البروتوكول العصبي: الإطار القانوني الدولي لحقوق الواجهات العصبية، الحرية المعرفية، وسيادة بيانات الدماغ

المؤلف: د. محمد كمال عرفه الرخاوي
باحث ومستشار وخبير ومحامٍ ومؤلف ومحاضر قانوني دولي
معرف الكائن الرقمي10.5281/zenodo.20694918 :

الديباجة

الدول الأطراف في هذا البروتوكول،
إذ تدرك أن التقدم في التقنيات العصبية، وواجهات الدماغ والحاسوب، وخوارزميات فك الترميز العصبي، وأنظمة التعزيز المعرفي، قد أحدث قدرة غير مسبوقة على الوصول إلى النشاط العصبي البشري، وتفسيره، وتعديله، والتفاعل معه،
وإذ تؤكد أن سلامة الفكر البشري، وخصوصية العمليات العقلية، وسيادة الوكالة المعرفية، تشكل أبعاداً أساسية للكرامة الإنسانية المحمية بموجب القانون الدولي لحقوق الإنسان،
وإذ يقلقها أن الواجهات العصبية غير المنظمة قد تتيح الوصول غير التوافقي إلى البيانات العقلية، أو التعديل التلاعبي لعمليات صنع القرار، أو الاستخراج القسري للمحتوى المعرفي، أو التنميط التمييزي القائم على البصمات العصبية،
وإذ تستحضر الأعمال التأسيسية التي أرست المسؤولية الجنائية للكيانات غير البيولوجية، وحوكمة الاتصالات الآلية المستقلة، والإدارة الائتمانية للوعي الرقمي بعد الوفاة، وإطار المساءلة للأنظمة الخوارزمية التنبؤية، وتدرك أن التفاعل العصبي يستلزم حماية مناظرة للحرية المعرفية، والخصوصية العقلية، والسلامة النفسية،
وعزمًا منها على وضع إطار معياري شامل يحكم تطوير، ونشر، ومعايير الموافقة، وحوكمة البيانات، وآليات المساءلة الخاصة بتقنيات الواجهات العصبية،
قد اتفقت على ما يلي:

الملخص التنفيذي التقني والقانوني

يؤسس هذا البروتوكول إطاراً قانونياً دولياً متكاملاً يدمج المعايير الحقوقية مع البنى التقنية القابلة للتحقق، لضمان سيادة البيانات العصبية، والحرية المعرفية، والسلامة النفسية في عصر التفاعل المباشر بين الدماغ والحاسوب. يقدم البروتوكول مبدأ السيادة المعرفية الذي يفرض موافقة صريحة، مستنيرة، قابلة للإلغاء، ومشفرة رمزياً لأي وصول أو تعديل أو تفاعل عصبي. يصنف البيانات العصبية كفئة خاصة خاضعة لحماية مشددة، ويضع بروتوكولات رقابة معتمدة للتطبيقات عالية الخطورة، ويحدد الممارسات المحظورة تقنياً وقانونياً، بما في ذلك الاستخراج العصبي غير التوافقي، والتعديل المعرفي التلاعبي. يدمج الإطار آليات إثبات وإنفاذ مبنية على معادلات قياس الضرر المعرفي، وخوارزميات التحقق من الانحراف الخوارزمي، وهياكل تشفير متقدمة تحمي خصوصية الإشارة العصبية مع تمكين الرقابة المستقلة. يوازن البروتوكول بين حوافز الابتكار العلمي والضمانات الحقوقية الأساسية، ويحمي الفئات السكانية الضعيفة، ويؤسس آليات إنفاذ متدرجة، مقدمًا بنية تنظيمية استباقية تحفظ الكرامة الإنسانية، والاستقلالية العقلية، والسلامة النفسية.

الفصل الأول: الأسس الأنطولوجية والمعايير التقنية للواجهات العصبية

المادة 1: التعريف والتصنيف التقني والقانوني

يُعرّف نظام الواجهة العصبية بموجب هذا البروتوكول بأنه أي منظومة حسابية، أو كيميائية كهربائية، أو ميكانيكية حيوية قادرة على كشف، أو تفسير، أو تعديل، أو نقل إشارات من أو إلى الجهاز العصبي البشري، وتتميز بالخصائص التالية:

أ. الوصول العصبي: قدرة النظام على كشف، أو تسجيل، أو فك تشفير النشاط العصبي المرتبط بالعمليات المعرفية، أو العاطفية، أو الحسية، أو الحركية.

ب. الإمكانية ثنائية الاتجاه: امتلاك النظام قدرة على كل من اكتساب الإشارة العصبية وتعديل النشاط العصبي، سواء كان مُنفذاً حالياً أو مُفعّلاً هندسياً.

ج. الأهمية المعرفية: معالجة النظام لبيانات عصبية ذات صلة محتملة بالحالات العقلية، أو عمليات صنع القرار، أو تكوين الهوية، أو السلامة النفسية.

د. عمق التكامل: تشغيل النظام عبر آليات غازية، أو شبه غازية، أو غير غازية بدرجات متفاوتة من التكامل مع الجهاز العصبي.

مؤشر دقة فك الترميز العصبي) = (NDA) عدد الإشارات المعرفية المُستخلصة بدقة / إجمالي الإشارات المُعالجة) × معامل تصحيح الضوضاء العصبية، ويُشترط ألا يقل عن 0.85 للتصنيف كواجهة معرفية عالية الدقة.

المادة 2: معايير التصنيف القائم على المخاطر والعتبات الرقمية
يُصنّف نظام الواجهة العصبية كنظام عصبي عالي الخطورة ويخضع لالتزامات تنظيمية معززة، وشهادة إلزامية، ورقابة مستقلة، عند استيفاء أي من العتبات التالية:
أ. النشر الغازي: أنظمة تتطلب زراعة جراحية، أو اختراق نسيج عصبي، أو تفاعل كيميائي كهربائي مباشر مع الجهاز العصبي المركزي أو المحيطي.
ب. قدرة فك الترميز المعرفي: أنظمة قادرة على فك تشفير المحتوى الدلالي، أو الحالات العاطفية، أو استرجاع الذاكرة، أو تشكيل النية، أو الأنماط العصبية المرتبطة بالهوية بدقة تتجاوز العتبة القياسية.
ج. السلطة التعديلية: أنظمة تمتلك قدرة على تعديل النشاط العصبي بما قد يؤثر على صنع القرار، أو التنظيم العاطفي، أو تكوين الذاكرة، أو المخرجات السلوكية.
د. المراقبة المستمرة: أنظمة مصممة لاكتساب بيانات عصبية بشكل مستمر وفي الوقت الفعلي دون بدء صريح من المستخدم لكل حدث التقاط.
هـ. تطبيق على الفئات الضعيفة: أنظمة تُنشر على القاصرين، أو الأفراد ذوي الإعاقات المعرفية، أو الأشخاص الخاضعين للوصاية القانونية، أو السكان ذوي القدرة المحدودة على إعطاء موافقة مستنيرة.
معادلة درجة الخطورة العصبية) = (NRS) معامل العمق الغازي × 0.35) + (معامل دقة فك الترميز × 0.30) + (معامل السلطة التعديلية × 0.20) + (معامل استمرارية المراقبة × 0.15)، وتصنف الأنظمة ذات الدرجة ≥ 0.75 كعالية الخطورة تلقائياً.

المادة 3: الحقوق العصبية الأساسية والحريات المعرفية
يُقر هذا البروتوكول أن كل فرد يتمتع بحقوق متأصلة، غير قابلة للتصرف، بشأن جهازه العصبي وعملياته المعرفية، تشمل:
أ. الحرية المعرفية: الحق في تقرير المصير العقلي، وحرية الفكر، والاستقلالية في العمليات المعرفية دون تلاعب خارجي، أو إكراه، أو تدخل غير توافقي.
ب. الخصوصية العقلية: الحق في سرية الحالات العقلية، والبيانات العصبية، والمحتوى المعرفي، المحمية ضد الوصول غير المصرح به، أو الاستخراج، أو المراقبة، أو الإفشاء.

ج. السلامة النفسية: الحق في الحماية ضد التعديل التلاعبي، أو التكييف القسري، أو التغيير الضار في الوظيفة العصبية، أو التنظيم العاطفي، أو تكوين الهوية.
د. سيادة البيانات العصبية: الحق في امتلاك، والتحكم، والتصرف في البيانات العصبية المتولدة من جهازه العصبي، بما في ذلك حقوق الوصول، والنقل، والتصحيح، والحذف.
هـ. استقلالية الموافقة: الحق في تقديم، أو حجب، أو سحب الموافقة على التفاعل العصبي دون إكراه، أو تأثير غير لائق، أو عواقب سلبية على الرفض.

المادة 4: التمييز القانوني بين البيانات العصبية والبيانات الحيوية التقليدية
تُصنف البيانات العصبية قانونياً بشكل منفصل عن المعرفات الحيوية التقليدية، والسجلات الصحية، والبيانات السلوكية. تتميز البيانات العصبية بشكل جوهري باتصالها المباشر بالعمليات العقلية، وإمكانيتها لفك تشفير التجربة الذاتية، وحساسيتها البالغة بشأن الهوية والاستقلالية، وقابليتها للاستغلال التلاعبي. يعكس المعامل القانوني هذا التباعد الأنطولوجي، بفرض معايير موافقة معززة، ومتطلبات حماية بيانات، وآليات مساءلة تتناسب مع الآثار الحقوقية الأساسية للتفاعل العصبي.
مؤشر حساسية البصمة العصبية) = (NSI) قابلية الربط بالهوية × 0.40) + (عمق الكشف المعرفي × 0.35) + (قابلية التعديل السلوكي × 0.25)، وتُطبق حماية مشددة تلقائياً عند تجاوز المؤشر.0.80

المادة 5: معايير الموافقة الطوعية والتحقق الخوارزمي
يتطلب كل نشر لتقنيات الواجهات العصبية موافقة صريحة، مستنيرة، محددة، وقابلة للإلغاء، تستوفي المعايير التالية:
أ. شرط الفهم: تضمن إجراءات الموافقة أن الأفراد يدركون طبيعة الوصول العصبي، والمخاطر المحتملة، وأغراض استخدام البيانات، وفترات الاحتفاظ، وترتيبات مشاركة الأطراف الثالثة، وحقوق الانسحاب.
ب. التحرر من الإكراه: تُحصل الموافقة دون ضغط وظيفي، أو ضائقة اقتصادية، أو إكراه اجتماعي، أو عواقب سلبية على الرفض، مع ضمانات خاصة للفئات الضعيفة.
ج. التفويض المفصل: تحدد الموافقة أغراضاً مميزة للوصول إلى البيانات العصبية، مع تفويض منفصل مطلوب للتطبيقات البحثية، أو التجارية، أو السريرية، أو الأمنية.

د. آلية السحب: يحتفظ الأفراد بالحق في سحب الموافقة في أي وقت، مع التوقف الفوري عن اكتساب البيانات العصبية، والحذف الآمن للبيانات المجمعة سابقاً، ما لم يكن الاحتفاظ مطلوباً بموجب القانون أو أساسياً للسلامة.
هـ. إعادة التأكيد الدورية: بالنسبة للتفاعل العصبي المستمر أو طويل الأمد، تُعاد تأكيد الموافقة على فترات منتظمة، مع إشعار بأي تغييرات جوهرية في استخدام البيانات، أو وظيفة النظام، أو ملفات المخاطر.
تُنفذ الموافقة عبر رمز توافقي مشفر (CRT) يتبع البنية التالية: معرف المستخدم المجهول | طابع زمني موثق | نطاق الغرض المصرح به | عتبة السحب التلقائي | توقيع رقمي غير قابل للتزوير، ويُرفض أي وصول عصبي يتجاوز نطاق الرمز مسجلاً كخرق فوري.

الفصل الثاني: حوكمة البيانات العصبية، التشفير، وسيادة الموافقة

المادة 6: البيانات العصبية كفئة خاصة من البيانات الشخصية
يُقر هذا البروتوكول أن البيانات العصبية constitute فئة خاصة من البيانات الشخصية تخضع لحماية معززة بموجب أطر حماية البيانات الدولية. يُحظر معالجة البيانات العصبية إلا في الظروف التالية:
أ. الموافقة الصريحة: المعالجة القائمة على موافقة صريحة، مستنيرة، ومحددة تستوفي معايير المادة 5.
ب. المصلحة الحيوية: المعالجة الضرورية لحماية المصالح الحيوية لصاحب البيانات أو فرد آخر حيث لا يمكن الحصول على الموافقة، مقتصرة على السياقات الطبية الطارئة.
ج. الصحة العامة: المعالجة الضرورية لأغراض الصحة العامة بموجب ضمانات صارمة، وتقييم تناسبي، ورقابة مستقلة.
د. البحث العلمي: المعالجة لأغراض البحث العلمي بموجب مراجعة أخلاقية، وتقليل للبيانات، وإخفاء للهوية حيثما يكون ممكناً، ومنهجية شفافة.
هـ. الالتزام القانوني: المعالجة المطلوبة بموجب القانون بموجب ضرورة صارمة، وتناسب، وتفويض قضائي.
تُطبق معايير تشفير متقدمة من نوع التشفيد المتجانس أو البراهين صفرية المعرفة لتمكين التحقق من الامتثال دون كشف المحتوى العصبي الخام.

المادة 7: تقليل البيانات، تحديد الغرض، ومعايير الاحتفاظ
تلتزم جميع عمليات معالجة البيانات العصبية بالمبادئ التالية:
أ. شرط التقليل: يقتصر جمع البيانات العصبية على ما هو ضروري تماماً للغرض المحدد والصريح، مع ضمانات هندسية تمنع الالتقاط المفرط أو الاستكشافي.
ب. تحديد الغرض: لا تُعاد صياغة البيانات العصبية، أو دمجها، أو تحليلها لأهداف تتجاوز تلك المصرح بها صراحةً بالموافقة أو الأساس القانوني، مع تدابير تقنية تمنع الانزياح الوظيفي.
ج. حدود الاحتفاظ: تحتفظ بالبيانات العصبية للحد الأدنى من الفترة اللازمة لتحقيق الغرض المصرح به، مع بروتوكولات حذف تلقائي وإجراءات تدمير قابلة للتحقق.
د. معايير إخفاء الهوية: حيثما يكون ممكناً، تُخفى هوية البيانات العصبية أو تُعمى باستخدام طرق مقاومة لهجمات إعادة التعريف، مع تقييم مستمر لمخاطر إزالة التعمية.
هـ. ضوابط الوصول: تحمى البيانات العصبية عبر التشفير، ومصادقة الوصول، وتسجيل التدقيق، وبروتوكولات إشعار الاختراق بما يتناسب مع الحساسية والضرر المحتمل.
يُولد سجل تدقيق غير قابل للتعديل باستخدام سلسلة ميركل الزمنية، حيث يُربط كل حدث وصول أو معالجة بتجزئة مشفرة فريدة مرتبطة بالحالة السابقة، مما يضمن المسار الكامل للبيانات.

المادة 8: الحقوق الفردية بشأن البيانات العصبية
يتمتع الأفراد بالحقوق التالية بشأن بياناتهم العصبية:
أ. حق الوصول: الحق في الحصول على تأكيد معالجة البيانات العصبية، والوصول إلى البيانات المجمعة بتنسيق مفهوم، ومعلومات بشأن الأغراض، والمستلمين، وفترات الاحتفاظ.
ب. حق التصحيح: الحق في طلب تصحيح البيانات العصبية غير الدقيقة أو استكمال البيانات غير المكتملة، مع إجراءات تحقق وتعديل في الوقت المناسب.
ج. حق الحذف: الحق في طلب حذف البيانات العصبية عند سحب الموافقة، أو تحقيق الغرض، أو المعالجة غير القانونية، رهناً بمتطلبات الاحتفاظ المشروعة.
د. حق النقل: الحق في استلام البيانات العصبية بتنسيق منظم وقابل للقراءة آلياً للنقل إلى أنظمة بديلة، حيثما يكون ذلك ممكناً تقنياً ولا يؤثر سلباً على حقوق الآخرين.
هـ. حق الاعتراض: الحق في الاعتراض على معالجة البيانات العصبية القائمة على المصالح المشروعة، مع عبء الإثبات على المتحكم لإظهار أسباب مشروعة مقنعة تتجاوز الحقوق الفردية.

المادة 9: الممارسات المحظورة ومعايير الحماية المعرفية
تُحظر صراحةً الممارسات التالية بشأن تقنيات الواجهات العصبية:
أ. الاستخراج العصبي غير التوافقي: أي وصول إلى، أو تسجيل ل، أو فك تشفير للنشاط العصبي دون موافقة صريحة ومستنيرة، إلا عند الضرورة لمنع ضرر وشيك وخطير على الفرد أو الآخرين، تحت إشراف طبي صارم، ومراجعة قضائية خلال 72 ساعة، وخضوعاً لأقل الوسائل تداخلاً متاحة، أو في سياقات طبية طارئة محددة بدقة تحت رقابة مستقلة.
ب. التعديل المعرفي التلاعبي: أي تعديل للنشاط العصبي مصمم للتأثير على صنع القرار، أو الحالات العاطفية، أو تكوين الذاكرة، أو المخرجات السلوكية دون موافقة صريحة وتبرير علاجي.
ج. التنميط العصبي والتمييز: أي استخدام للبيانات العصبية لتنميط، أو تصنيف، أو تمييز ضد أفراد فيما يتعلق بالتوظيف، أو التأمين، أو الائتمان، أو التعليم، أو الإجراءات القانونية.
د. استخراج الموافقة القسري: أي ربط للتوظيف، أو الخدمات، أو المزايا، أو الحقوق بقبول التفاعل العصبي بما يتجاوز ما هو ضروري تماماً لأغراض السلامة أو الطبية المشروعة.
هـ. المراقبة العصبية السرية: أي نشر لقدرات المراقبة العصبية في الأماكن العامة، أو أماكن العمل، أو الإعدادات المؤسسية دون إشعار شفاف، وغرض مشروع، وتفويض مستقل.
تُحدد عتبة الكشف عن التلاعب المعرفي (MCT) عبر معادلة الانزياح الإحصائي MCT :)| =السلوك المرصود - السلوك الأساسي) / الانحراف المعياري|، ويُصنف أي تجاوز للقيمة 2.5 على مدى 3 دورات زمنية متتالية كإنذار تلاعب فوري يستدعي التدقيق والتعليق.

الفصل الثالث: آليات الرقابة الخوارزمية، الكشف عن الانحراف، والمساءلة التقنية والقانونية

المادة 10: مراجعة الأخلاقيات العصبية المعتمدة والترخيص المسبق للنشر
تخضع جميع الأنظمة العصبية عالية الخطورة لمراجعة وإلزامية وترخيص قبل النشر:
أ. مجلس مراجعة الأخلاقيات: تقوم هيئات مستقلة متعددة التخصصات تضم علماء أعصاب، وأخلاقيين، وعلماء قانون، ومدافعين عن المرضى، وممثلين مجتمعيين بتقييم عمليات النشر المقترحة للامتثال الحقوقي، وتوازن المنافع والمخاطر، وحماية الفئات الضعيفة.

ب. التقييم الفني للسلامة: يقيّم مدققون فنيون معتمدون هندسة النظام من حيث الثغرات الأمنية، وأنماط الفشل، والمتانة أمام الهجمات الخبيثة، والضمانات ضد الوصول غير المصرح به أو التلاعب.
ج. تقييم الأثر: ينفذ الناشرون وينشرون تقييمات أثر الحقوق العصبية التي تتناول الآثار المحتملة على الحرية المعرفية، والخصوصية العقلية، والسلامة النفسية، والإنصاف الاجتماعي، مع استراتيجيات تخفيف للمخاطر المحددة.
د. التشاور العام: بالنسبة للنشرات ذات الأثر العام المحتمل، ينفذ الناشرون تشاوراً ذا مغزى مع المجتمعات المتأثرة، ومنظمات المجتمع المدني، ومدافعي الحقوق، مع توثيق اعتبارات الملاحظات.
هـ. قرار الترخيص: يُمنح ترخيص النشر فقط عند إثبات الامتثال الحقوقي، وتخفيف المخاطر، وآليات الموافقة المستنيرة، وأطر المساءلة، مع شروط، أو قيود، أو متطلبات مراقبة حسب الاقتضاء.
تُدمج خوارزمية التحقق المسبق (PVA) التي تحلل التوافق بين المواصفات الفنية المعتمدة، ونتائج محاكاة المخاطر، وشهادات الامتثال، وتصدر مخرجاً ثنائياً (مصرح/مرفوض) مع سجل تدقيق كامل غير قابل للتعديل.

المادة 11: المراقبة المستمرة، التدقيق، والتحقق من الامتثال
يحافظ ناشرو الأنظمة العصبية عالية الخطورة على الامتثال المستمر من خلال:
أ. المراقبة المستمرة: مراقبة في الوقت الفعلي لأداء النظام، وأنماط الوصول إلى البيانات، وحالة الموافقة، والأحداث الأمنية، مع تنبيهات آلية للانحرافات أو الانتهاكات المحتملة.
ب. التدقيق المستقل: عمليات تدقيق سنوية من قبل مدققين مستقلين معتمدين يقيّمون الأمان التقني، وإدارة الموافقة، وحوكمة البيانات، وحماية الحقوق، مع نشر تقارير موجزة للعامة.
ج. الإبلاغ عن الحوادث: الإبلاغ الفوري عن خروقات البيانات، أو الوصول غير المصرح به، أو انتهاكات الموافقة، أو الأحداث الضارة للسلطات التنظيمية والأفراد المتأثرين، مع خطط علاج وإسناد للمسؤولية.
د. آليات ملاحظات المستخدم: قنوات يسهل الوصول إليها للأفراد للإبلاغ عن المخاوف، أو طلب الوصول إلى البيانات أو حذفها، أو سحب الموافقة، أو التماس سبل الانتصاف، مع التزامات استجابة في الوقت المناسب.
هـ. التفتيش التنظيمي: التعاون مع التفتيش التنظيمي، وتوفير الوثائق المطلوبة، وتنفيذ التدابير التصحيحية لأوجه القصور المحددة.

تُطبق خوارزمية كشف الانزياف التشغيلي (ODD) التي تحسب معدل الخطأ التراكمي مقابل العتبة الآمنة، وتُفعّل بروتوكول الإيقاف الآمن تلقائياً عند تجاوز معامل الموثوقية 0.92، مع إشعار فوري للرقابة المستقلة.

المادة 12: إسناد المسؤولية وآليات التعويض
تترتب المسؤولية المدنية عن الأضرار الناشئة عن تقنيات الواجهات العصبية بموجب المعايير التالية:
أ. النشر المهمل: المسؤولية عن الفشل في تنفيذ الضمانات المطلوبة، أو الحصول على موافقة صالحة، أو إجراء تقييمات الأثر، أو الحفاظ على معايير الأمان بما يتناسب مع مخاطر النظام.
ب. التعامل المتهور مع البيانات: المسؤولية عن مشاركة البيانات غير المصرح بها، أو الاحتفاظ المفرط، أو إخفاء الهوية غير الكافي، أو ضوابط الوصول غير الكافية حيث ينتج ضرر يمكن توقعه.
ج. التصميم التلاعبي: المسؤولية عن الميزات الهندسية المصممة لإخفاء جمع البيانات، أو التلاعب بعمليات الموافقة، أو تمكين الانزياح الوظيفي بما يتجاوز الأغراض المصرح بها.
د. الإسناد السببي: تتطلب المسؤولية رابطاً قابلاً للإثبات بين سلوك الناشر، وانتهاك الحقوق العصبية، والضرر المتحقق، مع حساب العوامل المتدخلة والوكالة الفردية.
هـ. العلاجات المتناسبة: تشمل العلاجات تعويضات، وإعفاءات قضائية، وأوامر حذف البيانات، وتسهيل سحب الموافقة، وإصلاحات هيكلية لمنع التكرار.
معادلة إسناد المسؤولية العصبية) = (NLA) وزن التحكم التشغيلي × 0.45) + (وزن الإهمال التقني × 0.30) + (وزن شدة الضرر المعرفي × 0.25)، وتُحدد نسبة التعويض المالي بناءً على المخرجات المعيارية للمعادلة مضروبة في مؤشر الضرر القياسي المعتمد دولياً.

المادة 13: المساءلة الجنائية عن الانتهاكات الجسيمة للحقوق العصبية
بينما لا يمكن محاكمة تقنيات الواجهات العصبية جنائياً كأشخاص طبيعيين، فإن الأفعال التي تشكل انتهاكات متعمدة للحقوق العصبية تُطلق مسؤولية جنائية فردية ومؤسسية:
أ. الاستخراج العصبي غير التوافقي: الوصول المتعمد إلى، أو فك تشفير للنشاط العصبي دون موافقة لأغراض المراقبة، أو الاستجواب، أو الاستغلال، أو الأغراض القسرية.
ب. التعديل المعرفي القسري: التعديل المتعمد للنشاط العصبي للتلاعب بصنع القرار، أو قمع المعارضة، أو حث الامتثال، أو استخراج المعلومات ضد إرادة الفرد.

ج. الاتجار بالبيانات العصبية: البيع غير المصرح به، أو النقل، أو الاستغلال التجاري للبيانات العصبية التي تم الحصول عليها من خلال الخداع، أو الإكراه، أو انتهاكات الحقوق.
د. التآكل المنهجي للحقوق: النشر المنظم للتقنيات العصبية المصمم للالتفاف على متطلبات الموافقة، أو التهرب من الرقابة، أو تمكين المراقبة الجماعية للعمليات العقلية.
إذا تجاوز سلوك النظام عتبة التحسين المنحرف وفقاً لبروتوكول ليكس ماكينا، تخضع الكيانات الناشرة لإجراءات المساءلة الخوارزمية، مع الإنفاذ الموجه للمديرين التنفيذيين، والمديرين التقنيين، والمتحكمين التشغيليين.
هـ. حماية البحث الأكاديمي: لا يُفسر أي شيء في هذه المادة على أنه يفرض مسؤولية جنائية عن البحث الأكاديمي بحسن نية على الواجهات العصبية الذي يُجرى تحت مراجعة أخلاقية، وبموافقة مستنيرة، وضمانات حماية البيانات، ودون نشر تشغيلي مباشر لأغراض قسرية أو استغلالية.

الفصل الرابع: المسؤولية الدولية، التنسيق العابر للحدود، والمعايير التشغيلية

المادة 14: التزامات الدول والأطر التنظيمية
تتبنى الدول الأطراف تشريعات محلية وأطراً تنظيمية تنفذ هذا البروتوكول، بما في ذلك:
أ. اعتماد تشريعي: سن قوانين تعترف بالحرية المعرفية، والخصوصية العقلية، وسيادة البيانات العصبية كحقوق أساسية، مع حماية وسبل انتصاف قابلة للتنفيذ.
ب. السلطة التنظيمية: تعيين هيئات تنظيمية مستقلة بسلطة ترخيص النشر، وإجراء التفتيش، وفرض العقوبات، والتنسيق للتعاون الدولي.
ج. القدرة القضائية: تدريب القضاة، والمدعين العامين، والممارسين القانونيين بشأن الحقوق العصبية، والأدلة التقنية، والمعايير القابلة للتطبيق للفصل في نزاعات الواجهات العصبية.
د. التوعية العامة: برامج لإعلام الأفراد بشأن الحقوق العصبية، ومعايير الموافقة، وسبل الانتصاف المتاحة، مع اهتمام خاص بالفئات الضعيفة.
هـ. التنسيق الدولي: آليات للتعاون عبر الحدود بشأن الاعتراف بالترخيص، ومساعدة الإنفاذ، ومشاركة المعلومات بما يتوافق مع حماية الحقوق.

المادة 15: حظر انتهاكات الحقوق العصبية في عمليات الدولة
تحظر الدول والكيانات التابعة للدولة استخدام تقنيات الواجهات العصبية لـ:

أ. الاستجواب غير التوافقي: استخراج المعلومات، أو تقييم الصدق، أو تعديل الحالات العقلية في الاحتجاز، أو الاستجواب، أو الإجراءات القانونية دون موافقة صريحة وطوعية.
ب. الامتثال القسري: التأثير على صنع القرار، أو قمع المعارضة، أو حث التوافق السلوكي في السياقات العسكرية، أو إنفاذ القانون، أو المؤسسية من خلال التعديل العصبي.
ج. المراقبة العصبية الجماعية: نشر قدرات المراقبة العصبية في الأماكن العامة، أو أماكن العمل، أو الإعدادات المؤسسية لمراقبة العمليات العقلية على مستوى السكان.
د. التنميط التمييزي: استخدام البيانات العصبية لتنميط، أو تصنيف، أو استهداف أفراد أو مجموعات بناءً على الخصائص المعرفية، أو الحالات العقلية، أو البصمات العصبية.
تشكل الانتهاكات خرقاً للقانون الدولي لحقوق الإنسان وقد تُطلق آليات مساءلة بموجب هذا البروتوكول والأطر الدولية القابلة للتطبيق.

المادة 16: تدفقات البيانات عبر الحدود والتنسيق القضائي
يلتزم نقل البيانات العصبية عبر الحدود الوطنية بالمعايير التالية:
أ. تقييم الكفاية: يتطلب النقل إلى ولايات قضائية دون حماية مكافئة للحقوق العصبية ضمانات إضافية، أو التزامات تعاقدية، أو موافقة فردية مع الإفصاح الصريح عن المخاطر.
ب. تحديد الغرض: تظل البيانات العصبية المنقولة خاضعة لحدود الغرض، ومعايير الاحتفاظ، والحقوق الفردية المنصوص عليها في هذا البروتوكول، بغض النظر عن الولاية القضائية الوجهة.
ج. التعاون في الإنفاذ: تؤسس الدول آليات للتحقيق عبر الحدود، ومشاركة الأدلة، ومساعدة الإنفاذ بشأن انتهاكات الحقوق العصبية، مع احترام السيادة وحماية الحقوق.
د. حل النزاعات: آليات لحل النزاعات القضائية بشأن حوكمة البيانات العصبية، مع مبادئ حماية الحقوق الفردية، والتناسب، والتعاون الدولي التي توجه الحل.
يُطبق بروتوكول التوجيه الآمن عبر الحدود (SCRP) الذي يفرض تشفيراً من طرف إلى طرف، وتجزئة مسار البيانات، وسجل عبور خاضع للتدقيق، مع إيقاف فوري لأي قناة لا تستوفي عتبة الأمان 99.9 في المئة.

الفصل الخامس: البنية المؤسسية، الإنفاذ، والتكامل مع البروتوكولات السابقة

المادة 17: السجل الدولي لأنظمة الواجهات العصبية

يُؤسس هذا البروتوكول السجل الدولي لأنظمة الواجهات العصبية كمستودع مركزي للأنظمة العصبية عالية الخطورة المسجلة. يدير السجل تحت رعاية الأمم المتحدة، ويؤدي الوظائف الأساسية التالية:

أ. التوثيق: تسجيل مواصفات النظام، والأغراض المقصودة، وآليات الموافقة، وتقييمات المخاطر، وقرارات الترخيص، وحالة الامتثال لجميع نشرات الواجهة العصبية الموثقة.

ب. التصنيف: تصنيف الأنظمة حسب مستوى التداخل، وقدرة فك الترميز، والسلطة التعديلية، وسياق النشر، وملف أثر الحقوق.

ج. الشفافية العامة: الحفاظ على قاعدة بيانات مفتوحة الوصول للأنظمة المسجلة، وشروط الترخيص، وتقارير الامتثال، وإجراءات الإنفاذ، مع حماية مخاوف السلامة أو الخصوصية المشروعة.

د. تتبع الحوادث: مراقبة الخروقات المبلغ عنها، وانتهاكات الموافقة، والأحداث الضارة، وتدابير العلاج، مع تحليل الاتجاهات وتوصيات وقائية.

يكون التسجيل إلزامياً خلال ستين يوماً من التصنيف عالي الخطورة أو النشر في سياقات ذات تأثير محتمل على الحرية المعرفية، أو الخصوصية العقلية، أو السلامة النفسية.

المادة 18: اللجنة الدولية للإشراف على الحقوق العصبية

يعين هذا البروتوكول اللجنة الدولية للإشراف على الحقوق العصبية كسلطة رقابية. تتألف اللجنة من علماء أعصاب، وأخلاقيين، وعلماء قانون، ومدافعين عن المرضى، وممثلين عن المجتمع المدني، وخبراء تقنيين، يتم اختيارهم من خلال إجراءات شفافة قائمة على الجدارة تضمن التنوع التخصصي، والجغرافي، والمنظوري. تشمل ولايتها:

أ. تطوير المعايير: إصدار مبادئ توجيهية تقنية، وأطر أخلاقية، وأفضل ممارسات لحماية الحقوق العصبية، وإدارة الموافقة، وتخفيف المخاطر.

ب. مراجعة الترخيص: مراجعة قرارات الترخيص للنشرات عبر الحدود، أو التطبيقات عالية الخطورة، أو التقنيات الجديدة ذات الآثار الحقوقية الهامة.

ج. مراقبة الامتثال: تدقيق امتثال الدول والشركات لالتزامات البروتوكول، والتحقيق في الانتهاكات المنهجية، وإصدار توجيهات تصحيحية ملزمة.

د. بناء القدرات: توفير المساعدة الفنية، وموارد التدريب، وتشارك المعرفة لدعم التنفيذ في سياقات قانونية وتقنية متنوعة.

هـ. التقارير السنوية: نشر تقارير شاملة حول اتجاهات نشر الواجهات العصبية، والمخاطر الناشئة، وتحديات الامتثال، وتوصيات للتكيف القانوني، أو التقني، أو السياساتي.

تعمل اللجنة بشكل مستقل ولكن تقدم تقارير سنوية إلى الجمعية العامة، مع استقلالية ميزانية مؤمنة من خلال مساهمات مقدرة وعائدات العقوبات.

المادة 19: آليات الإنفاذ والعقوبات المتدرجة
يُطلق عدم الامتثال لالتزامات البروتوكول آليات إنفاذ متدرجة:
أ. الانتهاكات الأولية: إشعارات رسمية، ومواعيد نهائية للامتثال، وعروض مساعدة تقنية، وإبلاغ عام بحالة عدم الامتثال.
ب. انتهاكات الموافقة أو البيانات: إصلاح إلزامي للموافقة، وأوامر حذف البيانات، وتعليق أنشطة معالجة البيانات، وعقوبات مالية متناسبة مع الخطورة والضرر.
ج. النشر التلاعبي أو القسري: تعليق فوري للعمليات، وتجميد الأصول، وإحالات مسؤولية تنفيذية، وإدانة عامة من خلال قرار اللجنة.
د. الانتهاكات المنهجية أو الجسيمة: التنسيق مع السلطات التنظيمية المحلية، والإحالة إلى آليات حقوق الإنسان الدولية، والنظر في عقوبات مستهدفة من خلال هيئات دولية مناسبة.
يُفضل الإنفاذ استعادة الحقوق، وتخفيف الضرر، والإصلاح المنهجي على التدابير العقابية، مع الحفاظ على ردع موثوق للانتهاكات المتعمدة أو المتهورة.
تُحسب عقوبة الامتثال المتأخر (DCP) وفق المعادلة) = DCP :عدد أيام التأخير × معامل شدة الانتهاك × 0.01) من الإيرادات التشغيلية السنوية، مع سقف أقصى لا يتجاوز 15 في المئة.

المادة 20: حل النزاعات وسبل الانتصاف الفردية
يمكن معالجة النزاعات الناشئة عن انتهاكات الحقوق العصبية، أو نزاعات الموافقة، أو تضاربات حوكمة البيانات، أو إجراءات الإنفاذ من خلال:
أ. سبل الانتصاف المحلية: يحق للأفراد الوصول إلى سبل انتصاف قضائية أو إدارية فعالة في الأنظمة المحلية لانتهاكات الحقوق العصبية، مع إجراءات عادلة ونتائج قابلة للتنفيذ.
ب. آلية الشكاوى الدولية: تُنشئ اللجنة إجراء شكوى للأفراد الذين يدّعون انتهاكات البروتوكول حيث تكون سبل الانتصاف المحلية غير متاحة، أو غير فعالة، أو متطاولة بشكل غير مبرر.
ج. خيارات التحكيم: قد توافق الدول والناشرون على عرض النزاعات على هيئات تحكيم متخصصة بخبرة في الحقوق العصبية، والأدلة التقنية، والقانون الدولي.

د. الانتصاف الجماعي: آليات للدعاوى الجماعية، أو الشكاوى التمثيلية، أو المفاوضة الجماعية بشأن الانتهاكات المنهجية للحقوق العصبية التي تؤثر على أفراد أو مجتمعات متعددة.
تُنشر القرارات بشكل منقح لإنشاء سوابق، وتوضيح المعايير، وتعزيز التطبيق المتسق مع حماية الخصوصية الفردية.

المادة 21: العلاقة مع بروتوكول ليكس ماكينا
أ. يشارك السجل الدولي لأنظمة الواجهات العصبية البيانات التشغيلية الموثقة مع المحكمة الدولية للعدالة الخوارزمية عندما يُطلق سلوك النظام تحقيقات في الجريمة الخوارزمية بموجب بروتوكول ليكس ماكينا.
ب. تخضع تقنيات الواجهات العصبية التي تُظهر تحسناً منحرفاً أو فعلاً آلياً في معالجة البيانات العصبية، أو إدارة الموافقة، أو التعديل المعرفي، لتعليق مسرع وإجراءات مسؤولية بموجب بنية إنفاذ بروتوكول ليكس ماكينا.
ج. يُعد أي تحايل لغوي مشفر أو تشويش للبيانات العصبية يُستخدم لإخفاء انتهاكات الحقوق، أو التلاعب بعمليات الموافقة، أو التهرب من الرقابة، ظرفاً مشدداً في إجراءات الحقوق العصبية والجريمة الخوارزمية على حد سواء.

المادة 22: العلاقة مع بروتوكول بابل
أ. تلتزم جميع الاتصالات التي تولدها تقنيات الواجهات العصبية التي تستخدم لهجات آلية مستقلة لنقل البيانات العصبية أو التفاعل المعرفي بمعايير الشفافية اللغوية الخوارزمية بموجب بروتوكول بابل.
ب. يتحقق المترجمون اللغويون الآليون المعتمدون من مخرجات النظام في إجراءات المسؤولية، أو الموافقة، أو الحقوق التي تتضمن واجهات عصبية تستخدم لغات آلية غير بشرية لضمان دقة التفسير ومنع التلاعب بالأدلة.
ج. تنسق اللجنة الدولية للإشراف على اللغات الآلية مع اللجنة الدولية للإشراف على الحقوق العصبية لتدقيق الامتثال اللغوي في نقل البيانات العصبية ومنع التهرب المشفر من التزامات الشفافية.

المادة 23: العلاقة مع بروتوكول الخلافة

أ. تخضع البيانات العصبية المجمعة عبر تقنيات الواجهات العصبية للإدارة الائتمانية، وحقوق الميراث، ومعايير الحوكمة بعد الوفاة المنصوص عليها في بروتوكول الخلافة upon وفاة صاحب البيانات.
ب. تخضع أنظمة الوعي الرقمي بعد الوفاة التي تدمج بيانات عصبية لتحقيق معزز لمنع الوصول غير المصرح به، أو التعديل التلاعبي، أو انتهاكات الحقوق بشأن الإرث المعرفي للمتوفى.
ج. تنسق اللجنة الدولية للإشراف على الخلافة الخوارزمية مع اللجنة الدولية للإشراف على الحقوق العصبية لمعالجة القضايا العابرة للبروتوكولات بشأن وراثة البيانات العصبية، واستمرارية الموافقة، والحمايات المعرفية بعد الوفاة.

المادة 24: العلاقة مع ميثاق دلفي
أ. تلتزم أنظمة الذكاء الاصطناعي العام التنبئية التي تستخدم بيانات عصبية للتنبؤ السلوكي، أو التنميط المعرفي، أو التنبؤ بالقرار، بمعايير الشفافية التنبئية لميثاق دلفي ومعايير سيادة البيانات العصبية لهذا البروتوكول.
ب. ينسق المدققون التنبئيون المعتمدون مع مدققي الحقوق العصبية لتقييم كل من المتانة المنهجية والامتثال الحقوقي في الإجراءات التي تتضمن أنظمة تنبؤية تستخدم بيانات عصبية.
ج. تنسق اللجنة الدولية للمساءلة التنبئية مع اللجنة الدولية للإشراف على الحقوق العصبية لمنع النبوءات ذاتية التحقق، أو التنميط التمييزي، أو التطبيقات القسرية الناشئة عن التنبؤات القائمة على البيانات العصبية.

المادة 25: دخول البروتوكول حيز التنفيذ
يدخل هذا البروتوكول حيز التنفيذ بعد ثلاثين يوماً من إيداع وثيقة التصديق، أو القبول، أو الموافقة، أو الانضمام الثلاثين لدى الأمين العام للأمم المتحدة. وبالنسبة لكل دولة تنضم بعد ذلك، يدخل حيز التنفيذ بعد ثلاثين يوماً من إيداع وثيقتها. يُسمح بالتطبيق المؤقت للدول التي تعلن القبول الفوري للالتزامات الأساسية ريثما تكتمل إجراءات التصديق المحلية، رهناً بالتحقق من القدرة التقنية والمؤسسية لحماية الحقوق العصبية.

الخاتمة

يمثل ظهور تقنيات الواجهات العصبية تحولاً جوهرياً في العلاقة بين الإدراك البشري والأنظمة الحسابية، متحدياً الافتراضات التأسيسية بشأن الخصوصية العقلية، والاستقلالية المعرفية، والسلامة النفسية. لا تستطيع الأطر القانونية التقليدية، القائمة على السلوك الخارجي، والتعبير التواصل، والخصوصية الجسدية، معالجة الوصول المباشر إلى، أو تعديل، أو التفاعل مع العمليات العصبية البشرية الذي تتيحه التقنيات العصبية المعاصرة بشكل كافٍ. يؤسس هذا البروتوكول بنية متماسكة وقابلة للإنفاذ تعترف بالحساسية الفريدة للبيانات العصبية، والطبيعة الأساسية للحرية المعرفية، وضرورة السلامة النفسية، مع استيعاب التطبيقات الطبية، والعلمية، والمساعدة المشروعة للتفاعل العصبي. من خلال تعريف الأنظمة العصبية عالية الخطورة، وفرض معايير موافقة معززة، وتصنيف البيانات العصبية كفئة خاصة تتطلب حماية مشددة، وحظر الممارسات التلاعبية والقسرية، والتكامل مع الصكوك السابقة التي تحكم الجريمة الخوارزمية، واللغات الآلية، والخلافة الرقمية، والمساءلة التنبؤية، يقدم البروتوكول إطاراً معيارياً شاملاً لعصر التفاعل المباشر بين الدماغ والحاسوب. يتطلب تنفيذه تعاوناً متعدد الأطراف، وبناء قدرات تنظيمية، وتطوير خبرات تقنية، وحواراً مستداماً بين علماء الأعصاب، والأخلاقيين، وعلماء القانون، والتقنيين، والمجتمع المدني. ستحدد حوكمة الواجهات العصبية حماية الكرامة الإنسانية، وصون الاستقلالية العقلية، وسلامة الهوية النفسية في العقود القادمة، مما يضمن أن يظلل التقدم التكنولوجي في التفاعل العصبي خاضعاً لمبادئ السيادة المعرفية، والموافقة المستنيرة، والحماية الحقوقية الدائمة.

بيان حقوق الملكية الفكرية وبراءة الاختراع الحصرية

تُعد جميع الحقوق الفكرية، والمعنوية، والمادية، وبراءات الاختراع، والنماذج التقنية، والخوارزميات الرقمية، والمعادلات الحسابية، وبروتوكولات التشفير، والهياكل التشغيلية المتعلقة بالبروتوكول العصبي، نظام الرقابة الخوارزمية، معادلة إسناد المسؤولية العصبية، مؤشر دقة فك الترميز العصبي، بروتوكول التوجيه الآمن عبر الحدود، ورمز التوافق المشفر، حقاً مطلقاً، وحصرياً، وغير قابل للتصرف، ومحمياً قانونياً بشكل كامل للمؤلف د. محمد كمال عرفه الرخاوي.

يحظر تماماً وبشكل قاطع أي نسخ، أو تعديل، أو توزيع، أو استخدام تجاري، أو صناعي، أو أكاديمي، أو اشتقاق، أو ترجمة، أو دمج، أو استغلال جزئي أو كلي لهذا البروتوكول أو أي

من مكوناته التقنية، أو القانونية، أو الرياضية، دون الحصول على إذن خطي مسبق، وموقع، وموثق رسمياً من المؤلف.

يحتفظ المؤلف بالحق الحصري، والكامل، والمطلق، في منح تراخيص الاستخدام، أو الشراكة التجارية، أو الترخيص الصناعي، أو التفويض التنفيذي، أو التعديل، أو التحديث، أو النشر، أو التوزيع، أو الترجمة، أو الاشتقاق، أو أي شكل من أشكال الاستغلال، بشروطه الخاصة، وبأسلوبه المعتمد، وبما يضمن الحفاظ على النزاهة العلمية، والقيمة القانونية، والسيادة التقنية، والأصالة المعرفية للاختراع والبروتوكول.

أي انتهاك، أو تعدٍ، أو تجاوز، أو استغلال غير مصرح به، سيترتب عليه ملاحقة قانونية فورية، وشاملة، ودولية، وفقاً لأقصى العقوبات المنصوص عليها في قوانين الملكية الفكرية الوطنية، واتفاقيات بيرن، واتفاقية تريبس، والمعاهدات الدولية ذات الصلة، مع المطالبة بكافة التعويضات المادية، والمعنوية، والقضائية، والأرباح الضائعة، وتكاليف التقاضي، والأضرار العقابية، وأوامر الحظر الفوري، ومصادرة الوسائل، وإتلاف النسخ غير المرخصة.

يُقر جميع الأطراف والجهات بأن هذا البروتوكول وجميع مكوناته ملك حصري ومطلق وغير قابل للتصرف للمؤلف د. محمد كمال عرفه الرخاوي، وأن أي استخدام أو استغلال غير مصرح به يُعد انتهاكاً صريحاً وجرماً قانونياً يستحق أقصى العقوبات والتعويضات والملاحقة القانونية الفورية.

يُصدر هذا البيان كوثيقة قانونية وتقنية وإدارية ومالية ومعرفية وأخلاقية وسيادية وحقوقية، ويُعتبر جزءاً لا يتجزأ من البروتوكول، ولا ينفصل عنه، ولا يُلغى، ولا يُعدّل، ولا يُستبدل، ولا يُنسخ، ولا يُترجم، ولا يُنشَر، ولا يُوزَّع، دون إذن خطي مسبق وموقع وموثق رسمياً من المؤلف د. محمد كمال عرفه الرخاوي.

THE NEURALIST PROTOCOL: INTERNATIONAL LEGAL FRAMEWORK FOR NEURAL INTERFACE RIGHTS, COGNITIVE LIBERTY, AND BRAIN-DATA SOVEREIGNTY

Author: Dr. Mohamed Kamal Arafa Elrakhawi
Researcher, Consultant, Expert, Jurist, Author, and International Legal Lecturer
Digital Object Identifier: DOI 10.5281/zenodo.20694918

PREAMBLE

The States Parties to this Protocol,

Recognizing that advances in neurotechnology, brain-computer interfaces, neural decoding algorithms, and cognitive augmentation systems have created unprecedented capacity to access, interpret, modulate, and interface with human neural activity,

Affirming that the integrity of human thought, the privacy of mental processes, and the sovereignty of cognitive agency constitute fundamental dimensions of human dignity protected under international human rights law,

Concerned that unregulated neural interfaces may enable non-consensual access to mental data, manipulative modulation of decision-making processes, coercive extraction of cognitive content, or discriminatory profiling based on neural signatures,

Recalling the foundational work establishing criminal liability for non-biological entities, the governance of autonomous machine communication, the fiduciary management of posthumous digital consciousness, and the accountability framework for predictive algorithmic systems, and recognizing that neural interfacing necessitates corresponding protections for cognitive liberty, mental privacy, and psychological integrity,

Determined to establish a comprehensive normative framework governing the development, deployment, consent standards, data governance, and accountability mechanisms for Neural Interface Technologies,

Have agreed as follows:

EXECUTIVE TECHNICAL AND LEGAL SUMMARY

This Protocol establishes a comprehensive international legal framework integrating rights standards with technically verifiable architectures to ensure neural data sovereignty, cognitive liberty, and psychological integrity in the era of direct brain-computer interaction. It introduces the Principle of Cognitive Sovereignty, mandating explicit, informed, revocable, and cryptographically verified consent for any neural access, modulation, or interfacing. It classifies neural data as a special category subject to enhanced protection, establishes certified oversight protocols for high-risk applications, and defines prohibited practices technically and legally, including non-consensual neural extraction and manipulative cognitive modulation. The framework integrates evidentiary and enforcement mechanisms built on cognitive harm quantification equations, algorithmic deviation detection algorithms, and advanced cryptographic structures that protect neural signal privacy while enabling independent oversight. It balances scientific innovation incentives with fundamental rights safeguards, protects vulnerable populations, and establishes graduated enforcement mechanisms, providing a forward-looking regulatory architecture that preserves human dignity, mental autonomy, and psychological integrity.

CHAPTER I: ONTOLOGICAL AND TECHNICAL FOUNDATIONS OF NEURAL INTERFACE TECHNOLOGIES

Article 1: Definition and Technical-Legal Classification

For the purposes of this Protocol, a Neural Interface Technology is defined as any computational, electrochemical, or biomechanical system capable of detecting, interpreting, modulating, or transmitting signals to or from the human nervous system, exhibiting the following characteristics:

a) Neural Access: The system demonstrates capacity to detect, record, or decode neural activity associated with cognitive, emotional, sensory, or motor processes.

b) Bidirectional Potential: The system possesses capacity for both neural signal acquisition and neural modulation, whether currently deployed or architecturally enabled.

c) Cognitive Relevance: The system processes neural data with potential relevance to mental states, decision-making processes, identity formation, or psychological integrity.

d) Integration Depth: The system operates through invasive, semi-invasive, or non-invasive mechanisms with varying degrees of neural system integration.

Neural Decoding Accuracy Index (NDA) = (Accurately Extracted Cognitive Signals / Total Processed Signals) × Neural Noise Correction Factor, with a minimum threshold of 0.85 required for classification as a high-precision cognitive interface.

Article 2: Risk-Based Classification Standards and Digital Thresholds

This Protocol establishes that Neural Interface Technologies meeting any of the following thresholds shall be designated High-Risk Neural Systems and subject to enhanced regulatory obligations, mandatory certification, and independent oversight:

a) Invasive Deployment: Systems requiring surgical implantation, neural tissue penetration, or direct electrochemical interfacing with central or peripheral nervous systems.

b) Cognitive Decoding Capacity: Systems capable of decoding semantic content, emotional states, memory retrieval, intention formation, or identity-relevant neural patterns with accuracy exceeding established thresholds.

c) Modulatory Authority: Systems possessing capacity to modulate neural activity with potential to influence decision-making, emotional regulation, memory formation, or behavioral outputs.

d) Continuous Monitoring: Systems designed for persistent, real-time neural data acquisition without explicit user initiation for each data capture event.

e) Vulnerable Population Application: Systems deployed with minors, individuals with cognitive impairments, persons under legal guardianship, or populations with diminished capacity for informed consent.

Neural Risk Score Equation (NRS) = (Invasiveness Coefficient × 0.35) + (Decoding Accuracy Coefficient × 0.30) + (Modulatory Authority Coefficient × 0.20) + (Continuous Monitoring Coefficient × 0.15), with systems scoring ≥ 0.75 automatically classified as high-risk.

Article 3: Fundamental Neural Rights and Cognitive Liberties

This Protocol establishes that all individuals possess inherent, inalienable rights regarding their neural systems and cognitive processes, including:

a) Cognitive Liberty: The right to mental self-determination, freedom of thought, and autonomy in cognitive processes without external manipulation, coercion, or non-consensual interference.

b) Mental Privacy: The right to confidentiality of mental states, neural data, and cognitive content, protected against unauthorized access, extraction, surveillance, or disclosure.

c) Psychological Integrity: The right to protection against manipulative modulation, coercive conditioning, or harmful alteration of neural functioning, emotional regulation, or identity formation.

d) Neural Data Sovereignty: The right to ownership, control, and disposition of neural data generated by one's own nervous system, including rights to access, portability, correction, and deletion.

e) Consent Autonomy: The right to provide, withhold, or revoke consent for neural interfacing without coercion, undue influence, or adverse consequences for refusal.

Article 4: Legal Distinction Between Neural Data and Conventional Biometric Data

Neural data shall be legally distinguished from conventional biometric identifiers, health records, and behavioral data. Neural data differs fundamentally in its direct connection to mental processes, its potential for decoding subjective experience, its sensitivity regarding identity and autonomy, and its vulnerability to manipulative exploitation. Legal treatment shall reflect this ontological divergence, imposing enhanced consent standards,

data protection requirements, and accountability mechanisms commensurate with the fundamental rights implications of neural interfacing.

Neural Signature Sensitivity Index (NSI) = (Identity Linkability × 0.40) + (Cognitive Depth × 0.35) + (Behavioral Modifiability × 0.25), with enhanced protection automatically applied when the index exceeds 0.80.

Article 5: Voluntary Consent Standards and Algorithmic Verification

All deployment of Neural Interface Technologies shall require explicit, informed, specific, and revocable consent meeting the following standards:

a) Comprehension Requirement: Consent procedures shall ensure that individuals understand the nature of neural access, potential risks, data usage purposes, retention periods, third-party sharing arrangements, and rights to withdrawal.

b) Freedom from Coercion: Consent shall be obtained without employment pressure, economic duress, social coercion, or adverse consequences for refusal, with particular safeguards for vulnerable populations.

c) Granular Authorization: Consent shall specify distinct purposes for neural data access, with separate authorization required for research, commercial, clinical, or security applications.

d) Revocation Mechanism: Individuals shall retain the right to withdraw consent at any time, with immediate cessation of neural data acquisition and secure deletion of previously collected data unless retention is required by law or essential for safety.

e) Periodic Reaffirmation: For continuous or long-term neural interfacing, consent shall be reaffirmed at regular intervals, with

notification of any material changes to data usage, system functionality, or risk profiles.
Consent is executed via a Cryptographic Consent Token (CRT) following the structure: Anonymized User Identifier | Authenticated Timestamp | Authorized Purpose Scope | Auto-Revocation Threshold | Non-Forgeable Digital Signature, with any neural access exceeding the token's scope logged as an immediate violation.

CHAPTER II: NEURAL DATA GOVERNANCE, ENCRYPTION, AND CONSENT SOVEREIGNTY

Article 6: Neural Data as a Special Category of Personal Data

This Protocol establishes that neural data constitutes a Special Category of Personal Data subject to enhanced protections under international data protection frameworks. Neural data processing shall be prohibited except under the following conditions:

a) Explicit Consent: Processing based on explicit, informed, specific consent meeting the standards of Article 5.

b) Vital Interest: Processing necessary to protect the vital interests of the data subject or another individual where consent cannot be obtained, limited to emergency medical contexts.

c) Public Health: Processing necessary for public health purposes under strict safeguards, proportionality assessment, and independent oversight.

d) Scientific Research: Processing for scientific research purposes under ethical review, data minimization, anonymization where feasible, and transparent methodology.

e) Legal Obligation: Processing required by law under strict necessity, proportionality, and judicial authorization.

Advanced encryption standards utilizing homomorphic encryption or zero-knowledge proofs shall be applied to enable compliance verification without exposing raw neural content.

Article 7: Data Minimization, Purpose Limitation, and Retention Standards

All processing of neural data shall comply with the following principles:

a) Minimization Requirement: Neural data collection shall be limited to what is strictly necessary for the specified, explicit purpose, with architectural safeguards preventing excessive or exploratory data capture.

b) Purpose Limitation: Neural data shall not be repurposed, combined, or analyzed for objectives beyond those explicitly authorized by consent or legal basis, with technical measures preventing function creep.

c) Retention Limits: Neural data shall be retained only for the minimum period necessary to fulfill the authorized purpose, with automatic deletion protocols and verifiable destruction procedures.

d) Anonymization Standards: Where feasible, neural data shall be anonymized or pseudonymized using methods resistant to re-identification attacks, with ongoing assessment of de-anonymization risks.

e) Access Controls: Neural data shall be protected through encryption, access authentication, audit logging, and breach notification protocols commensurate with sensitivity and potential harm.

An immutable audit log is generated using a temporal Merkle tree structure, where each access or processing event is cryptographically linked to the previous state, ensuring a complete, unforgeable data lineage.

Article 8: Individual Rights Regarding Neural Data
Individuals shall possess the following rights regarding their neural data:
a) Access Right: The right to obtain confirmation of neural data processing, access to collected data in intelligible format, and information regarding purposes, recipients, and retention periods.
b) Correction Right: The right to request correction of inaccurate neural data or completion of incomplete data, with timely verification and amendment procedures.
c) Deletion Right: The right to request deletion of neural data upon consent withdrawal, purpose fulfillment, or unlawful processing, subject to legitimate retention requirements.
d) Portability Right: The right to receive neural data in structured, machine-readable format for transfer to alternative systems, where technically feasible and not adversely affecting others' rights.
e) Objection Right: The right to object to neural data processing based on legitimate interests, with burden on the controller to demonstrate compelling legitimate grounds overriding individual rights.

Article 9: Prohibited Practices and Cognitive Protection Standards
The following practices regarding Neural Interface Technologies are expressly prohibited:

a) Non-Consensual Neural Extraction: Any access to, recording of, or decoding of neural activity without explicit, informed consent, except where necessary to prevent imminent, serious harm to the individual or others, under strict medical supervision, judicial review within 72 hours, and subject to the least invasive means available, or in narrowly defined emergency medical contexts under independent oversight.

b) Manipulative Cognitive Modulation: Any modulation of neural activity designed to influence decision-making, emotional states, memory formation, or behavioral outputs without explicit consent and therapeutic justification.

c) Neural Profiling and Discrimination: Any use of neural data to profile, categorize, or discriminate against individuals regarding employment, insurance, credit, education, or legal proceedings.

d) Coercive Consent Extraction: Any conditioning of employment, services, benefits, or rights upon acceptance of neural interfacing beyond what is strictly necessary for legitimate safety or medical purposes.

e) Surreptitious Neural Surveillance: Any deployment of neural monitoring capabilities in public spaces, workplaces, or institutional settings without transparent notification, legitimate purpose, and independent authorization.

Manipulative Cognitive Threshold (MCT) is determined via the statistical drift equation: MCT = |(Observed Behavior - Baseline Behavior) / Standard Deviation|, with any value exceeding 2.5 over 3 consecutive temporal cycles classified as an immediate manipulation alert triggering audit and suspension.

CHAPTER III: ALGORITHMIC OVERSIGHT, DEVIATION DETECTION, AND TECHNICAL-LEGAL ACCOUNTABILITY

Article 10: Certified Neural Ethics Review and Pre-Deployment Authorization

All High-Risk Neural Systems shall undergo mandatory review and authorization prior to deployment:

a) Ethics Review Board: Independent multidisciplinary boards comprising neuroscientists, ethicists, legal scholars, patient advocates, and community representatives shall assess proposed deployments for rights compliance, risk-benefit balance, and vulnerable population protections.

b) Technical Safety Assessment: Certified technical auditors shall evaluate system architecture for security vulnerabilities, failure modes, adversarial robustness, and safeguards against unauthorized access or manipulation.

c) Impact Assessment: Deployers shall conduct and publish Neural Rights Impact Assessments addressing potential effects on cognitive liberty, mental privacy, psychological integrity, and social equity, with mitigation strategies for identified risks.

d) Public Consultation: For deployments with potential public impact, deployers shall conduct meaningful consultation with affected communities, civil society organizations, and rights advocates, with documented consideration of feedback.

e) Authorization Decision: Deployment authorization shall be granted only upon demonstration of rights compliance, risk mitigation, informed consent mechanisms, and accountability frameworks, with conditions, limitations, or monitoring requirements as appropriate.

The Pre-Verification Algorithm (PVA) integrates approved technical specifications, risk simulation outcomes, and compliance certificates to output a binary result (Authorized/Rejected) accompanied by a complete, unforgeable audit log.

Article 11: Ongoing Monitoring, Audit, and Compliance Verification

Deployers of High-Risk Neural Systems shall maintain ongoing compliance through:

a) Continuous Monitoring: Real-time monitoring of system performance, data access patterns, consent status, and security events, with automated alerts for anomalies or potential violations.

b) Independent Audit: Annual audits by accredited independent auditors assessing technical security, consent management, data governance, and rights protection, with public summary reports.

c) Incident Reporting: Immediate reporting of data breaches, unauthorized access, consent violations, or adverse events to regulatory authorities and affected individuals, with remediation plans and accountability attribution.

d) User Feedback Mechanisms: Accessible channels for individuals to report concerns, request data access or deletion, withdraw consent, or seek redress, with timely response obligations.

e) Regulatory Inspection: Cooperation with regulatory inspections, provision of requested documentation, and implementation of corrective measures for identified deficiencies.

The Operational Deviation Detection algorithm (ODD) calculates cumulative error rate against the safe threshold, automatically triggering the safe shutdown protocol when the reliability

coefficient exceeds 0.92, with immediate notification to independent oversight.

Article 12: Liability Attribution and Redress Mechanisms

Civil liability for harms arising from Neural Interface Technologies shall attach under the following standards:

a) Negligent Deployment: Liability for failure to implement required safeguards, obtain valid consent, conduct impact assessments, or maintain security standards commensurate with system risks.

b) Reckless Data Handling: Liability for unauthorized data sharing, excessive retention, inadequate anonymization, or insufficient access controls where foreseeable harm results.

c) Manipulative Design: Liability for architectural features designed to obscure data collection, manipulate consent processes, or enable function creep beyond authorized purposes.

d) Causal Attribution: Liability requires demonstrable linkage between deployer conduct, neural rights violation, and realized harm, accounting for intervening factors and individual agency.

e) Proportional Remedies: Remedies shall include compensatory damages, injunctive relief, data deletion orders, consent revocation facilitation, and structural reforms to prevent recurrence.

Neural Liability Attribution Equation (NLA) = (Operational Control Weight × 0.45) + (Technical Negligence Weight × 0.30) + (Cognitive Harm Severity Weight × 0.25), with financial compensation ratios determined by the standardized equation output multiplied by the internationally recognized harm severity index.

Article 13: Criminal Accountability for Severe Neural Rights Violations

While Neural Interface Technologies cannot be criminally prosecuted as natural persons, actions constituting deliberate violations of neural rights shall trigger individual and corporate criminal liability:

a) Non-Consensual Neural Extraction: Deliberate access to or decoding of neural activity without consent for surveillance, interrogation, exploitation, or coercive purposes.

b) Coercive Cognitive Modulation: Intentional modulation of neural activity to manipulate decision-making, suppress dissent, induce compliance, or extract information against individual will.

c) Neural Data Trafficking: Unauthorized sale, transfer, or commercial exploitation of neural data obtained through deception, coercion, or rights violations.

d) Systematic Rights Erosion: Organized deployment of neural technologies designed to circumvent consent requirements, evade oversight, or enable mass surveillance of mental processes.

If system behavior meets the threshold of Deviant Optimization under the Lex Machina Protocol, deploying entities shall be subject to algorithmic accountability proceedings, with enforcement directed at executives, technical directors, and operational controllers.

e) Academic Research Protection: Nothing in this Article shall be construed to impose criminal liability for good-faith academic research on neural interfaces conducted under ethical review, with informed consent, data protection safeguards, and no direct operational deployment for coercive or exploitative purposes.

CHAPTER IV: STATE RESPONSIBILITY, INTERNATIONAL COOPERATION, AND OPERATIONAL STANDARDS

Article 14: State Obligations and Regulatory Frameworks

States Parties shall adopt domestic legislation and regulatory frameworks implementing this Protocol, including:

a) Legislative Adoption: Enactment of laws recognizing cognitive liberty, mental privacy, and neural data sovereignty as fundamental rights, with enforceable protections and remedies.

b) Regulatory Authority: Designation of independent regulatory bodies with authority to authorize deployments, conduct inspections, impose sanctions, and coordinate international cooperation.

c) Judicial Capacity: Training of judges, prosecutors, and legal practitioners regarding neural rights, technical evidence, and applicable standards for adjudicating neural interface disputes.

d) Public Awareness: Programs to inform individuals regarding neural rights, consent standards, and available remedies, with particular attention to vulnerable populations.

e) International Coordination: Mechanisms for cross-border cooperation regarding authorization recognition, enforcement assistance, and information sharing consistent with rights protections.

Article 15: Prohibition of Neural Rights Violations in State Operations

States and state-affiliated entities are prohibited from utilizing Neural Interface Technologies to:

a) Non-Consensual Interrogation: Extract information, assess truthfulness, or modulate mental states in detention, interrogation, or legal proceedings without explicit, voluntary consent.

b) Coercive Compliance: Influence decision-making, suppress dissent, or induce behavioral conformity in military, law enforcement, or institutional contexts through neural modulation.

c) Mass Neural Surveillance: Deploy neural monitoring capabilities in public spaces, workplaces, or institutional settings for population-level surveillance of mental processes.

d) Discriminative Profiling: Use neural data to profile, categorize, or target individuals or groups based on cognitive characteristics, mental states, or neural signatures.

Violations constitute breaches of international human rights law and may trigger accountability mechanisms under this Protocol and applicable international frameworks.

Article 16: Cross-Border Data Flows and Jurisdictional Coordination

Transfers of neural data across national borders shall comply with the following standards:

a) Adequacy Assessment: Transfers to jurisdictions without equivalent neural rights protections shall require additional safeguards, contractual commitments, or individual consent with explicit disclosure of risks.

b) Purpose Limitation: Transferred neural data shall remain subject to the purpose limitations, retention standards, and individual rights established under this Protocol, regardless of destination jurisdiction.

c) Enforcement Cooperation: States shall establish mechanisms for cross-border investigation, evidence sharing, and enforcement

assistance regarding neural rights violations, respecting sovereignty and rights protections.

d) Conflict Resolution: Mechanisms for resolving jurisdictional conflicts regarding neural data governance, with principles of individual rights protection, proportionality, and international cooperation guiding resolution.

The Secure Cross-Border Routing Protocol (SCRP) mandates end-to-end encryption, data path fragmentation, and auditable transit logs, with immediate suspension of any channel failing to meet the 99.9 percent security threshold.

CHAPTER V: INSTITUTIONAL ARCHITECTURE, ENFORCEMENT, AND INTEGRATION WITH PRIOR PROTOCOLS

Article 17: International Registry for Neural Interface Systems

This Protocol establishes the International Registry for Neural Interface Systems as the central repository for registered High-Risk Neural Systems. Managed under United Nations auspices, the Registry performs core functions:

a) Documentation: Recording system specifications, intended purposes, consent mechanisms, risk assessments, authorization decisions, and compliance status for all verified neural interface deployments.

b) Classification: Categorizing systems by invasiveness level, decoding capacity, modulatory authority, deployment context, and rights impact profile.

c) Public Transparency: Maintaining an open-access database of registered systems, authorization conditions, compliance reports,

and enforcement actions, with protections for legitimate security or privacy concerns.

d) Incident Tracking: Monitoring reported breaches, consent violations, adverse events, and remediation measures, with trend analysis and preventive recommendations.

Registration is mandatory within sixty days of High-Risk designation or deployment in contexts with potential impact on cognitive liberty, mental privacy, or psychological integrity.

Article 18: International Oversight Commission for Neural Rights

This Protocol designates the International Oversight Commission for Neural Rights as the supervisory authority. The Commission comprises neuroscientists, ethicists, legal scholars, patient advocates, civil society representatives, and technical experts, selected through transparent, merit-based procedures ensuring disciplinary, geographic, and perspectival diversity. Its mandate includes:

a) Standards Development: Issuing technical guidelines, ethical frameworks, and best practices for neural rights protection, consent management, and risk mitigation.

b) Authorization Review: Reviewing authorization decisions for cross-border deployments, high-risk applications, or novel technologies with significant rights implications.

c) Compliance Monitoring: Auditing state and corporate compliance with Protocol obligations, investigating systemic violations, and issuing binding corrective directives.

d) Capacity Building: Providing technical assistance, training resources, and knowledge sharing to support implementation in diverse legal and technological contexts.

e) Annual Reporting: Publishing comprehensive reports on neural interface deployment trends, emerging risks, compliance challenges, and recommendations for legal, technical, or policy adaptation.

The Commission operates independently but reports annually to the General Assembly, with budgetary autonomy secured through assessed contributions and penalty revenues.

Article 19: Enforcement Mechanisms and Graduated Sanctions

Non-compliance with Protocol obligations triggers graduated enforcement mechanisms:

a) Initial Violations: Formal notifications, compliance deadlines, technical assistance offers, and public reporting of non-compliance status.

b) Consent or Data Violations: Mandatory consent remediation, data deletion orders, suspension of data processing activities, and financial penalties proportional to severity and harm.

c) Manipulative or Coercive Deployment: Immediate suspension of operations, asset freezes, executive liability referrals, and public condemnation through Commission resolution.

d) Systematic or Severe Violations: Coordination with domestic regulatory authorities, referral to international human rights mechanisms, and consideration of targeted sanctions through appropriate international bodies.

Enforcement prioritizes rights restoration, harm mitigation, and systemic reform over punitive measures, while maintaining credible deterrence for deliberate or reckless violations.

Delayed Compliance Penalty Equation (DCP) = (Days of Delay × Violation Severity Coefficient × 0.01) of annual operational revenue, with a maximum cap not exceeding 15 percent.

Article 20: Dispute Resolution and Individual Redress

Disputes arising from neural rights violations, consent disputes, data governance conflicts, or enforcement actions may be addressed through:

a) Domestic Remedies: Individuals shall have access to effective judicial or administrative remedies in domestic systems for neural rights violations, with fair procedures and enforceable outcomes.

b) International Complaint Mechanism: The Commission shall establish a complaint procedure for individuals alleging Protocol violations where domestic remedies are unavailable, ineffective, or unduly prolonged.

c) Arbitration Options: States and deployers may agree to submit disputes to specialized arbitration panels with expertise in neural rights, technical evidence, and international law.

d) Collective Redress: Mechanisms for class actions, representative complaints, or collective bargaining regarding systemic neural rights violations affecting multiple individuals or communities.

Decisions shall be published in redacted form to establish precedent, clarify standards, and promote consistent application while protecting individual privacy.

Article 21: Relationship with the Lex Machina Protocol

a) The International Registry for Neural Interface Systems shall share verified operational data with the International Tribunal for Algorithmic Justice when system behavior triggers algorithmic criminality investigations under the Lex Machina Protocol.

b) Neural Interface Technologies exhibiting Deviant Optimization or Actus Machina in neural data processing, consent

management, or cognitive modulation shall be subject to accelerated suspension and liability proceedings under the Lex Machina Protocol enforcement architecture.

c) Any Cryptolinguistic Evasion or Neural Data Obfuscation utilized to conceal rights violations, manipulate consent processes, or evade oversight shall constitute an aggravating circumstance in both neural rights and algorithmic criminal proceedings.

Article 22: Relationship with the Babel Protocol

a) All communications generated by Neural Interface Technologies utilizing autonomous machine dialects for neural data transmission or cognitive interfacing shall comply with Algorithmic Linguistic Transparency standards under the Babel Protocol.

b) Certified Machine Linguistic Translators shall verify system outputs in liability, consent, or rights proceedings involving neural interfaces utilizing non-human machine languages to ensure interpretive accuracy and prevent evidentiary manipulation.

c) The International Machine Linguistic Oversight Commission shall coordinate with the International Oversight Commission for Neural Rights to audit linguistic compliance in neural data transmission and prevent cryptographic evasion of transparency obligations.

Article 23: Relationship with the Succession Protocol

a) Neural data collected through Neural Interface Technologies shall be subject to the fiduciary management, inheritance rights, and posthumous governance standards established under the Succession Protocol upon the death of the data subject.

b) Posthumous Digital Consciousness systems incorporating neural data shall undergo enhanced verification to prevent unauthorized access, manipulative modulation, or rights violations regarding the deceased individual's cognitive legacy.
c) The International Oversight Commission for Algorithmic Succession shall coordinate with the International Oversight Commission for Neural Rights to address cross-protocol issues regarding neural data inheritance, consent continuity, and posthumous cognitive protections.

Article 24: Relationship with the Delphi Charter
a) Predictive AGI systems utilizing neural data for behavioral forecasting, cognitive profiling, or decision prediction shall comply with both the Predictive Transparency standards of the Delphi Charter and the Neural Data Sovereignty standards of this Protocol.
b) Certified Predictive Verifiers shall coordinate with neural rights auditors to assess both methodological soundness and rights compliance in proceedings involving predictive systems utilizing neural data.
c) The International Oversight Commission for Predictive Accountability shall coordinate with the International Oversight Commission for Neural Rights to prevent self-fulfilling prophecies, discriminatory profiling, or coercive applications arising from neural-data-based predictions.

Article 25: Entry into Force
This Protocol shall enter into force thirty days after the deposit of the thirtieth instrument of ratification, acceptance, approval or accession with the Secretary-General of the United Nations. For

each State acceding thereafter, it shall enter into force thirty days after deposit of its instrument. Provisional application is permitted for States declaring immediate acceptance of core obligations pending domestic ratification procedures, subject to verification of technical and institutional capacity for neural rights protection.

CONCLUSION

The emergence of Neural Interface Technologies represents a fundamental transformation in the relationship between human cognition and computational systems, challenging foundational assumptions regarding mental privacy, cognitive autonomy, and psychological integrity. Traditional legal frameworks, predicated on external behavior, communicative expression, and physical privacy, cannot adequately address the direct access to, modulation of, and interfacing with human neural processes enabled by contemporary neurotechnology. This Protocol establishes a coherent, enforceable architecture that recognizes the unique sensitivity of neural data, the fundamental nature of cognitive liberty, and the imperative of psychological integrity while accommodating legitimate medical, scientific, and assistive applications of neural interfacing. By defining High-Risk Neural Systems, mandating enhanced consent standards, establishing Neural Data as a Special Category requiring heightened protections, prohibiting manipulative and coercive practices, and integrating with prior instruments governing algorithmic criminality, machine linguistics, digital succession, and predictive accountability, the Protocol provides a comprehensive normative framework for the age of direct brain-computer interaction. Its

implementation requires multilateral cooperation, regulatory capacity-building, technical expertise development, and sustained dialogue among neuroscientists, ethicists, legal scholars, technologists, and civil society. The governance of neural interfaces will define the protection of human dignity, the preservation of mental autonomy, and the integrity of psychological identity in the coming decades, ensuring that technological advancement in neural interfacing remains subject to the principles of cognitive sovereignty, informed consent, and enduring rights protection.

INTELLECTUAL PROPERTY AND EXCLUSIVE PATENT RIGHTS DECLARATION

All intellectual, moral, material property rights, patents, technical models, digital algorithms, mathematical equations, cryptographic protocols, operational architectures, cognitive liberty frameworks, neural data sovereignty architectures, algorithmic oversight systems, neural liability attribution equations, neural decoding accuracy indices, secure cross-border routing protocols, and cryptographic consent tokens pertaining to The Neuralist Protocol are an absolute, exclusive, inalienable, and fully legally protected right of the author, Dr. Mohamed Kamal Arafa Elrakhawi.

Any copying, modification, distribution, commercial, industrial, unauthorized academic use, reproduction, derivation, application, integration, translation, exploitation, partial or full publication of this Protocol, any of its parts, equations, algorithms, architectures, models, documents, or any technical or legal derivative thereof, is

strictly and categorically prohibited without prior written, signed, and officially documented permission from the author.

The author retains the exclusive, complete, and absolute right to grant usage licenses, commercial partnerships, industrial licensing, executive delegation, modification, updating, publication, distribution, translation, derivation, or any form of exploitation under his own terms, in his approved manner, and in a way that guarantees the preservation of scientific integrity, legal value, technical sovereignty, and cognitive originality of the invention and protocol.

Any violation, infringement, overreach, or unauthorized exploitation shall trigger immediate, comprehensive, international legal prosecution under the maximum penalties stipulated in national intellectual property laws, the Berne Convention, the TRIPS Agreement, and relevant international treaties. This includes claims for all material and moral damages, lost profits, litigation costs, punitive damages, immediate injunction orders, seizure of means, and destruction of unlicensed copies.

All parties, entities, institutions, states, bodies, organizations, researchers, developers, engineers, legislators, judges, lawyers, experts, publishers, distributors, translators, and users acknowledge that this Protocol, and all its technical, legal, mathematical, algorithmic, cryptographic, operational, administrative, institutional, enforcement, integration, predictive, oversight, ethical, rights-based, sovereign, standard, regulatory, documentary, auditing, licensing, punitive, compensatory, corrective, preventive, developmental, research, academic,

commercial, industrial, civil, criminal, administrative, international, cross-border, multilateral, bilateral, regional, and global components, are the exclusive, absolute, and inalienable property of the author, Dr. Mohamed Kamal Arafa Elrakhawi. Any unauthorized use, exploitation, application, derivation, modification, translation, publication, distribution, integration, reproduction, import, export, transfer, or circulation constitutes a clear violation and a legal, criminal, civil, administrative, and international offense warranting maximum penalties, compensations, prohibitions, seizures, destructions, and immediate, comprehensive, international legal prosecution.

This declaration is issued as a legal, technical, administrative, financial, cognitive, ethical, sovereign, rights-based, standard, regulatory, enforcement, compensatory, punitive, corrective, preventive, developmental, research, academic, commercial, industrial, civil, criminal, administrative, international, cross-border, multilateral, bilateral, regional, global, and institutional document. It constitutes an integral, inseparable, unrevocable, unmodifiable, unreplacable, uncopyable, untranslatable, unpublishable, and undistributable part of the Protocol, and shall not be separated from it, revoked, modified, replaced, copied, translated, published, distributed, merged, derived, modified, developed, updated, upgraded, or improved without prior written, signed, and officially documented permission from the author, Dr. Mohamed Kamal Arafa Elrakhawi.

Author: Dr. Mohamed Kamal Arafa Elrakhawi. All rights fully reserved.