Privacy by Design

I 7 principi fondazionali

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

La *Privacy by Design* è un concetto che ho sviluppato negli anni '90, per far fronte agli effetti sempre crescenti e sistematici delle Tecnologie dell'Informazione e della Comunicazione, e dei sistemi di dati delle reti su larga scala.

La *Privacy by Desig*n anticipa la visione che il future della privacy non può essere assicurato unicamente dal processo di conformità con il sistema normativo; piuttosto, la garanzia della privacy deve costituire idealmente un modo di operare di default di un'organizzazione.

Inizialmente, l'attuazione delle tecnologie per rafforzare la privacy (Privacy-Enhancing Technologies - PETs) era vista come la soluzione. Oggi, realizziamo che è richiesto un approccio più sostanziale – che estende l'uso delle PET alle PETS Plus – con un approccio di valore aggiunto (di massima funzionalità), e non di valore zero. Questo è il Plus nelle PET Plus: valore aggiunto, non se/o di valore zero (una falsa dicotomia).

La *Privacy by Design* comprende a una "Trilogia" di applicazioni: 1) sistemi IT; 2) pratiche commerciali corrette; e 3) progettazione strutturale e infrastrutture di rete.

I principi della *Privacy by Design* possono essere applicati a tutti i tipi di informazioni personali, ma devono essere applicati con particolare vigore ai dati sensibili come le informazioni mediche e finanziarie. La forza degli interventi della privacy tende ad essere proporzionata alla sensibilità dei dati.

Gli obiettivi della *Privacy by Design* – assicurando la privacy e garantendo il controllo sulle proprie informazioni personali, e per le organizzazioni, ottenendo un vantaggio competitivo sostenibile - possono essere attuate osservando i seguenti 7 principi fondazionali (vedi la pagina seguente):

I 7 principi fondazionali

1. ***Proattivo*** non reattivo; ***prevenire non correggere***

L'approccio alla Privacy by Design (PbD) è caratterizzato da interventi di tipo proattivo piuttosto che reattivo. Esso anticipa e previene gli eventi invasivi della privacy prima che essi accadano. La PbD non attende che i rischi della privacy si concretizzano, né offre rimedi per risolvere le violazioni della privacy una volta occorse – ha lo scopo di prevenirli dal verificarsi. In breve, la Privacy by Design viene prima del fatto e non dopo.

2. Privacy come impostazione di default

Possiamo tutti essere certi di una cosa - la regola di base ! La Privacy by Design cerca di realizzare il massimo livello di privacy assicurando che i dati personali sono automaticamente protetti in un qualunque sistema IT o di pratica commerciale. Se un individuo non fa nulla, la sua privacy rimane ancora intatta. Non è richiesta alcuna azione da parte dell'individuo per proteggere la propria privacy - è incorporata nel sistema per default.

3. Privacy ***incorporata nella progettazione***

La PbD è incorporata nella progettazione e nell'architettura dei sistemi IT e delle pratiche commerciali. Non è agganciata come un'aggiunta, dopo il fatto. Il risultato è che la privacy diventa un componente essenziale per la realizzazione del nucleo funzionale. La privacy è integrata nel sistema, senza diminuirne la funzionalità.

4. Massima funzionalità – ***Valore positivo, non valore zero***

La Privacy by Design mira a conciliare tutti gli interessi legittimi e gli obiettivi con modalità di valore positivo "vantaggioso per tutti", non attraverso un approccio datato di valore zero, dove sono inutili i compromessi. La Privacy by Design evita la pretesa di false dicotomie, come la privacy contro la sicurezza, dimostrando che è possibile avere entrambi.

5. Sicurezza fino alla fine – ***Piena protezione del ciclo vitale***

La Privacy by Design essendo stata incorporata nel sistema prioritariamente rispetto alla acquisizione del primo elemento di informazione, si estende in modo sicuro attraverso l'intero ciclo vitale dei dati - solidi interventi di sicurezza sono essenziali per la privacy, dall'inizio alla fine. Questo assicura che tutti i dati sono conservati con cura, e poi distrutti in modo sicuro alla fine del processo, in maniera opportuna. Pertanto, la Privacy by Design assicura dalla culla alla tomba, un'intera e sicura gestione delle informazioni, fino alla fine.

6. ***Visibilità*** e ***trasparenza*** – Mantenere la trasparenza

La Privacy by Design cerca di assicurare che tutti i soggetti interessati, qualunque sia la prassi aziendale o tecnologia utilizzata, è di fatto, operativa secondo promesse ed obiettivi stabiliti, soggetti a verifica indipendente. I suoi componenti e operazioni restano visibili e trasparenti sia agli utenti sia ai fornitori. Si ricorda di fidarsi ma di verificare.

7. ***Rispetto per la privacy dell'utente*** – Centralità dell'utente

Al di là di tutto, la Privacy by Design richiede ai progettisti e agli operatori di considerare prioritari gli interessi degli individui offrendo efficaci interventi di default della privacy, informazioni appropriate e potenziando opzioni di facile utilizzo per l'utente. Si raccomanda la centralità dell'utente.

Published: February 2011
Translation provided by: Nicola Fabiano, PbD Ambassador

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario • CANADA • M4W 1A8

Telephone: 416-326-3333 • 1-800-387-0073
Web: www.ipc.on.ca • www.privacybydesign.ca
E-mail: info@ipc.on.ca