

ACCORDO EX ART. 4 LEGGE N. 300 DEL 1970

Il giorno 22 ottobre 2020

Tra

ING Bank N.V. – Milan Branch rappresentata da Silvia Cassano, Andrea Chiesa e Alice Marini (di seguito anche “la Banca o IBI”)

E

Le Organizzazioni Sindacali rappresentate dalle rispettive RSA (di seguito anche “le OOSS”)

- RSA FABI rappresentata da Claudio Casazza, Federica Fontana e Simona Marrone
- RSA FIRST CISL rappresentata da Matilde D’Alessandro, Davide Bossoletti e Marcello Infurna
- RSA FISAC CGIL rappresentata da Anna Andreutti, Luca Centrone e Sami Zambon
- RSA UILCA rappresentata da Antonio Talamo
- RSA UNISIN rappresentata da Nicola Cerruti, Michele Del Giudice e Paolo Siagonidis

(di seguito congiuntamente definite le “Parti”)

Premesso che

- la Banca ha la necessità di porre in essere verifiche inerenti le comunicazioni elettroniche che intervengono sugli strumenti messi a disposizione dei dipendenti per lo svolgimento della prestazione lavorativa. Tale necessità è volta a tutelare il patrimonio della Banca ed in particolare le informazioni riservate della stessa e dei propri clienti, nonché a prevenire la commissione di illeciti da parte di dipendenti e quindi ad evitare l'applicazione di sanzioni da parte delle Autorità di Vigilanza previste dalla normativa di settore;
- in particolare, il Regolamento (UE) n. 596/2014 prescrive agli operatori del mercato e alle imprese di investimento che gestiscono una sede di negoziazione di istituire e mantenere dispositivi, sistemi e procedure efficaci al fine di prevenire e individuare abusi di informazioni privilegiate, manipolazioni del mercato e tentativi di abuso di informazioni privilegiate e manipolazioni del mercato;
- i dipendenti della Banca operanti all’interno dei dipartimenti di Financial Markets (incluso Debt Capital Market) e Bank Treasury (i “Dipendenti”) possono venire a conoscenza, in ragione del proprio ambito operativo, di informazioni privilegiate rispetto alle quali trova applicazione la normativa di settore sopra richiamata;
- per le medesime ragioni sopra riportate, la Banca si trova altresì nella necessità che le conversazioni telefoniche effettuate/ricevute attraverso i dispositivi aziendali dai Dipendenti che operano nel Financial Markets, già oggetto di registrazione in conformità all’accordo sindacale del 26 giugno 2015 e s.m.i., vengano trascritte su supporto digitale;
- le verifiche inerenti le comunicazioni elettroniche e le trascrizioni delle conversazioni telefoniche che, come sopra esposto, la Banca ha la necessità di porre in essere possono essere effettuate tramite l’utilizzo di appositi sistemi ed applicativi informatici, mutevoli nel tempo principalmente in ragione dell’evolversi della tecnologia, che ricercano automaticamente alcune parole chiave predefinite e preimpostate all’interno dei canali di comunicazione selezionati;

- i canali di comunicazione disponibili tramite gli applicativi “Bloomberg” e “Reuters”, le e-mail aziendali e le telefonate effettuate attraverso dispositivi messi a disposizione dalla Banca (congiuntamente i “Canali di Comunicazione”) sono strumenti di lavoro utilizzati dai Dipendenti per lo svolgimento della propria prestazione lavorativa;
- il trattamento dei dati personali avverrà in conformità alle vigenti disposizioni in materia di protezione dei dati personali.

Tutto ciò premesso, le parti convengono quanto segue:

- 1) le premesse formano parte integrante del presente accordo.
- 2) Presso la Banca viene implementato un sistema identificato come “**Communication Surveillance**”, avente ad oggetto le comunicazioni elettroniche in entrata e in uscita inviate e ricevute dai Dipendenti per il tramite delle piattaforme Bloomberg e Reuters e – per quanto riguarda i dipendenti che operano nel Financial Markets – avente ad oggetto anche le comunicazioni di posta elettronica inviate e ricevute attraverso gli account aziendali.
- 3) Il c.d. sistema di “Communication Surveillance” è finalizzato ad individuare l’utilizzo di parole chiave, previamente identificate e periodicamente aggiornate, il cui utilizzo determini l’insorgere di un sospetto di “incident” o di una violazione regolatoria. Tale sistema si compone di una serie di applicativi che operano appunto attraverso un insieme di parole chiave, al cui utilizzo si innescano degli alert. In particolare, a tal fine:
 - a) con riferimento alla piattaforma Reuters viene utilizzato l’applicativo denominato “Global Relay”;
 - b) per la piattaforma Bloomberg viene utilizzato l’applicativo denominato “Bloomberg Vault”;
 - c) in relazione alle e-mail inviate/ricevute tramite gli indirizzi di posta elettronica aziendali vengono utilizzati i sistemi denominati “Intelligent Voice” e “Relativity”. Intelligent Voice ingloba i dati e li trasferisce all’interno di Relativity, che è lo strumento che permette di ricercare in modo automatico le e-mail sulla base di parole chiave;
- 4) Le conversazioni telefoniche effettuate/ricevute attraverso i dispositivi aziendali (con esclusione dei telefoni cellulari aziendali) dai dipendenti che operano nel Financial Markets, già oggetto di registrazione, vengono trascritte su supporto digitale attraverso i sistemi denominati “Intelligent Voice” and “Relativity”; tali trascrizioni potranno in seguito essere consultate qualora tramite Relativity, che è lo strumento che consente di ricercare nell’ambito dei dati trascritti le parole chiave selezionate, venga individuato l’utilizzo di una o più parole chiave e si inneschi quindi un alert.
- 5) Le informazioni raccolte dal sistema di “Communication Surveillance” vengono registrate su supporto digitale e conservate all’interno del server aziendale ubicato in Olanda. Tale conservazione viene mantenuta per i 5 anni successivi alla raccolta, fatte salve speciali esigenze di ulteriore conservazione in relazione al caso in cui si dovrà aderire ad una specifica richiesta investigativa dell’autorità giudiziaria o di polizia giudiziaria o per esigenze di esercizio del diritto di difesa in giudizio o su richiesta delle Autorità di Vigilanza. Decorso tale periodo i dati raccolti verranno cancellati.
- 6) Le informazioni raccolte dal sistema di “Communication Surveillance” sono accessibili al personale autorizzato, facente parte del team “Compliance” della Banca, il quale vi accede attraverso profili di accesso specifici e personali. Le predette informazioni sono accessibili anche al personale autorizzato della succursale ING Business Shared Services B.V. sita in Manila (“IBSS Manila”) e della capogruppo ING Bank N.V. (“ING HQ”), in forza delle c.d. “Binding Corporate Rules” al fine di consentire il trasferimento di dati personali all’interno del Gruppo ING, anche al di fuori dei Paesi appartenenti all’Unione Europea.

7) In particolare, qualora si inneschi un alert e, quindi in caso di sospetto di un "incident" o di una violazione regolatoria, il team IBSS Manila accede alle informazioni raccolte, al fine di effettuare una prima valutazione. Qualora si rendesse necessario una valutazione più approfondita, in seconda battuta il team a ciò dedicato istituito all'interno di ING HQ accede alle informazioni raccolte e, laddove fosse ulteriormente necessario un approfondimento specifico, alle informazioni raccolte accede il personale autorizzato facente parte del team "Compliance" della Banca, per una valutazione finale.

8) I dati registrati dal sistema di cui al presente accordo non verranno utilizzati per l'adozione di provvedimenti disciplinari, a meno che dagli accertamenti non emergano comportamenti dolosi o gravemente colposi o attuati in violazione di specifiche normative regolamentari, contrattuali e/o di legge. In particolare, la colpa grave dovrà comportare un danno oggettivo e non potenziale per la Banca.

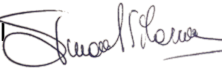


9) Le Parti convengono altresì che ove si verificasse la necessità di apportare significative modifiche e/o integrazioni ai suddetti sistemi, la Banca ne darà preventiva comunicazione alle OO.SS. Le Parti valuteranno congiuntamente l'eventuale necessità di modificare o integrare l'accordo stesso.




10) La Banca si impegna ad informare i lavoratori in ordine ai predetti sistemi, anche attraverso la consegna a mezzo email di specifica informativa redatta in conformità alla vigente normativa (in allegato il format dell'informativa individuale).




11) Le Parti si danno atto che, con la sottoscrizione del presente accordo, è stata validamente esperita e completata la procedura di cui all'art. 4, comma 1, L. n. 300/70, con esito positivo.


Letto, firmato e sottoscritto

Milano, 22 ottobre 2020

FABI    ING Bank NV - Succursale di Milano

FIRST CISL   

FISAC CGIL   

UILCA 

UNISIN 