Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

Le regole attuative del sistema pubblico di prevenzione delle frodi ai consumatori mediante furto di identità: le norme sulla identità digitale nell'ordinamento italiano e il Regolamento del Ministero dell'Economia n. 95/2014.

di:
Prof. Avv. Alessandro del Ninno
Studio Legale Tonucci & Partners
adelninno@tonucci.com

Indice

§ 1. La ricostruzione preliminare del quadro normativo in materia di identità digitale e furto di identità nell'ordinamento italiano.

§ 2. Il decreto del Ministero dell'Economia n. 95 del 19 maggio 2014 - Regolamento recante norme di attuazione del sistema pubblico di prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo, con specifico riferimento al furto d'identità.

§ 2.1. Segue: i dati oggetto di riscontro delle verifiche di autenticità.
§ 2.2. Segue: i dati sulle frodi subite e sui rischi di frode comunicate dagli aderenti diretti per alimentare l'Archivio.
§ 2.3. Segue: la struttura dell'Archivio anti-frode e i diversi livelli e diritti di accesso alle informazioni.
§ 2.4. Segue: le modalità di invio della richiesta di riscontro di autenticità e del riscontro anti-frode.

---

§ 1. La ricostruzione preliminare del quadro normativo in materia di identità digitale e furto di identità nell'ordinamento italiano.

Di recente, con la pubblicazione nella Gazzetta Ufficiale n. 150 del 1° luglio 2014 del decreto del Ministero dell'Economia n. 95 del 19 maggio 2014 ("*Regolamento recante norme di attuazione del sistema pubblico di prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo, con specifico riferimento al furto d'identità*"), sono entrate in vigore le norme di attuazione del decreto legislativo 141/2010 che ha fissato i principi normativi generali per combattere le frodi nel settore del credito al consumo e dei pagamenti differiti o dilazionati, con specifico riferimento al furto d'identità.

Prima di analizzare la portata pratica delle nuove norme regolamentari, appare utile fornire un sintetico richiamo ad alcune norme dell'ordinamento che definiscono i concetti di "*identità digitale*" e di "*furto di identità*".

Il decreto legislativo 11 aprile 2011, n. 64, novellando proprio il decreto legislativo 13 agosto 2010, n. 141 sopra richiamato, ha per la prima volta introdotto nell'ordinamento italiano la nozione di "*furto di identità*" (sia pure non a fini penali, visto che il Legislatore non ha previsto affatto una nuova fattispecie di reato; difatti, in mancanza di una fattispecie incriminatrice specifica, il furto di identità viene ricondotto dalla giurisprudenza di legittimità nell'ambito del reato di cui all'art. 494 c.p., relativo alla "*sostituzione di persona*", secondo il quale: "*chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome o un falso stato ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino a un anno*", e ciò anche se la "*sostituzione di persona*" non è congruente, come fattispecie, al "*furto di identità*").

Ai sensi del decreto legislativo 64/2011, dunque, il furto di identità può avvenire mediante:

a) *l'impersonificazione totale*: cioè, l'occultamento totale della propria identità mediante l'utilizzo indebito di dati relativi all'identità e al reddito di un altro soggetto. L'impersonificazione può riguardare l'utilizzo indebito di dati riferibili sia ad un soggetto in vita sia ad un soggetto deceduto;

b) *l'impersonificazione parziale*: cioè l'occultamento parziale della propria identità mediante l'impiego, in forma combinata, di dati relativi alla propria persona e l'utilizzo indebito di dati relativi ad un altro soggetto, nell'ambito di quelli di cui alla lettera a).

Successivamente, l'art. 9, co. I, lett. a), della legge 15 ottobre 2013, n. 119 - che ha convertito in legge, con modificazioni, il decreto-legge 14 agosto 2013, n. 93 - ha novellato l'art. 640 del codice penale (rubricato "*Frode informatica*") introducendo il nuovo articolo 640-*ter* rubricato"*Frode informatica commessa con sostituzione d'identità digitale*". Detta disposizione legislativa dispone che la "*pena e' della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto e' commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti*". Ma tale intervento ha sollevato numerose polemiche ed evidenziato quelle che saranno gravissime lacune in sede interpretativa, visto che il Legislatore non ha affatto fornito una definizione di "identità digitale" né ha chiarito le modalità pratiche con le quali dovrebbe avvenire il furto.

Per avere una prima definizione normativa di "*identità digitale*" occorre attendere il decreto della Presidenza del Consiglio dei Ministri 24 ottobre 2014 (pubblicato sulla Gazzetta Ufficiale n. 285 del 9 dicembre 2014) intitolato "*Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche*

amministrazioni e delle imprese" (SPID che dovrebbe diventare operativa entro Aprile 2015). Il Sistema Pubblico per la gestione delle Identità Digitali di cittadini e imprese sarà costituito da una rete di autenticatori sia pubblici che privati – i *gestori dell'identità digitale* - che gestiranno i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete per conto di cittadini e imprese. In sintesi, il cittadino, una volta effettuate le procedure di autenticazione con uno dei soggetti coinvolti, potrà usare tutti i servizi *online* forniti da tutti gli altri soggetti che hanno aderito al network).

L'articolo 1, co. 1, lettera (o) definisce la "*identità digitale*"come: "*la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità di cui al presente decreto e dei suoi regolamenti attuativi*" (anche se con tale definizione – più precisamente – sembrerebbe rimandarsi più a un metodo di identificazione informatica piuttosto che a un vero e proprio concetto di identità digitale, richiamandosi più che altro una norma già presente nel Codice dell'Amministrazione Digitale - l'art. 1, co. 1, lett. e), del d.lgs. 7 marzo 2005, n. 82 - in cui è stato chiarito che, per "*identificazione informatica*" si intende la "*validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso*").

Non è questa la sede per analizzare criticamente la portata operativa delle varie norme sopra richiamate per meri fini di ricostruzione del quadro normativo; non ci si può però esimere dal rilevare l'estrema difficoltà che caratterizzerà la pur necessaria attività di coordinamento interpretativo ed applicativo di norme e concetti tecnici, sovrapposti e slegati tra di loro. Solo per fare un esempio: il coordinamento tra l'*identità digitale* come definita dal DPCM sullo SPID e l'identità come tratta dal *documento digitale unificato* -DDU previsto dal *Decreto Crescitalia* del Governo Monti - il d.l. 18 ottobre 2012, n. 179 – che dovrebbe sostituire la carta d'identità e la tessera sanitaria e offrire al cittadino la possibilità di accedere in via telematica ai servizi erogati dalle amministrazioni pubbliche. Non è affatto sembrata chiarificatrice la posizione dell'Agenzia per l'Italia Digitale che – sul punto – si è limitata a segnalare che lo SPID realizza un modello federato adatto a vari scenari - tecnologici, organizzativi e di business, anche in mobilità - nel quale oltre alle identità personali sono gestiti i ruoli, i titoli e le qualifiche professionali, non gestiti con il DDU.

O si pensi, per fare un altro esempio, al coordinamento tra la *identità digitale* e il *domicilio digitale*. Con l'art. 14 del decreto legge 69/2013 è stata difatti introdotta una specifica disposizione che prevede il domicilio digitale via PEC: "*all'atto della richiesta del documento unificato DDU, ovvero all'atto dell'iscrizione anagrafica o della dichiarazione di cambio di residenza a partire dall'entrata a regime dell'Anagrafe nazionale della popolazione residente, è assegnata al cittadino una casella di posta elettronica certificata, con la funzione di*

domicilio digitale, ai sensi dell'articolo 3-bis del Codice dell'Amministrazione Digitale, successivamente attivabile in modalità telematica dal medesimo cittadino."

Si fa poi rinvio ad un successivo decreto del Ministro dell'interno con cui verranno stabilite le modalità di rilascio del *domicilio digitale* all'atto di richiesta del DDU. Ma né tale decreto, ne quelli relativi all'attivazione dell'Anagrafe Nazionale della Popolazione Residente (ANPR, che subentrerà alle anagrafi e attraverso un'applicazione web e alcuni strumenti online fornirà ai comuni i dati anagrafici dei residenti e consentirà tutte le operazioni inerenti l'elaborazione delle informazioni anagrafiche di interesse), né le regole attuative del documento digitale unificato DDU hanno ancora visto la luce, e non si conoscono attualmente i tempi di attuazione.

Si aggiunga infine che in materia di identità digitale il quadro normativo si dovrà altresì coordinare con le disposizioni contenute nel *Regolamento UE n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno* (che abroga la Direttiva UE sulle firme elettroniche del 1999). Tale Regolamento (immediatamente applicabile negli ordinamenti nazionali degli Stati Membri senza necessità alcuna di recepimento) - noto con l'acronimo di *eIDAS electronic IDentification Authentication and Signature (eTS electronic Trust Services*) - stabilisce le condizioni per il riconoscimento reciproco in ambito di identificazione elettronica e le regole comuni per le firme elettroniche, l'autenticazione web ed i relativi servizi fiduciari per le transazioni elettroniche. Entrato in vigore il 17 Settembre 2014, sarà applicabile a partire dal 1° Luglio 2016. In tema di identità digitale, esso introduce una serie di definizioni che articolano il quadro, rendendo ben più difficile il coordinamento con le norme italiane in materia già vigenti. Intanto – e deve dirsi più correttamente – il Legislatore comunitario (art. 3, Reg. eIDAS) parla non di "*identità digitale*" ma di "*identificazione elettronica*" contrapposta ai "*dati di identificazione personale*" (e questo è forse invece un diverso concetto più vicino a quello di identità, appunto il risultato di un insieme di dati):

- «*identificazione elettronica*», il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica;
- «*dati di identificazione personale*», un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica;

per poi istituire un «*regime di identificazione elettronica*» (cioè un sistema di identificazione elettronica per cui si forniscono mezzi di identificazione elettronica alle persone fisiche o giuridiche, o alle persone fisiche che rappresentano persone giuridiche) nell'ambito del quale procedere alla vera e propria «*autenticazione*» (cioè un

processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure l'origine e l'integrità di dati in forma elettronica).

A fronte di queste differenze concettuali tra norme italiane e comunitarie, non si deve essere così certi della facile convivenza – interpretativa e applicativa – delle menzionate regole. E ciò anche se l'Agenzia per l'Italia Digitale ha evidenziato che dopo l'emanazione del Regolamento *eIDAS* e la notifica da parte del governo italiano del DPCM che regolamenta lo SPID alla Commissione europea, il sistema italiano – primo del genere - sarà accettato dagli altri Stati membri dell'UE e il combinato disposto dei due provvedimenti regolatori consentirà di realizzare l'interoperabilità del sistema SPID nel panorama tecnologico europeo.

* * * *

§ 2. Il decreto del Ministero dell'Economia n. 95 del 19 maggio 2014: i partecipanti e i principi in materia di protezione dei dati personali.

Come già segnalato in apertura del presente contributo, il decreto del Ministero dell'Economia n. 95 del 19 maggio 2014 (di seguito, "*Regolamento*") ha introdotto le norme di attuazione ed esecuzione dei principi normativi generali di cui al d.lgs. 141/2010 al fine di permettere la verifica dell'autenticità dei dati contenuti nella documentazione fornita dalle persone fisiche, per combattere le frodi nel settore del credito al consumo e dei pagamenti differiti o dilazionati, con specifico riferimento al furto d'identità. L'insieme delle nuove regole esecutive disciplina la struttura del sistema di prevenzione (istituito presso lo stesso Ministero dell'Economia, titolare del relativo archivio, mentre la sua gestione è delegata alla la Concessionaria servizi assicurativi pubblici S.p.A. – Consap, nella qualità di "*ente gestore*"), le tipologie di dati trattati, le modalità di collegamento dell'archivio informatizzato con le banche dati pubbliche, le fasi che caratterizzano la procedura di riscontro, nonché la misura della contribuzione a carico degli aderenti diretti.

Partecipano a tale sistema (e sono destinatari delle relative regole):

a) le banche, comprese quelle comunitarie e quelle extracomunitarie, e gli intermediari finanziari iscritti nell'elenco generale di cui all'articolo 106 del decreto legislativo 1º settembre 1993, n. 385 (Testo Unico delle norme bancarie e finanziarie);

b) i fornitori di servizi di comunicazione elettronica, ai sensi dell'articolo 1, comma 1, lettera gg), del codice di cui al decreto legislativo 1º agosto 2003, n. 259;

c) i fornitori di servizi interattivi associati o di servizi di accesso condizionato ai sensi dell'articolo 2, comma 1, lettera q), del decreto legislativo 31 luglio 2005, n. 177;

d) le imprese di assicurazione;

complessivamente definiti come gli «*aderenti diretti*», e ne sono altresì parte, in base ad apposita convenzione con il Ministero dell'Economia e delle Finanze, i gestori di sistemi di informazioni creditizie (cioè le centrali rischi private) e le imprese che offrono agli aderenti diretti (ad eccezione delle imprese di assicurazione) servizi assimilabili alla prevenzione, sul piano amministrativo, delle frodi (questi ultimi soggetti rientrano nella categoria dei cosiddetti «*aderenti indiretti*»).

Fin dalle prime disposizioni, il Regolamento fissa e prescrive ovvi obblighi di rigoroso rispetto della disciplina sul trattamento dei dati personali (stante la delicatezza delle informazioni trattate) di cui al Codice della privacy (d.lgs. 30 Giugno 2003, n. 196): d'altra parte, la stessa Autorità Garante per la protezione dei dati personali aveva indicato al Ministero le necessarie modifiche al testo, condizione di rilascio del parere favorevole (si veda difatti il relativo Parere dell'Autorità n. 135 del 21 Marzo 2013).

Il trattamento dei dati personali, da parte del Ministero dell'Economia - titolare dell'archivio - dell'ente gestore e degli aderenti diretti e indiretti è dunque autorizzato esclusivamente per le finalità inerenti alla prevenzione del furto d'identità nei settori del credito al consumo, dei pagamenti dilazionati e differiti, dei servizi di comunicazione elettronica e interattivi, nonché nel settore assicurativo (tale formulazione si conforma ad una specifica richiesta del Garante che nel Parere 135/2013 aveva richiesto che fossero esplicitati le finalità del trattamento e l'ambito applicativo del Regolamento, con la previsione ulteriore che le informazioni trattate presso il Ministero e da tutti i soggetti coinvolti e che accedono all'archivio non potessero essere utilizzate per scopi diversi o comunque incompatibili con quelli indicati nel decreto legislativo 14172010 e nel Regolamento).

E proprio in tale ottica, sempre seguendo le indicazioni del Garante per la privacy, gli aderenti diretti partecipano al sistema di prevenzione esclusivamente in relazione ai dati personali, pertinenti e non eccedenti, necessari al perseguimento delle specifiche finalità inerenti al settore commerciale di appartenenza. Invece gli aderenti indiretti - previo conferimento di apposito incarico o delega da parte degli aderenti diretti - vi partecipano esclusivamente in relazione ai dati personali, pertinenti e non eccedenti, necessari allo scopo di offrire agli aderenti diretti i servizi riguardanti l'invio alla Consap di richieste di verifica dell'autenticità dei dati oggetto di riscontro.

Come principio privacy di carattere generale, poi, il Regolamento prescrive che tutti i soggetti che a vario titolo partecipano al sistema sono obbligati ad adottare tutte le misure logistiche, organizzative e di sicurezza necessarie ad assicurare un elevato livello di protezione dei dati personali oggetto di trattamento: sul rispetto di tale fondamentale obbligo in capo a tutti i soggetti coinvolti sovrintende lo stesso Ministero dell'Economia, nella sua qualità di titolare del trattamento. Mentre la Consap, in qualità di ente gestore, ha il compito di dare esecuzione ai provvedimenti del Garante

per la protezione dei dati personali che dispongono il blocco del trattamento dei dati personali, la rettifica o la cancellazione dei medesimi dall'Archivio.

§ 2.1. Segue: i dati oggetto di riscontro delle verifiche di autenticità.

Prima di analizzare la struttura dell'archivio, è opportuno chiarire ed elencare quali dati entreranno a farne parte e costituiranno l'oggetto di riscontro delle richieste di verifica di autenticità. In tale ambito, nella definizione di tali informazioni, il Regolamento distingue tre macro-categorie, dettagliando gli specifici e (tassativi) dati, cioè:

1. quelli relativi ai documenti di identità (a loro volta suddivisi in elementi identificativi del soggetto che richiede di effettuare l'operazione - cioè nome e cognome; data e luogo di nascita; sesso; cittadinanza; domicilio fiscale; provincia; codice avviamento postale; riscontro dell'esistenza in vita – ed elementi identificativi dei documenti di identità in quanto tali, cioè tipologia di documento; numero del documento; data di rilascio del documento; data di scadenza del documento; ente che ha rilasciato il documento; provincia del comune che ha rilasciato il documento; numero di serie del supporto plastico; riscontro della presenza del documento nell'archivio dei documenti smarriti o rubati);

2. quelli relativi alle tessere sanitarie, ai codici fiscali, alle partite IVA e ai documenti che attestano il reddito, riferibili alle persone fisiche (cioè numero della tessera sanitaria; data di rilascio della tessera sanitaria; data di scadenza della tessera sanitaria; numero del codice fiscale; numero della partita IVA; data di attribuzione della partita IVA; anno dell'ultima presentazione della dichiarazione dei redditi; riscontro della fascia di reddito entro la quale la persona fisica è collocata);

3. quelli relativi alle posizioni contributive previdenziali ed assistenziali (cioè data di inizio del rapporto di lavoro; tipologia del rapporto di lavoro; qualifica; periodo di competenza del prospetto di paga; imponibile previdenziale del prospetto di paga; numero posizione contributiva previdenziale del datore di lavoro; numero posizione assicurativa del datore di lavoro; nominativo del datore di lavoro o del rappresentante legale; numero del codice fiscale del datore di lavoro; numero della partita IVA del datore di lavoro).

Di seguito (come peraltro anche nel Regolamento) l'insieme delle sopra elencate informazioni è definito complessivamente come "*Dati*".

§ 2.2. Segue: i dati sulle frodi subite e sui rischi di frode comunicate dagli aderenti diretti per alimentare l'Archivio.

Il Regolamento prevede che gli aderenti diretti – per poter beneficiare delle richieste di verifica preventiva di autenticità delle informazioni – debbano a loro volta alimentare l'archivio con specifiche informazioni: (a) sulle frodi effettivamente subite (da trasmettersi in via telematica entro due giorni lavorativi decorrenti dalla loro acquisizione); (b) sul rischio di potenziali frodi (da trasmettersi in via telematica entro un giorno lavorativo decorrente dalla loro acquisizione). La massa di informazioni incrociate che alimenta e confluisce nell'Archivio da parte di ciascun aderente diretto, renderà ovviamente più puntuali i riscontri quando quegli stessi aderenti richiederanno la verifica preventiva di autenticità.

Le informazioni relative alle frodi subite che gli aderenti diretti devono comunicare all'Archivio sono composte dalle seguenti cinque macro-categorie informative:

a) elementi identificativi dell'aderente diretto e data della segnalazione;

b) elementi identificativi del soggetto che ha disconosciuto l'operazione (nome e cognome; data e luogo di nascita; sesso; cittadinanza; codice fiscale);

c) elementi identificativi del documento di identità e del documento che attesta il reddito utilizzati per l'operazione disconosciuta (tipologia di documento di identità; numero del documento di identità; data di rilascio del documento di identità; data di scadenza del documento di identità; ente che ha rilasciato il documento di identità; documento di identità smarrito o rubato; tipologia di documento di reddito utilizzato);

d) elementi identificativi dell'operazione disconosciuta (data dell'operazione; tipologia dell'operazione; importo dell'operazione; modalità di rimborso dell'operazione; finalità dell'operazione; data in cui è stata disconosciuta l'operazione; motivo del disconoscimento; estremi della denuncia presentata all'Autorità giudiziaria dal soggetto che ha disconosciuto l'operazione);

e) elementi identificativi dell'esercizio commerciale dove e' stata effettuata l'operazione disconosciuta (ragione o denominazione sociale; indirizzo; provincia; codice avviamento postale; partita IVA).

I dati sulle frodi subite restano iscritte nell'Archivio per tre anni dalla data di ricevimento.

Per quanto riguarda il rischio di frodi, lo stesso Regolamento detta un parametro specifico: si configura il rischio di frodi che comporta la comunicazione quando sono

rilevate tre o più incongruenze in sede di riscontro dell'autenticità' dei Dati forniti dal soggetto che richiede di effettuare l'operazione.

Invece, le informazioni relative al paventato rischio di frodi (obbligatorie da comunicare, stabilito il parametro che precede) sono composte dalle seguenti sei macro-categorie informative:

a) elementi identificativi dell'aderente diretto e data della segnalazione;

b) elementi identificativi del soggetto che richiede di effettuare l'operazione (nome e cognome; data e luogo di nascita; sesso; cittadinanza; codice fiscale);

c) elementi identificativi del documento di identità e del documento che attesta il reddito presentati dal soggetto (tipologia di documento di identità;numero del documento di identità; tipologia di documento di reddito presentato);

d) elementi identificativi dell'operazione (data della richiesta relativa all'operazione; tipologia dell'operazione; importo dell'operazione; modalità di rimborso dell'operazione; finalità dell'operazione; operazione autorizzata o negata);

e) elementi identificativi dell'esercizio commerciale dove e' stata presentata la richiesta di effettuare l'operazione (ragione o denominazione sociale; indirizzo; provincia; codice avviamento postale; partita IVA);

f) causale della comunicazione.

Vi è da precisare che circa la comunicazione delle informazioni sui meri rischi di frode, l'aderente diretto comunica al Ministero dell'Economia l'apertura di un periodo di monitoraggio diretto ad accertare l'effettiva sussistenza del rischio di frode (tale periodo non può superare i quindici giorni). All'esito del monitoraggio, l'aderente diretto ne comunica l'esito alla Consap in termini di «*accertamento della frode subita*» o di «*conclusione del monitoraggio senza ulteriori provvedimenti*». Sulla base di tale comunicazione, la Consap provvederà – rispettivamente - a riqualificare le informazioni da "rischio di frode" a "frode subita" oppure provvederà alla loro cancellazione (le informazioni sono altresì cancellate se l'aderente diretto non comunica l'esito del monitoraggio).

§ 2.3. Segue: la struttura dell'Archivio anti-frode e i diversi livelli e diritti di accesso alle informazioni.

Per quanto riguarda la struttura dell'archivio anti-frode centralizzato nell'ambito del sistema di prevenzione ("*Archivio*") è prevista una articolata struttura in sei diversi livelli, con diversi diritti di accesso in capo ai partecipanti: difatti gli

aderenti indiretti non possono accedere oltre il terzo livello dell'Archivio, mentre gli aderenti diretti necessitano in alcuni casi di specifiche autorizzazioni da parte del Ministero dell'Economia).

Intanto, l'adesione al sistema e ciascuna richiesta di verifica, riferita ad un singolo nominativo, comportano da parte degli aderenti diretti il pagamento di un contributo alla Consap - previa stipula di apposita - articolato in modo tale da garantire sia le spese di progettazione e di realizzazione dell'Archivio centrale informatizzato, sia il costo pieno del servizio svolto dall'ente gestore stesso.

Per l'adesione al sistema, gli aderenti diretti sono assoggettati al pagamento pro quota, in parti uguali, di un contributo, al netto dell'IVA, di complessivi 3.919.443,80 euro (fermo restando tale importo complessivo, per gli aderenti diretti il cui valore dell'attivo dello stato patrimoniale, risultante dall'ultimo bilancio sia superiore a euro 5.000.000.000,00, l'importo del contributo può essere incrementato fino al doppio di quello stabilito). Per ciascuna richiesta di verifica, invece, il singolo aderente diretto è assoggettato al pagamento di un contributo, al netto dell'IVA, di 0,30 euro.

Per quanto riguarda i livelli di accesso alle informazioni contenute nell'Archivio, ed i relativi diritti, sono previsti i seguenti:

1. il primo livello contiene le liste nominative degli aderenti diretti, la normativa di riferimento ed ogni altro elemento di carattere divulgativo. Il contenuto del primo livello è disponibile su un apposito sito web del Ministero dell'Economia e delle finanze;

2. il secondo livello contiene l'elaborazione dei dati statistici, in forma aggregata e anonima, concernenti i casi il cui riscontro ha evidenziato la non autenticità di una o più categorie di Dati presenti nelle richieste di verifica ed è accessibile agli aderenti diretti. L'accesso al secondo livello può essere altresì consentito agli aderenti indiretti e ad altri enti interessati, previa autorizzazione del Ministero dell'Economia;

3. il terzo livello contiene l'interfaccia informatica che consente agli aderenti diretti di inviare richieste di verifica dell'autenticità dei Dati in loro possesso al fine di operare, tramite l'interconnessione di rete, il riscontro con quelli detenuti nelle banche dati degli enti e amministrazioni pubbliche. Il terzo livello e' accessibile agli aderenti diretti e indiretti;

4. il quarto livello contiene le informazioni relative alle frodi subite da parte degli aderenti diretti (le specifiche informazioni sulle frodi includono: elementi identificativi dell'aderente diretto e data della segnalazione; elementi identificativi del soggetto che ha disconosciuto l'operazione; elementi identificativi del

documento di identità e del documento che attesta il reddito utilizzati per l'operazione disconosciuta; elementi identificativi dell'operazione disconosciuta; elementi identificativi dell'esercizio commerciale dove è stata effettuata l'operazione disconosciuta) e le segnalazioni relative ai soggetti che hanno subito frodi (è previsto infatti anche un servizio gratuito, telefonico e telematico, deputato a ricevere le segnalazioni di qualsiasi soggetto che ha o teme di aver subito frodi configuranti ipotesi di furto di identità; la Consap verifica le segnalazioni e nel caso le inserisce nell'Archivio dove resteranno registrate per un tempo massimo di tre anni). Il quarto livello e' accessibile agli aderenti diretti (i quali non necessitano di autorizzazione da parte del Ministero per accedere ai dati sulle frodi subite e ai dati sulle segnalazioni inviate tramite il citato servizio telefonico e telematico);

5. il quinto livello contiene le informazioni relative al rischio di frodi (le specifiche informazioni sul mero rischio di frode includono: elementi identificativi dell'aderente diretto e data della segnalazione; elementi identificativi del soggetto che richiede di effettuare l'operazione; elementi identificativi del documento di identità e del documento che attesta il reddito presentati dal soggetto; elementi identificativi dell'operazione; elementi identificativi dell'esercizio commerciale dove e' stata presentata la richiesta di effettuare l'operazione; causale della comunicazione). Il quinto livello è accessibile solo agli aderenti diretti (i quali non necessitano di autorizzazione da parte del Ministero per accedere ai dati sulle frodi subite ma – al contrario - necessitano di tale autorizzazione per l'accesso ai dati sui rischi di frode, che il Ministero concederà solo se l'aderente diretto avrà dimostrato di volta in volta di aver comunicato, con regolarità e completezza, i dati sui rischi di frode da lui segnalati);

6. il sesto livello contiene infine le segnalazioni di specifiche allerta preventive trasmesse dallo stesso Ministero dell'Economia agli aderenti diretti, nonché i risultati di specifico interesse.

§ 2.4. Segue: le modalità di invio della richiesta di riscontro di autenticità e del riscontro anti-frode.

Le richieste di verifica dell'autenticità dei Dati sono inviate al sistema di prevenzione per via telematica, nel momento in cui il singolo aderente diretto riceve una richiesta di effettuare l'operazione. La Consap, verificata la completezza dei Dati trasmessi e delle informazioni immesse provvede alla loro convalida.

I Dati sui cui gli aderenti richiedono un riscontro preventivo di sono assoggettati a riscontro, mediante procedure telematiche compatibili, con quelli detenuti nelle banche dati dei seguenti enti e amministrazioni pubbliche Agenzia delle entrate, Ministero dell'interno, Ministero delle infrastrutture e dei trasporti; Ministero

dell'economia e delle finanze; INPS e INAIL (la Consap autorizza di volta in volta la procedura di collegamento dell'Archivio alle banche dati degli enti e amministrazioni pubbliche).