ABI Associazione Bancaria Italiana

Prefettura di Milano

OSSIF

PROTOCOLLO DI INTESA PER LA PREVENZIONE DELLA CRIMINALITÀ AI DANNI DELLE BANCHE E DELLA CLIENTELA

La Prefettura, l'A.B.I. e le banche firmatarie del *Protocollo d'intesa per la prevenzione della criminalità ai danni delle banche e della clientela* (di seguito "*Protocollo*")

VISTI

- il Regolamento (CE) 27/04/2016, n. 2016/679/UE, del Parlamento Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- la legge 20 maggio 1970, n. 300, recante: "*Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento*" e, in particolare, l'art. 4 il quale prevede, tra l'altro, che gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale;
- la legge 1° aprile 1981, n. 121, recante: "*Nuovo ordinamento dell'Amministrazione della pubblica sicurezza*" e, in particolare, l'art. 13 il quale stabilisce che il Prefetto è Autorità provinciale di pubblica sicurezza, ha la responsabilità generale dell'ordine e della sicurezza pubblica nella provincia e sovraintende all'attuazione delle direttive emanate in materia;
- la legge 26 marzo 2001, n. 128, recante: "*Interventi legislativi in materia di tutela della sicurezza dei cittadini*" e, in particolare, l'art. 17, comma 1, che prevede che il Ministro dell'Interno impartisce e aggiorna annualmente le direttive per la realizzazione, a livello provinciale e nei maggiori centri urbani, di piani coordinati di controllo del territorio da attuare a cura dei competenti Uffici della Polizia di Stato e dei Comandi dell'Arma dei Carabinieri e, per i servizi pertinenti alle attività d'istituto, del Corpo della Guardia di Finanza, con la partecipazione di contingenti dei corpi o servizi di Polizia Municipale, previa richiesta al Sindaco, o

nell'ambito di specifiche intese con la predetta Autorità, prevedendo anche l'istituzione di presidi mobili di quartiere nei maggiori centri urbani, nonché il potenziamento e il coordinamento, anche mediante idonee tecnologie, dei servizi di soccorso pubblico e pronto intervento per la sicurezza dei cittadini;

- il decreto legislativo 10 agosto 2018, n. 101, recante: *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016";*
- il decreto del Ministro dell'Interno 9 gennaio 2008, recante*: "Individuazione delle infrastrutture critiche informatiche di interesse nazionale";*
- la direttiva del Ministro dell'Interno del 30 aprile 2015 in materia di *"nuove linee strategiche per il controllo coordinato del territorio";*
- la direttiva del Ministro dell'Interno del 15 agosto 2017 sui "*comparti delle Specialità e sulla razionalizzazione dei presidi di polizia";*
- lo Statuto dell'A.B.I.;
- l'Atto istitutivo dell'"OSSIF", Centro di Ricerca dell'Abi sulla "*Sicurezza Anticrimine";*
- il Decreto Legislativo 18 maggio 2018, n.51, rubricato *"Attuazione della Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016",* relativa "*alla protezione delle persone fisiche con riguardo al trattamento dei dati personale da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati";*
- il Decreto del Presidente della Repubblica 15 gennaio 2018, n.51, recante il "*Regolamento a norma dell'art.57 del Decreto Legislativo 30 giugno 2003, n.196*" relativo all'"*Individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia".*

CONSIDERATO

- che la domanda di sicurezza investe il settore bancario, esposto agli attacchi della criminalità comune e organizzata;
- che alle Forze di Polizia spetta istituzionalmente la difesa del cittadino;
- che la necessità di proteggere le dipendenze bancarie è un preciso impegno delle banche nei confronti dei dipendenti e della clientela e risponde all'esigenza di consentire l'operatività in condizioni di sicurezza;
- che l'azione della criminalità contro le dipendenze bancarie evolve grazie alle potenzialità delle nuove tecnologie, in particolare come dimostra l'emergere di attacchi con tecniche di "*cyber physical security*", cioè attacchi multi vettoriali in cui vengono usate congiuntamente tecniche di violazione fisica, informatica e di social *engineering*;

PRESO ATTO

- della proficua collaborazione tra Prefetture, Forze di Polizia, ABI e banche per contrastare la criminalità ai danni delle banche;
- dei contenuti del Protocollo d'intesa tra ABI e il Dipartimento della Pubblica Sicurezza del Ministero dell'Interno sottoscritto il 5 dicembre 2022 in materia di acquisizione, scambio e analisi dei dati attinenti ai reati predatori in danno delle banche, nonché di altri operatori e/o soggetti economici rappresentati nell'ambito dell'OSSIF, al fine di ottimizzare le misure di prevenzione e di sicurezza passiva.

CONVENGONO QUANTO SEGUE

Art.1 - Oggetto e finalità

Le *Parti* con il presente *Protocollo* intendono rafforzare la collaborazione per promuovere misure concernenti la sicurezza anticrimine nel settore bancario, la "*cyber physical*

security", la prevenzione dei reati predatori ai danni delle banche e della clientela, degli atti vandalici e terroristici, nonché delle aggressioni al personale non a scopo predatorio.

In ragione del ruolo centrale di Autorità provinciale di pubblica sicurezza, il Prefetto promuove riunioni di coordinamento delle Forze di Polizia o del Comitato Provinciale per l'Ordine e la Sicurezza Pubblica per la gestione delle problematiche inerenti alla sicurezza bancaria, anche a seguito di situazioni di particolare criticità che dovessero essere segnalate dalle Forze di Polizia e/o dalle Parti del presente *Protocollo*, ovvero dalle Organizzazioni Sindacali di categoria, individuando le esigenze prioritarie di sicurezza e le relative soluzioni, anche al fine della predisposizione dei Piani di Controllo Coordinato del Territorio nelle aree interessate ai sensi della direttiva del Ministro dell'Interno del 30 aprile 2015 in materia di *nuove linee strategiche* per il controllo coordinato del territorio.

Art. 2 - Informazioni di carattere generale

Le banche si impegnano, possibilmente entro un termine di 25 giorni dalla sottoscrizione, a inserire sul portale www.ossif.it le seguenti informazioni:

- il nome e il numero telefonico di un referente per le problematiche concernenti le singole dipendenze o, in alternativa, un recapito telefonico facente capo ad una centrale operativa della banca a cui far riferimento nelle 24 ore;
- l'elenco delle dipendenze con i relativi indirizzi e numeri telefonici;
- l'orario di apertura al pubblico antimeridiana e pomeridiana, dal lunedì al venerdì, e di apertura eventuale nelle giornate di sabato e domenica.

OSSIF, il Centro di Ricerca dell'A.B.I. sulla sicurezza anticrimine, provvederà a trasmettere le suddette informazioni alla Prefettura.

Art. 3 - Segnalazione di situazioni di rischio

Le banche si impegnano a segnalare alle Forze di Polizia ai numeri telefonici indicati nell'unito prospetto:

- carenze gravi e imprevedibili delle misure di sicurezza (es. guasto dei sistemi relativi al controllo degli accessi);
- movimenti sospetti di persone all'interno e all'esterno delle dipendenze bancarie;
- eccezionali aggravamenti del rischio (es. aumento anomalo giacenze di cassa);
- lavori da svolgere durante l'orario di apertura della dipendenza che inficino l'efficacia delle misure di sicurezza (es. sostituzione di un sistema di allarme);
- altre situazioni particolari di rischio in cui versano le dipendenze bancarie.

Art. 4 - Valutazione dei Rischi

La valutazione dei rischi che possono riguardare il personale, la clientela e i beni aziendali deve considerare eventi come le rapine, i furti ai danni delle apparecchiature ATM, le rapine ed i furti ai danni delle cassette di sicurezza, i furti ai dispositivi di custodia del contante, gli attacchi multi vettoriali *(cyber physical security)*, le truffe alla clientela, gli atti vandalici e terroristici, le aggressioni al personale non a scopo predatorio. [1]

La probabilità di accadimento degli eventi "rapina" e "furto ATM" (e la conseguente valutazione del rischio delle dipendenze) può essere quantificato solo in misura limitata, in quanto condizionata da molteplici fattori che, da un lato, esulano dallo spazio di intervento delle banche (fattori esogeni), dall'altro seguono dinamiche non prevedibili e non riconducibili a modelli previsionali definiti.

Ciò nonostante, le banche si impegnano a valutare il rischio rapina di ciascuna dipendenza e il rischio di furto alle apparecchiature ATM aggiornando periodicamente detta

[1] Per "aggressioni al personale non a scopo predatorio" si intendono azioni quali, ad esempio, minacce e atti di aggressione fisica praticati sul luogo di lavoro da soggetti esterni all'organizzazione tali da mettere a repentaglio la salute o la sicurezza del personale dipendente.

valutazione, in relazione all'evoluzione dei fenomeni criminosi e alle eventuali informazioni fornite dalle Forze di Polizia.

In questa prospettiva, le banche si impegnano altresì ad utilizzare strumenti di analisi territoriale predisposti in collaborazione con OSSIF e/o condivisi con lo stesso Osservatorio per determinare le aree a maggior rischio (es. *Geocrime Analyst*).

La probabilità di accadimento delle rapine e dei furti ai danni delle cassette di sicurezza e dei furti ai dispositivi di custodia del contante non può essere quantificata, in quanto determinata da fattori che esulano dallo spazio di intervento delle banche e dalle informazioni disponibili alle stesse.

La probabilità di accadimento degli "atti vandalici e terroristici" può essere considerata solo in misura qualitativa e non può essere riferita puntualmente alle singole dipendenze. Pertanto, la sua valutazione si basa: sull'analisi delle fonti pubbliche prodotte dalle deputate Istituzioni dello Stato, su analisi in materia realizzate da qualificate Associazioni esterne, sulla condivisione di informazioni tra le banche. Analogamente, la probabilità di accadimento delle "aggressioni al personale non a scopo predatorio" può essere considerata solo in misura qualitativa e non puntuale, in quanto si tratta di azioni soggettive non prevedibili, spesso condotte senza motivazioni apparenti.

Art. 5 - Misure di sicurezza a mitigazione delle rapine

Le banche si impegnano a comunicare le notizie sulle rapine ai danni delle proprie dipendenze inserendo nel Data-Base Anticrimine di OSSIF le relative informazioni di dettaglio nei giorni successivi al verificarsi dell'evento criminoso.

Le banche si impegnano a dotare ciascuna dipendenza - entro tre mesi dalla data di sottoscrizione - di almeno 5 misure di sicurezza, di cui obbligatoriamente la videoregistrazione e il dispositivo di custodia valori ad apertura ritardata o il dispositivo

di erogazione temporizzata del denaro[2]. Le altre 3 misure devono essere individuate tra quelle di seguito elencate:

1. bussola
2. metal detector
3. rilevatore biometrico
4. vigilanza
5. videocollegamento/videosorveglianza
6. videoregistrazione
7. sistema anticamuffamento
8. allarme antirapina
9. sistema di protezione perimetrale attiva/passiva
10. bancone blindato/area blindata ad alta sicurezza
11. dispositivo di custodia valori ad apertura ritardata
12. dispositivo di erogazione temporizzata del denaro
13. gestione centralizzata dei mezzi forti
14. sistema di macchiatura delle banconote
15. sistema di tracciabilità delle banconote
16. procedure comportamentali codificate per operare in sicurezza[3]
17. formazione e informazione anticrimine.

[2] L'impegno di adottare il dispositivo di erogazione temporizzata del denaro non si applica alle dipendenze sprovviste di casse – ad esempio dipendenze con solo macchine self service gestite da personale della banca

[3] Le procedure comportamentali si intendono adeguate ai fini del presente Protocollo se: (a) sono codificate per iscritto, (b) vengono diramate a tutte le filiali, (c) sono periodicamente aggiornate rispetto all'evoluzione dei modelli distributivi e delle soluzioni di sicurezza della banca, (d) individuano responsabilità e modalità operative almeno per i seguenti ambiti: apertura della filiale, gestione degli ingressi del pubblico, controllo dei fornitori in filiale, custodia delle chiavi della filiale, custodia delle chiavi dei mezzi forti, cautele per lavorare il contante in sicurezza, cautele per lo scambio di valori con istituti specializzati, limiti di contante detenibile nelle casse, limiti di contante detenibile negli ATM (con o senza riciclo), comportamenti da tenere in caso di rapina, cautele per la gestione di informazioni sensibili per la sicurezza, controlli sullo stato delle misure di protezione realizzabili dai dipendenti di filiale.

Con riferimento alla videoregistrazione, le banche si impegnano, per le nuove istallazioni e per l'adeguamento delle preesistenti, ad utilizzare la tecnologia digitale, che gradualmente sostituirà quella analogica.

Ferme restando le misure minime concordate, ogni banca si impegna a selezionare sia quantitativamente sia qualitativamente i sistemi di difesa più opportuni in funzione della valutazione del rischio della singola dipendenza.

In caso di recrudescenza delle rapine in specifica dipendenza – caratterizzata da almeno tre rapine nell'arco di vigenza del presente Protocollo d'intesa (2 anni) – le banche si impegnano ad adottare quale intervento di mitigazione una misura aggiuntiva a quelle minime stabilite nel presente articolo.

Sono escluse le dipendenze in cui il personale non lavora contante[4].

Art. 6 - Misure di sicurezza a mitigazione dei furti agli ATM

Le banche si impegnano a comunicare le notizie sulle rapine e sui furti subìti ai danni delle proprie apparecchiature ATM inserendo nel Data-Base Anticrimine di OSSIF le relative informazioni di dettaglio nei giorni successivi al verificarsi dell'evento criminoso.

Compatibilmente con la rischiosità delle singole installazioni, le banche si impegnano a proteggere le proprie apparecchiature ATM, dotandole, entro sei mesi dalla data di sottoscrizione, di almeno tre sistemi di sicurezza tra quelli di seguito elencati:

1. protezione con impianto di allarme locale e/o remoto connesso a sensori antiscasso/antintrusione
2. blindatura del mezzo forte

[4] Ad esempio: dipendenze dedicate solo alla consulenza; dipendenze senza casse e con macchine self service gestite da operatori esterni specializzati; punti informativi; ecc..

3. rinforzo aggiuntivo della vetrina ove è installata l'apparecchiatura ATM o dello spazio antistante con difese passive quali putrelle, archetti, dissuasori atti ad impedire l'asportazione del mezzo forte
4. sensori per la presenza di gas e/o dispositivi atti a impedire l'esplosione
5. sistemi per localizzare e/o tracciare le banconote rubate e/o dispositivi per rendere inutilizzabili le banconote rubate
6. dispositivi per localizzare/rintracciare gli ATM asportati
7. dispositivi attivi per proteggere il locale contenente il mezzo forte e/o la vetrina ove è installato il mezzo forte
8. dispositivi atti ad impedire l'introduzione di esplosivo liquido, solido o gassoso nel mezzo forte
9. misure hardware e/o software per la protezione delle componenti per l'interazione con la carta
10. collocazione del mezzo forte in area blindata ad alta sicurezza
11. dispositivi passivi per rafforzare la blindatura e l'ancoraggio del mezzo forte (c.d. *gabbie esterne*)
12. videoregistrazione
13. sistemi predittivi di analisi
14. rinforzo dei dispositivi di riferma
15. ATM disassati, cioè in cui il percorso di erogazione delle banconote non è in asse con l'interno della cassaforte, per evitare l'inserimento di oggetti dall'esterno (es. cariche esplosive, tubi con gas).

In caso di recrudescenza degli attacchi ai danni di una specifica apparecchiatura ATM caratterizzata da almeno tre attacchi nell'arco di vigenza del presente *Protocollo d'intesa* (2 anni) – le banche si impegnano ad adottare su tale apparecchiatura, quale intervento di mitigazione, una misura aggiuntiva a quelle minime stabilite nel presente articolo.

Gli ATM collocati presso terzi non rientrano nel presente Accordo in quanto si avvalgono anche dei dispositivi di sicurezza adottati dalla proprietà[5].

Art. 7 – Misure di sicurezza a mitigazione dei furti e delle rapine alle cassette di sicurezza

Le banche si impegnano a comunicare le notizie sui furti e sulle rapine ai danni delle cassette di sicurezza, contenenti beni e valori dei clienti e custodite presso le proprie Filiali, inserendo nel Data-Base Anticrimine di OSSIF le relative informazioni di dettaglio nei giorni successivi al verificarsi dell'evento criminoso.

Art. 7.1 - Misure di sicurezza a mitigazione dei furti alle cassette di sicurezza

Per furto alle cassette di sicurezza locate dalla Banca alla clientela si intende l'asportazione fraudolenta dei beni e dei valori dei clienti per effrazione delle cassette a filiale chiusa in assenza di personale e clientela.
Entro sei mesi dalla data di sottoscrizione del *presente Protocollo*, le banche si impegnano a dotare le proprie dipendenze di almeno 5 sistemi di sicurezza tra quelli di seguito elencati:

1. camere corazzate (*caveaux*)
2. mezzi corazzati compattabili
3. mezzi forti blindati
4. cassette di sicurezza antieffrazione
5. presenza di giro ronda esterno alle camere corazzate, che ne consenta l'ispezione perimetrale
6. protezione passiva dei locali (es. mura perimetrali in cemento armato, blindature metalliche, ecc.) contenenti le cassette di sicurezza

[5] Ad esempio: ATM presso caserme, comuni, ospedali, centri commerciali, ecc.

7. battente rifermato da almeno due serrature di sicurezza per la chiusura delle porte delle camere corazzate e/o dei mezzi forti blindati
8. dispositivi di blocco (c.d. *time lock*) per impedire, in determinate fasce orarie, l'apertura delle porte delle camere corazzate e/o dei mezzi forti blindati
9. combinatori elettronici
10. sistemi di *relocking*
11. collocazione dei mezzi blindati in zone non perimetrali della filiale (es. non in prossimità di vetrine o di pareti perimetrali esterne)
12. ancoraggio alla soletta dei dispositivi contenenti cassette di sicurezza (es. blocchiere nei *caveaux*) e/o loro fissaggio alle strutture murarie
13. protezione con impianto di allarme locale e/o remoto
14. servizio di *Control Room* aziendale e/o esterna – h24/g7 - per la gestione allarmi da remoto
15. servizio di Pronto (o Primo) Intervento con Istituto di Vigilanza
16. videoregistrazione
17. servizi di vigilanza fissa
18. servizi di televigilanza da remoto
19. regole e/o sistemi per l'autorizzazione e la storicizzazione dei nominativi dei soggetti (es. tecnici) che accedono ai sistemi di sicurezza, ad esempio per la loro installazione iniziale, per eventuali successivi incrementi migliorativi e/o per la loro manutenzione periodica.

Art. 7.2 - Misure di sicurezza a mitigazione delle rapine alle cassette di sicurezza

Per rapina alle cassette di sicurezza locate dalla Banca alla clientela, si intende l'asportazione fraudolenta dei beni e dei valori dei clienti per effrazione delle cassette a filiale aperta in presenza di personale e/o clientela. Entro sei mesi dalla data di sottoscrizione del *presente Protocollo*, le banche si impegnano a dotare le proprie dipendenze di almeno 5 sistemi di sicurezza tra quelli di seguito elencati:

1. camere corazzate (*caveaux*)
2. mezzi corazzati compattabili
3. mezzi forti blindati
4. cassette di sicurezza antieffrazione
5. combinatori elettronici
6. dispositivi di blocco (*c.d. time lock*) per impedire, in determinate fasce orarie, l'apertura delle porte di accesso al locale di custodia e/o dei mezzi di custodia delle cassette di sicurezza
7. sistemi di *relocking*
8. protezione con impianto di allarme locale e/o remoto
9. servizio di *Control Room* aziendale/esterna - h24/g7 - per la gestione allarmi e video da remoto
10. servizio di Pronto (o Primo) Intervento con Istituto di Vigilanza
11. videoregistrazione
12. servizi di vigilanza fissa.
13. servizi di televigilanza da remoto
14. sistemi di analisi ambientale delle aree interne ai *caveaux* (lunga permanenza, conteggio persone, ecc.)
15. dispositivi di controllo che impediscono l'apertura simultanea di più mezzi forti contenenti cassette di sicurezza
16. normative comportamentali per disciplinare, secondo logiche di sicurezza, l'apertura, l'accesso e la chiusura dei locali interessati e la custodia dei meccanismi di apertura e chiusura (chiavi, combinazioni, ecc.)
17. formazione al personale dipendente sui comportamenti e sulla gestione dei dispositivi di sicurezza e dei meccanismi di apertura.

Art. 8 - Misure di sicurezza a mitigazione dei furti a dispositivi di custodia del contante

Premesso che per dispositivi di custodia del contante si intendono i sistemi di cassa e le casseforti ove viene ricoverata la dotazione di contante delle filiali, le banche si impegnano a comunicare le notizie sui furti a tali dispositivi inserendo nel Data-Base Anticrimine di OSSIF le relative informazioni di dettaglio nei giorni successivi al verificarsi dell'evento criminoso.

Inoltre, entro sei mesi dalla data di sottoscrizione del *presente Protocollo*, le banche si impegnano a dotare le proprie dipendenze di almeno 5 sistemi di sicurezza tra quelli di seguito elencati:

1. dispositivi di custodia del contante blindati
2. protezione passiva dei locali (es. mura perimetrali in cemento armato, blindature metalliche, ecc.) contenenti i dispositivi di custodia del contante
3. battente rifermato da almeno due serrature di sicurezza per la chiusura dei dispositivi di custodia del contante
4. combinatori elettronici
5. dispositivi di blocco (*c.d. time lock*) per impedire, in determinate fasce orarie, l'apertura dei mezzi di custodia del contante
6. collocazione dei dispositivi di custodia del contante in zone non perimetrali della filiale (es. non in prossimità di vetrine o di pareti perimetrali esterne)
7. ancoraggio e fissaggio al pavimento dei dispositivi di custodia del contante con sistemi atti a garantire un'adeguata resistenza allo strappo
8. protezione con impianto di allarme locale e/o remoto
9. servizio di *Control Room* aziendale/esterna -h24/g7 - per la gestione allarmi e video da remoto
10. servizio di Pronto (o Primo) Intervento con Istituto di Vigilanza
11. dispositivi di disorientamento spaziale (es. nebbiogeni, luci stroboscopiche, sirene)
12. videoregistrazione
13. servizi di televigilanza da remoto

14. formazione al personale dipendente sui comportamenti e sulla gestione dei sistemi di sicurezza e dei meccanismi di chiusura dei dispositivi di custodia del contante
15. normative comportamentali per disciplinare, secondo logiche di sicurezza, la custodia dei meccanismi di apertura e chiusura (chiavi, combinazioni, ecc.) dispositivi di custodia del contante.

Art 9 - Prevenzione dei rischi multivettoriali *(cyber physical security)*

Le banche si impegnano a prevenire gli attacchi multi vettoriali realizzati con tecniche di "*cyber physical security*" a danno delle dipendenze bancarie, che integrano le tecniche di violazione di tipo fisico con quelle di tipo informatico e di ingegneria sociale.

In particolare, le banche si impegnano a censire gli attacchi realizzati ai danni delle dipendenze bancarie con le nuove tecniche di "*cyber physical security*".
OSSIF provvederà ad acquisire i dati presso le diverse fonti di raccolta per effettuare analisi che verranno messe a disposizione delle Forze di Polizia.

Inoltre, OSSIF si impegna ad attivare specifiche iniziative per monitorare la diffusione degli attacchi "multi vettoriali", promuovere la creazione e la condivisione di metodologie di prevenzione e mitigazione, stimolare lo sviluppo della cultura della 2*cyber physical security*".

Nella fase attuativa del presente *Protocollo* potranno essere coinvolti gli Uffici dipendenti dal Servizio Polizia Postale e delle Comunicazioni, per gli aspetti di specifica competenza[6].

---

[6] Il tema della sicurezza bancaria rientra nelle competenze istituzionali del Servizio Polizia Postale e delle Comunicazioni, per quanto concerne:
- la protezione delle infrastrutture critiche informatizzate, attraverso l'attività del CNAIPIC ed anche tramite forme di cooperazione con le amministrazioni, nonché con il mondo delle imprese pubbliche e private, stipulando apposite convenzioni per la protezione delle infrastrutture esposte "a rischio";
- la prevenzione e il contrasto dei fenomeni di criminalità informatica, legata in particolare alla violazione o all'illecito utilizzo di codici di servizi bancari *on line* e di carte di pagamento nelle transazioni elettroniche.

Art. 10 - Prevenzione delle truffe

Le banche si impegnano a contribuire alla prevenzione delle truffe ai danni della popolazione di età più avanzata, ovvero con educazione finanziaria contenuta.

Le attività di prevenzione potranno riguardare:

- consigli generali per evitare l'esposizione al rischio truffe anche suggerendo di non custodire in casa rilevanti somme di denaro;
- numeri di soccorso utili per reazione immediata;
- un attento monitoraggio delle truffe al fine di individuare le buone pratiche da condividere ed estendere nei diversi ambiti territoriali.

Art. 11 - Prevenzione degli attacchi vandalici e terroristici

Le banche si impegnano a censire le notizie relative agli atti vandalici e terroristici ai danni delle proprie dipendenze. OSSIF provvederà ad acquisire i dati presso le diverse fonti di raccolta per effettuare analisi che verranno messe a disposizione delle Forze di Polizia.

Le banche si impegnano altresì ad informare e/o formare il proprio personale sulle cautele da adottare.

Art. 12 - Prevenzione delle aggressioni al personale non a scopo predatorio

Le banche si impegnano a censire gli atti di aggressione al personale delle proprie dipendenze, non inerenti alla commissione di reati a scopo predatorio (quali le rapine).

Le banche si impegnano altresì ad informare e/o formare il proprio personale sulle cautele da adottare.

Art. 13 - Comunicazione delle misure di sicurezza

Le banche per aumentare la deterrenza delle misure di sicurezza devono adottare, ove ritenuto necessario, strumenti di comunicazione (vetrofanie o similari) che pubblicizzino alcune delle soluzioni di sicurezza presenti nelle proprie dipendenze.

Allo scopo può essere utilizzata, ad esempio, la "messaggistica di sicurezza" predisposta da OSSIF, il Centro di Ricerca dell'ABI sulla sicurezza anticrimine."

Art. 14 - Manutenzione delle misure di sicurezza

Le banche si impegnano ad attuare, almeno su base annua e per tutti i dispositivi di sicurezza che lo richiedano, le attività di verifica e/o manutenzione preventiva atte a consentirne il miglior funzionamento. Le banche si impegnano altresì ad assicurare in tempi brevi il ripristino di impianti di sicurezza che hanno subito guasti.

Art. 15 - Mappatura unica nazionale dei sistemi di videosorveglianza e dei sistemi di sicurezza

Le banche si impegnano a segnalare nel Data-Base Anticrimine di OSSIF tutti gli apparati di videosorveglianza presenti su pubblica via e tutte le misure di sicurezza adottate presso le proprie dipendenze in conformità ai precedenti articoli 5 e 6.

Ciò al fine di costituire una mappatura unica nazionale dei sistemi di videosorveglianza e delle misure di sicurezza presenti nelle agenzie delle Banche, con cui soddisfare eventuali richieste delle Prefetture e delle Forze di Polizia in merito al censimento, alla mappatura e alla georeferenziazione di tutti gli apparati di sicurezza installati in luoghi pubblici o aperti al pubblico, ad opera di Enti pubblici o privati.

In questo modo le Forze di Polizia saranno in grado di conoscere la presenza e la disponibilità di fonti multimediali in una determinata area di interesse con evidenti benefici nell'azione di prevenzione e investigativa.

Tutto ciò anche nell'ambito dell'attuazione delle *linee-guida* diramate dal Ministero dell'Interno il 30 aprile 2015.

Art. 16 - Prevenzione dei rischi di infiltrazioni criminali nell'economia legale

Il presente *Protocollo* ha, altresì, lo scopo di finalizzare la collaborazione tra le parti allo scambio di conoscenze, valutazioni ed approfondimenti, in chiave di analisi e di prevenzione del rischio di infiltrazione nell'economia legale da parte della criminalità organizzata, fermo restando il rispetto delle prerogative degli attori istituzionali richiamati dal Decreto Legislativo n. 231 del 2007.

Art. 17 - Adesione ad OSSIF

Le banche si impegnano, attraverso l'adesione ad OSSIF, a condividere le migliori prassi di sicurezza, allo scopo di elaborare linee-guida per la prevenzione dei rischi che rientrano nel perimetro del presente *Protocollo*.

Art. 18 - Esigenze di *privacy*

Le banche si impegnano a dare piena e completa applicazione alle previsioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

Per quanto riguarda i sistemi di videoregistrazione, i trattamenti di dati personali dovranno essere effettuati altresì rispettando le misure e gli accorgimenti prescritti dal Garante per la protezione dei dati personali ("*Provvedimento in materia di videosorveglianza – 8 aprile 2010*").

Dovrà essere, altresì, assicurata l'osservanza delle prescrizioni emanate dal Garante, nel Provvedimento n. 513 del 12 novembre 2014, in caso di ricorso al dispositivo del rilevatore biometrico.

Dovrà essere, inoltre, assicurato il rispetto delle disposizioni contenute nel decreto legislativo 10 agosto 2018, n. 101, recante *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)"*.

L'utilizzo dei sistemi di videoregistrazione, inoltre, dovrà tener conto delle indicazioni contenute nella circolare del Ministero dell'Interno n.558/1/421.2/70/456 datata 8 febbraio 2005.

Le banche, nell'adempiere alla normativa generale vigente in materia di protezione dei dati personali, confermano altresì che le apparecchiature che consentono la registrazione visiva degli ambienti, destinati al pubblico e allo svolgimento del lavoro, sono state istallate e continueranno ad essere adottate e utilizzate nel rispetto di quanto previsto dall'art. 4 della Legge 20 maggio 1970 n. 300.

Art. 19 - Ruolo delle Forze di Polizia

Le Forze di Polizia si impegnano nei confronti delle banche a:

- segnalare, anche per il tramite di OSSIF, eventuali informazioni utili per le attività di prevenzione, sempre nel pieno rispetto dei vincoli in materia di segreto di ufficio/di indagine;
- intervenire, su richiesta delle banche e a fronte di reali stati di necessità, a specifici incontri con le banche stesse per fornire informazioni in materia di sicurezza anticrimine;

- partecipare a *workshop* organizzati da OSSIF per promuovere presso le banche la cultura della sicurezza anticrimine, della *cyber physical security,* della prevenzione delle truffe alla clientela - che deve avere come obiettivo primario gli illeciti commessi ai danni della popolazione di età avanzata ovvero con educazione finanziaria contenuta, in coerenza con quanto già previsto al precedente art.10, rubricato "Prevenzione delle truffe" -, degli atti vandalici e terroristici, nonché delle aggressioni al personale non a scopo predatorio;
- condividere *linee-guida* per la prevenzione e il contrasto della criminalità ai danni delle banche e della clientela.

Art. 20 - Ruolo dell'ABI

L'A.B.I. si impegna a trasmettere alle Forze di Polizia - su richiesta della Prefettura - attraverso OSSIF, una relazione annuale sull'andamento degli eventi nella provincia ai fini delle valutazioni sullo specifico ambito.

Art. 21 – Durata

Il *Protocollo* che le *parti* sottoscrivono, ciascuna per quanto di competenza, in relazione agli impegni espressamente indicati, avrà la durata di 24 (ventiquattro) mesi a decorrere dalla data odierna e sarà tacitamente rinnovato a scadenza salvo diverse intese tra le parti.

Milano, 7 novembre 2024

PREFETTURA DI MILANO
Prefetto dott. Claudio Sgaraglia

ASSOCIAZIONE BANCARIA ITALIANA
dott. Marco Iaconis

ABI Associazione Bancaria Italiana

Prefettura di Milano

OSSIF

Allegato 1

REFERENTI FORZE DI POLIZIA

A cura della Prefettura

POLIZIA DI STATO
Commissario Capo, Dott. Michele Scarola
0262265506
michele.scarola@poliziadistato.it

Vice Questore Aggiunto, Dott.ssa Annalisa Stefani
0262265550
annalisa.stefani@poliziadistato.it

Primo Dirigente, Dott.ssa Manuela De Giorgi
0243333003
manuela.degiorgi@poliziadistato.it

Vice Questore, Dott. Rocco Nardulli
0243333034
rocco.nardulli@poliziadistato.it

CARABINIERI
Comandante del Reparto Operativo di Milano, Col. Antonio Coppola

GUARDIA DI FINANZA
Capo Ufficio Operazioni, Ten. Col. Claudia Meloni
028283/2820

Capo Sala Operativa, Ten. Claudio Formica
028283/2825

ABI Associazione Bancaria Italiana

Prefettura di Milano

OSSIF

Allegato 2

BANCHE ADERENTI

ALLIANZ BANK

BANCA CENTROPADANA

BANCA DEL FUCINO

BANCA DEL PIEMONTE

BANCA DI ASTI

BANCA GENERALI

BANCA MONTE DEI PASCHI DI SIENA

BANCA NAZIONALE DEL LAVORO

BANCA PASSADORE

BANCA POPOLARE DI PUGLIA E BASILICATA

BANCA POPOLARE DI SONDRIO

BANCA POPOLARE ETICA

BANCA SELLA

BANCA VALSABBINA

BANCO DI SARDEGNA

BANCO BPM

BAPR – BANCA AGRICOLA POPOLARE DI RAGUSA

BCC DI BARLASSINA

BCC DI CARATE BRIANZA

BCC DI LODI

BCC DI TREVIGLIO

BDM BANCA

BPER BANCA

ABI Associazione Bancaria Italiana

Prefettura di Milano

OSSIF

COMPASS BANCA

CREDIT AGRICOLE

CREDITO EMILIANO

DEUTSCHE BANK

FIDEURAM

INTESA SAN PAOLO

LA CASSA DI RAVENNA

MEDIOBANCA PREMIER

UNICREDIT