

ISTANZA GIURIDICA DI ACCERTAMENTO, INIBITORIA E RICONOSCIMENTO DEL VAGLIO DEMOCRATICO

CON CLAUSOLA DI AUTODETERMINAZIONE E RISARCIMENTO INDIVIDUALE

INAPPLICABILITÀ DELLE NORMATIVE DI SORVEGLIANZA E CONTROLLO DIGITALE PER IL POPOLO ITALIANO AUTODETERMINATO

Richiesta di inapplicabilità radicale, disapplicazione e riconoscimento del difetto assoluto di legittimazione di ogni normativa, direttiva o proposta di:

✓ SORVEGLIANZA DI MASSA ✓ CHAT CONTROL ✓ DIRECTIVES ANTI-RICICLAGGIO

✓ CONTROLLI FINANZIARI INTRUSIVI

SOVRANITÀ POPOLARE

DIRITTI INALIENABILI

A. OGGETTO DELL'ISTANZA

Si richiede l'inapplicabilità, l'inefficacia e la nullità di ogni atto normativo o amministrativo che imponga forme di sorveglianza, monitoraggio e controllo digitale senza il preventivo vaglio referendario vincolante del popolo.

Si afferma il principio di autogoverno individuale per ogni cittadino appartenente al popolo italiano autodeterminato, con riserva di richiesta giudiziale di indennizzo patrimoniale pari a € 1.000.000,00 (UN MILIONE DI EURO) per ciascun atto di imposizione che violi i diritti fondamentali e inalienabili aggirando la sovranità popolare originaria.

DIRITTI INVIOLABILI

Privacy
Libertà di comunicazione
Dignità umana
Autodeterminazione informativa

CLAUSOLA RISARCITORIA

€ 1.000.000,00
per ogni violazione individuale accertata

DIRITTI FONDAMENTALI COINVOLTI

Rispetto della vita privata e familiare (Art. 8 CEDU - Art. 7 CDFUE)

Protezione dei dati personali (Art. 8 CDFUE - Reg. UE 2016/679)

Libertà di espressione e informazione (Art. 11 CDFUE - Art. 10 CEDU)

Libertà e segretezza delle comunicazioni (Art. 15 Cost. - Art. 8 CEDU)

Libertà personale (Art. 13 Cost.)

Tutela giurisdizionale effettiva (Art. 24 Cost. - Art. 47 CDFUE - Art. 13 CEDU)

B. PREMESSE IN FATTO E IN DIRITTO: L'INSUFFICIENZA DELLA RAPPRESENTANZA DERIVATA

1 IL FALLIMENTO DEL MODELLO RAPPRESENTATIVO DERIVATO

- Il sistema della rappresentanza delegata ha esaurito la propria funzione nel momento in cui impone decisioni lesive della libertà, della privacy, della crittografia e della dignità dei cittadini.
- Nessun atto normativo "top-down" che non tragga la propria forza da una deliberazione diretta ed espressa del popolo è giuridicamente valido.
- Difetto radicale di competenza, mandato e legittimazione democratica.

2 LA SOVRANITÀ ORIGINARIA DEL POPOLO ITALIANO

- Il popolo italiano conserva il diritto inalienabile all'autodeterminazione e all'autogoverno.
- Nessun trattato, accordo intergovernativo o direttiva burocratica può prevalere sulla riserva di sovranità popolare in materia di diritti fondamentali.
- L'imposizione di standard di controllo digitale preventivo e di sorveglianza di massa rappresenta un atto di eversione dell'ordine costituzionale democratico.

3 L'AUTOGOVERNO INDIVIDUALE E LA TUTELA RISARCITORIA

- Quando lo Stato derivato viola il patto sociale e calpesta i diritti inviolabili senza il vaglio del popolo sovrano, decade il vincolo di subordinazione politica del cittadino.
- Ogni cittadino mantiene il diritto di agire individualmente per la tutela della propria sfera giuridica, patrimoniale e personale.
- Riserva di azione giudiziale e richiesta di risarcimento patrimoniale individuale.

C. FORMULAZIONE DELLE RICHIESTE, DEGLI ACCERTAMENTI E DELLE CLAUSOLE PATRIMONIALI

1 LA PIENA INAPPLICABILITÀ PER IL POPOLO ITALIANO AUTODETERMINATO

- Si dichiara la totale inapplicabilità, inefficacia e nullità di qualsiasi normativa concernente il monitoraggio delle comunicazioni (Chat Control) o il controllo finanziario forzoso nei confronti dei cittadini del popolo italiano autodeterminato.
- Difetto a monte di qualsiasi approvazione referendaria a democrazia diretta.

2 IL RICONOSCIMENTO DELL'AUTORITÀ DI AUTOGOVERNO INDIVIDUALE

- Il singolo cittadino autodeterminato agisce a tutela della legalità costituzionale originaria, rifiutando ogni sottomissione a standard normativi imposti senza il consenso popolare diretto.
- Ogni decisione lesiva dei diritti fondamentali senza vaglio referendario è priva di legittimità e non vincola il cittadino sovrano.

3 LA CLAUSOLA INDENNITARIA E RISARCITORIA (1.000.000 € PER VIOLAZIONE)

- Ogni singola decisione, atto amministrativo, direttiva o forzatura legislativa che prevalga i diritti fondamentali e le libertà inalienabili senza previa consultazione referendaria legittimerà il cittadino danneggiato a richiedere giudizialmente, in via autonoma e individuale, un indennizzo patrimoniale risarcitorio pari a € 1.000.000,00 (UN MILIONE DI EURO).

PRINCIPI FONDAMENTALI RICHIESTI

LEGALITÀ

PROPORZIONALITÀ

NECESSITÀ

MINIMIZZAZIONE DEI DATI

TRASPARENZA

CONTROLLO GIUDIZIARIO

PARTECIPAZIONE DEMOCRATICA

AUTODETERMINAZIONE

RISARCIMENTO INDIVIDUALE

DEMOCRAZIA DIRETTA

Nessuna misura strutturale di sorveglianza può essere introdotta senza il preventivo vaglio democratico del popolo sovrano.

BASI GIURIDICHE DI RIFERIMENTO

- Costituzione della Repubblica Italiana: artt. 1, 2, 3, 13, 14, 15, 21, 24, 25, 42
- Carta dei Diritti Fondamentali dell'Unione Europea: artt. 7, 8, 11, 16, 20, 21, 47, 52
- Convenzione Europea dei Diritti dell'Uomo: artt. 8, 10, 11, 13
- Patto Internazionale sui Diritti Civili e Politici: artt. 17, 19, 22
- Regolamento (UE) 2016/679 (GDPR) e normative nazionali ed europee applicabili
- Principi di diritto internazionale e giurisprudenza nazionale ed europea

CLAUSOLA DI RISERVA E FIRMA

Ogni diritto, azione, eccezione, opposizione, ricorso, domanda cautelare, domanda inhibitoria e pretesa risarcitoria resta espressamente riservato, nei limiti e secondo le procedure previste dall'ordinamento competente.

Luogo e data: _____

Il richiedente (firma): _____

OMNIA IURA RESERVATA

1

**ISTANZA GIURIDICA DI ACCERTAMENTO, INIBITORIA E RICONOSCIMENTO DEL
VAGLIO DEMOCRATICO CON CLAUSOLA DI AUTODETERMINAZIONE E
RISARCIMENTO INDIVIDUALE**

**INAPPLICABILITÀ, DISAPPLICAZIONE E CONTROLLO DI LEGITTIMITÀ DELLE
MISURE DI SORVEGLIANZA, MONITORAGGIO DIGITALE E CONTROLLO
FINANZIARIO INVASIVO NEI CONFRONTI DEL POPOLO ITALIANO
AUTODETERMINATO**

Sua Eccellenza Franco Paluan

Esperto Giuridico Internazionale in materia di Diritti Umani e Diritto dei Popoli

(His Excellency Franco Paluan — International Human Rights and Peoples' Rights Legal Expert)

**ISTANZA FORMALE DI ACCERTAMENTO, TUTELA INIBITORIA, PREVENZIONE DEL
DANNO, VAGLIO DEMOCRATICO, PROTEZIONE DEI DIRITTI FONDAMENTALI,
AUTODETERMINAZIONE INDIVIDUALE E RISERVA DI AZIONE RISARCITORIA**

**ALLE AUTORITÀ DELLA REPUBBLICA ITALIANA
ALLE ISTITUZIONI DELL'UNIONE EUROPEA
ALLE AUTORITÀ GARANTI COMPETENTI
ALLE AUTORITÀ GIUDIZIARIE E AMMINISTRATIVE COMPETENTI
AGLI ORGANI LEGISLATIVI COMPETENTI
A OGNI AUTORITÀ PUBBLICA O SOGGETTO INVESTITO DI POTERI DI CONTROLLO,
MONITORAGGIO O TRATTAMENTO DI DATI PERSONALI**

PREAMBOLO

La presente istanza viene formulata nell'esercizio dei diritti di **petizione, partecipazione, autodeterminazione democratica, tutela giurisdizionale, protezione della vita privata, libertà personale, libertà di comunicazione, libertà di espressione, protezione dei dati personali, libertà economica e difesa dei diritti inviolabili** riconosciuti dall'ordinamento costituzionale, europeo e internazionale.

L'istanza assume quale principio fondamentale che la **sicurezza pubblica, la prevenzione dei reati e la tutela del sistema finanziario** costituiscono finalità legittime soltanto quando perseguite mediante strumenti:

- **conformi alla legge;**
- **necessari;**
- **proporzionati;**
- **determinati;**
- **controllabili;** e
- **rispettosi dei diritti fondamentali.**

Nessuna finalità di interesse pubblico può trasformarsi automaticamente in titolo per instaurare forme **generalizzate, indiscriminate o sproporzionate di sorveglianza della popolazione.**

La presente istanza riguarda, in particolare, ogni misura normativa, regolamentare, amministrativa, tecnica o infrastrutturale suscettibile di introdurre o ampliare:

- monitoraggio sistematico delle comunicazioni private;
- scansione generalizzata dei contenuti digitali;
- controllo automatizzato delle comunicazioni personali;
- sorveglianza preventiva della messaggistica;
- indebolimento o aggiramento della crittografia;
- raccolta massiva di metadati;
- profilazione comportamentale;
- monitoraggio finanziario eccedente le esigenze specificamente previste dalla legge;
- interconnessione generalizzata di banche dati;
- sorveglianza economica automatizzata;
- sistemi di identificazione o classificazione automatica dei cittadini;
- meccanismi di blocco o limitazione automatica dell'accesso a risorse economiche;
- qualsiasi ulteriore tecnologia capace di trasformare infrastrutture pubbliche o private in strumenti permanenti di sorveglianza generalizzata.

PREMESSA — IL CLNI COME AUTORITÀ NAZIONALE DEL POPOLO ITALIANO AUTODETERMINATO

La presente Istanza è promossa dal **Comitato di Liberazione Nazionale Italiano (CLNI)**, che si presenta e opera quale **autorità nazionale provvisoria del Popolo Italiano in Autodeterminazione**.

Il CLNI non è un movimento politico tra gli altri, né un'associazione privata: esso rivendica e assume la veste di **soggetto istituzionale metacostituzionale**, chiamato a rappresentare quella parte del popolo italiano che, ritenendo esaurita la legittimità dell'ordinamento statuale attuale, ha deciso di riorganizzarsi per riprendere il pieno controllo della propria sovranità, in continuità con i principi della Resistenza e con la tradizione dei Comitati di Liberazione Nazionale che, dal 1943 al 1946, rappresentarono la volontà del popolo italiano contro l'occupazione e la dittatura.

Tale legittimazione trova fondamento nei principi del diritto internazionale, in particolare nell'**articolo 1 della Carta delle Nazioni Unite**, che sancisce il principio dell'**"uguaglianza dei diritti e dell'autodeterminazione dei popoli"**, e nell'**articolo 1 del Patto Internazionale sui Diritti Civili e Politici**, secondo cui "tutti i popoli hanno il diritto di autodeterminazione" e "determinano liberamente il loro statuto politico e perseguono liberamente il loro sviluppo economico, sociale e culturale".

Il CLNI, in quanto autorità nazionale del popolo italiano autodeterminato, ritiene proprio dovere istituzionale:

- **accertare** la natura costituzionalmente rilevante delle trasformazioni in materia di sorveglianza e controllo digitale;
- **richiedere** che esse siano sottoposte a un preventivo e effettivo vaglio democratico;
- **vigilare** affinché i diritti fondamentali del popolo italiano non vengano compressi da scelte tecnologiche compiute in assenza di legittimazione popolare;

- **proporre** gli strumenti giuridici e partecipativi necessari a garantire che le scelte fondamentali in materia di sorveglianza e protezione dei dati siano rimesse al popolo sovrano.
-

A. OGGETTO DELL'ISTANZA

1. Richiesta principale

Con la presente si chiede formalmente **l'accertamento, la prevenzione e, ove ne ricorrano i presupposti giuridici, l'inibizione o disapplicazione** delle misure di sorveglianza e controllo digitale incompatibili con i diritti fondamentali, nonché il riconoscimento della necessità di un **effettivo controllo democratico** sulle trasformazioni normative e tecnologiche aventi incidenza strutturale sulle libertà individuali.

In particolare, si chiede che nessuna misura avente carattere **generale, sistematico o potenzialmente permanente di sorveglianza delle comunicazioni o di controllo digitale della popolazione** venga considerata automaticamente legittima per il solo fatto di essere contenuta in un atto legislativo, regolamentare o amministrativo.

La sua legittimità deve essere verificata secondo:

BASE GIURIDICA + COMPETENZA + NECESSITÀ + PROPORZIONALITÀ + DETERMINATEZZA + FINALITÀ SPECIFICA + MINIMIZZAZIONE + CONTROLLO INDIPENDENTE + TUTELA GIURISDIZIONALE EFFETTIVA.

B. PRINCIPIO DI SUPREMA TUTELA DEI DIRITTI FONDAMENTALI

2. Primato della persona e dei diritti inviolabili

L'ordinamento costituzionale italiano riconosce la centralità della persona e dei diritti inviolabili.

In particolare, assumono rilievo:

- **Articolo 1 della Costituzione** — sovranità popolare;
- **Articolo 2** — riconoscimento e garanzia dei diritti inviolabili;
- **Articolo 3** — uguaglianza;
- **Articolo 13** — libertà personale;
- **Articolo 14** — inviolabilità del domicilio;
- **Articolo 15** — libertà e segretezza delle comunicazioni;
- **Articolo 21** — libertà di espressione;
- **Articolo 24** — diritto alla tutela giurisdizionale;
- **Articolo 25** — principio di legalità;
- **Articolo 42** — diritto di proprietà;
- nonché gli ulteriori principi costituzionali applicabili.

La **libertà e la segretezza delle comunicazioni** costituiscono una garanzia fondamentale.

Ne consegue che qualsiasi sistema tecnologico capace di analizzare sistematicamente comunicazioni private deve essere sottoposto a un controllo particolarmente rigoroso sulla propria base giuridica e sulla proporzionalità delle misure adottate.

C. PROTEZIONE EUROPEA E INTERNAZIONALE

3. Carta dei diritti fondamentali dell'Unione europea

Devono essere specificamente considerati, tra gli altri:

- **Articolo 7** — rispetto della vita privata e familiare;
- **Articolo 8** — protezione dei dati personali;
- **Articolo 11** — libertà di espressione e informazione;
- **Articolo 16** — libertà d'impresa;
- **Articolo 17** — diritto di proprietà;
- **Articolo 20** — uguaglianza davanti alla legge;
- **Articolo 21** — non discriminazione;
- **Articolo 47** — tutela giurisdizionale effettiva;
- **Articolo 52** — portata e interpretazione dei diritti e dei principi.

Ogni limitazione deve pertanto rispettare le condizioni previste dal sistema europeo di tutela dei diritti fondamentali.

D. CONVENZIONE EUROPEA DEI DIRITTI DELL'UOMO

4. Tutela della vita privata e delle comunicazioni

Devono essere considerati, secondo la rispettiva applicabilità:

- **Articolo 8 CEDU** — diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza;
- **Articolo 10 CEDU** — libertà di espressione;
- **Articolo 11 CEDU** — libertà di riunione e associazione;
- **Articolo 13 CEDU** — diritto a un ricorso effettivo.

Qualsiasi sistema di sorveglianza deve pertanto essere soggetto a garanzie effettive contro:

- l'arbitrarietà;
 - l'eccesso;
 - la raccolta indiscriminata;
 - l'utilizzazione ulteriore dei dati.
-

E. PATTO INTERNAZIONALE SUI DIRITTI CIVILI E POLITICI

5. Protezione contro interferenze arbitrarie

Si richiama inoltre la tutela prevista, per quanto applicabile, dagli **articoli 17, 19 e 22 del Patto internazionale sui diritti civili e politici**.

Il principio fondamentale è che **nessuna persona debba essere sottoposta ad interferenze arbitrarie o illegittime nella propria vita privata, famiglia, domicilio o corrispondenza**.

La lotta alla criminalità non elimina tale principio.

Al contrario, proprio l'esistenza di finalità pubbliche di sicurezza rende necessario stabilire limiti **rigorosi, verificabili e giuridicamente controllabili**.

F. PRINCIPIO DI LEGALITÀ TECNOLOGICA

6. Nessun potere di sorveglianza senza una base giuridica determinata

Nessun soggetto pubblico o privato può acquisire un potere generale di sorveglianza semplicemente perché dispone della capacità tecnica di esercitarlo.

Si afferma pertanto il seguente principio:

LA CAPACITÀ TECNOLOGICA DI MONITORARE NON COSTITUISCE, DI PER SÉ, UN'AUTORIZZAZIONE GIURIDICA AL MONITORAGGIO.

La disponibilità tecnica di un sistema non può trasformarsi automaticamente in una fonte autonoma di potere pubblico.

G. DIVIETO DI SORVEGLIANZA GENERALIZZATA

7. Principio di individualizzazione del controllo

Le misure di sorveglianza devono essere, ove richiesto dalla legge e secondo i relativi presupposti, specificamente giustificate rispetto a finalità determinate e soggetti o situazioni concretamente rilevanti.

Non può essere automaticamente considerata proporzionata una metodologia secondo la quale:

prima si raccolgono sistematicamente i dati di tutti → successivamente si cercano eventuali elementi sospetti.

La logica della prevenzione non può trasformare l'intera popolazione in un insieme permanente di soggetti sottoposti a controllo.

Si richiede pertanto il riconoscimento del principio:

PRESUNZIONE GENERALE DI NON SORVEGLIANZA DEL CITTADINO NON SOSPETTATO

H. "CHAT CONTROL" E SCANSIONE DELLE COMUNICAZIONI

8. Divieto di trasformazione della comunicazione privata in oggetto di controllo generalizzato

Qualsiasi proposta o disciplina comunemente indicata come "Chat Control", nonché qualsiasi tecnologia avente effetti sostanzialmente equivalenti, dovrà essere sottoposta a rigoroso esame di:

- **necessità;**
- **proporzionalità;**
- **efficacia;**
- **precisione;**
- **minimizzazione dei falsi positivi;**
- **tutela della crittografia;**
- **tutela della riservatezza;**
- **controllo giudiziario;**
- **limitazione temporale;**
- **limitazione soggettiva;**
- **limitazione delle finalità.**

Non potrà essere considerata sufficiente una generica finalità di contrasto alla criminalità per legittimare automaticamente la scansione generalizzata delle comunicazioni di persone non sospettate.

I. PROTEZIONE DELLA CRITTOGRAFIA

9. La crittografia quale strumento di sicurezza e libertà

La crittografia costituisce contemporaneamente uno strumento di:

- **sicurezza informatica;**
- **protezione dei dati;**
- **riservatezza;**
- **sicurezza economica;**
- **protezione delle infrastrutture;**
- **libertà comunicativa.**

Qualsiasi obbligo tecnico destinato a creare vulnerabilità sistemiche, accessi privilegiati, scansione indiscriminata o meccanismi equivalenti di aggiramento della crittografia dovrà essere sottoposto a rigorosa valutazione dei rischi.

Si chiede pertanto di riconoscere il principio:

NESSUNA MISURA DI SICUREZZA PUBBLICA PUÒ ESSERE REALIZZATA MEDIANTE LA CREAZIONE DI UNA VULNERABILITÀ GENERALE CAPACE DI ESPORRE L'INTERA POPOLAZIONE A RISCHI INFORMATICI SUPERIORI A QUELLI CHE LA MISURA INTENDE PREVENIRE.

L. PROTEZIONE DEI DATI PERSONALI

10. Principi di minimizzazione e limitazione delle finalità

Qualsiasi trattamento deve essere sottoposto, secondo il quadro normativo applicabile, ai principi di:

- **liceità;**
- **correttezza;**
- **trasparenza;**
- **limitazione della finalità;**
- **minimizzazione;**
- **esattezza;**
- **limitazione della conservazione;**
- **integrità;**
- **riservatezza;**
- **responsabilizzazione.**

Particolare attenzione dovrà essere riservata alla possibilità che dati originariamente raccolti per una finalità vengano successivamente utilizzati per finalità differenti.

Si richiede quindi il riconoscimento del principio:

NO FUNCTION CREEP

Nessun sistema creato per una determinata finalità può essere progressivamente trasformato in un'infrastruttura generale di sorveglianza senza una nuova, specifica e rigorosa base giuridica.

M. SORVEGLIANZA FINANZIARIA E NORMATIVA ANTIRICICLAGGIO

11. Contrasto al riciclaggio e tutela della persona

Il contrasto al riciclaggio, al finanziamento del terrorismo e alla criminalità economica costituisce finalità legittima di interesse pubblico.

Tuttavia, tale finalità deve essere perseguita mediante strumenti:

- **mirati;**
- **necessari;**
- **proporzionati;**
- **fondati sulla legge;**
- **sottoposti a controllo;**
- **rispettosi della protezione dei dati;**
- **soggetti a limiti temporali e finalistici.**

Non può essere automaticamente ritenuto proporzionato un sistema nel quale ogni cittadino sia trattato come potenziale soggetto sospetto mediante raccolta e analisi eccedente rispetto alle esigenze concrete della normativa.

N. PRINCIPIO DI PROPORZIONALITÀ RAFFORZATA

12. Quattro livelli di controllo

Ogni misura invasiva dovrà superare almeno quattro verifiche:

I. LEGALITÀ

Esiste una precisa e accessibile base giuridica?

II. IDONEITÀ

La misura è realmente idonea a conseguire la finalità dichiarata?

III. NECESSITÀ

Esiste una soluzione meno invasiva dei diritti fondamentali?

IV. PROPORZIONALITÀ IN SENSO STRETTO

Il vantaggio pubblico ottenuto è proporzionato al sacrificio imposto al cittadino?

Qualora una misura fallisca uno di tali test, dovrà essere richiesta la sua **modifica, limitazione, sospensione o disapplicazione** nei casi e secondo le procedure previste dall'ordinamento.

O. PRINCIPIO DI PRECAUZIONE DIGITALE

13. Rischio tecnologico sistemico

Prima dell'implementazione di sistemi di sorveglianza generalizzata devono essere valutati anche:

- **vulnerabilità informatiche;**
- **attacchi da parte di soggetti criminali;**
- **accessi abusivi;**
- **falsi positivi;**
- **errori algoritmici;**
- **discriminazioni;**
- **perdita di dati;**
- **reidentificazione;**
- **interconnessione delle banche dati;**
- **trasferimenti internazionali;**
- **utilizzazioni secondarie;**
- **abuso dei poteri;**
- **concentrazione informativa.**

In presenza di rischi sistemici non adeguatamente mitigati deve essere applicato il **principio di precauzione**.

P. PRINCIPIO DI SEPARAZIONE DEL POTERE INFORMATIVO

14. Divieto di concentrazione assoluta dei dati

Nessuna singola autorità o infrastruttura dovrebbe concentrare senza adeguate garanzie tutte le funzioni di:

IDENTIFICAZIONE + RACCOLTA + CONSERVAZIONE + ANALISI + PROFILAZIONE + SORVEGLIANZA + DECISIONE + SANZIONE.

La **separazione funzionale** costituisce una garanzia contro l'abuso del potere informativo.

Q. PRINCIPIO DI CONTROLLO UMANO

15. Divieto di automatismo lesivo

Nessun cittadino dovrebbe subire automaticamente conseguenze sostanziali sulla propria libertà, reputazione, disponibilità economica o accesso a servizi fondamentali sulla sola base di una decisione algoritmica non verificabile.

Devono essere assicurati:

- **controllo umano;**
 - **motivazione;**
 - **possibilità di contestazione;**
 - **accesso alle informazioni pertinenti;**
 - **rettifica;**
 - **revisione;**
 - **ricorso;**
 - **tutela giudiziaria.**
-

R. PRINCIPIO DI AUTODETERMINAZIONE INDIVIDUALE

16. Autogoverno della persona

Il cittadino che si riconosce nel Popolo Italiano Autodeterminato afferma il proprio diritto all'**autogoverno individuale** quale principio politico e giuridico da sottoporre, nelle forme previste dall'ordinamento, alla tutela delle autorità competenti.

L'autogoverno individuale viene inteso come:

- **autonomia della persona;**
- **libertà di coscienza;**
- **libertà di comunicazione;**
- **autodeterminazione informativa;**
- **autonomia patrimoniale;**
- **libertà di associazione;**
- **diritto alla privacy;**
- **diritto alla tutela giurisdizionale;**
- **diritto di partecipazione democratica.**

Tale affermazione non viene intesa quale autorizzazione unilaterale alla violazione delle leggi vigenti, bensì quale **riserva espressa di tutti i diritti fondamentali** che il soggetto dichiara di voler esercitare e difendere attraverso gli strumenti costituzionali, legislativi, amministrativi e giudiziari disponibili.

S. CLAUSOLA DI AUTODETERMINAZIONE DEMOCRATICA

17. Riserva di sovranità popolare

Si afferma il principio secondo cui le trasformazioni strutturali dell'ordinamento aventi incidenza diretta e generalizzata sui diritti fondamentali devono essere accompagnate dal **massimo livello possibile** di:

- **informazione pubblica;**
- **trasparenza;**
- **partecipazione;**
- **controllo parlamentare;**
- **controllo giudiziario;**
- **partecipazione civica;**
- **strumenti referendari ove previsti dall'ordinamento.**

Il principio di sovranità popolare deve essere interpretato come **obbligo permanente delle istituzioni di rendere conto dell'esercizio del potere.**

T. VAGLIO DEMOCRATICO RAFFORZATO

18. Richiesta di referendum nei casi costituzionalmente e legislativamente previsti

Qualora una misura di sorveglianza digitale comporti una trasformazione strutturale e permanente dell'esercizio delle libertà fondamentali, si chiede alle autorità competenti di valutare l'utilizzo degli **strumenti di democrazia diretta disponibili nell'ordinamento.**

In particolare, si chiede di valutare:

- **referendum consultivo;**
- **referendum abrogativo;**
- **referendum confermativo;**
- **consultazioni pubbliche;**
- **audizioni parlamentari;**
- **iniziative legislative popolari;**
- **procedure di partecipazione civica.**

La presente istanza richiede che la democrazia diretta non venga considerata un elemento meramente ornamentale quando siano in gioco trasformazioni strutturali della sfera dei diritti fondamentali, nei limiti e secondo le procedure previste dalla Costituzione e dal diritto applicabile.

U. PRINCIPIO DI NON ELUSIONE DEMOCRATICA

19. Divieto di conseguire indirettamente ciò che non potrebbe essere conseguito direttamente

Nessuna trasformazione strutturale dei diritti fondamentali dovrebbe essere realizzata mediante una successione di provvedimenti tecnici apparentemente separati che, considerati nel loro complesso, producano un sistema di sorveglianza generalizzata.

Si introduce pertanto il seguente principio:

PRINCIPIO DI NON ELUSIONE DEMOCRATICA E TECNOLOGICA

L'eventuale valutazione di legittimità deve considerare anche l'**effetto cumulativo** delle misure.

V. CLAUSOLA DI NON SORVEGLIANZA GENERALIZZATA

20. Riserva individuale

Il sottoscritto, quale cittadino e componente del Popolo Italiano Autodeterminato, formula espressa riserva di contestare ogni trattamento dei propri dati personali che ecceda i limiti stabiliti dalla legge, nonché ogni forma di sorveglianza che risulti **illegittima, arbitraria, sproporzionata o priva di adeguata base giuridica**.

Tale riserva comprende:

- **comunicazioni;**
 - **metadati;**
 - **dati finanziari;**
 - **dati biometrici;**
 - **dati di localizzazione;**
 - **dati comportamentali;**
 - **dati sanitari, ove applicabili;**
 - **dati relativi alle relazioni sociali;**
 - **dati derivanti da sistemi automatizzati.**
-

W. DIRITTO ALLA TRASPARENZA

21. Diritto di conoscere l'esistenza del trattamento

Si richiede che ogni cittadino possa conoscere, nei limiti stabiliti dalla legge:

- **quali dati vengono raccolti;**
- **chi li raccoglie;**
- **per quale finalità;**

- su quale base giuridica;
 - per quanto tempo vengono conservati;
 - con chi vengono condivisi;
 - quali algoritmi vengono utilizzati;
 - quali autorità possono accedervi;
 - quali procedure di contestazione sono disponibili;
 - quali rimedi esistono contro l'abuso.
-

X. DIRITTO ALLA CONTESTAZIONE E ALLA TUTELA GIURISDIZIONALE

22. Effettività del rimedio

Ogni cittadino deve poter ottenere tutela contro:

- raccolta illegittima;
- trattamento illegittimo;
- conservazione illegittima;
- profilazione illegittima;
- sorveglianza illegittima;
- trasferimento illegittimo;
- utilizzo secondario illegittimo;
- decisione automatizzata illegittima;
- divulgazione illegittima.

Il rimedio deve essere **effettivo, accessibile e tempestivo**.

Y. CLAUSOLA DI PREVENZIONE DEL DANNO

23. Tutela preventiva

Laddove sussista un rischio concreto di violazione grave e difficilmente reversibile dei diritti fondamentali, si chiede che siano adottate, secondo gli strumenti cautelari disponibili, misure idonee a impedire il verificarsi del danno prima che esso divenga irreversibile.

La tutela non deve essere esclusivamente successiva.

DOVE IL DANNO ALLA PRIVACY È IRREVERSIBILE, LA TUTELA DEVE POTER ESSERE PREVENTIVA.

Z. CLAUSOLA INDENNITARIA E RISARCITORIA INDIVIDUALE

24. Riserva espressa di azione risarcitoria

Il cittadino formula espressa e preventiva riserva di esercitare **ogni azione giudiziaria risarcitoria, restitutoria, inibitoria e di accertamento** consentita

dall'ordinamento qualora una misura illegittima determini una lesione concreta dei propri diritti.

La presente istanza formula altresì una **richiesta parametrica di risarcimento e/o indennizzo** pari a **€ 1.000.000,00 (un milione/00)** per ciascuna violazione individualmente accertata, ove tale importo sia ritenuto ammissibile e giustificato dal giudice competente alla luce della **natura, gravità, durata, diffusività, irreversibilità e conseguenze** della violazione.

Tale importo viene indicato quale **domanda risarcitoria e parametro di quantificazione**, e non quale automatica sanzione pecuniaria autoesecutiva.

AA. CRITERI DI QUANTIFICAZIONE DEL DANNO

25. Danno patrimoniale e non patrimoniale

La richiesta risarcitoria potrà comprendere, secondo le categorie riconosciute dall'ordinamento:

- **danno patrimoniale;**
- **danno non patrimoniale;**
- **danno alla riservatezza;**
- **danno all'autodeterminazione informativa;**
- **danno alla libertà personale;**
- **danno alla reputazione;**
- **danno derivante da profilazione;**
- **danno derivante da trattamento illecito dei dati;**
- **danno derivante da decisioni automatizzate;**
- **danno derivante dalla divulgazione dei dati;**
- **danno derivante dalla perdita del controllo sui dati personali;**
- **ulteriori danni concretamente dimostrabili.**

AB. RESPONSABILITÀ INDIVIDUALE E ISTITUZIONALE

26. Accertamento delle responsabilità

Qualora venga accertata una violazione, dovranno essere individuati, secondo le rispettive competenze e responsabilità:

- **autore dell'atto;**
- **autorità emanante;**
- **soggetto responsabile del trattamento;**
- **eventuale responsabile del trattamento per conto terzi;**
- **soggetto che ha materialmente disposto l'operazione;**
- **soggetti che abbiano concorso causalmente alla violazione.**

Non potrà essere automaticamente trasferita sul cittadino la conseguenza di una violazione derivante da un esercizio illegittimo del potere pubblico.

AC. RESPONSABILITÀ PER VIOLAZIONI SISTEMICHE

27. Danno cumulativo

Qualora una tecnologia produca violazioni sistematiche su una pluralità di cittadini, dovrà essere verificata anche la dimensione collettiva del fenomeno.

In particolare dovranno essere valutati:

- **numero delle persone interessate;**
- **durata della pratica;**
- **quantità di dati trattati;**
- **natura dei dati;**
- **grado di intrusività;**
- **possibilità di reidentificazione;**
- **possibilità di abuso;**
- **irreversibilità;**
- **conseguenze economiche e sociali.**

La diffusività della violazione non può costituire, di per sé, una ragione per diminuire la tutela del singolo.

AD. PRINCIPIO DI NON IMPUTABILITÀ DELLA COLPA AL CITTADINO

28. Il cittadino non può essere trasformato in oggetto permanente di sospetto

Si contesta ogni modello nel quale il cittadino, in assenza di elementi individualizzati e giuridicamente rilevanti, venga preventivamente trattato come potenziale autore di illeciti.

La prevenzione criminale deve rimanere distinta dalla **presunzione tecnologica generalizzata di sospetto**.

AE. PRINCIPIO DI PROTEZIONE DELLA PERSONA DIGITALE

29. Nuova dimensione dell'autodeterminazione

L'identità digitale, i dati personali, le comunicazioni private e i dati economici costituiscono componenti essenziali della dimensione contemporanea della persona.

La tutela della persona deve pertanto estendersi anche alla sua dimensione digitale.

Si afferma il seguente principio:

NESSUNA PERSONA PUÒ ESSERE RIDOTTA A UN PROFILO DIGITALE SOGGETTO A CLASSIFICAZIONE, MONITORAGGIO E VALUTAZIONE PERMANENTE DA PARTE DEL POTERE PUBBLICO O DI SOGGETTI PRIVATI INVESTITI DI FUNZIONI PUBBLICISTICHE.

AF. PRINCIPIO DI NEUTRALITÀ TECNOLOGICA

30. La tecnologia non può modificare i diritti

L'adozione di una nuova tecnologia non può essere utilizzata per ridurre il livello di tutela già riconosciuto alla persona.

Pertanto:

NESSUNA INNOVAZIONE TECNOLOGICA PUÒ ESSERE UTILIZZATA COME STRUMENTO PER AGGIRARE GARANZIE GIURIDICHE GIÀ ESISTENTI.

Se una condotta sarebbe illegittima se realizzata manualmente, la sua automatizzazione non la rende automaticamente lecita.

AG. PRINCIPIO DI REVERSIBILITÀ

31. Divieto di infrastrutture irreversibili

Ogni infrastruttura di sorveglianza deve essere:

- **delimitata;**
- **controllabile;**
- **auditabile;**
- **temporalmente definita;**
- **tecnicamente reversibile;**
- **giuridicamente revocabile.**

Devono essere previste procedure effettive per la **cancellazione dei dati raccolti illegittimamente** e per la **cessazione dei trattamenti non più giustificati**.

AH. RICHIESTA DI MORATORIA PRECAUZIONALE

32. Sospensione preventiva delle misure sproporzionate

Si chiede, nei casi in cui sussistano i presupposti giuridici, di disporre o promuovere una **moratoria cautelare** sulle misure di sorveglianza generalizzata che non abbiano ancora superato una verifica indipendente di compatibilità con i diritti fondamentali.

La moratoria dovrà permanere sino a:

- **completa identificazione della base giuridica;**
- **valutazione d'impatto;**
- **verifica di proporzionalità;**
- **valutazione di sicurezza;**
- **verifica della necessità;**
- **consultazione pubblica;**
- **definizione dei rimedi;**

- **controllo dell'autorità indipendente competente.**

AI. PETITUM — DOMANDE FORMALI

Alla luce di tutto quanto sopra esposto, si **CHIEDE FORMALMENTE**, ciascuna autorità per quanto di propria competenza, di:

1. **ACCERTARE** la natura fondamentale dei diritti alla privacy, alla segretezza delle comunicazioni, alla protezione dei dati personali e all'autodeterminazione informativa.
2. **ACCERTARE** che nessuna capacità tecnologica di sorveglianza costituisca, di per sé, fonte autonoma di legittimazione giuridica.
3. **ACCERTARE** la necessità di una specifica base legale per ogni trattamento invasivo.
4. **ACCERTARE** la necessità di verificare concretamente necessità, idoneità e proporzionalità di ogni misura.
5. **ACCERTARE** l'incompatibilità, ove sussistente, delle forme di sorveglianza generalizzata con i diritti fondamentali applicabili.
6. **INIBIRE, SOSPENDERE O LIMITARE**, secondo gli strumenti giuridici disponibili, le misure che risultino illegittime, sproporzionate o prive di adeguata base giuridica.
7. **IMPEDIRE**, ove giuridicamente possibile, l'implementazione di sistemi capaci di realizzare una sorveglianza generalizzata della popolazione non giustificata da specifiche esigenze legali.
8. **GARANTIRE** la tutela della crittografia e impedire vulnerabilità sistemiche non necessarie e sproporzionate.
9. **GARANTIRE** il principio di minimizzazione dei dati.
10. **GARANTIRE** il principio di limitazione delle finalità.
11. **GARANTIRE** il diritto alla conoscibilità dei trattamenti.
12. **GARANTIRE** il diritto di accesso, rettifica, cancellazione e opposizione nei casi previsti dalla normativa applicabile.
13. **GARANTIRE** il diritto a un rimedio effettivo davanti a un'autorità indipendente e al giudice competente.
14. **GARANTIRE** il controllo umano sulle decisioni automatizzate suscettibili di produrre conseguenze giuridiche o effetti sostanziali sulla persona.
15. **VERIFICARE** la compatibilità delle misure di sorveglianza digitale con gli **articoli 7, 8, 11, 16, 20, 21, 47 e 52 della Carta dei diritti fondamentali dell'Unione europea**.
16. **VERIFICARE** la compatibilità con gli **articoli 8, 10, 11 e 13 CEDU**, secondo la rispettiva applicabilità.
17. **VERIFICARE** la compatibilità con gli **articoli 17, 19 e 22 ICCPR**, secondo la rispettiva applicabilità.
18. **VERIFICARE** la compatibilità con gli **articoli 1, 2, 3, 13, 14, 15, 21 e 24 della Costituzione italiana** e con gli ulteriori principi costituzionali pertinenti.
19. **VALUTARE** la possibilità e necessità di sottoporre alle forme di democrazia diretta previste dall'ordinamento le trasformazioni strutturali incidenti sui diritti fondamentali.
20. **RICONOSCERE** il diritto del cittadino a partecipare ai procedimenti decisionali aventi incidenza sostanziale sulla propria libertà digitale.

21. **RICONOSCERE** il diritto del cittadino a contestare individualmente ogni trattamento illegittimo.
22. **RICONOSCERE** la piena riserva di azione giudiziaria individuale.
23. **RICONOSCERE** la riserva di richiesta risarcitoria fino all'importo parametrico di **€ 1.000.000,00** per ciascuna violazione individualmente accertata, con quantificazione definitiva rimessa all'autorità giudiziaria competente.
24. **ACCERTARE**, ove richiesto, l'eventuale responsabilità civile, amministrativa o di altra natura dei soggetti che abbiano causato una violazione concretamente accertata.
25. **ORDINARE O PROMUOVERE**, nei casi previsti dalla legge, la cessazione del trattamento illegittimo e la cancellazione dei dati illegittimamente acquisiti.
26. **GARANTIRE** che nessuna misura tecnologica possa produrre una riduzione del livello di tutela dei diritti fondamentali già riconosciuti.
27. **DISPORRE**, OVE NE RICORRANO I PRESUPPOSTI, le necessarie misure cautelari per impedire danni gravi, irreversibili o difficilmente riparabili.
28. **DICHIARARE** che ogni misura di sorveglianza che non superi il test di proporzionalità rafforzata (legalità, idoneità, necessità e proporzionalità in senso stretto) è inapplicabile nel territorio e nei confronti del Popolo Italiano Autodeterminato.
29. **RICONOSCERE** il diritto dei cittadini che aderiscono al Popolo Italiano Autodeterminato di rifiutare, in base al principio di autodeterminazione individuale, ogni forma di sorveglianza generalizzata non basata su un sospetto specifico, individualizzato e legalmente giustificato.
30. **GARANTIRE** che nessun cittadino possa essere sottoposto a trattamento discriminatorio per aver esercitato i diritti riconosciuti nella presente istanza.

AJ. CLAUSOLA SPECIALE DI AUTODETERMINAZIONE

33. Riserva individuale irrevocabile di tutela

Il cittadino sottoscrittore dichiara di non rinunciare, né espressamente né implicitamente, ai diritti fondamentali riconosciuti dalla Costituzione italiana, dal diritto dell'Unione europea e dagli strumenti internazionali applicabili.

Dichiara inoltre di riservarsi:

- **il diritto di petizione;**
- **il diritto di ricorso;**
- **il diritto di opposizione nei casi previsti;**
- **il diritto di accesso;**
- **il diritto alla tutela cautelare;**
- **il diritto alla tutela risarcitoria;**
- **il diritto alla protezione dei dati;**
- **il diritto alla segretezza delle comunicazioni;**
- **il diritto alla libertà di espressione;**
- **il diritto all'autodeterminazione informativa;**
- **ogni ulteriore diritto riconosciuto dall'ordinamento.**

AK. CLAUSOLA DI SALVAGUARDIA DEI DIRITTI

34. Interpretazione più favorevole alla persona

Qualora una disposizione possa essere interpretata secondo differenti modalità, dovrà essere privilegiata, nei limiti consentiti dall'ordinamento, quella maggiormente conforme alla tutela effettiva dei diritti fondamentali.

Nessuna disposizione dovrà essere interpretata come autorizzazione generale alla sorveglianza indiscriminata.

AL. CLAUSOLA DI NON RINUNCIA

35. Nessuna acquiescenza

La mancata contestazione immediata di una specifica misura non potrà essere interpretata, salvo quanto previsto dalla legge, come rinuncia ai diritti fondamentali né come consenso generale a future forme di sorveglianza.

Il consenso al trattamento dei dati, quando giuridicamente rilevante, deve rimanere distinto dalla mera impossibilità pratica di sottrarsi a un'infrastruttura digitale.

AM. CLAUSOLA DI REVISIONE DEMOCRATICA

36. Riesame periodico

Qualsiasi infrastruttura permanente di sorveglianza dovrà essere sottoposta a riesame periodico relativamente a:

- **efficacia;**
- **necessità;**
- **proporzionalità;**
- **sicurezza;**
- **impatto sui diritti;**
- **numero delle persone interessate;**
- **falsi positivi;**
- **incidenti;**
- **abusi;**
- **accessi non autorizzati;**
- **utilizzi secondari;**
- **costi sociali;**
- **risultati effettivamente conseguiti.**

La mera esistenza di una tecnologia non costituisce prova della sua necessità permanente.

AN. PRINCIPIO FONDAMENTALE DI NON TRASFORMAZIONE DEL CITTADINO IN OGGETTO DI SORVEGLIANZA

Si chiede di riconoscere formalmente il seguente principio:

IL CITTADINO NON È UN DATO DA SORVEGLIARE, MA UNA PERSONA TITOLARE DI DIRITTI.

E conseguentemente:

LA SICUREZZA DELLA COLLETTIVITÀ NON PUÒ ESSERE PERSEGUITA MEDIANTE LA NORMALIZZAZIONE DELLA SORVEGLIANZA PERMANENTE DI TUTTI I CITTADINI.

AO. PRINCIPIO DI EQUILIBRIO TRA SICUREZZA E LIBERTÀ

La presente istanza non contesta in via generale la funzione dello Stato e delle istituzioni nel contrasto:

- **alla criminalità;**
- **al terrorismo;**
- **al riciclaggio;**
- **agli abusi sui minori;**
- **alla criminalità organizzata;**
- **alle frodi;**
- **agli attacchi informatici;**
- **alle minacce alla sicurezza pubblica.**

Contesta e sottopone a verifica esclusivamente l'utilizzo di strumenti che, per **ampiezza, durata, automatismo, indiscriminatezza o invasività**, possano eccedere quanto necessario e proporzionato per perseguire tali finalità.

La vera sicurezza democratica deve infatti essere costruita attraverso l'equilibrio tra:

SICUREZZA + LIBERTÀ + PRIVACY + PROPORZIONALITÀ + CONTROLLO GIUDIZIARIO + RESPONSABILITÀ PUBBLICA.

AP. FORMULA SOLENNE DI RISERVA

Il sottoscritto, in qualità di cittadino e componente del Popolo Italiano Autodeterminato, **FORMULA ESPRESSA RISERVA DI OGNI DIRITTO, AZIONE, ECCEZIONE, OPPOSIZIONE, RICORSO, DOMANDA CAUTELARE, DOMANDA INIBITORIA E PRETESA RISARCITORIA** riconosciuta dall'ordinamento nazionale, europeo e internazionale applicabile.

La presente istanza deve intendersi quale:

ATTO DI PETIZIONE + ATTO DI DIFFIDA ALLA VIOLAZIONE DEI DIRITTI + RISERVA DI TUTELA GIURISDIZIONALE + RICHIESTA DI PREVENZIONE DEL DANNO + RISERVA RISARCITORIA INDIVIDUALE.

AQ. RICHIESTA DI PROTOCOLLAZIONE E RISCONTRO

Si richiede formalmente:

- la **protocollazione** della presente istanza;
- l'**identificazione** dell'ufficio competente;
- la **comunicazione** del responsabile del procedimento, ove previsto;
- la **comunicazione** delle autorità alle quali l'istanza sia eventualmente trasmessa;
- un **riscontro scritto e motivato**;
- l'**indicazione** delle basi giuridiche applicabili;
- l'**indicazione** degli strumenti di ricorso disponibili;
- la **conservazione agli atti** della presente riserva di diritti.

AR. CONCLUSIONE

La presente istanza afferma un principio essenziale dell'ordinamento democratico:

IL POTERE TECNOLOGICO NON PUÒ DIVENTARE, PER LA SOLA ESISTENZA DELLA TECNOLOGIA, POTERE GIURIDICO.

E ancora:

LA LOTTA ALLA CRIMINALITÀ NON PUÒ TRASFORMARSI IN SORVEGLIANZA GENERALIZZATA.

LA SICUREZZA NON PUÒ DIVENTARE UN'AUTORIZZAZIONE GENERALE ALL'ACCESSO ALLA VITA PRIVATA.

L'INNOVAZIONE DIGITALE NON PUÒ COMPORTARE UNA RIDUZIONE AUTOMATICA DELLA LIBERTÀ.

LA PERSONA PRECEDE L'ALGORITMO, IL DIRITTO PRECEDE LA TECNOLOGIA E LA DEMOCRAZIA PRECEDE L'ESERCIZIO DEL POTERE.

Pertanto, ogni misura di sorveglianza digitale dovrà essere sottoposta a verifica secondo la seguente gerarchia sostanziale:

**PERSONA → DIRITTI FONDAMENTALI → LEGALITÀ → NECESSITÀ →
PROPORZIONALITÀ → TRASPARENZA → CONTROLLO INDIPENDENTE → TUTELA
GIURISDIZIONALE → DEMOCRAZIA.**

E nessuna infrastruttura tecnologica potrà essere considerata legittima esclusivamente perché tecnicamente possibile.

CLAUSOLA FINALE DI SALVAGUARDIA

La presente istanza non costituisce rinuncia ad alcun diritto, né acquiescenza rispetto a eventuali trattamenti futuri, presenti o pregressi che risultino illegittimi.

Ogni diritto, azione, eccezione, ricorso, domanda cautelare, domanda inibitoria, domanda di cancellazione, domanda restitutoria e domanda risarcitoria resta espressamente riservato, nei limiti e secondo le procedure previste dall'ordinamento competente.

SI CHIEDE CHE LA PRESENTE ISTANZA SIA ACQUISITA AGLI ATTI, PROTOCOLLATA, ESAMINATA E TRASMESSA AGLI ORGANI COMPETENTI PER OGNI DETERMINAZIONE DI RISPETTIVA COMPETENZA.

LUOGO E DATA: _____

IL RICHIEDENTE: _____

QUALIFICA: CITTADINO / COMPONENTE DEL POPOLO ITALIANO
AUTODETERMINATO

FIRMA: _____

RECAPITO PER LE COMUNICAZIONI: _____

PEC / E-MAIL: _____

FORMULA DI RISERVA FINALE

OMNIA IURA RESERVATA.

TUTTI I DIRITTI FONDAMENTALI, COSTITUZIONALI, EUROPEI E INTERNAZIONALI RESTANO ESPRESSAMENTE RISERVATI.

NESSUN SILENZIO, NESSUNA TOLLERANZA E NESSUNA PARTECIPAZIONE A UN SISTEMA TECNOLOGICO POTRÀ ESSERE INTERPRETATA, SALVO ESPRESSA DISPOSIZIONE DI LEGGE, COME RINUNCIA AI DIRITTI INVIOLABILI DELLA PERSONA.

ALLEGATO — INTEGRAZIONE CON LA STRATEGIA DI DIRITTO INTERNAZIONALE EX ART. 38 DELLO STATUTO DELLA CIG

La presente istanza è ulteriormente rafforzata dai principi del diritto internazionale ai sensi dell'**articolo 38 dello Statuto della Corte Internazionale di Giustizia**:

Fonte ex Art. 38	Applicazione a sorveglianza e controllo digitale	Riferimenti
Art. 38(1)(a) — Trattati	I trattati sui diritti umani	ICCPR art. 17; CEDU art. 8;

	vietano la sorveglianza arbitraria e proteggono la privacy	Carta UE artt. 7, 8
Art. 38(1)(b) — Consuetudine	Il diritto alla privacy e la libertà dalla sorveglianza arbitraria sono norme consuetudinarie	Nicaragua (1986); Dichiarazione Universale dei Diritti Umani
Art. 38(1)(c) — Principi generali	I principi di <i>nulla potestas sine populo</i> , proporzionalità e dignità umana richiedono controllo democratico	Principi comuni alle nazioni civili
Art. 38(1)(d) — Decisioni e dottrina	La giurisprudenza internazionale vieta la sorveglianza di massa e la conservazione dei dati senza garanzie	Digital Rights Ireland (2014); S. e Harper (2008)
Art. 38(2) — <i>Ex aequo et bono</i>	L'equità richiede che le libertà fondamentali siano protette da intrusioni tecnologiche sproporzionate	Applicazione equitativa in assenza di disciplina specifica

Il CLNI, in qualità di autorità nazionale provvisoria del Popolo Italiano in Autodeterminazione, si fa portavoce della presente istanza, confidando che le autorità competenti e la comunità internazionale vogliano riconoscere la legittimità e l'urgenza delle questioni sollevate e adottare ogni determinazione necessaria a garantire che le scelte fondamentali in materia di sorveglianza e controllo digitale siano rimesse, come di dovere, al popolo sovrano.

1. Le somme eventualmente riconosciute a titolo di risarcimento saranno versate nel **conto della Tesoreria del SIPSE**, accessibile tramite il sito

ufficiale <https://sipsesovereign.org/>, per essere destinate alla riparazione dei danni subiti dai Popoli d'Europa e dal **Popolo Veneto**, alla ricostituzione del tessuto produttivo e sociale, e alla promozione di strumenti di emancipazione economica sovrana quali il **Zecchino Veneto** e i **V-Bond**.

Redatto e adottato in nome dei Popoli d'Europa e del **Popolo Veneto**.

Sede di riferimento:

Sistema delle Istituzioni dei Popoli per la Sovranità Economica (SIPSE)
<https://sipsesovereign.org/>

In coordinamento con:

Comitato di Liberazione Nazionale Italiano (CLNI)
Reti istituzionali dei Popoli d'Europa
Rappresentanze del Popolo Veneto

Notificato a:

Corte Europea dei Diritti dell'Uomo • Corte di Giustizia dell'Unione Europea • Corte Penale Internazionale • OCSE – Punto di Contatto Nazionale • Segretario Generale delle Nazioni Unite • Commissione Europea • Banca Centrale Europea • Parlamento Europeo • Comitato ONU per i Diritti Economici, Sociali e Culturali • Comitato Europeo dei Diritti Sociali • Mediatore Europeo • Autorità nazionali, europee e internazionali competenti

DEPOSITO CONGIUNTO E NOTARIZZAZIONE SU BLOCKCHAIN

ATTO N. 2026/09-IPE

OGGETTO: Istanza internazionale dei Popoli d'Europa e del Popolo Veneto del SIPSE – Atto di Autorità, Protezione dei Diritti Inalienabili e Affermazione della Sovranità Economica contro le Coercizioni Sistemiche della Banca Centrale Europea.

DATA: [/]

ORA: []

LUOGO: [____]

DEPOSITANTE: [Nome e Cognome / Ente / Rappresentanza]

QUALITÀ: [Rappresentante legale / Portatore dell'istanza / Delegato del SIPSE / Delegato del Popolo Veneto]

DOCUMENTO DEPOSITATO: Atto n. 2026/09-IPE, composto da [] *pagine, più allegati n. []*.

FORMATO: [originale digitale PDF / originale cartaceo / copia conforme / duplice originale]

HASH SHA-256 DEL DOCUMENTO: []

HASH SHA-256 DEGLI ALLEGATI: []

SEZIONE A – DEPOSITO PRESSO LA CANCELLERIA DELL'ORGANIZZAZIONE SUI GENERIS SIPSE

Il/La sottoscritto/a [Nome e Cognome], in qualità di [qualità], deposita presso la Cancelleria dell'Organizzazione sui generis **SIPSE – Sistema delle Istituzioni dei Popoli per la Sovranità Economica**, con sede in [indirizzo], il documento sopra indicato, in [originale / copia conforme / duplice originale], chiedendone la registrazione al **Protocollo Generale del SIPSE** e il deposito permanente agli atti.

Registro di Protocollo SIPSE:

N. []/2026

Categoria: [Atti di Sovranità e Tutela dei Diritti Inalienabili]

Data di registrazione: []

Ora di registrazione: []

Hash SHA-256 registrato: [_____]

Hash blockchain associato: [_____]

Attestazione del Cancelliere SIPSE:

Il sottoscritto Cancelliere attesta che il documento è stato ricevuto, protocollato e depositato negli archivi del SIPSE in data [], **al n. []/2026**, unitamente alla notarizzazione su blockchain di cui alla Sezione C.

Timbro e firma: _____

SEZIONE B – DEPOSITO PRESSO LA CANCELLERIA DELLA CORTE INTERNAZIONALE DI AUTODETERMINAZIONE DEI POPOLI

Il/La sottoscritto/a [Nome e Cognome], in qualità di [qualità], deposita presso la Cancelleria della **Corte Internazionale di Autodeterminazione dei Popoli**, con sede in [indirizzo], il medesimo Atto n. 2026/09-IPE, chiedendone l'iscrizione al **Registro dei Depositi di Istanze Collettive e dei Ricorsi dei Popoli** e la notifica ai soggetti destinatari indicati nell'Atto stesso.

Registro di Deposito della Corte:

N. []/2026

Categoria: [Istanza Collettiva dei Popoli – Tutela dei Diritti Inalienabili e della Sovranità Economica]

Data di deposito: []

Ora di deposito: []

Hash SHA-256 registrato: [_____]

Hash blockchain associato: [_____]

Attestazione del Cancelliere della Corte:

Il sottoscritto Cancelliere attesta che il documento è stato ricevuto, iscritto al Registro dei Depositi e acquisito agli atti della Corte in data [], **al n. []/2026**, unitamente alla notarizzazione su blockchain di cui alla Sezione C.

Timbro e firma: _____

SEZIONE C – NOTARIZZAZIONE SU BLOCKCHAIN

Il documento oggetto del presente deposito è stato sottoposto a **notarizzazione su blockchain** mediante ancoraggio crittografico e marcatura temporale, al fine di garantirne l'esistenza, l'integrità, l'immutabilità e la verificabilità pubblica.

Dati della notarizzazione blockchain:

- **File notarizzato:** Atto n. 2026/09-IPE
- **Formato file:** [PDF / TXT / DOCX / altro]
- **Dimensione file:** [____] bytes
- **Algoritmo di hash:** SHA-256
- **Hash SHA-256 del file:** [_____]
- **Hash SHA-256 degli allegati:** [_____]
- **Timestamp UTC:** [_____]
- **Blockchain utilizzata:** [Ethereum / Polygon / Bitcoin / Arweave / altra]
- **Rete:** [mainnet / testnet]
- **Transazione hash / TXID:** [_____]
- **Numero del blocco:** [_____]
- **Smart contract / notary contract:** [_____]
- **Standard:** [ERC-721 / ERC-1155 / OP_RETURN / altro]
- **IPFS CID:** [_____]
- **Wallet address del depositante:** [_____]
- **Explorer di verifica:** [https://_____]
- **QR code di verifica:** [allegato / generato]
- **Notaio / perito blockchain:** [Nome e Cognome / Ente]
- **Firma digitale del notaio / perito:** [_____]

Attestazione di notarizzazione blockchain:

Si attesta che il documento sopra descritto è stato ancorato alla blockchain indicata in data **[] alle ore []** UTC, con il TXID sopra riportato. La notarizzazione su blockchain certifica l'esistenza del documento a quella data e ora e la corrispondenza tra il file depositato e l'hash registrato. Qualsiasi modifica successiva al file comporterebbe un hash diverso e renderebbe impossibile la verifica di corrispondenza.

Clausola di salvaguardia:

La notarizzazione su blockchain costituisce prova tecnologica di esistenza e integrità del documento, nonché strumento di pubblicità e trasparenza. Essa non sostituisce, ove richiesta dalla legge, la notarizzazione tradizionale o l'autenticazione da parte di pubblico ufficiale, ma integra e rafforza il deposito presso la Cancelleria del SIPSE e presso la Cancelleria della Corte Internazionale di Autodeterminazione dei Popoli.

SEZIONE D – DICHIARAZIONE FINALE DI DOPPIO DEPOSITO E NOTARIZZAZIONE BLOCKCHAIN

Il presente Atto è depositato in duplice originale presso:

1. la Cancelleria dell'Organizzazione sui generis **SIPSE**;
2. la Cancelleria della **Corte Internazionale di Autodeterminazione dei Popoli**.

Il medesimo Atto è inoltre **notarizzato su blockchain** ai sensi della Sezione C, con registrazione del relativo hash SHA-256, del timestamp UTC, del TXID e degli altri dati di verifica.

Il doppio deposito e la notarizzazione su blockchain sono effettuati ai fini di pubblicità, certezza, conservazione, notifica, verificabilità e opponibilità *erga omnes*, senza pregiudizio per ogni ulteriore azione dinanzi alle giurisdizioni nazionali, europee e internazionali competenti.

Luogo e data: [_____]

Firma del Depositante: _____

Timbro SIPSE: _____

Timbro Corte Internazionale di Autodeterminazione dei

Popoli: _____

Attestazione blockchain / TXID: _____

E-Mail: ambasciatore.sv@statovenetoinautodeterminazione.org

E-Mail: procuragenerale@statovenetoinautodeterminazione.org

E-Mail: comitatoliberazionenazionaleitaliano@pec.it

E-Mail: statovenetoinautodeterminazione@pec.it

E-Mail: confederazionestatiunitideuropa@pec.it

Sito Istituzionale: <https://sipsesovereign.org/>

Sito Istituzionale: <https://statovenetoinautodeterminazione.org/>

Sito Istituzionale: <https://comitatoliberazionenazionaleitaliano.org/>

E-Mail: cancelleria@statovenetoinautodeterminazione.org

E-Mail: ufficioprotocollo@statovenetoinautodeterminazione.org

E-Mail: segreteria generale@statovenetoinautodeterminazione.org

E-Mail: corteinternazionaleaut.popoli@statovenetoinautodeterminazione.org



For the General Assembly of SIPSE



Franco Paluan

*Head of the Savi – Venetian State in Self-Determination
Responsible for the legal and technical functions of SIPSE*



His Excellency Paolo Albertin

*President of the Self-Determined Italian People
Special Representative of the Peoples of Europe adhering to SIPSE*



JUDICIAL APPLICATION FOR ASCERTAINMENT, INJUNCTION, AND RECOGNITION OF DEMOCRATIC VALUE

WITH A CLAUSE OF SELF-DETERMINATION AND INDIVIDUAL REDRESS



INAPPLICABILITY OF DIGITAL SURVEILLANCE AND CONTROL RULES FOR THE SELF-DETERMINED ITALIAN PEOPLE

Request for radical inapplicability, unenforceability, and nullification of the absolute debt of legitimation of any rule, directive, or proposal regarding:
MASS SURVEILLANCE, CHAT CONTROL, ANTI-MONEY LAUNDERING DIRECTIVES, INTRUSIVE FINANCIAL CONTROLS

A. SUBJECT OF THE APPLICATION

The inapplicability, unenforceability, and nullity of any administrative or judicial act imposing forms of surveillance, monitoring, and digital control without the preventing will of the people is requested.

The principle of individual self-governance is affirmed for every citizen belonging to the self-determined Italian people, with a judicial reservation of one million euros for each act imposing violations of fundamental and inalienable rights against popular sovereignty.


INVIOLENT RIGHTS
 Privacy, Freedom of communication, Human dignity, Self-determination, Informative self-autonomy


INDEMNITY CLAUSE
€ 1,000,000.00
 for every verified individual violation

FUNDAMENTAL RIGHTS VIOLATED

-  Respect for private and family life (Art. 8 CFREU - Art. 7 CDFUE)
-  Protection of personal data (Art. 8 CDFUE - Reg. UE 2016/679)
-  Freedom of expression and information (Art. 11 CDFUE - Art. 10 CEDU)
-  Liberty and security of the person (Art. 15 Cost. - Art. 5 CEDU)
-  Personal liberty (Art. 13 Cost.)
-  Effective judicial protection (Art. 24 Cost. - Art. 47 CDFUE - Art. 13 CEDU)

B. PREMISES IN FACT AND IN LAW: THE INSUFFICIENCY OF DERIVED REPRESENTATION

1 THE FAILURE OF THE DERIVED REPRESENTATIVE MODEL

- The system of delegate representation has exhausted its function at a time when it makes decisions that are offensive to the freedom, privacy, dignity, and self-criticism of citizens.
- No rule that is a "top-down" act has its own force from a direct and expressed democratic will.
- Radical defect of competence, mandate, and democratic legitimation.



2 THE ORIGINAL SOVEREIGNTY OF THE ITALIAN PEOPLE

- The Italian people retain the inalienable right to self-determination and self-governance.
- No treaty, intergovernmentally agreed directive, or bureaucratic standard can prevail over the reservation of popular sovereignty in fundamental rights matters.
- The digital control and mass surveillance standard is an act of evasion of the democratic constitutional order.



3 INDIVIDUAL SELF-GOVERNMENT AND THE RIGHT TO REDRESS

- When the derived State violates the social pact and encroaches upon inviolable rights without the will of the people, the bond of political subjection of the citizen is broken.
- Every citizen retains the right to act individually for the protection of their own judicial and personal sphere.
- Judicial action and individual claim for individual patrimonial compensation.

INVIOLENT RIGHTS INDIVIDUALE
€ 1,000,000.00



C. FORMULATION OF REQUESTS, ASCERTAINMENTS, AND INDEMNITY CLAUSES

1 THE INAPPLICABILITY PENALTY FOR THE SELF-DETERMINED ITALIAN PEOPLE

- The total inapplicability, unenforceability, and nullity of any constitutional rule concerning the monitoring of communications (Chat Control) and the forced financial control of self-determined Italian citizens is declared.
- Defect of manifestly unlawful approval of referendums on direct democracy.





2 THE RECOGNITION OF THE AUTHORITY OF INDIVIDUAL SELF-GOVERNMENT

- The individual self-governed citizen acts to protect the original constitutional legitimacy, refusing subjection to standard rules imposed without direct popular consent.
- Any decision violating fundamental rights of freedom is devoid of legitimacy and does not bind the sovereign citizen.



NO TWINTIAL NORMEITANCE
NO TO INALIENABLE



3 THE INDEMNITY CLAUSE AND REDRESS (1,000,000 € PER VIOLATION)

- Any single decision, administrative or directive act that violates fundamental rights and inalienable liberties without prior legitimate consultation, forces the citizen to judicially demand an individual patrimonial indemnity of € 1,000,000.00 (ONE MILLION EUROS).

INDIVIDUAL PATRIMONIAL INDEMNITY REDRESS
€ 1,000,000.00
 for every verified violation



REQUESTED FUNDAMENTAL PRINCIPLES


 LEGALITY


 PROPORTIONALITY


 NECESSITY


 DATA MINIMIZATION


 TRANSPARENCY


 JUDICIAL CONTROL


 DEMOCRATIC PARTICIPATION


 SELF-DETERMINATION


 INDIVIDUAL REDRESS

DIRECT DEMOCRACY

No structural surveillance measure can be introduced without the democratic will of the sovereign people.

LEGAL REFERENCE BASES

- Constitution of the Italian Republic: art. 1, 2, 3, 13, 14, 15, 21, 24, 25, 42
- Charter of Fundamental Rights of the European Union: art. 7, 8, 11, 16, 20, 21, 47, 52
- European Convention on Human Rights: art. 8, 10, 11, 13
- European Social Charter: art. 17, 19, 23
- EU Regulation 2016/679 (GDPR) and applicable European directives
- Principles of EU law and national and European jurisprudence

RESERVATION AND SIGNATURE CLAUSE

Any right, action, exception, opposition, appeal, cautionary demand, injunctive action, and claim for damages remains expressly reserved, reserved for the citizen and according to the procedures provided by the legal system.

Place and date: The applicant (signature): _____



LEGAL PETITION FOR ACCERTATION, INJUNCTIVE RELIEF, AND RECOGNITION OF DEMOCRATIC SCRUTINY WITH A CLAUSE OF SELF-DETERMINATION AND INDIVIDUAL COMPENSATION

NON-APPLICABILITY, DISAPPLICATION, AND LEGITIMACY REVIEW OF SURVEILLANCE MEASURES, DIGITAL MONITORING, AND INVASIVE FINANCIAL CONTROL AGAINST THE SELF-DETERMINED ITALIAN PEOPLE

FORMAL PETITION FOR ACCERTATION, PROTECTIVE INJUNCTION, DAMAGE PREVENTION, DEMOCRATIC SCRUTINY, PROTECTION OF FUNDAMENTAL RIGHTS, INDIVIDUAL SELF-DETERMINATION, AND RESERVATION OF COMPENSATORY ACTION

ADDRESSED TO:

- Authorities of the Italian Republic
 - Institutions of the European Union
 - Competent Supervisory Authorities
 - Competent Judicial and Administrative Authorities
 - Competent Legislative Bodies
 - Every Public Authority or Subject Invested with Powers of Control, Monitoring, or Processing of Personal Data
-

PREAMBLE

This Petition is formulated in the exercise of the rights of petition, participation, democratic self-determination, judicial protection, protection of private life, personal liberty, freedom of communication, freedom of expression, personal data protection, economic freedom, and defense of inviolable rights recognized by the constitutional, European, and international legal orders.

The Petition assumes as a fundamental principle that public security, crime prevention, and the protection of the financial system constitute legitimate objectives only when pursued through instruments that are:

- **in conformity with the law;**
- **necessary;**
- **proportionate;**
- **determined;**
- **controllable;** and
- **respectful of fundamental rights.**

No public interest objective can automatically transform into a title for establishing generalized, indiscriminate, or disproportionate forms of surveillance of the population.

This Petition concerns, in particular, every regulatory, administrative, technical, or infrastructural measure capable of introducing or expanding:

- systematic monitoring of private communications;
- generalized scanning of digital content;
- automated control of personal communications;
- preventive surveillance of messaging;
- weakening or circumvention of encryption;
- mass collection of metadata;
- behavioral profiling;
- financial monitoring exceeding the specific requirements provided for by law;
- generalized interconnection of databases;
- automated economic surveillance;
- systems for automatic identification or classification of citizens;
- mechanisms for automatic blocking or limitation of access to economic resources;
- any further technology capable of transforming public or private infrastructures into permanent instruments of generalized surveillance.

PREMISE — THE CLNI AS THE NATIONAL AUTHORITY OF THE SELF-DETERMINED ITALIAN PEOPLE

This Petition is promoted by the **Italian National Liberation Committee (CLNI)** , which presents and operates as the **provisional national authority** of the **Self-Determined Italian People**.

The CLNI is not a political movement among others, nor a private association: it claims and assumes the role of a **metaconstitutional institutional subject**, called to represent that part of the Italian people which, considering the legitimacy of the current state order to be exhausted, has decided to reorganize itself to regain full control of its sovereignty, in continuity with the principles of the Resistance and with the tradition of the National Liberation Committees which, from 1943 to 1946, represented the will of the Italian people against occupation and dictatorship.

This legitimacy finds foundation in the principles of international law, in particular in **Article 1 of the Charter of the United Nations**, which enshrines the principle of "**equal rights and self-determination of peoples**" , and in **Article 1 of the International Covenant on Civil and Political Rights**, according to which "all peoples have the right to self-determination" and "freely determine their political status and freely pursue their economic, social and cultural development."

The CLNI, as the national authority of the Self-Determined Italian People, considers it its institutional duty to:

- **ascertain** the constitutionally relevant nature of surveillance and digital control transformations;
- **request** that they be subjected to prior and effective democratic scrutiny;
- **monitor** that the fundamental rights of the Italian people are not compressed by technological choices made in the absence of popular legitimacy;

- **propose** the legal and participatory instruments necessary to ensure that fundamental choices on surveillance and data protection are entrusted to the sovereign people.
-

A. SUBJECT MATTER OF THE PETITION

1. Main Request

This Petition formally requests the **ascertainment, prevention, and, where the legal prerequisites exist, the inhibition or disapplication** of surveillance and digital control measures incompatible with fundamental rights, as well as the recognition of the necessity of **effective democratic control** over regulatory and technological transformations having a structural impact on individual freedoms.

In particular, it is requested that no measure having a general, systematic, or potentially permanent character of **surveillance of communications or digital control of the population** be automatically considered legitimate merely because it is contained in a legislative, regulatory, or administrative act.

Its legitimacy must be verified according to:

LEGAL BASIS + COMPETENCE + NECESSITY + PROPORTIONALITY + DETERMINATENESS + SPECIFIC PURPOSE + MINIMIZATION + INDEPENDENT CONTROL + EFFECTIVE JUDICIAL PROTECTION.

B. PRINCIPLE OF SUPREME PROTECTION OF FUNDAMENTAL RIGHTS

2. Primacy of the Person and Inviolable Rights

The Italian constitutional order recognizes the centrality of the person and inviolable rights.

In particular, the following are relevant:

- **Article 1 of the Constitution** — popular sovereignty;
- **Article 2** — recognition and guarantee of inviolable rights;
- **Article 3** — equality;
- **Article 13** — personal liberty;
- **Article 14** — inviolability of the home;
- **Article 15** — freedom and secrecy of communications;
- **Article 21** — freedom of expression;
- **Article 24** — right to judicial protection;
- **Article 25** — principle of legality;
- **Article 42** — right to property;
- as well as further applicable constitutional principles.

The freedom and secrecy of communications constitute a fundamental guarantee.

Consequently, any technological system capable of systematically analyzing private communications must be subjected to a particularly rigorous control over its legal basis and the proportionality of the measures adopted.

C. EUROPEAN AND INTERNATIONAL PROTECTION

3. Charter of Fundamental Rights of the European Union

The following must be specifically considered, among others:

- **Article 7** — respect for private and family life;
- **Article 8** — protection of personal data;
- **Article 11** — freedom of expression and information;
- **Article 16** — freedom to conduct a business;
- **Article 17** — right to property;
- **Article 20** — equality before the law;
- **Article 21** — non-discrimination;
- **Article 47** — right to an effective remedy and to a fair trial;
- **Article 52** — scope and interpretation of rights and principles.

Every limitation must therefore comply with the conditions provided for by the European system of fundamental rights protection.

D. EUROPEAN CONVENTION ON HUMAN RIGHTS

4. Protection of Private Life and Communications

The following must be considered, according to their respective applicability:

- **Article 8 ECHR** — right to respect for private and family life, home, and correspondence;
- **Article 10 ECHR** — freedom of expression;
- **Article 11 ECHR** — freedom of assembly and association;
- **Article 13 ECHR** — right to an effective remedy.

Any surveillance system must therefore be subject to effective guarantees against:

- arbitrariness;
 - excess;
 - indiscriminate collection;
 - further use of data.
-

E. INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS

5. Protection Against Arbitrary Interference

Reference is also made to the protection provided, as applicable, by **Articles 17, 19, and 22 of the International Covenant on Civil and Political Rights**.

The fundamental principle is that **no person shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence**.

The fight against crime does not eliminate this principle.

On the contrary, precisely the existence of public security objectives makes it necessary to establish rigorous, verifiable, and legally controllable limits.

F. PRINCIPLE OF TECHNOLOGICAL LEGALITY

6. No Surveillance Power Without a Determined Legal Basis

No public or private subject can acquire a general power of surveillance simply because it possesses the technical capacity to exercise it.

The following principle is therefore affirmed:

TECHNOLOGICAL CAPACITY TO MONITOR DOES NOT CONSTITUTE, IN ITSELF, A LEGAL AUTHORIZATION FOR MONITORING.

The technical availability of a system cannot automatically transform into an autonomous source of public power.

G. PROHIBITION OF GENERALIZED SURVEILLANCE

7. Principle of Individualization of Control

Surveillance measures must, where required by law and according to the relevant prerequisites, be specifically justified with respect to determined purposes and concretely relevant subjects or situations.

A methodology according to which:

first, data is systematically collected from everyone → then, possible suspicious elements are sought

cannot automatically be considered proportionate.

The logic of prevention cannot transform the entire population into a permanent set of subjects subjected to control.

Recognition of the following principle is therefore requested:

GENERAL PRESUMPTION OF NON-SURVEILLANCE OF THE NON-SUSPECTED CITIZEN

H. "CHAT CONTROL" AND SCANNING OF COMMUNICATIONS

8. Prohibition of the Transformation of Private Communication into an Object of Generalized Control

Any proposal or regulation commonly referred to as "Chat Control," as well as any technology having substantially equivalent effects, must be subjected to rigorous examination of:

- **necessity;**
- **proportionality;**
- **effectiveness;**
- **accuracy;**
- **minimization of false positives;**
- **protection of encryption;**
- **protection of confidentiality;**
- **judicial control;**
- **temporal limitation;**
- **subjective limitation;**
- **limitation of purposes.**

A generic objective of combating crime cannot be considered sufficient to automatically legitimize the generalized scanning of communications of non-suspected persons.

I. PROTECTION OF ENCRYPTION

9. Encryption as an Instrument of Security and Freedom

Encryption constitutes simultaneously an instrument of:

- **cybersecurity;**
- **data protection;**
- **confidentiality;**
- **economic security;**
- **infrastructure protection;**
- **communicative freedom.**

Any technical obligation intended to create systemic vulnerabilities, privileged access, indiscriminate scanning, or equivalent mechanisms of encryption circumvention must be subjected to rigorous risk assessment.

Recognition of the following principle is therefore requested:

NO PUBLIC SECURITY MEASURE CAN BE REALIZED THROUGH THE CREATION OF A GENERAL VULNERABILITY CAPABLE OF EXPOSING THE ENTIRE POPULATION TO CYBER RISKS GREATER THAN THOSE THE MEASURE INTENDS TO PREVENT.

L. PROTECTION OF PERSONAL DATA

10. Principles of Minimization and Limitation of Purposes

Any processing must be subjected, according to the applicable regulatory framework, to the principles of:

- **lawfulness;**
- **fairness;**
- **transparency;**
- **purpose limitation;**
- **minimization;**
- **accuracy;**
- **storage limitation;**
- **integrity;**
- **confidentiality;**
- **accountability.**

Particular attention must be paid to the possibility that data originally collected for one purpose may subsequently be used for different purposes.

Recognition of the following principle is therefore requested:

NO FUNCTION CREEP

No system created for a determined purpose can be progressively transformed into a general surveillance infrastructure without a new, specific, and rigorous legal basis.

M. FINANCIAL SURVEILLANCE AND ANTI-MONEY LAUNDERING REGULATION

11. Combating Money Laundering and Protection of the Person

The fight against money laundering, terrorist financing, and economic crime constitutes a legitimate objective of public interest.

However, this objective must be pursued through instruments that are:

- **targeted;**
- **necessary;**
- **proportionate;**
- **founded on law;**
- **subject to control;**
- **respectful of data protection;**
- **subject to temporal and purpose limitations.**

A system in which every citizen is treated as a potential suspect through collection and analysis exceeding the concrete needs of the regulation cannot automatically be considered proportionate.

N. PRINCIPLE OF REINFORCED PROPORTIONALITY

12. Four Levels of Control

Every invasive measure must pass at least four tests:

I. LEGALITY

Does a precise and accessible legal basis exist?

II. SUITABILITY

Is the measure actually suitable to achieve the declared purpose?

III. NECESSITY

Does a less invasive solution of fundamental rights exist?

IV. PROPORTIONALITY IN THE STRICT SENSE

Is the public benefit obtained proportionate to the sacrifice imposed on the citizen?

Where a measure fails any of these tests, its modification, limitation, suspension, or disapplication must be requested in the cases and according to the procedures provided for by the legal order.

O. PRINCIPLE OF DIGITAL PRECAUTION

13. Systemic Technological Risk

Before the implementation of generalized surveillance systems, the following must also be evaluated:

- **cyber vulnerabilities;**
- **attacks by criminal subjects;**
- **abusive access;**
- **false positives;**
- **algorithmic errors;**
- **discrimination;**
- **data loss;**
- **re-identification;**
- **database interconnection;**
- **international transfers;**
- **secondary uses;**
- **abuse of powers;**
- **informational concentration.**

In the presence of systemic risks not adequately mitigated, the precautionary principle must be applied.

P. PRINCIPLE OF SEPARATION OF INFORMATIONAL POWER

14. Prohibition of Absolute Concentration of Data

No single authority or infrastructure should concentrate, without adequate guarantees, all the functions of:

IDENTIFICATION + COLLECTION + STORAGE + ANALYSIS + PROFILING + SURVEILLANCE + DECISION + SANCTION.

Functional separation constitutes a guarantee against the abuse of informational power.

Q. PRINCIPLE OF HUMAN CONTROL

15. Prohibition of Harmful Automatism

No citizen should automatically suffer substantial consequences on their liberty, reputation, economic availability, or access to fundamental services solely on the basis of an unverifiable algorithmic decision.

The following must be ensured:

- **human control;**
 - **reasoning;**
 - **possibility of contestation;**
 - **access to relevant information;**
 - **rectification;**
 - **review;**
 - **appeal;**
 - **judicial protection.**
-

R. PRINCIPLE OF INDIVIDUAL SELF-DETERMINATION

16. Self-Governance of the Person

The citizen who recognizes themselves as part of the Self-Determined Italian People affirms their right to **individual self-governance** as a political and legal principle to be submitted, in the forms provided for by the legal order, to the protection of the competent authorities.

Individual self-governance is understood as:

- **autonomy of the person;**
- **freedom of conscience;**
- **freedom of communication;**
- **informational self-determination;**
- **patrimonial autonomy;**
- **freedom of association;**
- **right to privacy;**
- **right to judicial protection;**
- **right to democratic participation.**

This affirmation is not intended as unilateral authorization to violate current laws, but rather as an **express reservation of all fundamental rights** that the subject declares they intend to exercise and defend through the available constitutional, legislative, administrative, and judicial instruments.

S. CLAUSE OF DEMOCRATIC SELF-DETERMINATION

17. Reservation of Popular Sovereignty

The principle is affirmed according to which structural transformations of the legal order having a direct and generalized impact on fundamental rights must be accompanied by the **maximum possible level** of:

- **public information;**
- **transparency;**
- **participation;**
- **parliamentary control;**
- **judicial control;**
- **civic participation;**
- **referendum instruments where provided for by the legal order.**

The principle of popular sovereignty must be interpreted as a **permanent obligation of institutions to account for the exercise of power.**

T. REINFORCED DEMOCRATIC SCRUTINY

18. Request for Referendum in Cases Provided for by the Constitution and Law

Where a digital surveillance measure entails a structural and permanent transformation of the exercise of fundamental freedoms, the competent authorities are requested to evaluate the use of **instruments of direct democracy available in the legal order.**

In particular, evaluation is requested of:

- **consultative referendum;**
- **abrogative referendum;**
- **confirmatory referendum;**
- **public consultations;**
- **parliamentary hearings;**
- **popular legislative initiatives;**
- **civic participation procedures.**

This Petition requests that direct democracy not be considered a merely ornamental element when structural transformations of the sphere of fundamental rights are at stake, within the limits and according to the procedures provided for by the Constitution and applicable law.

U. PRINCIPLE OF NON-EVASION OF DEMOCRACY

19. Prohibition of Indirectly Achieving What Could Not Be Achieved Directly

No structural transformation of fundamental rights should be realized through a succession of apparently separate technical provisions which, considered in their entirety, produce a system of generalized surveillance.

The following principle is therefore introduced:

PRINCIPLE OF NON-EVASION OF DEMOCRACY AND TECHNOLOGY

Any assessment of legitimacy must also consider the cumulative effect of the measures.

V. CLAUSE OF NON-GENERALIZED SURVEILLANCE

20. Individual Reservation

The undersigned, as a citizen and member of the Self-Determined Italian People, expressly reserves the right to contest every processing of their personal data that exceeds the limits established by law, as well as any form of surveillance that is **illegitimate, arbitrary, disproportionate, or lacking adequate legal basis**.

This reservation includes:

- **communications;**
 - **metadata;**
 - **financial data;**
 - **biometric data;**
 - **location data;**
 - **behavioral data;**
 - **health data, where applicable;**
 - **data relating to social relationships;**
 - **data deriving from automated systems.**
-

W. RIGHT TO TRANSPARENCY

21. Right to Know the Existence of Processing

It is requested that every citizen be able to know, within the limits established by law:

- **which data are collected;**
- **who collects them;**
- **for what purpose;**
- **on what legal basis;**
- **for how long they are stored;**
- **with whom they are shared;**

- **which algorithms are used;**
 - **which authorities can access them;**
 - **which contestation procedures are available;**
 - **which remedies exist against abuse.**
-

X. RIGHT TO CONTESTATION AND JUDICIAL PROTECTION

22. Effectiveness of the Remedy

Every citizen must be able to obtain protection against:

- **illegitimate collection;**
- **illegitimate processing;**
- **illegitimate storage;**
- **illegitimate profiling;**
- **illegitimate surveillance;**
- **illegitimate transfer;**
- **illegitimate secondary use;**
- **illegitimate automated decision;**
- **illegitimate disclosure.**

The remedy must be **effective, accessible, and timely.**

Y. CLAUSE OF DAMAGE PREVENTION

23. Preventive Protection

Where there exists a concrete risk of serious and hardly reversible violation of fundamental rights, it is requested that measures suitable to prevent the damage from occurring before it becomes irreversible be adopted, according to available precautionary instruments.

Protection must not be exclusively subsequent.

WHERE DAMAGE TO PRIVACY IS IRREVERSIBLE, PROTECTION MUST BE ABLE TO BE PREVENTIVE.

Z. CLAUSE OF INDEMNITY AND INDIVIDUAL COMPENSATION

24. Express Reservation of Compensatory Action

The citizen expressly and preventively reserves the right to exercise every judicial action for compensation, restitution, injunction, and accertation permitted by the legal order where an illegitimate measure determines a concrete injury to their rights.

This Petition also formulates a **parametric request for compensation and/or indemnity** equal to **€1,000,000.00 (one million/00)** for each individually ascertained violation, where such amount is considered admissible and justified by the competent judge in light of the **nature, gravity, duration, diffusiveness, irreversibility, and consequences** of the violation.

This amount is indicated as a **compensatory claim and quantification parameter**, and not as an automatic self-executing pecuniary sanction.

AA. CRITERIA FOR QUANTIFICATION OF DAMAGE

25. Patrimonial and Non-Patrimonial Damage

The compensatory request may include, according to the categories recognized by the legal order:

- **patrimonial damage;**
 - **non-patrimonial damage;**
 - **damage to confidentiality;**
 - **damage to informational self-determination;**
 - **damage to personal liberty;**
 - **damage to reputation;**
 - **damage deriving from profiling;**
 - **damage deriving from unlawful data processing;**
 - **damage deriving from automated decisions;**
 - **damage deriving from data disclosure;**
 - **damage deriving from loss of control over personal data;**
 - **further damages concretely demonstrable.**
-

AB. INDIVIDUAL AND INSTITUTIONAL RESPONSIBILITY

26. Accertation of Responsibilities

Where a violation is ascertained, the following must be identified, according to their respective competences and responsibilities:

- **author of the act;**
- **emanating authority;**
- **controller;**
- **possible processor;**
- **subject who materially ordered the operation;**
- **subjects who have causally contributed to the violation.**

The consequence of a violation deriving from an illegitimate exercise of public power cannot be automatically transferred onto the citizen.

AC. RESPONSIBILITY FOR SYSTEMIC VIOLATIONS

27. Cumulative Damage

Where a technology produces systematic violations on a plurality of citizens, the collective dimension of the phenomenon must also be verified.

In particular, the following must be evaluated:

- **number of persons concerned;**
- **duration of the practice;**
- **quantity of data processed;**
- **nature of the data;**
- **degree of intrusiveness;**
- **possibility of re-identification;**
- **possibility of abuse;**
- **irreversibility;**
- **economic and social consequences.**

The diffusiveness of the violation cannot, in itself, constitute a reason to diminish the protection of the individual.

AD. PRINCIPLE OF NON-IMPUTABILITY OF FAULT TO THE CITIZEN

28. The Citizen Cannot Be Transformed into a Permanent Object of Suspicion

Any model in which the citizen, in the absence of individualized and legally relevant elements, is preventively treated as a potential perpetrator of offenses is contested.

Criminal prevention must remain distinct from the **generalized technological presumption of suspicion**.

AE. PRINCIPLE OF PROTECTION OF THE DIGITAL PERSON

29. New Dimension of Self-Determination

Digital identity, personal data, private communications, and economic data constitute essential components of the contemporary dimension of the person.

The protection of the person must therefore extend also to their digital dimension.

The following principle is affirmed:

NO PERSON CAN BE REDUCED TO A DIGITAL PROFILE SUBJECT TO PERMANENT CLASSIFICATION, MONITORING, AND EVALUATION BY PUBLIC POWER OR PRIVATE SUBJECTS INVESTED WITH PUBLIC FUNCTIONS.

AF. PRINCIPLE OF TECHNOLOGICAL NEUTRALITY

30. Technology Cannot Modify Rights

The adoption of a new technology cannot be used to reduce the level of protection already recognized to the person.

Therefore:

NO TECHNOLOGICAL INNOVATION CAN BE USED AS AN INSTRUMENT TO CIRCUMVENT EXISTING LEGAL GUARANTEES.

If a conduct would be illegitimate if carried out manually, its automation does not automatically make it lawful.

AG. PRINCIPLE OF REVERSIBILITY

31. Prohibition of Irreversible Infrastructures

Every surveillance infrastructure must be:

- **delimited;**
- **controllable;**
- **auditable;**
- **temporally defined;**
- **technically reversible;**
- **legally revocable.**

Effective procedures must be provided for the deletion of data collected illegitimately and for the cessation of processing no longer justified.

AH. REQUEST FOR PRECAUTIONARY MORATORIUM

32. Preventive Suspension of Disproportionate Measures

It is requested, in cases where the legal prerequisites exist, to order or promote a **precautionary moratorium** on generalized surveillance measures that have not yet passed an independent verification of compatibility with fundamental rights.

The moratorium must remain until:

- **complete identification of the legal basis;**
 - **impact assessment;**
 - **proportionality verification;**
 - **security assessment;**
 - **necessity verification;**
 - **public consultation;**
 - **definition of remedies;**
 - **control by the competent independent authority.**
-

AI. PETITUM — FORMAL REQUESTS

In light of all the foregoing, **WE FORMALLY REQUEST**, each authority according to its respective competence:

1. **AS CERTAIN** the fundamental nature of the rights to privacy, secrecy of communications, personal data protection, and informational self-determination.
2. **AS CERTAIN** that no technological capacity for surveillance constitutes, in itself, an autonomous source of legal legitimation.
3. **AS CERTAIN** the necessity of a specific legal basis for every invasive processing.
4. **AS CERTAIN** the necessity to concretely verify the necessity, suitability, and proportionality of every measure.
5. **AS CERTAIN** the incompatibility, where it exists, of forms of generalized surveillance with applicable fundamental rights.
6. **INHIBIT, SUSPEND, OR LIMIT**, according to available legal instruments, measures that prove to be illegitimate, disproportionate, or lacking adequate legal basis.
7. **PREVENT**, where legally possible, the implementation of systems capable of realizing generalized surveillance of the population not justified by specific legal requirements.
8. **GUARANTEE** the protection of encryption and prevent systemic vulnerabilities that are unnecessary and disproportionate.
9. **GUARANTEE** the principle of data minimization.
10. **GUARANTEE** the principle of purpose limitation.
11. **GUARANTEE** the right to knowability of processing.
12. **GUARANTEE** the right of access, rectification, erasure, and objection in cases provided for by applicable law.
13. **GUARANTEE** the right to an effective remedy before an independent authority and the competent judge.
14. **GUARANTEE** human control over automated decisions capable of producing legal consequences or substantial effects on the person.
15. **VERIFY** the compatibility of digital surveillance measures with **Articles 7, 8, 11, 16, 20, 21, 47, and 52 of the Charter of Fundamental Rights of the European Union**.
16. **VERIFY** compatibility with **Articles 8, 10, 11, and 13 ECHR**, according to their respective applicability.
17. **VERIFY** compatibility with **Articles 17, 19, and 22 ICCPR**, according to their respective applicability.
18. **VERIFY** compatibility with **Articles 1, 2, 3, 13, 14, 15, 21, and 24 of the Italian Constitution** and with further relevant constitutional principles.
19. **EVALUATE** the possibility and necessity of subjecting structural transformations affecting fundamental rights to the forms of direct democracy provided for by the legal order.
20. **RECOGNIZE** the citizen's right to participate in decision-making procedures having a substantial impact on their digital freedom.
21. **RECOGNIZE** the citizen's right to individually contest every illegitimate processing.
22. **RECOGNIZE** the full reservation of individual judicial action.
23. **RECOGNIZE** the reservation of compensatory claim up to the parametric amount of **€1,000,000.00** for each individually ascertained violation, with final quantification left to the competent judicial authority.

24. **AS CERTAIN**, where requested, the possible civil, administrative, or other nature liability of subjects who have caused a concretely ascertained violation.
25. **ORDER OR PROMOTE**, in cases provided for by law, the cessation of illegitimate processing and the deletion of data illegitimately acquired.
26. **GUARANTEE** that no technological measure can produce a reduction in the level of protection of fundamental rights already recognized.
27. **ORDER**, WHERE THE PREREQUISITES EXIST, the necessary precautionary measures to prevent serious, irreversible, or hardly repairable damage.
28. **DECLARE** that any surveillance measure that does not pass the test of reinforced proportionality (legality, suitability, necessity, and proportionality in the strict sense) is inapplicable within the territory and with respect to the Self-Determined Italian People.
29. **RECOGNIZE** the right of citizens who adhere to the Self-Determined Italian People to refuse, on the basis of the principle of individual self-determination, any form of generalized surveillance not based on a specific, individualized, and legally justified suspicion.
30. **GUARANTEE** that no citizen can be subjected to discriminatory treatment for exercising the rights recognized in this Petition.
-

AJ. SPECIAL CLAUSE OF SELF-DETERMINATION

33. Individual Irrevocable Reservation of Protection

The undersigned citizen declares that they do not renounce, either expressly or implicitly, the fundamental rights recognized by the Italian Constitution, European Union law, and applicable international instruments.

They further declare that they reserve:

- **the right of petition;**
 - **the right of appeal;**
 - **the right of objection in cases provided for;**
 - **the right of access;**
 - **the right to precautionary protection;**
 - **the right to compensatory protection;**
 - **the right to data protection;**
 - **the right to secrecy of communications;**
 - **the right to freedom of expression;**
 - **the right to informational self-determination;**
 - **every further right recognized by the legal order.**
-

AK. CLAUSE OF SAFEGUARD OF RIGHTS

34. Interpretation More Favorable to the Person

Where a provision can be interpreted in different ways, the interpretation most consistent with the effective protection of fundamental rights must be privileged, within the limits permitted by the legal order.

No provision shall be interpreted as a general authorization for indiscriminate surveillance.

AL. CLAUSE OF NON-RENUNCIATION

35. No Acquiescence

The failure to immediately contest a specific measure shall not be interpreted, except as provided by law, as a renunciation of fundamental rights nor as general consent to future forms of surveillance.

Consent to data processing, where legally relevant, must remain distinct from the mere practical impossibility of avoiding a digital infrastructure.

AM. CLAUSE OF DEMOCRATIC REVIEW

36. Periodic Re-examination

Any permanent surveillance infrastructure must be subjected to periodic re-examination regarding:

- **effectiveness;**
- **necessity;**
- **proportionality;**
- **security;**
- **impact on rights;**
- **number of persons affected;**
- **false positives;**
- **incidents;**
- **abuses;**
- **unauthorized access;**
- **secondary uses;**
- **social costs;**
- **results actually achieved.**

The mere existence of a technology does not constitute proof of its permanent necessity.

AN. FUNDAMENTAL PRINCIPLE OF NON-TRANSFORMATION OF THE CITIZEN INTO AN OBJECT OF SURVEILLANCE

Formal recognition of the following principle is requested:

THE CITIZEN IS NOT A DATA POINT TO BE SURVEILLED, BUT A PERSON WHO HOLDS RIGHTS.

And consequently:

THE SECURITY OF THE COMMUNITY CANNOT BE PURSUED THROUGH THE NORMALIZATION OF PERMANENT SURVEILLANCE OF ALL CITIZENS.

AO. PRINCIPLE OF BALANCE BETWEEN SECURITY AND FREEDOM

This Petition does not generally contest the function of the State and institutions in combating:

- **crime;**
- **terrorism;**
- **money laundering;**
- **child abuse;**
- **organized crime;**
- **fraud;**
- **cyberattacks;**
- **threats to public security.**

It contests and subjects to verification exclusively the use of instruments that, for **breadth, duration, automatism, indiscriminateness, or invasiveness**, may exceed what is necessary and proportionate to pursue such purposes.

True democratic security must in fact be built through the balance between:

SECURITY + FREEDOM + PRIVACY + PROPORTIONALITY + JUDICIAL CONTROL + PUBLIC ACCOUNTABILITY.

AP. SOLEMN FORMULA OF RESERVATION

The undersigned, as a citizen and member of the Self-Determined Italian People, **EXPRESSLY RESERVES EVERY RIGHT, ACTION, EXCEPTION, OPPOSITION, APPEAL, PRECAUTIONARY REQUEST, INJUNCTIVE REQUEST, AND COMPENSATORY CLAIM** recognized by the applicable national, European, and international legal order.

This Petition must be understood as:

PETITION ACT + NOTICE OF NON-COMPLIANCE AGAINST RIGHTS VIOLATION + RESERVATION OF JUDICIAL PROTECTION + REQUEST FOR DAMAGE PREVENTION + INDIVIDUAL COMPENSATORY RESERVATION.

AQ. REQUEST FOR REGISTRATION AND RESPONSE

Formal request is made for:

- **registration** of this Petition;
 - **identification** of the competent office;
 - **communication** of the person responsible for the procedure, where provided;
 - **communication** of the authorities to which the Petition may be transmitted;
 - a **written and reasoned response**;
 - **indication** of the applicable legal bases;
 - **indication** of the available remedies;
 - **preservation** in the records of this reservation of rights.
-

AR. CONCLUSION

This Petition affirms an essential principle of the democratic legal order:

TECHNOLOGICAL POWER CANNOT BECOME, BY THE MERE EXISTENCE OF TECHNOLOGY, LEGAL POWER.

And further:

THE FIGHT AGAINST CRIME CANNOT TRANSFORM INTO GENERALIZED SURVEILLANCE.

SECURITY CANNOT BECOME A GENERAL AUTHORIZATION FOR ACCESS TO PRIVATE LIFE.

DIGITAL INNOVATION CANNOT ENTAIL AN AUTOMATIC REDUCTION OF FREEDOM.

THE PERSON PRECEDES THE ALGORITHM, THE LAW PRECEDES TECHNOLOGY, AND DEMOCRACY PRECEDES THE EXERCISE OF POWER.

Therefore, every digital surveillance measure must be subjected to verification according to the following substantive hierarchy:

PERSON → FUNDAMENTAL RIGHTS → LEGALITY → NECESSITY → PROPORTIONALITY → TRANSPARENCY → INDEPENDENT CONTROL → JUDICIAL PROTECTION → DEMOCRACY.

And no technological infrastructure can be considered legitimate exclusively because technically possible.

FINAL SAFEGUARD CLAUSE

This Petition does not constitute a renunciation of any right, nor acquiescence with respect to any future, present, or past processing that proves to be illegitimate.

Every right, action, exception, appeal, precautionary request, injunctive request, erasure request, restitution request, and compensatory claim is expressly reserved, within the limits and according to the procedures provided for by the competent legal order.

IT IS REQUESTED THAT THIS PETITION BE RECEIVED, REGISTERED, EXAMINED, AND TRANSMITTED TO THE COMPETENT BODIES FOR EVERY DETERMINATION WITHIN THEIR RESPECTIVE COMPETENCES.

PLACE AND DATE: _____

THE APPLICANT: _____

QUALIFICATION: CITIZEN / MEMBER OF THE SELF-DETERMINED ITALIAN PEOPLE

SIGNATURE: _____

ADDRESS FOR COMMUNICATIONS: _____

PEC / E-MAIL: _____

FINAL RESERVATION FORMULA

OMNIA IURA RESERVATA.

ALL FUNDAMENTAL, CONSTITUTIONAL, EUROPEAN, AND INTERNATIONAL RIGHTS ARE EXPRESSLY RESERVED.

NO SILENCE, NO TOLERANCE, AND NO PARTICIPATION IN A TECHNOLOGICAL SYSTEM SHALL BE INTERPRETED, UNLESS EXPRESSLY PROVIDED BY LAW, AS A RENUNCIATION OF THE INVIOABLE RIGHTS OF THE PERSON.

ANNEX — INTEGRATION WITH THE INTERNATIONAL LAW STRATEGY EX ART. 38 ICJ STATUTE

This Petition is further reinforced by the principles of international law pursuant to **Article 38 of the Statute of the International Court of Justice**:

Source ex Art. 38	Application to Surveillance and Digital Control	References
Art. 38(1)(a) — Treaties	Human rights treaties prohibit arbitrary surveillance and protect privacy	ICCPR art. 17; ECHR art. 8; EU Charter arts. 7, 8
Art. 38(1)(b)	The right to privacy and freedom from	Nicaragua (1986);

— Custom	arbitrary surveillance are customary norms	Universal Declaration of Human Rights
Art. 38(1)(c) — General principles	Principles of <i>nulla potestas sine populo</i> , proportionality, and human dignity require democratic control	Principles common to civilized nations
Art. 38(1)(d) — Decisions and doctrine	International jurisprudence prohibits mass surveillance and data retention without safeguards	Digital Rights Ireland (2014); S. and Marper (2008)
Art. 38(2) — <i>Ex aequo et bono</i>	Equity requires that fundamental freedoms be protected from disproportionate technological intrusion	Equitable application in the absence of specific discipline

The CLNI, as the provisional national authority of the Self-Determined Italian People, acts as spokesperson for this Petition, trusting that the competent authorities and the international community will recognize the legitimacy and urgency of the issues raised and adopt every necessary determination to ensure that the fundamental choice regarding surveillance and digital control is entrusted, as is due, to the sovereign people.

ACCERTAMENTO CHAT CONTROL

14/09/2026 21:20:36

0.01 ZECCHINO

FROM:

3P8VN8uzJsZJk23urkxdLFoHCbEjSsDdL3T

TO:

3P8VN8uzJsZJk23urkxdLFoHCbEjSsDdL3T

Message:

ACCERTAMENTO CHAT CONTROL, SHA256:

08c5dd2d397eddc8d5f9f78f21c31b0c5ab824c3fb02ee55e596520c879d047e

TX: [Guardala con l'explorer](#)

Fee:0.05 ZECCHINO