Parere Garante per la Protezione dei Dati Personali 17 aprile 2012 n. 1886775

Comunicazione dei dati contabili all'anagrafe tributaria da parte di banche e operatori finanziari: parere all'Agenzia delle entrate sulle modalità di trasmissione e di conservazione dei dati - 17 aprile 2012

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Daniele De Paoli, segretario generale;

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

VISTA la richiesta di parere dell'Agenzia delle entrate del 12 marzo 2012, relativa allo schema di provvedimento del Direttore dell'Agenzia in materia di "Disposizioni di attuazione dell'articolo 11, commi 2 e 3, del decreto legge 6 dicembre 2011 n. 201, convertito, con modificazioni, dalla legge 22 dicembre 2011 n. 214. Comunicazione integrativa annuale all'archivio dei rapporti finanziari";

VISTE le note dell'Agenzia delle entrate con le quali sono state riscontrate le richieste di informazioni del Garante (note del 27 marzo, 29 marzo, 2 aprile e 5 aprile 2012);

VISTA la nota dell'Agenzia delle entrate con la quale sono state trasmesse alcune modifiche tecniche al tracciato record allegato allo schema di provvedimento (nota del 3 aprile 2012);

VISTO il provvedimento del Direttore dell'Agenzia delle entrate del 19 gennaio 2007 sul quale il Garante ha espresso il proprio parere in data 11 gennaio 2007;

VISTA la documentazioni 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

L'Agenzia delle entrate ha sottoposto al Garante, per l'acquisizione del relativo parere, uno schema di provvedimento del Direttore dell'Agenzia concernente le "Disposizioni di attuazione dell'articolo 11, commi 2 e 3, del decreto legge 6 dicembre 2011 n. 201, convertito, con modificazioni, dalla legge 22 dicembre 2011 n. 214. Comunicazione integrativa annuale all'archivio dei rapporti finanziari", che stabilisce le modalità e i termini della comunicazione integrativa dei dati relativi ai rapporti finanziari.

A. Il quadro normativo

1. L'archivio dei rapporti finanziari

Gli operatori finanziari comunicano all'anagrafe tributaria l'esistenza e la natura dei rapporti e delle operazioni di natura finanziaria compiute al di fuori di un rapporto continuativo (ad esclusione di quelle effettuate tramite bollettino di conto corrente postale per un importo unitario inferiore a 1.500 euro), ai sensi dell'articolo 7, sesto comma, del decreto del Presidente della Repubblica 29 settembre 1973, n. 605.

Con il provvedimento del 19 gennaio 2007 del Direttore dell'Agenzia delle entrate, sul quale il Garante ha espresso il proprio parere in data 11 gennaio 2007 (disponibile in www.garanteprivacy.it, doc. web 1381941), sono state stabilite le modalità e i termini di comunicazione dei predetti dati all'anagrafe tributaria da parte degli operatori finanziari. Il contenuto di tale provvedimento è stato integrato e modificato da ulteriori provvedimenti che hanno aggiunto alcuni dati soggetti all'obbligo di comunicazione e sono intervenuti sulle modalità tecniche di comunicazione dei dati.

In base alle predette disposizioni, nell'apposita sezione separata dell'anagrafe tributaria, c.d. archivio dei rapporti finanziari, attualmente confluiscono:

a) i dati identificativi del rapporto, compreso il codice univoco del rapporto;

b) i dati identificativi, compreso il codice fiscale, del soggetto persona fisica o non fisica che ha la disponibilità del rapporto, inclusi procuratori e delegati;

c) i dati identificativi, compreso il codice fiscale, di tutti i cointestatari del rapporto, nel caso di intestazione a più soggetti.

L'accesso all'archivio dei rapporti finanziari è, allo stato, previsto per le indagini finanziarie da parte dell'Agenzia delle entrate e della Guardia di finanza (art. 32, comma 1, n. 7, del d.P.R. 29 settembre 1973, n. 600 e art. 51, comma 2, n. 7 del d.P.R. 26 ottobre 1972, n. 633), oltre che per le ulteriori finalità di cui all'art. 7, comma 11, del d.P.R. n. 605 del 1973. Una volta acquisite tali informazioni sui rapporti finanziari, i soggetti legittimati possono richiedere attraverso un'apposita procedura telematica tutti i dati di dettaglio direttamente agli operatori finanziari presso i quali i contribuenti sono stati censiti.

Dalla documentazione in atti acquisita dall'Agenzia delle entrate, risulta che, attualmente, l'archivio dei rapporti finanziari contiene circa 600.000.000 (seicento milioni) di rapporti attivi e che annualmente gli operatori finanziari effettuano circa 155.000.000 (centocinquantacinque milioni) di comunicazioni relative alle sole variazioni dei rapporti in essere e alle c.d. operazioni extraconto.

2. La comunicazione integrativa annuale all'archivio dei rapporti finanziari

Al fine di agevolare l'emersione della base imponibile, la nuova normativa introdotta dal citato decreto legge n. 201 del 2011 prevede che, oltre a quanto già comunicato, gli operatori finanziari inviino

periodicamente all'anagrafe tributaria, a far data dal 1° gennaio 2012, anche le movimentazioni che hanno interessato i rapporti già censiti, ed ogni informazione relativa ai predetti rapporti necessaria ai fini dei controlli fiscali, nonché l'importo delle operazioni finanziarie (art. 11, comma 2).

L'art. 11, comma 3, prevede che "con provvedimento del Direttore dell'Agenzia delle entrate, sentiti le associazioni di categoria degli operatori finanziari e il Garante per la protezione dei dati personali, sono stabilite le modalità della comunicazione di cui al comma 2, estendendo l'obbligo di comunicazione anche ad ulteriori informazioni relative ai rapporti strettamente necessarie ai fini dei controlli fiscali. Il provvedimento deve altresì prevedere adeguate misure di sicurezza, di natura tecnica e organizzativa, per la trasmissione dei dati e per la relativa conservazione, che non può superare i termini massimi di decadenza previsti in materia di accertamento delle imposte sui redditi".

Il citato art. 11 prevede, altresì, al comma 4, che i dati comunicati, oltre che per le finalità sopra citate per le quali viene già consultato l'archivio dei rapporti finanziari, potranno essere trattati dall'Agenzia delle entrate per l'elaborazione con procedure centralizzate, secondo i criteri individuati con provvedimento del Direttore della medesima Agenzia, di specifiche liste selettive di contribuenti a maggior rischio di evasione.

B. Il contenuto dello schema di provvedimento

1. Dati oggetto della comunicazione

Lo schema di provvedimento in esame prevede che gli operatori finanziari inviino le seguenti informazioni in relazione alla tipologia di rapporti sopra citati, attivi nel corso dell'anno di riferimento:

a) i dati relativi ai saldi del rapporto, distinti in saldo iniziale al 1° gennaio e saldo finale al 31 dicembre, dell'anno cui è riferita la comunicazione di riferimento;

b) per i rapporti accesi nel corso dell'anno il saldo iniziale alla data di apertura, per i rapporti chiusi nel corso dell'anno il saldo alla data di chiusura;

c i dati relativi agli importi totali degli accrediti e degli addebiti delle operazioni attive e passive conteggiati su base annua.

Nello schema è stabilito che la comunicazione debba avvenire annualmente entro il 31 marzo dell'anno successivo a quello a cui sono riferite le informazioni, mentre per l'anno 2011 i dati devono essere trasmessi entro il 31 ottobre 2012. Anche tali informazioni sono archiviate nell'apposita sezione dell'anagrafe tributaria già denominata archivio dei rapporti finanziari.

Con riferimento ai tempi di conservazione, lo schema di provvedimento prevede che siano quelli massimi previsti dal legislatore, ovvero quelli di decadenza in materia di accertamento delle imposte sui redditi.

La specificazione delle informazioni da inviare per ciascun rapporto è indicata nella tabella allegata allo schema di provvedimento, di seguito riportata.

Tipo rapporto	Descrizione	Importo 1	Importo 2	Importo 3	Importo 4	Altre informazioni
1	Conto corrente	Saldo Contabile alla data di fine anno precedente	Saldo Contabile alla data di fine anno	Importo totale degli accrediti effettuati nell'anno	Importo totale degli addebiti effettuati nell'anno	Vale zero
2	Conto deposito titoli e/o obbligazioni	Controvalore dei titoli rilevato contabilmente alla data di fine anno precedente (come da estratto conto)	Controvalore dei titoli rilevato contabilmente alla data di fine anno (come da estratto conto)	Importo totale degli acquisti di titoli, fondi ecc effettuati nell'anno	Importo totale dei disinvestimenti effettuati nell'anno	Vale zero
3	Conto deposito a risparmio libero/vincolato	Saldo Contabile alla data di fine anno precedente	Saldo Contabile alla data di fine anno	Importo totale degli accrediti effettuati nell'anno	Importo totale degli addebiti effettuati nell'anno	Vale zero
4	Rapporto fiduciario ex legge n. 1966/1939	Controvalore rilevato contabilmente a fine anno precedente	Controvalore rilevato contabilmente a fine anno	Importo totale distintamente individuato dei conferimenti (parziali/totali) effettuati nell'anno.	Importo totale distintamente individuato dei prelievi (parziali/totali) effettuati nell'anno.	Vale zero
5	Gestione collettiva del risparmio	Ammontare del contratto di gestione alla data di fine anno precedente	Ammontare del contratto di gestione alla data di fine anno	Importo totale delle sottoscrizioni di quote nell'anno	Importo totale dei imborsi di quote nell'anno	Vale zero
6	Gestione patrimoniale	Valore globale del patrimonio a data di fine anno precedente	Valore globale del patrimonio a data fine anno	Importo totale degli apporti effettuati nell'anno	Importo totale dei prelievi effettuati nell'anno	Vale zero
7	Certificati di deposito e buoni fruttiferi	Totale degli importi facciali dei Certificati o dei buoni a fine anno precedente	Totale degli importi facciali dei Certificati o dei buoni a fine anno	Importo totale delle accensioni effettuate nell'anno al di fuori di quelle transitate su un deposito titoli	Importo totale delle estinzioni effettuate nell'anno al di fuori di quelle transitate su un deposito titoli	Numero totale dei certificati o dei buoni fruttiferi
8	Portafoglio	Vale zero	Vale zero	Vale zero	Vale zero	Vale zero
9	Conto terzi individuale/globale	Saldo Contabile alla data di fine anno	Saldo Contabile alla data di fine anno	Importo totale degli accrediti effettuati nell'anno	Importo totale degli addebiti effettuati nell'anno	Vale zero
10	Dopo incasso	Saldo Contabile alla data di fine anno precedente	Saldo Contabile alla data di fine anno	Importo totale degli incassi effettuati nell'anno	Vale zero	Vale zero
11	Cessione indisponibile	Vale zero	Vale zero	Vale zero	Vale zero	Vale zero
12	Cassette di sicurezza	Vale zero	Vale zero	Vale zero	Vale zero	Numero totale degli accessi effettuati nell'anno
13	Depositi chiusi	Vale zero	Vale zero	Vale zero	Vale zero	Vale zero
14	Contratti derivati	Vale zero	Vale zero	Importo totale dei contratti accesi nell'anno.	Importo totale dei contratti chiusi nell'anno.	Numero totale dei contratti stipulati
15	Carte di credito/debito	Utilizzo del plafond di spesa a fine anno precedente	Utilizzo del plafond di spesa a fine anno	Per le carte prepagate Ricaricabili, l'importo totale delle ricariche effettuate nell'anno. Per le carte prepagate non Ricaricabili l'importo totale delle carte acquistate	importo totale degli acquisti effettuati nell'anno.	Vale zero
16	Garanzie	Vale zero	Vale zero	Vale zero	Vale zero	Vale zero
17	Crediti	Vale zero	Vale zero	Vale zero	Vale zero	Vale zero
18	Finanziamenti	Vale zero	Vale zero	Vale zero	Vale zero	Vale zero
19	Fondi pensione	Vale zero	Vale zero	Vale zero	Vale zero	Vale zero
20	Patto compensativo	Vale zero	Vale zero	Vale zero	Vale zero	Vale zero
21	Finanziamento in pool	Vale zero	Vale zero	Vale zero	Vale zero	Vale zero
22	Partecipazione	Vale zero	Vale zero	Vale zero	Vale zero	Vale zero
23	Prodotti finanziari emessi da imprese di assicurazione	Vale zero	Vale zero	Importo totale degli incrementi della polizza effettuati nell'anno	Importo totale dei riscatti della polizza effettuati nell'anno	Vale zero
24	Acquisto e vendita di oro e metalli preziosi	Vale zero	Vale zero	Importo totale del valore degli acquisti effettuati nell'anno.	Importo totale del valore delle vendite effettuate nell'anno.	Numero totale delle operazioni effettuate
98	Operazione Extra-conto	Vale zero	Vale zero	Ammontare delle operazioni nell'anno	Vale zero	Numero delle operazioni effettuate
99	Altro rapporto	Vale zero	Vale zero	Vale zero	Vale zero	Vale zero

2. Modalità di trasmissione

In relazione alle modalità di trasmissione, lo schema prevede che venga utilizzato il servizio telematico Entratel (già sottoposto all'attenzione del Garante in relazione alle altre comunicazioni di dati all'anagrafe tributaria), secondo il tracciato record ivi allegato, ovvero altri canali telematici che verranno comunque preventivamente comunicati al Garante; in base a quanto dichiarato dall'Agenzia, tale servizio è stato integrato con le misure previste dal provvedimento del Garante del 18 settembre 2008 (disponibile in www.garanteprivacy.it, doc. web 1549548).

Secondo l'Agenzia, la sicurezza nella trasmissione dei dati sarebbe garantita dal meccanismo di identificazione ed autorizzazione fondato su un dispositivo CNS dell'utente e relativo PIN di sblocco o sul codice identificativo dell'utente abbinato ad una password. La riservatezza nella trasmissione dei dati viene, invece, assicurata attraverso l'uso di chiavi asimmetriche che ne garantiscono la cifratura. Per la trasmissione telematica delle comunicazioni, i soggetti sono tenuti ad utilizzare i prodotti software di controllo distribuiti gratuitamente dall'Agenzia, al fine di verificare la congruenza dei dati comunicati con quanto previsto dalle suddette specifiche tecniche. In seguito all'invio il sistema fornisce una ricevuta, contenuta in un file, munito del codice di autenticazione per il servizio Entratel, in cui è indicato, in particolare, il numero delle comunicazioni contenute in ciascuna trasmissione.

3. Trattamento dei dati

Con riferimento al trattamento dei dati, lo schema di provvedimento stabilisce che i dati e le notizie che pervengono all'anagrafe tributaria siano raccolti e ordinati su scala nazionale al fine della valutazione della capacità contributiva, nel rispetto dei diritti e delle libertà fondamentali dei contribuenti.

In particolare, viene previsto che i dati di cui alle sopra citate lett. a), d), e) e f) di cui ai precedenti punti A e B.1. siano trattati dall'Agenzia delle entrate unicamente per la formazione con procedure centralizzate di specifiche liste selettive di contribuenti a maggior rischio di evasione, secondo i criteri che verranno individuati con successivo provvedimento del Direttore della medesima Agenzia. Le posizioni, così individuate, saranno segnalate per l'avvio delle attività di controllo fiscale.

L'Agenzia ha precisato che i dati contenuti nella nuova comunicazione integrativa annuale non costituiranno oggetto diretto dell'attività di accertamento. Nello schema viene, infatti, stabilito che le nuove informazioni non implementeranno i dati accessibili attraverso la procedura delle indagini finanziarie illustrata al punto A.1.

Secondo quanto dichiarato dall'Agenzia, tali nuove informazioni, pur archiviate nell'archivio dei rapporti finanziari, non saranno visibili ai soggetti già abilitati a visualizzare i dati presenti in tale apposita sezione dell'anagrafe tributaria.

OSSERVA:

C. Osservazioni preliminari

Occorre preliminarmente evidenziare che la normativa di cui lo schema di provvedimento in esame è attuativo pone rilevanti problematiche di carattere generale relative alla protezione dei dati personali sia con riferimento all'eccezionale concentrazione presso l'anagrafe tributaria di un'enorme quantità di informazioni personali, sia in relazione alle finalità di classificazione degli interessati cui la raccolta di tali informazioni risulta preordinata.

Come più volte ribadito da questa Autorità, da ultimo anche nell'audizione svolta dal Presidente giovedì 29 marzo 2012 presso la Commissione parlamentare di vigilanza sull'anagrafe tributaria, non è in discussione l'esigenza di disporre di ogni necessaria idonea informazione per l'azione di verifica e contrasto dell'evasione fiscale, bensì l'integrale acquisizione e duplicazione presso l'anagrafe tributaria di una moltitudine di dati che, laddove necessari a fini di accertamento, risultano già disponibili all'amministrazione finanziaria attraverso la procedura delle indagini finanziarie che consente la puntuale e dettagliata acquisizione di tutte le informazioni finanziarie dei contribuenti.

Secondo le valutazioni effettuate dall'Agenzia, tali dati sarebbero tutti necessari ai fini dell'elaborazione con procedure centralizzate, secondo i criteri da individuarsi con provvedimento del Direttore della medesima Agenzia non ancora adottato, di specifiche liste selettive di contribuenti a maggior rischio di evasione.

Va rilevato, quindi, che la previsione di un'ingente concentrazione di tali categorie di dati presso un unico titolare genera un incremento esponenziale dei rischi insiti nel trattamento di dati personali rispetto alla quantità di informazioni raccolte, anche laddove il trattamento avvenga nel più rigoroso rispetto delle misure di sicurezza. Ciò, soprattutto, in relazione all'interesse che il valore strategico di una simile banca dati può suscitare sia con riferimento ad accessi abusivi ed a utilizzi impropri, che alla proliferazione di interconnessioni e raffronti.

Pertanto, nell'occasione dell'espressione del presente parere, che deve intervenire in ordine alle modalità di comunicazione dei dati, occorre valutare con particolare rigore le misure di sicurezza, di natura tecnica e organizzativa, per la trasmissione dei dati e per la relativa conservazione individuate nello schema di provvedimento (art. 11, comma 3).

Nell'ambito dell'istruttoria preliminare sullo schema in esame, sono stati svolti specifici accertamenti, anche di carattere ispettivo, al fine di valutare l'idoneità delle modalità di trasmissione scelte dall'Agenzia per la comunicazione annuale integrativa dei dati contabili all'anagrafe dei rapporti, nel caso di specie il servizio telematico Entratel, già in uso per numerose comunicazioni all'anagrafe tributaria, tra cui, in particolare, l'alimentazione da parte degli operatori finanziari dell'archivio dei rapporti finanziari.

A tal fine l'Autorità ha esaminato, nella prospettiva della comunicazione annuale integrativa, le attuali misure predisposte per l'invio mensile delle comunicazioni all'archivio dei rapporti finanziari da parte degli operatori attraverso il servizio telematico Entratel.

In tale contesto sono emerse numerose criticità riferibili sia ai trattamenti effettuati dagli operatori finanziari che all'utilizzo del servizio telematico Entratel e risulta necessario evidenziare taluni profili problematici di seguito illustrati relativi alla sicurezza dei trattamenti.

D. La sicurezza

Sulla base degli accertamenti svolti dall'Ufficio, occorre evidenziare come le criticità relative alla sicurezza complessiva del flusso di informazioni siano in parte riconducibili a caratteristiche tecniche dello stesso servizio Entratel in relazione alla specifica finalità di alimentazione dell'archivio dei rapporti finanziari, e in parte conseguenti agli aspetti tecnico-organizzativi dell'intera filiera di trattamento, che va dalla loro estrazione dai sistemi informativi dei soggetti tenuti all'adempimento, alla loro organizzazione nel formato richiesto dall'Agenzia per la relativa trasmissione verso l'anagrafe tributaria.

1. Il trattamento da parte degli operatori finanziari

1.1. Criticità

Sul versante degli operatori finanziari, si rileva preliminarmente che lo schema di provvedimento richiede l'invio all'anagrafe tributaria di una mole di dati che per loro natura la gran parte degli operatori finanziari solitamente tratta con diversi sistemi applicativi. La raccolta e l'aggregazione in forma di file secondo quanto richiesto dal servizio Entratel comporta quindi già all'origine una concentrazione di informazioni e, di conseguenza, un potenziale di rischio che difficilmente si riscontra nell'ordinario esercizio dell'attività finanziaria o bancaria. Benché le informazioni di base siano tutte nella disponibilità dell'operatore finanziario, solo questa specifica esigenza di conformità all'adempimento previsto dallo schema in esame rende necessaria l'aggregazione presso l'operatore medesimo, in un unico "oggetto informatico", della variegata tipologia di dati che risiederebbero altrimenti nelle diverse componenti applicative del sistema informativo.

Se tali osservazioni possono essere riferite anche all'elaborazione dei file per la comunicazione mensile all'anagrafe dei rapporti, la costituzione di tale nuovo "oggetto informatico" presso ciascun operatore finanziario per assolvere all'obbligo di comunicazione annuale rappresenta di per sé elemento idoneo ad incrementare notevolmente i rischi per gli interessati, in considerazione della quantità, qualità e delicatezza delle informazioni contabili ivi contenute, imponendo di conseguenza agli operatori finanziari particolari cautele al fine di prevenire accessi non autorizzati o non conformi rispetto alle finalità del trattamento (art. 31 del Codice).

In proposito, si rileva che l'Agenzia si è prevalentemente concentrata sugli aspetti di sicurezza legati alla fase di comunicazione dei dati, senza curare le misure e gli accorgimenti, anche di carattere organizzativo, a monte dell'alimentazione della propria banca dati. D'altra parte, la diversificata platea degli operatori finanziari e della rispettiva strutturazione dei sistemi informativi non consente di dettare regole specifiche di dettaglio sull'estrazione dei dati e la loro aggregazione, aspetti che sono riconducibili alla responsabilità dei singoli titolari.

Tuttavia, come sopra rilevato, si ritiene che negli aspetti organizzativi del flusso si annidino le principali fonti di potenziale insicurezza complessiva del trattamento, tenuto conto della natura dei dati da trattare e della loro delicatezza anche connessa al volume aggregato di informazioni in possesso di singoli operatori finanziari. Pertanto, le misure di sicurezza, di natura tecnica e organizzativa, che l'Agenzia è chiamata ad individuare nello schema di provvedimento in esame devono riguardare anche il trattamento posto in essere dagli operatori finanziari finalizzato alla comunicazione dei dati.

1.2. Integrazione dello schema di provvedimento

In tale quadro, lo schema di provvedimento deve essere integrato in merito, tenuto conto delle seguenti indicazioni elaborate sulla base delle principali problematiche rilevate in atti in relazione alle procedure, già in essere, di comunicazione mensile all'archivio dei rapporti finanziari attraverso il servizio Entratel:

1) la prima fase che ciascun operatore finanziario deve eseguire ai fini della comunicazione all'Agenzia consiste nella estrapolazione dei dati relativi ai rapporti finanziari in essere dai diversi archivi nei quali sono normalmente memorizzati per il soddisfacimento delle ordinarie esigenze operative dei singoli operatori finanziari. Il prodotto di tale attività è normalmente costituito da un unico file, che può raggiungere dimensioni considerevoli (anche dell'ordine delle centinaia di megabyte), nel quale sono riportate in formato testo "in chiaro" (alfanumerico non cifrato) le informazioni relative alle variazioni intervenute nel periodo in esame rispetto a tutte le tipologie di rapporti finanziari censite nell'archivio in questione (cfr. tabella sopra indicata). Sarebbe opportuno che, anche in considerazione delle dimensioni dell'operatore finanziario, già in tale fase fosse possibile utilizzare meccanismi di cifratura e di sicurezza, rispettivamente finalizzati a proteggere le informazioni contenute nel file durante i successivi passaggi all'interno dell'operatore finanziario e ad assicurare l'integrità del contenuto e a prevenirne alterazioni (ad es., mediante meccanismi di hashing);

2) le eventuali trasmissioni interne all'operatore finanziario dovrebbero avvenire esclusivamente su protocolli sicuri (https/ssl, SFTP, ecc.);

3) nel caso in cui le comunicazioni all'archivio dei rapporti finanziari vengano effettuate con l'intervento di un utente, tali soggetti devono essere scelti dagli operatori finanziari sulla base di elevati requisiti di idoneità soggettiva, preferibilmente tra soggetti che abbiano un rapporto stabile con essi;

4) l'accesso al file, nelle successive fasi del trattamento, dovrebbe essere circoscritto ad un numero il più possibile limitato di incaricati, i quali non dovrebbero poter effettuare alcun intervento di modifica delle informazioni contenute nel file;

5) qualora la comunicazione all'Agenzia delle entrate avvenga mediante l'utilizzo di postazioni client, tali postazioni devono disporre di versioni aggiornate del sistema operativo, del browser, di programmi antivirus e anti-intrusione e degli altri software applicativi utilizzati sulla postazione medesima, al fine di ridurre i rischi connessi ad accessi non consentiti o all'azione di virus o altri malware. Le postazioni abilitate all'invio dei dati attraverso il canale predisposto dall'Agenzia delle entrate dovrebbero essere dotate di

misure di sicurezza aggiuntive per assicurare che sia i suddetti file che le relative chiavi di cifratura non possano essere copiati su supporti esterni. In relazione alle dimensioni del singolo operatore finanziario, dovrebbe essere valutata la possibilità di riservare una postazione, opportunamente configurata e messa in sicurezza, dedicata all'invio di tali comunicazioni all'Agenzia delle entrate;

6) in seguito all'invio, l'eventuale conservazione del file dovrebbe essere effettuata da parte dell'operatore finanziario esclusivamente in forma cifrata;

7) dalla documentazione in atti, è emerso che uno cospicuo numero di operatori si avvalgono della possibilità di effettuare le comunicazioni mensili all'archivio dei rapporti finanziari mediante gli intermediari e che il medesimo intermediario può trasmettere le comunicazioni relative ad una pluralità di operatori, con la conseguenza che tali soggetti esterni (es. commercialisti, associazioni di professionisti, CAF, consulenti fiscali, ecc.) possono ricevere in chiaro il file da trasmettere prima della firma e della cifratura, con ulteriori rischi di accessi non conformi, utilizzi abusivi delle informazioni e alterazione dei dati. Pertanto, laddove gli operatori finanziari decidano di affidare la comunicazione a soggetti esterni, responsabili o incaricati del trattamento, il file dovrà essere loro fornito già cifrato.

In ogni caso, tenuto conto che gli aspetti relativi alla sicurezza dei trattamenti effettuati presso gli operatori finanziari ai fini della comunicazione annuale all'archivio dei rapporti finanziari sono correlati alle modalità di trasmissione che in concreto verranno individuate dall'Agenzia delle entrate in base alle osservazioni contenute nel presente parere, il Garante si riserva di effettuare eventuali approfondimenti al fine di individuare ulteriori misure laddove risulti necessario incrementarne i livelli di sicurezza.

2. Il servizio telematico Entratel

Il servizio Entratel è il principale canale telematico predisposto dall'Agenzia delle entrate per assolvere per via telematica, direttamente o tramite intermediari, agli obblighi relativi alla presentazione di dichiarazioni e comunicazioni, non solo di carattere fiscale, e costituisce un vero e proprio strumento "multi-uso" per la realizzazione di flussi di alimentazione delle banche dati dell'Agenzia.

La scelta di utilizzare un unico canale per la ricezione da parte dell'Agenzia delle entrate di un'ampia e diversificata gamma di comunicazioni se, da un lato, può rendere più semplice l'assolvimento degli adempimenti da parte dei destinatari, dall'altro non consente di modulare le cautele di volta in volta necessarie rispetto alla specifica tipologia di dati che formano oggetto di ciascuna categoria di comunicazione.

Conseguentemente, pur potendo lo strumento prescelto dall'Agenzia risultare astrattamente idoneo rispetto all'invio della gran parte delle dichiarazioni e comunicazioni, è risultato necessario valutarne l'adeguatezza in concreto (anche in seguito alle modifiche apportate dall'Agenzia a tale servizio telematico in ottemperanza al citato provvedimento del Garante del 18 settembre 2008) rispetto a specifiche tipologie di comunicazioni, quali quelle relative all'archivio dei rapporti, in ragione della qualità e della quantità delle informazioni ivi contenute.

2.1. Criticità

In tale quadro, dalle risultanze degli accertamenti effettuati, si osservano le seguenti criticità.

Il servizio Entratel non supporta l'invio di file di dimensioni superiori ai 3 megabyte e quindi ogni singolo file da inviare tramite tale servizio deve essere precedentemente suddiviso in file aventi ognuno tale dimensione massima e, prima dell'invio, ciascuno deve essere singolarmente sottoposto alle procedure di autenticazione e cifratura attraverso l'applicativo client Entratel e le chiavi asimmetriche fornite dall'Agenzia. Come rilevato nel corso degli accertamenti, già in relazione all'invio mensile delle variazioni all'archivio dei rapporti finanziari da parte di operatori di grandi dimensioni, tale limitazione non favorisce lo scambio di file di grandi dimensioni.

Rispetto a tale comunicazione mensile, i volumi di dati che gli operatori finanziari saranno tenuti a trasmettere annualmente all'archivio dei rapporti finanziari con la comunicazione integrativa saranno decisamente maggiori in quanto relativi non alle sole variazioni intervenute nell'arco di trenta giorni, ma alla totalità dei rapporti attivi nell'anno precedente con le informazioni contabili aggiuntive previste dallo schema di provvedimento. Inoltre, come si evince dal tracciato record fornito dall'Agenzia, le comunicazioni annuali integrative dovranno includere obbligatoriamente anche i singoli riferimenti a tutte le trasmissioni già effettuate all'archivio per il rapporto finanziario in oggetto, rendendo il trasferimento ancor più rilevante in termini di mole di dati.

Peraltro, durante le verifiche ispettive è stato accertato che in sede di prima costituzione dell'archivio dei rapporti finanziari, per forniture di dati relative alla totalità dei rapporti in essere presso l'operatore finanziario (analoghe a quelle in esame ma senza i dati contabili), per via della enorme quantità di dati da trasmettere è stato ritenuto necessario in taluni casi utilizzare supporti ottici (DVD) per l'invio all'Agenzia, con i conseguenti rischi che ciò ha comportato.

Come sinteticamente sopra già illustrato, in ragione del meccanismo di funzionamento del servizio Entratel, il file da trasmettere rimane esposto, dal momento dell'estrazione dei dati dai sistemi dell'operatore finanziario fino all'invio dei dati stessi all'anagrafe tributaria, a rischi di accessi illegittimi e di alterazione del contenuto della comunicazione.

Alla luce di ciò, si ritiene quindi che, per soggetti di medio-grandi dimensioni obbligati alla trasmissione annuale di comunicazioni integrative all'archivio dei rapporti finanziari, il servizio Entratel così come attualmente configurato non risulti adeguato alla trasmissione dei dati per via delle voluminose quantità di scambio previste, rispetto alle potenzialità e alle limitanti caratteristiche tecniche dello strumento per il caso specifico in esame.

Le rilevanti criticità sopra illustrate risultano già determinanti ai fini della valutazione di inadeguatezza della scelta di utilizzare il servizio Entratel –nella sua attuale configurazione- ai fini della trasmissione dei dati di cui allo schema di provvedimento in esame da parte di soggetti di medio-grandi dimensioni. Inoltre, tale servizio, pur rispettando le misure minime di cui all'allegato B al Codice, presenta ulteriori criticità che

rendono necessaria l'introduzione di alcune misure e accorgimenti volti a incrementarne i livelli di sicurezza anche nel caso di invii effettuati da soggetti di piccole dimensioni. In sintesi, le principali problematiche riscontrate sono riferibili:

- all'assenza di un sistema di autorizzazione interno all'applicativo web che consenta di attribuire al singolo operatore la visibilità delle sole funzioni applicative necessarie per ciascuna categoria di invio;

- alla condivisione, tra gli utenti della medesima sede telematica, dell'ambiente di sicurezza (con la conseguente riproduzione delle chiavi asimmetriche -coppia di chiavi private di firma e cifratura- su vari supporti, ad es. floppy disk o USB);

- alla mancanza di applicazione delle misure di sicurezza perimetrale, volte all'identificazione delle postazioni da cui vengono effettuati gli accessi, basandosi sul mutuo riconoscimento tra i server che erogano il servizio e le postazioni che accedono a esso. L'accesso a Entratel, allo stato, può avvenire infatti anche da una rete generica senza che la postazione di lavoro sia stata precedentemente autenticata e non sono altresì presenti ulteriori filtri (ad es. sull'indirizzamento IP) che impediscano tale accesso incondizionato. Ciò implica, anche in considerazione della condivisione dell'ambiente di sicurezza di cui al precedente punto, che risulta possibile utilizzare le chiavi private e effettuare invii all'Agenzia anche da postazioni remote esterne all'operatore finanziario;

- quanto descritto al punto precedente pone problemi anche in considerazione del fatto che, dopo aver effettuato l'accesso, le persone fisiche possono disporre della funzionalità denominata "Scelta utenza di lavoro" con la quale possono decidere di operare sia per conto proprio (con i servizi dell'Agenzia rivolti ai privati cittadini) che per conto di terzi (ad es., per ragioni di servizio per conto del proprio datore di lavoro), accedendo, ad esempio da casa o da reti esterne al proprio ambito lavorativo, anche all'"utenza di lavoro" dell'ente senza dover nuovamente digitare la password di accesso né prevedendo il superamento di ulteriori meccanismi di autenticazione;

- ad alcuni aspetti relativi alla procedura di autorizzazione on line da parte dei gestori incaricati, con riferimento alla funzione dell'applicativo denominata "Funzioni relative agli incaricati" per la definizione di ulteriori gestori incaricati e/o operatori incaricati.

2.2. Misure e accorgimenti necessari

Sulla base di quanto sopra evidenziato, occorre, pertanto, che:

1) l'Agenzia predisponga l'uso di canali di comunicazione diversi e alternativi a Entratel, soprattutto per le comunicazioni da parte di soggetti di medio-grandi dimensioni detentori di una elevata quantità di dati come i gruppi bancari, privilegiando l'interconnessione application-to-application tra i rispettivi sistemi informativi, con le opportune misure di sicurezza. Ciò consentirebbe di automatizzare il più possibile il processo di raccolta dei dati presso i soggetti esterni, rafforzando l'intera filiera di trattamento delle informazioni che, altrimenti, risulterebbero accessibili a una molteplicità di soggetti incaricati amplificando

le possibilità di loro utilizzo illegittimo. Se ne gioverebbe inoltre la qualità dei dati trasmessi, su cui gravano al momento diversi passaggi manuali effettuati da operatori con differenziati livelli di capacità tecnica;

2) nel caso in cui l'Agenzia, differentemente da quanto previsto al precedente punto 1), ritenga di utilizzare il servizio telematico Entratel, ovvero altro canale telematico che l'Agenzia riterrà di predisporre per la trasmissione dei dati di cui al presente schema di provvedimento, devono essere introdotti misure e accorgimenti volti ad assicurare che:

- l'operatore finanziario possa inviare il file, già cifrato all'origine, in un'unica soluzione;

- vengano individuate e autorizzate le singole e sole postazioni client tramite cui viene effettuata la comunicazione, ricorrendo a misure organizzative o tecniche, quale ad esempio, la certificazione digitale delle postazioni client (riducendo al minimo la possibilità di trasferimento dei certificati, che andrebbero generati tenuto conto di diversi parametri connessi strettamente alla postazione remota) o altra misura equivalente;

- la sicurezza delle postazioni periferiche sia verificata con gli strumenti che la tecnologia mette a disposizione in fase di interazione web, rifiutando l'accesso all'applicativo alle postazioni non conformi ai requisiti richiesti. Oltre alle versioni del sistema operativo o del browser utilizzati, ricavabili dai dati trasmessi tramite protocollo http, potrebbero essere rilevate con strumenti software integrativi altre qualità inerenti la sicurezza come, ad esempio, lo stato di aggiornamento dei sistemi di protezione antivirus, la presenza di protezioni contro i malware e altri parametri tecnici connessi alla sicurezza. In tal modo l'Agenzia raggiungerebbe due obiettivi collaterali apprezzabili nell'ottica di innalzamento complessivo della sicurezza: promuoverebbe da un lato l'utilizzo da parte dei soggetti alimentatori delle proprie banche dati di strumenti software aggiornati e più sicuri, con possibile effetto sulla qualità dei dati e ridurrebbe dall'altro i rischi potenzialmente derivanti dalla compromissione delle postazioni terminali a opera di malware di vario genere, che potrebbe comportare violazioni della sicurezza dei dati presso l'operatore finanziario o il soggetto che effettua la comunicazione;

- per l'autenticazione siano utilizzati sistemi di autenticazione informatica basati su tecniche di strong authentication, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione per tutti gli utilizzatori del sistema. Consideri l'Agenzia, inoltre, anche forme differenti di strong authentication rispetto alla CNS Carta nazionale dei servizi che assicurino un livello equivalente di sicurezza. Strumenti alternativi alla CNS sono opportuni qualora l'Agenzia riscontri effettive insormontabili incompatibilità tra l'utilizzo della CNS quale strumento di strong authentication con altre misure di sicurezza prescritte dal Garante, relative alla certificazione digitale delle postazioni client che interagiscono con l'applicativo Entratel;

- l'applicazione sia offerta all'accesso in rete quantomeno su indirizzi o porte diverse allo scopo di differenziare all'origine il bacino di utenza "privato" (persone fisiche) dall'utenza "aziendale": ciò perché l'identificazione dell'utente comporta, allo stato attuale del sistema Entratel, la necessità da parte dell'utente abilitato di dichiarare il proprio ruolo, ovvero se operi nella qualità di dipendente di un soggetto

esterno o in proprio quale persona fisica; sia assicurata, inoltre, la separazione tra i profili di autorizzazione, consentendone una più completa e flessibile gestione. Valuti eventualmente l'Agenzia forme equivalenti di realizzazione della separazione degli ambiti che consentano l'applicazione di differenziate misure di sicurezza e di controllo in base alla natura dei dati trasmessi e al ruolo rivestito dall'utente;

3) l'Agenzia, a prescindere dalla modalità di trasmissione prescelta di cui ai precedenti punti 1) e 2), deve assicurarsi che il procedimento di cifratura del file da trasmettere da parte dell'operatore finanziario possa avvenire già contestualmente alla estrazione dei dati dai sistemi, o, quantomeno, nella fase immediatamente successiva, preferibilmente con l'utilizzo di strumenti automatici che non prevedano l'intervento di un operatore.

Per quanto riguarda, invece, l'adeguatezza del servizio Entratel rispetto alle altre comunicazioni all'anagrafe tributaria per le quali attualmente è utilizzato, il Garante si riserva di esaminare le predette criticità in separata sede, anche congiuntamente all'Agenzia delle entrate.

3. La conservazione dei dati presso l'anagrafe tributaria

Come direttamente previsto dal legislatore (art. 11, comma 2, del decreto legge citato), lo schema di provvedimento stabilisce che i dati oggetto della comunicazione annuale da parte degli operatori finanziari sono destinati ad essere archiviati nell'apposita sezione separata dell'anagrafe tributaria, denominata archivio dei rapporti finanziari.

Viene altresì previsto che tali dati contabili, trattati unicamente per la formazione con procedure centralizzate di specifiche liste selettive di contribuenti a maggior rischio di evasione, non implementeranno i dati accessibili attraverso la procedura delle indagini finanziarie.

Tuttavia, il citato art. 11, comma 4, prevede che tali informazioni possano essere utilizzate anche per le ulteriori finalità di cui all'art. 7, comma 11, d.P.R. n. 605, per le quali allo stato è consentito accedere all'attuale versione dell'archivio dei rapporti finanziari.

Pertanto, laddove vengano previsti casi di trattamento dei dati oggetto della comunicazione integrativa annuale ulteriori rispetto a quanto previsto nello schema di provvedimento in esame, occorre sottoporre alla verifica preliminare del Garante tale circostanza ai fini dell'individuazione di procedure e garanzie idonee a consentire il rispetto dei diritti e delle libertà fondamentali, nonché della dignità degli interessati (art. 17 del Codice).

Per quanto riguarda i tempi di conservazione, l'Agenzia ha scelto di avvalersi del termine massimo previsto dal legislatore, ovvero quello di decadenza in materia di accertamento delle imposte sui redditi, pur senza aver definito i criteri di formazione delle liste ai sensi dell'art. 11, comma 4 del citato decreto. Su tali aspetti si rileva, tuttavia, che la conservazione dei dati deve essere commisurata al tempo necessario e predeterminato a raggiungere la finalità perseguita.

Pertanto, si ritiene che nello schema di provvedimento debbano essere esplicitati i periodi di conservazione necessari e che, in ogni caso, allo scadere di tale periodo deve essere disposta l'integrale e automatica cancellazione dei dati.

Con riferimento alle misure di sicurezza relative alla conservazione dei dati in anagrafe tributaria, resta ferma l'esigenza di esaminare organicamente, in altra sede e in un più ampio contesto, l'ulteriore incremento di livelli di sicurezza da garantire rispetto a trattamenti di dati quali quelli effettuati presso l'archivio dei rapporti finanziari.

E) Ulteriori osservazioni

A margine del presente parere, riferito unicamente alle modalità di comunicazione, nonché delle misure di sicurezza per la trasmissione e la conservazione dei dati, si evidenzia che lo schema di provvedimento in esame prevede la raccolta massiva dei dati contabili (saldi iniziali e finali del rapporto finanziario e dati aggregati delle movimentazioni con l'evidenza del dare e avere) relativi a tutta la platea di soggetti titolari di rapporti già censiti nell'archivio dei rapporti finanziari al fine di classificare l'intera popolazione in base al rispettivo rischio di evasione.

Alla luce di quanto stabilito nello schema, infatti, la raccolta di tali dati riferiti alla totalità dei contribuenti è finalizzata unicamente all'elaborazione con procedure centralizzate delle liste selettive di contribuenti a maggior rischio di evasione, secondo i criteri che dovranno essere successivamente individuati con provvedimento del Direttore dell'Agenzia (art. 11, comma 4, del citato decreto legge). Le posizioni, così individuate, saranno segnalate per l'avvio delle attività di controllo fiscale.

Al riguardo, si sottolinea che l'individuazione di criteri astratti volti ad analizzare il comportamento del contribuente, soprattutto laddove effettuati sulla base di numerose tipologie di dati presenti in anagrafe tributaria, presenta rischi specifici per i diritti fondamentali e la libertà, nonché la dignità degli interessati, che richiedono la previsione di adeguate garanzie, fermo restando il divieto di adottare atti o provvedimenti amministrativi fondati unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato (artt. 14 e 17 del Codice).

Nell'occasione dell'espressione del presente parere, pertanto, considerati i predetti rischi che comporta una siffatta attività di classificazione del contribuente, si ritiene necessario che l'Agenzia sottoponga a questa Autorità ai fini di una verifica preliminare il provvedimento del Direttore dell'Agenzia delle entrate con il quale saranno definiti i criteri per l'elaborazione delle liste al fine di individuare eventuali misure e accorgimenti idonei a garantire l'applicazione dei principi in materia di protezione dei dati personali (artt. 14 e 17 del Codice), fermo restando l'obbligo di notificazione al Garante ai sensi dell'art. 37, comma 1, lett. d), del Codice.

TUTTO CIO' PREMESSO IL GARANTE:

ai sensi dell'articolo 154, commi 4 e 5, del Codice, esprime il parere richiesto sullo schema di provvedimento del Direttore dell'Agenzia delle entrate concernente le "Disposizioni di attuazione dell'articolo 11, commi 2 e 3, del decreto legge 6 dicembre 2011 n. 201, convertito, con modificazioni, dalla legge 22 dicembre 2011 n. 214. Comunicazione integrativa annuale all'archivio dei rapporti finanziari" con le osservazioni relative all'esigenza che:

1) lo schema di provvedimento deve essere integrato con l'individuazione di adeguate misure di sicurezza, di natura tecnica e organizzativa, anche in relazione al trattamento posto in essere dagli operatori finanziari per la comunicazione annuale volte a garantire che, qualora la trasmissione non avvenga con interconnessione application-to-application tra i rispettivi sistemi informativi:

a) anche in considerazione delle dimensioni dell'operatore finanziario, vengano utilizzati meccanismi di cifratura e di sicurezza, rispettivamente finalizzati a proteggere le informazioni contenute nel file durante i successivi passaggi all'interno dell'operatore stesso e ad assicurare l'integrità del contenuto e a prevenirne alterazioni;

b) le eventuali trasmissioni interne all'operatore finanziario avvengano esclusivamente su protocolli sicuri (https/ssl, SFTP, ecc.);

c) nel caso in cui le comunicazioni all'archivio dei rapporti finanziari vengano effettuate con l'intervento di un utente, tali soggetti devono essere scelti dagli operatori finanziari sulla base di elevati requisiti di idoneità soggettiva, preferibilmente tra soggetti che abbiano un rapporto stabile con essi;

d) l'accesso al file, nelle successive fasi del trattamento, sia circoscritto ad un numero il più possibile limitato di incaricati, non abilitati alla modifica delle informazioni contenute nel file;

e) qualora la comunicazione all'Agenzia delle entrate avvenga mediante l'utilizzo di postazioni client, tali postazioni devono disporre di versioni costantemente aggiornate del sistema operativo, del browser, dei programmi antivirus e anti-intrusione e degli altri software applicativi utilizzati sulla postazione medesima, al fine di ridurre i rischi connessi ad accessi non consentiti o all'azione di virus o altri malware. In relazione alle dimensioni del singolo operatore finanziario, deve essere valutata la possibilità che le postazioni abilitate all'invio dei dati attraverso il canale predisposto dall'Agenzia delle entrate siano dotate di misure di sicurezza aggiuntive (per assicurare che sia i suddetti file che le relative chiavi di cifratura non possano essere copiati su supporti esterni), ovvero l'opportunità di riservare una postazione, opportunamente configurata e messa in sicurezza, dedicata all'invio di tali comunicazioni all'Agenzia delle entrate;

f) in seguito all'invio, l'eventuale conservazione del file da parte dell'operatore finanziario deve avvenire esclusivamente in forma cifrata;

g) i soggetti incaricati del trattamento relativo alle comunicazioni all'archivio dei rapporti finanziari siano scelti dagli operatori finanziari sulla base di elevati requisiti di idoneità soggettiva, preferibilmente tra soggetti che abbiano un rapporto stabile con essi. Qualora gli operatori finanziari decidano di affidare la

comunicazione a soggetti esterni, responsabili o incaricati del trattamento, il file dovrà essere loro fornito già cifrato;

2) l'Agenzia predisponga l'uso di canali di comunicazione diversi e alternativi al servizio Entratel, soprattutto per le comunicazioni da parte di soggetti detentori di una elevata quantità di dati come i gruppi bancari, privilegiando l'interconnessione application-to-application tra i rispettivi sistemi informativi, con le opportune misure di sicurezza. Ciò consentirebbe di automatizzare il più possibile il processo di raccolta dei dati presso i soggetti esterni, rafforzando l'intera filiera di trattamento delle informazioni che, altrimenti, risulterebbero accessibili a una molteplicità di soggetti incaricati amplificando le possibilità di loro utilizzo illegittimo. Se ne gioverebbe inoltre la qualità dei dati trasmessi, su cui gravano al momento diversi passaggi manuali effettuati da operatori con differenziati livelli di capacità tecnica;

3) nel caso in cui l'Agenzia, differentemente da quanto previsto al precedente punto 2), ritenga di utilizzare il servizio telematico Entratel, ovvero altro canale telematico che l'Agenzia riterrà di predisporre per la trasmissione dei dati di cui al presente schema di provvedimento, devono essere introdotti misure e accorgimenti volti ad assicurare che:

a) l'operatore finanziario possa inviare il file, già cifrato all'origine, in un'unica soluzione;

b) venga effettuata la certificazione digitale delle postazioni client o altra misura equivalente;

c) la sicurezza delle postazioni periferiche sia verificata con gli strumenti che la tecnologia mette a disposizione in fase di interazione web, rifiutando l'accesso all'applicativo alle postazioni non conformi ai requisiti richiesti, che dovranno tenere conto della versione del sistema operativo e del browser utilizzati; valuti l'Agenzia anche l'utilizzo di strumenti software integrativi idonei a rilevare altre qualità inerenti la sicurezza come, ad esempio, lo stato di aggiornamento dei sistemi di protezione antivirus, la presenza di protezione contro il malware e altri parametri tecnici;

d) per l'autenticazione siano utilizzati sistemi di autenticazione informatica basati su tecniche di strong authentication, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione per tutti gli utilizzatori del sistema. Consideri l'Agenzia, inoltre, anche forme differenti di strong authentication rispetto alla CNS Carta nazionale dei servizi che assicurino un livello equivalente di sicurezza. Strumenti alternativi alla CNS sono opportuni qualora l'Agenzia riscontri effettive insormontabili incompatibilità tra l'utilizzo della CNS quale strumento di strong authentication con altre misure di sicurezza prescritte dal Garante, relative alla certificazione digitale delle postazioni client che interagiscono con l'applicativo Entratel;

e) sia assicurata la separazione tra i profili di autorizzazione, consentendone una più completa e flessibile gestione, anche offrendo l'accesso in rete all'applicazione quantomeno su indirizzi o porte diverse da quelli utilizzabili in qualità di privato cittadino. Valuti eventualmente l'Agenzia forme equivalenti di realizzazione della separazione degli ambiti che consentano l'applicazione di differenziate misure di sicurezza e di controllo in base alla natura dei dati trasmessi e al ruolo rivestito dall'utente;

4) l'Agenzia, a prescindere dalla modalità di trasmissione prescelta di cui ai precedenti punti 2) e 3), deve assicurarsi che il procedimento di cifratura del file da trasmettere da parte dell'operatore finanziario possa avvenire già contestualmente alla estrazione dei dati dai sistemi, o, quantomeno, nella fase immediatamente successiva, preferibilmente con l'utilizzo di strumenti automatici che non prevedano l'intervento di un operatore;

5) laddove vengano previsti casi di trattamento dei dati oggetto della comunicazione integrativa annuale ulteriori rispetto a quanto previsto nello schema di provvedimento in esame, l'Agenzia sottoponga alla verifica preliminare del Garante tale circostanza ai fini dell'individuazione di procedure e garanzie idonee a consentire il rispetto dei diritti e delle libertà fondamentali, nonché della dignità degli interessati (art. 17 del Codice);

6) nello schema di provvedimento siano esplicitati i periodi di conservazione necessari e che, in ogni caso, allo scadere di tale periodo deve essere disposta l'integrale e automatica cancellazione dei dati.

Per le ragioni illustrate nelle osservazioni (punto E), si richiama l'attenzione in ordine alla circostanza che venga sottoposto a questa Autorità, ai fini di una verifica preliminare, il provvedimento del Direttore dell'Agenzia delle entrate con il quale saranno definiti i criteri per l'elaborazione delle liste al fine di individuare adeguate garanzie a tutela degli interessati (artt. 14 e 17 del Codice).

Roma, 17 aprile 2012

IL PRESIDENTE

Pizzetti

IL RELATORE

Pizzetti

IL SEGRETARIO GENERALE

De Paoli