Parere del Garante su uno schema di Convenzione tra il Ministero dell'interno e il Ministero dell'economia e delle finanze riguardante l'accesso da parte delle forze di polizia, tramite il C.e.d. del Dipartimento della pubblica sicurezza, al Sistema informatizzato di prevenzione amministrativa delle frodi sulle carte di pagamento (S.i.p.a.f.) - 12 luglio 2012

Registro dei provvedimenti n. 205 del 12 luglio 2012

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della prof.ssa Licia Califano e della dott.ssa Giovanna Bianchi Clerici, componenti e del dott. Daniele De Paoli, segretario generale;

Vista la richiesta di parere del Ministero dell'interno-Dipartimento della pubblica sicurezza;

Visto il Codice in materia di protezione dei dati personali (d. lg. 30 giugno 2003, n. 196), in particolare l'art. 54;

Esaminata 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 la dott.ssa Augusta Iannini;

PREMESSO

Il Ministero dell'interno-Dipartimento della pubblica sicurezza ha chiesto il parere del Garante in ordine a uno schema di Convenzione, e all'Allegato tecnico che ne costituisce parte integrante, da stipularsi tra il Ministero dell'interno e il Ministero dell'economia e delle finanze avente a oggetto l'accesso da parte delle forze di polizia, tramite il Centro elaborazione dati (C.e.d.) del Dipartimento della pubblica sicurezza, ai dati e alle informazioni contenuti nel Sistema informatizzato di prevenzione amministrativa delle frodi sulle carte di pagamento (S.i.p.a.f.) gestito dall'Ufficio centrale antifrode dei mezzi di pagamento (U.c.a.m.p.) del Ministero dell'economia e delle finanze.

Il parere è richiesto ai sensi dell'art. 54, comma 1, del Codice nella parte in cui prevede la stipula da parte del Ministero dell'interno, previo parere conforme del Garante, di convenzioni-tipo volte ad agevolare la consultazione di pubblici registri, elenchi, schedari e banche di dati da parte di autorità di pubblica sicurezza e di forze di polizia nei casi in cui esse possono acquisire da altri soggetti informazioni, atti e documenti, in conformità a vigenti disposizioni di legge o di regolamento, anche per via telematica.

Il parere è reso tenendo conto delle informazioni e degli elementi forniti dalle due amministrazioni, che hanno fornito piena collaborazione, anche nel corso di alcuni incontri tecnici tenuti presso questa Autorità e si riferisce a una versione aggiornata dello schema di Convenzione (che reca ora quindici articoli, in luogo dei sette originari) e dell'Allegato redatti all'esito degli approfondimenti svolti nell'ambito di detti incontri, che hanno permesso di chiarire e specificare numerosi aspetti della Convenzione.

Sono stati, in primo luogo, più esattamente formulati alcuni riferimenti normativi indicati nella premessa della Convenzione, ove vengono ora citati gli artt. 2, 3 comma 1 e 7, comma 2 della legge 17 agosto 2005, n. 166 che, nell'istituire il sistema di prevenzione delle frodi sulle carte di pagamento, dispone l'accesso da parte del Dipartimento della pubblica sicurezza ai dati e alle informazioni ivi contenute.

É stato inserito all'art. 1 un completo indice delle definizioni volte a chiarire gli esatti significati dei termini citati nel testo; tra queste, le definizioni di "dati" e di "informazioni" a cui le forze di polizia possono accedere (lett. f) e g)).

Nello stesso articolo sono state introdotte le figure dei soggetti responsabili della corretta applicazione della Convenzione ("responsabili della Convenzione") e della sua gestione operativa ("referenti tecnici") per il C.e.d. e per l'U.c.a.m.p. (lett. da j) a m)); tali figure vengono specificamente individuate nell'art. 8.

In coerenza con la normativa citata nella premessa, sono stati opportunamente distinti l'oggetto della Convenzione (art. 2) e le finalità dell'accesso (art. 3), disposizioni a cui si richiama l'art. 4 nel delineare i limiti all'accesso a cui gli operatori delle forze di polizia a ciò autorizzati sono tenuti ad attenersi. A tale proposito, nell'art. 5 viene specificato, tra l'altro, che l'accesso al sistema S.i.p.a.f. è consentito esclusivamente dalle postazioni di lavoro certificate delle forze di polizia e ad operatori cui sia stato rilasciato dal C.e.d. uno specifico codice identificativo personale (comma 5).

Gli introdotti artt. 6 e 7 individuano ora puntualmente gli adempimenti posti a carico rispettivamente dell'U.c.a.m.p. e del C.e.d.; tra questi, assumono particolare rilievo gli obblighi, per l'U.c.a.m.p., di fornire al C.e.d. strumenti idonei a consentire il monitoraggio da parte del Centro delle operazioni effettuate dagli utenti (art. 6, comma 2), per il C.e.d., di sottoporre gli accessi degli operatori di polizia ai sistemi di monitoraggio degli accessi e di alert su anomalie in uso al Centro (art. 7, commi 3 e 4) e di istruire i dirigenti degli uffici (nella Convenzione denominati "supervisori locali") sull'obbligo di verifica degli alert (art. 7, comma 5). Gli utenti sono informati dell'attività di tracciamento svolta dalle due amministrazioni (art. 11), ed è previsto che il C.e.d. impartisca direttive agli incaricati del trattamento sulle responsabilità connesse all'uso illegittimo delle informazioni e dei dati raccolti (art. 9, comma 3).

In conformità ai provvedimenti del Garante concernenti l'adozione di misure di sicurezza in materia di trattamento dei dati personali presso il C.e.d. (provv. 17 novembre 2005 e 11 ottobre 2006), si è reso opportuno chiarire che il Centro verifica ogni sessanta giorni le abilitazioni degli utenti autorizzati ad accedere al sistema S.i.p.a.f. (art. 7, comma 7).

Disposizioni sull'obbligo per il C.e.d. di attuare al proprio interno alcune necessarie regole di sicurezza (registrazione e identificazione degli utenti, adozione di credenziali di autenticazione, utilizzo di meccanismi crittografici nelle procedure di autenticazione) sono state introdotte nell'art. 9, commi 4 e 5 della Convenzione.

Eventuali variazioni delle modalità, delle condizioni e dei tempi di svolgimento del servizio possono essere definite dalle parti della Convenzione previo parere favorevole del Garante (art. 13, comma 1).

OSSERVA

1. La base normativa

Il sistema di prevenzione, sul piano amministrativo, delle frodi sulle carte di pagamento è stato istituito con la legge 17 agosto 2005, n. 166, la quale prevede la costituzione presso il Ministero dell'economia e delle finanze di un apposito archivio informatizzato gestito dall'Ufficio centrale antifrode dei mezzi di pagamento, alimentato dalle società, dalle banche e dagli intermediari finanziari – denominati "società segnalanti" – che emettono carte di pagamento e gestiscono reti commerciali di accettazione delle carte (art. 1).

La legge indica rispettivamente agli artt. 2 e 3 le tipologie di "dati" e di "informazioni" che alimentano l'archivio, rinviando ad un successivo decreto del Ministero dell'economia e delle finanze la specificazione delle singole voci che devono essere comunicate (art. 7, comma 1).

L'art. 7 della legge prevede espressamente l'accesso ai dati e alle informazioni in possesso dell'Ufficio centrale antifrode da parte del Dipartimento della pubblica sicurezza del Ministero dell'interno e degli uffici competenti delle forze di polizia di cui all'art. 16, comma 1, della legge 1° aprile 1981, n. 121 – ovvero della Polizia di Stato, dell'Arma dei Carabinieri, del Corpo della Guardia di finanza, del Corpo degli Agenti di custodia (ora Corpo di Polizia penitenziaria) e del Corpo forestale dello Stato –, rinviando al successivo decreto la definizione delle modalità operative dell'accesso (comma 2).

Il Ministero dell'economia e delle finanze ha dato attuazione al disposto di legge con il d.m. 30 aprile 2007, n. 112.

In particolare, agli artt. 6 e 7 del decreto vengono rispettivamente elencati, nel dettaglio, i dati e le informazioni che le società segnalanti sono tenute a comunicare, per via telematica, all'Ufficio centrale antifrode e che alimentano l'archivio informatizzato.

Per quanto concerne l'accesso all'archivio da parte del Dipartimento della pubblica sicurezza e delle forze di polizia, l'art. 16, al comma 1 stabilisce che esso avvenga "attraverso un collegamento tra il predetto archivio e il Centro elaborazione dati del Ministero dell'interno", secondo "procedute telematiche compatibili con le caratteristiche tecniche del predetto Centro e dello stesso archivio e nel rispetto degli standard previsti dal Sistema pubblico di connettività".

3. La Convenzione

3.1. Tipologie di dati e finalità dell'accesso

La Convenzione nell'art. 2 individua specificamente le tipologie di dati e di informazioni che possono essere consultati dagli utenti del C.e.d., attraverso il riferimento all'elenco contenuto negli artt. 6 e 7 del d.m. n. 112/2007.

L'accesso alla banca dati da parte delle forze di polizia è espressamente limitato alle "finalità di prevenzione e repressione dei reati connessi o comunque collegati all'utilizzo di carte di credito o di altri mezzi di pagamento" (art. 3 della Convenzione).

Tali finalità risultano conformi a quelle espresse dal Garante nel parere reso il 19 ottobre 2006 sullo schema di decreto attuativo della legge n. 166/2005; in tale occasione l'Autorità ha rilevato che la consultazione dei dati e delle informazioni poteva essere consentito per le sole finalità di "prevenzione, accertamento e repressione di illeciti, anche penali, connessi o comunque collegati all'utilizzo di carte di credito o altri mezzi di pagamento".

3.2. Utenti abilitati all'accesso

Possono accedere alla banca dati gli operatori delle forze di polizia cui siano stati attribuiti dal C.e.d., anche in funzione dell'incarico svolto, specifici profili di abilitazione (art. 4) che vengono sottoposti a verifica ogni sessanta giorni (art. 7, comma 7), e credenziali di autenticazione personali (art. 9, comma 5). Il C.e.d. adotta procedure di registrazione che prevedono il riconoscimento diretto e l'identificazione certa dell'utente.

L'accesso è consentito esclusivamente dalle postazioni di lavoro certificate delle forze di polizia; al fine di consentire il controllo degli accessi alla banca dati, il C.e.d. rilascia agli utenti codici identificativi personali (art. 5, comma 5).

Nella Convenzione vengono specificati gli obblighi a carico degli utenti di utilizzare le informazioni acquisite per le sole finalità di cui all'art. 3, e di osservare la normativa del Codice in tema di rispetto dei principi di pertinenza nel trattamento delle informazioni e di osservanza delle necessarie misure di sicurezza (art. 9, commi 1 e 2).

É posto l'obbligo per il C.e.d. di impartire al personale abilitato direttive relative alle responsabilità connesse all'accesso improprio alla banca dati, all'uso illegittimo delle informazioni e alla loro indebita divulgazione, comunicazione e cessione a terzi (art. 9, comma 3).

Sono stati, inoltre, previsti specifici divieti a carico del C.e.d., e il correlativo obbligo di impartire direttive al riguardo agli utenti, in materia di duplicazione delle informazioni acquisite per la creazione di autonome banche dati e di utilizzo di dispositivi automatici (robot) che consentono la consultazione in forma massiva dei dati personali (art. 10).

3.3. Sicurezza nel flusso dei dati

Il d.m. n. 112/2007 stabilisce che il collegamento telematico tra il C.e.d. e l'archivio informatizzato gestito dall'U.c.a.m.p. deve avvenire "nel rispetto degli standard previsti dal Sistema pubblico di connettività" (comma 1).

Nell'Allegato tecnico, che costituisce parte integrante della Convenzione e che disciplina le "specifiche operative e tecniche del collegamento telematico e della gestione delle modalità di accesso" (art. 5, comma 2), viene quindi specificato (punto 2. Misure di sicurezza) che "per quanto concerne la sicurezza, gli utenti del CED Interforze accedono al Sipaf esclusivamente tramite VPN (Virtual Private Network) site to site su rete SPC" – ovvero Sistema pubblico di connettività – "con protocollo "IPsec/tunnel" utilizzando inoltre il protocollo SSL (Secure Sockets Layer) per garantire le funzionalità di crittografia dei dati trasferiti tra client e server".

Come previsto anche nel testo della Convenzione, nell'Allegato viene ribadito, tra l'altro, che "il C.e.d. effettua il tracciamento delle attività di sua competenza all'interno del suo dominio di applicazione", mentre "l'applicativo Sipaf effettua il tracciamento delle operazioni svolte dagli utenti del CED Interforze, storicizzando periodo di interrogazione, parametri di ricerca e risultati della ricerca".

3.4 Tracciamento degli accessi e delle operazioni effettuate

Il C.e.d. provvede al tracciamento degli accessi alla banca dati e l'U.c.a.m.p. provvede al tracciamento anche dell'accesso ai dati ivi detenuti, che consente di verificare le operazioni eseguite da ciascun utente (art. 11). Gli utenti sono informati di tali attività di tracciamento (art. 4).

3.5 Reportistica e sistemi di alert

La Convenzione prevede l'obbligo per l'Ufficio centrale antifrode di fornire al C.e.d. strumenti idonei a consentire al Centro – ad esempio, attraverso una reportistica trasmessa con periodicità non superiore al trimestre – di effettuare il monitoraggio e, conseguentemente, il controllo delle operazioni svolte dagli utenti (art. 6, comma 2).

Il C.e.d. sottopone l'accesso all'archivio informatico ai sistemi per il monitoraggio degli accessi e di alert su anomalia in uso al Centro. I risultati dell'attività di monitoraggio e di alert sono resi disponibili per trenta giorni ai supervisori locali tramite un'applicazione accessibile attraverso il portale del C.e.d.. I supervisori ricevono dal C.e.d. istruzioni per la tempestiva verifica degli alert (art. 7, commi 3, 4 e 5).

3.6 Responsabili della Convenzione e modalità di modifica della stessa

Lo schema di Convenzione individua, per ciascuna parte, le figure dei responsabili della corretta applicazione e delle attività di gestione della medesima (v. definizioni all'art. 1), giuridicamente preposti, rispettivamente, alla gestione dei rapporti e delle comunicazioni tra le parti, e all'avvio e alla gestione

operativa del servizio di accesso alla banca dati (art. 8). Lo schema indica inoltre la necessità della consultazione del Garante nell'ipotesi di modifiche o integrazioni alla Convenzione (art. 13).

4. Osservazioni

L'accesso, previsto dalla Convenzione, da parte delle forze di polizia alla banca dati gestita dall'Ufficio centrale antifrode dei mezzi di pagamento (U.c.a.m.p.) del Ministero dell'economia e delle finanze rispetta la normativa introdotta con la legge 17 agosto 2005, n. 166 e con il d.m. 30 aprile 2007, n. 112 del Ministero dell'economia e delle finanze, sia quanto alla tipologia delle informazioni consultabili, sia relativamente alle finalità perseguite.

Le disposizioni contenute nella Convenzione, sopra riportate, non presentano profili di criticità in rapporto al rispetto della disciplina in materia di protezione dei dati personali, ivi compreso il profilo della sicurezza.

TUTTO CIÒ PREMESSO IL GARANTE

esprime, ai sensi dell'art. 54 del Codice, parere favorevole sullo schema di Convenzione da stipularsi tra il Ministero dell'interno e il Ministero dell'economia e delle finanze avente a oggetto l'accesso da parte delle forze di polizia, tramite il Centro elaborazione dati (C.e.d.) del Dipartimento della pubblica sicurezza, ai dati e alle informazioni contenuti nel Sistema informatizzato di prevenzione amministrativa delle frodi sulle carte di pagamento (S.i.p.a.f.) gestito dall'Ufficio centrale antifrode dei mezzi di pagamento (U.c.a.m.p.) del Ministero dell'economia e delle finanze.

Roma, 12 luglio 2012

IL PRESIDENTE
Soro

IL RELATORE
Iannini

IL SEGRETARIO GENERALE
De Paoli