ATTUALITÀ

Cashback è lo specchietto delle allodole della privacy

di **Fondazione AIDR** · 19 dicembre 2020, 11:19

di Giuseppe Gorga, socio Aidr

L'*utilizzo degli strumenti di pagamento elettronici: il cashback*

La pandemia di Covid-19 ha dato una forte accelerazione alla digitalizzazione dei servizi di mobilità, rivoluzione che ricopre un ruolo prioritario nelle strategie industriali e nei nuovi modelli di business che vedono coinvolte le PA e le aziende. La costante crescita delle soluzioni di pagamento elettronico ha confermato il trend, già assecondato nel settore dei trasporti prima della crisi, che va verso il principio di *"mobility as a service"* Considerando il ruolo sempre più attivo degli utenti nella smart mobility, diverse aziende hanno sentito la necessità di adottare un'unica semplice infrastruttura che consenta l'accesso diretto dei cittadini a tutti i servizi di mobilità.

Tra gli esempi di portata "minore" va segnalata la piattaforma sviluppata da SIA, società controllata da CDP Equity. Lo strumento digitale comprende al suo interno una suite completa di servizi per pagare direttamente con carta o smartphone i ticket per i bus, metro e parcheggi, con la garanzia della migliore tariffa. Il servizio innovativo permette di pagare il biglietto della rete metro e ferroviaria direttamente al tornello tramite carte di credito e di debito contactless (Mastercard, VISA e American Express), anche virtualizzate su smartphone e dispositivi wearable, in modo facile, veloce e sicuro è inoltre possibile utilizzare la propria carta di credito come se fosse un abbonamento mensile: una modalità a disposizione degli utenti che, dopo aver acquistato online l'abbonamento con una carta di credito contactless, possono avvalersi della stessa carta per spostarsi sull'intera rete di trasporto pubblico cittadino.

Il fenomeno ha assunto una rilevanza notevole e pertanto, come fenomeno massivo, non poteva non cadere nelle maglie della regolamentazione privacy quale fenomeno diffuso di cashback. In merito lo schema di regolamento – al vaglio dell'autorità Garante privacy – del Ministero dell'economia e delle finanze, recante le condizioni e i criteri per l'attribuzione delle misure

premiali per l'utilizzo degli strumenti di pagamento elettronici, c.d. cashback, adottato ai sensi dell'articolo 1, commi dal 288 al 290, della legge 27 dicembre 2019, n. 160[1], disposizioni modificate e integrate dal decreto-legge 14 agosto 2020, n. 104 all'art. 73 che ha aggiunto due commi il 289-bis e il 289-ter, (Legge di Bilancio di previsione dello Stato per l'anno finanziario 2020 e bilancio pluriennale per il triennio) si innesta nella strategia, da tempo propagandata dal Governo Italiano, che vuole disincentivare l'uso del contante, nelle transazioni tra operatori economici e dei consumatori, prevedo anche un rimborso in denaro sui pagamenti effettuati mediante strumenti elettronici, la cd. "lotteria" degli scontrini contenuta in quest'ultima legge di bilancio.

Nel caso specifico il nuovo comma 289-bis, del testo normativo in esame, prevede che per l'attuazione della misura premiale il Ministero dell'economia e delle finanze dovrà utilizzare la piattaforma tecnologica per l'interconnessione e l'interoperabilità tra le pubbliche amministrazioni e i prestatori di servizi di pagamento abilitati, prevista all'articolo 5, comma 2, del decreto legislativo 7 marzo 2005, n. 82, gestita dalla società PagoPA S.p.A.. Viene precisato poi che il Ministero dovrà affidare alla società PagoPA S.p.A. i servizi di progettazione, realizzazione e gestione del sistema informativo strumentale al calcolo del rimborso. Inoltre con il comma 289-ter si prevede che il medesimo dicastero affidi a Consap – Concessionaria servizi assicurativi pubblici S.p.A. – tutti i servizi inerenti alle operazioni di erogazione del rimborso e le ulteriori attività accessorie e strumentali compresa la gestione del contenzioso.

Il regolamento del cashback

Il regolamento – che si compone di 12 articoli – che qui è esaminato, in via essenziale e puntuale, detta la disciplina delle condizioni, i casi, i criteri e le modalità attuative per l'attribuzione di un rimborso in denaro, a favore delle persone fisiche maggiorenni, residenti nel territorio dello Stato, che, fuori dall'esercizio di una attività d'impresa, arte o professione, effettuano acquisti da esercenti, con strumenti di pagamento elettronici (art. 2). Com'è evidente, dalla scelta dei soggetti, il legislatore si è preoccupato *in primis* di impedire che i minori possano partecipare a questa specie di "lotteria" e *in secundis* che vi possano partecipare i soggetti maggiorenni nell'esercizio di una attività di impresa, arte o professione.

Come è stato anticipato il Programma di rimborso, realizzato attraverso il "Sistema Cashback" è stato predisposto ed è gestito dalla società PagoPA S.p.a. nell'ambito della piattaforma tecnologica – prevista e disciplinata all'articolo 5, comma 2, del CAD – che raccoglie i dati, ai fini della partecipazione al Programma, degli "aderenti" e degli "esercenti", e che una volta definita la graduatoria trasmette le relative informazioni all'APP IO e ai sistemi messi a disposizione dai c.d.

“issuer convenzionati” e, ai fini dell’erogazione del rimborso, alla Consap-Concessionaria servizi assicurativi pubblici S.p.A..

All’articolo 3 sono indicati in maniera dettagliata quali sono le modalità di adesione al Programma di rimborso, e viene sottolineato, in particolare, la volontarietà della partecipazione al programma stessa che comporta un rilascio di dati personali che vanno da quelli molto invasivi, come il codice fiscale a quelli bancari. La norma, infatti, prevede che il soggetto “aderente” è tenuto a registrare nell’APP IO, o nei sistemi messi a disposizione da un issuer convenzionato, il proprio codice fiscale e uno o più strumenti elettronici di cui intende avvalersi per effettuare i pagamenti, dichiarando, al momento della registrazione, di utilizzare gli strumenti di pagamento registrati esclusivamente per acquisti effettuati fuori dall’esercizio di attività d’impresa, arte o professione (art. 3, commi 1, 2 e 3).

All’ articolo 4 del regolamento, infatti, si specifica in particolare le modalità tecniche di adesione al sistema da parte dei cd. “acquirer convenzionati” e, cioè, da parte dei soggetti che hanno concluso un accordo con l’”esercente” per l’accettazione di strumenti di pagamento attraverso dispositivi fisici, titolari di una convenzione con la PagoPA S.p.A. per la partecipazione al Programma, ovvero Bancomat S.p.A., sul presupposto della sottoscrizione della convenzione con la stessa PagoPA S.p.A. All’articolo 5 si prevedono apposite convenzioni tra il Ministero dell’economia e delle finanze e PagoPA S.p.A. e tra il predetto dicastero e Consap S.p.A. per il funzionamento del Programma. In particolare il comma 1 dell’articolo 5, disciplina la convenzione tra il Ministero e PagoPA S.p.A., per la progettazione, realizzazione e gestione di specifiche funzioni all’interno del Sistema Cashback, quali la raccolta dei dati relativi agli aderenti e ai pagamenti e, quindi, una quantità notevole di dati ad alto rischio per la stessa libertà e dignità dei soggetti aderenti al programma. Il comma 2, invece, disciplina la convenzione MEF-Consap S.p.A., per la gestione dei rimborsi e dei reclami, dove vi saranno ulteriori dati personali che potranno approdare anche in sede giudiziaria. La disciplina di dettaglio del cashback la troviamo all’articolo 6 dove sono anche stabilite le misura e i periodi di riferimento, mentre l’articolo 7 si prevede una fase sperimentale temporanea, valida dal 1° dicembre 2020 al 31 dicembre 2020, volta a permettere un anticipazione dell’attuazione del programma di rimborso, esclusivamente per gli aderenti che abbiano effettuato un certo numero di transazioni. All’articolo 8, invece, si istituisce un rimborso speciale per i primi centomila aderenti che abbiano totalizzato il maggior numero di transazioni con strumenti di pagamento elettronici.

Si specificano all’art. 9 le modalità di erogazione del rimborso, che avviene mediante accredito per mezzo del codice IBAN comunicato dall’aderente al momento dell’adesione al Programma, o in un

momento successivo, mentre l'articolo 10 si disciplina le modalità di gestione dei reclami. In particolare, il comma 1 prevede che PagoPA S.p.A., metta a disposizione un servizio di Help Desk dedicato all'assistenza degli aderenti per tutti gli aspetti relativi alla gestione del profilo utente e ai servizi erogati attraverso l'APP IO, incluse eventuali contestazioni in merito alla registrazione delle transazioni effettuate. Infine, l'articolo 12 – rubricato come "Trattamento dei dati personali" – disciplina alcuni importanti aspetti di protezione dati. Innanzitutto individua i ruoli, le funzioni e le responsabilità dei diversi soggetti coinvolti dal sistema, vale a dire il Ministero dell'economia e delle finanze, PagoPA S.p.A., Consap S.p.A. e gli issuer e gli acquirer convenzionati – titolarità, responsabilità e sub-responsabilità del trattamento; commi 1-5- . Si prevede, poi, che il Ministero effettui, prima del trattamento, la valutazione di impatto ai sensi dell'articolo 35 del Regolamento e la sottoponga alla verifica preventiva del Garante; si prevede che per la valutazione devono essere indicate anche le misure tecniche e organizzative predisposte e ricolte a garantire un livello di sicurezza adeguato al rischio, disciplinati i tempi e le modalità di cancellazione dal Programma (commi 6 e 7). Nel rispetto del principio delle finalità del trattamento, i dati personali raccolti potranno essere trattati esclusivamente per lo svolgimento del Programma e per la realizzazione del previsto rimborso, limitando il trattamento del dato relativo all'identificativo dell'esercente al solo fine di verificare le transazioni oggetto di reclamo (comma 8). Infine il comma 9 dell'articolo autorizza il Ministero a effettuare statistiche sull'attuazione del Programma trattando anche i dati personali degli aderenti, relativi alla partecipazione al Programma, al numero e al valore delle transazioni effettuate, nonché ai rimborsi erogati, nel rispetto delle pertinenti regole deontologiche (Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema Statistico nazionale, di cui all'allegato A al Codice, che è opportuno citare per esteso nello schema).

E' da osservare in questa sede che è di tutta evidenza che il trattamento dei dati sotteso al funzionamento del Programma presenta rischi elevati per i diritti e le libertà degli interessati derivanti dalla raccolta massiva e generalizzata di informazioni di dettaglio, potenzialmente riferibili ad ogni aspetto della vita quotidiana dell'intera popolazione, che richiedono specifiche valutazioni in ordine alla proporzionalità del trattamento e all'individuazione delle misure da adottare al fine di rispettare i requisiti del Regolamento. Sul testo, infatti, i rilievi e i suggerimenti dell'Autorità garante privacy sono stati precisi e pertinenti. Così in sintesi è da ritenersi che la base giuridica che lo autorizza dovrebbe essere proporzionata rispetto alle finalità perseguite e contenere gli altri requisiti di liceità previsti dalla normativa europea e nazionale in materia di protezione dati (art. 6, par. 3, Regolamento). Sotto tale profilo il regolamento presenta, infatti, evidenti criticità in quanto non viene precisato che il sistema informatico in questione – Sistema

Cashback – non coincide con la piattaforma tecnologica di cui all'articolo 5, comma 2, del CAD, ma opera nell'ambito della stessa. Inoltre non sono stati individuati espressamente i ruoli e le responsabilità dei diversi soggetti coinvolti dal sistema sotto il profilo della protezione dati (art. 12, commi 1-5). La normativa regolamentare dovrebbe, perciò, essere rivolta all'esigenza di circoscrivere alle finalità di realizzazione del cd. cashback i trattamenti effettuati nel rispetto del principio di limitazione della finalità, e introdurre un'ulteriore specifica garanzia in relazione al trattamento degli identificativi degli esercenti presso i quali saranno effettuate le transazioni trasmesse al Sistema Cashback (art. 12, comma 8).

Inoltre si dovrebbero introdurre misure volte a garantire che gli acquirenti trasmettano al sistema esclusivamente i dati relativi alle transazioni effettuate attraverso gli strumenti di pagamento indicati dai soggetti aderenti all'iniziativa (artt. 4, commi 1 e 2, e 5, comma 1) e ciò anche per meglio definire le modalità con cui l'APP IO, o i sistemi messi a disposizione dagli issuer, rendono disponibili agli aderenti, nel rispetto del principio di minimizzazione, gli importi dei rimborsi spettanti e la posizione nella graduatoria (art. 5, commi 1, lett. e). Occorrerà anche individuare le modalità e i tempi di conservazione dei dati e le misure necessarie a garantire che le informazioni siano trattate per il tempo strettamente necessario al conseguimento delle specifiche finalità e successivamente cancellate (artt. 4, comma 5, e 12, commi 7 e 9), nonché definire, in chiave di maggior garanzia, alcune misure di sicurezza da adottare nel trattamento dei dati, con particolare riferimento alla protezione, mediante funzioni crittografiche non reversibili, degli identificativi degli strumenti di pagamento elettronici (PAN, Primary Account Number) in uso ai soggetti che aderiscono all'iniziativa, anche in conformità allo standard PCI DSS (Payment Card Industry Data Security Standard) (art. 4, comma 1). Occorrerà, poi, anche precisare le garanzie da applicare al trattamento dei dati personali effettuato dal Ministero per scopi statistici nell'ambito del Sistema Statistico Nazionale, limitando le tipologie di dati che possono essere elaborate (art. 12, comma 9) ed effettuare una valutazione di impatto del trattamento, a fronte del rischio elevato in esso riscontrato, al fine di individuare le misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato (art. 12, commi 6 e 7).

Infine, nell'ambito della verifica sulla valutazione di impatto dovrebbe essere esaminare le caratteristiche dell'APP IO in particolare, al previsto utilizzo di notifiche push, all'attivazione automatica di servizi non espressamente richiesti dall'utente, nonché al trasferimento di dati personali verso Paesi terzi, peraltro da attualizzarsi alla luce della recente sentenza della Corte di giustizia relativa al caso Schrems II (16 luglio 2020, causa C-311/18).

3 *La sicurezza del cashback*

Per quanto attiene i profili di sicurezza del cashback occorre tenere presente che titolare del trattamento dei dati personali è il Ministero dell'Economia e delle Finanze (MEF), che si avvale di PagoPA S.p.A. e Consap S.p.A., società partecipate dallo Stato, in qualità di Responsabili del trattamento dei dati personali ai sensi dell'art. 28 del RGPD) per lo svolgimento delle attività necessarie a garantire la partecipazione degli Aderenti al Programma e la puntuale erogazione dei rimborsi in loro favore, nonché a consentire la gestione di eventuali reclami e/o del contenzioso derivante dalla partecipazione al Programma.

Si pone, quindi, un problema di sicurezza dei dati, in mano pubblica, in quanto nella specifica materia sono concessi tramite la app IO dati personali e particolari in ordine alla qualità e categoria dei beni che si acquistano oltre degli IBAN dei conti correnti bancari.

In relazione al delirio della cd "lotteria degli scontrini" un flusso enormi di dati che corrono sulla rete internet saranno costantemente esposti alla possibilità di essere intercettati atteso che la stessa procedura di registrazione avviata ha già posto tanti e tali problemi che non è difficile pronosticare un vulnus nei conti correnti con conseguenti profili di responsabilità tra MEF, Banche e gestori della rete.

E' da rilevare, poi, che anche la società PagoPA Spa a sua volta si dichiara Titolare del trattamento laddove il MEF li qualifica, invece, come responsabili al trattamento. PagoPA si dichiara titolare ma solo per l'utilizzo dei sistemi informatici e le procedure software preposte al funzionamento del sito e dei dati che si acquisiscono nel corso del loro normale esercizio di trasmissione che implicano nell'uso dei protocolli di comunicazione di Internet. Ora acquisito che i cashback è su base volontaria in quanto l'utente deve quindi attivarsi per poterlo avere ed inserire, sempre su base volontaria quali, carte, bancomat o carta di credito con IBAN attivare sul quale fare i versamenti del "premio" tutto rimesso all'azione e alla responsabilità degli utenti. E' però amaro segnalare che dopo la fallimentare app IMMUNI il cui destino è stato segnato dal pericolo alla privacy con l'app IO ossia con una operazione di cd. "cashback di stato" per gli Italiani la privacy vale solo 150 euro.

Articolo pubblicato su Istituzioni24: https://www.istituzioni24.it/2020/12/19/cashback-e-lo-specchietto-delle-allodole-della-privacy/

© 2026 Istituzioni24