



Berna, 13 marzo 2026

Ordinanza concernente la comunicazione elettronica nei procedimenti giudiziari e amministrativi di diritto federale (OCEP)

Rapporto esplicativo
per l'avvio
della procedura di consultazione



Compendio

Situazione iniziale

Il 20 dicembre 2024 l'Assemblea federale ha adottato la legge federale concernente le piattaforme per la comunicazione elettronica in ambito giudiziario (LCEG; FF 2025 19, RU 2025 583). Questa legge introduce l'obbligo di comunicare per via elettronica per i professionisti del diritto. Ciò riguarda in particolare le autorità, compresi i tribunali e i pubblici ministeri, nonché gli avvocati. La Confederazione e i Cantoni possono introdurre l'obbligo in modo differenziato per i loro procedimenti durante un periodo transitorio di cinque anni. È inoltre prevista la costituzione di un ente di diritto pubblico responsabile dell'allestimento, dell'esercizio e dello sviluppo della piattaforma centrale mediante la quale si svolgerà la comunicazione elettronica nei procedimenti civili e penali e nella giurisdizione amministrativa. Per i procedimenti amministrativi della Confederazione, la LCEG prevede che un'unità amministrativa dell'Amministrazione federale centrale allestisca una piattaforma.

Il termine referendario per la LCEG è scaduto inutilizzato il 19 aprile 2025. Una prima parte della legge¹ è entrata in vigore il 1° ottobre 2025; affinché la parte restante della legge possa entrare in vigore, devono essere adempiute le seguenti condizioni:

- costituzione dell'ente justitia.swiss (Confederazione e almeno 18 Cantoni);*
- autorizzazione e messa in esercizio della piattaforma justitia.swiss;*
- accessibilità a una piattaforma di tutti i tribunali federali e cantonali contemplati dalla LCEG;*
- adozione delle disposizioni esecutive relative alla LCEG.*

Queste condizioni saranno verosimilmente adempite al più presto il 1° gennaio 2027.

Contenuto del progetto

Il progetto contiene in particolare disposizioni relative al rilascio di un'autorizzazione di esercizio alle piattaforme secondo la LCEG, ai mezzi di autenticazione per l'utilizzo delle piattaforme, ai formati e alle dimensioni ammessi per i documenti, nonché all'importo degli emolumenti e alla loro riscossione.

¹ RS 172.023

Indice

1	Situazione iniziale.....	4
2	Punti essenziali del progetto	5
2.1	Autorizzazione d'esercizio	5
2.2	Mezzo di autenticazione	6
2.3	Formati e dimensioni ammessi dei documenti	6
2.4	Digitalizzazione di atti cartacei	6
2.5	Emolumenti	7
2.6	Proposte normative rifiutate	7
3	Commento ai singoli articoli	9
4	Commenti all'allegato 1 (abrogazione e modifica di altri atti normativi)	34
4.1	Abrogazione dell'ordinanza del 18 giugno 2010 sulla comunicazione per via elettronica nell'ambito di procedimenti amministrativi (OCE-PA) 34	
4.2	Abrogazione dell'ordinanza del 18 giugno 2010 sulla comunicazione per via elettronica nell'ambito di procedimenti civili e penali nonché di procedure d'esecuzione e fallimento (OCE-PCPE).....	34
4.3	Ordinanza del 23 novembre 2016 sulla firma elettronica.....	34
5	Commento all'articolo 26 capoverso 5 LCEG.....	35
6	Ripercussioni	36
6.1	Ripercussioni per la Confederazione	36
6.2	Ripercussioni per i Cantoni e i Comuni.....	36
6.3	Ripercussioni sull'economia	37
6.4	Ripercussioni sulla società	37
7	Aspetti giuridici.....	38
7.1	Sicurezza delle informazioni.....	38
7.2	Protezione dei dati	38

Rapporto esplicativo

1 Situazione iniziale

Il 20 dicembre 2024 l'Assemblea federale ha adottato la legge federale concernente le piattaforme per la comunicazione elettronica in ambito giudiziario (LCEG; FF 2025 19, RU 2019 583). Questa legge introduce l'obbligo di comunicare per via elettronica per i professionisti del diritto. Ciò riguarda in particolare le autorità, compresi i tribunali e i pubblici ministeri, nonché gli avvocati. La Confederazione e i Cantoni possono introdurre l'obbligo in modo differenziato per i loro procedimenti durante un periodo transitorio di cinque anni. È inoltre prevista la costituzione di un ente di diritto pubblico responsabile dell'allestimento, dell'esercizio e dello sviluppo della piattaforma centrale mediante la quale si svolgerà la comunicazione elettronica nei procedimenti civili e penali e nella giurisdizione amministrativa. Per i procedimenti amministrativi della Confederazione, la LCEG prevede che un'unità amministrativa dell'Amministrazione federale centrale allestisca una piattaforma.

Il termine referendario per la LCEG è scaduto inutilizzato il 19 aprile 2025. Il 19 settembre 2025 il Consiglio federale ha deciso di porre in vigore per il 1° ottobre 2025 la parte della LCEG (in particolare art. 1–17) necessaria per la creazione di una piattaforma centrale ai sensi della suddetta legge. Affinché la parte restante della legge possa entrare in vigore, devono essere adempiute le seguenti condizioni:

- *costituzione dell'ente justitia.swiss (Confederazione e almeno 18 Cantoni);*
- *autorizzazione e messa in esercizio della piattaforma justitia.swiss;*
- *accessibilità a una piattaforma di tutti i tribunali federali e cantonali contemplati dalla LCEG;*
- *adozione delle disposizioni esecutive relative alla LCEG.*

Queste condizioni saranno verosimilmente adempite al più presto il 1° gennaio 2027.

Per poter testare tempestivamente la piattaforma centrale, sulla base delle disposizioni vigenti in materia di comunicazione elettronica in ambito giudiziario sono state autorizzate diverse fasi pilota secondo l'articolo 13a dell'ordinanza del 18 giugno 2010² sulla comunicazione per via elettronica nell'ambito di procedimenti civili e penali nonché di procedure d'esecuzione e fallimento (OCE-PCPE). Questi progetti pilota hanno fornito preziosi riscontri e hanno contribuito a ottimizzare la piattaforma centrale conformemente ai requisiti, per approntarla all'uso operativo da parte degli utenti. Non si sono verificati problemi degni di nota.

² RS 272.1

2 Punti essenziali del progetto

Con la LCEG, il Parlamento ha creato le basi per procedimenti giudiziari interamente digitali e senza discontinuità di supporto. La gestione degli atti si svolge per via elettronica. Per i professionisti del diritto, in particolare i tribunali, le autorità e gli avvocati, comunicare in questo modo diventa obbligatorio. Il presente progetto di ordinanza concernente la comunicazione elettronica nei procedimenti giudiziari e amministrativi di diritto federale (di seguito: AP-OCEP) serve principalmente ad attuare la LCEG. L'AP-OCEP concretizza le condizioni per l'autorizzazione di esercizio e la procedura di autorizzazione per le piattaforme ai sensi della LCEG; disciplina inoltre i mezzi di autenticazione ammessi, i formati ammessi per la trasmissione e le loro dimensioni, la digitalizzazione dei documenti cartacei da parte dei tribunali e delle autorità, nonché gli emolumenti. L'AP-OCEP riprende inoltre alcune regole della e-LEF³, finora contenute nell'OCE-PCPE. Quest'ultima sarà abrogata con l'entrata in vigore definitiva della LCEG. Il presente progetto modifica inoltre l'ordinanza del 23 novembre 2016⁴ sui servizi di certificazione nel campo della firma elettronica e di altre applicazioni di certificati digitali (ordinanza sulla firma elettronica, OFiEle).

L'AP-OCEP si applica a tutte le piattaforme soggette alla LCEG, in particolare anche alla futura piattaforma per le procedure amministrative della Confederazione e alla trasmissione elettronica nell'ambito della LEF. Il quadro tecnico della futura piattaforma della Confederazione non è ancora noto. Qualora per il suo funzionamento fossero necessarie ulteriori disposizioni a livello di ordinanza, queste saranno elaborate durante la procedura di consultazione o introdotte successivamente, dopo l'entrata in vigore dell'AP-OCEP, mediante una revisione. Ciò vale in particolare per la regolamentazione della ripartizione dei costi interni all'Amministrazione federale connessi con l'utilizzo della piattaforma.

Per garantire l'applicabilità dell'ordinanza, è stato istituito un gruppo di accompagnamento costituito da rappresentanti dell'Amministrazione federale, del Tribunale federale e del Tribunale amministrativo federale, del Ministero pubblico della Confederazione, dei tribunali e ministeri pubblici cantonali nonché della Federazione svizzera degli avvocati.

2.1 Autorizzazione d'esercizio

Oltre alla piattaforma centrale dell'ente di diritto pubblico e alla piattaforma generale per le procedure amministrative della Confederazione, i Cantoni possono sviluppare

³ e-LEF è uno standard informatico per lo scambio di dati in materia di esecuzione e fallimenti tra persone fisiche, persone giuridiche di diritto pubblico e privato e uffici d'esecuzione. Per ulteriori informazioni cfr.: www.eschkg.ch.

⁴ RS 943.032

altre piattaforme secondo la LCEG. L'esercizio di tali piattaforme deve essere autorizzato dal Dipartimento federale di giustizia e polizia (DFGP) conformemente all'articolo 25 LCEG.

Per ottenere l'autorizzazione devono essere soddisfatti diversi requisiti relativi alla crittografia e alla gestione delle chiavi, alle ricevute, alla protezione e alla sicurezza dei dati nonché alle interfacce. Alcuni presupposti dell'autorizzazione figurano già nella stessa LCEG, altri nella presente ordinanza. L'avamprogetto affida infine al DFGP il compito di disciplinare in un'ordinanza dipartimentale i requisiti funzionali e d'esercizio delle piattaforme, nonché le prescrizioni tecniche e il formato dei dati delle interfacce.

Nell'ambito dell'attuazione, il DFGP valuterà l'opportunità di elaborare un promemoria che riassume in modo dettagliato tutti i presupposti dell'autorizzazione.

2.2 Mezzo di autenticazione

Come mezzo di autenticazione l'avamprogetto prevede AGOV, la procedura di login delle autorità. AGOV consente, tra l'altro, un login di questo tipo anche alle persone all'estero che presentano un passaporto o una carta d'identità validi.

2.3 Formati e dimensioni ammessi dei documenti

L'avamprogetto distingue tra comunicazioni delle autorità, atti delle altre parti al procedimento e allegati di tutte le autorità e parti coinvolte in un procedimento. Per le comunicazioni da parte delle autorità è prescritto il formato PDF/A e sono ammesse tutte le varianti standard ISO (da PDF/A-1 a PDF/A-4). Le altre parti al procedimento possono trasmettere i propri documenti in formato PDF o PDF/A. Gli allegati possono essere trasmessi in qualsiasi formato. Se l'autorità non è in grado di aprire l'allegato ricevuto, può chiedere alla parte interessata di rispedirlo in un formato leggibile. L'avamprogetto contiene un elenco di formati ai quali l'autorità che dirige il procedimento deve poter accedere.

Le dimensioni dei documenti sono limitate a 2 gigabyte, il che dovrebbe essere sufficiente per la maggior parte dei documenti trasmessi. Questo limite è nettamente superiore a quello che vale per la trasmissione dei documenti in ambito giudiziario mediante le piattaforme di trasmissione riconosciute, vale a dire una dimensione utile di 15 megabyte. Se, eccezionalmente, un documento supera i 2 gigabyte, può essere suddiviso in file di dimensioni inferiori.

2.4 Digitalizzazione di atti cartacei

L'avamprogetto stabilisce uno standard minimo di qualità da rispettare nell'ambito della digitalizzazione dei documenti cartacei. Impone inoltre alle autorità l'obbligo di controllare la qualità dei documenti digitalizzati.

2.5 Emolumenti

L'avamprogetto prevede la riscossione di emolumenti forfettari presso ogni Cantone e la Confederazione. La Confederazione si farà carico del 10 per cento degli emolumenti, quelli restanti saranno suddivisi tra i Cantoni in base al loro numero di abitanti.

L'importo degli emolumenti si basa sulla pianificazione finanziaria dell'ente di diritto pubblico. Quest'ultimo dovrà tenere conto, nella sua pianificazione finanziaria, anche di eventuali imprevisti e costituire una riserva pari al 10 per cento delle spese totali annuali, al fine di garantire la liquidità.

2.6 Proposte normative rifiutate

Restituzione di documenti

Durante le discussioni del gruppo di accompagnamento è stato suggerito di creare una disposizione, secondo cui determinati documenti fisici non devono essere restituiti. Nel concreto, si tratta di documenti redatti appositamente per le autorità (ad es. denunce penali), quindi disponibili in forma digitale presso l'autore, o di copie di documenti giuridicamente rilevanti, i cui originali rimangono in possesso delle persone che presentano un atto.

Questa proposta è stata respinta, poiché l'articolo 30 LCEG non lascia alcun margine di manovra per prevedere, a livello di ordinanza, che determinati documenti fisici non devono essere restituiti.

Invio in forma cartacea

Durante le discussioni del gruppo di accompagnamento è stato proposto di inviare alle persone che non comunicano per via elettronica con il tribunale o l'autorità una stampa dell'originale elettronico anziché una decisione firmata a mano. In particolare, è stato fatto valere che le leggi procedurali non prevedono che le firme dei membri delle autorità debbano essere autografe.

Nell'allegato della LCEG concernente la modifica di altri atti normativi, tutte le disposizioni che finora prevedevano una firma dell'autorità o del tribunale sono state integrate con la dicitura «se la decisione è inviata in forma cartacea» o una formulazione simile (cfr. p. es art. 238 lett. h del Codice di procedura civile [CPC]⁵, art. 353 cpv. 1 lett. k del Codice di procedura penale [CPP]⁶, art. 153 cpv. 3 della Procedura penale

⁵ RS 272

⁶ RS 312.0

militare del 23 marzo 1979 [PPM]⁷). Quindi, la LCEG stabilisce già esplicitamente che la firma è necessaria in caso di invio cartaceo. Una firma elettronica qualificata corredata di una marca temporale qualificata ai sensi della legge del 18 marzo 2016⁸ sulla firma elettronica (FiEle) è equiparata alla firma autografa (articolo 14 capoverso 2^{bis} del Codice delle obbligazioni [CO]⁹). Tuttavia, tale firma e la marca temporale non conservano la loro forma se stampate su carta. Non vi è alcun margine per una regolamentazione divergente a livello di ordinanza.

Disposizione transitoria per continuare a utilizzare IncaMail e PrivaSphere

Nelle discussioni del gruppo di accompagnamento è stata anche menzionata la necessità di disposizioni transitorie che, per un periodo di tempo limitato, permettano di continuare a utilizzare le piattaforme di trasmissione finora riconosciute.

Questo non è possibile perché le basi legali delle attuali ordinanze sulla comunicazione per via elettronica contenute nelle leggi procedurali verranno abrogate con l'entrata in vigore definitiva della LCEG; non è possibile rimediare alla mancanza di basi legali mediante le disposizioni transitorie di un'ordinanza; occorrono disposizioni transitorie di una legge in senso formale.

Va tuttavia sottolineato che le piattaforme di trasmissione finora riconosciute potranno continuare a essere utilizzate per i procedimenti pendenti al momento dell'entrata in vigore definitiva. Le leggi di procedura contengono disposizioni transitorie che permettono di applicare il diritto previgente ai procedimenti pendenti. Ciò vale anche per la trasmissione elettronica tramite le piattaforme di trasmissione attualmente riconosciute. Per i nuovi procedimenti occorre invece utilizzare una piattaforma secondo la LCEG.

Inoltre, l'articolo 6a capoverso 4 PA nella versione riveduta dalla LCEG permette di continuare a utilizzare le piattaforme di trasmissione finora riconosciute.

In base al sistema riguardante i diritti di cui all'articolo 24 LCEG, è ipotizzabile quanto segue: le piattaforme di trasmissione finora riconosciute possono aprire un conto d'organizzazione sulla nuova piattaforma. Gli utenti che desiderano continuare a utilizzare le piattaforme di trasmissione finora riconosciute possono conferire alla piattaforma da loro utilizzata il diritto di trasmettere e consultare i documenti. Questi utenti possono continuare a utilizzare una delle piattaforme di trasmissione attualmente riconosciute senza dover modificare i loro processi. Se l'utente è un'autorità pubblica, deve però utilizzare un sigillo elettronico regolamentato (cfr. art. 22 cpv 2 LCEG) invece della firma elettronica qualificata.

⁷ RS 322.1

⁸ RS 943.03

⁹ RS 220

3 Commento ai singoli articoli

Ingresso

La LCEG modifica una serie di leggi procedurali, aumentando quindi il numero delle norme di delega. Per motivi di chiarezza l'ingresso menziona la LCEG nella sua interezza ma non elenca le singole norme di delega. Sono inoltre elencate nell'ingresso le disposizioni delle leggi procedurali che riguardano la comunicazione con modalità non contemplate dalla LCEG e che estendono quindi il campo d'applicazione dell'avamprogetto.

Capitolo 1: Esercizio e utilizzo di piattaforme

Sezione 1: Campo d'applicazione

Art. 1

Cpv. 1

La presente disposizione definisce il campo d'applicazione del capitolo 1 dell'avamprogetto. Precisa a quali piattaforme e procedimenti si applicano le dettagliate norme che seguono in particolare quanto all'esercizio e all'utilizzo delle piattaforme e ai requisiti tecnici e organizzativi. Tali norme sono imperative per le piattaforme elencate nel capoverso 1.

Cpv. 2

Le *disposizioni del capitolo 1* si applicano anche ad altre piattaforme, rette da leggi speciali, nella misura in cui la LCEG si applica a tali piattaforme e procedimenti. Molte leggi speciali rinviano già oggi alla legge del 20 dicembre 1968¹⁰ sulla procedura amministrativa (PA) e quindi indirettamente ai mezzi di comunicazione elettronica. Se e nella misura in cui questi rinvii comprendono le piattaforme secondo la LCEG, in seguito alle modifiche apportate da tale legge, le piattaforme rette da queste leggi speciali sottostanno alle disposizioni del capitolo 1.

Cpv. 3

Questo capoverso precisa che le disposizioni specifiche di altre leggi federali o delle relative ordinanze che divergono dall'OCEP prevalgono su quest'ultima.

¹⁰ RS 172.021

Sezione 2: Autorizzazione d'esercizio

Art. 2 Requisiti delle piattaforme

Cpv. 1

Il capoverso disciplina le condizioni per ottenere un'autorizzazione d'esercizio di una piattaforma secondo la LCEG. Quest'ultima prevede in particolare anche i requisiti che le piattaforme devono soddisfare in materia di protezione e sicurezza dei dati (cfr. articolo 27 seg. LCEG). Oltre ai requisiti della LCEG, le piattaforme devono adempiere ulteriori regole esposte in seguito.

Lett. a

Alla luce delle disposizioni in materia di protezione dei dati (art. 8 cpv. 1 della legge federale del 25 settembre 2020¹¹ sulla protezione dei dati [LPD]) e anche al fine di conservare la fiducia della popolazione nella giustizia, le piattaforme devono proteggere i documenti salvati da accessi e modifiche non autorizzati mediante misure tecniche quali il criptaggio, il controllo e la verbalizzazione degli accessi e dei tentativi di accesso. Per quanto riguarda il criptaggio durante la trasmissione, si vedano i commenti alla lettera b.

Inoltre, le piattaforme devono essere in grado di respingere attacchi quali tentativi di hacking o manipolazioni. Senza tali meccanismi di difesa, non sarebbe possibile garantire la protezione dei dati e il diritto in materia di sicurezza delle informazioni. Le piattaforme devono essere in grado di riconoscere e bloccare potenziali attacchi al fine di garantire la confidenzialità (nessun accesso per persone non autorizzate) e l'integrità dei dati (nessuna modifica non autorizzata).

Lett. b

Il criptaggio dei dati deve rispettare gli standard dell'Amministrazione federale. Ciò significa che per proteggere i dati durante la trasmissione e il salvataggio devono essere utilizzati algoritmi come AES-256 o metodi analoghi o più recenti. È così possibile garantire che la comunicazione elettronica in ambito giudiziario rispetti requisiti di sicurezza elevati e compatibili con gli standard internazionali.

Le piattaforme devono anche essere in grado di garantire comunicazioni secondo gli standard dell'Amministrazione federale in materia di trasmissione sicura. Di fatto si tratta di protocolli quali HTTPS o TLS, che garantiscono una trasmissione sicura dei dati. Una panoramica di queste specifiche è disponibile all'indirizzo: bk.admin.ch > Trasformazione digitale e governance delle TIC > Direttive.

¹¹ RS 235.1

Lett. c

Le piattaforme devono poter ricevere e trasmettere documenti di dimensioni fino a 2 gigabyte, limite sufficiente nella maggior parte dei casi. I documenti di testo e i fogli di calcolo difficilmente raggiungono queste dimensioni, a meno che non includano contenuti multimediali. Anche le foto scattate con i cellulari attuali difficilmente raggiungono questo limite. Solo le fotocamere digitali attuali con l'impostazione di salvataggio delle foto in formato raw e i video possono superare il limite di 2 gigabyte.

L'attuale comunicazione elettronica in ambito giudiziario mediante e-mail limita ogni invio a una dimensione massima di 15 megabyte. Pertanto, i 2 gigabyte per documento sono molto più generosi e appaiono sufficienti. Inoltre, i documenti possono essere facilmente suddivisi in più parti, in particolare i file video. Per suddividere altri formati di file potrebbe essere necessario ricorrere a un software di archiviazione come Zip o 7-Zip.

I gestori delle piattaforme possono accettare il trasferimento di documenti più voluminosi. Le copie del contenuto di computer o telefoni cellulari sequestrati superano di norma il limite di 2 gigabyte. I dispositivi sequestrati vengono ad esempio analizzati dai laboratori forensi e poi trasmessi alle competenti autorità di perseguimento penale. I volumi di dati trasmessi possono raggiungere centinaia di gigabyte o addirittura terabyte.

La trasmissione standard mediante le piattaforme non è progettata per questi casi specifici, ma è comunque necessario poter trasmettere anche questi dati. Affinché tali copie e tali dati possano essere trasmessi senza essere suddivisi in più parti, i gestori delle piattaforme possono consentire a determinati utenti di trasmettere documenti più voluminosi.

Il consenso può essere dato verbalmente, per scritto o facendo salve clausole di esclusioni di responsabilità. Di norma sarà dato per scritto ma in casi urgenti può in un primo momento essere dato verbalmente.

In alternativa è possibile consentire all'autorità l'accesso a un'applicazione forense, affinché possa consultare gli allegati.

Lett. d

Le piattaforme devono permettere agli utenti di cancellare in qualsiasi momento i documenti presenti sul loro profilo. Questa funzione è importante in particolare per le persone che utilizzano un'interfaccia utente secondo l'articolo 19 capoverso 1 LCEG e che desiderano fare ordine nella casella di entrata/uscita. La cancellazione di un documento dal profilo non necessariamente ha effetto sulla piattaforma. Dal punto di vista tecnico, la cancellazione avviene come segue: un documento trasmesso, ad esempio, da un'autorità a più partecipanti al procedimento viene salvato una sola volta sulla piattaforma centrale e ne è consentito l'accesso ai rispettivi destinatari come pure all'autorità che lo ha inviato. Fintanto che altre parti possono accedervi, se

una parte cancella un documento, ciò comporta comporta solo la revoca del suo diritto. Tale parte non potrà più accedere al documento. La cancellazione fisica avviene solo dopo che tutti i diritti di accesso sono stati revocati (automaticamente o manualmente).

Cpv. 2

Il capoverso 2 precisa che il DFGP concretizzerà i requisiti funzionali e d'esercizio delle piattaforme, comprese le interfacce, nel quadro della competenza esecutiva del Consiglio federale. La portata esatta della delega al DFGP sarà definita nel corso della procedura di consultazione.

Le piattaforme devono fornire interfacce che consentano ad altri programmi di comunicare con esse. In questo modo, i terzi possono collegare le loro applicazioni specifiche (ad es. software di gestione aziendale) alla piattaforma senza costi aggiuntivi, trasmettere i documenti alla piattaforma e consultarli in via automatica. Questa funzione, particolarmente importante per gli utenti professionali che trasmettono e consultano giornalmente documenti, contribuisce a ottimizzare i processi e a semplificare la comunicazione con le autorità in ambito giudiziario. L'accettazione delle piattaforme è accresciuta dal fatto che le interfacce della piattaforma centrale e della piattaforma secondo l'articolo 6a capoverso 2 PA sono gratuite.

Per garantire una comunicazione elettronica in ambito giudiziario sicura e interoperabile, il DFGP emana prescrizioni tecniche in materia di protocolli (come RESTful APIs, SOAP o standard di sicurezza specifici come TLS 1.3), requisiti in materia di prestazioni (ad es. tempi di risposta) o direttive di integrazione. Queste misure garantiscono che le interfacce siano robuste, scalabili e resistenti ai guasti. Il DFGP determina anche il formato dei dati durante la trasmissione, ad esempio XML o JSON.

Le modifiche del quadro tecnico delle interfacce e altre modifiche dell'avamprogetto saranno apportate in accordo con tutti i gestori delle piattaforme secondo la LCEG (p. es. mediante una consultazione informale). La piattaforma centrale deve fornire le sue interfacce a titolo gratuito conformemente all'articolo 32 capoverso 1 LCEG, secondo cui l'ente pubblico riscuote emolumenti soltanto dalle autorità. A tal proposito, il numero 4.2.2.4 del messaggio del 15 febbraio 2023¹² sulla legge federale concernente le piattaforme per la comunicazione elettronica nella giustizia (LCEG) sottolinea esplicitamente l'importanza di non creare alcuna barriera pecuniaria all'uso della piattaforma.

Il DFGP valuterà se sia opportuno pubblicare un promemoria con le condizioni dell'autorizzazione e gli elementi da verificare, per aiutare i gestori delle piattaforme a redigere la domanda e a raccogliere i documenti necessari.

¹² FF 2023 679

Art. 3 Procedura di autorizzazione

Cpv. 1 e 2

Il DFGP è competente per la procedura di autorizzazione delle piattaforme secondo la LCEG. Questa soluzione si è dimostrata efficace nella pratica, perché già oggi il DFGP è competente per autorizzare le piattaforme di trasmissione ed è inoltre il dipartimento responsabile dei lavori legislativi condotti nell'ambito della LCEG. Chi desidera gestire una piattaforma secondo la LCEG deve presentare una domanda presso il DFGP, in cui attesta l'adempimento di tutte le condizioni. In particolare, dovrà presentare i seguenti documenti:

- un piano che attesta l'adempimento di tutte le condizioni d'autorizzazione;
- i documenti relativi alle specifiche tecniche della piattaforma;
- i certificati di sicurezza che provano il rispetto dei requisiti legali; e
- i dati sulla struttura dell'impresa del richiedente.

Queste condizioni servono ad assicurare che l'autorizzazione sia rilasciata alle sole piattaforme che soddisfano gli elevati standard della LCEG e garantiscono così la protezione degli utenti e l'integrità della comunicazione elettronica in ambito giudiziario.

Cpv. 3

Il DFGP ha l'obbligo di disciplinare i dettagli della procedura di autorizzazione in un'ordinanza dipartimentale e di stabilire in particolare quali dati devono essere forniti con la domanda. Il contenuto dell'ordinanza dipartimentale sarà elaborato nel corso della procedura di consultazione.

Cpv. 4

Considerati i progressi tecnologici e la costante evoluzione delle minacce nel settore digitale, l'autorità preposta all'autorizzazione deve verificare con regolarità l'adempimento delle condizioni di autorizzazione da parte di una piattaforma e, se tale non è più il caso, revocare eventualmente in ultima ratio l'autorizzazione concessa. Questa disposizione è necessaria per garantire la protezione degli utenti, l'integrità della comunicazione elettronica in ambito giudiziario e la fiducia degli utenti. La revoca non va tuttavia ordinata con leggerezza. Il DFGP può in particolare adottare una misura più mite fissando un termine per ripristinare la situazione legale, con la comminatoria che l'autorizzazione sarà revocata se il termine scade infruttuoso.

Se l'autorizzazione di una piattaforma è revocata in ultima ratio, i Cantoni che la utilizzavano devono immediatamente collegarsi a un'altra piattaforma, per non interrompere la comunicazione elettronica con le loro autorità. La Confederazione non è al momento a conoscenza di alcuna iniziativa per sviluppare ulteriori piattaforme secondo l'articolo 4 LCEG.

Cpv. 5

Per l'esame della domanda e il rilascio dell'autorizzazione è fatturata una tariffa oraria di 250 franchi. Si applicano inoltre le disposizioni dell'ordinanza generale dell'8 settembre 2004¹³ sugli emolumenti (OgeEm).

Sezione 3: Documenti, ricevute e sigilli

Art. 4 Formato dei documenti

Cpv. 1

Questa disposizione prevede che le autorità, in particolare i tribunali, i pubblici ministeri e le autorità amministrative di tutti i livelli, indipendentemente dal fatto che dirigano una procedura o che vi partecipino in un'altra funzione, trasmettano i loro documenti nel formato PDF/A. I documenti interessati sono quelli creati dalle autorità stesse, come ad esempio sentenze, decisioni ed eventuali lettere di accompagnamento.

Alle autorità è imposto l'utilizzo di un formato idoneo per l'archiviazione, ossia il formato PDF/A (in tutte le sue versioni), perché si prevede che le autorità renderanno automatico l'invio dei loro documenti e l'apposizione del sigillo (cfr. art. 22 cpv. 2 LCEG).

Gli altri partecipanti alla procedura (escluse le autorità che la dirigono o che vi partecipano) possono trasmettere i loro atti alle autorità nel formato PDF o PDF/A. Nel caso degli altri partecipanti alla procedura non è possibile partire dal presupposto di un'automazione del processo, poiché l'uso della piattaforma per le comunicazioni elettroniche è aperto a tutti, non solo agli utenti professionali. Il formato PDF/A non deve rappresentare un ostacolo per le persone che raramente contattano tribunali o altre autorità.

Cpv. 2

Gli allegati possono essere trasmessi in qualsiasi formato. Tuttavia, nella misura del possibile, dovranno essere trasmessi nel formato PDF o PDF/A, poiché si tratta del formato più adatto a garantire interoperabilità e riproducibilità massime in un contesto molto eterogeneo con diversi attori (tribunali, pubblici ministeri, autorità amministrative, avvocati). In linea di principio, il rischio che un'autorità non riesca ad aprire e utilizzare un allegato è a carico del mittente, che deve pertanto domandarsi (p. es. a causa dei suoi obblighi di diligenza di avvocato) se l'allegato potrà essere aperto dal tribunale o dall'autorità che lo riceve. È possibile trasmettere gli allegati direttamente

¹³ RS 172.041.1

alla piattaforma, senza dapprima convertirli in un formato archiviabile come ZIP o 7-Zip.

Cpv. 3

Il capoverso 3 elenca i formati che i tribunali e le autorità devono imperativamente poter aprire. Si evita così che tribunali e autorità possano chiedere, in base al capoverso 4, il rinvio degli allegati in un determinato formato (p. es. PDF). La lista è volutamente concisa e prende in considerazione formati che possono aperti da sistemi e dispositivi comuni (Windows, macOS, Linux, tablet, smartphone). Un determinato formato può a volte avere diverse versioni; è ad esempio il caso del formato PDF/A, ulteriormente essere suddiviso nelle versioni PDF/A1 –PDF/A4. Quando si cita il formato PDF/A, sono incluse anche tutte le sue versioni comuni.

Cpv. 4 e 5

Le autorità fissano ai partecipanti alla procedura un termine adeguato per il rinvio di un allegato che non hanno potuto aprire. Possono chiedere al mittente di rinviare l'allegato in un formato specifico o di consentire loro l'accesso in modo adeguato. In via di principio è anche possibile che singoli tribunali e autorità stabiliscano (p. es. in un promemoria) quali formati possono utilizzare. Devono tuttavia rispettare lo standard minimo stabilito dal capoverso 3. Disposizioni analoghe figurano già nel CPC e nel CPP (cfr. art. 132 cpv. 2 CPC e art. 110 cpv. 4 CPP).

Il motivo per cui un tribunale o un'autorità non è in grado di aprire l'allegato non è importante. Il software necessario per la lettura di un determinato formato può non essere installato o, in determinati casi, le norme relative alla sicurezza dei dati possono imporre ai tribunali e alle autorità di aprire solo formati specifici. Questa disposizione non significa tuttavia che tribunali e autorità possono sistematicamente chiedere che gli allegati siano loro trasmessi in formato PDF o PDF/A.

Dati strutturati

Nella pratica è necessario poter trasmettere dati strutturati. Poiché non sono prescritti formati per la trasmissione di allegati, i dati strutturati possono sempre essere trasmessi come allegato.

Tuttavia, a causa della necessità di apporre un sigillo prevista dall'articolo 22 capoverso 2 LCEG, i dati strutturati non possono essere trasmessi come documenti perché non può esservi apposto un sigillo. I processi di trasmissione tramite una piattaforma saranno probabilmente automatizzati in particolare per quanto riguarda le autorità, in modo tale che queste ultime possano allestire una lettera d'accompagnamento corredata di un sigillo (ai sensi del cpv. 1) e trasmettere i dati strutturati come allegato.

Token

I token o altre credenziali possono essere trasmessi come allegati in un documento separato, visto che non esistono prescrizioni sul formato degli allegati. Inoltre, i token possono essere trasmessi in forma testuale, come codice QR o in altro modo nei documenti delle autorità o delle altre parti al procedimento (ai sensi del cpv. 1).

Soluzione rifiutata: successiva richiesta del formato originale

È stata esaminata la possibilità per le autorità di chiedere per ragioni oggettive che i documenti siano loro trasmessi nel formato d'origine. Questa eventualità potrebbe essere ipotizzabile, ad esempio, quando una parte converte fogli di calcolo complessi in un PDF che poi trasmette come allegato. All'autorità il documento nel formato originale può essere utile, poiché le dà accesso a tutte le formule e i collegamenti che facilitano il trattamento e la verifica del documento. Questa soluzione è stata rifiutata per diverse ragioni, legate anzitutto alla certezza del diritto: la parte che invia un atto deve poter essere sicura di aver rispettato i termini stabiliti, che l'invio sia avvenuto conformemente alla legge e che non vi sia alcun ulteriore onere. Inoltre, il formato originale può contenere informazioni che la parte non vuole trasmettere. La conversione in PDF ha il vantaggio di convertire solo la parte visibile, tralasciando le versioni precedenti e i metadati che risultano dal trattamento del documento. Inoltre, la conversione dei documenti PDF nel formato di origine è in linea di principio possibile ed è abbastanza semplice per i documenti di solo testo. Invece, nel caso di fogli di calcoli sotto forma di tabelle, vengono convertiti solo i numeri ma non le formule.

Soluzione rifiutata: elenco esaustivo dei formati consentiti

È stata inoltre presa in considerazione la possibilità di prevedere un elenco esaustivo dei formati consentiti per gli allegati. Esistono dei formati standard che in linea di principio possono essere aperti da tutti i sistemi e i dispositivi (Windows, macOS, Linux, tablet, smartphone). Le discussioni in seno al gruppo di accompagnamento hanno tuttavia mostrato che un elenco del genere non sarebbe opportuno. Sarebbe infatti necessario chiarire come trattare i formati che non figurano nell'elenco e spiegare perché determinati formati sono ammessi e altri formati equivalenti no. Inoltre, sarebbe troppo gravoso in particolare per gli utenti non professionisti documentarsi sui formati ammessi e ciò ridurrebbe l'attrattiva della piattaforma.

Art. 5 Ricevute

Cpv. 1

L'articolo 22 capoverso 4 LCEG potrebbe suscitare l'impressione che per ogni documento trasmesso debba essere rilasciata una ricevuta. Il capoverso 1 precisa che la piattaforma rilascia una sola ricevuta anche se più documenti sono presentati insieme.

Cpv. 2

Questo capoverso precisa le indicazioni minime che devono figurare sulle ricevute: il tipo di ricevuta, il nome del mittente e quello del destinatario, compreso l'indirizzo sulla piattaforma. Se il mittente agisce per conto di un'organizzazione, va indicato anche il nome di quest'ultima. Inoltre, la ricevuta di consegna deve indicare il nome, le dimensioni e il valore hash di ogni documento trasmesso. Sono indicati anche il nome e le dimensioni di quei documenti non trasmessi a causa del controllo antivirus.

Anche l'ora di trasmissione è un elemento importante. L'ora indicata sulla ricevuta corrisponde al momento dell'effettiva esecuzione dell'atto e non all'inizio o alla fine dei termini legali o procedurali. Se, ad esempio, il primo accesso a una notificazione è effettuato di domenica, tale momento viene riportato sulla ricevuta ed è determinante per la prova della data di notificazione (cfr. art. 20 cpv. 2^{ter} seg. PA nella versione della LCEG e le analoghe disposizioni parallele). Il momento della trasmissione deve essere indicato anche sulla ricevuta di mancato accesso.

Quando una persona invia o consulta un documento in virtù di un diritto concessole, non è il suo nome che figura sulla ricevuta ma il nome della persona per conto della quale agisce.

Le dimensioni e il valore hash dell'intero invio non vanno sommati, ma indicati separatamente per ogni documento trasmesso. Nel caso in cui diversi file sono trasmessi in un file zip, sulla ricevuta vanno indicati la dimensione e il valore hash di quest'ultimo e non dei documenti in esso contenuti.

Se il controllo antivirus rileva software nocivi in uno o più documenti, questi ultimi non sono trasmessi ai destinatari (cfr. art. 14 cpv. 5) ma sono comunque elencati sulla ricevuta con solo il nome e le dimensioni. In questi casi è possibile omettere il valore hash, poiché tali documenti non vengono trasmessi e non è quindi possibile verificarne l'integrità.

Non occorre indicare il nome della piattaforma sulla ricevuta perché esso risulta dal sigillo apposto dalla piattaforma.

L'avamprogetto rinuncia a prescrivere che le ricevute debbano contenere anche indicazioni relative al successo, all'eventuale ritardo o all'interruzione della trasmissione. Ai sensi dell'articolo 22 capoverso 4 lettera a LCEG, una ricevuta di consegna viene emessa non appena il documento è stato trasmesso. Di conseguenza, prima che la trasmissione abbia avuto successo non può essere rilasciata alcuna ricevuta.

Cpv. 3-5

Da un lato le ricevute devono essere facilmente comprensibili, affidabili e avere valore probatorio per poter essere utilizzate nella pratica; dall'altro devono contenere dati leggibili elettronicamente, per consentire registrazioni automatiche nei sistemi degli utenti. Poiché è difficile soddisfare queste due esigenze con una sola ricevuta, è pre-

visto che le piattaforme possano rilasciare due ricevute separate. Quando una piattaforma rilascia una ricevuta leggibile elettronicamente e un'altra leggibile dall'essere umano, solo quest'ultima dovrà essere in formato PDF/A e corredata di sigillo elettronico e marca temporale.

Art. 6 Apposizione di un sigillo da parte dell'autorità mittente

Secondo l'articolo 22 capoverso 2 LCEG l'autorità che dirige il procedimento e quelle che vi partecipano sono tenute ad apporre un sigillo e una marca temporale sulle loro comunicazioni. Non necessitano di un ulteriore sigillo solo i documenti già muniti di firma elettronica qualificata, oppure di sigillo elettronico regolamentato con marca temporale elettronica qualificata.

Le piattaforme devono verificare che le autorità abbiano apposto il sigillo e la marca temporale necessari. Se manca un sigillo o una marca temporale, la piattaforma non accetta i documenti (cfr. art. 22 cpv. 2 secondo periodo LCEG).

Art. 7 Apposizione di un sigillo da parte della piattaforma

Lo scopo principale del sigillo è di proteggere l'integrità dei documenti e di renderla verificabile. L'apposizione del sigillo non impedisce la manipolazione di un documento, ma consente di verificare se vi è stata una tale manipolazione.

Esistono diversi modi per apporre un sigillo: da un lato può essere apposto direttamente sul documento stesso; tuttavia, questo metodo non è possibile per tutti i tipi di file. Dall'altro, il sistema può calcolare il valore hash del documento da sigillare e inserirlo in un altro documento, anch'esso, da sigillare. Il valore hash che figura nel documento sigillato consente alla persona competente di verificare che l'altro documento non è stato modificato. Entrambe le procedure portano allo stesso risultato.

Secondo gli avvocati le piattaforme non devono modificare i documenti trasmessi. È stato espresso il timore che le autorità o altri partecipanti alla procedura non possano più stabilire quale versione del documento è stata presentata tempestivamente. Se il sigillo è apposto direttamente sui documenti trasmessi, questi subiscono una modifica; invece, se è apposto su un documento separato, i documenti trasmessi rimangono immutati.

Cpv. 1

La presente disposizione disciplina l'apposizione del sigillo qualora più documenti siano trasmessi contemporaneamente. Potrebbe essere il caso normale poiché un atto scritto è spesso corredato di allegati. In tal caso la piattaforma appone il sigillo e la marca temporale su un documento separato. In tal modo si tiene conto delle preoccupazioni degli avvocati e del fatto che gli allegati, conformemente all'articolo 4 capoverso 2, possono essere trasmessi in qualsiasi formato.

Cpv. 2

Se un documento reca già un sigillo, non occorre apporre un altro, poiché il primo è sufficiente per provare l'integrità del documento.

Consultazione degli atti

Gli articoli 6 e 7 AP-OCEP non si applicano alla consultazione degli atti, poiché in questo caso non occorre alcun sigillo o marca temporale (art. 22 LCEG e *contrario*). L'obbligo di apporre un sigillo (art. 22 cpv. 2 e 3 LCEG) si applica solo alle notificazioni e agli atti scritti (cfr. p. es. art. 130 segg. e 136 segg. CPC), ovvero agli atti con cui le autorità fissano termini alle parti o mediante i quali le parti a un procedimento presentano nuovi documenti. Per questa ragione, è necessario apporre un sigillo che garantisca l'integrità dei documenti presentati e una marca temporale che confermi il rispetto del termine.

Il legislatore non ha mai voluto l'obbligo di apporre un sigillo sugli atti da consultare. In caso di consultazione degli atti, non è presentato alcun documento nuovo ma una parte è autorizzata a consultare documenti già esistenti. Non è quindi necessario alcun sigillo. Nemmeno occorre marca temporale, considerato che l'autorità, concedendo la consultazione degli atti, determina la durata di accesso agli atti medesimi. Il momento in cui la parte consulta gli atti nell'arco del termine stabilito non ha alcuna importanza.

Sezione 4 Autenticazione, profili, interfacce e diritti

Art. 8 Autenticazione degli utenti

Cpv. 1

È previsto di consentire l'autenticazione soltanto tramite AGOV. Secondo l'articolo 20 capoverso 2 LCEG il Consiglio federale stabilisce i mezzi d'identificazione elettronici che possono essere impiegati a tale scopo. AGOV risponde alle esigenze poiché fornisce identità elettroniche native, registrate nel self-service per gli utenti finali. Esso costituisce inoltre un sistema federato con altre identità elettroniche riconosciute che possono essere impiegate come credenziali autonome per l'accesso¹⁴. AGOV adempie le condizioni secondo l'articolo 20 capoverso 2 LCEG, poiché può fornire identità elettroniche in seguito a una procedura di controllo e federare identità elettroniche riconosciute.

Uno dei vantaggi di AGOV è che ogni persona munita di un passaporto o di una carta d'identità validi può ottenere un login AGOV di livello 300 (cosiddetta universalità). Quindi anche le persone all'estero sprovviste di un passaporto o una carta d'identità svizzeri possono partecipare alla comunicazione elettronica in ambito giudiziario in

¹⁴ Cfr. «Informazioni per le autorità» sul sito www.agov.admin.ch > Per le autorità

Svizzera. Ciò riguarda in particolare gli avvocati dell'UE che possono rappresentare le parti anche dinanzi ai tribunali svizzeri e utilizzare la piattaforma per la comunicazione elettronica senza dover designare un recapito in Svizzera (p. es. art. 11b cpv. 1 PA e art. 39 cpv. 3 della legge federale del 17 giugno 2005¹⁵ sul Tribunale federale [LTF] nella versione della LCEG).

Chi dispone di un mezzo d'identificazione elettronico per persone fisiche (e-ID), può creare un login AGOV di livello 300 senza fornire ulteriori prove. Inoltre, l'e-ID svizzera dovrà essere accettata come mezzo d'identificazione conformemente all'articolo 24 della legge federale del 20 dicembre 2024¹⁶ sul mezzo d'identificazione elettronico e altri mezzi di autenticazione elettronici (legge sull'Id-e, LIdE). Non è pertanto necessario citare espressamente l'e-ID nell'ordinanza.

Potrebbero essere ammessi anche altri documenti di identità elettronici, ma dovrebbero essere integrati nella piattaforma centrale ed eventualmente anche in altre piattaforme. Ciò aumenterebbe tuttavia la complessità del sistema e comporterebbe ulteriori costi. Poiché in via di principio ogni persona può ottenere un login AGOV di livello 300, non sono necessari ulteriori mezzi d'identificazione.

Cpv. 2

I Cantoni che usano altre piattaforme secondo l'articolo 4 LCEG devono utilizzare AGOV come servizio di autenticazione, o altri servizi equivalenti sotto il profilo qualitativo. Ai sensi della LIdE, devono inoltre accettare l'e-ID svizzera come mezzo di autenticazione.

Cpv. 3

Secondo l'articolo 21 LCEG, gli utenti che utilizzano una piattaforma mediante l'applicazione di un'autorità non sono tenuti ad autenticarsi sulla piattaforma se il gestore della piattaforma li ha autorizzati ad accedervi direttamente. Ci vorrà del tempo prima che tutte le autorità interessate colleghino le loro applicazioni alla piattaforma mediante un'interfaccia. È inoltre ipotizzabile che le piccole autorità che comunicano solo sporadicamente tramite la piattaforma continuino a utilizzare il login web della piattaforma. In questi casi è opportuno che i gestori delle piattaforme possano accettare anche altri fornitori di identità, ad esempio cantonali, purché questi ultimi offrano un livello di protezione adeguato. I gestori non hanno l'obbligo di accettare questi altri fornitori d'identità.

¹⁵ RS 173.110

¹⁶ FF 2025 20

Cpv. 1

Le piattaforme devono consentire la creazione di più profili in un conto utente. Con un solo conto gli utenti potranno così comunicare in ruoli diversi. Una persona fisica può ad esempio essere obbligata a utilizzare la piattaforma in quanto avvocato, ma potrebbe volerla utilizzare anche per uso privato, indipendentemente dall'obbligo legato alla sua professione. Se questa persona è anche membro del consiglio di amministrazione di una o più società anonime e membro del comitato direttivo di un'associazione locale potrà cambiare profilo e inviare e ricevere messaggi nei diversi ruoli.

Cpv. 2-4

Per evitare nella misura del possibile errori di notificazione, i singoli profili devono contenere alcune indicazioni minime.

Il profilo di un'autorità deve contenere le seguenti indicazioni minime: il nome dell'autorità, il suo indirizzo postale e il nome del sigillo. Mentre i primi due servono a identificare correttamente l'autorità, il nome del sigillo ha uno scopo diverso. Considerato che le autorità sono tenute ad apporre un sigillo elettronico sui documenti trasmessi, il nome del sigillo nel profilo consentirà alle piattaforme di verificare che almeno un documento sia munito del sigillo corretto (cfr. art. 22 cpv. 2 LCEG).

Nei certificati il campo «nome comune» (*common name, CN*) designa il sigillo. Il CN è un elemento centrale dei certificati X.509 e funge da identificativo primario per il titolare del certificato. Il suo scopo e utilizzo variano a seconda del tipo di certificato. Nei certificati SSL/TLS, il CN deve corrispondere al nome del dominio del sito Internet. Nel caso di documenti muniti di sigillo, il CN contiene il nome dell'organizzazione.

Le persone fisiche devono indicare nome, cognome, indirizzo postale e data di nascita; mentre le organizzazioni il loro nome o la ditta e l'indirizzo postale. Queste indicazioni escludono di fatto errori nella notificazione.

Quando una persona soggetta all'obbligo di utilizzare la piattaforma crea un profilo, indicherà l'eventuale organizzazione di appartenenza e l'indirizzo postale professionale. È inoltre usuale per gli avvocati indicare anche il nome del loro studio legale e in particolare utilizzare la carta intestata per le lettere.

Le organizzazioni di cui ai capoversi 3 e 4 possono essere persone giuridiche, ma anche altre forme organizzative come società semplici o collettive. In particolare, gli studi legali sono spesso organizzati in società semplici o collettive.

Se il profilo appartiene a una persona fisica, AGOV ne conferma l'identità. Non esiste una procedura simile per le organizzazioni: il loro nome e il diritto di rappresentanza non sono verificati. Tuttavia, per ogni organizzazione viene sempre registrato il nome di una persona responsabile, che coincide con il nome della persona fisica che ha creato il conto dell'organizzazione. Il nome può essere modificato in seguito, con il

consenso della nuova persona responsabile. Nel quadro della procedura le autorità dovranno verificare, come fanno già, l'eventuale esistenza dell'organizzazione e la validità della procura.

Art. 10 Interfaccia

L'accesso mediante l'interfaccia avviene tramite un token API, ovvero una chiave alfanumerica sicura. Il token API funziona come una password digitale generata appositamente per la comunicazione automatizzata tra applicazioni o servizi, senza che sia necessario condividere dati sensibili dell'utente. Questi token vengono spesso utilizzati per garantire un accesso sicuro e controllato.

Creare un token di questo tipo equivale a concedere diritti a un altro utente. Occorre pertanto confermare i token API regolarmente, altrimenti vengono automaticamente cancellati o bloccati.

Art. 11 Conferma e revoca di diritti

Mediante il sistema di trasferimento dei diritti, un utente può consentire a terze persone di inviare e ricevere documenti in suo nome (cfr. art. 24 LCEG). Considerate le conseguenze estese che potrebbero derivarne, gli utenti devono verificare questi diritti almeno una volta all'anno.

Se una persona non reagisce confermando o rifiutando i diritti ricevuti, le piattaforme li revocano automaticamente tre mesi dopo l'ultima richiesta di conferma.

Gli utenti interessati, ovvero quelli che hanno concesso i diritti e quelli che li hanno ricevuti sono informati della revoca automatica. Se la revoca è indesiderata, le persone interessate possono fare quanto necessario affinché i diritti siano ripristinati. Ad esempio, la persona alla quale erano stati concessi i diritti può contattare la persona che glieli aveva concessi e chiedere che le siano nuovamente attribuiti.

Sezione 5 Protezione dei dati, sicurezza dei dati e controllo antivirus

Art. 12 Durata massima di conservazione dei documenti e delle ricevute

Cpv. 1

L'articolo 22 capoverso 5 LCEG prevede un termine minimo di 90 giorni durante il quale le piattaforme non possono distruggere automaticamente i documenti trasmessi e le ricevute rilasciate. La presente disposizione fissa a sei mesi il termine massimo di

conservazione. Sono fatti salvi i termini di conservazione di cui all'articolo 21 dell'ordinanza del 15 novembre 2017¹⁷ sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT).

I documenti non devono essere distrutti esattamente alla scadenza dei sei mesi successivi alla loro trasmissione. Le piattaforme, a seconda del loro sovraccarico, hanno qualche ora supplementare per farlo. La distruzione deve tuttavia aver luogo entro 24 ore dalla scadenza dei sei mesi.

Cpv. 2

Nel momento in cui concede la consultazione di determinati atti, l'autorità fissa un termine durante il quale i documenti saranno disponibili. Allo scadere del termine, le piattaforme cancelleranno automaticamente gli atti. Il termine di sei mesi di cui al capoverso 1 non vale in questi casi.

Soluzione rifiutata

È stata anche presa in considerazione la possibilità di far dipendere il termine massimo di conservazione dall'attività o inattività delle parti in un procedimento. Così, se per un determinato periodo non sono trasmessi nuovi documenti o non è effettuato alcun atto, i documenti vengono cancellati. Questa variante è stata scartata perché, per motivi tecnici, le piattaforme non sono in grado di determinare con certezza se il documento trasmesso fa parte di un procedimento esistente o di uno nuovo.

Art. 13 Sicurezza dei dati

L'abuso di informazioni o la perturbazione dei sistemi d'informazione possono pregiudicare gravemente gli interessi essenziali della Svizzera e i diritti delle persone. L'evoluzione verso una società dell'informazione comporta dei rischi sempre più complessi e dinamici. Con la legge del 18 dicembre 2020¹⁸ sulla sicurezza delle informazioni (LSIn), il Parlamento ha creato un quadro giuridico uniforme, fondato su standard riconosciuti in campo internazionale, per gestire e attuare la sicurezza delle informazioni nell'ambito di competenza della Confederazione.

Poiché la Confederazione partecipa sia alla piattaforma centrale che alla piattaforma generale per le procedure amministrative, è opportuno che i requisiti in materia di sicurezza dei dati siano disciplinati secondo LSIn. La Confederazione ha riunito in un solo atto normativo le basi giuridiche più importanti per la sicurezza delle informazioni e dei mezzi informatici della Confederazione. L'obiettivo è quello di raggiungere un li-

¹⁷ RS 780.11

¹⁸ RS 128

vello di sicurezza il più uniforme possibile, che valga anche per le piattaforme secondo la LCEG. L'articolo 13 si applica solo ai Cantoni, poiché le disposizioni della LSIIn sono in ogni caso applicabili alla Confederazione.

Inoltre, l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) esercita la vigilanza in materia di protezione dei dati sulle piattaforme (cfr. art. 27 cpv. 6 LCEG) e pertanto anche l'articolo 8 LPD è applicabile.

Art. 14 Scansione antivirus

Cpv. 1

In base alle regole in materia di protezione e sicurezza dei dati (art. 27 seg. LCEG), le piattaforme devono verificare la presenza di software nocivi nei documenti trasmessi. Per motivi linguistici l'avamprogetto usa le nozioni di «virus» e «scansione antivirus». Queste espressioni indicano in generale i software nocivi e l'individuazione di software nocivi. Maggiore è la dimensione dei documenti trasmessi, maggiori sono le risorse necessarie per eseguire un controllo antivirus. Le piattaforme possono controllare i documenti fino a una dimensione di 64 MB senza cali di prestazioni. Per questo motivo, tale dimensione viene introdotta come valore limite per un controllo antivirus ordinario.

Cpv 2

Quando sono trasmessi documenti le cui dimensioni superano i 64 MB, le piattaforme possono suddividerli in parti da 64 MB che sottopongono a un controllo antivirus. In questo caso sussiste il rischio che un software nocivo sia segmentato all'interno di un documento e che l'antivirus non possa quindi individuarlo correttamente. Per questo motivo, l'avamprogetto prevede di contrassegnare questi documenti, per avvisare il destinatario e permettergli di trattarli con la necessaria prudenza.

Cpv. 3

È anche possibile che documenti contenenti software nocivi vengano trasmessi intenzionalmente, ad esempio nel caso in cui le autorità di perseguimento penale sequestrano computer o dispositivi mobili. I software nocivi contenuti in questi dispositivi fanno quindi parte dei mezzi di prova e non devono essere modificati. L'avamprogetto prevede pertanto che il gestore di una piattaforma, su domanda dell'utente, possa rinunciare alla scansione antivirus.

Il consenso da parte del gestore può essere dato verbalmente o per scritto o facendo salve le esclusioni di responsabilità, per esempio. Può essere concesso per una sola volta o per un periodo di tempo determinato o indeterminato. Di norma sarà dato per scritto o in un primo momento verbalmente in casi urgenti.

Cpv. 4

I documenti non sottoposti a una scansione antivirus o sottoposti a una scansione limitata secondo il capoverso 2 devono essere contrassegnati in modo speciale dalla piattaforma, affinché i destinatari possano trattarli con la diligenza necessaria.

Cpv. 5

Se constata che uno o più documenti trasmessi contengono software nocivi, la piattaforma rifiuta di trasmetterli ai destinatari. Se vi sono diversi documenti da trasmettere insieme, essa consegnerà ai destinatari soltanto quelli non infettati. A fini probatori, le ricevute secondo l'articolo 11 contengono un elenco dei documenti non trasmessi e le loro dimensioni. Inoltre, il vigente diritto processuale disciplina già come trattare gli atti viziati (cfr. art. 132 cpv. 1 CPC). Di norma, sarà fissato un congruo termine per l'invio dei documenti mancanti.

Nella pratica, la presente norma dovrebbe essere applicata solo raramente, poiché gran parte dei documenti è trasmessa nei formati PDF o PDF/A. Quando un nuovo documento PDF è creato con strumenti di conversione legittimi, ad esempio mediante la funzione «salva con nome» o «esporta» di Microsoft Office o con la stampa di un documento PDF, ad esempio con il software PDF24, il processo di conversione trasforma essenzialmente il contenuto visibile in un formato statico e rimuove gli elementi eseguibili che potrebbero contenere software nocivi. Non si può comunque escludere l'esistenza di software nocivi nel sistema operativo o nei driver della stampante PDF né che vengano trasferiti nei documenti PDF durante il processo di conversione. Non si è tuttavia a conoscenza di siffatti software nocivi.

Sezione 6 *Emolumento per l'utilizzo della piattaforma centrale*

Secondo l'articolo 32 LCEG, l'ente di diritto pubblico riscuote annualmente dalle autorità emolumenti per l'utilizzo della piattaforma; il Consiglio federale può prevedere importi forfettari. Il messaggio spiega, nei commenti all'articolo 32 LCEG, che il termine «forfettario» non si riferisce solo agli emolumenti stessi, ma anche alla fatturazione. Al fine di semplificare il conteggio, il Consiglio federale può prevedere che gli emolumenti siano riscossi complessivamente dai Cantoni e dalla Confederazione, invece che da ogni singola autorità.

Art. 15 *Calcolo dell'emolumento*

Cpv. 1

La disposizione costituisce la base di calcolo dell'importo complessivo dell'emolumento annuale. Quest'ultimo deve coprire le spese di esercizio e di sviluppo della piattaforma centrale (principio di copertura dei costi); può anche comprendere una riserva che non deve superare il 10 per cento delle spese di esercizio annuali. Essa serve per garantire la liquidità dell'ente di diritto pubblico (p. es. per garantire i flussi di pagamento, spese improvvise e picchi di finanziamento a breve termine). Si tratta di

una riserva limitata e non di un margine di profitto. Dal calcolo dell'emolumento complessivo occorre inoltre dedurre le entrate provenienti dai Cantoni che non sono membri dell'ente e che pagano le prestazioni alle quali fanno ricorso. In tal modo si evita che i membri finanzino spese già coperte da terzi non membri e quindi un pagamento a doppio.

Cpv. 2

Il DFGP fissa ogni tre anni l'importo dell'emolumento annuale sulla base della pianificazione finanziaria dell'ente di diritto pubblico; si accrescono così le possibilità pianificatorie, si riduce l'onere amministrativo (la tariffa e l'emolumento non sono adeguati ogni anno) e si tiene conto della copertura delle spese.

L'emolumento è fissato in funzione dei parametri concreti della pianificazione (budget/pianificazione pluriennale, roadmap d'investimento e di sviluppo, calcolo aziendale). Questi parametri rispondono ai requisiti di oggettività e documentazione su cui si basa la decisione del DFGP in materia di emolumenti. Nel concreto l'ente di diritto pubblico invia ogni anno una documentazione aggiornata al DFGP che ogni tre anni fissa l'emolumento con una decisione formale.

Cpv. 3

Se, durante il periodo di cui al capoverso 2, constata che l'emolumento non copre le spese di esercizio e di sviluppo o che la riserva eccede il limite fissato al capoverso 1, il DFGP può adeguare l'emolumento. Il capoverso 3 costituisce un correttivo del calcolo triennale: se le previsioni si rivelano sbagliate o le spese aumentano inaspettatamente e la riserva non basta, il finanziamento deve comunque essere garantito. Lo stesso vale nel caso in cui l'emolumento è troppo alto e la riserva eccede il limite stabilito.

Soluzione rifiutata: ripartizione delle spese per l'istituzione della piattaforma centrale

Il Consiglio federale parte dal presupposto che l'insieme della LCEG potrà entrare in vigore soltanto quando sarà terminata l'istituzione della piattaforma centrale, ma non prima. Per queste ragioni l'avamprogetto non affronta il tema del finanziamento delle spese di istituzione secondo l'articolo 33 LCEG.

Art. 16 Ripartizione dell'emolumento

In caso di riscossione forfettaria degli emolumenti occorre stabilire quale quota debba essere finanziata dalla Confederazione e quale dai Cantoni. Nel messaggio sulla LCEG¹⁹ sono state riportate le statistiche del Tribunale federale per il 2020. Tenendo conto dei procedimenti chiusi dal Ministero pubblico della Confederazione e dai pubblici ministeri cantonali, la quota della Confederazione era pari a circa il

¹⁹ FF 2023 679, pag. 36

2,17 per cento. Nel frattempo, il Tribunale federale ha aggiornato le statistiche per il 2024:

Procedimenti chiusi	Confederazione	Cantoni	Totale
Autorità giudiziarie	15 090	390 899	405 989
Ministero pubblico della Confederazione/ pubblici ministeri cantonali	1 646	550 458	552 104
Totale	16 736	941 357	958 093
Rapporto	1.75 %	98.25 %	100 %

Rispetto al 2020, il numero di procedimenti della Confederazione chiusi è leggermente diminuito. Tuttavia, queste statistiche non includono i procedimenti penali amministrativi della Confederazione e dei Cantoni. Il loro numero è difficile da determinare. Soprattutto nel settore delle imposte federali, in particolare dell'imposta sul valore aggiunto, delle dogane e della Commissione federale delle case da gioco, si dovrebbe aggiungere un numero non trascurabile di procedimenti penali amministrativi.

Per i seguenti motivi è tuttavia appropriato fissare una quota forfettaria della Confederazione più elevata, ovvero al 10 per cento: da un lato, i tribunali cantonali svolgono alcuni lavori preparatori per il Tribunale federale, come la digitalizzazione degli atti e degli allegati cartacei. Dall'altro, la digitalizzazione della giustizia comporta per la Confederazione anche un aumento dell'efficienza che non può essere espresso in cifre. L'importo più elevato tiene conto anche del fatto che, dal punto di vista istituzionale, la legge accorda alla Confederazione un ruolo importante nell'ambito dell'ente. La convenzione sull'ente di diritto pubblico prevede che la Confederazione disponga di due dei sette membri del comitato direttivo, l'organo strategico supremo dell'ente.

Il progetto Justitia 4.0 prevede attualmente costi annuali pari a 10-12 milioni di franchi all'anno per l'esercizio e l'ulteriore sviluppo della piattaforma centrale. Con una partecipazione della Confederazione pari al 10 per cento, ciò corrisponde a un importo compreso tra 1 000 000 e 1 200 000 franchi a carico della Confederazione e tra 9 000 000 e 10 800 000 franchi a carico dei Cantoni.

La quota della Confederazione è ripartita a metà tra l'Amministrazione federale e i tribunali federali. La quota dei Cantoni è ripartita tra i singoli Cantoni in funzione della loro popolazione.

Ordinanza generale sugli emolumenti (OgeEm)

L'OgeEm si applica nella misura in cui l'avamprogetto non prevede disposizioni specifiche.

Soluzione rifiutata: ripartizione delle spese secondo l'utilizzo effettivo

Piuttosto di prevedere quote forfettarie in funzione del numero di abitanti per i Cantoni e delle procedure sbrigative per la Confederazione, gli emolumenti potrebbero essere riscossi anche in funzione dell'uso effettivo della piattaforma centrale. La piattaforma

centrale acquisisce già statistiche dettagliate sull'utilizzo da parte delle singole autorità che permetterebbero di calcolare gli emolumenti.

Considerato che non vi è un obbligo nazionale di utilizzare la piattaforma e che il suo uso può variare fortemente da un Cantone all'altro, la riscossione degli emolumenti in funzione dell'utilizzo effettivo è problematica. I Cantoni che introducono l'obbligo prima degli altri – o la Confederazione – finanzierebbero una quota di costi molto maggiore, mentre i Cantoni che introducono l'obbligo in seguito ne trarrebbero vantaggio.

Art. 17 Quota dell'Amministrazione federale e del MPC

Cpv. 1

Il DFGP paga l'emolumento a carico dell'Amministrazione federale e funge da servizio di pagamento centrale nei rapporti con l'ente di diritto pubblico. Ciò semplifica il conteggio. Si tratta del disbrigo dei pagamenti e della competenza verso l'esterno, non della ripartizione interna delle spese.

Cpv. 2

Il Consiglio federale stabilisce ogni tre anni la ripartizione della quota dell'Amministrazione federale tra i dipartimenti, la Cancelleria federale e il Ministero pubblico della Confederazione. La ripartizione delle spese è così oggetto di una decisione uniforme con una legittimità politica. Stabilire l'emolumento ogni tre anni contribuisce anche ad aumentare la sicurezza della pianificazione.

Cpv. 3

I dipartimenti e la Cancelleria federale potranno conteggiare la loro parte alle unità amministrative centralizzate o decentralizzate loro subordinate. Al loro livello i dipartimenti potranno così applicare il principio di casualità. Si tratta di una disposizione potestativa; i dipartimenti e la Cancelleria federale non sono tenuti a ripartire le spese.

Poiché non vi sono unità amministrative subordinate al Ministero pubblico della Confederazione, non occorre una ripartizione dei costi.

Art. 18 Quota dei tribunali della Confederazione

Cpv. 1

Il Tribunale federale funge da centro di costo e paga la quota a carico dei tribunali federali. Assume lo stesso ruolo che il DFGP svolge per l'Amministrazione federale e centralizza così il pagamento esterno per l'insieme della giurisdizione federale, semplificando il conteggio e i pagamenti.

Cpv. 2

Il Tribunale federale stabilisce la chiave di ripartizione per i tribunali federali dopo averli sentiti, per garantire equità e accettazione. Ciò è inoltre conforme al diritto vigente: secondo l'articolo 1 capoverso 2 LTF, il Tribunale federale esercita la vigilanza sulla gestione del Tribunale penale federale, del Tribunale amministrativo federale e del Tribunale federale dei brevetti. Tra gli strumenti di vigilanza di cui dispone il Tribunale federale vi è la vigilanza sulle finanze, che viene effettuata tramite una pianificazione finanziaria comune su più anni, nonché l'esame e la discussione dei progetti di preventivo e di consuntivo (art. 3 lett. c in combinato disposto con l'art. 6 lett. a e b del regolamento dell'11 settembre 2006 sulla vigilanza del Tribunale federale²⁰).

Diversamente da quanto previsto per l'Amministrazione federale non sussiste alcuna frequenza per stabilire la ripartizione; questa può essere adeguata in maniera più flessibile, ad esempio, annualmente o in caso di una forte variazione dell'uso della piattaforma.

Art. 19 Scadenza

Cpv. 1

L'ente di diritto pubblico riscuoterà gli emolumenti ogni anno. La loro scadenza fissata per il 1° gennaio garantisce che l'ente di diritto pubblico disponga della liquidità necessaria.

Cpv. 2

La disposizione prevede una regola specifica per il primo anno di esercizio: l'emolumento sarà dovuto il giorno dell'entrata in vigore dell'ordinanza. Si evita così un deficit di finanziamento, nel caso in cui la data di entrata in vigore non coincidesse con il 1° gennaio.

Art. 20 Servizio contabile cantonale

Ogni Cantone designa un servizio contabile unico per facilitare la fatturazione e i pagamenti all'ente di diritto pubblico.

Art. 21 Valutazione della normativa sugli emolumenti

Considerato l'esteso margine di manovra che il legislatore ha conferito al Consiglio federale nel disciplinare l'importo dell'emolumento, è opportuno esaminare tale modalità di calcolo dopo un determinato periodo di tempo. Occorre verificare se le regole stabilite sono ancora pertinenti e coerenti e permettono di garantire la stabilità finanziaria quando la piattaforma sarà a pieno regime. Il DFGP è incaricato di effettuare la

²⁰ SR 173.110.132.

valutazione due anni dopo l'introduzione dell'obbligo per la Confederazione e i Cantoni di utilizzare la piattaforma centrale nei procedimenti previsti dalla LCEG. Il DFGP garantisce così una valutazione basata su dati reali d'esercizio. Anche il Sorvegliante dei prezzi parteciperà alla valutazione.

Capitolo 2: Digitalizzazione di documenti fisici

Art. 22

Le basi legali relative alla digitalizzazione di documenti fisici risultano dalle leggi processuali in combinato disposto con l'articolo 29 LCEG. Per quanto concerne il Tribunale amministrativo federale, la base legale non deriva direttamente dalla PA, ma dall'articolo 37a della legge del 17 giugno 2005²¹ sul Tribunale amministrativo federale.

Cpv. 1 e 2

I tribunali e le autorità sono tenuti a digitalizzare nel formato PDF/A i documenti fisici loro trasmessi. Questi documenti PDF/A devono poi essere convertiti mediante uno strumento di riconoscimento ottico dei caratteri (optical character recognition [OCR]) in documenti consultabili e modificabili: l'OCR converte le lettere scritte a mano o stampate in dati leggibili elettronicamente. Il riconoscimento ottico dei caratteri migliora l'efficienza, facilitando il salvataggio, la ricerca e il trattamento. Non è necessario che la ricerca tramite riconoscimento ottico dei caratteri sia accurata al 100 per cento, ma deve essere automatizzata secondo il principio del «best effort». Ad esempio, a seconda della grafia il riconoscimento ottico dei caratteri non sarà molto accurato per i testi scritti a mano (ad esempio un testamento).

I documenti digitalizzati secondo il presente articolo sono considerati la versione determinante (cfr. art. 29 cpv. 3 LCEG).

I documenti elettronici devono avere una profondità di colore di almeno 8 bit (con 256 gradazioni di colore o di grigio) e una risoluzione di 300 DPI, per garantire chiarezza e leggibilità. Se necessario, ad esempio nel caso di originali a colori o dettagliati, è necessario prevedere valori più elevati (p. es. 24 bit di profondità di colore o 600 DPI). Questi standard minimi di qualità garantiscono documenti nitidi anche in caso di ingrandimento o stampa.

Cpv 3

Le autorità devono effettuare un adeguato controllo di qualità per garantire che i documenti digitalizzati corrispondano all'originale, sia dal punto di vista visivo (p. es. layout, immagini) che dal punto di vista del contenuto (p. es. accuratezza del testo). Si possono così prevenire errori quali pagine mancanti, parti poco chiare o illeggibili e

²¹RS 173.32

immagini distorte. La versione digitale deve sostituire integralmente l'originale. In pratica ciò comporta l'introduzione di processi quali la verifica manuale a campione, la validazione automatizzata o la certificazione. I dettagli della procedura per il controllo di qualità sono lasciati all'apprezzamento delle autorità.

Capitolo 3: Trasmissione elettronica al di fuori di una piattaforma secondo la LCEG

Sezione 1 Utilizzazione di altre soluzioni per la trasmissione di documenti

Art. 23 *Requisiti*

La trasmissione degli atti può avvenire anche con modalità diverse dalle piattaforme secondo la LCEG. In tal caso occorre soddisfare i requisiti di seguito riportati.

Lett. a

I momenti della trasmissione devono essere registrati in modo adeguato. L'avamprogetto non indica come procedere sul piano tecnico. Il sistema potrà emettere ricevute separate, un file log o un audit trail. È tuttavia importante che il momento della trasmissione non possa essere modificato senza che la modifica sia visibile.

Lett. b

Oltre a registrare i momenti, occorre anche garantire che questi corrispondano all'ora ufficiale svizzera. Sono ammesse lievi differenze fino a un minuto rispetto all'ora ufficiale svizzera. Anche se un minuto di differenza può sembrare tanto, ritardi di questa durata possono essere causati da un sovraccarico inaspettato del sistema.

Lett. c

La presente disposizione garantisce che gli atti trasmessi al di fuori di una piattaforma siano protetti da accessi e modifiche non autorizzati, non solo a destinazione ma anche durante la trasmissione.

Art. 24 *Trasmissione per via elettronica tra autorità*

Anche lo scambio di documenti tra autorità, compresi i tribunali e i pubblici uffici secondo l'articolo 128c capoverso 2 CPC, può avvenire al di fuori di una piattaforma secondo la LCEG. Secondo la LCEG la comunicazione elettronica è una procedura tracciabile per tutte le parti poiché per tutte le azioni rilevanti viene emessa una ricevuta contenente un sigillo elettronico regolamentato. Questa tracciabilità non può essere elusa servendosi delle deroghe previste nelle leggi procedurali.

Il presente articolo presuppone pertanto che la tracciabilità sia garantita mediante una registrazione non modificabile del nome, delle dimensioni e dei valori hash dei documenti trasmessi, nonché delle date e degli orari.

Distinzione rispetto alle ricerche dirette nella banca dati

L'autorità competente verifica inoltre se l'attività prevista costituisce effettivamente una trasmissione di documenti ai sensi della LCEG. Tale non è il caso se viene effettuata una consultazione diretta nella banca dati di un'altra autorità, come ad esempio i controlli di identità delle persone effettuati con il sistema MACS (Multiple Applications Coordination Services) o i controlli dei veicoli effettuati con il sistema d'informazione sull'ammissione alla circolazione. In entrambi i casi, le forze di polizia consultano direttamente le banche dati.

Sezione 2: Trasmissione di documenti per via elettronica nel settore dell'esecuzione e del fallimento

Art. 25

Nell'ambito dell'esecuzione e del fallimento, la rete di scambio di dati «e-LEF» (LEF elettronica) si è affermata mediante Sedex, una piattaforma sicura per lo scambio elettronico di dati in Svizzera, gestita e sorvegliata dalla Confederazione. È utilizzata per il progetto «e-LEF» e consente a creditori, debitori e uffici di esecuzione di scambiare in modo criptato e automatizzato i dati relativi alle esecuzioni, come i precetti esecutivi, gli atti di pignoramento o le domande di realizzazione. Nel 2024 sono stati trasmessi tramite «e-LEF»/Sedex 2 598 112 procedimenti esecutivi e 878 919 estratti del registro.

Finora la disposizione sull'«e-LEF» figurava nell'OCE-PCPE; il suo contenuto con l'entrata in vigore della LCEG sarà ripreso a livello di legge nell'articolo 33b LEF. Nell'AP-OCEP è dunque sufficiente una delega della competenza normativa al DFGP. Così sussiste ancora una base legale sufficiente per l'ordinanza del 9 febbraio 2011²² sulla comunicazione per via elettronica nel settore esecuzione.

Il capoverso 2 utilizza la terminologia specifica dell'«e-LEF». Il termine «casella postale elettronica» non indica una casella dell'e-mail ma un servizio di trasmissione e ricezione giuridicamente vincolante.

Sezione 3 Conferma elettronica dell'esattezza dei verbali nella procedura penale e nella procedura penale militare

Art. 26

Cpv. 1

Le parti che confermano l'esattezza del processo verbale dovranno farlo personalmente e di propria mano senza l'intervento di terzi o di dispositivi automatici. Ciò è

²² RS 281.112.1

sottolineato dalla nozione di «firma autografa». Si vuole così impedire che le conferme siano copiate o falsificate e garantire che l'autore della conferma sia fisicamente presente.

Cpv. 2

Il dispositivo non deve verbalizzare soltanto il momento esatto della conferma ma anche dettagli biometrici, ossia la qualità del tratto (p. es. spessore e forma), la pressione, il flusso del movimento (p. es. la velocità) e la direzione dei movimenti. Questi dati devono essere collegati alla conferma. Si tratta di garantire la tracciabilità forense: questi dati rendono la conferma unica e verificabile, comparabile a un'analisi grafologica di una grafia.

Cpv. 3

Il dispositivo elettronico utilizzato per registrare la conferma deve essere configurato in modo tale che, dopo l'apposizione della prima conferma, non sia più possibile modificare il verbale tranne per aggiungervi ulteriori conferme (p. es. di altre persone interessate). Si garantisce così l'integrità del verbale e si impediscono modifiche successive o falsificazioni.

Cpv. 4

Questa disposizione stabilisce che i verbali che devono essere firmati esclusivamente da membri delle autorità possono essere confermati in modo giuridicamente valido anche per via elettronica. In concreto, i sigilli elettronici regolamentati o le firme elettroniche qualificate equivalgono a conferme elettroniche apposte su un «dispositivo elettronico» secondo le leggi procedurali pertinenti.

Capitolo 4 Disposizioni finali

Art. 27 Abrogazione e modifica di altri atti normativi

L'allegato 1 elenca i due atti normativi da abrogare e l'atto da modificare con l'entrata in vigore della presente ordinanza.

Art. 28 Entrata in vigore

Questa disposizione indica la data dell'entrata in vigore della presente ordinanza.

4 Commenti all'allegato 1 (abrogazione e modifica di altri atti normativi)

4.1 Abrogazione dell'ordinanza del 18 giugno 2010²³ sulla comunicazione per via elettronica nell'ambito di procedimenti amministrativi (OCE-PA)

Le vigenti disposizioni della PA relative alla trasmissione per via elettronica costituiscono la base legale dell'OCE-PA. Poiché tali disposizioni saranno sostituite da altre in seguito all'entrata in vigore definitiva della LCEG, occorre abrogare l'OCE-PA perché priva di una base legale.

4.2 Abrogazione dell'ordinanza del 18 giugno 2010²⁴ sulla comunicazione per via elettronica nell'ambito di procedimenti civili e penali nonché di procedure d'esecuzione e fallimento (OCE-PCPE)

Vedi i commenti al numero 4.1

4.3 Ordinanza del 23 novembre 2016²⁵ sulla firma elettronica

Art. 14a Firme e sigilli verificati dal validatore

Cpv. 1

La presente disposizione limita l'obbligo di verifica alle firme elettroniche qualificate, ai sigilli elettronici regolamentati e alle marche temporali elettroniche qualificate perché soltanto queste firme hanno validità giuridica. Inoltre, se lo ritiene opportuno, il validatore può verificare altre firme elettroniche, ad esempio, il certificato di classe B dell'Amministrazione federale.

Cpv. 2

Il 29 gennaio 2025 il Consiglio federale ha incaricato il DATEC (UFCOM) di elaborare, insieme al DFAE, un mandato negoziale con l'UE sul riconoscimento reciproco delle firme elettroniche. Nel quadro di questo mandato negoziale è emerso il timore che il validatore potesse diventare il servizio di controllo per l'intera UE. Il capoverso 2 stabilisce che i pertinenti accordi internazionali devono contenere un obbligo esplicito di verificare le firme reciprocamente riconosciute, altrimenti il validatore verifica solo le firme secondo il diritto svizzero.

²³ RS 172.021.2

²⁴ RS 272.1

²⁵ RS 943.032

Cpv. 3

Nel caso di documenti con più firme o sigilli, il validatore deve indicare in modo dettagliato quali di essi soddisfano i requisiti della FiEle o degli accordi internazionali. Invece di una valutazione generica, l'utente (ad es. un'autorità) riceve un elenco dettagliato degli elementi validi e di quelli non validi. Questa procedura facilita l'elaborazione di documenti complessi come i contratti tra più parti, evita malintesi e aiuta a decidere se un documento può essere accettato nella sua interezza. Il validatore non fornisce tuttavia alcuna informazione sull'efficacia giuridica di un documento verificato.

Cpv. 4

Nel caso di un sigillo di un'autorità, il validatore può comunicare che si tratta di un documento di un'autorità e indicare per quale scopo tale documento è stato creato. Può ad esempio indicare se si tratta di una comunicazione ufficiale, di documenti della piattaforma di pubblicazione della Confederazione, di un estratto del casellario giudiziario o di documenti analoghi. Fornendo tali informazioni, il validatore agevola la classificazione dei documenti verificati e può aumentare l'efficienza.

Art. 14b Apposizione e validazione di firme e sigilli elettronici

Uno dei principali problemi riscontrati nell'ambito della validazione delle firme elettroniche consiste nell'ampio margine di manovra lasciato dalle norme tecniche internazionali. Questa libertà è fonte di problemi, perché non è possibile tenere conto di ogni singola implementazione. Questa disposizione consente all'UFCOM di disciplinare chiaramente il processo di validazione e promuovere così la creazione di standard uniformi che garantiscano validazioni affidabili e riproducibili. Questa disposizione potestativa non deve essere intesa come l'attribuzione all'UFCOM del mandato di disciplinare il processo di validazione.

Se fosse necessario che l'UFCOM elabori norme relative al processo di validazione, esso dovrebbe tenere conto degli standard internazionali e limitare il disciplinamento agli ambiti in cui gli standard internazionali non prevedono regole chiare.

5 Commento all'articolo 26 capoverso 5 LCEG

L'articolo 26 capoverso 5 LCEG non è stato commentato nel messaggio perché è stato aggiunto durante i dibattiti parlamentari, nel cui ambito il Consiglio federale ha proposto di commentare la disposizione in seguito. Questo spiega l'aggiunta del presente capitolo.

Il capoverso 5 intende offrire un mezzo supplementare, oltre a quello previsto dall'articolo 26 capoverso 1 LCEG, di rispettare il termine. Il capoverso 1 non consente infatti di coprire tutti i casi, ad esempio un'imminente assenza per ferie dell'utente che non può quindi attendere che la piattaforma sia nuovamente disponibile.

Pertanto, secondo l'articolo 26 capoverso 5 il termine è pure rispettato quando l'utente ha consegnato tutti i documenti in formato cartaceo alla posta o a una rappresentanza diplomatica o consolare.

Se i documenti e i loro allegati sono voluminosi, può risultare impossibile imbucarli in una buca delle lettere dopo la chiusura della posta. Per questa ragione l'articolo 26 capoverso 5 LCEG considera rispettato il termine nel caso in cui l'utente provi l'esistenza di documenti da presentare. Tale prova può essere fornita indicando la somma dei valori hash dei documenti allegati alla lettera, in modo analogo a quanto indicato nelle ricevute di consegna. Tuttavia, ciò non esonera il destinatario dall'obbligo di imbucare i documenti o consegnarli a una rappresentanza diplomatica o consolare entro i termini. Occorre inoltre utilizzare un algoritmo di hash sicuro, per esempio SHA-256, SHA-512, SHA-3, BLAKE2 e BLAKE3. Algoritmi obsoleti come MD5 o SHA-1 non vanno utilizzati, poiché non più sicuri.

6 Ripercussioni

6.1 Ripercussioni per la Confederazione

L'ordinanza non ha ulteriori ripercussioni sul personale oltre a quelle già esposte al numero 6.1 del messaggio sulla LCEG. Dal punto di vista finanziario, il messaggio ha già precisato che le spese d'esercizio e di sviluppo della piattaforma saranno finanziate mediante emolumenti e ampiamente compensate dai risparmi a medio e lungo termine.

Le unità amministrative della Confederazione dovranno inoltre aprire un conto sia sulla piattaforma centrale sia sulla piattaforma per le procedure amministrative e verificarlo regolarmente, a meno che vi accedano mediante un'interfaccia.

6.2 Ripercussioni per i Cantoni e i Comuni

Le considerazioni di cui al numero 6.1 valgono anche per i Cantoni e i Comuni, fermo restando che solo i tribunali, i ministeri pubblici e le autorità di polizia devono avere un conto sulla piattaforma centrale a partire dall'entrata in vigore. Le altre autorità cantonali potranno, se necessario, accedere alla piattaforma successivamente, quando dovranno comunicare per la prima volta con i tribunali, i ministeri pubblici o le autorità di polizia oppure con unità amministrative della Confederazione.

I Cantoni dovranno inoltre, se del caso, adeguare le basi legali che rimandano all'OCE-PA o all'OCE-PCPE, poiché queste ordinanze saranno abrogate con l'entrata in vigore dell'AP-OCEP.

6.3 Ripercussioni sull'economia

La digitalizzazione procede a grandi passi e un numero crescente di transazioni può oramai essere effettuato in linea. Come il Consiglio federale ha fatto già notare in occasione dell'elaborazione del CPC, un'efficiente amministrazione della giustizia contribuisce alla prosperità economica e infine migliora anche la qualità della vita.

Anche in ambito digitale, la normativa e la sicurezza degli scambi concorrono in maniera essenziale a rendere attrattiva e competitiva la piazza economica svizzera. Il Consiglio federale intende far sì che lo Stato contribuisca nel migliore dei modi al passaggio della Svizzera alla società dell'informazione. A tal fine ha adottato numerose misure concernenti per lo più l'adeguamento del quadro normativo (p. es. la FiEle) o l'allestimento dell'infrastruttura (p. es. numeri d'identificazione univoci per le persone e le imprese nonché i corrispondenti registri). Con la LCEG il Consiglio federale compie un ulteriore passo introducendo l'obbligo di comunicare per via elettronica per i tribunali, le autorità e i professionisti del diritto. A tal proposito è prevista la creazione di una piattaforma sicura e di facile utilizzo, interessante anche per le persone e le imprese che non soggiacciono all'obbligo di comunicare per via elettronica. Questa piattaforma consentirà di svolgere i procedimenti in modo completamente elettronico, favorendo una maggiore efficienza nell'amministrazione della giustizia efficiente.

L'obbligo interessa in particolare gli avvocati. Questi in futuro potranno inoltrare gli atti scritti e gli allegati ai tribunali e alle autorità (di perseguimento penale) esclusivamente per via elettronica. Questa novità modifica il modo di lavorare, ma non necessariamente implica costi aggiuntivi, che potrebbero invece risultare dalla necessità di adeguare l'infrastruttura, da un cambiamento del fabbisogno di personale o da un aumento del tempo necessario per svolgere determinati compiti.

6.4 Ripercussioni sulla società

L'avamprogetto ha poche ripercussioni dirette sulla società.

La comunicazione con la giustizia delle persone che non soggiacciono all'obbligo di comunicazione elettronica non cambia. Queste persone possono continuare a comunicare con i giudici e le autorità per via postale. La novità consiste nella possibilità di beneficiare del nuovo sistema per comunicare per via elettronica in modo semplice e sicuro con tribunali e autorità. La decisione spetta al singolo. Per beneficiare della comunicazione elettronica, occorre soltanto disporre di una connessione a Internet, di un conto sulla piattaforma centrale o sulla piattaforma per le procedure amministrative e di un login AGOV.

Per i professionisti del diritto valgono le stesse condizioni.

7 Aspetti giuridici

7.1 Sicurezza delle informazioni

L'utilizzazione abusiva delle informazioni così come le perturbazioni della piattaforma centrale possono pregiudicare gravemente gli interessi essenziali della Svizzera e i diritti delle persone. Rischiano inoltre di compromettere i compiti legali connessi con l'esercizio della piattaforma centrale e della piattaforma per le procedure amministrative. La LSIⁿ e l'ordinanza dell'8 novembre 2023²⁶ sulla sicurezza delle informazioni (OSIⁿ) costituiscono le basi legali per garantire nel miglior modo possibile la sicurezza delle informazioni.

Non occorre disciplinare in modo dettagliato nell'avamprogetto come affrontare le minacce alla sicurezza delle informazioni, perché la LSIⁿ e la OSIⁿ prevedono già le pertinenti basi giuridiche. Come per la LPD, anche in questo caso si fa riferimento all'attuale sistematica del diritto. Ciò significa che le normative vigenti sono già sufficienti per affrontare in modo sicuro i potenziali rischi in materia di sicurezza delle informazioni.

7.2 Protezione dei dati

La LPD e le relative ordinanze si applicano alla piattaforma centrale e alla piattaforma per le procedure amministrative. Per quanto riguarda i procedimenti pendenti, il trattamento di dati personali e i diritti delle persone interessate sono retti dal diritto processuale applicabile (art. 2 cpv. 3 LPD). Al fine di evitare ripetizioni e facilitare l'interpretazione delle norme, l'avamprogetto rinuncia a rinviare alle disposizioni della LPD. Le disposizioni d'esecuzione concretizzano il quadro istituito nella LCEG per il trattamento, la conservazione e la cancellazione di dati.

²⁶ RS 128.1