Cognitive Liberty Institute

Protecting Cognitive Sovereignty in a Digital World

DOMESTIC LEGISLATION MODEL

COGNITIVE SOVEREIGNTY PROTECTION ACT

Note to legislative drafters: This model legislation provides a template for implementing the International Accord on Cognitive Sovereignty within domestic legal frameworks. It should be adapted to align with national legal traditions, constitutional requirements, and existing regulatory structures. Text in [brackets] indicates areas requiring jurisdiction-specific customization.

COGNITIVE SOVEREIGNTY PROTECTION ACT

PART I: PRELIMINARY PROVISIONS

Section 1: Short Title

This Act may be cited as the Cognitive Sovereignty Protection Act.

Section 2: Commencement

This Act shall come into force on [date/period after enactment].

Section 3: Purpose

The purpose of this Act is to protect and promote the cognitive sovereignty of individuals by: (a) Establishing cognitive sovereignty as a legally protected right; (b) Ensuring transparency regarding technological systems that influence cognitive processes; (c) Requiring designs that respect cognitive autonomy; (d) Establishing special protections for neural interface technologies; (e) Creating institutional mechanisms for oversight and enforcement; and (f) Promoting education and research regarding cognitive sovereignty.

Section 4: Interpretation

(1) In this Act, unless the context otherwise requires:

"Algorithmic system" means a computational process, including one derived from machine learning, statistics, or other data processing techniques, that makes a decision or facilitates human decision-making or shapes content exposure.

"Cognitive process" means any mental process including attention allocation, information processing, belief formation, emotional response, and decision-making.

"Cognitive sovereignty" means an individual's right to maintain autonomy over their own cognitive processes, free from concealed or coercive technological influence.

"Dark pattern" means a user interface designed to manipulate users into making decisions that they would not otherwise make, through exploitation of cognitive biases or deceptive practices.

"Digital service" means any service provided at a distance, by electronic means, at the individual request of a recipient of services, whether provided for remuneration or not.

"Influence technique" means any method designed to affect user behavior through psychological or neurological mechanisms.

"Neural interface" means any technology that directly interacts with neural activity, including brain-computer interfaces, neural stimulation devices, and technologies that monitor or interpret neural signals.

"Oversight Authority" means the [Cognitive Sovereignty Oversight Authority/existing regulatory body] established/designated under Section 24 of this Act.

"Provider" means any natural or legal person who provides a digital service or neural interface technology.

(2) This Act shall be interpreted in a manner consistent with the International Accord on Cognitive Sovereignty.

Section 5: Application

(1) This Act applies to: (a) All providers offering digital services or neural interface technologies to individuals within [jurisdiction], regardless of the provider's place of establishment; (b) All digital services and neural interface technologies used by individuals within [jurisdiction], regardless of the location of the service's processing operations.

(2) This Act does not apply to: (a) Activities necessary for national security as defined by [relevant national security legislation], subject to proportionality requirements and oversight mechanisms established in that legislation; (b) Strictly private or household activities with no commercial component; (c) [Other jurisdiction-specific exemptions, if necessary].

PART II: FUNDAMENTAL RIGHTS AND PROTECTIONS

Section 6: Right to Cognitive Sovereignty

(1) Every individual has the right to maintain autonomy over their own cognitive processes.

(2) This right includes, but is not limited to: (a) The right to make decisions free from concealed or manipulative technological influence; (b) The right to control the allocation of one's attention in digital environments; (c) The right to understand how algorithmic systems may influence one's perception, beliefs, or decisions; (d) The right to access digital services without submitting to unnecessary psychological or neurological influence.

(3) No person may waive or be required to waive the protections provided by this Act.

Section 7: Special Protections for Vulnerable Individuals

(1) Enhanced protections apply to services directed at or likely to be accessed by: (a) Children under the age of [16/18]; (b) Older adults with cognitive vulnerabilities; (c) Individuals with conditions affecting decision-making capacity.

(2) Digital services and neural interface technologies directed at or likely to be accessed by these populations must: (a) Implement the highest level of transparency regarding influence techniques; (b) Prohibit dark patterns entirely; (c) Minimize attention-capturing mechanisms; (d) Provide enhanced explanations suitable to the capacity of the intended users; (e) Undergo special assessment and certification by the Oversight Authority before deployment.

PART III: TRANSPARENCY OBLIGATIONS

Section 8: General Transparency Requirements

(1) Providers of digital services using algorithmic systems that influence user behavior must disclose, in clear and accessible language: (a) The existence and nature of algorithmic mediation in the service; (b) The primary objectives and optimization targets of such systems; (c) The categories of data used to personalize content or influence user behavior; (d) The general methodology used to select, prioritize, or deprioritize content.

(2) The information required under subsection (1) must be: (a) Provided before users engage with the service; (b) Permanently accessible through an easily located link or menu option; (c) Written in plain language appropriate to the intended user population; (d) Updated whenever significant changes are made to the algorithmic system.

Section 9: Influence Technique Disclosure

(1) Providers using psychological or neurological influence techniques must explicitly disclose: (a) The specific techniques employed; (b) The intended effects of these techniques; (c) How users can minimize or disable these effects if they wish.

(2) Prohibited techniques include: (a) Subliminal techniques that operate below the threshold of conscious awareness; (b) Exploitation of known psychological vulnerabilities to promote addictive behavior; (c) Deceptive presentation of artificial engagement metrics designed to manipulate social proof; (d) [Other jurisdiction-specific prohibitions].

Section 10: Documentation Requirements

(1) Providers must maintain comprehensive internal documentation including: (a) Design documentation showing consideration of cognitive impacts; (b) Risk assessments regarding potential for manipulation or deception; (c) Testing records regarding user autonomy and understanding; (d) Mitigation strategies for identified risks to cognitive sovereignty.

(2) This documentation must be: (a) Updated regularly throughout the development and operation of the service; (b) Made available to the Oversight Authority upon request; (c) Preserved for a minimum of [3/5] years after a service or feature is discontinued.

PART IV: DESIGN REQUIREMENTS

Section 11: Cognitive Respect by Design

(1) Digital services likely to influence cognitive processes must be designed with respect for user autonomy as a core principle.

(2) This principle requires: (a) Consideration of cognitive impacts throughout the design process; (b) Favoring user-directed rather than system-directed engagement; (c) Designing systems that augment rather than replace human judgment; (d) Avoiding features that exploit cognitive vulnerabilities.

(3) The Oversight Authority shall issue guidelines detailing best practices for cognitive respect by design within [6 months] of the commencement of this Act.

Section 12: Opt-Out Requirements

(1) Digital services using algorithmic personalization or behavioral prediction must provide users with straightforward options to: (a) Disable personalization features; (b) Access content in chronological rather than algorithmically-curated order where applicable; (c) Use core service functions without behavioral prediction systems.

(2) These options must be: (a) Clearly explained in user-friendly language; (b) Accessible through the main user interface rather than hidden in secondary menus; (c) Functional without significant degradation of service quality.

Section 13: Attention Protection

(1) Digital services must incorporate features that respect users' time and attention, including: (a) Clear indications of time spent using the service; (b) Optional reminders after extended usage periods; (c) Tools to set usage limits or scheduled breaks; (d) Mechanisms to reduce interruptions and notifications.

(2) Services may not: (a) Use unlimited scroll or autoplay features without simple and persistent opt-out options; (b) Employ variable reward mechanisms designed to maximize engagement through uncertainty; (c) Use artificial scarcity or urgency claims unless factually justified.

Section 14: Prohibition of Dark Patterns

(1) No digital service may employ user interface designs that manipulate, deceive, or coerce users into actions contrary to their interests or intentions.

(2) Prohibited dark patterns include but are not limited to: (a) Forced continuity without clear and simple cancellation options; (b) Hidden costs revealed only after significant user investment in a process; (c) Misdirection through visual hierarchy that obscures important information; (d) Confirmshaming that penalizes users for declining optional features; (e) Interfaces that make refusal significantly more difficult than acceptance.

(3) The Oversight Authority shall maintain and regularly update a catalog of prohibited dark patterns with specific examples.

PART V: NEURAL INTERFACE GOVERNANCE

Section 15: Neural Interface Registration

(1) All neural interface technologies must be registered with the Oversight Authority before being offered to users within [jurisdiction].

(2) Registration requires submission of: (a) Comprehensive technical documentation; (b) Risk assessment regarding cognitive autonomy impacts; (c) Clinical testing results where applicable; (d) Clear delineation of information flows between human and machine; (e) Data security and user control mechanisms.

Section 16: Cognitive Boundary Requirements

(1) Neural interface technologies must maintain clear boundaries between: (a) Human and machine cognition; (b) Individual and collective thought; (c) Private and shared cognitive experiences.

(2) These boundaries must be preserved through: (a) Clear user awareness of technological mediation; (b) Explicit consent for each category of neural interaction; (c) Unmistakable delineation of external versus internal cognitive content; (d) User-controlled termination of neural interactions.

Section 17: Neural Data Protection

(1) Information derived directly from neural activity is classified as specially protected data with the following requirements: (a) Absolute ownership retained by the individual; (b) Explicit, specific, and granular consent required for any collection or use; (c) Prohibition on inferential uses beyond the specific purposes consented to; (d) Mandatory encryption during storage and transmission; (e) Right to complete erasure upon request.

(2) Neural data may not be: (a) Used for commercial purposes beyond the direct functionality of the interface; (b) Combined with other data sources to create enhanced profiles; (c) Retained longer than necessary for the consented purpose; (d) Transferred to third parties without explicit, separate consent for each transfer.

Section 18: Cognitive Integrity Requirements

(1) Neural interfaces must: (a) Preserve the authenticity of thought processes; (b) Prevent unauthorized modification of cognitive content; (c) Maintain continuous user awareness of technological mediation; (d) Support rather than supplant natural cognitive functions.

(2) Providers of neural interfaces must: (a) Conduct regular cognitive impact assessments; (b) Implement monitoring for unintended cognitive effects; (c) Provide mechanisms for immediate disengagement; (d) Ensure transparency regarding all cognitive modifications.

PART VI: ASSESSMENT AND CERTIFICATION

Section 19: Cognitive Impact Assessment

(1) Providers of high-risk digital services and all neural interfaces must conduct a Cognitive Impact Assessment before deployment.

(2) High-risk digital services include: (a) Social media platforms with more than [threshold number] users in [jurisdiction]; (b) Digital services specifically targeted at children; (c) Services using advanced personalization or prediction systems; (d) Services designed to influence significant life decisions; (e) Other categories as determined by the Oversight Authority.

(3) The Cognitive Impact Assessment must evaluate: (a) Potential effects on user autonomy and decision-making; (b) Risks of manipulation or deception; (c) Impacts on attention and cognitive load; (d) Potential for addiction or compulsive usage; (e) Specific impacts on vulnerable populations; (f) Mitigation measures for identified risks.

(4) Completed assessments must be submitted to the Oversight Authority for review.

Section 20: Certification Requirements

(1) Based on the Cognitive Impact Assessment, the Oversight Authority shall determine whether: (a) The service or technology may proceed without modifications; (b) Specific modifications are required before deployment; (c) Ongoing monitoring requirements apply; (d) The service or technology is prohibited due to unacceptable risks.

(2) The Oversight Authority shall issue a certification decision within [60 days] of receiving a complete assessment.

(3) Certifications must be renewed every [two years] or whenever significant changes are made to the service or technology.

PART VII: ENFORCEMENT

Section 21: Complaints and Investigations

(1) Any person may file a complaint with the Oversight Authority alleging a violation of this Act.

(2) The Oversight Authority may also initiate investigations on its own authority.

(3) Upon receiving a complaint or initiating an investigation, the Oversight Authority may: (a) Request information from the provider; (b) Conduct inspections of documentation and systems; (c) Interview relevant personnel; (d) Order technical testing of services or technologies; (e) Solicit expert opinions on technical or psychological aspects.

(4) Providers must cooperate fully with investigations, including providing access to non-public documentation and technical systems as necessary.

Section 22: Enforcement Actions

(1) If the Oversight Authority determines that a violation has occurred, it may issue: (a) Warnings for minor first violations; (b) Compliance orders specifying required remedial actions; (c) Administrative fines; (d) Orders to cease specific features or practices; (e) Prohibition of service provision in cases of serious violations.

(2) Administrative fines shall be calculated based on: (a) The nature, gravity, and duration of the infringement; (b) The intentional or negligent character of the infringement; (c)

Previous infringements by the provider; (d) The size and market position of the provider; (e) The number of affected users; (f) The level of cooperation with the investigation.

(3) Maximum fines shall be: (a) For minor violations: up to [amount or percentage of annual revenue]; (b) For serious violations: up to [amount or percentage of annual revenue]; (c) For repeated violations: up to [amount or percentage of annual revenue].

Section 23: Private Right of Action

(1) Any person who suffers harm as a result of a violation of this Act may bring an action in [appropriate court] for: (a) Actual damages; (b) Injunctive relief; (c) [Statutory damages of specified amount per violation]; (d) Reasonable attorney's fees and costs for successful claims.

(2) Class actions may be brought on behalf of affected users.

(3) The limitation period for such actions shall be [period] from the date the violation was discovered or reasonably should have been discovered.

PART VIII: INSTITUTIONAL FRAMEWORK

Section 24: Oversight Authority

(1) The [Cognitive Sovereignty Oversight Authority is hereby established / existing regulatory body is hereby designated] as the primary regulatory authority responsible for implementing this Act.

(2) The Authority shall be: (a) Structurally independent from both government and commercial interests; (b) Funded through [funding mechanism]; (c) Led by [leadership structure] appointed for terms of [duration] by [appointment process]; (d) Staffed with technical, legal, and psychological expertise.

(3) The Authority shall have the following responsibilities: (a) Developing detailed regulations and guidelines; (b) Reviewing Cognitive Impact Assessments; (c) Issuing certifications; (d) Investigating potential violations; (e) Enforcing compliance through appropriate measures; (f) Promoting public awareness and education; (g) Conducting and supporting research; (h) Engaging in international cooperation; (i) Reporting annually to [legislature/executive] on implementation.

Section 25: Technical Standards Body

(1) A Technical Standards Committee is hereby established within the Oversight Authority.

(2) The Committee shall: (a) Develop technical standards for measuring algorithmic influence; (b) Establish methodologies for assessing cognitive impact; (c) Create

frameworks for evaluating transparency compliance; (d) Develop testing protocols for manipulative design patterns; (e) Regularly update standards to address technological evolution.

(3) The Committee shall include representatives from: (a) Technical experts in relevant fields; (b) Cognitive science and psychology professionals; (c) Consumer advocacy organizations; (d) Industry representatives (in non-voting capacity); (e) Academic researchers.

PART IX: EDUCATION AND RESEARCH

Section 26: Educational Initiatives

(1) The [appropriate educational authority] shall, in consultation with the Oversight Authority: (a) Develop age-appropriate curriculum materials on cognitive sovereignty; (b) Integrate digital literacy focusing on algorithmic influence into educational standards; (c) Create teacher training programs on these topics; (d) Develop resources for parents and caregivers.

(2) The Oversight Authority shall: (a) Conduct public awareness campaigns; (b) Develop informational resources for the general public; (c) Create specialized resources for vulnerable populations; (d) Engage in media education efforts.

Section 27: Research Promotion

(1) A Cognitive Sovereignty Research Fund is hereby established, administered by [appropriate body].

(2) The Fund shall support independent research into: (a) Effects of algorithmic systems on cognition; (b) Methods to detect and measure cognitive manipulation; (c) Tools to enhance cognitive resilience; (d) Techniques for enhancing algorithmic transparency; (e) Long-term impacts of digital technologies on autonomy and decision-making.

(3) Research findings shall be made publicly available and used to inform ongoing regulatory development.

PART X: INTERNATIONAL COOPERATION

Section 28: Cross-Border Coordination

(1) The Oversight Authority shall cooperate with similar authorities in other jurisdictions to: (a) Share information on violations and enforcement actions; (b) Coordinate investigations of cross-border services; (c) Develop compatible regulatory approaches; (d) Exchange best practices and research findings.

(2) The [appropriate minister/official] may enter into agreements with other jurisdictions to facilitate such cooperation.

PART XI: MISCELLANEOUS PROVISIONS

Section 29: Relationship with Other Laws

(1) This Act supplements and does not replace protections provided by: (a) Data protection and privacy laws; (b) Consumer protection legislation; (c) Competition law; (d) Telecommunications regulations; (e) [Other relevant legislation].

(2) In case of conflict between this Act and other legislation, the provision offering the greater protection for cognitive sovereignty shall prevail.

Section 30: Review and Adaptation

(1) This Act shall be reviewed every [three years] to assess: (a) Effectiveness in protecting cognitive sovereignty; (b) Adaption requirements due to technological developments; (c) Implementation challenges and successes; (d) International regulatory developments.

(2) The Oversight Authority shall submit a comprehensive report with recommendations for amendments to [legislature] following each review.

Section 31: Transitional Provisions

(1) Existing services and technologies must comply with this Act within: (a) [6 months] for transparency requirements; (b) [12 months] for design requirements; (c) [18 months] for assessment and certification requirements; (d) [24 months] for neural interface governance requirements.

(2) The Oversight Authority may grant extensions of up to [6 months] based on demonstrated need and good-faith compliance efforts.

Note to legislative drafters: The above model legislation provides a comprehensive framework that should be adapted to your specific legal system, constitutional requirements, and regulatory traditions. Particular attention should be paid to integration with existing regulatory bodies and legal frameworks. The bracketed text indicates areas requiring jurisdiction-specific determinations.

This model legislation implements the core requirements of the International Accord on Cognitive Sovereignty while providing the detail necessary for practical domestic application. It is designed to be adaptable to different legal systems while maintaining the essential protections required by the Accord.