

Digitalizzazione

Una politica dei dati basata sulla fiducia, ***per il progresso e l'innovazione***

12 marzo 2018

A colpo d'occhio

Nell'era digitale la Svizzera deve preservare i punti di forza che hanno contribuito alla sua prosperità. Questo vale in particolare per l'utilizzo dei dati. È necessario un mix di spirito di innovazione e di fiducia tra economia e società affinché la Svizzera possa continuare a far parte dei vincitori della trasformazione digitale dell'economia. Per questo, una politica dei dati basata sulla fiducia è essenziale. Gli ambienti economici intendono svolgere attivamente il loro ruolo.



Ivette Djonova

Projektleiterin Wettbewerb & Regulatorisches



Erich Herzog

Responsabile del Dipartimento concorrenza e regolamentazione, General Counsel, membro della direzione allargata

L'essenziale in breve

L'utilizzo innovativo di dati cela un potenziale inaspettato, consente di accedere a nuovi ambiti di applicazione e promuove la creazione di nuovi modelli commerciali. Al contempo i cambiamenti legati alla trasformazione digitale sono però anche fonte di timori. Cosa accade con i dati negli abissi delle reti globali? Come è possibile garantire che i dati non finiscano nelle mani sbagliate? Come è possibile garantire la sicurezza nei sistemi interconnessi e migliorarla costantemente? A queste domande ne seguono altre: come deve reagire la politica a questi sviluppi? Quali sono i compiti del singolo, dell'economia e dello Stato? economiesuisse risponde a queste domande proponendo la sua politica dei dati. Quest'ultima è stata sviluppata con dei rappresentanti di tutti i rami, nonché di aziende grandi e piccole. La politica dei dati permette - andando ben oltre alle mere questioni relative alla protezione dei dati – di discutere le questioni aperte e di presentare i diversi interessi in gioco, trovando un equilibrio tra innovazione e concorrenzialità della Svizzera. Nella gestione dei dati conquistare la fiducia del singolo è un compito di centrale importanza.

Posizione **di economiesuisse**

- Nessuna regolamentazione statale preventiva nella politica dei dati:** in un contesto tecnologico dinamico regole precipitose e incisive rischiano di ostacolare la creazione di valore e i futuri sviluppi.
- Equilibrio sostenibile tra protezione dei dati e innovazione:** i dati sono il motore di modelli commerciali innovativi. Le innovazioni devono essere in giusto equilibrio con la protezione dei dati del singolo.
- Accettare e riconoscere le soluzioni di autoregolamentazione:** l'autoregolamentazione permette di affrontare meglio molte sfide in materia di dati rispetto a una rigida regolamentazione statale. In caso contrario, lo Stato dispone di mezzi sufficienti per responsabilizzare le aziende.
- Adottare degli standard economici come raccomandazioni:** in molti settori è possibile ottenere una sicurezza giuridica con raccomandazioni dell'economia che stabiliscono uno standard generalmente valido per la gestione dei dati.

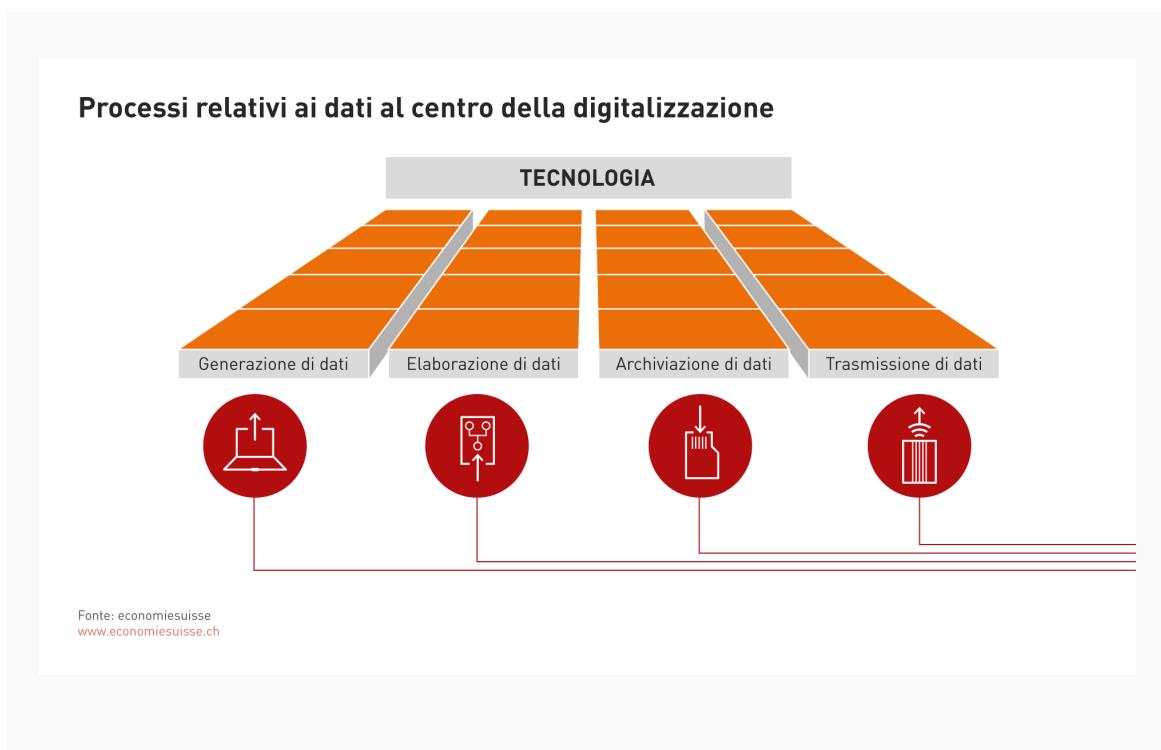
- **Preservare la libertà d'agire in tutta responsabilità dei privati:** nella gestione dei dati un'intrusione dello Stato non contribuisce a raggiungere gli obiettivi. Nei limiti delle condizioni quadro tecnologiche, i privati devono avere la possibilità di decidere essi stessi in merito ai propri dati.
- **Utilizzo di strumenti tecnici per garantire la fiducia:** nuove tecnologie e strategie devono essere impiegate in modo sistematico. Questo garantisce una gestione dei dati in grado di rafforzare la fiducia e di promuovere al contempo la responsabilità personale.
- **Utilizzare degli strumenti legislativi esistenti:** è possibile rispondere a quasi tutte le questioni giuridiche con gli strumenti esistenti. Si pensi ad esempio alla legge federale contro la concorrenza sleale (LCSI), alla legge sul diritto d'autore (LDA), ad altri diritti della proprietà intellettuale e alla legge sui cartelli (LCart).



Digitalizzazione **e dati**

La digitalizzazione è la base sulla quale l'economia, la scienza e la società si sviluppano. La pubblicazione di economiesuisse «Economia digitale» indica cosa deve fare la Svizzera per essere tra i vincitori di queste trasformazioni tecnologiche e restare nel plotone di testa. Al centro della digitalizzazione vi è la possibilità di generare, elaborare, archiviare e trasmettere dati. I dati sono il vero e proprio motore innovativo per la società. Tutti i modelli commerciali digitali si basano sull'utilizzo dei dati, ciò che viene illustrato in dettaglio nei seguenti esempi.

Grafico 1



Semplificazione della mobilità Già oggi è possibile riunire in una stessa applicazione vari mezzi di trasporto, come i taxi, i trasporti pubblici, i veicoli a noleggio. L'applicazione calcola l'itinerario più diretto. Essa può anche integrare altri parametri individuali e permettere la fornitura di acquisti o ordini di ristoranti nel proprio luogo di residenza. **Diagnosi precoce delle malattie** Se una foto ritratta con il flash mostra una macchia bianca, e non rossa, nell'occhio di un bambino, può trattarsi di un tumore. L'applicazione "White eye detector" esamina le foto presenti sul telefono mobile alla ricerca di segnali d'allarme per il cancro degli occhi. Gli occhi ritenuti anomali sono immediatamente identificati e segnalati dall'applicazione. Quest'ultima può procedere ad un rapido test di scoperta del cancro dell'occhio con l'apparecchio fotografico del telefono mobile. Nel contempo, alcuni algoritmi utilizzati da Google permettono di scoprire delle malattie oculari a partire dalle foto degli occhi. Recentemente è stata sviluppata un'applicazione in grado di rilevare la pressione sanguigna elevata e il rischio di infarto. Queste soluzioni sono più vantaggiose, più rapide e meno invasive dei metodi convenzionali. **Sostegno ai pazienti nel settore medico e sviluppo di nuove terapie** Grazie a dei sensori e a un'applicazione, gli strumenti di cura (come un inalatore) potranno ben presto fornire dati e valori al medico curante. Ciò permetterà di migliorare la sua valutazione. Il medico e il paziente riceveranno direttamente delle informazioni sul tipo di terapia, gli effetti secondari, le infezioni e, se necessario, si potrà intervenire immediatamente. Questa raccolta

di dati su grande scala permette di sviluppare nuove conoscenze e contribuisce a migliorare le terapie per pazienti. **Scoperta di pianeti e galassie** Nel 2017, la NASA (National Aeronautics and Space Administration) ha scoperto, con l'aiuto di Google, un nuovo sistema solare, simile al nostro, che conta otto pianeti. Con i suoi motori di ricerca, il gruppo ha analizzato dei dati dal telescopio Kepler. Ciò ha permesso di analizzare molto rapidamente un volume di dati molto più importante di ciò che era possibile fare manualmente. In quattro anni, il telescopio Kepler ha osservato 200'000 stelle e scattato una foto ogni 30 minuti. Ha così raccolto bilioni di dati. Degli astronomi avrebbero impiegato molto più tempo per effettuare questo lavoro.

dati sui dati

Nel 2016 il volume di dati prodotto attraverso il mondo ha raggiunto 16,1 zettabyt. Sotto forma di testi scritti a computer, questo rappresenterebbe 230'000 bilioni di pagine A4, ossia una pila che rappresenterebbe 82 volte la distanza tra il sole e Nettuno. Una luce posta sull'ultimo foglio impiegherebbe 14 giorni e 8 ore per riuscire a illuminare il primo, sulla terra (cf. economiesuisse/W.I.R.E., Il futuro della Svizzera digitale, p. 15)..



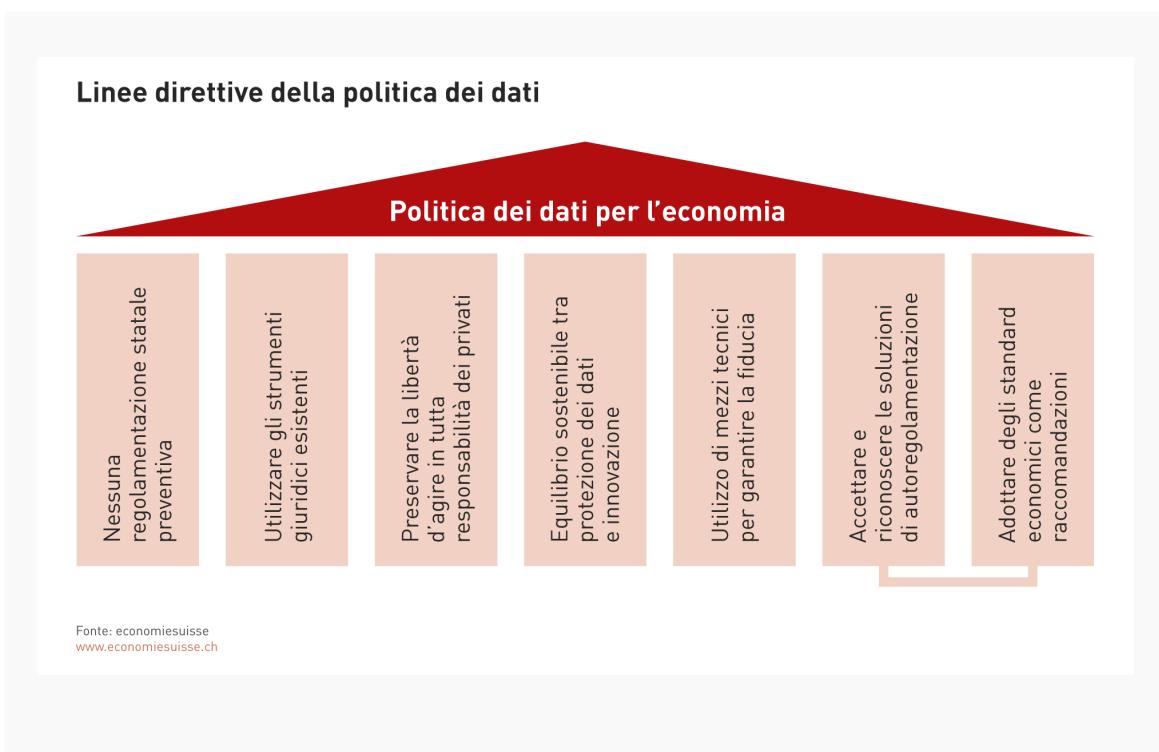
Politica in materia ***di dati dell'economia***

Una delle sfide delle aziende è conquistare la fiducia delle singole persone nell'utilizzo dei dati. Senza fiducia non è possibile un'economia dei dati a lungo termine. Il singolo mette a disposizione i suoi dati se sa che è garantita una gestione adeguata. Trasparenza nel rilevamento e nell'utilizzo dei dati permette a ognuno di decidere quali offerte sfruttare e quali no.

Pilastri fondamentali della politica dei dati

Con i suoi parametri l'economia definisce i pilastri fondamentali di una politica dei dati. Ne risultano richieste e campi d'azione che vengono approfonditi nel presente dossier. Si tratta di mostrare, in maniera costruttiva, come gestire i dati, trovando un equilibrio tra interessi diversi.

Grafico 2



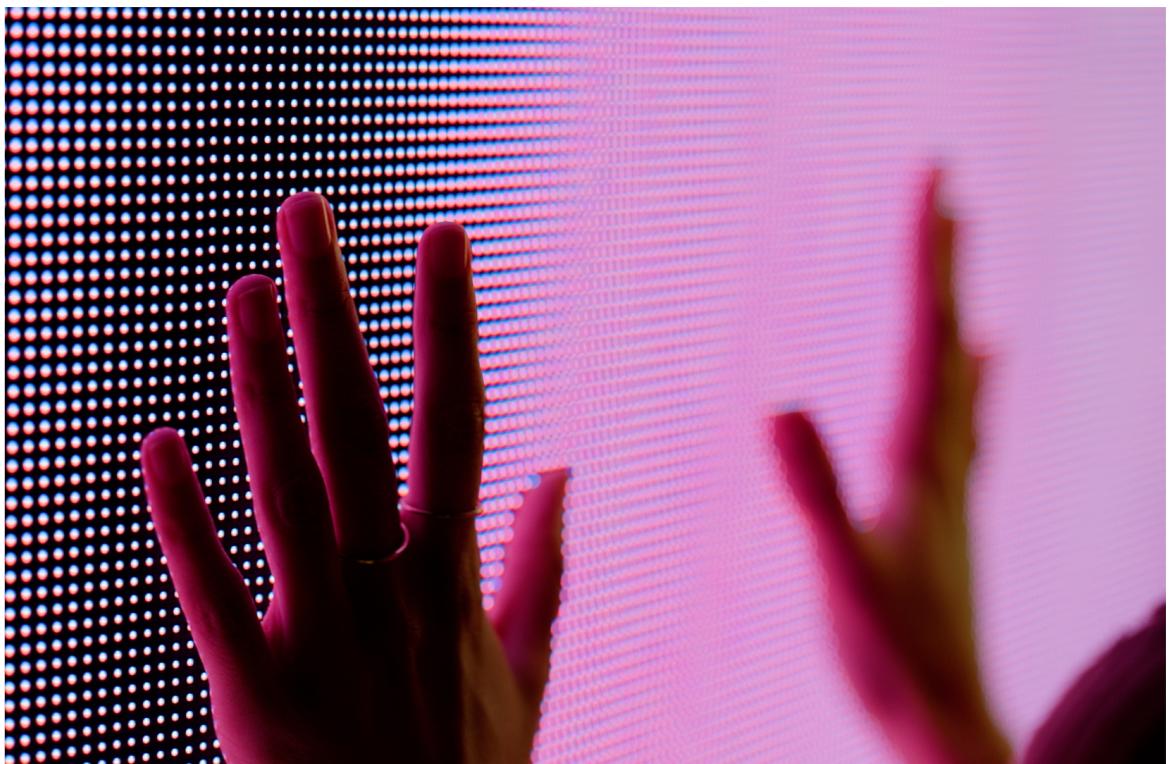
Richieste e campi d'azione

Ecco le domande e i campi d'azione identificati a partire dalle linee direttive della politica dei dati:
 1. Nessun diritto di proprietà di dati
 2. Nessuna nuova legge che limiti il trasferimento di dati
 3. Strumenti legislativi esistenti per garantire l'accesso a dati e la sicurezza degli investimenti in prodotti basati sui dati
 4. Fiducia quale base per l'elaborazione di dati e l'innovazione
 5. Nessun diritto legislativo generale alla trasferibilità dei dati
 6. Standard di anonimizzazione dell'economia
 7. Promozione dell'approccio basato sui rischi nella governance dei dati
 8. Sostegno dei dati aperti dell'amministrazione pubblica (Open Government Data (OGD))
 9. Norme minime e settoriali per la cybersicurezza e il miglioramento della gestione dei rischi e delle crisi

Buone pratiche molto più efficaci di una regolamentazione statale preventiva

Negli ambiti in cui è necessario fare chiarezza, raramente è richiesto l'intervento del legislatore. Da un lato la legislazione non può tenere il passo con gli sviluppi dinamici. Dall'altro nelle questioni di fondo relative alla fiducia si tratta di avere uno scambio tra economia e società. Le norme di buona

pratica dell'economia possono sviluppare questa fiducia in modo migliore e più efficiente rispetto a regolamentazioni legislative preventive.



Nove richieste **e campi d'azione**

1. Nessun diritto di proprietà di dati

Attualmente il concetto di «proprietà di dati» è sulla bocca di tutti. Viene presentato come soluzione che permette a privati di ottenere la sovranità sui propri dati e alle aziende di proteggere i propri investimenti. La richiesta viene già fatta valere anche nella politica. Ma un diritto di proprietà sui dati è giustificato? E come potrebbe essere attuato? La situazione iniziale nei paradigmi dei diritti materiali ha acquisito dinamica nel quadro dello sviluppo tecnologico. Oggi sono possibili forme di esercizio di possesso e proprietà che finora erano ipotizzabili solo a livello teorico oppure difficilmente attuabili: la disponibilità di informazioni evita costi di ricerca e unisce persone con esigenze simili. Si può osservare questo sviluppo con le nuove forme di noleggio (ad es. Uber e Airbnb) oppure nel fatto che oggi consumiamo spesso contenuti che non ci appartengono (ad es. servizi di streaming). Un film su DVD può essere visto solo dalla persona che possiede fisicamente il DVD; un film su Netflix è accessibile contemporaneamente a molte persone. Attualmente i dati

non sono definiti come oggetti di diritto. Con essi non è nemmeno possibile far valere diritti assoluti come ad esempio diritti di proprietà. Ciononostante il diritto vigente garantisce a tutte le persone interessate una gestione adeguata dei dati. Non è di conseguenza necessaria l'introduzione di un tale oggetto di diritto e dunque nemmeno di una proprietà di dati. In particolare, la creazione di una proprietà di dati è in contraddizione con le esigenze e le conquiste della digitalizzazione. Qualora a settori specifici occorresse un adeguamento giuridico - ad esempio nel contesto della blockchain – simili adeguamenti dell'ordinamento giuridico possono avvenire in modo puntuale e mirato, senza che risulti un impatto generale indesiderato sull'economia digitalizzata. Un ulteriore problema riguarda il fatto che le esigenze poste alla configurazione di tali diritti non sono concrete. Se i dati fossero fissati in un quadro giuridico, senza un coordinamento a livello internazionale sarebbero fortemente minacciate anche la certezza del diritto e di pianificazione. Vi sono altri metodi sufficienti per garantire la protezione dei dati e mantenere gli investimenti. Il diritto della personalità permette ad esempio la protezione dell'individuo anche nell'ambito dell'economia dei dati. **Quanto detto vale anche per gli algoritmi** Gli algoritmi sono delle direttive operative per macchinari, proprio come le ricette sono delle istruzioni per preparare pietanze. Una nuova limitazione legislativa degli algoritmi andrebbe nella direzione sbagliata proprio come nel caso di un diritto di proprietà sui dati e rallenterebbe lo sviluppo in questo ambito. Gli algoritmi estrapolano infatti un importante valore aggiunto dai dati:

- il motore di ricerca Google risponde alle ricerche in base ad algoritmi;
- le applicazioni di navigazione indicano la via con l'aiuto di algoritmi;
- gli algoritmi nel settore bancario permettono la valutazione dei rischi nelle operazioni di credito.

Grafico 3

Problemi causati da un diritto di proprietà relativo ai dati*

Problemi che potrebbero verificarsi con l'introduzione della proprietà dei dati

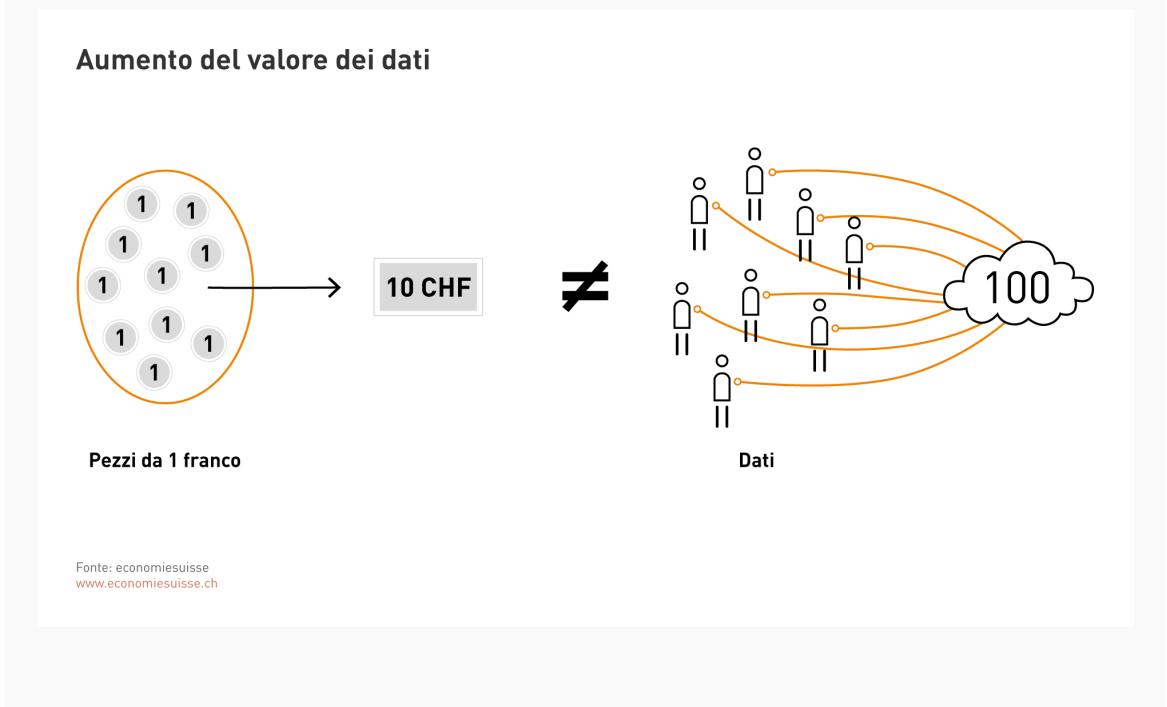
- ▶ Difficoltà, perfino impossibilità, di valutare le conseguenze giuridiche (per degli sviluppi tecnologici futuri)
- ▶ Creazione di un maggiore rischio di monopolio
- ▶ Necessità di introdurre nuovi strumenti giuridici
- ▶ Danni inflitti alla piazza economica svizzera in mancanza di un'armonizzazione internazionale
- ▶ Conflitti con leggi esistenti (soprattutto la LPD)
- ▶ Messa in pericolo della certezza del diritto

* Basato su: Università di Zurigo, Center for Information Technology Society and Law, professori Rolf H. Weber e Florent Thouvenin, conferenza del 29 novembre 2017 sui bisogni in materia di proprietà dei dati

Fonte: economiesuisse
www.economiesuisse.ch

In caso di nuovi modelli commerciali, in situazioni eccezionali possono esservi dei punti da chiarire, ad esempio con i dati che risultano nell'ambito di un fallimento. Salvando le fotografie su una cloud, è possibile aumentare la memoria del cellulare oltre le possibilità dell'apparecchio. Anche le aziende usano la memoria cloud per motivi di accesso semplificato e di altri servizi offerti da provider di servizi cloud. In caso di fallimento di un provider di soluzioni cloud, un'azienda non ha alcuna possibilità di esigere la restituzione dei dati nella memoria cloud. Questo nonostante i dati in questione siano necessari per l'esercizio. Ciò è dovuto al fatto che dal punto di vista giuridico i dati non rappresentano beni mobili rilevanti per il fallimento. In questi casi una regolamentazione dei diritti sui può essere eccezionalmente sensata. **Il valore dei dati risulta solo in un contesto specifico** Se si è in possesso di una moneta da un franco, è possibile acquistare merci per il rispettivo controvalore. Se dieci persone raccolgono un franco ciascuno, risultano dieci franchi. Nel caso dei dati il valore si misura in modo diverso. Un singolo dato non ha di per sé alcun valore. Solo una volta inseriti i dati in un contesto relativo a origine o altri record di dati può risultare un valore. Ad esempio singoli dati sui movimenti, insignificanti da soli, se combinati possono improvvisamente acquisire importanza per un sistema di noleggio di biciclette, poiché forniscono informazioni che l'azienda può interpretare. Non è possibile ricondurre questo valore al singolo dato.

Grafico 4



2. Il traffico di dati non può essere limitato con nuove leggi

Per «traffico di dati» si intende il flusso di dati all'interno delle vie di trasmissione digitali tra i diversi interessati. Ogni volta che vengono trasmesse informazioni, in senso lato avviene anche un traffico di dati. Per le persone che partecipano al traffico di dati vi sono diritti e doveri. Un traffico di dati illimitato, indipendentemente dall'ubicazione degli interessati (ovvero anche a livello internazionale), è di importanza fondamentale per l'economia. Va respinto ogni tipo di limitazione statale o nuove regolamentazioni legislative. Questo vale in particolare anche per i blocchi della rete. **I blocchi della rete devono essere respinti**
Blocchi della rete o limitazioni d'accesso sono misure tecniche con cui, su ordine dello Stato, viene limitata la raggiungibilità di determinati fornitori di prestazioni in internet. Il progetto di legge sui giochi in denaro prevede ad esempio dei blocchi di rete, affinché i fornitori stranieri senza concessione in Svizzera possano essere esclusi dal mercato dei giochi in denaro. Gli utenti non potrebbero così accedere alle pagine Web che propongono queste offerte, grazie a barriere tecniche controllate dallo Stato e attuate dai fornitori d'acces-

so a Internet. Simili blocchi sono totalmente inappropriati e perfino pericolosi in quanto compromettono la sicurezza e la stabilità delle reti. **Traffico di dati: vantiaggi dell'autonomia privata e delle buone pratiche** Interessati, privati e aziende disciplinano già oggi tra di loro il traffico di dati. Questo avviene di regola in virtù di accordi contrattuali, condizioni di utilizzo e applicando le disposizioni legali esistenti. Non è dunque necessaria una regolamentazione legislativa supplementare. Le norme di buona pratica sono regole di comportamento che si impongono i settori o l'economia. Nel settore del traffico di dati, con l'aiuto di norme di buona pratica è possibile evitare un'informazione insufficiente dei partecipanti più deboli e promuovere la sicurezza del traffico di dati. In questo modo è possibile garantire una gestione responsabile dei dati. Le norme di buona pratica sono tra l'altro possibili nelle forme seguenti:

- clausole standard / elementi contrattuali con diritti e doveri dei partecipanti corretti ed equilibrati, che possono essere ripresi da questi ultimi nell'ambito di contratti;
- standard tecnici relativi a tecnologia e sicurezza;
- descrizione comune dei ruoli dei partecipanti al traffico di dati.

Le norme di buona pratica non garantiscono solo la responsabilità dei partecipanti al traffico di dati, ne rappresentano bensì anche un'accelerazione e semplificazione grazie, ad esempio, a elementi contrattuali standard. Creano infine una certezza del diritto. **Le discontinuità rallentano i processi aziendali** Si parla di discontinuità quando, durante una trasmissione o un'elaborazione di dati digitali, le informazioni devono essere trasferite manualmente (ad esempio inserite a mano in un computer). Proprio nello scambio con le autorità, tali discontinuità possono portare a un grande onere supplementare. Se un'informazione elaborata elettronicamente nell'azienda deve essere rielaborata manualmente per l'inoltro a un'autorità di vigilanza (ad esempio stampata su carta o inserita in una maschera online), questo significa un onere di tempo supplementare, fonti d'errore supplementari e di conseguenza perdite in termini di qualità per il relativo processo. Nelle relazioni con lo Stato, simili discontinuità paralizzano regolarmente uno scambio efficiente. Nell'estate 2017 la SECO ha svolto un'indagine presso l'economia in merito all'adeguamento delle leggi concernenti la digitalizzazione (test digitale): è stato possibile identificare numerose disposizioni che ostacolano uno scambio digitale con le autorità.

3. Strumenti legislativi esistenti garantiscono l'accesso a dati e assicurano investimenti in prodotti basati sui dati

I dati che una persona comunica in generale si sottraggono in determinata misura al suo controllo. Tali dati possono trovarsi in un'amministrazione pubblica, in un'azienda o presso un'altra persona. Dei diritti di accesso sono attribuiti a persone autorizzate ad accedere ai dati. Questo vale ad esempio anche nei rapporti tra due aziende. La protezione degli investimenti mira a proteggere in modo adeguato le spese legate ai dati contro un utilizzo non autorizzato da parte di terzi. Uno sviluppo nel settore di prodotti basati su dati non deve poter essere usato da terzi (o almeno non senza un indennizzo). **Esempi: leggi come LCSI, LCART e LDA offrono numerose possibilità** Utilizzato correttamente, il nostro arsenale giuridico permette di regolamentare l'accesso ai dati in maniera ragionevole e di garantire la protezione degli investimenti in prodotti basati su dati:

- La legge federale contro la concorrenza sleale (LCSI) prevede un cosiddetto diritto di protezione delle prestazioni che è possibile invocare davanti a un giudice per impedire l'utilizzo di una propria prestazione da parte di terzi.
- Il fatto che delle imprese rivendichino l'accesso a dati di altre imprese per svolgere le loro attività su un determinato mercato non è nuovo. Questa tematica è sempre stata trattata da un punto di vista del diritto dei cartelli e del controllo degli abusi di posizione dominante (LCart). Il termine «essential facility» dovrebbe presto comparire in relazione ai dati.
- Nell'Unione europea (UE) è prevista una protezione specifica per banche dati. Una tale regolamentazione non è tuttavia indispensabile. A determinate condizioni, nel diritto svizzero le banche dati possono ad esempio rientrare nella protezione del diritto d'autore (LDA). Una protezione sufficiente è garantita anche in questo caso in particolare dal diritto di protezione della prestazione della LCSI.

Gli strumenti giuridici esistenti permettono ai tribunali di giudicare le controversie in modo adeguato Nel 2005 il Tribunale federale si è occupato di una controversia tra diversi offerenti di inserzioni immobiliari online. Un'azienda setacciava sistematicamente Internet alla ricerca di inserzioni immobiliari per

poi pubblicarle sul proprio sito online. Lo scopo era sfruttare le inserzioni a livello commerciale. Il Tribunale federale si è occupato della questione se questa pratica fosse ammissibile. Dopo un'ampia ponderazione giuridica, il Tribunale federale ha deciso il caso in via definitiva in virtù della legge federale contro la concorrenza sleale (LCSI).

4. Fiducia quale base per elaborazione di dati e innovazione

Oggi l'utente vuole sempre più disporre su richiesta, in ogni momento e ovunque di contenuti adeguati e che lo interessano. Spesso ad essere in primo piano non è più la fedeltà nei confronti di un offerente, bensì l'acquisizione di informazioni e servizi. Nuovi modelli commerciali rispondono alle esigenze di tali utenti. La digitalizzazione favorisce l'offerta di nuove prestazioni che facilitano la vita e aumentano la diversità dell'offerta. L'elaborazione di grandi volumi di dati è al centro di numerosi nuovi modelli commerciali. Colui che mette a disposizione i dati deve poter confidare nel fatto che la loro gestione avvenga in modo adeguato. Deve essere garantito che i propri dati non vengano usati illecitamente per altri scopi. Quanto considerato accettabile da un utente, può andare troppo oltre per un altro. Il desiderio dell'individuo deve essere al centro della questione su cosa sia ammissibile o meno. Proprio in questo settore, una protezione dei dati esagerata e dominante porta perciò a un'importante limitazione di nuovi sviluppi. Utenti e offerenti devono armonizzare

Riflessioni di carattere etico, autoregolamentazione e norme di buona pratica dell'economia nell'elaborazione dei dati

Le possibilità offerte dall'analisi di grandi volumi di dati sono molteplici. La Cina, ad esempio, cerca di spingere l'intera popolazione ad adottare determinati comportamenti auspicati dal governo tramite il cosiddetto «big nudging». Simili forme di manipolazione e controllo vanno chiaramente respinte. È significativo che spesso, per motivi diversi, è lo Stato ad accedere ai dati dei cittadini. Le parole chiave in questo contesto sono l'affare Snowden o l'archiviazione preventiva di dati per analisi successive. Per l'economia è di importanza fondamentale mostrare con principi etici i

limiti di quanto sia ammissibile dal punto di vista economico. Occorre ad esempio evitare il pericolo che i clienti vengano manipolati o che procedure non trasparenti portino a decisioni sfavorevoli. L'economia è disposta ad autoregolamentarsi nell'ambito dell'elaborazione dei dati in virtù di riflessioni di carattere etico. Essa vuole mostrarsi degna della fiducia dei propri clienti.

Attuale revisione della legislazione sulla protezione dei dati e rapporto con la digitalizzazione

L'economia riconosce l'importanza di un'adeguata protezione dei dati. Recentemente in Europa le regole sono diventate più severe, con ripercussioni dirette per la Svizzera. Di conseguenza, la legge federale sulla protezione dei dati (LPD) è attualmente in revisione. La protezione dei dati si riferisce al primo livello di utilizzo dei dati (raccolta, archiviazione e definizione di dati). Ma questo approccio superato di protezione dei dati non permetterà di seguire il ritmo della trasformazione digitale ancora a lungo.

5. Nessun diritto legislativo generale alla trasferibilità dei dati

La trasferibilità dei dati si occupa anche della possibilità di trasmettere dati su altri sistemi. Una persona attiva su Facebook, ad esempio, trasferisce ogni sorta di dati sulla piattaforma: amicizie, like, foto caricate, ecc. In questo modo l'offerente della piattaforma può risalire ad altre informazioni (basate su dati) osservando il relativo comportamento. Optando per un'altra piattaforma dei social media, nel quadro della trasferibilità dei dati si pone la questione se sia possibile riavere i dati inseriti e le informazioni raccolte e trasferirli in una nuova piattaforma. Per quanto riguarda la trasferibilità dei dati si tratta dunque di rispondere alla domanda se le aziende devono essere obbligate a consegnare i dati raccolti sugli utenti in forma strutturata o a trasmetterli a terzi designati. **La trasferibilità assoluta dei dati è sproporzionata** Conformemente alla nuova legislazione dell'UE, aziende e autorità sono obbligate a permettere la trasferibilità dei dati. Questo obbligo mira a garantire un miglior controllo da parte dell'utente e a promuovere la concorrenza tra i fornitori di servizi. I consumatori avrebbero ad esempio diritto a dati grezzi o dati di contatori

intelligenti, motori di ricerca e braccialetti fitness. Il diritto svizzero non prevede un tale diritto assoluto alla trasferibilità dei dati. Nell'esempio citato all'inizio è possibile riconoscere i limiti di una strategia assoluta. Di regola, a un utente di una rete sociale non risulta alcun vantaggio se ottiene i suoi dati. Ad essere interessanti per l'utente sono in primo luogo le conoscenze e le informazioni ricavate con i suoi dati, in particolare in riferimento a terzi. I loro dati non si possono tuttavia estrapolare dal sistema senza entrare in conflitto con i loro interessi. **Alternative alla trasferibilità assoluta dei dati** Le imprese investono regolarmente degli importi considerevoli nel settore della protezione dei dati. È possibile in ogni momento fornire i dati all'utente quando le due parti, il cliente e l'impresa, sono concordi. Sarebbe tuttavia sbagliato obbligare l'azienda a consegnare in ogni caso i dati e a dettarle le prescrizioni tecniche su come deve avvenire tale consegna. Il fatto che spesso tali dati siano salvati in forma anonima nel sistema oppure non sia addirittura possibile attribuirli a una singola persona, rende ancora più difficile la consegna. Una trasmissione diretta da un offerente a un privato può inoltre rappresentare delle difficoltà tecniche, a seconda delle prescrizioni legislative relative al formato. Per diritti ragionevoli e oggettivi alla consegna di dati vi sono altre possibilità:

- utilizzo di strumenti tecnici e legali esistenti;
- accordi tra le parti, eventualmente con contratti;
- buone pratiche.

6. Standard di anonimizzazione dell'economia

Anonimizzazione e pseudonimizzazione sono due processi relativi alla protezione dei dati. Nella pseudonimizzazione il nome o un altro identificatore personale viene sostituito da uno pseudonimo (combinazioni di lettere o cifre). Con l'anonymizzazione i dati vengono modificati in modo tale da non essere più attribuibili a una persona. Se un professore di una scuola universitaria vuole ad esempio comunicare in modo semplice i risultati di un esame scritto, durante l'esame può invitare gli studenti a indicare uno pseudonimo di loro scelta sui fogli. Dopo la correzione, il professore può pubblicare un elenco (anche in Internet) con tutti i risultati secondo lo schema pseudonimo / voto. L'associazione dello pseudonimo al rispettivo studente è possibile solo da parte del professore o del singolo studente. Si tratterebbe invece di anonymizzazione se in seguito

i fogli d'esame con gli pseudonimi indicati dagli studenti venissero distrutti. Le indicazioni sull'elenco dei voti sarebbero anonimizzate per il pubblico, poiché non sarebbe più possibile un'associazione al rispettivo studente.

Vantaggi degli standard di anonimizzazione dell'economia

Nell'elaborazione di nuove strategie, le aziende non possono lavorare in modo efficace con i dati se devono chiedere ogni volta l'autorizzazione a chi li fornisce. Di regola, durante lavori di questo tipo, non sono nemmeno interessate alla parte dei dati relativa alle persone. Ecco perché anonimizzazione e pseudonimizzazione permettono e semplificano la gestione di simili dati nel rispetto della protezione della personalità.

Le strategie di anonimizzazione che prevedono anche possibilità di pseudonimizzazione diventano rapidamente obsolete. Invece di prescrizioni rigide, in questo contesto sono necessari standard affidabili dell'economia che abbiano un costante sviluppo e garantiscano così la protezione dei diritti della personalità.

Le anonimizzazioni compensano inoltre il fatto che la delimitazione tra dati riferiti a persone e a oggetti è praticamente impossibile nella prassi. Molti dati, ad esempio i dati di esercizio di una fresatrice, possono essere riferiti a una persona. I dati dell'orologio interno della macchina potranno essere collegati al piano d'intervento dei collaboratori. In questo modo è possibile risalire a informazioni relative all'utilizzo di chi ha manovrato il macchinario. Se si vogliono sfruttare i dati d'esercizio per migliorare i processi di fabbricazione, i diritti della personalità del manovratore potrebbero rappresentare un ostacolo.

Un'anonymizzazione permette l'ulteriore elaborazione e l'analisi dei dati con contemporanea protezione ottimale dei diritti della personalità.

7. Promozione dell'approccio basato sui rischi nella governance dei dati

La governance dei dati di un'impresa rappresenta l'insieme delle regole sulla disponibilità, l'utilizzo, l'integrità e la protezione dei dati dell'impresa. L'implementazione di un sistema di governance dei dati in un'impresa prevede diversi passi. Si inizia con la definizione della base di dati, passando per la regolamentazione delle competenze interne per determinati record di dati fino alla definizione di un meccanismo di controllo e alla formazione dei collaboratori.

Con l'approccio basato sui rischi si procede agli investimenti più importanti nella protezione dei dati laddove vi è il maggiore potenziale di rischio. Se un'azienda rileva dei dati ad esempio attraverso una carta fedeltà personale con la quale si raccolgono dei punti durante gli acquisti, per i dati

così raccolti non vi sono di per sé rischi particolari. Attraverso l'analisi dei big data si presentano tuttavia diverse possibilità per l'elaborazione dei dati. La combinazione di punti fedeltà con dati della cassa malati della stessa persona può ad esempio essere significativa. In questo ambito a rischio elevato le aziende procederanno a investimenti maggiori per la protezione dei dati e per la garanzia del rispetto di standard etici rispetto a dati di altri ambiti. **Solo l'approccio basato sui rischi può rilevare i rischi in modo adeguato** L'approccio basato sui rischi della governance dei dati è necessario per soddisfare la complessità di un'azienda e le diverse possibilità di combinazione e di utilizzo dei dati. In base alle loro possibilità di combinazione, i dati possono portare a situazioni di diverso grado di rischio. In un'azienda vi sono inoltre altri fattori da osservare: esistono dati non strutturati, terzi che possono accedere ai dati, procedure durante le quali vengono elaborati importanti dati di persone o dati che esistono solo a livello di applicazione. Con l'approccio basato sui rischi è possibile rivolgere maggiore attenzione alle situazioni con gradi di rischio più marcate. Le risorse di un'azienda vengono impiegate in modo mirato dove si individuano rischi effettivi e per evitare dispersioni.

8. Sostegno ai dati aperti dell'amministrazione pubblica (Open Government Data (OGD))

Le basi di dati del settore pubblico sono molteplici e molto vaste. Le amministrazioni raccolgono infatti regolarmente diversi dati nell'ambito dei loro compiti ufficiali. Si tratta in particolare delle statistiche della popolazione, di dati meteorologici, di rilevamenti topografici dei confini comunali della Svizzera, di documenti storici, di dati sul traffico o di raccolte della letteratura svizzera. Questi dati non rappresentano un valore aggiunto solo per l'amministrazione, ma anche per terzi, ad esempio per un'azienda o privati. L'azienda è eventualmente interessata all'ulteriore elaborazione di tali dati o a un loro nuovo utilizzo. È dunque possibile che i dati disponibili abbiano una nuova combinazione e non permettano così solo un nuovo modello commerciale, creino bensì anche un valore aggiunto per l'intera popolazione. **Gli OGD devono essere resi accessibili al pubblico** Tutti i dati che lo Stato rileva nell'adempimento dei suoi compiti sovrani e che non sono riferiti a persone (non permettono quindi di risalire a un individuo) devono essere a disposizione della collettività e dunque anche dell'economia. Vanno tuttavia posti dei limiti: i privati che collaborano con lo Stato o aziende statali attive nell'economia privata sono esonerati dall'obbligo

di consegna dei dati. D'altro canto le aziende statali attive nell'economia privata devono essere assoggettate alle regole della concorrenza.

Cosa sono gli «OGD»?

Gli Open Government Data (OGD) sono dati che vengono rilevati dallo Stato nel quadro dell'adempimento dei suoi compiti sovrani. Il rilevamento di tali dati è stato finanziato con imposte e tasse.

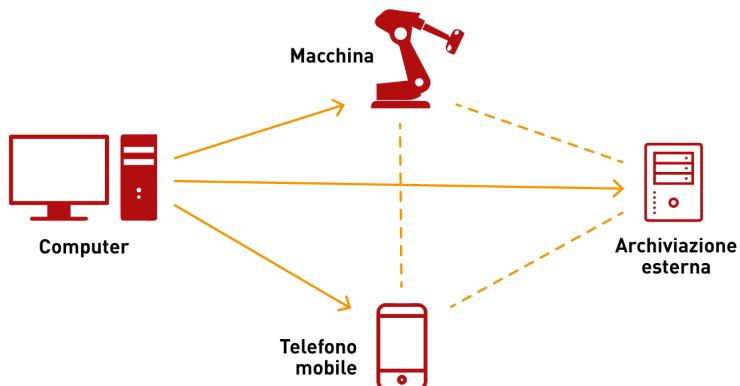
9. Requisiti minimi specifici dei settori per sicurezza informatica e miglioramento della gestione di minacce e crisi

La digitalizzazione e la conseguente interconnessione di sistemi ci porta a un livello di vulnerabilità del tutto nuovo. Dall'impiego di tecnologie e dalla loro interconnessione, complessità e dinamica nascono dei pericoli. Questa sensazione viene rafforzata dagli articoli quasi quotidiani nei media relativi ad attacchi e manipolazioni. Queste attività criminali avvengono per i motivi più diversi e con le procedure più disparate. Anche nel mondo digitale dobbiamo proteggerci da attività criminali commesse da terzi, proprio come facciamo nella vita reale. **Requisiti minimi dell'economia specifici dei settori** Uno standard di sicurezza uniforme e prescritto dallo Stato non può soddisfare le sfide poste dalla cybercriminalità, poiché vi è il rischio di una sicurezza informatica unilaterale e dunque insufficiente. È piuttosto necessario un sistema flessibile e decentralizzato. Laddove indicato per questioni specifiche del settore, l'economia può aumentare la sicurezza informatica con requisiti minimi prestabiliti. Agli anelli più deboli della catena deve essere dedicata particolare attenzione poiché, vista l'interconnessione con altri sistemi, un livello di protezione inferiore alla media può essere trasferito ad altre aziende. Questo rende ancora più importanti i requisiti minimi formulati in questo ambito dall'economia, poiché le aziende protette in modo meno sicuro possono beneficiare del know-how di altre aziende. Questo permette di evitare delle asimmetrie in ambito informatico tra i vari rami. Con la creazione di standard minimi può inoltre essere applicato l'approccio basato sui rischi: l'attuazione avviene nel giusto equilibrio con il rischio per l'azienda. L'interconnessione avviene in particolare anche tra

apparecchi. Se all'interno dell'azienda non vengono sottoposti regolarmente a manutenzione, possono rappresentare il punto di partenza per un attacco.

Grafico 5

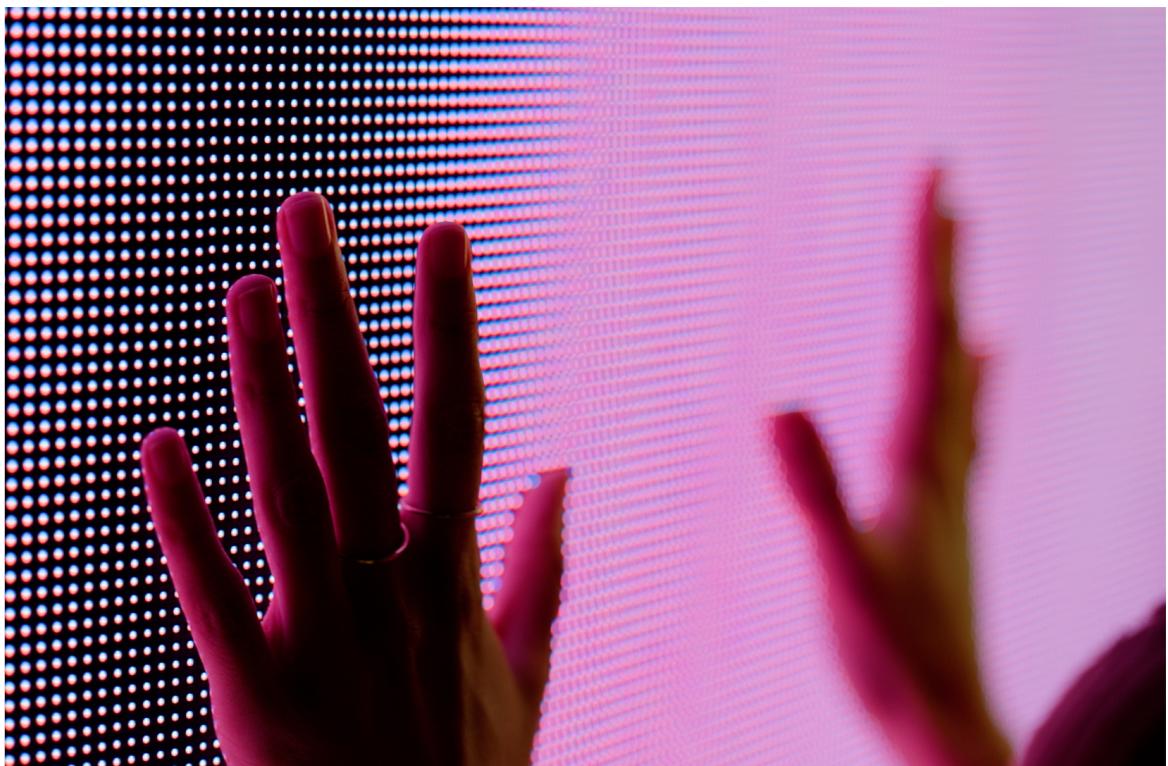
Trasferimento dei cyberrischi a seguito della messa in rete di oggetti e imprese



Fonte: economiesuisse
www.economiesuisse.ch

È necessaria una ripartizione dei compiti tra economia privata e Stato in caso di crisi e una promozione delle notifiche di attacchi informatici Nel rapporto tra economia privata e Stato è necessaria una chiara ripartizione dei compiti in caso di crisi. Lo Stato deve essere dotato dei mezzi necessari per perseguire i crimini informatici a livello internazionale. Al contempo lo Stato deve provvedere con strumenti adeguati e fondati su incentivi che gli incidenti informatici vengano notificati. In questo modo è in grado di reagire e di fornire delle raccomandazioni. Nel rapporto tra Stato e aziende è necessaria una cultura della collaborazione e non della costrizione. Una notifica deve avvenire quando un'azienda lo auspica e nel modo che le sembra appropriato. Promuovendo le notifiche si mira a ottenere una maggiore trasparenza, un miglior rilevamento delle minacce e una riduzione delle ripercussioni su terzi. **Sensibilizzazione di popolazione, aziende, amministrazione e politica** La sicurezza informatica è un classico compito comune e non interessa solo le imprese e lo Stato, bensì anche i privati. Per questo motivo la comprensione per i rischi in-

formatici deve essere migliorata in generale e occorre avviare un cambiamento del comportamento. Le banche inviano ad esempio regolarmente delle note ai propri clienti per informarli in merito a questi attacchi informatici o per metterli in guardia nei confronti di e-mail o telefonate fraudolente.



Presa di posizione ***da parte degli ambienti economici***

Le esigenze poste alle norme di buona pratica dell'economia risultano da parametri e campi d'azione localizzati. In questo modo degli standard generalmente riconosciuti nell'ambito del traffico di dati possono evitare un'asimmetria informativa tra le parti, promuovere la sicurezza del traffico di dati e accelerarlo. Contribuiscono inoltre alla certezza del diritto senza paralizzare lo sviluppo. Le norme di buona pratica portano vantaggi a tutti gli interessati anche durante l'elaborazione di dati. Uno standard di anonimizzazione in costante sviluppo delle aziende può garantire che le strategie di anonimizzazione siano sempre aggiornate e che sia dunque garantita la protezione della personalità. I requisiti minimi specifici dei settori nell'ambito della sicurezza informatica possono realizzare un sistema informatico flessibile e decentralizzato della sicurezza nel cyberspazio ed evitare asimmetrie. Le norme di buona pratica aiutano inoltre a considerare riflessioni di carattere etico e tecnico in relazione con i dati e sostituiscono in modo adatto un diritto legislativo assoluto alla trasferibilità dei dati. Con l'applicazione di norme di buona pratica la regolamentazione

legislativa, in particolare quella preventiva, è superflua nei campi d'azione indicati.

Conclusione

Lo sviluppo tecnologico avanza rapidamente. La Svizzera deve garantire di essere anche in futuro tra i capofila. L'economia dei dati e numerosi campi d'applicazione risultanti, da sharing economy a intelligenza artificiale, in futuro caratterizzeranno in modo determinante la nostra vita economica. È di fondamentale importanza che vi sia un equilibrio degli interessi tale che la fiducia del singolo sia protetta e non venga danneggiata la forza innovativa della piazza economica. L'economia è disposta ad assumersi la responsabilità in questo ambito. Essa presenta gli strumenti con i quali assicurare la fiducia nelle nostre aziende e al contempo i mezzi necessari per partecipare in prima linea al progresso nella concorrenza a livello internazionale di cui dispone la Svizzera. È fondamentale che possibili sviluppi non vengano interrotti o addirittura ostacolati da regole rigide. La presente politica dei dati dell'economia mostra come ciò possa funzionare trovando un equilibrio tra gli interessi.

Grafico 6

Le linee direttive, i campi d'azione e i bisogni identificati sono la base per una presa di posizione da parte degli ambienti economici.





Ringraziamenti

Un ringraziamento particolare va ai membri del gruppo di lavoro sulla Politica dei dati di economiesuisse, nonché ai numerosi partecipanti dei vari sottogruppi e alle persone che erano responsabili della gestione dei sottogruppi:

- Dr. Matthias Bossardt, Responsabile Cybersecurity KPMG Schweiz, KPMG AG, responsabile del sottogruppo Cybersecurtiy nell'ambito del gruppo di lavoro Politica dei dati di economiesuisse
- Maria Chiara Atzori, Head Data Privacy CH, Novartis International AG, responsabile del sottogruppo di lavoro Autodeterminazione per le informazioni concernenti le persone e i big data nell'ambito del gruppo di lavoro Politica dei dati di economiesuisse
- Werner W. Wyss, Head Regulatory Affairs, Zürcher Kantonalbank, responsabile del sottogruppo di lavoro Traffico dati nell'ambito del gruppo di lavoro Politica dei dati di economiesuisse
- Gema Olivar Pascual, Designated General Counsel, PricewaterhouseCoopers AG, responsabile del sottogruppo di lavoro Dati & Algoritmi in quanto soggetti di diritto nell'ambito del gruppo di lavoro Politica dei dati di economiesuisse

- Jean-Marc Hensch, direttore, swico; responsabile del sottogruppo di lavoro Diritti d'accesso e di utilizzo nell'ambito del gruppo di lavoro Politica dei dati di economiesuisse
- Nadine Büchler; collaboratrice scientifica Concorrenza & Regolamentazione presso economiesuisse, segretaria e coordinatrice del gruppo di lavoro Politica dei dati fino a settembre 2017