الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة الشهيد الشيخ العربي التبسي –تبسة-
كلية الحقوق والعلوم السياسية
مخبر الدراسات الاستراتيجية و التنمية في الوطن العربي

"ينظم الملتقى الوطني الحضوري /عن بعد ، الموسوم بـ:

تحديات الامن السيبراني في عصر الذكاء الاصطناعي

-علاقة تأثر وتأثير

يوم 30 نوفمبر 2025

المشرف العام للملتقى:

الرئيس الشرفي للملتقى : أ.د. / قواسمية عبد الكريم رئيس الجامعة

المشرف العام للملتقى الوطني

عميد الكلية الدكتور مخلوف طارق

رئيس الملتقى

الدكتورة شعبان لامية

رئيس اللجنة العلمية للملتقى

الأستاذة الدكتورة بن طيبة صونية

رئيس اللجنة التنظيمية للملتقى

الأستاذة خمايسية حفيظة

Shot on POWER PDF
Scanné avec CamScanner

برنامج الملتقى

الجلسة الافتتاحية

انطلاق أشغال الملتقى: 9:00
استقبال الضيوف والمتدخلين
تلاوة آيات من القرآن الكريم
النشيد الوطني
كلمة الأستاذ الدكتور مخلوف طارق عميد كلية الحقوق والعلوم السياسية
كلمة الأستاذ الدكتور البار أمين مدير مخبر الدراسات الإستراتيجية والتنمية في الوطن العربي
كلمة رئيس الملتقى الدكتورة شعبان لامية
كلمة رئيس اللجنة التنظيمية الأستاذة حفيظة خمايسية
كلمة الأستاذ المميز قواسمية عبد الكريم مدير الجامعة والإعلان الرسمي عن افتتاح الملتقى
استراحة
مداخلة السيد محافظ الشرطة مصباحي لزهر التحقيق في الجرائم المرتكبة عن طريق الذكاء الاصطناعي في ظل احترام حقوق الانسان
مداخلة الأستاذة الدكتورة سماعلي عواطف و الدكتور جديدي طلال دور التشريع في ضبط وتنظيم استخدام الذكاء الاصطناعي في الجزائر

رابط الجلسة الافتتاحية

https://meet.google.com/ngw-vyyk-kcb

Scanné avec CamScanner

الجلسة الحضورية الرئيسية . المدرج 06

رئيس الجلسة: أ.د. ثابت دنيا زاد

الرقم	المتدخل	مؤسسة الانتماء	عنوان المداخلة	التوقيت
01	د/ أحمد الحمزة أ.د/ تسعديت مسيح الدين	جامعة الشهيد الشيخ العربي التبسي –تبسة- المدرسة الوطنية العليا للعلوم السياسية – الجزائر	توظيف تقنيات الذكاء الاصطناعي في حماية القضاء السيبراني دراسة حالة مواقع التواصل الاجتماعي	انطلاق أشغال الجلسة على الساعة 10.30 تمنح 15 دقيقة لكل متدخل
02	د/ حنان رزايقية د/ لحواسنية ياسمين	جامعة الشهيد الشيخ العربي التبسي –تبسة-	أهمية الذكاء الاصطناعي في دعم استراتيجيات تعزيز السيادة السيبرانية	
03	أ.د/ فيصل الوافي	جامعة الشهيد الشيخ العربي التبسي –تبسة-	اليات تصدي الجزائر للجرائم السيبرانية	
04	د/محرز مبروكة	جامعة الشهيد الشيخ العربي التبسي –تبسة-	مكافحة الجريمة المنظمة العابرة للحدود	
05	د/منصوري نورة	جامعة الشهيد الشيخ العربي التبسي –تبسة-	الآليات الوطنية لمواجهة التهديدات السيبرانية في الجزائر في ظل التحديات التكنولوجية الراهنة	
نقاش				

Scanné avec CamScanner

الجلسة الحضورية الأولى: القاعة 23 ج

رئيس الجلسة: أ.د. قادري مليكة

الرقم	المتدخل	مؤسسة الانتماء	عنوان المداخلة	التوقيت
01	د/ دبيلي كمال	جامعة الشهيد الشيخ العربي التبسي –تبسة	تطور التهديدات السيبرانية في ظل الذكاء الاصطناعي	انطلاق أشغال الجلسة على الساعة 10.30 ـــــــ تمنح 15 دقيقة لكل متدخل
02	أ/عباد أمير	جامعة الشهيد الشيخ العربي التبسي –تبسة	تطور مفهوم الأمن وتأثره بالتطور التكنولوجي خصوصا في المجال الالكتروني الرقمي	
03	د/بودبار نوال د/ بودبار فوزي	جامعة الشهيد الشيخ العربي التبسي –تبسة	الذكاء الاصطناعي والأمن السيبراني "المدلول والتحديات"	
04	أ.د/ بومعزة نبيلة	جامعة الشهيد الشيخ العربي التبسي –تبسة	مخاطر الذكاء الإصطناعي على الخصوصية والأمن الشخصي	
05	د/ لحمر نعيمة	جامعة الشهيد الشيخ العربي التبسي –تبسة	توظيف الذكاء الاصطناعي في تعزيز الأمن السيبراني	
06	أ.د/ملاك وردة	جامعة الشهيد الشيخ العربي التبسي –تبسة	الذكاء الاصطناعي ومدى تأثيره في تحقيق الأمن السيبراني	
07	د/ معيفي محمد	جامعة الشهيد الشيخ العربي التبسي –تبسة	الذكاء الاصطناعي بين دعم الأمن السيبراني وتهديده دراسة قانونية على ضوء التشريع الجزائري	
08	أ.د./أجعود سعاد أ. د/ ثابت دنيا زاد	جامعة الشهيد الشيخ العربي التبسي –تبسة	آثار الذكاء الاصطناعي على الأمن السيبراني	
09	د/ رقية بلقاسمي	جامعة الشهيد الشيخ العربي التبسي –تبسة	دور الذكاء الاصطناعي في التنبؤ بالهجمات السيبرانية وتحسين الاستجابة الأمنية	
10	د/الحمزة بلال زغلامي حسيبة	جامعة قسنطينة 02 جامعة الشهيد الشيخ العربي التبسي –تبسة	الثقافة الرقمية والأمن السيبراني لدى الطلبة **دراسة سوسيولوجية لتمثلات المخاطر الإلكترونية**	
11	ط.د/ نسيمة العلمي	جامعة الشهيد الشيخ العربي التبسي –تبسة	الإطار القانوني والمؤسساتي الجزائري لمواجهة التهديدات السيبرانية	
12	د/ خذيري حنان	جامعة الشهيد الشيخ العربي التبسي- تبسة-	الاتجار بالبشر والفضاء الإلكتروني رهانات المكافحة في البيئة الرقمية	
	د /سعايدية حورية	جامعة الشهيد الشيخ العربي التبسي- تبسة	مكافحة جريمة الاتجار بالبشر في العصر الرقمي– إشكالات قانونية وتحديات عملية–	

Shot on POWER P55

Scanné avec CamScanner

13	[illegible]رق لخضر	جامعة صفاقس – تونس-	الذكاء الاصطناعي والأمن السيبراني سياسات واستراتيجيات على المستوى الدولي	
نقاش				

Scanné avec CamScanner

الجلسة الحضورية الثانية القاعة 24 ج

رئيس الجلسة: د. شليخر هاجر

الرقم	المتدخل	مؤسسة الانتماء	عنوان المداخلة	التوقيت
01	د/حملة عبر الرحمان	جامعة الشهيد الشيخ العربي التبسي –تبسة	الدليل الرقمي في الجرائم السيبرانية	انطلاق أشغال الجلسة على الساعة 10.30 ـــــــــ تمنح 15 دقيقة لكل متدخل
02	د/ صبرينة بلغيث	جامعة الشهيد الشيخ العربي التبسي –تبسة	الأمن السيبراني وتحديات التوجه نحو الحوكمة الإلكترونية	
03	د/ عبير بعقيقي د/ منصر نصر الدين	جامعة الشهيد الشيخ العربي التبسي –تبسة	تحقيق الأمن السيبراني على ضوء اتفاقية الأمم المتحدة لمكافحة الجرائم السيبرانية لسنة 2024	
04	د/ مريم عثمانية د/ زايدي حميدة	جامعة الشهيد الشيخ العربي التبسي –تبسة	الوكالة الوطنية لأمن نظم المعلومات (ANSSI) ركيزة الإستراتيجية الوطنية للأمن السيبراني في الجزائر	
05	د/ لامية شعبان أ.د/ نبيلة كردي	جامعة الشهيد الشيخ العربي التبسي –تبسة	التشريع الجزائري وجرائم الذكاء الاصطناعي	
06	د/ دريدي محمود د/ عمر سعداوي	جامعة الشهيد الشيخ العربي التبسي –تبسة جامعة يومرداس	دور الذكاء الاصطناعي في تحول موازين القوى في النظام الدولي	
07	د/ فضل عائشة	جامعة التكوين المتواصل- تبسة	حماية المعطيات الشخصية بين ذكاء الخوارزميات وسيادة الأمن السيبراني	
08	د/ تقي الدين مباركية ط.د. سعاد مباركية	جامعة الشهيد الشيخ العربي التبسي –تبسة جامعة ام البواقي	الذكاء الاصطناعي في الأمن القضائي البريطاني: دراسة تقييمية لتطبيقات التعرف الوجهي وتقييم المخاطر الجنائية	
09	د/بشارة عبد المالك د/ خالدي خديجة	جامعة الشهيد الشيخ العربي التبسي –تبسة	الاطار القانوني لمكافحة الجرائم السبرانية في التشريع الجزائري	
10	د/ فرحي ربيعية أ.د/مقران ريمة	جامعة الشهيد الشيخ العربي التبسي –تبسة	الذكاء الاصطناعي سلاح الجريمة وآلية التصدي – قراءة في تحديات تحقيق الأمن السيبراني	
11	د/خالدي شريفة	جامعة الشهيد الشيخ العربي التبسي –تبسة	اجراءات التحري في الجرائم السبرانية على ضوء القانون 14/25	
12	د/بوعزيز عبد الوهاب أ.د/ بوراس منير	جامعة باجي مختار – عنابة جامعة الشهيد الشيخ العربي التبسي –تبسة	الهجمات السيبرانية الذكية: المفهوم والانواع "	

Scanné avec CamScanner

13	[illegible] عماد [illegible] شنيخر أمينة	جامعة صفاقس – تونس	الذكاء الاصطناعي كأداة لتطوير سياسات الأمن السيبراني	
نقاش				

Shot on POWER P55
20:04
Scanné avec CamScanner

الجلسة الحضورية: الثالثة القاعة 25 ج

رئيس الجلسة: اجعود سعاد

الرقم	المتدخل	مؤسسة الانتماء	عنوان المداخلة	التوقيت
01	أ.د/ عثماني عز الدين د/ خذيري عفاف	جامعة الشهيد الشيخ العربي التبسي –تبسة	جرائم الاعتداء على الحياة الخاصة عبر الوسائط الرقمية	انطلاق أشغال الجلسة على الساعة 10.30 ـــــــ تمنح 15 دقيقة لكل متدخل
02	أ.د/ مخلوف طارق	جامعة الشهيد الشيخ العربي التبسي –تبسة	**الذكاء الاصطناعي والامن السبراني – المفاهيم الاساسية والتحديات المعاصرة-**	
03	د/بوجراف فهيم أ.د/ جبيري ياسين	جامعة الشهيد الشيخ العربي التبسي –تبسة	المخاطر السيبرانية والأمن القانوني في المجتمع الرقمي	
04	د/ بورزق علاء الدين	جامعة التكوين المتواصل –تبسة	دور الذكاء الاصطناعي في تعزيز استدامة الأمن السيبراني للمؤسسات الحيوية في الجزائر- مقاربة تشريعية وتقنية-	
05	د/ لبيوض أسماء	جامعة الشهيد الشيخ العربي التبسي –تبسة	التحصين ضد الهجمات الذكية: تحليل تحديات الأمن السيبراني المعتمد على الذكاء الاصطناعي	
06	ط.د/ نجود طراد	جامعة الشهيد الشيخ العربي التبسي –تبسة	الذكاء الاصطناعي كآلية استراتيجية لتعزيز الأمن السيبراني	
07	د/ هاني غنية	جامعة الشهيد الشيخ العربي التبسي –تبسة	متطلبات الأمن الوطني في عصر الذكاء الاصطناعي: الفرص والتحديات	
08	د/ موسى عائشة	جامعة الشهيد الشيخ العربي التبسي –تبسة	الاتفاقيات الدولية لمكافحة الجرائم السبرانية	
09	د/ سماح سهايلية أ.د/ سمير كيم	جامعة الشهيد الشيخ العربي التبسي –تبسة	مستقبل الأمن: كيف يعيد الذكاء الاصطناعي تشكيل قواعد اللعبة في الفضاء السيبراني؟	
10	د/شيباني إيناس أ.د/قادري مليكة	جامعة الشهيد الشيخ العربي التبسي –تبسة	دور التقنيات الذكية في كشف الهجمات السيبرانية المتقدمة	
11	د/بولعراس مختار د/ نور الدين بريك	جامعة الشهيد الشيخ العربي التبسي –تبسة	آليات الاستراتيجية الوطنية لضبط استغلال مجالات الذكاء الإصطناعي وفق متطلبات الامن السبراني	
12	أ/خمايسية حفيظة ط.د. بولخوة ابتسام	جامعة الشهيد الشيخ العربي التبسي –تبسة	الإطار القانوني للأمن السيبراني في مواجهة تحديات الذكاء الإصطناعي: بين القصور التشريعي والمتطلبات المستجدة	
نقاش				

Scanné avec CamScanner

رابط الجلسة الأولى عن بعد: https://meet.google.com/ibv-zvch-gnw

رئيس الجلسة: د/ حنان رزايقية

الرقم	المتدخل	مؤسسة الانتماء	عنوان المداخلة	التوقيت
01	د/ بوبكر صبرينة	جامعة سوق أهراس	ديناميكيات العلاقة بين الذكاء الاصطناعي والأمن السيبراني	انطلاق أشغال الجلسة على الساعة 10.30 تمنح 10 دقائق لكل متدخل
02	ط.د/ يسرى جواد أ.د/ زواتيني عبد العزيز	جامعة أكلي محند أولحاج- البويرة-	الذكاء الاصطناعي بين سلطة الحماية ومخاطر الاختراق- جدلية الأمن السيبراني في العصر الرقمي	
03	د/ فرد حياة د/ أم الخير عيشون	جامعة أكلي محند أولحاج- البويرة-	الأمن السيبراني في عصر الذكاء الاصطناعي دراسة في العلاقة والتأثر	
04	ط.د/حورية بوعبد الله	جامعة الجزائر 03	تأثيرات الذكاء الاصطناعي على الأمن السيبراني: بين التعزيز والتهديد	
05	د/فخر الدين مهوبي د/ وليد صيقي	جامعةمحمد خيضر- بسكرة-	إدارة المفارقة الأمنية: توظيف الذكاء الاصطناعي لتعزيز الحماية السيبرانيةومواجهة تهديداته المتطورة	
06	د/ منصور نورة د/ خالدي زينب	جامعة ميلة جامعة الشهيد الشيخ العربي التبسي – تبسة-	الآليات القانونية لمكافحة جريمة الإتلاف العمدي للمعطيات في التشريع الجزائري	
07	د/ محمد مرسلي	جامعة غرداية	المسؤولية القانونية عن الجرائم السيبرانية الناتجة عن استخدام أنظمة الذكاء الاصطناعي -نحو نموذج تشريعي جزائري -	
نقاش				

Shot on POWER P55

Scanné avec CamScanner

رابط الجلسة الثانية عن بعد https://meet.google.com/qjq-ktyw-jrh

رئيس الجلسة: د/سماح سهايلية

الرقم	المتدخل	مؤسسة الانتماء	عنوان المداخلة	التوقيت
01	أ.د./هدى عزاز د./هاجر شنيخر	جامعة الشهيد الشيخ العربي التبسي – تبسة	الأمن السيبراني والذكاء الاصطناعي بين التطور التكنولوجي والتنظيم القانوني	انطلاق أشغال الجلسة على الساعة 10.30 تمنح 10 دقائق لكل متدخل
02	ط.د/ بن ذيب تقوى ط/ غنيات عامر	جامعة الشهيد الشيخ العربي التبسي – تبسة	فعالية المنظومة القانونية الجزائرية في مكافحة الجريمة السيبرانية	
03	أ.د/أمين البار أ.د/ دني إيمان	جامعة الشهيد الشيخ العربي التبسي – تبسة جامعة محمد خيضر – بسكرة	التعاون الدولي في مكافحة التهديدات السيبرانية في عصر الذكاء الاصطناعي و التحول الرقمي	
04	د/ بسكري منير	جامعة بسكرة	التعاون الدولي وأثره في تعزيز الأمن السيبراني في ظل تطور تقنيات الذكاء الاصطناعي	
05	د/طاجين نسيمة ط/د.كعبش عبد الوهاب	جامعة برج بوعريريج جامعة الجزائر 01	الدفاع السيبراني كامتداد للأحلاف العسكرية حلف شمال الاطلسي - الناتو - نموذجًا	
06	أ/ ميموني سليمة	المركز الجامعي الشهيد سي الحواس بريكة	أثر الذكاء الاصطناعي على تعزيز الأمن السيبراني	
07	د/ رقية دهينة د/ جلال قصار الليل	جامعة باجي مختار عنابة	رؤية تقييمية لاستخدامات الذكاء الاصطناعي في المجال الأمني + دراسة حالات حقيقية وتجارب دولية	
نقاش				

Scanné avec CamScanner

رابط الجلسة الثالثة عن بعد https://meet.google.com/vgx-ogrr-ppx

رئيس الجلسة: د/صبرينة بلغيث

الرقم	المتدخل	مؤسسة الانتماء	عنوان المداخلة	التوقيت
01	ط.د/ قادري حفيظة أ/ العربي شحط أمينة	جامعة وهران 02 جامعة الجزائر 01	الاستراتيجية المنتهجة من طرف الجزائر في مجال تعزيز الأمن السيبراني "رهانات وتحديات"	انطلاق أشغال الجلسة على الساعة 10.30 ـــــــ تمنح 10 دقائق لكل متدخل
02	د/ بوعكاز نسرين د/ نويرة نوال	جامعة يحي فارس-المدية جامعة الشهيد الشيخ العربي التبسي- تبسة-	دور السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي في تحقيق الأمن السيبراني	
03	د/ شتوح زوهير	جامعة باجي مختار –عنابة-	حماية النظام العام الإلكتروني: فرص وتحديات الذكاء الاصطناعي	
04	د/ باسل سهام	جامعة سكيكدة	المسؤولية عن الأضرار الناتجة عن استخدام الأنظمة الذكية في الفضاء السيبراني	
05	أ.د/بخوش هشام	جامعة محمد الشريف مساعدية-سوق أهراس	دور الامن السبراني في حماية المعطيات والبيانات ذات الطابع الشخصي	
06	ط.د/ بلحسن عبد المالك	جامعة محمد الشريف مساعدية- سوق أهراس	الجهود الدولية لتحقيق الأمن السيبراني في عصر تكنولوجيا المعلومات والذكاء الاصطناعي	
07	د/ عبد الحي محمد ط.د/ قواسمية عبد اللطيف	جامعة خنشلة جامعة الشهيد الشيخ العربي التبسي- تبسة -	جهود وآليات التعاون الدولي لتحقيق الأمن السيبراني في عصر الذكاء الاصطناعي	
08	ط.د// زياني أميمة د/ خربيش زوهير	جامعة تيارت	أثر الذكاء الاصطناعي على تطوير الهجمات السبرانية الذكية واستراتيجيات مواجهتها – قراءة سوسيو تنظيمية -	
نقاش				

Scanné avec CamScanner

الجلسة الختامية

قراءة توصيات الملتقى

الإعلان عن اختتام فعاليات الملتقى الوطني

رابط الجلسة الختامية

https://meet.google.com/ngw-vyyk-kc

Scanné avec CamScanner

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة الشهيد الشيخ العربي التبسي

تبسة



كلية الحقوق والعلوم السياسية

مخبر الدراسات الاستراتيجية و التنمية في الوطن العربي

"ينظم الملتقى الوطني الحضوري /عن بعد، الموسوم بـ:

تحديات الامن السيبراني في عصر الذكاء الاصطناعي

-علاقة تأثر وتأثير-

30 نوفمبر 2025

الرئيس الشرفي: أ.د. / قواسمية عبد الكريم رئيس الجامعة

المشرف العام للملتقى الوطني: عميد الكلية الدكتور

مخلوف طارق

رئيس الملتقى الوطني: الدكتورة شعبان لامية

رئيسة اللجنة العلمية للملتقى: أ.د بن طية صونية

رئيس اللجنة التنظيمية: أ.حمايسية حفيظة

ديباجة الملتقى:

يمثل الامن السيبراني في عصر تكنولوجيا المعلومات الذرع الرقمي الذي يحمي عالمنا المتصل بالانترنت حيث تتداخل حياتنا مع الشبكة العنكبوتية ليصبح الامن السيبراني امرا ضروريا للحفاظ على الخصوصية وامن البيانات خاصة مع تطور الذكاء الاصطناعي الذي يمكن ان يساهم في الكشف المبكر عن التصرفات المشبوهة والتهديدات المحتملة في الفضاء السيبراني وبالتالي رفع امكانيات مواجهة هذه التهديدات .

الا ان ذلك لا ينفي ان دمج الذكاء الاصطناعي في الامن السيبراني يخلق تحديات عديدة كإساءة الاستخدام المحتملة لهذا الاخير، والذي يمكن ان يساهم في تعزيز قدرات الهجمات والتهديدات السيبرانية وجعلها اكثر تطورا وتعقيدا في الوقت نفسه.

وعليه يمكن القول انه في الوقت الذي يسهم فيه الذكاء الاصطناعي في الحماية والرصد المبكر للتهديدات السيبرانية فانه يستغل ايضا لتنفيذ هجمات سيبرانية اكثر تطورا وذكاءا يصعب اكتشافها بالوسائل التقليدية الامر الذي يطرح كيفية تحقيق التوازن بين توظيف الذكاء الاصطناعي لخدمة الامن السيبراني من جهة، والحد من مخاطره من جهة اخرى.

-وفي هذا الصدد تسعى الجزائر كغيرها من الدول الى مواجهة هذه التهديدات الامنية في صورتها المستحدثة محاولة خلق اليات سواء على الصعيد التقني او التشريعي او المؤسساتي الامر الذي يطرح مسألة مدى موائمة القواعد القانونية مع تطبيقات الذكاء الاصطناعي وما يستتبع ذلك من ضبط لقواعد التجريم والعقاب وتقرير قواعد إجرائية خاصة.

وعليه يصبح البحث في هذا الموضوع ضرورة ملحة تفرضها التطورات التكنولوجية و على رأسها الذكاء الاصطناعي الذي اصبح المحرك الاساسي لعمل الاجهزة الامنية للدولة .

إشكالية الملتقى.

وعليه تبلور إشكالية الملتقى على النحو التالي: الى أي مدى يمكن تحقيق الامن السيبراني في ظل تحديات عصر التكنولوجيا والذكاء الاصطناعي ؟

أهداف الملتقى:

يسعى هذا الملتقى إلى تحقيق جملة من الأهداف أهمها:

- – تحديد مفهوم الامن السيبراني
- -تحديد المفاهيم المتعلقة بالذكاء الاصطناعي ومجالات استخدامه.
- – التعرف على اهم تطبيقات الذكاء الاصطناعي في المجال الامني خصوصا ما تعلق بحماية الخصوصية والبيانات الشخصية .
- مناقشة الجوانب التشريعية والتنظيمية الخاصة بالامن السيبراني والذكاء الاصطناعي خاصة فيما يتعلق بتحديد المسؤولية الجزائية والبحث في مدى كفاية الاطر القانونية لمواجهة التهديدات الجديدة .
- محاولة تقييم كفاءة وكفاية الجهود المبذولة لتحقيق الامن السيبراني
- التوصل الى نتائج قد تسهم في تشخيص أوجه القصور في التشريعات العقابية – الوطنية والدولية– القائمة واقتراح الحلول المناسبة بما يضمن صون الحقوق في البيئة الافتراضية.
- وبناء على ما تقدم تم تحديد محاور الملتقى وفق ما يلي:

محاور الملتقى:

المحور الأول: الامن السيبراني والذكاء الاصطناعي (المفاهيم والعلاقة و التطور).

المحور الثاني: الذكاء الاصطناعي بين تعزيز الامن السيبراني و تهديده .

المحور الثالث: الاليات الوطنية – تقنية .تشريعية . مؤسساتية– لمواجهة التهديدات السيبرانية في الجزائر في ظل التحديات التكنولوجية الراهنة .

المحور الرابع : الجهود الدولية لتحقيق الامن السيبراني في عصر تكنولوجيا المعلومات والذكاء الاصطناعي .

المحور الخامس : رؤية تقييمية لاستخدامات الذكاء الاصطناعي في المجال الأمني +دراسة حالات حقيقية وتجارب دولية .

Scanné avec CamScanner

اللجنة العلمية للملتقى:

رئيسة اللجنة العلمية: الدكتورة بن طيبة صونية

الأعضـــــاء

أ.د.ثابت دنيا زاد –جامعة –تبسة

أ.د.البار أمون –جامعة تبسة

أ.د.دبي ايمان –جامعة تبسة

د شارني نوال جامعة تبسة

أ.د عثماني عزدين –جامعة تبسة

د.فرحي ربيعة – جامعة تبسة

د.كردي نبيلة – جامعة تبسة

د.حذيري عفاف –جامعة تبسة

د.بلقاسمي رقية–جامعة تبسة

د. بن بوعبد الله منية – جامعة سوق اهراس

د.بوعزيز عبد الوهاب –جامعة عنابة

د.زغلامي حسية –جامعة تبسة

د.وليد صيفي – جامعة بسكرة

د.حاحلي عواطف –جامعة تبسة

د.لحواسنية ياسين –جامعة تبسة

د.كردي نبيلة –جامعة تبسة

د.هاجر شيخر –جامعة تبسة

د.بوعيد عز الدين – جامعة تيارت

د. بلعيد محية –جامعة تبسة

د.منصر نصر الدين – جامعة تبسة

د.دريدي محمود –جامعة تبسة

د.معيفي محمد – جامعة تبسة

د. هاني غنية – جامعة تبسة

د. حذيري حنان– جامعة تبسة

د. سعايدية حورية جامعة تبسة

د. محرز مووكة– جامعة تبسة

د. بوبكر صونية – جامعة سوق اهراس

أ.د. احمود سعاد – جامعة تبسة

أ.د. قادري مليكة – جامعة تبسة

أ.د.كيم سحر – جامعة تبسة

أ.د ملاك وردة – جامعة تبسة

أ.د بوخميس سهيلة –جامعة قالمة

أ.د يومعزة نبيلة –جامعة تبسة

أ.د فوري فهيمة –جامعة باتنة 01

أ.د. لعجال ليلى–جامعة تبسة

د. قحقاح وليد –جامعة تبسة

د. عثمانية كوصر – جامعة خنشلة

د. حديدي طلال –جامعة تبسة

د.خالدي شريفة جامعة تبسة

د. منير بسكري – جامعة بسكرة

د. مقران رتيبة –جامعة تبسة

د. خالدي خديجة –جامعة تبسة

د. –بوجوراف فهيم جامعة تبسة

د.بودبار نوال– جامعة تبسة

د. خوادجية سميحة حنان –قسنطينة1

د. بشارة عبد المالك – جامعة تبسة

د. منصوري نورة – جامعة تبسة

د. موسى عائشة – جامعة تبسة

د. حلة عبد الرحمن – جامعة تبسة

د.فخر الدين مبهولي – جامعة بسكرة

د. احمد الحمزة – جامعة تبسة

د. صالح زمال – جامعة تبسة

د. ماهر بديار – جامعة سوق اهراس

د مزوزي فارس جامعة الطارف

رئيسة اللجنة التنظيمية: الاستاذة حمايسية حفيظة

أعضاء اللجنة التنظيمية:

أ.سعدي عبد المجيـــد / أ.مير عباد / أ.بن حدة باديس /أ.حاجي محمد/ ط.د. ثابت مريم / ط.د شيخر دنيا / ط/د بوشكيوة ياسين شارف هشام / يحياوي محمد رستم / بوخالفة وليـة / معلم لطيفة/ فارح منى / بوخضرة نعيم / دريس فايزة / بوعلاق أمينة / بوعلاق حياة / مهدي وهيبة / فرحات أمير بحي / فارح أمال

شروط المشاركة:

– المشاركة مفتوحة للاساتذة الجامعيين وطلبة الدكتوراه والباحثين في القانون

– أن يتميز البحث بالتأصيل والحداثة، وأن لا يكون متصلا بمداخلة أو مقال قد سبقت المشاركة به في فعاليات اخرى

– الالتزام بمحاور الملتقى واهدافه المحددة .

– ارفاق الملخص بالعربية بملخص مترجم الى اللغة الانجليزية

– أن يتم التهميش وايراد المصادر والمراجع آخر البحث وبشكل كامل .

اللغة العربية: خط: Sakkal majalla حجم 16 للمتن وحجم 12 للهوامش. اما اللغة الأجنبية: خط: Time New Roman حجم 12 للمتن وحجم 10 للهوامش.

– يتراوح عدد الصفحات بين 10 و 20 صفحة باحتساب المراجع والملاحق

تواريخ مهمة:

آخر أجل لإرسال الملخصات: 12 نوفمبر 2025.

الرد على الملخصات المقبولة: 14 نوفمبر 2025

آخر أجل لإرسال المداخلات كاملة: 24 نوفمبر 2025

استمارة المشاركة

اسم المشارك ولقبه: .....

الوظيفة : .....

الرتبة العلمية : .....

المؤسسة المستخدمة: .....

- العنوان: .....

- الهاتف : .....

- البريد الالكتروني : .....

المحور : .....

عنوان المداخلة : .....

.....

الملخص

.....

.....

.....

.....

.....

.....

الكلمات المفتاحية : .....

.....

.....

.....

Scanné avec CamScanner

اثار الذكاء الاصطناعي على الأمن السيبراني

سعاد اجعود **دنيا زاد ثابت**

جامعة الشهيد الشيخ العربي التبسي – تبسة - **جامعة الشهيد الشيخ العربي التبسي – تبسة**

souad.ajaoud@univ-tebessa.dz **douniazed tabet@univ-tebessa.dz**

الملخـــص

يشكل الذكاء الاصطناعي تحولًا جذريًا في مجال الأمن السيبراني، حيث يعزز الدفاعات من خلال التحليل الذكي للبيانات والكشف المبكر عن الهجمات، ويساعد على التنبؤ بالتهديدات والتعامل معها بسرعة وفعالية. وفي الوقت نفسه، يمكن استغلاله من قبل المهاجمين لتطوير هجمات متقدمة وبرمجيات خبيثة ذكية واستغلال الثغرات بشكل أكثر تطورًا. كما يتيح الذكاء الاصطناعي مراقبة الأنماط المشبوهة وتحليل السلوكيات غير الطبيعية في الشبكات، مما يقلل من المخاطر ويزيد من قدرة المؤسسات على حماية بياناتها. ومع ذلك، يثير استخدامه تحديات قانونية وأخلاقية تتعلق بالخصوصية والمسؤولية عن القرارات التلقائية، مما يجعل تطوير أطر تنظيمية وتقنية متكاملة أمرًا ضروريًا.

الكلمات المفتاحية: الذكاء الاصطناعي / الأمن السيبراني / الهجمات المتقدمة / الكشف المبكر عن التهديدات الخصوصية وحماية البيانات.

Abstract

Artificial intelligence (AI) represents a transformative force in cybersecurity, enhancing defenses through intelligent data analysis and early threat detection, while enabling the prediction and rapid response to potential attacks. At the same time, it can be exploited by attackers to develop advanced attacks, intelligent malware, and sophisticated exploitation of vulnerabilities. AI also allows monitoring of suspicious patterns and analysis of abnormal network behaviors, reducing risks and strengthening organizations' data protection capabilities. However, its use raises legal and ethical challenges regarding privacy and responsibility for automated decisions, making the development of comprehensive regulatory and technical frameworks essential.

Keywords: Artificial Intelligence (AI) – Cybersecurity – Advanced attacks – Intelligent data analysis – Early

التشريع الجزائـــري وجرائـــــم الذكـــــاء الاصطنـــاعي

شعبان لامية
جامعة الشهيد الشيخ العربي التبسي – تبسة
lamia.chaaben@univ-tebessa.dz

كردي نبيلة
جامعة الشهيد الشيخ العربي التبسي – تبسة
nabila .kardi@univ-tebessa.dz

الملخـــــص

اولي التشريع الجزائري أهمية متزايدة لمواجهة الجرائم المرتبطة باستخدام تقنيات الذكاء الاصطناعي، رغم حداثة هذا النوع من الجرائم وتسارع تطوره التقني. فبالرغم من عدم وجود نصوص قانونية خاصة تُجرّم صراحة جرائم الذكاء الاصطناعي، إلا أن المشرّع الجزائري يعتمد على القواعد العامة الواردة في قانون العقوبات، إلى جانب قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، لتجريم الأفعال التي تُرتكب باستخدام هذه التقنيات، متى مست بأمن الدولة أو النظام العام أو حقوق الأفراد.

ويُظهر هذا التوجه سعي المشرّع إلى التكييف القانوني للجرائم المستحدثة وفق النصوص القائمة، مع ضرورة تطوير الإطار التشريعي مستقبلاً لمواكبة المخاطر الخاصة التي يطرحها الذكاء الاصطناعي، لا سيما ما يتعلق بالمسؤولية الجنائية، وحماية البيانات الشخصية، ومنع إساءة استخدام الأنظمة الذكية في ارتكاب الجرائم السيبرانية

الكلمات المفتاحية : جرائم الذكاء الاصطناعي، التشريع الجزائري، الجرائم السيبرانية، المسؤولية الجنائية، حماية البيانات الشخصية، الجرائم المستحدثة، تكنولوجيات الإعلام والاتصال.

Abstract

The Algerian legislator has shown increasing interest in addressing crimes related to the use of artificial intelligence, despite the novelty of this type of crime and the rapid pace of technological development. Although there are no specific legal provisions that explicitly criminalize artificial intelligence–related crimes, Algerian legislation relies on the general rules set forth in the Penal Code, as well as the Law on the Prevention and Suppression of Offenses Related to Information and Communication Technologies, to criminalize acts committed through these technologies whenever they threaten state security, public order, or individual rights.

This approach reflects the legislator's effort to adapt existing legal frameworks to emerging crimes, while highlighting the need to further develop the legislative system to keep pace with

the specific risks posed by artificial intelligence, particularly with regard to criminal liability, personal data protection, and the prevention of misuse of intelligent systems in the commission of cyber crimes

Key words Artificial Intelligence Crimes, Algerian Legislation, Cybercrime, Criminal Liability, Data Protection, Emerging Crimes, Information and Communication Technologies (ICT)

الذكاء الاصطناعي سلاح الجريمة وألية التصدي – قراءة في تحديات تحقيق الامن السيبراني-

د/ ربيعة فرحي
جامعة الشهيد الشيخ العربي التبسي-تبسة
rabiaa.ferhi@univ-tebessa.dz

مقران ريمة
جامعة الشهيد الشيخ العربي التبسي-تبسة
rima.mokrane@univ-tebessa.dz

الملخــص

تتناول هذه المداخلة استكشاف دور الذكاء الاصطناعي في تعزيز قدرات الجريمة الحديثة، من خلال استعراض أبرز أشكال الهجمات المعاصرة التي استغلت التقنيات الذكية، مثل الاحتيال الإلكتروني والاختراقات الرقمية، والتزييف العميق (Deepfake). كما تُسلط المداخلة الضوء على المخاطر الناشئة عن الاستخدام غير المشروع للذكاء الاصطناعي، وتأثيرها على الأمن الرقمي والمجتمعي.

وبالموازاة تقدم المداخلة قراءة نقدية للآليات القانونية والتقنية المتاحة للتصدي لهذه الهجمات، مع التأكيد على أهمية الجمع بين التشريعات الحديثة، التوعية المجتمعية، والتقنيات المضادة لضمان حماية الأفراد والمؤسسات. وتهدف المداخلة إلى إبراز التحديات الأمنية المعاصرة، مع تقديم توصيات عملية لتعزيز القدرة الوقائية والاستجابة السريعة للهجمات الرقمية المدعومة بالذكاء الاصطناعي. ونتناول من خلالها:

1- نماذج هجمات معاصرة باستخدام الذكاء الاصطناعي

2- الية التصدي للهجمات بواسطة الذكاء الاصطناعي وتحديات تحقيق الامن السيبراني

الكلمات المفتاحية: الذكاء الاصطناعي، الجريمة الرقمية، الأمن السيبراني، الهجمات المعاصرة، آليات التصدي

Abstract

This presentation explores the role of artificial intelligence in enhancing modern crime capabilities, reviewing the most prominent forms of contemporary attacks that have exploited smart technologies, such as cyber fraud, digital breaches, and deepfakes. It also highlights the risks arising from the illegal use of artificial intelligence and its impact on digital and community security. At the same time, the presentation offers a critical review of the legal and technical mechanisms available to counter these attacks, emphasizing the importance of combining modern legislation, community awareness, and counter-technologies to ensure the protection of individuals and institutions. The presentation aims to highlight contemporary security

challenges and provide practical recommendations to enhance preventive capabilities and rapid response to AI-powered digital attacks. We will address the following topics:

1- Contemporary models of attacks using artificial intelligence

2- Mechanisms for countering attacks using artificial intelligence and the challenges of achieving cybersecurity

Keywords: Artificial intelligence, digital crime, cybersecurity, contemporary attacks, countermeasures.

أليات الاستراتيجية الوطنية لضبط استغلال مجالات الذكاءالاصطناعي وفق متطلبات الامن السيبراني

نورالدين بريك
جامعة الشهيد الشيخ العربي التبسي.تبسة
noureddine.brik@univ-tebessa.dz

مختاربولعراس
جامعة الشهيد الشيخ العربي التبسي.تبسة
Mokhtar.boulaares@univ-tebessa.dz

الملخـــص

ضمانا لتجسيد متطلبات الأمن السبراني اثناء استغلال المنصات الرقمية المرتبطة بقاعدةالبيانات المسيرة لما يعرف بالذكاء الإصطناعي، سعى المشرع الجزائري إلى وضع إطار قانوني متدرج يضبط الولوج إلى هذا المجال، وهذا بغرض تحقيق التوازن بين فكرة الحريةوحماية الحق، حيث تقوم هذه العملية القانونية على مجموعةمن الأطر تظهر ضمن متطلبات الاستراتيجية الوطنية لتفعيل آليات الأمن السيبيراني، والتي تتبنى غاية جوهرية تتجسد في فكرة حماية الفضاء الرقمي من أجل تعزيز الثقة في الخدمات الالكترونية، فتم استحداث نصوص قانونية تتعلق بالمعوماتيةو المعطيات الشخصيةوكيفية حمايتها ومكافحة الجرائم المرتبطة بها.، كماتم استحداث مجموعة من الهيئات الوطنية من اجل تفعيل وبلورة هذه النصوص مع متطلبات التطور التكنولوجي وتأثيره على مختلف المجالات. أين تم إعتماد مجموعة من المعايير لتحقيق السلامة الرقمية وفق نظم التشفير وتحصين الشبكات وتفعيل آليات الكشف المبكر عن الهجمات والرقابة الاستباقية والاستجابة للتعامل مع الحوادث السيبيرانية.

الكلمات المفتاحية: الامن السيبيراني، الذكاء الاصطناعي، الأمن المعلوماتي،.

Abstract:

To ensure that cybersecurity requirements are met when using digital platforms linked to databases powered by artificial intelligence, Algerian lawmakers have sought to establish a progressive legal framework governing access to this field. The aim is to strike a balance between freedom and the protection of rights. This legal process is based on a set of frameworks that appear within the requirements of the national strategy for activating cybersecurity mechanisms, which adopts the fundamental goal of protecting the digital space in order to enhance confidence in electronic services. Legal texts have been developed relating to information technology and personal data, how to protect them and combat related crimes. A group of national bodies has also been established to activate and develop these texts in line with technological developments and their impact on various fields.

A set of standards has been adopted to achieve digital security in accordance with encryption systems, network fortification, and the implementation of mechanisms for early detection of attacks, proactive monitoring, and response to cyber incidents.

Keywords: cyber security, artificial intelligence, information security.

تأثيرات الذكاء الاصطناعي على الأمن السيبراني: بين التعزيز والتهديد

ط د/ حورية بوعبد الله

جامعة الجزائر3

houriaaddouche@gmail.com

الملخـــص

يشهد مجال الأمن السيبراني تحولًا جذريًا بفعل تطور تقنيات الذكاء الاصطناعي، التي باتت تلعب دورًا مزدوجًا يتراوح بين تعزيز الحماية الرقمية وخلق تهديدات جديدة ومعقدة. تهدف هذه الدراسة إلى تحليل التأثيرات المتباينة للذكاء الاصطناعي على الأمن السيبراني، من خلال استعراض آليات التمكين التي توفرها هذه التقنيات، مقابل التحديات الأمنية التي تنجم عن استخدامها غير المشروع. من جهة، يساهم الذكاء الاصطناعي في تحسين قدرات الكشف المبكر عن الهجمات السيبرانية، وتطوير أنظمة دفاعية ذكية قادرة على التعلم والتكيف مع التهديدات المتغيرة. كما يعزز من فعالية الاستجابة للحوادث الأمنية ويقلل من زمن التعافي. ومن جهة أخرى، يتيح الذكاء الاصطناعي للمهاجمين تطوير برمجيات خبيثة أكثر تطورًا، وتنفيذ هجمات دقيقة يصعب رصدها بالوسائل التقليدية، فضلًا عن استخدام تقنيات التزييف العميق في اختراق الأنظمة وخداع المستخدمين.

الكلمات المفتاحية: الذكاء الاصطناعي، الأمن السيبراني، التهديدات الرقمية

Abstract

The field of cybersecurity is undergoing a profound transformation driven by the rapid advancement of artificial intelligence (AI) technologies, which now play a dual role ranging from strengthening digital protection to generating new and complex threats. This study aims to analyze the contrasting impacts of AI on cybersecurity by examining the enabling mechanisms these technologies provide, alongside the security challenges arising from their illicit use.On the one hand, AI contributes to enhancing early detection capabilities against cyberattacks and to the development of intelligent defense systems capable of learning and adapting to evolving threats. It also improves the effectiveness of incident response and reduces recovery time. On the other hand, AI enables attackers to design more sophisticated malware and to carry out precise attacks that are difficult to detect using traditional methods, in addition to employing deepfake technologies to infiltrate systems and deceive users.

Keywords: Artificial Intelligence, Cybersecurity, Digital Threats

الاستراتيجية المنتهجة من طرف الجزائر في مجال تعزيز الأمن السيبيراني "رهانات وتحديات".

ط/د. العربي شحط أمينة
جامعة الجزائر1
hafidak32@gmail.com

ط/د. قـــادري حفيظة
جامعة وهران2
larbichahtamina246@ gamil.com

الملخـــــص

يعتبر الامن السيبيراني من الركائز الاساسية في الوقت الراهن الذي يقوم على كل ما هو رقمي وتكنولوجي اذ انه يساهم في حماية الافراد والمؤسسات وكذا الدول من المخاطر التي قد تمس الفضاء الالكتروني وبالحديث عن الدول تعتبر الجزائر من الدول التي تسعى جاهدة من اجل تعزيز امنها السيبيراني عبر انتهاج مجموعة من الاليات والاستراتيجيات. وبطبيعة الحال فاتها في سبيل ذلك تواجه مجموعة من العراقيل فتجعل في ظل مسار تعزيزها لأمنها السيبيراني عائقا بين الفعالية والتحديات .

الكلمات المفتاحية : الامن السيبيراني –استراتيجيات-الجزائر –التحديات .

Abstract :

Here is a precise legal translation of your text into English, maintaining the formal and technical tone suitable for legal or official contexts:Cybersecurity is currently considered one of the fundamental pillars in a time that relies heavily on everything digital and technological, as it contributes to protecting individuals, institutions, and states from risks that may affect the cyber space. Regarding states, Algeria is among the countries that are making significant efforts to enhance its cybersecurity by adopting a set of mechanisms and strategies.
Naturally, in this process, it will inevitably face a range of obstacles that create a barrier between the effectiveness of its cybersecurity enhancement and the challenges encountered.

Keywords : cybersecurity-strategies-Alegria-challenges.

الذكاء الاصطناعي بين سلطة الحماية ومخاطر الاختراق: جدلية الأمن السيبراني في العصر الرقمي

ط د/ يسرى جواد
جامعة آكلي محند أولحاج-البويرة-
y.djouad@univ-bouira.dz

أ.د/ عبد العزيز زواتيني
جامعة آكلي محند أولحاج-البويرة-
a.zouatini@univ-bouira.dz

الملخـــــص

تهدف هذه الدراسة إلى تسليط الضوء على الجدلية المعقدة بين الذكاء الاصطناعي والأمن السيبراني، في ظل التحولات الرقمية المتسارعة التي جعلت من الخوارزميات فعلا رئيسيا في تأمين الفضاءات المعلوماتية من جهة، وفي تهديدها من جهة أخرى، فقد أضحى الذكاء الاصطناعي يستثمر على نطاق واسع في تطوير أنظمة الإنذار المبكر، والكشف الآلي عن الاختراقات، وتحليل البيانات الضخمة لحماية المؤسسات، غير أن نفس القدرات التقنية تستغل في المقابل لابتكار هجمات سيبرانية ذكية قادرة على التكيف والتخفي. ومن هذا المنظور تتناول الدراسة العلاقة المزدوجة التي تربط الذكاء الاصطناعي بالامن السيبراني، بإعتبارها علاقة جدلية بين الحماية والتهديد، الثقة والخطر، السيطرة والحرية. كما تسعى إلى تحليل الانعكاسات الاجتماعية والأخلاقية لهذه الظاهرة على مستوى الأفراد والمؤسسات والمجتمعات، في ظل تصاعد الاعتماد على الانظمة المؤتمتة والبيانات الحساسة. ونستنتج من خلال هذه الورقة البحثية أن تحقيق توازن فعال بين الأمن والتطور التقني يتطلب مقاربة شاملة تجمع بين البعد التكنولوجي والبعد الانساني، تقوم على حوكمة رقمية رشيدة وتأطير أخلاقي وتشريعي يضمن توظيف الذكاء الاصطناعي في خدمة الامن دون المساس بحقوق الأفراد وحرياتهم الرقمية، كما تؤكد النتائج أن الأمن السيبراني في عصر الذكاء الاصطناعي لم يعد مسؤولية تقنية فحسب، بل أصبح مسؤولية اجتماعية ومؤسساتية مشتركة .

الكلمات المفتاحية: الذكاء الاصطناعي، الحماية، مخاطر الاختراق، الأمن السيبراني.

Abstract

This study aims to shed light on the complex dialectic between artificial intelligence and cybersecurity, in light of the rapid digital transformations that have made algorithms a key factor in securing information spaces on the one hand, and threatening them on the other. Artificial intelligence is now widely used in the development of early warning systems, automated intrusion detection, and big data analysis to protect institutions. However, the same technical capabilities are also exploited to create intelligent cyberattacks that are capable of adaptation and concealment.From this perspective, the study addresses the dual relationship between artificial intelligence and cybersecurity, considering it a dialectical relationship

between protection and threat, trust and danger, control and freedom. It also seeks to analyze the social and ethical implications of this phenomenon at the level of individuals, institutions, and societies, in light of the increasing reliance on automated systems and sensitive data.This research paper concludes that achieving an effective balance between security and technological development requires a comprehensive approach that combines the technological and human dimensions, based on rational digital governance and an ethical and legislative framework that ensures the use of artificial intelligence in the service of security without compromising the rights and digital freedoms of individuals. The results also confirm that cybersecurity in the age of artificial intelligence is no longer just a technical responsibility, but has become a shared social and institutional responsibility.

Keywords: Artificial intelligence, Protection, Risks of Cyber Intrusion, Cybersecurity

أثر الذكاء الإصطناعي على تطوير الهجمات السيبرانية الذكية و إستراتيجيات مواجهتها
قراءة سوسيو تنظيمية

ط.د / زياني اميمة
جامعة إبن خلدون تيارت
oumaima.ziani@univ-tiaret.dz

د/ زوهير خريبش
جامعة إبن خلدون تيارت
kheribechemg@gmail.com

الملخـــــص

يشهد الإمن السيبراني تحول رقميا داخل العالم الرقمي,بفعل التطور الهائل في ميدان الذكاء الإصطناعي بمختلف أدواته و تقنياته الحديثة. فالخوارزميات الذكية و أنظمة المعلومات يقتصر دورها فقط على حماية الأنظمة المعلوماتية الخاصة بدولة ما بصفة عامة أو مؤسسة أو شركة بصفة خاصة, بل أصبحت قادرة أيضا على تطوير أنظمة إلكترونية متقدمة يستصعب على المختصين في مجال الامن السيبراني كشفها و التعرف إليها, و هذا ما أدى إلى إنتقال الهجومات السيبرانية من كونها عملية عشوائية بسيطة إلى عملية مبرمجة أو مخطط إليها بإحكام .إذ أن الذكاء الإصطناعي في عصرنا الحالي مكن القراصنة و المحترقين من تطوير برمجيات و أساليب إلكترونية خبيثة خارجة عن الإطار القانوني و التشريعي ,في مجال التحول الرقمي و ذات قدرة على التكون و التعلم الذاتي تستطيع إختراق البيانات الرقمية و تفادي أنظمة الدفاع و بالتالي إكتشاف الثغرات الامنية الخاصة بالمستهدف موظفين في هذا الإختراق, آليات التعلم الإلكتروني أخرى كما لابد من الإشارة إلى أن ميدان الأمن السيبراني أصبح يواجه خصم ذكي, يستخدم نفس الأداة التي يعتمد عليها مختصين الأمن السيبراني أي انه يمتلك نفس وسائل التحليل الذكية التي تستخدمها أنظمة الحماية و المراقبة و هذا ما يفرض على المؤسسات تبني إستراتيجيات أمنية ذات خطط بعيدة المدى, و كذا العمل على تكوين المختصين لتنبؤ الفوري بالهجمات و توقع المخاطر المهنية و ردعها ,و في هذه الحالة الذكاء الإصطناعي اداة و وسيلة دفاعية تهدف إلى لتعرف و الكشف المسبق لمختلف الإختراقات الغير قانونية و الإستجابة التلقائية و الفورية للحوادث الامنية التي ربما ستواجه على سبيل المثال المؤسسات و الشركات. أما بالنسبة إلى إستراتيجية المقاومة و التحدي فهي تحاول الدمج بين العنصر التقني و العنصر البشري داخل نسق متكامل يهدف إلى تحقيق التوازن و الإستقرار أي إنشاء فرق عمل مختصة في مجال التحول الرقمي و قادرة على تحليل أنظمة رقمية معلوماتية, و إستخدام وسائل و تقنيات متطورة في مجال الامن السبراني مع ضرورة الدعم المادي و التكويني لهذه الفرق .كما أن التحدي و المواجهة الحقيقة لا تقتصر فقط على تطوير برامج دفاعية وقائية ,بل في تعزيز الوعي و الثقافة الرقمية و التوازن بين التطور التكنولوجي و حماية القيم الإنسانية و الأمن المؤسسي و تعزيز الضمير المهني.

الكلمات المفتاحية : الذكاء الإصطناعي/الأمن السيبراني/الهجمات السيبرانية الذكية/التعلم الآلي الذاتي/الخوارزميات الذكية.

Abstract

Cybersecurity is undergoing a profound digital transformation within the global digital sphere, driven by the tremendous advances in the field of artificial intelligence and its modern tools and techniques. Smart algorithms and information systems are no longer limited to protecting national or institutional information infrastructures; they have also become capable of developing advanced electronic systems that are difficult for cybersecurity specialists to detect or identify. This evolution has transformed cyberattacks from random, simple operations into well-planned and highly organized digital assaults. In the current era, artificial intelligence has enabled hackers and cybercriminals to develop malicious software and electronic techniques that operate outside the legal and regulatory frameworks of digital transformation. These tools possess self-learning and adaptive capabilities that allow them to penetrate digital data, bypass defense systems, and exploit specific security vulnerabilities within targeted organizations. Consequently, the field of cybersecurity now faces an intelligent adversary that employs the same analytical tools used by security professionals sharing the same intelligent mechanisms that drive protective and monitoring systems. This reality compels institutions to adopt long-term security strategies and to invest in the continuous training of specialists capable of predicting and preventing cyber risks before they occur. In this context, artificial intelligence represents both a defensive tool and a preventive mechanism, designed to enable early detection of illegal intrusions and automated, rapid responses to potential security incidents that may target institutions or companies. As for resistance and counter-strategy, it requires integrating the technical and human components within a comprehensive framework that seeks equilibrium and stability. This includes establishing specialized digital transformation teams capable of analyzing complex information systems, employing advanced cybersecurity technologies, and receiving adequate material and technical support. Ultimately, the real challenge lies not only in developing preventive defense programs but also in strengthening digital awareness, promoting a culture of cybersecurity, and ensuring a balance between technological progress, human values, institutional security, and professional ethics.

Keywords: Artificial Intelligence / Cybersecurity / Smart Cyberattacks / Machine Learning / Intelligent Algorithms

أثر الذكاء الاصطناعي على تعزيز الأمن السيبراني

د/ سليمة ميموني

المركز الجامعي الشهيد سي الحواس بريكة

salima.Mimouni@cu-arika.dz

الملخـــص

لقد كان للذكاء الاصطناعي دورا فعالا في تعزيز إمكانية اكتشاف التهديدات وتأمين المعلومات بسرعة هائلة وهو ما يعرف بالأمن السيبراني مما ساهم على الكشف المبكر للمخاطر وطرح الحلول الممكنة والاستجابة السريعة لها الأمر الذي كرّس العلاقة التفاعلية بين الذكاء الاصطناعي من جهة والأمن السيبراني من جهة أخرى.

الكلمات المفتاحية:الذكاء الاصطناعي، الأمن السيبراني، التهديدات الأمنية.

Abstract

Atificial intelligence has played a vital role in enhancing the ability to detect threats and secure information at an unprecedented rate—a field known as cybersecurity. This has contributed to the early detection of risks, the development of viable solutions, and rapid response, thus solidifying the interactive relationship between artificial intelligence and cybersecurity.

Keywords: Artificial intelligence, cybersecurity, security threats.

حماية النظام العام الإلكتروني: فرص وتحديات الذكاء الاصطناعي

د/ شتوح زوهير

جامعة باجي مختارعنابة.

zouhir.chettouh@univ-annaba.dz

الملخـــــص

يشهد النظام العام الإلكتروني تحديات متسارعة بفعل توسع الفضاء الرقمي، مما جعل الذكاء الاصطناعي أداة محورية لتعزيز الأمن السيبراني، ومكافحة الجرائم الإلكترونية، وتحليل البيانات للتنبؤ بالمخاطر، والرقابة على المحتوى الضار. ورغم فعاليته، يثير استعماله إشكالات تتعلق بالخصوصية، والمسؤولية القانونية، وإمكان تحولها إلى وسيلة للرقابة المفرطة. لذا يتطلب توظيف الذكاء الاصطناعي إطارًا قانونيًا وأخلاقيًا يحقق توازنًا بين حماية النظام الرقمي وصون الحقوق والحريات.

الكلمات المفتاحية : الذكاء الإصطناعي/الأمن السيبراني/الهجمات السيبرانية

Abstract

The electronic public order faces accelerating challenges due to the expansion of the digital space, making artificial intelligence a pivotal tool for enhancing cybersecurity, combating cybercrimes, analyzing data to predict risks, and monitoring harmful content. Despite its effectiveness, its use raises issues related to privacy, legal liability, and the risk of turning it into a tool of excessive surveillance. Therefore, employing AI requires a strict legal and ethical framework that balances protecting the digital system with safeguarding rights and freedoms.

Keywords: Artificial Intelligence / Cybersecurity / Cyberattacks

الذكاء الاصطناعي والامن السيبراني"المدلول والتحديات"

د/ بوالديارنوال **ط/د. بوالديارفوزي**

جامعة الشهيد الشيخ العربي التيسي – تبسة **جامعة حمة لخضر-الوادي**

nawal .boudiar@univ-tebessa.dz **fawzi.boudiar@univ- eloued.dz**

الملخـــــص

يُعد كلًا من الذكاء الاصطناعي والأمن السيبراني من صور التطور التكنولوجي الهائل الذي نعيشه منذ سنوات، وقد اكتسبا هذان المجالان شهرة هائلة في التكنولوجيا الحديثة، نظرًا لأدوارهما الحاسمة في تشكيل العالم الرقمي، إذ حرصت المؤسسات على الاستعانة بأدوات وأنظمة الأمن السيبراني التي تعمل بالذكاء الاصطناعي حتى تتمكن من اكتشاف التهديدات والاستجابة لها بشكل أسرع، هناك علاقة وثيقة بين الذكاء الاصطناعي والأمن الالكتروني أو السيبراني، إذ يتم تطوير أنظمة الذكاء الاصطناعي التي يمكن استخدامها لتعزيز الأمن السيبراني، إلى جانب تنفيذ تدابير أمنية لحماية أنظمة الذكاء الاصطناعي من الاختراق أو التلاعب. فبعد تزايد الجرائم الإلكترونية مثل سرقة البيانات والتصيد الاحتيالي؛ لجأت المنظمات إلى عدة وسائل لمكافحة تلك التهديدات، فاستعانت بفرق الأمن السيبراني المؤهلة المجهزة بأحدث التقنيات ومنها تقنية الذكاء الاصطناعي، التي تساعد على الكشف السريع عن الأنشطة الضارة ومواجهتها، وتحمي الشبكات من الهجمات الإلكترونية. ويعمل الذكاء الاصطناعي في مجال الأمن السيبراني على إنشاء تطبيقات آمنة بشكل افتراضي، تقضي على نقاط الضعف وتزيد من الدقة في اكتشاف المشكلات وتسريع التحقيقات، وأتمتة آليات الاستجابة.

الكلمات المفتاحية : الأمن السيبراني – الذكاء الاصطناعي

abstract

Both artificial intelligence and cybersecurity are manifestations of the tremendous technological advancement we have been experiencing over the years. These two fields have gained significant prominence in modern technology due to their crucial roles in shaping the digital world. Organizations are keen to utilize AI-powered cybersecurity tools and systems to detect and respond to threats more rapidly. There is a close relationship between AI and cybersecurity. AI systems are being developed to enhance cybersecurity, alongside implementing security measures to protect AI systems from breaches or manipulation. In light of the rise in cyber crimes such as data theft and phishing, organizations have turned to various means to combat these threats, equipping qualified cybersecurity teams with the latest technologies, including AI.

This technology aids in the swift detection of harmful activities and helps defend networks against cyber attacks.

AI in the realm of cybersecurity works to create virtually secure applications, eliminating vulnerabilities, increasing the accuracy of problem detection, speeding up investigations, and automating response mechanisms

Keywords Cybersecurity – Artificial Intelligence

المسؤولية القانونية عن الجرائم السيبرانية الناتجة عن استخدام أنظمة الذكاء الاصطناعي
-نحو نموذج تشريعي جزائري-

د/ محمد مرســــــــــلي
جامعة غرداية
morsli.mohamed@univ-ghardaia.edu.dz

الملخـــــص

أدى التوسع السريع في استخدام أنظمة الذكاء الاصطناعي إلى بروز تهديدات سيبرانية معقدة يصعب التنبؤ بها أو تحديد مصدرها، مما يثير إشكالية قانونية جديدة حول تحديد المسؤولية عن الجرائم الإلكترونية الناتجة عنها. تحاول هذه المداخلة دراسة الإطار القانوني للمسؤولية عن أفعال الذكاء الاصطناعي في الفضاء السيبراني، من خلال تحليل القوانين الجزائرية ذات الصلة ومقارنتها بالتشريعات الأجنبية الحديثة، خاصة القانون الأوروبي للذكاء الاصطناعي (AI Act 2024). تهدف الدراسة إلى اقتراح نموذج تشريعي جزائري يستجيب للتطور التكنولوجي ويحافظ على التوازن بين الابتكار الرقمي والأمن السيبراني، بما يضمن حماية فعالة للحقوق والحريات في البيئة الرقمية.

الكلمات المفتاحية: الذكاء الاصطناعي / الأمن السيبراني / الجرائم الإلكتروني / المسؤولية القانونية /التشريع الجزائري.

Abstract

The rapid expansion in the use of artificial intelligence (AI) systems has led to the emergence of complex cyber threats that are difficult to predict or attribute, raising a new legal dilemma concerning the determination of responsibility for cybercrimes committed through such systems. This paper seeks to examine the legal framework governing liability for AI-related acts in cyberspace, by analyzing relevant Algerian laws and comparing them with recent foreign legislations, particularly the European Artificial Intelligence Act (AI Act 2024). The study aims to propose an Algerian legislative model that aligns with technological advancements while maintaining a balance between digital innovation and cybersecurity, thereby ensuring effective protection of rights and freedoms in the digital environment.

Keywords : Artificial Intelligence – Cybersecurity – Cybercrime – Legal Liability – Algerian Legislation.

دور السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي في تحقيق الأمن السيبراني

د/نسرين بوعكاز
جامعة يحي فارس –المدية-
bouakez.nesrine82@gmail.com

د/ نويوة نوال
جامعة الشيخ الشهيدالعربي التبسي- تبسة-
Naouel.nouioua@gmail.com

الملخـــــص

تعتبر عملية حماية المعطيات ذات الطابع الشخصي من بين أهم العوامل التي تحقق الأمن السيبراني نظرا لما تمثله هذه المعطيات من قيمة قانونية واقتصادية وسياسية وأمنية، ولذلك أحدث المشرع الجزائري السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بموجب القانون 07/18 المـؤرخ في 0602018/10 لتتولى مهمة السهر على احترام الخصوصية وضمان معالجة المعلومات ذات الطابع الشخصي في بيئة قانونية أمنة، حيث تمارس هذه الأخيرة وظيفة مزدوجة وقائية من خلال الرقابة المسبقة على البيانات وردعية من خلال فرض العقوبات على المنتهكين، فالسلطة تعمل في إطار الموازنة بين حرية المعلومات وحماية الحياة الخاصة من خلال نشر الوعي القانوني في إطار تحقيق أمن رقمي مستدام.

الكلمات المفتاحية: معطيات- أمن سيبراني- سلطة - حماية معطيات -بيئة رقمية.

Abstract

The process of protecting personal data is considered one of the most important factors for achieving cybersecurity, given the legal, economic political, and security value that such data represent. For this reason the Algerian legislator created the National Authority for the protection of personal data under law n 18/07 of 10 june 2018 as amended and supplemented by law n 25/11 of 24 july 2025. The Authority is entrusted with the mission of ensuring compliance with privacy requirements and guaranteeing the processing of personal data within a safe legal environment. This Authority performs a dual preventive and deterrent function by supervising data processing and imposing sanctions on violators. It operates within a framework that seeks to balance freedom of information with the protection of private life, through the dissemination of legal awareness to ensure sustainable security.

Keywords : Data, Cybersecurity, Data Protection, Authority, Digital environment.

الأليات القانونية لمكافحة جريمة الإتلاف العمدي للمعطيات في التشريع الجزائري

د/ نورة منصور
جامعة عبد الحفيظ بوالصوف -ميلة-
mensour.n@centre-univ-mila.dz

د/خالدي زينب
جامعة الشهيد الشيخ العربي التبسي – تبسة-
zineb.khaldi@univ-tebessa.dz

الملخـــــص

تشمل جرائم المساس بأنظمة المعالجة الألية للمعطيات في التشريع الجزائري جريمة اتلاف النظام الالي بوسائل وتقنيات محددة وهذا عن طريق فيروس الحاسب الألي، وعلى هذا النحو يكون المشرع الجزائري قد ساير مختلف التشريعات المقارنة ،في مجال استحداث نصوص قانونية لمواجهة هذا النوع، تتمثل الآليات القانونية في التشريع الجزائري لمكافحة جريمة إتلاف المعطيات في تعديل قانون العقوبات بالقانون 04/06 الذي أضاف القسم السابع المكررالمتضمن جرائم المساس بأنظمة المعالجة الآلية للمعطيات وقد عرّف هذا القسم الجرائم الإلكترونية، بما في ذلك إتلاف النظام الآلي، وحدد عقوبات لها، بالإضافة إلى إنشاء هيئات متخصصة مثل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال. كما تم تكييف قانون الإجراءات الجزائية ليتناسب مع طبيعة هذه الجرائم، ودعم هذا الإطار القانوني بالمصادقة على الاتفاقيات الدولية ذات الصلة .

الكلمات المفتاحية : جريمة - إتلاف -معطيات – الألية-العمدي.

Abstract

Crimes against automated data processing systems in Algerian legislation include the crime of damaging the automated system by specific means and techniques, and this is through a computer virus. In this way, the Algerian legislator has kept pace with various comparative legislations in the field of creating legal texts to confront this type. The legal mechanisms in Algerian legislation to combat the crime of data destruction consist of amending the Penal Code by Law No 06/04 which added Section 7 bis, Tampering with Automated Data Processing System This section defines cybercrimes, including the destruction of automated systems, and specifies penalties for them, in addition to establishing bodies. Specialized bodies such as the National Authority for the Prevention of Crimes Related to Information and Communication Technologies have been established. Furthermore, the Code of Criminal Procedure has been adapted to address the nature of these crimes, and this legal framework has been strengthened by the ratification of relevant international conventions.

Keywords: Crime, destruction, data, mechanism, intentional.

إدارة المفارقة الأمنية: توظيف الذكاء الاصطناعي لتعزيز الحماية السيبرانية ومواجهة تهديداته المتطورة

د/فخر الدين مهوبي
جامعة محمد خيضر –بسكرة-
fakhreddine.mihoubi@univ-biskra.dz

د/وليد صيفي
جامعة محمد خيضر- بسكرة-
walid.saifi@univ-biskra.dz

الملخـــــــص

يقدم الذكاء الاصطناعي تحولًا جذريًا في مشهد الأمن السيبراني، فهو أداة ذات حدين تخلق معادلة أمنية جديدة ومعقدة. من جهة، يُعَد حليفًا استراتيجيًا لا غنى عنه؛ حيث تعمل خوارزمياته على تعزيز الحماية من خلال الكشف الذكي والمبكر عن التهديدات، وتحليل السلوكيات المشبوهة لتوقع الهجمات قبل وقوعها، وأتمتة الاستجابة للحوادث مما يقلل الوقت والجهد البشري. ولكن من جهة مقابلة، يُشكِّل نفس هذا التطور تهديدًا غير مسبوق؛ إذ يسلح المهاجمين بأدوات متطورة تمكنهم من شن هجمات أكثر ذكاءً وتعقيدًا، مثل الهجمات الإلكترونية ذاتية التعلّم، وتقنيات التزييف العميق (Deepfake) للتلاعب والاحتيال، وتطوير برمجيات خبيثة متكيفة تتجنب الكشف. لذلك، تهدف هذه المداخلة إلى تحليل هذه المعادلة الصعبة، وتسليط الضوء على آليات توظيف الذكاء الاصطناعي في تعزيز الأمن، وفي الوقت نفسه تشريح المخاطر الجديدة التي يولدها، مع التأكيد على الحاجة الماسة إلى تطوير أطر أمنية وقانونية وأخلاقية مرنة قادرة على مواكبة هذه الديناميكية المتسارعة، لتحقيق التوازن المنشود بين استغلال الفرص والتخفيف من حدة التهديدات.

الكلمات المفتاحية: الذكاء الاصطناعي، الأمن السيبراني، الهجمات الإلكترونية، التزييف العميق، الكشف عن التهديدات، الأمن الرقمي، الأطر التنظيمية.

Abstract

Artificial intelligence brings about a profound transformation in the cybersecurity landscape, as it constitutes a double-edged instrument that gives rise to a new and complex security paradigm. On the one hand, it represents an indispensable strategic ally; its algorithms enhance protection through intelligent and early threat detection, behavioral analysis to anticipate attacks before they occur, and the automation of incident response, thereby significantly reducing human time and effort. On the other hand, this very advancement poses an unprecedented threat, as it empowers attackers with sophisticated tools that enable more intelligent and complex attacks, including self-learning cyberattacks, deepfake technologies used for manipulation and fraud, and adaptive malware designed to evade detection.

Accordingly, this contribution seeks to analyze this challenging equation, shedding light on the mechanisms for leveraging artificial intelligence to strengthen cybersecurity, while

simultaneously examining the emerging risks it generates. It further underscores the urgent need to develop flexible security, legal, and ethical frameworks capable of keeping pace with this rapidly evolving dynamic, in order to achieve the desired balance between harnessing opportunities and mitigating threats.

Keywords: Artificial intelligence, cybersecurity, cyberattacks, deepfake technology, threat detection, digital security, regulatory frameworks.

ديناميكيات العلاقة بين الذكاء الاصطناعي والأمن السيبراني

د/ صبرينــة بوبكر
جامعة محمد الشريف مساعدية – ســوق أهــراس-
s.boubaker@univ-soukahras.dz

الملخـــــص

هناك علاقة معقدة ومتنامية في نفس الوقت بين الذكاء الاصطناعي والأمن السيبراني، فمن ناحية يقدم الذكاء الاصطناعي فرصا غير مسبوقة لتعزيز الدفاعات السيبرانية، حيث تستخدم تقنيات تعلم الآلة والتعلم العميق في الكشف الاستباقي عن التهديدات، وتحليل السلوكيات الشاذة في الشبكات، وأتمتة الاستجابة للحوادث بسرعة تفوق القدرات البشرية، هذه الأدوات تمثل درعا قويا في مواجهة الهجمات المتطورة، مما يقلل من زمن الاستجابة ويحسن من كفاءة إدارة الثغرات الأمنية. ومن ناحية أخرى، يفتح الذكاء الاصطناعي الباب أمام تحديات ومخاطر جسيمة، إذ أصبح أداة قوية في أيدي المهاجمين، حيث تستخدم تقنيات الذكاء الاصطناعي لتطوير برمجيات خبيثة ذاتية التطور (Polymorphic Malware)، وشن هجمات تصيد احتيالي شديدة التخصيص وواسعة النطاق، والتغلب على أنظمة الحماية التقليدية، كما يبرز مفهوم الذكاء الاصطناعي العدائي كأحد أخطر التهديدات، حيث يتم التلاعب بالنماذج الذكية لخداعها أو تسميم بياناتها التدريبية. بين هذا وذاك، يحاول التشريع التعامل مع الجرائم المرتكبة بواسطة أنظمة الذكاء الاصطناعي وبالتالي إيجاد حل لإشكاليات إسناد المسؤولية القانونية (الجنائية والمدنية)، وتحديات الخصوصية الناشئة عن استخدام الذكاء الاصطناعي في المراقبة، مع ضرورة تطوير أطر تنظيمية وتشريعية جديدة تواكب المستجدات المتسارعة التي تتسم بها هذه التكنولوجيا الحديثة.

الكلمات المفتاحية : الذكاء الاصطناعي- الأمن السيبراني - المسؤولية القانونية - التشريعات الرقمية - الذكاء الاصطناعي العدائي.

Abstract

There is a complex and simultaneously evolving relationship between artificial intelligence (AI) and cybersecurity. On one hand, AI presents unprecedented opportunities to enhance cybersecurity defences. Machine learning and deep learning techniques are utilized for proactive threat detection, analysing anomalous network behaviour, and automating incident response at speeds that surpass human capabilities. These tools act as a powerful shield against sophisticated attacks, reducing response times and improving the efficiency of vulnerability management. On the other hand, AI opens the door to significant challenges and risks, as it has become a potent tool in the hands of attackers. AI techniques are used to develop self-evolving malicious software Polymorphic Malware), launch highly personalized and large-scale phishing

attacks, and bypass traditional protection systems. Furthermore, the concept of emerges as one of the most serious threats, where intelligent models are manipulated to deceive them or their training data is poisoned. Navigating this dichotomy, legislation is attempting to address crimes committed by AI systems and, consequently, to find solutions for the complexities of assigning legal liability (both criminal and civil) and the privacy challenges arising from the use of AI in surveillance. This underscores the necessity of developing new regulatory and legislative frameworks that can keep pace with the rapid advancements characteristic of this modern technology.

Keywords Artificial Intelligence, Cybersecurity, Legal Liability, Digital Legislation, Adversarial AI.

المسؤولية عن الأضرار الناتجة عن استخدام الأنظمة الذكية في الفضاء السيبراني

د/باسل سهام

جامعة 20 اوت 1955 سكيكدة

s.bacel@univ-skikda.dz

الملخـــــص

يشهد العالم ثورة تكنولوجية هائلة، يلعب فيها الذكاء الاصطناعي) AI) دورا هاما في مختلف المجالات، بما في ذلك الفضاء السيبراني ، الأمر الذي أدى إلى بروز عدة تحديات و تهديدات تمس الأمن السيبراني الذي أصبح اليوم يشكل محورا للأمن القومي و الاقتصادي للدول ، حيث أصبحت الأنظمة الذكية قادرة على اتخاذ قرارات ذاتية في بيئة رقمية مفتوحة ، كما لها أن تقوم باختراقات إلكترونية ممكن أن تسبب أضرار جسيمة لمتعاملي هذا الفضاء . و هنا يثور التساؤل حول نظام المسؤولية عن الأضرار الناتجة عن استخدام الأنظمة الذكية في هذا الفضاء و كيف يتم تحديد المسؤول عن هذه الأضرار سواء مسؤولية مدنية أو جزائية فبالنسبة للمسؤولية المدنية التساؤل يكمن في ما إذا كانت القواعد التقليدية للمسؤولية العقدية و التقصيرية) كافية للتطبيق في هذه الحالة أم أن المشرع يحتاج إلى وضع نصوص أخرى أكثر دقة ووضوح و توازن بين حماية الحقوق الرقمية و تشجيع الابتكار التكنولوجي، ذلك أنه كلما كان نظام المسؤولية أكثر وضوحا في تحديد الفاعلين و الجزاءات المترتبة عن الأضرار الناتجة عن استخدامهم للأنظمة الذكية كلما ساهم ذلك في تعزيز الثقة في البيئة الرقمية و تحقيق مستوى أعلى من الأمن السيبراني . كما أن الفضاء السيبراني يعد بيئة افتراضية تمارس فيها أفعال قد تشكل جرائم إلكترونية كاختراق الأنظمة سرقة البيانات، أو نشر البرمجيات الخبيثة، و عندما ترتكب هذه الأفعال بواسطة أنظمة ذكية تعمل باستقلالية جزئية أو كلية يثار التساؤل حول من يتحمل المسؤولية الجزائية .

الكلمات المفتاحية: الأمن السيبراني – الذكاء الاصطناعي- المسؤولية .

Abstract

The world is witnessing a tremendous technological revolution in which Artificial Intelligence (AI) plays an important role in various fields, including cyberspace. This has led to the emergence of many challenges and threats that affect cybersecurity, which has now become a key component of national and economic security for states. Intelligent systems are increasingly capable of making autonomous decisions within an open digital environment and can also carry out cyber intrusions that may cause serious damages to users operating in this space. This raises important questions about the liability system for damages resulting from the use of intelligent systems in cyberspace and how responsibility for such damages should be determined, whether civil or criminal. With regard to civil liability, the issue is whether traditional rules of liability—both contractual and tortious—are sufficient to apply in such

cases, or whether legislators need to establish more precise and clearer rules that balance the protection of digital rights with the encouragement of technological innovation. Indeed, the clearer and more precise the liability system is in identifying responsible parties and the sanctions arising from damages caused by the use of intelligent systems, the more it contributes to strengthening trust in the digital environment and achieving a higher level of cybersecurity. Moreover, cyberspace constitutes a virtual environment in which actions that may amount to cybercrimes are carried out, such as system intrusions, data theft, or the dissemination of malicious software. When such acts are committed by intelligent systems operating with partial or full autonomy, the question arises as to who bears criminal responsibility.

Keywords: Cybersecurity – Artificial Intelligence – Liability.

تطورمفهوم الأمن وتأثره بالتطورالتكنولوجي خصوصا في المجال الإلكتروني والرقمي.

أ/أمير عباد

جامعة الشهيد الشيخ العربي التبسي. تبسة.

amir.abbad@univ-tebessa.com

الملخـــــــص

يكتسي مفهوم الأمن أهمية بالغة في حياتنا بشتى تفرعاتها؛ فهو أساس الحياة و استمراريتها؛ و لا شك أن هذا المفهوم شهد العديد من المحطات التي صقلته و أعطته نقلة نوعية من المفاهيم التقليدية البسيطة؛ إلى مفتهيم متطورة و معقدة تلامس أدق الأمور و أوسعها؛ فمن مفهوم الأمن بأبعاده المنحصرة في المجال العسكري و التسليح و تعظيم القوة بالمفهوم الواقعي؛ أصبحنا نتحدث عن الأمن الإنساني كمستوى فردي عولمي للمفهوم ؛ و صار الحديث أيضا يشمل التهديدات الرقمية التي تعتبر حتى وقت قريب مجرد زوبعة في فنجان لا تكاد تؤثر في جهاز حاسوب لشخص معين، لتصبح فيما بعد أخطر أنواع التهديدات التي يمكن أن تشل أقوى الدول على المستوى العالمي مع توجه المجتمع الدولي إلى الرقمنة و أعتماد الشبكة العنكبوتية في شتى مجالات الحياة، صغيرة كانت أو كبيرة. لذلك تعالج الورقة هذه الجزئية من تطور مفهوم الأمن و تأثره بالتطور التكنولوجي الرقمي.

الكلمات المفتاحية : الأمن- الامن السيبراني- التكنولوجيا

Abstract:

Security is a vital concept that touches every aspect of our lives; it is foundational to human existence. This concept has undoubtedly undergone numerous transformations, becoming more refined and shifting from traditional interpretations to more sophisticated and comprehensive understandings. Today, specialists explore both the broadest and most detailed dimensions of security. Historically, the concept was confined to military affairs, weaponry, and maximizing power in a practical sense. However, security has expanded to encompass a wider scope, including individual and global dimensions such as insurance and protection systems. Contemporary discussions now extend deeply into the digital realm a field that was once limited to brief, isolated computer operations but has since evolved into a cornerstone of modern life. Despite the many factors that could threaten the stability of nations, the international community has grown increasingly dependent on digital technologies and the Internet across all sectors. This dependency has made the relationship between security and digital technological development more critical than ever.

For this reason, the study of security and its influence on advancements in electronic and digital technologies has emerged as a significant and timely area of inquiry.

Key Words:Security, Digital Technology, Cybersecurity,

الذكاء الاصطناعـي و مدى تأثيـــره في تحقيـــق الأمن السيبراني

د/ملاك وردة

جامعة الشهيد الشيخ العربي التبسي- تبسة.

o.mallek@univ-tebessa.dz

الملخـــــص

أصبح من المؤكد اليوم أن الذكاء الاصطناعي بمختلف استخداماته في شتى القطاعات و الميادين، ضرورة حتمية لتسجيل تقدم في عصر التكنولوجيا و الرقمنة مما يجعله ذات أهمية بالغة في البحث عن دوره لتعزيز و تحقيق الأمن السيبراني، و إضفاء الحماية اللازمة على المعلومات و البيانات الشخصية المتعلقة بمستخدمي شبكة الأنترنت من التجاوزات و الاختراقات المفترض وقوعها. و هذا ما يعني وجود علاقة ترابط و تجاذب بين كل من مصطلحي الذكاء الاصطناعي و الأمن السيبراني، و اللذان أصبحا من الأولويات التي تخصص لها الدول آليات و جهود معتبرة لضبطها و تقنينها و حصر الأضرار التي يمكن أن تترتب عنها.

الكلمات المفتاحية: الذكاء الاصطناعي، الأمن السيبراني، القانون، المعلومات الرقمية، الاختراق.

Abstract

It has become evident today that artificial intelligence, in its various applications across different sectors and fields, constitutes an inevitable necessity for achieving progress in the era of technology and digitalization. This confers upon it great importance in examining its role in strengthening and ensuring cybersecurity, and in providing the necessary protection for information and personal data relating to Internet users against potential abuses and cyber intrusions. This implies the existence of an interdependent and interactive relationship between the concepts of artificial intelligence and cybersecurity, both of which have become priorities to which States devote significant mechanisms and efforts in order to regulate and control them and to limit the damages that may result therefrom.

Keywords: Artificial Intelligence, Cybersecurity, Law, Digital Information, Cyber Intrusion.

الذكاء الاصطناعي بين دعم الأمن السيبراني وتهديده دراسة قانونية على ضوء التشريع الجزائري

د/معيفي محمد
جامعة الشهيد الشيخ العربي التبسي- تبسة-
mohammed.maifi@univ-tebessa.dz

الملخـــص

انطلاقا من ما يحمله الذكاء الاصطناعي كأداة دعم للأمن السيبراني وكونه في الوقت ذاته مصدرا مهددا له وفي ظل التطور المتسارع للذكاء الاصطناعي وجعله عنصرا محوريا في منظومة الأمن السيبراني واستخدامه في الكشف عن الهجمات الالكترونية وتحسين آليات الوقاية، إلا أن ذلك في حد ذاته قد يحمل أساليب جديدة للاختراق و الاطلاع على البيانات الرقمية مما يفرض تحديات تشريعية و قانونية في هذا المجال. ومنه تهدف هذه الورقة البحثية إلى تحليل الازدواجية الذي يمثلها الذكاء الاصطناعي بين دعم الأمن السيبراني وتهديده ومن خلال دراسة تحليلية للإطار القانوني المنظم لتكنولوجيا الذكاء الاصطناعي ومدى مواكبة المنظومة القانونية الوطنية لتطورات وتهديدات التكنولوجيا الحديثة ومكافحة الجرائم السيبرانية وحماية المعطيات الشخصية مع اقتراح جملة من التوصيات في هذا المجال ،قصد استخدام الذكاء الاصطناعي و التطور التكنولوجي مع ضمان الأمن القانوني و الرقمي عند استخدامه.

الكلمات المفتاحية: الذكاء الاصطناعي / الأمن السيبراني / الجرائم الالكترونية / الحوكمة الرقمية / التهديدات الرقمية.

Abstract

It is now well established that artificial intelligence, in its various applications across diverse sectors and fields, constitutes an indispensable requirement for achieving progress in the era of technological advancement and digitalization. This underscores its critical importance in examining its role in strengthening and ensuring cybersecurity, as well as in providing adequate protection for information and personal data relating to Internet users against anticipated violations and cyber intrusions.

This situation reflects a relationship of interdependence and dynamic interaction between the concepts of artificial intelligence and cybersecurity, both of which have become strategic priorities to which states devote substantial legal, technical, and institutional mechanisms and efforts to regulate their deployment and to limit the potential harms and risks arising therefrom.

Keywords: Artificial intelligence, cybersecurity, law, digital information, cyber intrusion.

مستقبل الأمن: كيف يعيد الذكاء الاصطناعي تشكيل قواعد اللعبة في الفضاء السيبراني؟

أ/د. سمير كيم **د/سماح سهايلية**

المؤسسة: جامعة العربي التبسي- تبسة **المؤسسة: جامعة العربي التبسي- تبسة**

s.kime@univ-tebessa.dz **Samah.sehailia@univ- tebessa.dz**

الملخـــص

شهدت البيئة الأمنية الدولية تحولا جذريا مع التطور المتسارع للذكاء الاصطناعي (AI)، الذي تكمن خطورته وميزته في كونه قوة ضاربة للمهاجمين ودرعاللمدافعين في آن واحد. فمن ناحية، يقوم المهاجمون بتسخير قدرات الذكاء الاصطناعي لأتمتةالهجمات وجعلها أكثر دقة وتعقيدا، مما يقلب موازين القوى لصالح التهديدات المتقدمة، ويفرض تحديات غير مسبوقة على السيادة الوطنية وأمن البنى التحتية الحيوية. من ناحية أخرى، يُقدم الذكاء الاصطناعي الحلول الدفاعية الضرورية، مما يمكّن المدافعين من التحول من الاستجابة التفاعلية إلى الدفاع الاستباقي والذكي.

تهدف هذه المداخلة إلى تحليل طبيعة هذا السباق التكنولوجي المستمر بين الهجوم والدفاع، وتحديد التحديات الرئيسية التي يواجهها الأمن السيبراني في هذا العصر الجديد (مثل الحاجة إلى آليات كشف سريعة، وأطر أخلاقية للتعامل مع البيانات الضخمة)، وتقديم رؤية استراتيجية حول كيفية إعادة تشكيل قواعد اللعبة العالمية نحو بناء أنظمة أمنية أكثر مرونة وتكيفا واستدامة على مستوى الدول والمؤسسات.

الكلمات المفتاحية: الأمن السيبراني، الذكاء الإصطناعي، الفضاء السيبراني،الأمن القومي، السيادة

Abstract:

The international security landscape is undergoing a radical transformation with the rapid development of artificial intelligence (AI). AI's danger and advantage lie in its dual nature: it is both a powerful tool for attackers and a shield for defenders. On the one hand, attackers are harnessing AI capabilities to automate attacks, making them more precise and sophisticated. This shifts the balance of power in favor of advanced threats and poses unprecedented challenges to national sovereignty and the security of critical infrastructure. On the other hand, AI provides essential defensive solutions, enabling defenders to move from reactive responses to proactive and intelligent defense.

This paper aims to analyze the nature of this ongoing technological race between offense and defense, identify the key challenges facing cybersecurity in this new era (such as the need for rapid detection mechanisms and ethical frameworks for handling big data), and offer a strategic

vision for reshaping the global game towards building more resilient, adaptable, and sustainable security systems at the national and institutional levels.

Keywords: Cybersecurity, Artificial Intelligence, Cyberspace, National Security, Sovereignty

الثقافة الرقمية والأمن السيبراني لدى الطلبة: دراسة سوسيولوجية لتمثلات المخاطر الإلكترونية

د/الحمزة بلال **د/ زغلامي حسيبة**

عبد الحميد مهري قسنطينة02 **جامعة الشهيد الشيخ العربي التبسي – تبسة-**

bilal.elhamza@univ-constantine2.dz **hassiba.zoghlami@gmail.com**

الملخـــص

شهد العالم خلال العقود الأخيرة تحولات رقمية عميقة أدت إلى إعادة تشكيل أنماط الحياة، وأساليب التواصل، وطرق الوصول إلى المعرفة، فقد أصبحت التكنولوجيا الرقمية جزءا لا يتجزأ من البنية الاجتماعية الحديثة، مؤثرة في مختلف مجالات النشاط الإنساني، بما في ذلك قطاع التعليم الذي عرف اعتمادا واسعا على الوسائط الرقمية والمنصات الإلكترونية، وفي قلب هذا التحول برزت الثقافة الرقمية كرافد أساسي لفهم كيفية تفاعل الأفراد مع الفضاءات السيبرانية، وما تتيحه من فرص وما تحمله من تهديدات. ومع هذا الانتشار المتزايد للفضاء الرقمي، ظهرت تحديات أمنية جديدة تفرض نفسها بقوة عبر ما يعرف بـ الأمن السيبراني، وهو مجموعة من الإجراءات والممارسات الهادفة إلى حماية المعلومات والأنظمة والهوية الرقمية من الهجمات والاختراقات، وقد أصبح الأمن السيبراني اليوم أحد أهم انشغالات المؤسسات التعليمية، نظرا لكون الطلبة يشكلون أحد الفئات الأكثر نشاطا واستعمالا للتكنولوجيا، الأمر الذي يجعلهم عرضة لمختلف أشكال المخاطر الإلكترونية مثل الاختراق، الابتزاز الرقمي، سرقة المعطيات، وانتحال الهوية. كما يكتسب تناول الموضوع من زاوية سوسيولوجية أهمية خاصة، إذ لا يقتصر فهم الظاهرة على الجوانب التقنية فقط، بل يتعداها إلى تحليل تمثلات الطلبة للمخاطر السيبرانية، وكيفية إدراكهم لها وتفسيرهم لمنابعها، انطلاقا من خلفياتهم الاجتماعية وتجاربهم الرقمية اليومية، فالثقافة الرقمية ليست مجرد مهارات تقنية، بل هي منظومة معارف وقيم وممارسات تحدد طريقة استعمال الطلبة للتكنولوجيا، وتؤثر في تعاملهم مع التهديدات الإلكترونية.

الكلمات المفتاحية: الثقافة الرقمية، الأمن السيبراني، المخاطر الإلكترونية، تمثلات الطلاب، الوعي الرقمي، المؤسسات التعليمية.

Abstract

In recent decades, the world has witnessed profound digital transformations that have reshaped lifestyles, communication methods, and ways of accessing knowledge, Digital technology has become an integral part of modern social structures, influencing various areas of human activity, including the education sector, which has widely adopted digital media and electronic platforms. At the core of this transformation, digital culture has emerged as a fundamental framework for understanding how individuals interact with cyberspaces, the opportunities it provides, and the risks it carries. With the increasing spread of digital spaces, new security challenges have emerged, prominently through what is known as cybersecurity a set of procedures and practices aimed at protecting information, systems, and digital identities from

attacks and breaches, Today, cybersecurity has become one of the primary concerns of educational institutions, as students constitute one of the most active and frequent users of technology, making them vulnerable to various forms of cyber threats, such as hacking, digital blackmail, data theft and identity fraud

Addressing this topic from a sociological perspective is particularly important as understanding the phenomenon goes beyond technical aspects to includ the analysis of students' representations of cyber risks, how they perceive these risks, and how they interpret their sources, based on their social backgrounds and daily digital experiences. Digital culture is not merely a set of technical skills but a system of knowledge, values, and practices that shapes how students use technology and interact with cyber threats.

This study aims to explore the relationship between digital culture and students' cyber awareness, by analyzing their perceptions and representations of electronic risks and examining digital behaviors that may increase their vulnerability, It also seeks to understand the social factors shaping these representations, whether related to family, peers, the educational environment, or personal experiences in cyberspace.

Keywords: Digital Culture, Cybersecurity, Cyber Risks. Students'Representations, Digital Awareness, Educational Institution

الدفاع السبراني كامتداد استراتيجي للاحلاف العسكرية: حلف شمال الاطلسي(الناتو) نموذجا

د/طاجين نسيمة
جامعة محمد البشير الابراهيمي-برج بوعريريج
nacima.tadjin@univ-bba.dz

ط/د. كعبش عبد الوهاب
جامعة الجزائر01
abdoukaabeche79@gmail.com

الملخـــــص

شهدت التحالفات العسكرية التقليدية تحوالت كبيرة في العقدين األخيرين بفعل التطورات الرقمية والتهديدات السيبرانية العابرة للحدود، ما أفرز نوًعا جديًدا كنموذج عملي Pledge Defence Cyber NATO من التعاون بين الدول،يعرف باألحالف الدفاعية السبرانية، و تهدف هذه الدراسة إلى تحليل لهذه التحوالت، وفهم كيف أصبح الفضاء السيبراني امتدادًا للتحالفات العسكرية التقليدية في تعزيز الامن الجماعي، وتكتسب الدراسة أهميتها من كونها تسلط الضوء على نموذج عملي يجمع بين الاستراتيجية العسكرية والتكنولوجيا الحديثة، ويجيب على أسئلة حول الامن الجماعي في الفضاء الرقمي الذي يفتقر حتى الان إلى إطار قانوني دولي واضح، كما تقدم الدراسة إطاًرا تحليلًيا يمكن استخدامه لتقييم التحالفات السبرانية الاخرى مستقبلا، وتنطلق الدراسة من الاشكالية التالية: كيف يمكن للاحلاف الدفاعية السبرانية أن تعكس امتدادًا فعالا للتحالفات العسكرية التقليدية مع ضمان الامن الجماعي في مواجهة التهديدات السيبرانية؟. وتطرح مجموعة من التساؤلات الفرعية : ما طبيعة التحول من التحالفات العسكرية التقليدية إلى السبرانية؟ما التحديات القانونية والسياسية المرتبطة بهذا النموذج؟إلى أي مدى يساهم التحالف السيبراني في تعزيز الردع الجماعي وحماية الامن الرقمي؟

الكلمات المفتاحية: الاحلاف الدفاعية السبرانية- الاحلاف العسكرية التقليدية- الامن الجماعي

Abstract

Traditional military alliances have undergone significant transformations over the past two decades due to digital developments and cross-border cyber threats, giving rise to a new form of inter-state cooperation known as cyber defence alliances. This study aims to analyze the NATO Cyber Defence Pledge as a practical model of these transformations and to understand how cyberspace has become an extension of traditional military alliances in enhancing collective security. The importance of this study lies in its focus on a practical model that combines military strategy with modern technology, addressing questions about collective security in the digital domain, which still lacks a clear international legal framework. Additionally, the study provides an analytical framework that can be used to evaluate other cyber alliances in the future. The study is guided by the following research problem: How can cyber defence alliances effectively reflect an extension of traditional military alliances while ensuring collective security

in the face of cyber threats?. It also raises several sub-questions: What is the nature of the transition from traditional military alliances to cyber alliances?

What mechanisms does NATO implement under the Cyber Defence Pledge?

What legal and political challenges are associated with this model?

To what extent does the cyber alliance contribute to enhancing collective deterrence and protecting digital security?

Keywords: cyber alliances, traditional military alliances, collective security, NATO Cyber Defence Pledge, cyberspace

دور الذكاء الاصطناعي في التنبؤ بالهجمات السبرانية وتحسين الاستجابة الأمنية

د/ رقية بلقاسمي

جامعة الشهيد الشيخ العربي التبسي – تبسة-

rokaya.belcasmi07@gmail.com

الملخـــــص

يُعدّ الذكاء الاصطناعي من أبرز الأدوات الحديثة في مواجهة التهديدات السيبرانية المتنامية، إذ يسهم في تطوير أنظمة قادرة على التنبؤ بالهجمات الإلكترونية وتحليل أنماطها قبل وقوعها. تعتمد هذه الأنظمة على خوارزميات التعلم الآلي والتعلم العميق لاكتشاف السلوكيات غير الطبيعية ضمن الشبكات الرقمية، مما يتيح الاستجابة المبكرة والتلقائية للتهديدات. تهدف هذه الدراسة إلى تحليل دور الذكاء الاصطناعي في رفع كفاءة الأمن السيبراني عبر التنبؤ بالهجمات وتقليص زمن الاستجابة، مع التركيز على نماذج تحليل البيانات الضخمة وأنظمة المراقبة الذكية. كما تستعرض التحديات التقنية والأخلاقية المرتبطة باستخدام الذكاء الاصطناعي في هذا المجال، مثل مشكلة البيانات المضللة واحتمالات إساءة استخدام التكنولوجيا. وتخلص الدراسة إلى أن الدمج الفعّال بين الإنسان والآلة يمثل مستقبل الدفاع السيبراني، ويشكل خطوة أساسية نحو بناء بيئة رقمية أكثر أماناً واستدامة.

الكلمات المفتاحية: الأمن السيبراني، الذكاء الإصطناعي، الفضاء السيبراني .

Abastract

Artificial Intelligence (AI) has emerged as one of the most effective tools for addressing the growing challenges of cybersecurity. It enables the development of systems capable of predicting cyberattacks and analyzing their patterns before they occur. Through machine learning and deep learning algorithms, AI can detect abnormal behaviors within digital networks, allowing for early and automated responses to potential threats. This study aims to examine the role of AI in enhancing cybersecurity performance by forecasting attacks and reducing response time, with a focus on big data analytics and intelligent monitoring systems. It also discusses the technical and ethical challenges of using AI in cybersecurity, such as misleading data and the risk of technological misuse. The study concludes that effective human–AI collaboration represents the future of cyber defense and a crucial step toward a safer and more resilient digital environment.

Keywords: Cybersecurity, Artificial Intelligence, Cyberspace,

الإطار القانوني والمؤسساتي الجزائري لمواجهة التهديدات السيبرانية

ط/ د. نسيمة العلمي
جامعة الشهيد الشيخ العربي التبسي

lalmi.nassima@univ-tebessa.dz

الملخـــــص

تهدف هذه الدراسة إلى تقييم وتحليل الإطار القانوني والمؤسساتي الجزائري المُعتمد لمواجهة التهديدات السيبرانية المتزايدة، التي تستهدف البنية التحتية الوطنية الحيوية، وذلك في سياق التحول الرقمي المتسارع، وهو ما يجعل جاهزية وفعالية المنظومة الوطنية للأمن السيبراني على المحك. وتتمحور الإشكالية الرئيسية حول التساؤل الجوهري: ما مدى كفاية وفعالية الإطار القانوني والمؤسساتي الجزائري الحالي في توفير منظومة متكاملة وفعالة للحماية والردع والوقاية لمواجهة التهديدات السيبرانية المتطورة؟ ، ويتبين أن هذا الإطار عبارة عن منظومة ذات بعدين أساسيين: ركيزة تشريعية للردع والحماية، تتمثل في قانون مكافحة الجريمة الإلكترونية 09-04 لتجريم الأفعال الماسة بنظم المعطيات، وقانون حماية البيانات الشخصية 18-07 الذي يعزز الأمن السيبراني عبر ضوابط البيانات؛ وركيزة ثانية مؤسساتية للاستراتيجية والاستجابة، تتمثل في المجلس الوطني لأمن نظم المعلومات (CNSSI) لوضع الاستراتيجية العليا، والفريق الوطني للاستجابة للطوارئ السيبرانية (DZ-CERT) لإدارة الحوادث، مدعومة بأجهزة أمنية وعسكرية متخصصة مثل مصلحة الدفاع السيبراني. ومع اكتمال هذه الركائز، تُشير الدراسة إلى أن المنظومة تواجه تحديات تشغيلية كبيرة، أبرزها الثغرة البشرية المتمثلة في النقص النوعي والكمي في الكفاءات المتخصصة، مما يُعيق التتبع والتحليل والاستجابة المتقدمة للتهديدات المتطورة، ويستدعي ضرورة تعزيز التكوين الأكاديمي ورفع الوعي لضمان منظومة حماية وردع ووقاية متكاملة.

الكلمات المفتاحية: الأمن السيبراني، القانون 09-04، التهديدات السيبرانية،الوكالة الوطنية لأمن الانظمةالمعلوماتية الجريمة الإلكترونية، الحماية التشريعية..

Abstract

This study aims to evaluate and analyze the Algerian legal and institutional framework adopted to confront the increasing cyber threats that target the national vital infrastructure, in the context of accelerating digital transformation, which places the readiness and effectiveness of the national cybersecurity system at stake. The main problem centers around the fundamental question: How efficient and effective is the current Algerian legal and institutional framework in providing an integrated and effective system for protection, deterrence, and prevention to confront evolving cyber threats? It is clear that this framework is a system with two essential dimensions: a legislative pillar for deterrence and protection, represented by the Cybercrime Law 09-04 for criminalizing acts affecting data systems, and the Personal Data Protection Law 18-07 which enhances cybersecurity through data controls; and a second

institutional pillar for strategy and response, represented by the National Council for Information Systems Security (CNSSI) for setting the supreme strategy, and the National Computer Emergency Response Team (DZ-CERT) for incident management, supported by specialized security and military agencies such as the Cyber Defense Service. With the completion of these pillars, the study indicates that the system faces significant operational challenges, the most prominent of which is the human vulnerability represented by the qualitative and quantitative shortage of specialized competencies, which hinders advanced tracking, analysis, and response to evolving threats, necessitating the need to strengthen academic training and raise awareness to ensure an integrated system of protection, deterrence, and prevention.

Key Words: Cybersecurity. Law 09-04. Cyber Threats. National Agency for Information Systems Security (ANSSI). Cybercrime. Legislative Protection

الامن السيبراني في عصر الذكاء الاصطناعي – دراسة في العلاقة والتأثير

د/ حياة فرد
جامعة البويرة – الجزائر
h.ferd@univ-bouira.dz

د/ ام الخير عيشون
جامعة البويرة - الجزائر
o.aichone@univ-bouira.dz

الملخــص

يشهد العالم المعاصر تحوّلا جذريا بفعل التطورات المتسارعة في مجال الذكاء الاصطناعي، الذي أصبح يشكل أحد أهم المكونات الاستراتيجية في التحوّل الرقمي وصناعة القرار. غير أن هذا التطوّر التقني الهائل ترافق معه تصاعد في التهديدات السيبرانية وتنوّع في أساليب الهجوم والاختراق، الأمر الذي أفرز علاقة معقّدة بين الأمن السيبراني والذكاء الاصطناعي، قوامها التأثير المتبادل والتكامل أحياناً، والتعارض أحياناً أخرى وعليه كيف تتفاعل تقنيات الذكاء الاصطناعي مع الأمن السيبراني في الوقت نفسه كأداة للحماية وكتهديد محتمل؟

الكلمات المفتاحية: الأمن السيبراني – الذكاء الاصطناعي – التعلّم الآلي – التهديدات الرقمية – الحوكمة التكنولوجية – الذكاء الاصطناعي الأخلاقي .

Abstract

The contemporary world is witnessing a radical transformation driven by rapid developments in the field of Artificial Intelligence, which has become one of the most important strategic components of digital transformation and decision-making. However, this tremendous technological advancement has been accompanied by a rise in cyber threats and a diversification of attack and intrusion methods, resulting in a complex relationship between cybersecurity and artificial intelligence—one characterized by mutual influence, occasional complementarity, and at times, conflict. Problem Statement: How do artificial intelligence techniques interact with cybersecurity as both a protective tool and a potential threat?

Keywords: Cybersecurity / Artificial Intelligence/ Machine Learning / Digital Threats /Technological Governance /Ethical AI

التعاون الدولي في مكافحة التهديدات السبرانية في عصر الذكاء الاصطناعي والتحول الرقمي

أ/د .البار امين **أ/د. دني ايمان**

جامعة الشهيد الشيخ العربي التبسي – تبسة- **جامعة محمد خيضر – بسكرة –**

amine.elbar@univ.tebessa.dz **Denni.imene@univ-biskra.dz**

الملخــص

أصبح الفضاء السيبراني جزءًا لا يتجزأ من بنية الدولة والمجتمع؛ فهو يحمل فوائد اقتصادية واجتماعية وتعليمية هائلة، وفي المقابل يمثل ساحة للتحدّيات والتهديدات العابرة للحدود. مع تسارع الثورة الرقمية وظهور تطبيقات الذكاء الاصطناعي واسعة النطاق، تحول شكل التهديدات السيبرانية — فباتت الأدوات أكثر تعقيدًا وقدرة على التوسع، كما أن بعض الهجمات تتسم الآن بقدرات متقدمة مدعومة بنماذج تعلم آلي تولّد هجمات موجهة وذات تأثير واسع. لذلك لم يعد من الممكن لدولة واحدة مواجهة هذه التهديدات بمعزل عن الآخرين؛ فالتعاون الدولي صار شرطًا ضروريًا لحماية البنى التحتية الحيوية وتأمين الفضاء الرقمي، وتكمن أهمية هذا الموضوع من خلال : طابع التهديد العابر للحدود: الجرائم والهجمات السيبرانية تنتقل بسهولة بين الدول، ما يستلزم استجابات مشتركة،كذلك تعقّد الهجمات المدعومة بالذكاء الاصطناعي: أدوات المسح الآلي، التزييف العميق، وهجمات الاستهداف الذكي تزيد من الحاجة إلى تنسيق معلوماتي وتقني بين الدول، كذلك حماية البنى التحتية الحيوية والاقتصاد الرقمي: تعطل الخدمات يمكن أن يسبب خسائر اقتصادية واجتماعية جسيمة، والتعاون الدولي يقلل من احتمالات التصعيد والفساد السيبراني، كما لا ننسى الحاجة إلى أُطر قانونية وسياسات مشتركة: ضمان إنفاذ القوانين، تبادل الأدلة الرقمية، وتوحيد المعايير يتطلب آليات دولية واضحة.

الكلمات المفتاحية: الأمن السيبراني، التهديدات السيبرانية، التعاون الدولي، الذكاء الاصطناعي، التحول الرقمي، حماية البيانات، الأطر القانونية، الحوكمة الرقمية، الجرائم الإلكترونية.

Abstract

Cyberspace has become an integral part of the structure of states and societies. It offers immense economic, social, and educational benefits, yet at the same time constitutes a domain of cross-border challenges and threats. With the rapid acceleration of the digital revolution and the emergence of large-scale artificial intelligence) applications, the nature of cyber threats has evolved — tools have become more complex and scalable, and some attacks now possess advanced capabilities supported by machine learning models that generate targeted and wide-impact attacks.

Consequently, no single state can confront these threats in isolation; international cooperation has become a necessary condition for protecting critical infrastructures and securing the digital

space. The importance of this topic lies in several key aspects: The transnational nature of cyber threats: cybercrimes and attacks easily cross borders, requiring coordinated international responses. The complexity of AI-driven attacks: automated scanning tools, deepfakes, and intelligent targeting increase the need for technical and informational coordination between states. Protection of critical infrastructure and the digital economy: disruptions in digital services can cause severe economic and social losses, while international cooperation reduces the risks of escalation and cyber corruption. The need for unified legal and policy frameworks: enforcing laws, exchanging digital evidence, and harmonizing standards all require clear international mechanisms

Keywords: Cybersecurity, Cyber threats, International cooperation, Artificial Intelligence, Digital transformation, Data protection, Legal frameworks, Digital governance, Cybercrime.

التعاون الدولي و اثره في تعزيز الامن السبراني في ظل تطور تقنيات الذكاء الاصطناعي

د/بسكري منير
جامعة محمد خيضر بسكرة

Mounir.biskri@univ-biskra.dz

الملخـــص:

شهد العالم اليوم تحولاً عميقاً في بنية النظام الدولي بسبب الثورة الرقمية وتطور تكنولوجيا المعلومات، حيث أصبحت القوة لا تقتصر على القدرات العسكرية أو الاقتصادية، بل تشمل أيضاً السيطرة على البيانات والمعلومات والبنى الرقمية. في هذا الإطار، أصبح الفضاء السيبراني واحداً من أبرز ساحات التفاعل والصراع بين الدول، كونه فضاءً افتراضياً مفتوحاً تتلاقى فيه مصالح الدول والمؤسسات والأفراد. ورغم فوائده الاقتصادية والاجتماعية، فإنه أنتج تحديات غير مسبوقة تهدد الأمن القومي والاستقرار الداخلي للدول، خاصة مع تصاعد الهجمات السيبرانية والاختراقات الرقمية التي تستهدف المؤسسات الحيوية والمنشآت الاستراتيجية. أصبح الأمن السيبراني جزءاً أساسياً من الأمن الشامل في القرن الحادي والعشرين، لأنه يعتمد على تكنولوجيا معقدة لا تقيد بالحدود الجغرافية. ومع صعود الذكاء الاصطناعي كأحد أبرز الابتكارات، ازدادت فرص تقوية الأمن الرقمي عبر تقنيات التنبؤ والوقاية والتحليل الذكي، لكن التهديدات أيضاً تعقدت بسبب استخدام هذه التكنولوجيا نفسها في صنع أدوات هجومية متقدمة. لذا، برزت حاجة ملحة إلى تعاون دولي فعال يستطيع مواجهة التحديات العابرة للحدود في هذا المجال.

تنطلق الإشكالية الرئيسية لهذا البحث من التداخل المعقد بين التكنولوجيا والسياسة في الفضاء السيبراني، ومن التساؤل عن قدرة المجتمع الدولي على إنشاء آليات تعاون فعالة لمواجهة التهديدات الرقمية وسط التطورات السريعة للذكاء الاصطناعي. يمكن صياغة الإشكالية الأساسية كالتالي: إلى أي مدى يساهم التعاون الدولي في تقوية الأمن السيبراني مع التطور المتسارع لتقنيات الذكاء الاصطناعي، وما التحديات التي تعترض تحقيق أمن رقمي جماعي مستدام؟

الكلمات المفتاحية : الجريمة السيبرانية، الأمن السيبراني

Abstract

The world is currently witnessing a profound transformation in the structure of the international system as a result of the digital revolution and the advancement of information technology. Power is no longer limited to military or economic capabilities, but now also encompasses control over data, information, and digital infrastructures. Within this context, cyberspace has emerged as one of the most prominent arenas of interaction and conflict among states, as it constitutes an open virtual domain in which the interests of states, institutions, and individuals intersect. Despite its economic and social benefits, cyberspace has generated

unprecedented challenges that threaten national security and internal stability, particularly with the escalation of cyberattacks and digital intrusions targeting vital institutions and strategic facilities. Cybersecurity has thus become an integral component of comprehensive security in the twenty-first century, as it relies on complex technologies that transcend geographical boundaries. With the rise of artificial intelligence as one of the most significant contemporary innovations, opportunities to strengthen digital security have expanded through predictive, preventive, and intelligent analytical technologies. However, threats have also become more complex due to the use of the same technologies in the development of advanced offensive tools. Consequently, an urgent need has emerged for effective international cooperation capable of addressing the transnational challenges in this field.

The central research problem of this study stems from the complex interplay between technology and politics in cyberspace, and from questioning the ability of the international community to establish effective cooperation mechanisms to confront digital threats amid the rapid development of artificial intelligence. Accordingly, the main research question can be formulated as follows: To what extent does international cooperation contribute to strengthening cybersecurity in light of the accelerated evolution of artificial intelligence technologies, and what challenges hinder the achievement of sustainable collective digital security?

Key words cybercrime, cybersecurity.

جهود وأليات التعاون الدولي لتحقيق الأمن السيبراني في عصر الذكاء الاصطناعي

عبد الحي محمد **قواسمية عبد اللطيف**

جامعة عباس لغرور –خنشلة- **جامعة الشهيد الشيخ العربي التبسي – تبسة-**

mohamed.abdelhai.mae@gmail.com **gouasmiaabdelatif9@gmail.com**

الملخـــــص

يستعرض هذا الملخص الجهود الدولية الرامية إلى تعزيز الأمن السيبراني في عصر تتزايد فيه الاعتماد على النظم الرقمية وتطبيقات الذكاء الاصطناعي. يسلط الضوء على الإطار التنظيمي والمبادئ الطرفية التي توجه التعاون الدولي، بما في ذلك مسارات الأمم المتحدة مثل مجموعة الخبراء الحكوميين OEWG ومجموعة العمل المعنية بالأمن السيبراني GGE، إضافة إلى أطر تنظيمية إقليمية كـ 2NIS وEU AI Act. كما يناقش المعايير الدولية من ISO/IEC وNIST، وآليات العمل التعاوني مثل شبكات CERT/CSIRT، وبرامج بناء القدرات، والتمارين التشغيلية المشتركة، وتقييمات المخاطر المشتركة، مع مراعاة قضايا حوكمة البيانات والخصوصية والأخلاقيات. يعالج النص التحديات الناتجة عن فجوات القدرات بين الدول وتفاوت الموارد والقدرات التنظيمية، ويقترح مسارات لتعزيز الإنصاف التقني وتوسع التعاون لضمان حماية البنى التحتية الحيوية مع تعزيز الابتكار المسؤول. كما يطرح الملخّص منظوراً حول الدور المزدوج للذكاء الاصطناعي في تعزيز الدفاع السيبراني من خلال أدوات الكشف والتحليل، وفي المقابل المخاطر التي تتطلب حوكمة ورقابة فعّالة. ويناقش آفاق المستقبل نحو توحيد المعايير العالمية وتوسيع الشراكات في البحث والتطوير وتطوير أطر حوكمة AI تراعي الشفافية والخصوصية وحقوق الإنسان. الخلاصة: تعزيز الثقة في التحول الرقمي يستلزم إرادة سياسية مستمرة وتعاوناً مستداماً بين الحكومات والقطاع الخاص والمؤسسات الأكاديمية والمجتمع المدني لضمان أمن الفضاء الرقمي وتوجيه الابتكار نحو آمن ومسؤول.

الكلمات المفتاحية: الأمن السيبراني، الذكاء الاصطناعي، الجهود الدولية، التعاون الدولي.

Abstract

This abstract provides a concise overview of international efforts to strengthen cybersecurity in the AI era. It surveys policy frameworks, governance mechanisms, and international norms developed under United Nations processes such as the Open-ended Working Group (OEWG) and the Group of Governmental Experts (GGE), as well as regional initiatives like the EU's NIS2 directive and the AI Act. It also reviews global standards from ISO/IEC and NIST, and cooperative tools including CERT/CSIRT networks, capacity-building programs, joint exercises, and shared risk assessment practices, with attention to data governance and ethics. The abstract discusses challenges arising from disparities in capabilities among states, the security of AI-enabled supply chains, and governance of data privacy and ethics. It highlights opportunities to advance global cybersecurity governance through risk-based AI frameworks (e.g., NIST AI RMF),

greater transparency, and responsible innovation, while ensuring privacy and human rights protections. The paper argues for sustained political will and multi-stakeholder collaboration among governments, industry, academia, and civil society to secure critical digital infrastructure and enable safe AI-enabled innovation. Potential pathways for future policy development and research are suggested.

Keywords: cybersecurity, artificial intelligence, international efforts, international cooperation

استخدام الذكاء الاصطناعي في الامن السيبراني – حماية البنية التحتية الرقمية الامريكية وتحسين الاداء الامني

د/ رقية دهينة
جامعة باجي مختارعنابة.
reguia.deheina@univ-annaba.dz

د/ جلال قصار الليل
جامعة باجي مختارعنابة
djallel.gassarellil@univ-annaba.dz

الملخـــص

يشهد ميدان الأمن السيبراني في الولايات المتحدة تحولا نوعيا بفعل إدماج تقنيات الذكاء الاصطناعي التي أصبحت ركيزة مركزية في حماية البنية التحتية الوطنية. تتناول هذه المداخلة آليات توظيف الذكاء الاصطناعي لدعم الأنظمة الحيوية في مواجهة التهديدات الإلكترونية المتسارعة، مع التركيز على أهم تطبيقاته العملية، بما في ذلك كشف الأنماط غير المألوفة، والتحليل التنبئي، واستخبارات التهديدات، وأنظمة الاستجابة الآلية. كما تستعرض المداخلة أبرز التقنيات المستخدمة مثل (التعلم الآلي، ومعالجة اللغات الطبيعية، والشبكات العصبية)، مبيّنة دورها في رفع مستوى الصمود الرقمي وتعزيز قدرة المؤسسات على التعامل مع الهجمات المعقدة. وتبحث الدراسة في التحديات المصاحبة لهذا التوسع، خصوصا ما يتعلق بالأبعاد الأخلاقية والمخاطر الناتجة عن الاعتماد المتزايد على الأنظمة الذكية في القطاعات الحساسة.

الكلمات المفتاحية: الذكاء الاصطناعي/ الأمن السيبراني/ البنية التحتية الوطنية/ الولايات المتحدة الأمريكية.

Abstract:

The cybersecurity landscape in the United States is undergoing a significant transformation driven by the integration of artificial intelligence technologies, which have become a central pillar in protecting national digital infrastructure. This paper examines how AI is employed to support critical systems in the face of rapidly evolving cyber threats, highlighting key practical applications such as anomaly detection, predictive analytics, threat intelligence, and automated response mechanisms. The study also reviews prominent AI-based techniques used in the United States, including machine learning, natural language processing, and neural networks, showing how they contribute to strengthening digital resilience and enhancing institutional capabilities to counter sophisticated attacks. At the same time, it assesses the challenges associated with this expansion, particularly ethical considerations and the risks linked to growing reliance on intelligent systems in sensitive sectors.

Keywords: artificial intelligence, cybersecurity, national infrastructure, United States.

فعالية المنظومة القانونية الجزائرية في مكافحة الجريمة

ط/د . بن ذيب تقوى **غنيات عامر**

جامعة الشهيد الشيخ العربي التبسي- تبسة - **جامعة الشهيد الشيخ العربي التبسي- تبسة -**

takwa.bendib@univ-tebessa.dz **ameurdroit5@gmail.com**

الملخـــص

برزت في العصر الحديث نوعية جديدة من الجرائم اختلفت عن الجرائم التقليدية، تميزت بخطورتها العالية وصعوبة إثباتها، لا سيما في ظل التطور المبكر للأمن المعلوماتي. فقد سجّلت مؤخرًا العديد من حالات اختراق البيانات الشخصية واستهداف قواعد البيانات الوطنية، ما شكل تهديدًا مباشرًا للأمن القومي. وقد استدعى هذا الوضع تطوير آليات لمواجهة الجريمة الإلكترونية، لا سيما عبر منصات التواصل، مع التركيز على استراتيجيات الحماية المعلوماتية، أو ما يُعرف بالأمن السيبراني، ودوره في الحد من التجاوزات والممارسات الإجرامية المرتبطة بتكنولوجيا الاتصال. وفي هذا الإطار، تسعى الجزائر إلى تحديث تشريعاتها الجنائية وأنظمتها القانونية لمواجهة التحديات الناشئة عن الجرائم الإلكترونية، مع تطوير آليات فعّالة تشمل التدريب المستمر للقوات الأمنية وتعزيز التعاون بين الجهات المختصة على الصعيدين الداخلي والدولي. وتهدف هذه الورقة البحثية إلى تقديم استعراض شامل للآليات التي اعتمدتها الجزائر لمكافحة الجرائم السيبرانية، وفقًا للتشريعات المعمول بها، مع تحليل القوانين ذات الصلة وكيفية تطبيقها عمليًا ومدى فعاليتها، بالإضافة إلى دراسة دور مختلف الجهات المعنية في البحث والتحري ومكافحة الجريمة السيبرانية.

الكلمات المفتاحية: الجريمة السيبرانية، الأمن السيبراني، التشريعات الجزائرية، حماية البيانات.

Abstract

In the modern era, a new type of crime has emerged that differs from traditional crimes. It is characterized by its high seriousness and difficulty in proving, especially in light of the early development of information security. Several cases of personal data breaches and targeting of national databases have recently been recorded, posing a direct threat to national security. This situation has necessitated the development of mechanisms to combat cybercrime, particularly through social media platforms, with a focus on information protection strategies, or what is known as cybersecurity, and its role in reducing abuses and criminal practices related to communication technology. In this context, Algeria seeks to modernize its criminal legislation and legal systems to address the challenges arising from cybercrimes, while developing effective mechanisms that include continuous training of security forces and enhancing cooperation between competent authorities at the domestic and international levels. This research paper aims to provide a comprehensive review of the mechanisms adopted by Algeria to combat

cybercrime, in accordance with applicable legislation, analyzing the relevant laws, how they are applied in practice and their effectiveness, in addition to studying the role of the various parties concerned in researching, investigating and combating cybercrime.

Keywords: cybercrime, cybersecurity, Algerian legislation, data protection.

دورالتقنيات الذكية في كشف الهجمات السبرانية المتقدمة

د/ شيباني ايناس
جامعة الشهيد الشيخ العربي التبسي – تبسة
Ines.chibani@univ-tebessa.dz

أ/د قادري مليكة
جامعة الشهيد الشيخ العربي التبسي - تبسة
Malika.kadri@univ-tebessa.dz

الملخــص

يشكل الأمن السيبراني ركيزة أساسية لاستقرار الدول وحماية بنيتها التحتية الحيوية من الهجمات المتقدمة المستمرة (APT)، وهي هجمات مخططة بدقة وتتكيف مع أساليب الدفاع التقليدية. في هذا الإطار، أصبحت التقنيات الذكية مثل التعلم الآلي والتعلم العميق أدوات استراتيجية تمكن الدول من كشف الهجمات والتصدي لها بسرعة ودقة أكبر، بما يعزز قدرتها على اتخاذ قرارات استباقية واستراتيجية لحماية مصالحها الوطنية في الفضاء الرقمي..

الكلمات المفتاحية : الهجمات المتقدمة- التقنيات الذكية – الامن السبراني

Abstract:

Cybersecurity constitutes a fundamental pillar for the stability of states and the protection of their critical infrastructure against advanced persistent threats (APTs), which are highly sophisticated attacks capable of adapting to traditional defense mechanisms. In this context, intelligent technologies, such as machine learning and deep learning, have become strategic tools enabling states to detect and respond to attacks with greater speed and accuracy, thereby enhancing their capacity to make proactive and strategic decisions to safeguard national interests in the digital domain.

Keywords: Advanced Attacks / Intelligent Technologies / Cybersecurit

.

المخاطر السيبرانية والأمن القانوني في المجتمع الرقمي

د/بوجوراف فهيم
جامعة الشهيد الشيخ العربي التبسي – تبسة-
fahim.boudjouraf@univtebessa.dz

أ/د جبيري ياسين
جامعة الشهيد الشيخ العربي التبسي- تبسة-
yacine@univ-tebessa.dz.djebiri

الملخـــــص:

تتضمن بيئة المعلومات وتكنولوجيا المعلومات والاتصال العديد من التهديدات التي تمس بأمن المجتمع الرقمي، فقد أدى النقل السريع والعشوائي للبيانات الخاصة بالأفراد والمجتمعات للعالم الافتراضي إلى جعل أمنهم المجتمعي والهويات محل تهديد دائم، و يعاني في هذا الإطار المجتمع الجزائري من التبعات السلبية للانكشاف الرقمي والاستخدام العشوائي لمنصات التواصل الاجتماعي التي تمس قيمه الأساسية و تغير في الكثير من الأحيان ثوابته الأصلية، كما تخلق أيضا العديد من المشاكل النفسية داخل المجتمع بفعل غياب عنصري الرقابة والردع. تأتي هذه المداخلة للبحث في مضامين التهديدات السيبرانية وأمن المجتمع الرقمي في الجزائر، وذلك عبر التطرق في المحور الأول إلى المقصود من التهديدات السيبرانية وأشكالها، ثم في المحور الثاني إلى مخاطر انتهاك الخصوصية الرقمية وتبعاته على أمن المجتمع الرقمي ، وكذا مخاطر استخدام الفضاء السيبيراني في الترويج للتطرف، والفبركة الرقمية في البيئة السيبرانية.

الكلمات المفتاحية: التهديدات السيبرانية؛ الأمن؛ المجتمع الرقمي؛ الخصوصية الرقمية

Abstract

The information and communication technology environment includes many threats that affect the security of the digital society. The rapid and random transfer of data belonging to individuals and communities to the virtual world has made their community security and identities constantly under threat, in this context, Algerian society suffers from the negative consequences of digital exposure and the indiscriminate use of social media platforms, which affect its fundamental values and often change its original principles. It also creates many psychological problems within society due to the absence of the elements of control and deterrence. This intervention aims to explore the implications of cyber threats and the security of the digital society in Algeria, by addressing in the first section the meaning and forms of cyber threats, and then in the second section the risks of violating digital privacy and its consequences for the security of the digital community, as well as the risks of using cyberspace to promote extremism and digital fabrication in the cyber environment.

Keyword : Cyber threats; security; digital society; digital privacy

الآليات الوطنية لمواجهة التهديدات السيبرانية في الجزائر في ظل التحديات التكنولوجية الراهنة

د/منصوري نورة

جامعة الشهيد الشيخ العربي التبسي – تبسة-

mansourinora72@gmail.com

الملخـــــــص:

يشهد الفضاء السيبراني في الجزائر تنامياً متسارعاً للتهديدات الرقمية بفعل التطـور التكنولوجي الهـائل واتساع استخدام الأنظمة المعلوماتية في مختلف القطاعات الحيوية. وقد دفع هذا الواقع الدولة الجزائريـة إلى تبنّي جملة من الآليات التشريعية والمؤسساتية والتقنية بهدف تعزيـز الأمـن السيبـــراني وحمايـة المنظومات الرقمية من الهجمات والتسللات. تهدف هذه المداخلة إلى إبراز أبرز هذه الآليات من خلال تحليل الإطار القانوني الوطني، لاسيما القانون 18-04 المتعلق بالأمـن السيبراني، وهيئات الحمايـة واليقظة مثل الهيئة الوطنية للأمن السيبرانـي، إضافةـً إلى الاستراتيجيات الوطنيـة وبرامج التحسيس والتكوين. وتخلص الدراسة إلى أنّ تعزيز الأمـن السيبراني فـي الجزائـر يقتضي تطوير البنية التحتية الرقمية، وتكثيف التنسيق بين المؤسسات، وتعزيز القدرات البشرية، والانتقال نحو منظومة شاملة لحوكمة الفضاء السيبراني بما يواكب التحديات التكنولوجية الراهنة.

الكلمات المفتاحية: الأمن السيبراني/التهديدات السيبرانية / التشريعات / الحوكمة الرقمية / حماية البيانات/ التحول الرقمي.

Abstract:

Algeria's cyberspace is witnessing a rapid escalation of digital threats due to major technological advances and the growing reliance on information systems across vital sectors. This reality has prompted the Algerian state to adopt a set of legislative, institutional, and technical mechanisms aimed at strengthening cybersecurity and protecting digital infrastructures from intrusions and attacks. This paper seeks to highlight these mechanisms by analyzing the national legal framework particularly Law 18-04 on cybersecurity the roles of national protection and monitoring bodies such as the National Cybersecurity Authority, in addition to national strategies, awareness programs, and capacity-building initiatives. The study concludes that enhancing cybersecurity in Algeria requires developing digital infrastructure, improving inter-institutional coordination, strengthening human and adopting an integrated governance system capable of addressing current technological challenges.

Keywords :Cybersecurity / Cyber threats / Legislation/ Digital governance / Data protection Digital transformation.

الذكاء الاصطناعي في الأمن القضائي البريطاني: دراسة تقييمية لتطبيقات التعرف الوجهي وتقييم المخاطر الجنائية

د/ تقي مباركية
جامعة الشهيد الشيخ العربي التبسي –تبسة-
takki.mebarkia@univ-tebessa.dz

د/ سعاد مباركية
جامعـــــــة ام البواقي
mebarkia.souad@univ-oeb.dz

الملخـــص

تدرس هذه المداخلة التجربة البريطانية في استخدام الذكاء الاصطناعي عبر تطبيقين رئيسيين: تقنية التعرف الوجهي الحي التي أسفرت عن أكثر من 1400 توقيف منذ إطلاقها، ونظام تقييم المخاطر الجنائية OASys الذي يُجري أكثر من 1300 تقييما يومياً رغم الكفاءة التقنية العالية (معدل دقة 99.9997%)، كشفت الدراسات الرسمية عن تحيز عنصري واضح في النظام خاصة ضد الأقليات السوداء والآسيوية، وانتهاكات خصوصية جسيمة حيث تم مسح قرابة مليوني شخص دون علمهم. يسود الفراغ التشريعي الحالة البريطانية، إذ لا يوجد تشريع ملزم يحكم استخدام الذكاء الاصطناعي في الإجراءات الجنائية حتى سبتمبر ل تُعتمد مبادئ توجيهية غير ملزمة. تستخلص الدراسة أن التجربة البريطانية تعكس توتراً محورياً بين الكفاءة الأمنية وحماية الحقوق الأساسية، وتوصي بضرورة إقرار إطار تشريعي قبل التطبيق، واختبارات إلزامية للتحيز، ورقابة مستقلة عند تبني تقنيات مماثلة في السياق الجزائري.

الكلمات المفتاحية: التعرف الوجهي الحي؛ نظامOASys؛ التحيز الخوارزمي؛ الفراغ التشريعي؛ حقوق الإنسان.

Abstract:

This paper examines the British experience in deploying artificial intelligence through two principal mechanisms: Live Facial Recognition technology, which has resulted in over 1,400 arrests since implementation, and the OASys criminal risk assessment system, which conducts more than 1,300 evaluations daily. Despite exceptional technical accuracy (99.9997%), official studies have revealed pronounced racial bias particularly against Black and Asian minorities, and severe privacy violations affecting nearly two million individuals scanned without consent. The British framework suffers from acute legislative vacuums: as of September 2025, no binding statutory regulations govern AI use in criminal proceedings, relying instead on non-binding professional guidelines. The study concludes that the British experience exemplifies a fundamental tension between operational security efficiency and fundamental rights protection, and recommends that prior enactment of comprehensive legislation, mandatory

algorithmic bias testing, and independent regulatory oversight must precede any similar deployment within the Algerian context.

Keywords: Live Facial Recognition; OASys System; Algorithmic Bias; Legislative Gap; Human Rights.

توظيف تقنيات الذكاء الاصطناعي في حماية الفضاء السيبراني -دراسة حالة مواقع التواصل الاجتماعي-

د/احمد الحمزة
جامعة الشيخ الشهيد العربي التبسي –تبسة-
ahmed.elhamza@univ-tebessa.dz

د/ تسعديت مسيح الدين
المدرسة الوطنية العليا للعلوم السياسية- الجزائر
djamilam.78@gmail.com

الملخـــــص

تشكل الهجمات الإلكترونية على منصات التواصل الاجتماعي تهديداً متطوراً للخصوصية والأمن الوطني والمصلحة العامة. ومنه تهدف هذه المداخلة إلى استقصاء دور تقنيات الذكاء الاصطناعي في تعزيز أمن الفضاء السيبراني لهذه المنصات، مع التركيز على التحليل العملي للتحديات والفرص.، حيث تمكن تقنيات مثل التعلم الآلي ومعالجة اللغة الطبيعية من مراقبة منصات التواصل الاجتماعي بكفاءة عالية، للكشف عن التهديدات كالتصيد الاحتيالي والمحتوى الضار والهجمات المنسقة، والاستجابة لها تلقائيًا وبشكل استباقي. ومع ذلك، يواجه هذا التوظيف تحديات مثل الحاجة إلى بيانات تدريب عالية الجودة مع الحفاظ على خصوصية المستخدمين، ومخاطر الإنذارات الكاذبة، مما يستلزم وجود إشراف بشري مستمر وأطر أخلاقية راسخة لضمان تحقيق التوازن الأمثل بين الأمن والكفاءة في حماية المنصات الرقمية**الكلمات المفتاحية** : الذكاء الاصطناعي، مواقع التواصل الاجتماعي، الهجمات الالكترونية، تنظيم البيانات وحمايتها.

Abstract

Cyber attacks on social media platforms pose an evolving threat to privacy, national security, and the public interest. Hence, this paper aims to explore the role of artificial intelligence techniques in enhancing the cybersecurity of these platforms, focusing on a practical analysis of challenges and opportunities. Technologies such as machine learning and natural language processing enable efficient monitoring of social media platforms to detect threats like phishing, harmful content, and coordinated attacks, responding automatically and proactively. However, this implementation faces challenges, such as the need for high-quality training data while maintaining user privacy, and the risks of false alarms, necessitating continuous human oversight and robust ethical frameworks to ensure an optimal balance between security and efficiency in protecting digital platforms.

Keywords: artificial intelligence, social media, cyber attacks, data regulation and protection.

الذكاء الاصطناعي كالية استراتيجية لتعزيز الأمن السيبراني

ط/د. نجود طراد

جامعة الشيخ العربي التبسي – تبسة.

noujoud.trad@univ-tebessa.dz

الملخـــص

إن ظاهرة التهديدات السيبرانية تعد مختلفة عن طبيعة التهديدات التقليدية ، وتشكل خطرا يهدد أمن الأفراد والدول على حد سواء ، ومع ظهور الثورة التكنولوجية ، برز الذكاء الاصطناعي كتقنية غزت جميع المجالات بما في ذلك الأمن السيبراني . وعليه جاءت هذه الدراسة لتوضيح دور الذكاء الاصطناعي في تعزيز الأمن السيبراني وذلك من خلال ضرورة الاسراع في اعتماد التشريعات المتعلقة بالاستخدامات المختلفة لتكنولوجيا الذكاء الاصطناعي ، من أجل حماية الخصوصية والحفاظ عليها.

الكلمات المفتاحية : الأمن السيبراني / الذكاء الاصطناعي/ تعزيز الحماية .

Abstract

The phenomenon of cyber threats is different from the nature of traditional threats, and poses a threat to the security of individuals an countries alike. With the emergence of the technological revolution, artificial intelligence has emerged as a technology that has invaded all fields, including cybersecurity Accordingly, this study came to clarify the role of artificial intelligence in enhancing cybersecurity, through the necessity of accelerating the adoption of legislation related to the various uses of artificial intelligence technology, in order to protect and preserve privacy

Keywords: cybersecurity, artificial intelligence, enhanced protection

دور الذكاء الاصطناعي في تعزيز استدامة الأمن السيبراني للمؤسسات الحيوية في الجزائر: مقاربة تشريعية وتقنية

أ/ بورزق علاء الدين

جامعة التكوين المتواصل مركز–تبسة-

bourezgallaeddine5@gmail.com

الملخـــــص

يمثل الأمن السيبراني في عصر الرقمنة والإنترنت حجر الزاوية لاستقرار المؤسسات الحيوية، خاصة مع تزايد وتطور الهجمات السيبرانية التي تستهدف قواعد البيانات والبنى التحتية الوطنية. تأتي هذه المداخلة لتسليط الضوء على الإمكانات الثورية لتقنيات الذكاء الاصطناعي (AI) كأداة مزدوجة، فهي من جهة تمثل تحدياً جديداً يغذي الهجمات المتقدمة (كالخوارزميات الذكية للاختراق)، ومن جهة أخرى، تمثل خط دفاع استراتيجي قادر على اكتشاف الشذوذات، وتحليل التهديدات في الوقت الحقيقي، والتنبؤ بالهجمات المستقبلية بكفاءة تفوق الوسائل التقليدية. تهدف هذه الدراسة إلى تقديم تقييم نقدي لمدى استعداد المؤسسات الحيوية في الجزائر لدمج حلول الذكاء الاصطناعي في إستراتيجياتها الأمنية، مع التركيز على الموازنة بين الأبعاد التقنية والتنظيمية/التشريعية. تتناول المداخلة أهمية وضع إطار قانوني واضح يُمكن من الاستخدام الآمن والأخلاقي للذكاء الاصطناعي في عمليات المراقبة والتحليل الأمني (بما يضمن حماية الخصوصية والبيانات الشخصية)، إلى جانب تحديد أهم المتطلبات التقنية والبشرية اللازمة لتحويل هذه الإمكانات إلى واقع عملي.

الكلمات المفتاحية: الأمن السيبراني، الذكاء الاصطناعي، المؤسسات الحيوية، الإطار التشريعي، حماية البيانات، استدامة الأمن.

Abstract

In the age of digitalization and the internet, cybersecurity represents the cornerstone for the stability of critical infrastructure, especiall with the escalation and evolution of cyberattacks targeting national databases and infrastructure. This intervention aims to shed light on the revolutionary potential of Artificial Intelligence (AI) technologies as a double-edged sword. On one hand, AI presents a new challenge by fueling advanced attacks (such as smart exploitation algorithms), and on the other hand, it serves as a strategic defense line capable of real-time anomaly detection, threat analysis, and prediction of future attacks with efficiency that surpasses traditional methods. This study intends to provide a critical assessment of the readiness of Algerian critical institutions to integrate AI solutions into their

security strategies, focusing on balancing the technical and regulatory/legislative dimensions. The paper discusses the importance of establishing a clear legal framework that enables the safe and ethical use of AI in security monitoring and analysis operations (thereby ensuring the protection of privacy and personal data), in addition to defining the necessary technical and human requirements to translate these potentials into practical reality.

Keywords cybersecurity, Artificial Intelligence, Critical Institutions, Legislative Framework, Data Protection, Security Sustainability

التحصين ضد الهجمات الذكية: تحليل تحديات الأمن السيبراني المعتمد على الذكاء الاصطناعي.

د/ لبيوض أسماء

جامعة الشهيد الشيخ العربي التبسي- تبسة

Asmaa. labiod@univ-tebessa.dz

الملخـــص

يمثل تقاطع الأمن السيبراني والذكاء الاصطناعي تحدياً حاسماً، حيث يُستخدم من قبل المهاجمين لشن "هجمات ذكية" متطورة وقادرة على التكيف والتعلم، مما يتجاوز قدرة أنظمة الدفاع التقليدية. التحصين الفعال ضد هذه التهديدات يتطلب الانتقال إلى نموذج دفاعي يعتمد أيضاً على تقنيات الذكاء الاصطناعي والتعلم الآلي، مع التركيز على مرونة الأنظمة، وحماية البيانات المُدرّبة، واستخدام نماذج قابلة للتفسير لمواجهة التهديدات الجديدة والمتغيرة باستمرار.

الكلمات المفتاحية: الامن السيبراني، الذكاء الاصطناعي، تحديات، التحصين، حماية البيانات

Abstract:

The intersection of Cybersecurity and Artificial Intelligence (AI) represents a critical challenge, as AI is utilized by attackers to launch sophisticated "intelligent attacks" that are adaptable and capable of learning, thus surpassing the capabilities of traditional defense systems. Effectiv immunization against these threats requires a shift toward a defense model that also relies on AI and Machine Learning techniques, focusing on system resilience, protecting training data, and using interpretable models to confront new and constantly evolving threats.

Keywords: Cybersecurity.Artificial Intelligence. Challenges. Defense. Data Protection

متطلبات الأمن الوطني في عصر الذكاء الاصطناعي: الفرص والتحديات

د/ هاني غنية
جامعة الشهيد الشيخ العربي التبسي – تبسة-
Hhani8@gmail.com

الملخـــــص

يشهد مفهوم الأمن الوطني تحولاً جوهرياً في ظل الثورة التقنية التي يقودها الذكاء الاصطناعي، حيث لم تعد التهديدات تقتصر على الجوانب العسكرية التقليدية، بل امتدت لتشمل الفضاء السيبراني والأمن الاقتصادي والاستقرار الاجتماعي. ى جانب ذلك، يتطلب الأمن في هذا العصر تطوير قدرات المؤسسات من خلال تدريب الكوادر المتخصصة، ورفع وعي المستخدمين النهائيين بمخاطر الهجمات الرقمية، مع اعتماد استراتيجيات مرنة قابلة للتكيف مع التحديات المستقبلية لضمان حماية مستمرة وفعّالة. تقدم هذه الورقة تحليلاً شاملاً للمتطلبات الجديدة للأمن الوطني في هذا العصر، من حيث الفرص والتحديات.

الكلمات المفتاحية: الامن الوطني/ الذكاء الاصطناعي .

Abstract

The concept of national security is undergoing a fundamental transformation in the context of the technological revolution driven by artificial intelligence. Threats are no longer confined to traditional military domains but have expanded to include cyberspace, economic security, and social stability. In this era, ensuring security requires enhancing institutional capacities through the training of specialized personnel, raising end-users' awareness of digital threats, and adopting flexible strategies capable of adapting to future challenges to guarantee continuous and effective protection. This paper provides a comprehensive analysis of the new requirements for national security in this era, highlighting both opportunities and challenges.

Keywords : national security/ economic security.

الدليل الرقمي في الجرائم السيبرانية

د/ حملة عبد الرحمن

جامعة الشهيد الشيخ العربي التبسي – تبسة -

abderrahmane.hamla@univ-tebessa.dz

الملخـــص

يثور بصدد اثبات الجرائم السيبرانية العديد من الاشكالات القانونية والواقعية باعتبارها صورة من صور الجريمة المعلوماتية التي ترتكب في الفضاء الالكتروني – بيئة افتراضية – التي تختلف عن البيئة الطبيعية التي يسهل فيها تجميع أدلة الجريمة وتتبع أثارها . الامر الذي يؤدي إلى حتمية البحث عن أدلة تتناسب مع الطبيعة التقنية للجرائم الافتراضية التي نجد يصددها القاضي ملزما بالاستعداد لتقبل الدليل المستمد من الحاسوب أو الهاتف الخاص ، خاصة في ظل كفالة النصوص القانونية في الدولة لمبدأ حرية الاثبات الذي يعطي للقاضي حرية كاملة في تكوين قناعته في المواد الجنائية . وللإلمام بعناصر موضوع الدليل الرقمي وما يثيره من اشكالات قانونية في المواد الجنائية نتناول في هذه الورقة البحثية ما يلي :

أولا : تعريف الدليل الرقمي والخصائص المميزة له.

ثانيا : معوقات اكتشاف الدليل الرقمي

ثالثا : أنواع الأدلة الرقمية

رابعا : حجية الدليل الرقمي في الاثبات

الكلمات المفتاحية : الهجمات السيبرانية الذكية، الذكاء الاصطناع، الأمن السيبراني

Abstract

The proof of cybercrimes raises numerous legal and practical challenges, as they represent a form of computer crime committed in cyberspace—a virtual environment—which differs from the natural environment where collecting crime evidence and tracing its effects is easier. This necessitates the search for evidence appropriate to the technical nature of virtual crimes, whereby judges are obliged to be prepared to accept evidence derived from computers or private phones, particularly in light of legal provisions that guarantee the principle of freedom of proof, which grants judges complete freedom in forming their conviction in criminal matters.

To comprehensively address the elements of digital evidence and the legal challenges it poses in criminal matters, this research paper examines the following:

First: Definition of digital evidence and its distinctive characteristics.

- **Second:** Obstacles to discovering digital evidence.
- **Third:**Typesofdigitalevidence.
- **Fourth:**The evidential value of digital evidence in proo.

Keywords Smart Cyberattacks, Artificial Intelligence, , Cybersecurity

الوكالة الوطنية لأمن نظم المعلومات (ANSSI) ركيزة الاستراتيجية الوطنية للأمن السيبراني في الجزائر

د/ مريم عثمانية
جامعة الشهيد الشيخ العربي التبسي –تبسة-
mariemathamnia@yahoo.fr

د/زايدي حميدة
جامعة الشهيد الشيخ العربي التبسي –تبسة-
hamidazaidi2002@gmail.com

الملخـــــص

في عصر التحول الرقمي والتزايد المطرد للتهديدات الالكترونية، أصبح إنشاء هيئات وطنية متخصصة أمرا حيويا، في هذا الإطار تأتي الوكالة الوطنية لأمن نظم المعلومات في الجزائر كهيئة سيادية استراتيجية، تم إنشاؤها بموجب المرسوم الرئاسي رقم 22- 248 المؤرخ في 05 يوليو 2022، لتمثل الإرادة السياسية الراسخة للدولة في حماية فضاءها الرقمي وبناء سيادتها الإلكترونية. ومع إنشاء هذه الوكالة أظهرت الجزائر خطوة مهمة نحوتأسيس هيكل حكومي مركزي وفعال. ومن خلال هذه المداخلة سنحاول التعرف على النظام القانوني لهذه الوكالة ودورها في مجال الأمن السيبراني وحماية الفضاء الرقمي والسيادة الإلكترونية للدولة من خلال النظام القانوني الخاص.

الكلمات المفتاحية: الامن السيبراني، الذكاء الاصطناعي، تحديات، حماية البيانات

Abstract

In the era of digital transformation and the steady increase of cyber threats, the establishment of specialized national bodies has become vital. In this context, the National Agency for Information Systems Security in Algeria emerges as a strategic sovereign entity, established by Presidential Decree No. 22-248 dated July 5, 2022, representing the state's firm political will to protect its digital space and build its electronic sovereignty. With the creation of this agency, Algeria has taken an important step towards establishing a central and effective government structure. Through this presentation, we will attempt to understand the legal framework of this agency and its role in the field of cyber security, protecting the digital space, and the state's electronic sovereignty through its specific legal system.

Keywords: Cybersecurity/. Artificial Intelligence/ Data Protection

دورالذكاء الاصطناعي في تحول موازين القوى في النظام الدولي

د/ محمود دريــدي
جامعة الشيخ العربي التبسي-تبسة-
dridi.mahmoud@univ-tebessa.dz

د/ عمر سعداوي
جامعة امحمد بوقرة -يومرداس- الجزائر
a.saadaoui@univ-boumerdes.dz

الملخـــص

برز مجال الذكاء الاصطناعي قطاعًا قائدًا لتحولات جوهرية في العالم، تشمل حقل العلاقات الدولية، والمفاهيم الأساسية المتعارف عليها للعلاقات بين الدول. من المتوقع أن تحصل انعطافات حادة في النظام الدولي، تشمل تأثيراتها الأفراد والدول، على حدٍّ سواء، ويمتد هذا التأثير إلى مفاهيم وقواعد مثل سيادة الدولة، والديمقراطية، والدولة الحارسة. كما يشهد تحولات في مفاهيم القوة والأمن، وترتيب مكانة الدول في العالم، وسيكون من بين نتائج هذه النتيجة، أن تتحدد قوة الدولة، بمقدار تمكنها من إنتاج إمكانات الذكاء الاصطناعي، واستخدامها لتعويض ضعف عوامل الأمن القومي الأساسية فيها، ويفسر هذا السباق الحالي للسيطرة على موارد وقدرات التطور في حقل الذكاء الاصطناعي بين الدول الكبرى. و عليه يمكن في هذا الصدد معالجة النقاط التالية:

1/ مقدمة

2/ الذكاء الاصطناعي كفاعل مستجد في العلاقات الدولية

3/ تأثير الذكاء الاصطناعي على سيادة الدولة

4/ تحول القوة في موازين العلاقات الدولية في ظل مفاعيل الذكاء الاصطناعي

ABSTRACT

The proof of cybercrimes raises numerous legal and practical challenges, as they represent a form of computer crime committed in cyberspace a virtual environment which differs from the natural environment where collecting crime evidence and tracing its effects is easier. This necessitates the search for evidence appropriate to the technical nature of virtual crimes, whereby judges are obliged to be prepared to accept evidence derived from computers or private phones, particularly in light of legal provisions that guarantee the principle of freedom of proof, which grants judges complete freedom in forming their conviction in criminal matters. To comprehensively address the elements of digital evidence and the legal challenges it poses in criminal matters, this research paper examines the following:

- **First:** Definition of digital evidence and its distinctive characteristics.

- **Second:** Obstacles to discovering digital evidence.
- **Third:**Typesofdigitalevidence.
- **Fourth:**The evidential value of digital evidence in proo.

الاتفاقيات الدولية لمكافحة الجرائم السبرانية

د/ موسى عائشة

جامعة الشهيد الشيخ العربي التبسي- تبسة -

aicham0667@gmail.com

الملخـــــص

تعتبر الجرائم السيبرانية من الجرائم الحديثة نسبيا، تتعلق أساسا بالاعتداء على بيانات الكترونية، و تتميز هذه الاخيرة بانها من الجرائم العابرة للحدود الإقليمية للدول مما أدى إلى توجه المجتمع الدولي للتعاون من أجل التصدي لتلك الجرائم ، ذلك لمساسها بالأمن القومي للدول في جميع النواحي، لذلك سعت الدول إلى اتخاذ إجراءات مشتركة للتصدي لتلك الجرائم، وذلك من خلال إبرام اتفاقيات ومواثيق دولية لمواجهة تلك الجرائم والعمل على محاربتها خاصة جهود الأمم المتحدة، منها اتفاقية الأمم المتحدة لمكافحة الجرائم السيبرانية، واتفاقية بودابست لمكافحة الجرائم السيبرانية، وإتفاقية جامعة الدول العربية وكذلك الاتفاقيات الثنائية والمتعددة لتسليم المجرمين، والتي تعد من أهم أساليب مكافحة تلك الجرائم نظرا لما تتمتع به تلك الجريمة من خاصية اللاحدودية.

الكلمات المفتاحية : اتفاقيات دولية - جرائم سيبرانية- تعاون دولي

Abstract

Cybercrime is a relatively new crime, mainly involving attacks on electronic data. and are characterized by the fact that they transcend national borders, which has led the international community to cooperate in order to combat these crimes, as they affect the national security of states in all respects. Therefore, states have sought to take joint measures to combat these crimes by concluding international agreements and conventions to confront these crimes and work to combat them, particularly through the efforts of the United Nations, including the United Nations Convention on Cybercrime and the Budapest Convention on Cybercrime.The Arab League Convention, as well as bilateral and multilateral agreements on extradition, are among the most important methods of combating these crimes, given their borderless nature.

Keywords: international agreements, cybercrime, international cooperation.

دورالامن السبراني في حماية المعطيات والبيانات ذات الطابع الشخصي

أ/ د بخوش هشام
جامعة الشريف مساعدية – سوق أهراس
h.bekhouche@univ-soukahras.dz

الملخـــص

نظرا لأهمية وحجم البيانات التي يتم جمعها وتخزينها ومعالجتها إلكترونيان، وخطورة الاعتداء عليها، أصبح من الضروري إيجاد آليات قانونية فعالة لتوفير الحماية القانونية لهذه البيانات. وتظهر أهمية الحماية من خلال الجرائم الإلكترونية والاختراقات التي تقع على بنوك المعلومات، مسببة العديد من الانتهاكات والابتزاز. الأمر الذي استوجب سن قواعد خاصة بهذا المجال مثل اللائحة الأوروبية لحماية البياناتGDPR ، وقوانين عربية أخرى تفرض على الجهات المعالجة للبيانات مجموعة من الالتزامات القانونية الصارمة. على غرار القانون 18-07 الذي أنشأ من خلاله المشرع الجزائري السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، إضافة إلى 25/11 وتهدف هذه الدراسة إلى تقييم المنظومة التشريعية الوطنية المتعلقة بامن المعطيات الشخصية.

الكلمات المفتاحية: أمن المعطيات الشخصية -الأمن المعلوماتي- البيانات الشخصية -الفضاء الالكتروني،

Abstract

Given the importance and volume of data that is collected, stored, and processed electronically, and the seriousness of attacks on it, it has become necessary to establish effective legal mechanisms to provide legal protection for this data. The importance of protection is evident in the cybercrimes and breaches that occur in information banks, causing numerous violations and extortion. This has necessitated the enactment of specific rules in this area, such as the European General Data Protection Regulation (GDPR) and other Arab laws that impose a set of strict legal obligations on data processors. Similar to Law 18-07, through which the Algerian legislature established the National Authority for the Protection of Personal Data, in addition to Law 11/25, this study aims to evaluate the national legislative system related to personal data security.

Keywords Personal data security - Information security - Personal data - Cyberspace Abstract

الجهود الدولية لتحقيق الأمن السيبراني في عصر تكنولوجيا المعلومات والذكاء الاصطناعي

ط/د بلحسن عبد المالك

جامعة محمد الشريف مساعدية- سوق اهراس -

a.belahcene@univ-soukahras.dz

الملخـــــص

إن صياغة اتفاق عالمي ملزم قانونًا لتحديد أهم القواعد التي يجب اتباعها في الفضاء السيبراني، لحمايته من مخاطر ثورة نظم الذكاء الاصطناعي المتسارعة ، وتوضيح عواقب عدم الامتثال أمرًا مغريًا، ومع ذلك، لا يبدوا في الوقت الحالي أنه يقع على الإطلاق ضمن حدود الممكن، ويعود هذا لعدة أسباب، من أهمها أن المجال يتطور بسرعة كبيرة مما يجعل من المستحيل تقريبًا الاتفاق على مجموعة شاملة ومستدامة من القواعد الخاصة بهذا المجال ، والتي تضمن حماية مستدامه للأمن السيبراني الدولي. وعلى الرغم من أن الاتفاق على رؤية موحدة للأمن السيبراني لم يتم بعد، فقد ظهرت بوادر جديدة مشتركة في عمل كيانات دولية تسلط الضوء على طغيان الأمن السيبراني كأولوية عالمية للتعاون الدولي في الوقت الحالي.

الكلمات المفتاحية: الأمن السيبراني، الذكاء الاصطناعي، الاتفاقيات الدولية، التعاون الدولي.

Abstract

Perhaps drafting a legally binding global agreement to identify the most important rules to follow in cyberspace to protect it from the risks of the rapidly accelerating artificial intelligence revolution, explaining the consequences of non-compliance is tempting, however, It does not seem at the moment to be within the realm of possibility at all, this is due to several reasons, One of the most important aspects is that the field is evolving so rapidly that it is almost impossible to reach a consensus A comprehensive and sustainable set of rules specific to this field, which ensures sustainable protection of international cybersecurity. Despite, agreement on a unified vision for cybersecurity has not yet been reached. new commonalities have emerged in the work of international entities. highlights the dominance of cybersecurity as a global priority for international cooperation at the moment.

Keywords: Cybersecurity, Artificial Intelligence, International Agreements, International Cooperation.

مخاطر الذكاء الاصطناعي على الخصوصية والأمن الشخصي

أ/د.نبيلة أحمد بومعزة

جامعة الشهيد الشيخ العربي التبسي – تبسة

Nabila.boumaza@univ-tebessa.dz

الملخـــص

أدى التطور المتسارع لتقنيات الذكاء الاصطناعي إلى إحداث تحولات عميقة في مختلف مجالات الحياة، حيث أصبح الاعتماد على الأنظمة الذكية عنصرًا أساسيًا في تحسين الأداء، ترشيد القرارات، وتقديم خدمات أكثر كفاءة. غير أن هذا التقدم التكنولوجي، ورغم ما يحمله من فوائد كبيرة، أفرز تحديات قانونية وأخلاقية غير مسبوقة، لاسيما فيما يتعلق بحماية الخصوصية وضمان الأمن الشخصي للأفراد. فالذكاء الاصطناعي يعتمد بدرجة كبيرة على جمع ومعالجة كميات هائلة من البيانات الشخصية، وتحليل السلوكيات والأنماط الفردية، الأمر الذي يثير مخاوف متزايدة بشأن انتهاك الحياة الخاصة، وتوسّع المراقبة الرقمية، وإمكانية إساءة استخدام المعطيات الشخصية. كما أن تطور تقنيات التعرف على الهوية والأنظمة التنبؤية قد يؤدي إلى اتخاذ قرارات آلية تمس الحقوق والحريات الأساسية دون رقابة قانونية كافية. وتتمثل أبرز هذه المخاطر في التوسع في جمع وتحليل البيانات الشخصية، واستخدام أنظمة المراقبة الذكية وتقنيات التعرف على الهوية، بما قد يؤدي إلى المساس بالحياة الخاصة للأفراد دون ضمانات كافية. كما تطرح الخوارزميات الذكية تحديات تتعلق بأمن المعطيات الشخصية وإمكانية إساءة استخدامها أو استغلالها بطرق تهدد الحقوق والحريات الفردية. ومن هذا المنطلق، تكتسي دراسة مخاطر الذكاء الاصطناعي على الخصوصية والأمن الشخصي أهمية بالغة، باعتبارها من القضايا المعاصرة التي تفرض على المشرّع والباحث القانوني العمل على إيجاد توازن دقيق بين متطلبات التطور التكنولوجي وضرورة حماية الحقوق الأساسية للأفراد في العصر الرقمي.

الكلمات المفتاحية : الذكاء الاصطناعي ، الذكاء الاصطناعي ، حماية البيانات الشخصية .

Abstract

The rapid development of artificial intelligence technologies has led to profound transformations across various areas of life, as reliance on intelligent systems has become a fundamental element in improving performance, rationalizing decision-making, and delivering more efficient services. However, despite the significant benefits of this technological progress, it has generated unprecedented legal and ethical challenges, particularly with regard to the protection of privacy and the safeguarding of individuals' personal security. Artificial intelligence relies heavily on the collection and processing of vast amounts of personal data, as

well as the analysis of individual behaviors and patterns. This has raised growing concerns about violations of private life, the expansion of digital surveillance, and the potential misuse of personal data. Moreover, the development of identity recognition technologies and predictive systems may lead to automated decision-making processes that affect fundamental rights and freedoms without adequate legal oversight. The most prominent risks lie in the extensive collection and analysis of personal data, the use of intelligent surveillance systems, and identity recognition technologies, which may infringe upon individuals' private lives in the absence of sufficient safeguards. Intelligent algorithms also pose challenges related to the security of personal data and the possibility of its misuse or exploitation in ways that threaten individual rights and freedoms.

From this perspective, examining the risks of artificial intelligence to privacy and personal security is of paramount importance, as it represents one of the contemporary issues that require legislators and legal researchers to work toward achieving a delicate balance between the demands of technological advancement and the necessity of protecting individuals' fundamental rights in the digital age.

Keywords: Artificial Intelligence, Privacy, Personal Data Protection

تحقيق الأمن السيبراني على ضوء اتفاقية الأمم المتحدة لمكافحة الجرائم السيبرانية لسنة 2024

د/بعقيقي عبير **د/منصر نصر الدين**

جامعة الشهيد الشيخ العربي التبسي – تبسة - **جامعة الشهيد الشيخ العربي التبسي – تبسة –**

abir.baguigui@univ-tebessa.dz Menaceur.naceur@univ-tebessa.dz

الملخـــص

تُعدّ اتفاقية الأمم المتحدة لمكافحة الجرائم السيبرانية لعام 2024 أول إطار دولي شامل يُعنى بمواجهة التهديدات الإلكترونية المتزايدة، من خلال تبنّي قواعد موحّدة للتجريم وتعزيز التعاون بين الدول. وقد أكدت المنظمة الأممية على أهمية التوازن بين ضرورات الأمن السيبراني وحماية حقوق الإنسان والخصوصية الرقمية. وشكّل انضمام الجزائر للاتفاقية محطة مهمة، لاسيما بعد دورها البارز في مسار صياغة أحكامها وقيادة المفاوضات التقنية. وتوفر الاتفاقية أدوات فعّالة لتبادل الأدلة الإلكترونية، وتسليم المطلوبين، واسترجاع العائدات الإجرامية، إضافةً إلى آليات لحماية الضحايا وتأهيل الجناة. كما تُجرّم الاتفاقية صوراً متعددة من الجريمة السيبرانية، منها الدخول غير المشروع، اعتراض البيانات، إتلاف المعلومات، التزوير الإلكتروني، الاحتيال الرقمي، واستخدام الأدوات التقنية لأغراض إجرامية، فضلاً عن تجريم الاعتداء الجنسي على الأطفال عبر الإنترنت. وتركّز الاتفاقية أيضاً على الوقاية والاستباقية عبر تطوير استراتيجيات وطنية وتعاون مؤسسي بين القطاعين العام والخاص.

الكلمات المفتاحية :الأمن السيبراني، الجريمة الإلكترونية،التعاون الدولي،حماية الضحايا،الاتفاقيات الدولية.

Abstract

The 2024 United Nations Convention on Cybercrime constitutes the first comprehensive international instrument dedicated to addressing the expanding phenomenon of cybercriminality. Adopted by the UN General Assembly on 24 December 2024, the Convention seeks to harmonize criminalization standards, reinforce international cooperation, and ensure effective mechanisms for evidence-sharing, extradition, and mutual legal assistance. The Convention also emphasizes the need to strike a balance between cybersecurity imperatives and the protection of human rights and digital privacy. Algeria's accession represents a significant milestone, particularly given its leading role in negotiating and shaping the Convention's final text.

The Convention provides a robust legal and technical framework to counter cyber threats, including malware, intrusions, digital fraud, and data manipulation. It criminalizes a wide range of cyber-offences such as unlawful access to information systems, illegal interception of data, intentional damage or alteration of electronic information, system

interference, misuse of technological tools, electronic forgery, and digital fraud. Special provisions address the sexual exploitation of children online and mandate enhanced protection and support for victims. Additionally, the Convention adopts a preventive approach by encouraging States to develop national cybersecurity strategies and promote collaboration between public and private sectors.

Keywords: Cybersecurity,Cybercrime, International Cooperation, Victim Protection, International Conventions.

مفهوم الجرائم المرتكبة عن طريق الذكاء الاصطناعي

أ.د/خالدي خديجة **د/ بشارة عبد المالك**

جامعة الشهيد الشيخ العربي التبسي تبسة- **جامعة الشهيد الشيخ العربي التبسي – تبسة–**

الملخـــــص

تعد الجرائم السيبرانية من الجرائم المستحدثة التي يعرفها عصرنا الحالي، وذلك لارتباطها بالحاسوب وشبكة الإنترنت التي تشهد تطورًا سريعًا ومتواصلاً. وقد أصبحت هذه الجرائم تشكّل خطرًا حقيقيًا على حياة الأفراد وأمن المؤسسات، نظرًا لما تتميّز به من طابع عابر للحدود، فضلًا عن صعوبة اكتشافها وإثباتها. ويرتكب هذه الجرائم ما يُعرف بمجرمي المعلومات، الذين يتمتعون بقدر عالٍ من الذكاء والمهارة التقنية. ونظرًا لطبيعة الجرائم السيبرانية التي تتسم بالخفاء والهدوء، لم تعد الدولة وحدها قادرة على مجابهة هذا الخطر المتزايد، الأمر الذي يستوجب تعاون الدول فيما بينها من خلال تفعيل التعاون الأمني والقضائي، وإبرام الاتفاقيات الدولية، واستحداث تشريعات وقوانين حديثة. ويهدف كل ذلك إلى التصدي للجرائم السيبرانية التي أصبحت هاجس العصر الرقمي

الكلمات المفتاحية: الجرائم السيبرانية، الجريمة العابرة للحدود، الإثبات الرقمي، التعاون الدولي، الأمن السيبراني.

Abstract

Cybercrimes are newly emerging crimes that have come to be rec-ognized in our current era due to their association with computers and the rapidly evolving internet. These crimes pose a threat to the lives of indi-viduals and institutions as they are characterized by their cross-border nature, making them difficult to detect and prove. Cybercriminals, who are skilled and intelligent, perpetrate these offenses. Given the quiet nature of these crimes, it is no longer possible for a state to confront this danger alone; therefore, countries must cooperate through security and judicial collaboration, establishing agreements and creating new laws, all to com-bat cybercrimes that have become a concern of our time.

Keywords Cybercrime, Transnational Crime, Digital Evidence, International Cooperation, Cybersecurity

اجراءات التحري في الجرائم الالكترونية على ضوء القانون 14/25

د/خالدي شريفة
جامعة الشهيد الشيخ العربي التبسي – تبسة-
Cherifa.khalddi@univ-tebessa.dz

الملخـــــص

أصبحت الجريمة الالكترونية اليوم واقع مفزع ومؤلم يهدد الدول والأفراد بسبب تطور وسائل ارتكابها من الطرف المجرمين المبرمجين وكثرة ضحايا هذه الجرائم.

حيث عمل مشرع الجزائري على وضع إجراءات وقائية للحد من هذه الجرائم إذ تسمى هذه الإجراءات بمرحلة البحث والتحري باعتبارها مكرسة للكشف عن هذا نوع من الجرائم حيث أناط رجال الضبطية القضائية بالعديد من الاختصاصات في مكافحة هذا النوع من الجرائم كإجراءات تلقى الشكاوى والبلاغات في حالات العادية بالإضافة إلى اختصاصات استثنائية مادية كالمعاينة والتفتيش الالكتروني وشخصية كالتسرب والمراقبة الالكترونية واعتراض المراسلات والخبرة والتي تساعدهم على قبض على مرتكبي الجرائم ومعاقبتهم على أفعالهم.

الكلمات المفتاحية: الضبطية القضائية - الجريمة الالكترونية - البحث والتحري - المجرم الالكتروني.

Abstract

Today, cybercrime has become a terrifying and painful reality that threatens nations and individuals due to the evolving methods used by criminal programmers and the increasing number of victims of these crimes.

The Algerian legislator has worked to establish preventive measures to limit these crimes. These measures are known as the investigation and inquiry phase, dedicated to uncovering this type of crime. Judicial police officers have been entrusted with numerous powers to combat these crimes, such as receiving complaints and reports in normal circumstances. Additionally, they have exceptional material powers like electronic inspection and examination, and personal powers such as infiltration, electronic surveillance, interception of correspondence, and expert analysis, all of which assist them in apprehending and punishing perpetrators for their actions.

Keywords: Judicial police-Cybercrime-Investigation and inquiry-

توظيف الذكاء الاصطناعي في تعزيز الأمن السيبراني

د/ لحمر نعيمة

جامعة الشهيد الشيخ العربي التبسي –تبسة-

naima.lahmar@univ-tebessa.dz

الملخـــــــص

يشكل الذكاء الاصطناعي حجر زاوية في تطوير الأمن السيبراني الحديث، حيث يعزز من قدرة الأنظمة على الكشف الاستباقي والتكيفي عن الهجمات الإلكترونية المعقدة من خلال تحليل كميات هائلة من البيانات والتعرف على أنماط التهديد، مما يسرع من عمليات الإستجابة للحوادث ويحسن الدفاعات ضد التهديدات المستجدة مثل البرمجيات الخبيثة المتطورة وهجمات التصيد، لكنه يثير في المقابل تحديات تتعلق بإمكانية اختراق أو التلاعب بهذه النماذج الذكية نفسها ويثير أسئلة أخلاقية حول الخصوصية والاعتماد المفرط على الآلة. ومنه يستخدم الذكاء الاصطناعي تقنيات مثل التعلم الآلي ومعالجة اللغة الطبيعية لتحليل البيانات الكبيرة والتنبؤ بالهجمات قبل وقوعها. كما يمكن للذكاء الاصطناعي أن يساهم في أتمتة عمليات الأمان، مما يقلل من عبء العمل على الفرق البشرية ويزيد من سرعة الاستجابة للتهديدات.

الكلمات المفتاحية: الذكاء الاصطناعي، الأمن السيبراني، كشف التهديدات، الاستجابة، التعلم الآلي

Abstract

Artificial intelligence constitutes a cornerstone in the development of modern cybersecurity, as it enhances systems' capabilities for proactive and adaptive detection of complex cyberattacks by analyzing vast amounts of data and identifying threat patterns. This accelerates incident response processes and improves defenses against emerging threats such as advanced malware and phishing attacks. However, it simultaneously raises challenges related to the potential compromise or manipulation of these intelligent models themselves and poses ethical questions regarding privacy and over-reliance on automation.

AI employs techniques like machine learning and natural language processing to analyze big data and predict attacks before they occur. Furthermore, AI can contribute to automating security processes, reducing the workload on human teams and increasing the speed of response to threats.

Keywords: Artificial Intelligence, Cybersecurity, Threat Detection, Response, Machine Learning

جرائم الاعتداء على حرمة الحياة الخاصة عبر الوسائط الرقمية في التشريع الوطني

د/خذيري عفاف
جامعة الشهيد الشيخ العربي التبسي
afaf.khediri@univ-tebessa.dz

أ.د/ عثماني عزالدين
جامعة الشهيد الشيخ العربي التبسي –تبسة
Azeddine.atmani@univ-tebessa.dz

الملخـــــص

يعد الحق في الحياة الخاصة من أكثر الحقوق تعلق الشخصية وأشدها ارتباطا لكرامة الفرد، وذلك لجمعه لبن الجوانب المادية والمعنوية لشخصية الامسان وعلاقته الوثيقة لحقوق والحريات الأخرى، وأثره الشديد للمخاطر التي فرضها التطور العلمي والتكنولوجي لوسائل الاعلام و الاتصال، لذلك فقد أولى المشرع الجزائري له أهمية خاصة اعتباره حقا وواجبا دستوريا على الافراد مراعاته عند ممارستهم لحقوقهم وجرم الأخرى، وشكلت جرائم التعدي عليها محور التعديلات التي استحدثها بموجب القوانين العادية وذلك لتحديد صور وأشكال المساس بها، سواء من الجانب المادي والذي يتمثل في المسكن وسلامة الجسد أو من خلال الوسائط الرقمية فيما يتعلق بالمحادثات أو المراسلات الالكترونية أو التقاط الصور كذلك المعالجة الآلية لأنظمة المعطيات.

الكلمات المفتاحية: الحياة الخاصة، المراسلات الالكترونية، المحادثات .

abstract

The right to privacy is one of the rights most closely connected to an individual's personality and most strongly linked to human dignity, as it encompasses both the material and moral aspects of the human person and is closely related to other rights and freedoms. It has also been significantly affected by the risks imposed by scientific and technological developments in the fields of media and communication. For this reason, the Algerian legislator has accorded it special importance by recognizing it as a constitutional right and duty that individuals must respect when exercising their rights and freedoms, and by criminalizing acts that infringe upon it. Crimes against privacy have thus constituted the core of the amendments introduced by ordinary legislation in order to define the various forms and manifestations of such violations, whether from the material aspect, represented by the inviolability of the home and the integrity of the human body, or through digital media, with regard to electronic conversations and correspondence, the taking of photographs, as well as the automated processing of data systems.

Keywords: Privacy, Electronic Correspondence, Conversations.

الإطار القانوني للأمن السيبراني في مواجهة تحديات الذكاء الاصطناعي – بين القصور التشريعي والمتطلبات المستجدة-

أ/خمايسة حفيظة
جامعة الشهيد الشيخ العربي التبسي – تبسة
hafida.khemaisssia@univ-tebessa.dz

ط/د بولخوة إبتسام
جامعة الشهيد الشيخ العربي التبسي- تبسة-
Ibtissem.boulakhoua@univ-tebessa.dz

الملخـــــص

يشهد العالم تحولاً عميقاً في طبيعة التهديدات الرقمية بفعل التطور المتسارع للذكاء الاصطناعي، الذي لم يعد مجرد أداة مساعدة، بل أصبح فاعلاً رقمياً قادراً على التعلم الذاتي، وتطوير قدراته الهجومية، وتجاوز أنظمة الدفاع التقليدية، وقد أصبحت البيئة الرقمية أكثر تعقيداً وتشابكاً مع دخول أنظمة الذكاء الاصطناعي في البنية السيبرانية للدول، وخاصة في القطاعات الحيوية كالأمن والدفاع، المالية، الصحة، النقل، والخدمات العمومية. ومع هذا التوسع، تضاعفت التحديات القانونية والفجوات التشريعية التي تواجه المنظومة التقليدية للأمن السيبراني، إذ صُمِّمت القواعد القانونية لحماية نظم معلومات تقليدية، بينما تواجه اليوم خوارزميات قادرة على التعلم الآلي، توليد الهجمات تلقائياً، التكيف مع الدفاعات، وانتحال الهويات الرقمية بدرجة غير مسبوقة.

الكلمات المفتاحية : الذكاء الاصطناعي- الاطار القانوني التقليدي – الامن السبراني

Abstract

The nature of digital threats is rapidly evolving due to the advancement of artificial intelligence, which has become a digital actor capable of self-learning and enhancing its offensive capabilities, surpassing traditional defense mechanisms. As national cyber infrastructures intersect with AI systems across critical sectors such as security, defense, finance, health, and transportation, legislative gaps and legal challenges confronting traditional cybersecurity frameworks are increasing.

This presentation addresses the following issue: To what extent can national and international legislation keep pace with emerging threats generated by autonomous intelligent systems

Key words : Traditional Legal Framework /

الذكاء الاصطناعي كأداة لتطوير سياسات الأمن السيبراني

أ/ جويني عماد الدين
جامعة صفاقص –تونس-
jouiniimad72@gmail.com

ط/د شنيخر امينة
جامعة صفاقص – تونس-
aminachenikharr@gmail.com

الملخــص

يشهد مجال الأمن السيبراني تحولاً جذرياً بفعل التطور المتسارع للذكاء الاصطناعي، الذي لم يعد مجرد أداة تحليلية بل أصبح قادراً على التعلم الذاتي، واكتشاف الثغرات، والتنبؤ بالهجمات السيبرانية قبل وقوعها. تمثل هذه القدرات فرصة هامة لتطوير سياسات أمنية أكثر فاعلية، تتيح للدول والمؤسسات مواجهة التهديدات الرقمية بسرعة ودقة أكبر. تركز المداخلة على محورين رئيسيين:

1. **دور الذكاء الاصطناعي في تعزيز الأمن السيبراني :**من خلال تحليل البيانات الضخمة، رصد الهجمات في الزمن الحقيقي، وتحسين نظم الكشف والاستجابة.
2. **تطوير السياسات الأمنية بالاعتماد على الذكاء الاصطناعي :**استعراض استراتيجيات وإجراءات تنظيمية وقانونية تسمح بالاستفادة من تقنيات الذكاء الاصطناعي مع مراعاة الخصوصية، وحماية البيانات، وضمان الشفافية والمساءلة.

إن دمج الذكاء الاصطناعي في تصميم وتنفيذ سياسات الأمن السيبراني يمثل خطوة استراتيجية لتعزيز القدرة الدفاعية، وتقليل المخاطر الرقمية، وضمان استمرارية الخدمات الحيوية في بيئة رقمية متسارعة التطور.

abstract

The field of cybersecurity is undergoing a fundamental transformation due to the rapid advancement of artificial intelligence, which has evolved from a mere analytical tool to a self-learning system capable of detecting vulnerabilities and predicting cyberattacks before they occur. These capabilities offer a valuable opportunity to develop more effective security policies, enabling states and organizations to respond to digital threats with greater speed and precision.

The presentation focuses on two main axes:

1. **The Role of AI in Enhancing Cybersecurity:** Utilizing big data analytics, real-time threat detection, and improving monitoring and response systems.

2. **Developing Security Policies Based on AI:** Reviewing strategies and regulatory measures that allow leveraging AI technologies while ensuring privacy, data

Integrating AI into the design and implementation of cybersecurity policies represents a strategic step to strengthen defensive capabilities, reduce digital risks, and ensure continuity of critical services in a rapidly evolving digital environment

الذكاء الاصطناعي والأمن السيبراني: سياسات واستراتيجيات على المستوى الدولي

ط/د. شرقي لخضر
جامعة صفاقص – تونس
Cherguilakhder5@gmail.com

الملخـــــص

يشهد العالم تصاعدًا في الهجمات السيبرانية المتطورة مع الاعتماد المتزايد على التكنولوجيا الرقمية، مما يجعل الأمن السيبراني أولوية استراتيجية. يلعب الذكاء الاصطناعي دورًا مزدوجًا: فهو أداة لتعزيز الدفاع الرقمي من خلال الكشف المبكر عن التهديدات وتحليل البيانات الضخمة، وفي نفس الوقت قد يُستغل في الهجمات الذكية. على المستوى الدولي، ظهرت سياسات واستراتيجيات لتنسيق الجهود بين الدول، مثل الاتفاقيات الدولية والمبادرات المشتركة لتعزيز الحماية الرقمية وتبادل المعلومات. كما تؤكد هذه السياسات على أهمية الأطر القانونية والأخلاقية لضمان الاستخدام المسؤول للذكاء الاصطناعي، إلى جانب تدريب العنصر البشري لتعزيز القدرات الدفاعية. إن التعاون الدولي واستخدام الذكاء الاصطناعي بشكل متوازن يشكلان مفتاحًا لضمان الأمن السيبراني والاستقرار الرقمي العالمي.

الكلمات المفتاحية : الأمن السيبراني، الذكاء الاصطناعي، السياسات الدولية، التعاون بين الدول، الهجمات الرقمية.

Abstract

The world is witnessing a rise in sophisticated cyberattacks alongside the increasing reliance on digital technologies, making cybersecurity a strategic priority. Artificial intelligence (AI) plays a dual role: it serves as a tool to enhance digital defense through early threat detection and big data analysis, while at the same time it can be exploited in smart attacks. At the international level, policies and strategies have emerged to coordinate efforts among countries, such as international agreements and joint initiatives to strengthen digital protection and information sharing. These policies also emphasize the importance of legal and ethical frameworks to ensure the responsible use of AI, in addition to training human resources to enhance defensive capabilities. International cooperation and the balanced use of AI are key to ensuring global cybersecurity and digital stability.

Key words : Cybersecurity, Artificial Intelligence (AI), International Policies, International Cooperation, Cyber Attacks .

الهجمات السيبرانية الذكية: المفهوم والأنواع

د/ بوعزيزعبد الوهاب
جامعة الطـــــــارف
bouazizsofian93@gmail.com

أ.د/ بوراس منير
جامعة الشهيد الشيخ العربي التبسي – تبسة
Mounir.bouras@univ-tebessa.dz

الملخـــص

تشير الهجمات السيبرانية الذكية إلى نمط متطور من الهجمات الرقمية التي تعتمد على تقنيات الذكاء الاصطناعي والتعلم الآلي من أجل اختراق الأنظمة المعلوماتية بطرق أكثر دقة وفعالية. تتميز هذه الهجمات بقدرتها على التعلم والتكيف مع أنظمة الحماية، مما يجعل اكتشافها والحد من آثارها أكثر تعقيدًا مقارنة بالهجمات التقليدية. وتشمل الهجمات السيبرانية الذكية عدة أنواع، من أبرزها هجمات التصيد الاحتيالي المتقدم، والبرمجيات الخبيثة الذكية، وهجمات الهندسة الاجتماعية المعززة بالذكاء الاصطناعي، إضافة إلى الهجمات القائمة على تحليل البيانات وسلوك المستخدم. وتفرض هذه التهديدات تحديات أمنية جديدة تستوجب تطوير آليات دفاعية ذكية، وتعزيز التعاون الدولي، ووضع أطر قانونية وأخلاقية قادرة على مواكبة هذا التطور التقني المتسارع.

الكلمات المفتاحية : الهجمات السيبرانية الذكية، الذكاء الاصطناع، الأمن السيبراني، التهديدات الرقمية .

Abstract

Smart cyberattacks refer to an advanced form of digital threats that rely on artificial intelligence and machine learning techniques to infiltrate information systems with greater accuracy and effectiveness. These attacks are characterized by their ability to learn and adapt to security mechanisms, making their detection and mitigation more complex than traditional cyberattacks. Smart cyberattacks include several types, such as advanced phishing attacks, intelligent malware, AI-enhanced social engineering, and behavior-based attacks that exploit data analysis and user patterns. These evolving threats pose significant security challenges, necessitating the development of intelligent defense mechanisms, strengthened international cooperation, and the establishment of legal and ethical frameworks capable of keeping pace with rapid technological advancements.

Keywords Smart Cyberattacks, Artificial Intelligence, , Cybersecurity, Digital Threats.

الاتجار بالبشر والفضاء الإلكتروني: رهانات المكافحة في البيئة الرقمية

د/ خذيري حنان

جامعة الشهيد الشيخ العربي التبسي –تبسة-

khedirih2020@gmail.com

الملخـــــص

أفرز الفضاء الإلكتروني أنماطًا جديدة لممارسة جريمة الاتجار بالبشر، حيث باتت الشبكات الإجرامية تستغل المنصات الرقمية ووسائل التواصل الاجتماعي في استدراج الضحايا وتنظيم عمليات الاستغلال بعيدًا عن الرقابة التقليدية. وقد أدى هذا التحول إلى بروز رهانات قانونية وأمنية معقّدة، تتعلق بصعوبة الرصد والتتبع، وإثبات الجرائم الرقمية، وتحديد المسؤوليات الجنائية عبر الحدود. كما يطرح الطابع العابر للفضاء الإلكتروني تحديات على مستوى الاختصاص القضائي والتعاون الدولي. وعليه، تقتضي المكافحة الفعالة تطوير التشريعات الجزائية، وتعزيز آليات التحري الرقمي، وبناء شراكات دولية لمواجهة الاتجار بالبشر في البيئة الرقمية.

الكلمات المفتاحية: الاتجار بالبشر؛ الفضاء الإلكتروني؛ الجرائم الرقمية؛ الإثبات الإلكتروني؛ الاختصاص القضائي؛ التعاون الدولي.

Abstract:

The digital space has generated new patterns of human trafficking, as criminal networks increasingly exploit online platforms and social media to lure victims and organize exploitation beyond traditional control mechanisms. This transformation has given rise to complex legal and security challenges related to detection and monitoring difficulties, digital evidence, and the attribution of criminal responsibility across borders. Moreover, the transnational nature of cyberspace poses significant challenges regarding jurisdiction and international cooperation. Consequently, effective countermeasures require the modernization of criminal legislation, the strengthening of digital investigation mechanisms, and the establishment of international partnerships to combat human trafficking in the digital environment.

Keywords: Human trafficking; Cyberspace; Digital crimes; Electronic evidence; Jurisdiction; International cooperation.

مكافحة جريمة الاتجار بالبشر في العصر الرقمي: إشكالات قانونية وتحديات عملية

د.سعايدية حورية

جامعة الشهيد الشيخ العربي التبسي- تبسة-

houria.saaidia@yahoo.fr

الملخـــــص

تُعد جريمة الاتجار بالبشر من أخطر الجرائم العابرة للحدود، وقد ساهم التطور التكنولوجي في تعقيد آليات مكافحتها. إذ استغلّت الشبكات الإجرامية وسائل الاتصال الحديثة، ومنصات التواصل الاجتماعي، والعملات الرقمية في استقطاب الضحايا وتسهيل عمليات النقل والاستغلال مع صعوبة التتبع. كما تطرح الجرائم الإلكترونية المرتبطة بالاتجار بالبشر تحديات قانونية وإجرائية تتعلق بالإثبات الرقمي، والاختصاص القضائي، والتعاون الدولي. ويزيد ضعف التنسيق بين الدول وتفاوت التشريعات الوطنية من حدة هذه التحديات. وعليه، تبرز الحاجة إلى تطوير الأطر القانونية، وتعزيز القدرات التقنية للأجهزة المختصة، وتكثيف التعاون الدولي من أجل مواجهة فعّالة لهذه الجريمة في العصر الرقمي.

الكلمات المفتاحية: الاتجار بالبشر؛ التطور التكنولوجي؛ الجرائم الإلكترونية؛ الإثبات الرقمي؛ التعاون الدولي؛ الحماية القانونية.

Abstract

Human trafficking is one of the most serious transnational crimes, and technological development has significantly complicated efforts to combat it. Criminal networks increasingly exploit modern communication tools, social media platforms, and digital currencies to recruit victims and facilitate transportation and exploitation while evading detection. Moreover, cyber-related trafficking crimes raise complex legal and procedural challenges concerning digital evidence, jurisdiction, and international cooperation. The lack of coordination among states and disparities in national legislations further exacerbate these challenges. Therefore, there is an urgent need to update legal frameworks, strengthen the technical capacities of competent authorities, and enhance international cooperation to effectively combat human trafficking in the digital age.

Keywords: Human trafficking; Technological development; Cybercrime; Digital evidence; International cooperation; Legal protection

تطور مفهوم التهديدات السبرانية في ظل الذكاء الاصطناعي

د./ دبيلي كمال
جامعة الشهيد الشيخ العربي التبسي – تبسة
Kamel.debili@univ-tebessa.dz

الملخـــص

ساهم التطور المتسارع لتقنيات الذكاء الاصطناعي في إعادة تشكيل طبيعة التهديدات السيبرانية، حيث انتقلت الهجمات من أساليب تقليدية إلى أنماط ذكية تعتمد على التعلم الآلي وتحليل كميات ضخمة من البيانات. وتُمكّن هذه التقنيات المهاجمين من تحسين دقة الهجمات، وتجاوز أنظمة الحماية، وتنفيذ عمليات اختراق مؤتمتة يصعب التنبؤ بها أو اكتشافها في مراحلها الأولى. وقد أدى ذلك إلى تصاعد المخاطر التي تستهدف البيانات والبنى التحتية الرقمية، مما يستوجب تطوير آليات دفاع سيبراني متقدمة وإطارًا قانونيًا قادرًا على مواكبة هذا التحول التكنولوجي.

الكلمات المفتاحية : التهديدات السبرانية / التكنولوجيا / المخاطر / الاختراق .

Abstract

the rapid development of artificial intelligence technologies has contributed to reshaping the nature of cyber threats, as attacks have shifted from traditional methods to intelligent patterns based on machine learning and the analysis of large volumes of data. These technologies enable attackers to enhance the precision of their attacks, bypass security systems, and carry out automated intrusions that are difficult to predict or detect in their early stages. This has led to an escalation of risks targeting data and digital infrastructures, necessitating the development of advanced cyber defense mechanisms and a legal framework capable of keeping pace with this technological transformation.

Keyword : Cyber Threats / Technology / Risks / Intrusion. :

الذكاء الاصطناعي و الامن السبراني المفاهيم الاساسية والتحديات المعاصرة

أ.د / مخلوف طارق

جامعة الشهيد الشيخ العربي التبسي – تبسة -

Tarek.makhlouf @univ-tebessa.dz

الملخـــص

يتناول موضوع الذكاء الاصطناعي والأمن السيبراني المفاهيم الأساسية المرتبطة بكل منهما والتحديات التي يفرضها التطور التكنولوجي المعاصر. فالذكاء الاصطناعي يُقصد به مجموعة التقنيات التي تمكّن الأنظمة الحاسوبية من محاكاة القدرات الذهنية للإنسان مثل التعلّم، الاستنتاج، واتخاذ القرار. أما الأمن السيبراني فيُعنى بحماية الأنظمة والشبكات وقواعد البيانات من مختلف أشكال التهديدات والهجمات الإلكترونية. وتتمثل العلاقة بينهما في توظيف تقنيات الذكاء الاصطناعي لتعزيز قدرات الكشف المبكر عن الاختراقات، وتحليل المخاطر، والاستجابة الآلية للهجمات. غير أن هذا التطور يطرح في المقابل تحديات مهمة، من أبرزها استغلال الذكاء الاصطناعي في شن هجمات متطورة، تعقيد أساليب الجريمة السيبرانية، المساس بالخصوصية، وصعوبة مواكبة الأطر القانونية والأخلاقية لهذا التقدم التقني.

الكلمات المفتاحية : الذكاء الاصطناعي / الأمن السيبراني / حماية البيانات / التهديدات السيبرانية / الخصوصية / الرقمنة / أمن المعلومات.

abstract

The topic of Artificial Intelligence and Cybersecurity addresses the basic concepts of both fields and the challenges arising from contemporary technological development. Artificial Intelligence refers to technologies that enable computer systems to simulate human cognitive abilities such as learning, reasoning, and decision-making. Cybersecurity focuses on protecting systems, networks, and databases from various cyber threats and attacks. The relationship between them lies in using AI techniques to enhance early threat detection, risk analysis, and automated response. However, this advancement also poses major challenges, including the misuse of AI in launching sophisticated cyberattacks, the growing complexity of cybercrime, threats to privacy, and the difficulty of keeping legal and ethical frameworks up to date with rapid technological change.

Keywords : artificial Intelligence/ Cybersecurity / Data Protection / Cyber Threats/ Hacking – Privacy / Digitalization/ Information Security.

اهمية الذكاء الاصطناعي في دعم استراتيجيات السيادة الرقمية

د/رزايقية حنان **د/ لحواسنية ياسمين**

جامعة الشهيد الشيخ العربي التبسي – تبسة- **جامعة الشهيد الشيخ العربي التبسي – تبسة-**

hanane.rezaiguia@univ-tebessa.dz **Yasmine.lahouasnia@univ-tebessa.dz**

الملخص

لقد أنتج الفضاء السيبراني معضلة أساسية تتعلق بالتكييف القانوني لسلوك الدول ضمن هذا المجال باعتباره بيئة افتراضية عالمية؛ تربط بين مختلف دول العالم دون قيود ولا حواجز جغرافية، مما يؤثر بشكل مباشر على سيادة الدول، ويطرح بذلك تساؤلات جوهرية حول قدرة الدولة على ممارسة سيادتها في الفضاء السيبراني باعتباره مجالاً جديداً للتفاعلات الدولية.

يلعب الذكاء الاصطناعي دورًا محوريًا في تدعيم استراتيجيات السيادة الرقمية من خلال تعزيز قدرة الدول على التحكم في بياناتها وبناها التحتية الرقمية، ويساعد في تحليل كميات هائلة من البيانات محليًا، مما يقلل الاعتماد على منصات وتقنيات أجنبية.كما يساهم في تحسين الأمن السيبراني عبر التنبؤ بالتهديدات الرقمية والاستجابة لها بفعالية.ويدعم الذكاء الاصطناعي اتخاذ القرار الاستراتيجي من خلال نماذج ذكية تعزز التخطيط والسياسات الرقمية الوطنية.

الكلمات المفتاحية : استراتيجيات السيادة الرقمية / النماذج الذكية / الامن السيبراني.

abstract

Cyberspace has created a fundamental dilemma related to the legal characterization of state behavior within this domain, as it is considered a global virtual environment that connects countries worldwide without restrictions or geographical barriers. This directly affects state sovereignty and raises essential questions about the ability of states to exercise their sovereignty in cyberspace as a new arena for international interactions.

Artificial intelligence plays a pivotal role in strengthening digital sovereignty strategies by enhancing states' ability to control their data and digital infrastructure. It helps analyze vast amounts of data locally, thereby reducing dependence on foreign platforms and technologies. AI also contributes to improving cybersecurity by predicting digital threats and responding to them effectively, and it supports strategic decision-making through intelligent models that enhance planning and national digital policies.

Keywords digital sovereignty strategies / intelligent models/ cybersecurity

حماية المعطيات الشخصية بين ذكاء الخوارزميات وسيادة الامن السبراني – مقاربة قانونية في عصر التحول الرقمي

د/ فاضل عائشة

جامعة التكوين المتواصل –تبسة –

Misaichamsdk12@gmail.com

الملخص

في عصر التحول الرقمي، حيث تتقاطع المعطيات الشخصية مع الخوارزميات الذكية، يبرز تحدٍّ قانوني استراتيجي يتمثل في حماية الحقوق الفردية وتأمين البنية السيبرانية الوطنية. فالذكاء الاصطناعي يعتمد على كميات هائلة من البيانات الشخصية، وقد يؤدي أي خلل خوارزمي إلى تحيز أو استغلال أو مساس بحرمة الحياة الخاصة من خلال تحليلها وانتهاك الخصوصية. وفي المقابل، يوفّر هذا الذكاء فرصًا واعدة لتعزيز الأمن السيبراني عبر أنظمة متقدمة للكشف المبكر عن التهديدات، والتشفير التنبؤي، وتحليل المخاطر الوقائي. إن تحقيق التوازن بين هذه الأبعاد القانونية والتقنية يستوجب وضع إطار حوكمي رصين يضمن حماية المعطيات الشخصية دون كبح روح الابتكار أو عرقلة تطور الذكاء الاصطناعي، وذلك من خلال ترسيخ مبادئ الشفافية والمساءلة، والانسجام مع أفضل الممارسات الدولية، وتبنّي استراتيجية وطنية قائمة على تشريعات متخصصة، وهيئات رقابية مستقلة، وبرامج تكوين متقدمة، بما يكفل إرساء سيادة رقمية تحمي الحقوق وترتقي بالبلاد إلى مصاف الدول الرائدة.

الكلمات المفتاحية: التحول الرقمي – الذكاء الاصطناعي – حماية المعطيات الشخصية – الأمن السيبراني – الخصوصية

abstract

in the era of digital transformation, where personal data intersect with intelligent algorithms, a strategic legal challenge emerges in ensuring the protection of individual rights and the security of the national cyber infrastructure. Artificial intelligence relies on vast amounts of personal data, and any algorithmic malfunction may lead to bias, exploitation, or infringement of the sanctity of private life through unlawful analysis and violations of privacy. At the same time, this technology offers significant opportunities to enhance cybersecurity through advanced systems for early threat detection, predictive encryption, and preventive risk analysis. Achieving a balance between these legal and technical dimensions requires the establishment of a robust governance framework that guarantees the protection of personal data without restraining innovation or hindering the development of artificial intelligence. Such a framework should be based on the principles of transparency and accountability, aligned with international

best practices, and supported by a national strategy founded on specialized legislation, independent regulatory authorities, and advanced training programs, thereby ensuring digital sovereignty that safeguards rights and elevates the country to the ranks of leading nations.

Keywords Digital Transformation – Artificial Intelligence – Personal Data Protection – Cybersecurity – Privacy – Digital