tributaria, e dei rispettivi utenti, costituisce infatti la premessa per prevenire usi impropri e illeciti delle informazioni in essa contenute.

È stato inoltre riscontrato in atti che in alcune convenzioni stipulate per l'accesso all'anagrafe tributaria non risultano delimitate chiaramente le finalità per cui gli accessi vengono autorizzati; sotto tale aspetto, è stato rilevato che alcuni enti, attraverso gli amministratori locali (soggetti deputati all'abilitazione degli utenti), hanno abilitato di propria iniziativa alcuni utenti al fine di attivare nuovi flussi di dati per finalità ulteriori rispetto a quelle consentite.

Non risulta altresì dagli atti che gli operatori che effettuano gli accessi abbiano l'onere (o la possibilità) di registrare, anche al fine di successivi controlli, le ragioni a supporto delle interrogazioni eseguite.

È stato inoltre verificato che i dati visualizzabili attraverso gli applicativi non sono segmentabili in relazione al bacino di utenza dell'ente che chiede il collegamento (ad es., territorio comunale), e sono relativi a tutto il territorio nazionale.

Infine, le informazioni consultabili non risultano, talvolta, sufficientemente aggiornate per lo svolgimento delle funzioni istituzionali cui gli accessi sono finalizzati (ad es., in Siatel, ai fini

della verifica dell'Isee non sono visualizzabili i dati dell'ultima dichiarazione presentata e vengono invece visualizzati dati reddituali riferiti ad annualità pregresse, eccedenti e non pertinenti rispetto alle finalità perseguite, che non consentono di effettuare i puntuali controlli sulle autocertificazioni reddituali ai sensi del d.P.R. n. 445/2000).

Da ultimo, sulla base delle risultanze in atti, è stato rilevato che gli accessi all'anagrafe tributaria vengono effettuati talvolta per conoscere informazioni (ad es., la residenza) che, ai sensi della normativa vigente, dovrebbero essere invece controllate presso altri soggetti (ad es., amministrazioni certificanti ai sensi dell'art. 71 del d.P.R. n. 445/2000).

Prescrizioni

L'Agenzia deve disporre di informazioni complete e strutturate sulla molteplicità di soggetti che, a vario titolo, accedono alla banca dati dell'anagrafe tributaria. Occorre pertanto che la stessa rediga un documento, con formalità descrittive standard, che riporti tutti i flussi di trasferimento di dati da e verso l'anagrafe tributaria e tutti gli accessi di tipo interattivo, batch o di altro genere, specificando per ciascun flusso o accesso l'identità dei soggetti legittimati a realizzarlo, la base normativa (anche ai sensi dell'art. 19, comma 2 del Codice, previa comunicazione al Garante), la finalità istituzionale, la natura e la qualità dei dati trasferiti o a cui si è avuto accesso, la frequenza e il volume dei trasferimenti o degli accessi e il numero di soggetti che utilizzano la procedura. Tale documento dovrà essere mantenuto costantemente aggiornato, nonché reso disponibile nel caso di controlli.

L'Agenzia deve altresì verificare, con cadenza periodica annuale, l'attualità delle finalità per cui ha concesso l'accesso agli enti esterni, anche con riferimento al numero di utenze attive, inibendo gli accessi (autorizzazioni o singole utenze) effettuati al di fuori dei presupposti riconducibili all'art. 19 del Codice (norme di legge o regolamento, nonché eventuali comunicazioni al Garante ai sensi dell'art. 19 del Codice) e quelli non conformi a quanto stabilito nelle convenzioni. All'esito di tali verifiche, in particolare, devono essere eliminati gli accessi effettuati per conoscere informazioni che, ai sensi della normativa vigente, dovrebbero essere invece controllate presso altri soggetti.

Per vincolare effettivamente gli accessi alle finalità consentite, l'Agenzia deve introdurre nelle applicazioni volte all'uso interattivo da parte di incaricati un campo per l'indicazione obbliga-

toria del numero di riferimento della pratica (ad es. numero del protocollo o del verbale) nell'ambito della quale viene effettuata la consultazione.

L'Agenzia deve poi far sì che gli applicativi consentano, per quanto più possibile, la segmentazione dei dati visualizzabili -in particolare in modo cronologico (attuale o storico, per periodi di imposta), geografico (comune, provincia, regione) e per tipologia di dati (ad es. di sintesi)- al fine di rendere consultabili dall'utente, anche in base al proprio profilo e in relazione al bacino di utenza dell'ente che chiede il collegamento, esclusivamente i dati necessari rispetto alle finalità perseguite (ad es. l'ultimo domicilio fiscale o l'ultimo periodo di imposta).

2. I SISTEMI UTILIZZATI PER IL COLLEGAMENTO ALL'ANAGRAFE TRIBUTARIA

2.1. *Profili comuni*

Le principali criticità di carattere generale relative all'utilizzo degli applicativi riscontrate nel corso degli accertamenti ispettivi sugli accessi da parte dei soggetti esterni sono di seguito individuate.

2.1.1. Sicurezza dei sistemi di autenticazione

Criticità

Per le web application è stato utilizzato un certificato Ssl di tipo self signed (non firmato da una Ca, Certification authority, ufficiale) non attendibile che, in mancanza di una Ca affidabile, non offre le garanzie di certezza dell'identità dell'erogatore del servizio tipiche della certificazione digitale tramite Pki (public key infrastructure): risultano pertanto facilitate azioni di phishing in danno di utenti del sistema e la possibile acquisizione indebita di credenziali di autenticazione, idonea a consentire utilizzi impropri dell'applicazione.

Dalle risultanze agli atti emerge inoltre che, rispetto a taluni collegamenti, l'identificazione dell'utente finale dell'applicazione è in molti casi in capo all'ente esterno. L'Agenzia non ha pertanto alcuna conoscenza dell'effettiva identità e del numero degli utenti che accedono, con tali modalità di connessione, da sistemi informativi esterni collegati direttamente all'anagrafe tributaria (ad es., 3270 enti esterni e web services).

È risultato, poi, possibile accedere alle web application Siatel e Puntofisco attraverso l'utilizzo delle medesime credenziali contemporaneamente da postazioni diverse, anche con indirizzo Ip

diverso (perfino da rete esterna all'ente), nonostante, per quanto riguarda il Siatel, all'atto dell'accesso tale possibilità venga esclusa da un apposito avviso.

Prescrizioni

L'Agenzia deve prevedere che tutte le applicazioni accessibili da rete pubblica in forma di web application siano implementate con protocolli https/ssl provvedendo ad asseverare l'identità digitale dei server erogatori dei servizi tramite l'utilizzo di certificati digitali emessi da una Certification Authority ufficiale, evitando il ricorso a certificati di tipo self-signed.

Allo scopo di identificare le postazioni da cui vengono effettuati gli accessi, occorre inoltre che l'Agenzia implementi un sistema di certificazione digitale e di censimento delle postazioni terminali, in modo da realizzare procedure di autenticazione che, basandosi sul mutuo riconoscimento tra i server che erogano il servizio e le postazioni che accedono a esso, consentano di definire condizioni di accesso più complesse e sicure per determinate classi di incaricati o profili di autorizzazione.

A fronte dell'accertata possibilità per taluni applicativi di effettuare più accessi contemporanei con le medesime credenziali, al fine di consentire a ciascun utente di controllare l'utilizzo del proprio account, l'Agenzia deve poi prevedere -in considerazione della specificità dell'anagrafe tributaria- la visualizzazione, nella prima schermata successiva al collegamento, di informazioni relative all'ultima sessione effettuata con le stesse credenziali (almeno con l'indicazione di data, ora e indirizzo di rete da cui è stata effettuata la precedente connessione). Per accrescere la consapevolezza del controllo, le stesse informazioni devono essere riportate anche relativamente alla sessione corrente.

Infine, l'Agenzia deve disciplinare la possibilità di effettuare accessi contemporanei con le medesime credenziali (sessioni multiple), limitandone l'utilizzo ai soli casi necessari per esigenze di servizio (ad es., per le connessioni originate da una stessa postazione di lavoro). In ogni caso, tale possibilità deve essere consentita esclusivamente laddove il certificato digitale o l'indirizzo Ip siano sufficienti a discriminare l'identità digitale delle postazioni accedenti, come sopra descritto. Nel caso in cui non sia possibile individuare la postazione di lavoro, nelle more dell'attuazione delle prescrizioni sopra individuate, deve essere inibita la possibilità di accessi contemporanei.