



الجمهورية الجزائرية الديمقراطية الشعبية  
وزارة التعليم العالي والبحث العلمي  
جامعة طاهري محمد بشار- كلية الحقوق و العلوم السياسية  
مخبر الدراسات القانونية و مسؤولية المهنيين  
مشاريع البحث التكويني PRFU  
السياسة الجنائية في مواجهة جرائم رجال الاعمال  
و حوكمة المعاملات المالية الالكترونية



## شهادة مشاركة

تمنح هذه الشهادة لـ الدكتور : عبد الغني حجاب من جامعة محمد بوضياف- المسيلة - الجزائر نظير مشاركته (ا) في المؤتمر الدولي الموسوم بـ "المسؤولية القانونية عن استخدام تقنية الذكاء الاصطناعي و التحول الرقمي" المنظم من طرف مخبر الدراسات القانونية و مسؤولية المهنيين بالتعاون مع مخبر الدراسات القانونية التطبيقية- جامعة قسنطينة 1 الاخوة منتوري و مشاريع البحث التكويني PRFU السياسة الجنائية في مواجهة جرائم رجال الاعمال و حوكمة المعاملات المالية الالكترونية، المنعقد يومي 05-06 نوفمبر 2025 بجامعة طاهري محمد بشار، حضوري و عن بعد عبر تقنية التحاضر المرئي بمدخلة موسومة بـ "The Legal Maze of

"Artificial Intelligence: A Critical Analysis of Liability and the Challenges of Digital Transformation

مدير الجامعة



مديرة المخبر



# برنامج المؤتمر الدولي ليومي 05-06 نوفمبر 2025.



مراسيم افتتاح الملتقى على المساحة التاسعة صباحا

آيات من القرآن الكريم

النشيد الوطني



- ❖ كلمة السيدة رئيسة المؤتمر: أ.د. بورابة صورية مديرية مخبر الدراسات القانونية ومسؤولية المنهيين
- ❖ كلمة السيدة: أ.د كريمة محروق مديرية مخبر الدراسات القانونية التطبيقية جامعة قسنطينة 1
- ❖ كلمة السيد: أ.د. بركات أحمد عميد كلية الحقوق والعلوم السياسية
- ❖ كلمة السيد: أ.د برازي بوجمعة مدير جامعة طاهري محمد
- ❖ كلمة السيد: احمد بن يوسف والي ولاية بشار والإعلان الرسمي عن افتتاح أعمال المؤتمر الدولي.

برنامنج المؤتمر الدولي ليوم 05 نوفمبر 2025.

رئيسية الجلسات: أ.د. ابن خليفه سميرة



<https://meet.google.com/bqu-zccd-ezc>



العنوان المشاركة	مؤسسة الانتماء	اسم ولقب المشارك	الوقت
الإطار المظاهري للذكاء الاصطناعي	جامعة غليزان جامعة تيسمسيلت	د. بلوس براهيم د. عيسى اسيا زكريا	10:00-10:10 سا
ثورة الذكاء الاصطناعي في عالم القانون تحديات ومخاوف توظيف الذكاء الاصطناعي	جامعة طاهري محمد بشار	أ.د. لعرياوي نبيل صالح	10:10-10:20 سا
الأساس القانوني والتقيي للطائرة بدون طيار في التشريع الجزائري	جامعة جيلالي ليابس سيدى بلعباس	أ.د. معوان مصطفى	10:20-10:30 سا
آليات تطوير الذكاء الاصطناعي (A.I) لمكافحة الجريمة السيبرانية دراسة تطبيقية للجوانب الأمنية والتشريعية	المركز العربي للدراسات السياسية والإستراتيجية- مصر	أ. د. محمد صادق اسماعيل	10:30-10:40 سا
الذكاء الاصطناعي كأداة مبتكرة لكشف الجرائم: نحو مستقبل أمني أكثر أماناً	جامعة نجران المملكة العربية السعودية	د. هاله محمد امام محمد	10:40-10:50 سا
الحماية القانونية للخصوصية الرقمية من مخاطر الذكاء الاصطناعي	جامعة مرسي عبد الله بيبيارة جامعة الجيلالي بونعامة بخميس مليانة	أ.د مناع العلجة أ.د آيت عبد المالك نادية	10:50-11:00 سا
مسؤولية الدولة عن استخدام الرقمنة في إدارة مراقبتها	جامعة طاهري محمد بشار	أ.د سميرة ابن خليفة	11:00-11:10 سا
المسؤولية المدنية عن استخدام الذكاء الاصطناعي في مهب المصالح: الاتحاد الأوروبي يتردد تحت ضغط اللobbies	الجامعة اللبنانية - لبنان	د.اودين سلوم	11:10-11:20 سا
لوحة التحكم الذكية- نحو الادرة الرقمية للمحتوى الاعذاعي	نائب مدير التحول الرقمي للإذاعة الجزائرية	السيد تيبي عبد الحميد	11:20-11:30 سا
المسؤولية المدنية عن الذكاء الاصطناعي بين تجاذبات تطوير القواعد العامة ومبررات استحداث أحكام خاصة-	جامعة الجيلالي بونعامة خميس مليانة جامعة عبد الله مرسي .بيبارة	أ.د. علال طحطاح أ.د. عبد النور زيدان	11:30-11:40 سا
الإطار القانوني للمسؤولية الجزائرية عن أعمال الذكاء الاصطناعي	الجامعة الإسلامية بميسوتا-أمريكا	د.حسن حرب اللصاصمه	11:40-11:50 سا

Legal Accompaniment of AI Use in Banking Operations via Fintech in Algeria	Research Center in Applied Economics for Development (CREAD) Research Collaborator at the Center	Dr. Nadjib Allah Hakmi Dr. Khaled Magoura	12:00-11:50
الذكاء الاصطناعي بين المسؤولية القانونية والمساءلة الأخلاقية المساءلة القانونية عن تأثير الذكاء الاصطناعي على التلاعب بالمعلومات	جامعة أكتوبر للعلوم الحديثة والآداب - مصر جامعة الاخوة متوري قسطنطينة 1	د. رانيا عبد المنعم عبد الحميد أ.د. كريمة محروق	12:10-12:00 12:20-12:10
مناقشة			13:00-12:20



رئيسة الجلسة: د. سعدية قي

<https://meet.google.com/njq-skqx-buf>

برنامج الورشات ليوم الأول: 05 نوفمبر 2025  
تبدأ 14:30 و 10 دقائق لكل متدخل

عنوان المشاركة	مؤسسة الانتماء	اسم ولقب المشارك	التوقيت
حماية الخصوصية الرقمية ومصداقية المعلومة: التحديات الأخلاقية لاستخدام الذكاء الاصطناعي في صناعة المحتوى من وجهة نظر مستخدمي منصات الإعلام الجديد في الجزائر.	جامعة يحيى فارس بالمدية جامعة الجزائر	أ.د. أوروان هارون ط.د. ضويفي محمد	14:40-14:30
الذكاء الاصطناعي وتحديات البحث العلمي والملكية الفكرية	جامعة صالحى احمد بنالنعامة	أ.د عماري نور الدين	
إطار المسؤولية القانونية عن أضرار الذكاء الاصطناعي: من نموذج مسؤولية المنتج إلى نموذج الخوارزمية	جامعة سطيف	د.ملوك محفوظ	
الحماية الجنائية للحياة الخاصة في مواجهة انتهاكات الذكاء الاصطناعي في القانون الجزائري	جامعة ميلة	د. ابتسام رمضانى	
Artificial intelligence (AI) comes with both advantages and disadvantages	University of chelef University of Algiers 3, Algeria	Dr. Mohammed Mostefa behar Dr. Salhi Nadia	
حماية البيانات ذات الطابع الشخصي على ضوء الامر 07/18	جامعة الجزائر 1	د. كروان سمية ط.د. كروان اسماء	
أثر التحول الرقمي على الحق في الخصوصية	جامعة الصالحي احمد بنالنعامة	د.بوفلحة عبد الرحمن	

الشخصية القانونية للذكاء الاصطناعي بين التأييد والمعارضة	جامعة طاهري محمد بشار	د. راجي عزيزة د. بوحزمة نصيرة	
حماية الحق في الخصوصية المعلوماتية في ضوء الذكاء الاصطناعي في الجزائر	جامعة مولاي الطاهر، سعيدة	د. حمادو دحمان د. حمادو فاطيمة	
المسؤولية الجنائية عن أخطاء الذكاء الاصطناعي في التشريع الجزائري " دراسة في النطاق الشخصي للمسألة"	جامعة طاهري محمد بشار	د. بوشةة خالد	
الوصف(التكيف) القانوني لبرنامج الوكيل الذي الافتراضي	جامعة عبد الرحمن ميرة- بجاية	ط.د. سمية خذيري	
انتهك الحق في الخصوصية في عصر الذكاء الاصطناعي: المخاطر والحماية القانونية في التشريع الجزائري	جامعة تبزي وزو	ط.د. لونيس إسماعيل أ.د. سامية كصال	
نشاق وتطور الذكاء الاصطناعي	جامعة طاهري محمد بشار	د. درسي يمينة	

مناقشة

تبدأ 14:30 و 10 دقائق لكل متدخل

<https://meet.google.com/tdf-mnbb-ebc>

رابط الورشة

رئيسة الجلسة: د. هدى بن جيمة

عنوان المشاركة

الآليات البديلة للتعويض عن أضرار الذكاء الاصطناعي	مؤسسة الانتماء جامعة عين تموشنت	اسم ولقب المشارك د. مجاحي سعاد
نظرة عن كثب في أساسيات الذكاء الاصطناعي	المركز الجامعي - مغنية -	د. عبد الحليم مجدوب
الذكاء الاصطناعي: بين مطروقة الحق في تداول المعلومة وسندان التمكين من الجريمة	جامعة 8 ماي 1945 قالمة	د. لينة بوزيتونة د. بورجيبة اسيا
تطبيق نظرية المخاطر كآلية دولية لضمان المسؤولية القانونية عن أضرار الذكاء الاصطناعي	جامعة قسطنطينة 1	د. مريم حلايمية
المسؤولية الجنائية عن استخدام تقنيات الذكاء الاصطناعي في التزاعات المسلحة	جامعة طاهري محمد بشار	د. بن جيمة هدى
إشكالية البيانات الشخصية في البيئة الرقمية بين الخصوصية الشخصية والإتاحة الحرة للبيانات	جامعة تيسمسيلت	د. مناصرية حنان
الطفولة والوسائل الرقمية في الجزائر: المكتسبات الوطنية وأليات الوقاية من المخاطر	مركز البحث في الأنثروبولوجيا	د. هند بوعقادة



ال社会效益ية والثقافية، وهران		
جريمة التزوير الإلكتروني المدعوم بالذكاء الاصطناعي في ظل القانون الجزائري	جامعة أم البوافي	د.وفاء عمران
تأثير الذكاء الاصطناعي على مستقبل الوظائف القانونية	جامعة بجایة مديرية أملاك الدولة - مستغانم	د. وهيبة رابح نعيمة رابح
المسؤولية الجنائية عن الجرائم المرتكبة باستخدام تقنيات الذكاء الاصطناعي في ظل التشريع المصري "دراسة تحليلية".	جامعة الجيلالي بونعامة خميس مليانة	د. يعقوبي خالد
المسؤولية الجزائية عن انتهاك الحق في الخصوصية بواسطة تقنيات الذكاء الاصطناعي	جامعة مستغانم	د. بن قطاط خديجة
حماية البيانات الشخصية في ظل خوارزميات الذكاء الاصطناعي	جامعة محمد الصديق بن يحيى - جيجل	ط.د. لوط حميدة
إشكالية إسناد المسؤولية الجنائية عن استخدام تقنيات الذكاء الاصطناعي	جامعة تلمسان	ط.د. فرحات سمير

مناقشة



تبدأ 14:30 و 10 دقائق لكل متدخل

<https://meet.google.com/oek-runp-wkv>

التوقيع	اسم ولقب المشارك	مؤسسة الانتماء	عنوان المشاركة
د. عشبوش محمد	د. عشبوش محمد	جامعة أحمد زيانة غليزان	تطبيقات الذكاء الاصطناعي في المجال الأمني (الشرطة التنبؤية)
د. عطوي وداد	د. عطوي وداد	جامعة مرسلي عبد الله- تيزيز	التحديات القضائية في إثبات المسؤولية المدنية على الأضرار الناتجة عن أنظمة الذكاء الاصطناعي
د. عفان يونس د. بن سهيل لخضر	د. عفان يونس د. بن سهيل لخضر	جامعة محمد لمن دباغين سطيف 2	المسؤولية الدولية عن أضرار التي تسببها أسلحة الذكاء الاصطناعي ذاتية التشغيل
د. عقيبي يمينة د. بوكايس سميرة	د. عقيبي يمينة د. بوكايس سميرة	جامعة عين تموشنت	المسؤولية عن أضرار الذكاء الاصطناعي الذاتي: إشكالات قانونية
د. حمدوني علي د. طيار منى	د. حمدوني علي د. طيار منى	جامعة عبد الحفيظ بوالصوف-ميلة جامعة الجزائر 1	اثبات الشخصية القانونية للذكاء الاصطناعي

الشخصية القانونية للروبوتات الذكية بين المنع والمنع	جامعة محمد البشير الإبراهيمي برج بوعريريج	د. غري حورية	
تحديات تطبيق قواعد المسؤولية العقدية للتعويض عن أخطاء الذكاء الاصطناعي	جامعة محمد الصديق بن يحيى جيجل	د. فاطمة الزهراء بوقطة	
إشكال تحديد الطبيعة القانونية للوكيل المؤتمت	جامعة حسيبة بن بوعلي بالشلف	د. قلواز فاطمة الزهراء	
<b>The Role of Self-Regulation and Ethical Guidelines in Constructing a Complementary Liability Framework for Artificial Intelligence: Modern Trends towards AI Governance Preceding Legislative Intervention.</b>	<b>Université Tahri Mohamed Béchar</b>	<b>Dr.Bourbaba Elhouaria Pr.Kadri Syham</b>	
تجليات الذكاء الاصطناعي على العدالة في الجزائر	جامعة غردية	د. لحوش عبد الرحيم د. زرباني عبد الله	
التطبيقات الذكية مقاربة مفاهيمية	جامعة يحيى فارس بالمدية	د. لزار سميرة	
اشكالية تطبيق المسؤولية الجنائية على جرائم الذكاء الاصطناعي	جامعة بجایة	د. عبدالـيـ حمـيـدة	
المسؤولية الجنائية عن الجرائم المرتكبة عبر الأنظمة ذاتية التعلم (الروبوتات أو السيارات ذاتية القيادة)	جامعة علي كافي- تندوف	د. بن نور مختار	
اشكالية المسؤولية الجزائية عن اساءة استغلال الذكاء الاصطناعي	جامعة طاهري محمد بشار	ط.د. لعمري انتصار	

مناقشة

تبدأ 14:30 و 10 دقائق لكل متدخل

الرابـيـ سـالـجـلـسـةـ أـدـ جـارـدـ مـحـمـدـ

<https://meet.google.com/bqu-zccd-ezc>



التوقيع	اسم ولقب المشارك	مؤسسة الانتماء	عنوان المشاركة
د. بلبشير يعقوب أ. د. دلالي جيلالي	جامعة حسيبة بن بوعلي الشلف	المسؤولية المدنية في ظل الثورة الرقمية: نحو نموذج مستحدث لقواعد المسؤولية التقتصيرية عن مخاطر استخدام النظم والآلات الذكية	
Dr. LAHLOU Sihem	Saad Dahleb University	<b>Optimization of Architectural Processes through Artificial Intelligence: Towards Sustainable Rehabilitation of the Casbah of Algiers within the Framework of Urban Planning Rights</b>	
د. خرشف فاطمة	جامعة يحيى فارس المدية	الاطار القانوني والتنظيمي الدولي والإقليمي للذكاء الاصطناعي	

الشخصية القانونية للروبوت الذكي بين الواقع والتطبيق	جامعة علي كافي تندوف	د. ناصيري ربيعة د. بوحزمة كوثر
المسؤولية المدنية للروبوتات الطبية بين الأفاق القانونية والتحول الرقمي	جامعة أبو بكر بلقايد تلمسان	د. رحمونة قشيوش
المسؤولية التقصيرية عن استخدامات الذكاء الاصطناعي بين صعوبة التطبيق وحتمية التجديد	جامعة الجزائر 1	د. زينب لونادي
تأثير الذكاء الاصطناعي على الجريمة الالكترونية	جامعة ادرار	د. عثمانى التهامى
المركز القانوني للذكاء الاصطناعي على ضوء قواعد المسؤولية المدنية	جامعة المدية	د. شبايكى نزهة
المسؤولية الجزائية عن جرائم المركبات المسيرة ذاتيا	جامعة 08 ماي 1945 - قالمة.	د. شرايرية محمد
المسؤولية المدنية الناجمة عن أنظمة الذكاء الاصطناعي في ظل التشريع الجزائري- التحديات والطلعات	جامعة مرسلى عبد الله - تبازة	د. شريط نسيم
قراءة في المفاهيم الأساسية والنماذج المعرفية للذكاء الاصطناعي	جامعة حسيبة بن بوعلي بالشلف	د. شواش صلاح الدين
تأثير استخدام الذكاء الاصطناعي في تحقيق أهداف التنمية المستدامة -مقاربة قانونية-	جامعة الجزائر 1	د. صبرينة تونسي
دور الذكاء الاصطناعي في تحقيق العدالة الجنائية	جامعة تلمسان	د. عبد العالى بن خوان
إشكالات تقرير المسؤولية الجنائية التقليدية للروبوت الاصطناعي	جامعة احمد زيان غليزان	أ.صوفى بن داود
الطبيعة القانونية الاستخدام تطبيقات الذكاء الاصطناعي	جامعة الشهيد حمہ لخضر بالوادي	د.قني سعدية
الذكاء الاصطناعي وتطبيقاته	جامعة طاهري محمد بشار	د.ضييف الله أسماء د. ضييف الله وفاء
حماية الملكية الفكرية من مخاطر تطبيقات الذكاء الاصطناعي و الرقمنة لتعزيز الابتكار و التناصصية	جامعة تسمسليت	د. محمد لخضاري
تحديات الذكاء الاصطناعي على الامن الجماعي	جامعة طاهري محمد بشار	د. لمي حنان



تبدأ 14:30 و 10 دقائق لكل متدخل

رئيسة الجلسة: د. بن نور زينب

<https://meet.google.com/nhy-yaqk-aba>

## الورشة العلمية الخامسة: رابط الجلسة

التوقيت	اسم ولقب المشارك	مؤسسة الانتماء	عنوان المشاركة
14:40-14:30	د. سعيود زهرة	جامعة الجزائر 1	الذكاء الاصطناعي كمفهوم حديث: المفهوم، الأنواع، المجال
	أ.د. بشور فتحية أ.د. خلوفي خدوجة	جامعة أكلي مهند أول حاج- البويرة	قواعد المسؤولية التقتصيرية في مواجهة للذكاء الاصطناعي قراءة في القانون الفرنسي
	أ.د. دوار جميلة	جامعة محمد البشير الإبراهيمي- برج بوعريج-	مقتضيات العلاقة بين أنظمة الذكاء الاصطناعي و الطاقات المتعددة (مشروع الشجرة الذكية نموذجا)
	د. كتاب زاهية	جامعة عبد الحميد بن باديس مستغانم	تحديات القانون الدولي في تنظيم تقنيات الذكاء الاصطناعي الناشئة
	د. طبوش احمد د. مالكي طارق	جامعة طاهري محمد بشار	مستقبل البحث العلمي في مهب الذكاء الاصطناعي فرص وتحديات أخلاقية و منهجية
	د. نسيير فريزة	جامعة مولود معمرى تبزي وزو	مفهوم التطبيقات الذكية: دراسة تحليلية شاملة
	د. بنور زينب د. بوزيدي بوعلام	جامعة طاهري محمد بشار	المسؤولية القانونية عن قرارات الذكاء الاصطناعي (Claude, chat GPT, Gemini) في المجال الأكاديمي
	د. يخلف عبد القادر	جامعة الأغواط	من الأجهزة إلى المعطيات: أبعاد الحماية الجزائية للبيانات في العصر الرقمي
	د. خالدي صفاء هاجر د. بوراس صلاح الدين	جامعة غرداية	الحماية القانونية للمعطيات الشخصية في ظل التطبيقات الذكية في التشريع الجزائري
	د. حليمة ذكراوي ط. دعائشة بوعافية	المركز الجامعي -أفلو	الذكاء الاصطناعي تحدٍ جديد لقواعد المسؤولية المدنية
	ط. د. فارج يوسف	جامعة الشهيد الشيخ العربي التبسي - تبسة -	الذكاء الاصطناعي في صناعة الالتحاقات: اشكالية تحديد المسؤولية القانونية بين المطوريين، النظمات والخوارزميات



تبدأ 14:30 و 10 دقائق لكل متدخل

رئيس الجلسة: د. محمد مصطفى بحر

<https://meet.google.com/yrq-imdi-zcn>

الورشة العلمية السادسة: رايط الورشة

التوقيت	اسم ولقب المشارك	مؤسسة الانتماء	عنوان المشاركة
أ.د. نجوى عمريش	جامعة عبد الحميد مهري- قسنطينة 2-	الذكاء الاصطناعي قراءة في المفهوم والتطبيقات المعرفية المرتبطة به	
أ.د.بركاتات كريمة	جامعة أكلي محنـد أول حاج بالبـورـة	طبيعة وأسس المسؤولية المدنـية عن أضرار الذكاء الاصـطـنـاعـي	
د. بـسـعـديـ نـورـة	جامعة محمد بن أـحمدـ وـهـرـانـ 2	إـعادـةـ النـظـرـ فيـ أـسـاسـ المـسـؤـلـيـةـ المـدنـيـةـ فيـ ظـلـ الذـكـاءـ الـاصـطـنـاعـيـ (ـمـنـ الـخـطـأـ نـحـوـ اـعـتـمـادـ أـسـسـ)	ـ بـدـيـلـةـ)
دـ.ـ صـفـرـةـ بـشـيرـةـ	جـامـعـةـ يـحيـيـ فـارـسـ الـمـدـيـةـ	الـحـقـ فيـ الـخـصـوصـيـةـ بـيـنـ تـحـديـاتـ الذـكـاءـ الـاصـطـنـاعـيـ وـمـتـطـلـبـاتـ الـحـمـاـيـةـ الـقـانـوـنـيـةـ	
دـ.ـ بـوـنـاصـرـ إـيمـانـ	جـامـعـةـ عـمـارـ ثـلـيـجـيـ الـأـغـواـطـ	نـظـمـيـ الـمـسـؤـلـيـةـ وـالـتـأـمـيـنـ عـلـىـ مـخـاطـرـ الذـكـاءـ الـاصـطـنـاعـيـ كـأـحـدـ مـسـتجـدـاتـ الـتـكـنـوـلـوـجـيـاـ	
دـ.ـ نـبـيلـ مـقـدـرـ	جـامـعـةـ جـيـلـالـ لـيـابـسـ سـيـديـ بـلـعـبـاسـ	إـتـجـاهـاتـ إـقـرـارـ الـمـسـؤـلـيـةـ الـجـنـائـيـةـ لـلـذـكـاءـ الـاصـطـنـاعـيـ	
دـ.ـ حـبـيـبـةـ بـنـ عـمـارـ	جـامـعـةـ تـيـارـتـ	نـحـوـ مـسـؤـلـيـةـ جـدـيـدـةـ عـنـ إـسـتـخـدـامـاتـ الذـكـاءـ الـاصـطـنـاعـيـ فـيـ ظـلـ الـمـبـادـيـعـ الـعـامـةـ لـلـقـانـونـ الـمـدـنـيـ	
دـ.ـ بـوـطـبـلـ خـدـيـجـةـ	جـامـعـةـ حـسـيـبـةـ بـنـ بـوـعـلـيـ بـالـشـلـفـ	انـعـكـاسـاتـ وـتـأـثـيـرـاتـ الذـكـاءـ الـاصـطـنـاعـيـ عـلـىـ الـفـرـدـ وـالـمـجـتمـعـ وـعـلـىـ حـقـوقـ الـإـنـسـانـ وـالـحـرـيـاتـ الـعـامـةـ	
دـ.ـ سـارـةـ قـرـيمـسـ	جـامـعـةـ الشـاذـلـيـ بـنـ جـدـيدـ الطـارـفـ	الـمـسـؤـلـيـةـ الـجـزـائـيـةـ الـتـاجـمـةـ عـنـ اـسـتـخـدـامـ تـطـبـيـقـاتـ الذـكـاءـ الـاصـطـنـاعـيـ	
دـ.ـ زـيـادـ مـحـمـدـ أـنـيـسـ	جـامـعـةـ مـولـودـ مـعـمـريـ بـتـيـزـيـ وـزوـ	مـارـسـاتـ الذـكـاءـ الـاصـطـنـاعـيـ وـحـقـوقـ الـإـنـسـانـ	
دـ.ـ سـلـامـيـ أـمـالـ	جـامـعـةـ قـسـنـطـيـنـيـةـ 1ـ الـاخـوـةـ مـنـتـورـيـ	استـجـاهـاتـ التـشـرـيعـ لـثـورـةـ الذـكـاءـ الـاصـطـنـاعـيـ:ـ الـفـجـوةـ التـشـرـيعـيـةـ وـالـتـحـديـاتـ	
دـ.ـ فـهـيـمـةـ مـرـزوـقـيـ	جـامـعـةـ مـحـمـدـ الشـرـيفـ مـسـاعـدـيـ،ـ سـوقـ أـهـرـاسـ	أـسـاسـ قـيـامـ الـمـسـؤـلـيـةـ الـمـدـنـيـةـ عـنـ أـسـرـارـ اـسـتـخـدـامـ تـقـنـيـةـ الذـكـاءـ الـاصـطـنـاعـيـ	
دـ.ـ دـرـيـسيـ رـبـيعـةـ	جـامـعـةـ طـاهـريـ مـحـمـدـ بـشـارـ	الـمـسـؤـلـيـةـ الـقـانـوـنـيـةـ عـنـ فـعـلـ أـجـهـزـةـ الذـكـاءـ الـاصـطـنـاعـيـ	
دـ.ـ بـوـزـيـدـيـ نـورـةـ	جـامـعـةـ طـاهـريـ مـحـمـدـ بـشـارـ	الـوـضـعـيـةـ الـقـانـوـنـيـةـ لـلـرـوـبـوـتـاتـ الذـكـاءـيـةـ:ـ نـحـوـ تـقـنـيـنـ الـشـخـصـيـةـ الـقـانـوـنـيـةـ لـلـرـوـبـوـتـاتـ الـمـسـتـقـلـةـ	
مناقشة			



تبدأ 14:30 و 10 دقائق لكل متدخل

رئيس الجلسة: د. عاللي نصيرة

<https://meet.google.com/jzb-zdzt-bpx>

الورشة العلمية السابعة: رابط الجلسة

التوقيت	اسم ولقب المشارك	مؤسسة الانتماء	عنوان المشاركة
د. شهيناز صبيحي	جامعة حسيبة بن بوعلي-الشلف-	إشكالية المسؤولية الجنائية على الجرائم الإلكترونية للذكاء الاصطناعي	
د. عبد الغني حجاب د. أسامة خوجة	جامعة محمد بوضياف - المسيلة	<b>The Legal Maze of Artificial Intelligence: A Critical Analysis of Liability and the Challenges of Digital Transformation</b>	
د. بوجلال سمية	جامعة قسنطينة 1 الإخوة منتوري	نحو توازن رقمي: حماية الحق في الخصوصية الرقمية عبر الآليات القانونية الدولية في عصر الذكاء الاصطناعي	
د. بوغزة أمينة	جامعة أحمد صالحى النعامة	إشكالات تطبيق المسؤولية المدنية عن أضرار الذكاء الاصطناعي واستخداماته	
د. تباقى روميساء	جامعة محمد خضر - بسكرة	الإطار القانوني لتطبيقات الذكاء الاصطناعي في إدارة العقار الفلاحي	
د. تدرست كريمة	جامعة مولود معمري تizi وزو	الذكاء الاصطناعي في المدن الذكية وتحديات حماية الخصوصية	
د. تواب حبيب	جامعة أبو بكر بلقايد- تلمسان	التحدي القانوني في العصر الرقمي... إعادة تشكيل قواعد المسؤولية الجنائية لضمان حقوق المتصرين من الذكاء الاصطناعي	
د. عائشة كاملي	جامعة أم البوابي	الأحكام العامة للتعاقد المؤتمت وفقا للقانون التمودجي بشأن التعاقد المؤتمت-	
أ.د. الياس سليماني أ.د. فاطمة الزهراء بلحسن	جامعة طاهري محمد بشار	المواطنة الرقمية والامن السيبراني: المسؤولية المشتركة في الفضاء الالكتروني	
د. جفري أميرة	جامعة قسنطينة 1 الإخوة منتوري	الجرائم الوطنية والدولية المرتبطة بالذكاء الاصطناعي وأسس قيام المسؤولية الجنائية على مرتکبها.	
د. حطابي أمينة	جامعة وهران 2 محمد بن أحمد	تأثير الذكاء الاصطناعي على أنظمة الملكية الفكرية: إشكالات النسبة والحقوق الشخصية القانونية لروبوت الذكاء الاصطناعي	
د. رجاء أومدور	جامعة 8 ماي 1945 قابله	المسؤولية القانونية عن خرق أمن المعلومات في الانظمة الذكية بين حماية الخصوصية ومتطلبات الامن السيبراني	
د. عروس فوزية د. عروس كوثر	جامعة طاهري محمد بشار	الذكاء الاصطناعي بين سرعة التطور التكنولوجي وجمود النص القانوني.	
د. خشيبة حنان د. خلواتي مصطفى	جامعة وهران 2 جامعة النعامة		



التحديات القانونية الناشئة عن استخدام تقنيات الذكاء الاصطناعي	جامعة طاهري محمد بشار	د. مكاوي زوبير	
اثار الذكاء الاصطناعي على المسؤولية المدنية	جامعة طاهري محمد بشار	د. علالي نصيرة د. فلقات نورة	
الذكاء الاصطناعي وحماية المعلومات الشخصية - توازن حساس في الإطار القانوني المعاصر-	جامعة سوق أهرا	ط.د. مذكور زهير	

مناقشة



تبدأ 14:30 و 10 دقائق لكل متدخل

رئيسة الجلسة: د. صديق بونعامة

[meet.google.com/qog-qacj-kds](https://meet.google.com/qog-qacj-kds)

رابط الجلسة

التوقيت	اسم ولقب المشارك	مؤسسة الالتماء	عنوان المشاركة
14:40-14:30	أ.د. شيخ محمد ذكريا	المركز الجامعي مغنية	خصوصية المسؤولية المدنية الناشئة عن أضرار أنظمة الذكاء الاصطناعي
	د. نور الدين الحبشي د. جريو محمد الامين	جامعة مصطفى سطنبولي- معسکر	المسؤولية القانونية عن الاستخدام السيئ للذكاء الاصطناعي
	د. لواهم رضا	جامعة محمد لamine دياغن- سطيف 2	الحكومة القانونية لاستخدامات الذكاء الاصطناعي- إدماج البعد الأخلاقي لضمان حماية الحقوق
	د. العربي شحط امينة	جامعة وهران 1	جدلية الشخصية القانونية للذكاء الاصطناعي
	أ.د. سعاد دولي أ.د. مبارك بن زاير	جامعة طاهري محمد بشار	التحول الرقمي في المؤسسات العامة: نحو مؤسسات بلا ورق- دروس مستفادة من تجارب دولية-
	د. حسان سعاد	جامعة طاهري محمد بشار	الشخصية القانونية للذكاء الاصطناعي بين جدلية الاعتراف ومتطلبات التنظيم
	ط.د.سامحي سمية أ. بن خدة بولفجة	جامعة طاهري محمد بشار	تطبيق أحكام المسؤولية الجنائية على جرائم الذكاء الاصطناعي
	ط.د.بوبيرطخ نوال د. بوالكور رفيقة	جامعة محمد الصديق بن يحيى- جيجل	الذكاء الاصطناعي والدليل الرقمي: قراءة في حدود الشرعية الإجرائية
	د. سعود الحاجة	جامعة محمد لamine دياغن- سطيف 2	أثر دمج الذكاء الاصطناعي في القانون الجنائي على حق الشخصية في ظل غياب الضوابط والضمادات



القانونية - المخاطرة التحديات-		
الذكاء الاصطناعي والحق في الخصوصية	جامعة محمد الصديق بن يحيى -جيجيل	ط.د.الهام هزوات د.سهيلة بوزبرة
المسؤولية الإدارية عن أضرار الذكاء الاصطناعي	جامعة قسنطينة 1	د. خديجة لعرببي
التأصيل القانوني للحق في خصوصية المعلومات الصحية في ظل التحول الرقمي	جامعة الجزائر 1	د. محمد بوجمعة ط. د. عبد الرحمن بوكتة
المسؤولية الجزائية لمطوري ومشغلي تقنيات الذكاء الاصطناعي	جامعة مصطفى اسطمبولي معسکر	د. عبد القادر صديقي
تعزيز الشفافية في عصر الذكاء الاصطناعي	جامعة طاهري محمد- بشار	ط.د. عموري زوليخة
المسؤولية الجزائية عن الاهمال باستخدام الذكاء الاصطناعي	جامعة طاهري محمد بشار	د. حنفي الحاج



برنامـج الـيـوم الثـانـي: 06 نـوفـمبر 2025 عـلـى السـاعـة 09:00 صـبـاحـا

رئيس الجلس: أ.د محتال أمنة

<https://meet.google.com/bqu-zccd-ezc>

## الجلسة العلمية الأولى: رابط الجلسة

التوقيت	اسم ولقب المشارك	مؤسسة الانتماء	عنوان المشاركة
09:09-09:00 سا	Pr.Mehtalamina Pr. Djaredmohammed	Université Tahri Mohammed Béchar	La dialectique de l'adoption de la responsabilité pénale des actes de l'intelligence artificielle
09:10-09:20 سا	أ.د. كجرا زاهية حورية	جامعة مولود معمري -تizi وزو	مدى ملائمة أحكام المسئولية المدنية لتعويض الأضرار الناجمة عن الذكاء الاصطناعي
09:20-09:30 سا	أ.د بوربابة صورية	جامعة طاهري محمد بشار	الطبيعة الخاصة للجرائم المرتكبة باستخدام الذكاء الاصطناعي
09:30-09:40 سا	د. قنلي رمضان	جامعة طاهري محمد بشار	الذكاء الاصطناعي على ضوء قواعد المسئولية المدنية
09:40-09:50 سا	د. - قمر جمال محيسن	الجامعة الإسلامية- لبنان.	المسؤولية القانونية في عصر الذكاء الاصطناعي والتحول الرقمي : بين الإبتكار التقني والفراغ التشريعي.(لبنان نموذجاً)
09:50-09:50 سا	أ.حمسة خليل عوض القيسي	جامعة برج بوعريريج، الجزائر جامعة العلوم الإسلامية العالمية، الأردن	الاطار القانوني للمسؤولية المدنية عن أضرار الميتافيبرس - دراسة مقارنة بين التشريعين الأردني والجزائري -



الذكاء الاصطناعي والمسؤولية القانونية في مجال الأمن السيبراني: تحديات وآفاق مستقبلية	جامعة أبو بكر بلقايد-تلمسان-	د. أسامه بوحمة	10:10-10:00 مسا
الذكاء الاصطناعي كأداة في الإبادة الجماعية غزة وتداعياته على القانون الدولي الإنساني	جامعة الأزهر غزة- فلسطين	الباحث / براء رائد عمر أبو علي	10:20-10:10 مسا
الحق في ملكية العقار الافتراضي خيال علمي أم حتمية قانونية	جامعة طاهري محمد بشار	د. لحلو خديجة أ.د. معاشو لخضر	10:30-10:20 مسا
When Algorithms Judge: Artificial Intelligence and Human Justice	University of Tahri Mohamed – Béchar – Algeria	Dr.Bendjima Mostefa	10:40-10:30 مسا
إشكالية المسؤولية العقدية في ظل تداعيات استعمال الذكاء الاصطناعي كطرف في التعاقد	جامعة طاهري محمد بشار	د. صديق بونعامة م. بلغنامي انتصار	10:50-10:40 مسا
Artificial Intelligence and the Redefinition of State Sovereignty: Challenges and Opportunities in the Digital Era.	Cairo University Tahri Mohamed Bechar University	Dr. Dina Taman Pr. NadjatWassilaBelghanami	11:00-10:50 مسا
The application of artificial intelligence in criminal investigations: Opportunities, ethical challenges, and the future of forensic science	University of Eloued,	Dr. Mohammed Said ZENATI	11:10-11:00 مسا
تعلم الآلة والمسؤولية القانونية الناتجة عنها	مفتاشية أملاك الدولة لولاية بشار	د. عبد الكامل علي	11:20-11:10 مسا
مبادرات تحديد الغرض من المعالجة بين متطلبات حماية المعطيات الشخصية وتحديات الذكاء الاصطناعي	جامعة محمد بن عبد الله بن العباس-سطيف 2	د. نسمة بطحي	11:30-11:20 مسا
الرسوم والتماذج الصناعية ذات الطابع الرياضي في ظل إستخدام تقنيات الذكاء الاصطناعي	المركز الجامعي نو البشير البيضا	د. مومني محمد الامين د. بن طيبة زوليخة	11:40-11:30 مسا
مناقشة/ توصيات/ والإعلان عن الاختتام			

ورشة الذكاء الاصطناعي: يوم 06/11/2025 حضوري و عن بعد



***The Legal Maze of A.I: A Critical Analysis of Liability and the Challenges of Digital Transformation***  
متاهة الذكاء الاصطناعي القانونية: تحليل نقدي للمسؤولية وتحديات التحول الرقمي



Dr. Abdelghani Hadjab/ Mohamed Boudiaf University-M'sila  
[abdelghani.hadjab@univ-msila.dz](mailto:abdelghani.hadjab@univ-msila.dz)

Dr. Oussama Khodja/ Mohamed Boudiaf University-M'sila  
[oussama.khodja@univ-msila.dz](mailto:oussama.khodja@univ-msila.dz)

**Abstract:** This report critically analyzes the emerging legal challenges and liabilities associated with the rapid development and proliferation of artificial intelligence (AI) systems. The research addresses the fundamental conflict between the autonomous and self-learning nature of AI and traditional legal frameworks predicated on direct human action and mens rea (criminal intent). The report delves into the complexities of civil and criminal liability, the black box problem, and the implications for intellectual property, privacy, and cybersecurity. It provides a comparative analysis of global regulatory approaches by proposing a conceptual framework for a flexible and adaptable legal system, this research aims to contribute to the academic discourse on AI governance and to shape future policies.

**Keywords:** Artificial Intelligence (A.I); Legal Liability; Digital Transformation; Legal Personhood; Governance.

**الملخص:** يحلل هذا التقرير بشكل نقدي التحديات والمسؤوليات القانونية الناشئة المرتبطة بالتطوير السريع والانتشار الواسع لأنظمة الذكاء الاصطناعي. يتناول البحث التعارض الجوهرى بين الطبيعة المستقلة والقادرة على التعلم الذاتي للذكاء الاصطناعي والأطر القانونية التقليدية القائمة على الفعل البشري المباشر والقصد الجنائي. يغوص التقرير في تعقيدات المسؤولية المدنية والجنائية، ومشكلة الصندوق الأسود، وانعكاسات ذلك على الملكية الفكرية والخصوصية والأمن السيبراني. كما يقدم تحليلًا مقارنًا للمناهج التنظيمية العالمية من خلال اقتراح إطار مفاهيمي لنظام قانوني من ورقاب للتكيف، يهدف هذا البحث إلى الإسهام في الخطاب الأكاديمي حول حوكمة الذكاء الاصطناعي وتشكيل السياسات المستقبلية التي توازن بين الابتكار والمساءلة.

**الكلمات المفتاحية:** الذكاء الاصطناعي؛ المسؤولية القانونية؛ التحول الرقمي؛ الشخصية القانونية.

## Introduction

The perception of the future has evolved with the development of human thought, and based on the scientific advancements, AI is now considered the topic of the age. It is the most advanced technology currently, to the point that humans find themselves simply keeping up with it rather than fully controlling it. The accelerating pace of technological development and the widespread use of AI technologies in various applications have had a profound impact on many fields, making the discussion of this topic an urgent necessity in legal, economic, political, and social domains. Reality has shown that, despite the numerous benefits and advantages of AI applications, their use has led to many problems and harms. AI systems, which can work to improve healthcare or increase efficiency in manufacturing and resource management, also possess unprecedented capabilities for data breaches and the use of algorithms that can cause fundamental problems.

## Importance and Objectives of the Research

The importance of this topic lies in seeking the legal framework for the uses of AI and defining the basis of legal liability, which is constantly evolving with the accelerating pace of technological development at both national and international levels, to establish a legal framework that can keep pace with this technological evolution. It is essential for legislators to start setting legal controls before the full-scale deployment of AI mechanisms to address the legal problems that may arise, especially in the field of legal liability. This report aims to analyze the legal issues related to AI accountability, exchange international expertise and best practices in regulating smart technologies, and contribute to the formulation of balanced legislative visions that ensure the responsible and safe use of this technology.

## Problem Statement and Questions

The use of AI systems in various fields has created unfamiliar legal problems that go beyond the limits of traditional liability based on direct human action. Self-learning software can now make decisions that may result in material or moral harm, which raises profound questions about the nature of legal liability. Should the programmer or developer bear it? Or the owner? Or is there a need to redefine the concept of liability to fit the new digital actor?

To answer this problem statement, this report addresses the following questions:

- To what extent does legal liability arise from actions committed

by AI technologies, and what is its legal basis?

- What are the dimensions of legal liability arising from the risks and harms caused by AI technologies?
- What is the impact of using AI technologies on the law in its various branches?

#### **Hypothesis:**

- The autonomous and self-learning nature of AI creates a fundamental conflict with traditional legal frameworks based on direct human action and intent. This conflict results in a liability gap, making existing laws inadequate for addressing the harms caused by AI and posing significant challenges to digital transformation.
- Traditional civil liability theories (negligence, product liability) are insufficient due to the "black box" problem and issues of causation.
- The debate over granting AI legal personhood highlights a crisis in the human-centric legal system.
- AI exacerbates legal challenges in intellectual property & privacy.
- A proactive, risk-based regulatory approach is more effective than a fragmented, reactive one in governing AI.

#### **Literature Review**

Previous research has shown that AI has become an important part of modern life, and many studies have addressed its social impacts. Few have paid enough attention to the social effects of AI robots dealing with humans, even though these systems may replace humans in several fields. The existing legal studies on the subject are often fragmented, focusing on specific aspects such as liability or intellectual property. This report aims to fill this gap by providing a comprehensive and systematic analysis that integrates the various interconnected legal challenges of AI into a single framework.

#### **Study Methodology and Structure**

This report adopts an analytical, comparative, and forward-looking methodology. It begins by defining the conceptual frameworks of AI, then moves to examine its legal nature and qualification in the context of both civil and criminal liability. Following this, the report analyzes specific legal challenges in key areas such as intellectual property, privacy, and cybersecurity. Finally, the report provides a comparative study of global regulatory models, including the EU AI Act and the US framework, concluding with insights and recommendations for a future legal approach.

## 1. Conceptual and Theoretical Framework of A.I

### 1.1. Definition and Historical Development of A.I

A.I is defined as the ability of a machine to perform cognitive functions typically associated with the human mind, such as perception, learning, reasoning, problem-solving, and even creativity. AI is an umbrella term that covers a wide range of technologies, including machine learning, deep learning, and natural language processing. AI can be classified into four main types<sup>1</sup>.

- **Reactive machines:** This is the most basic type of AI. These machines do not possess any memory of past events but only react to the present moment. They can perform advanced tasks within a very narrow scope, such as playing chess, but are incapable of performing tasks outside of their limited context.
- **Limited memory machines:** These machines have a limited understanding of past events. They can interact with the world around them better than reactive machines, like self-driving cars that use their limited memory to make turns and monitor other vehicles.
- **Theory of mind machines:** This type represents an early form of artificial general intelligence (AGI). In addition to their ability to create representations of the world, these machines would also have an understanding of other entities in the world. This type of AI is currently far from being realized.
- **Self-aware machines:** This is the theoretically most advanced type of AI, possessing an understanding of the world, others, and themselves. This is what most people mean when they talk about achieving AGI, a goal that remains a distant reality.

The term "artificial intelligence" was coined in 1956 by computer scientist John McCarthy during a workshop at Dartmouth University. The concepts it describes today existed before that; Alan Turing, the famous mathematician, introduced the idea of the "imitation game" in his 1950 paper. Following this, AI went through several phases of development, starting with Symbolic AI, which was dominant until the late 1980s and relied on the use of symbols and logical reasoning. This type of AI struggled with the complexities of the real world. In contrast, neural networks, whose roots go back to 1943, have seen explosive growth in recent years, becoming the main technology behind current developments in generative AI due to their ability to learn from massive amounts of data<sup>2</sup>.

---

<sup>1</sup> Coursera Staff (2025) What Is AI? Definition, Uses, and Types, *Coursera*, accessed 21/9/, <https://www.coursera.org/articles/what-is-artificial-intelligence>

<sup>2</sup> What is AI? (2024) *McKinsey*, accessed 21/9/2025, <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-ai>

## 1.2.The Relationship Between AI, Big Data&Internet of Things

The relationship between AI, Big Data, and the Internet of Things (IoT) is deeply intertwined. These technologies work together in an integrated system, where IoT provides the devices, Big Data provides the information, and AI provides the ability to analyze that information. IoT is a network of physical devices equipped with sensors and software that collect and exchange data. These devices, such as sensors in smart agriculture,<sup>1</sup> or self-driving cars, generate unprecedented, massive amounts of real-time data. This huge volume of data is what is known as Big Data, which cannot be stored or processed by traditional means<sup>3</sup>.

In this system, AI plays a pivotal role, providing the necessary analytical tools and capabilities to extract useful insights from the Big Data collected by IoT devices. AI enables devices to learn from their environment and make decisions without human intervention, which increases efficiency. For example, AI can analyze data from sensors to predict machine failures in the industry<sup>4</sup>, or to optimize water usage in agriculture<sup>5</sup>.

The legal challenges associated with AI are not isolated; they are a direct result of this close interdependence. The massive amount of data collected by IoT and processed by AI creates unprecedented risks to privacy. AI systems need vast amounts of data for training, and this data often includes personal and sensitive information. The collection and processing of this data without a clear purpose or explicit consent from users raises significant legal challenges in the fields of privacy and data protection<sup>6</sup>.

<sup>3</sup> Tran Anh Tu (2023) The Relationship Between Big Data and IoT. *Journal of Computing and Electronic Information Management*, Vol. 10, no. 3, p. 150-154. <https://doi.org/10.54097/jceim.v10i3.8768>

<sup>4</sup> AI in IoT: Enhancing Connectivity and Efficiency, *Device Authority*, accessed 21/9/2025, <https://deviceauthority.com/artificial-intelligence-in-iot-enhancing-connectivity-and-efficiency/>

<sup>5</sup> Sinem Sargin; Artificial Intelligence. Smart Applications and Sustainable Consumption: A Theoretical Overview (2024) *Journal of Economics Business and Political Researches*, Vol. 9, no. 25, p. 803-20. <https://doi.org/10.25204/iktisad.1461652>

<sup>6</sup> Data Privacy and the Legal Implications of Emerging Technologies, *International Journal of Emerging Technologies and Innovative Research*, Vol.10, no 11, Nov. 2023, p. 219-240, accessed 21/9/2025, <http://www.jetir.org/papers/JETIR2311433.pdf>

Therefore, the legal problem is not limited to AI itself but arises from its fundamental reliance on data produced by other technologies. While traditional law focused on human action, it now faces the challenge of determining liability in a chain of interactions between multiple systems: an IoT device that collects data, an AI program that analyzes it, and an automated decision that causes harm.

## 2. Legal Nature and Qualification of Artificial Intelligence

### 2.1. The Debate on AI Legal Personhood

The debate over granting AI legal personhood is one of the most prominent legal problems stemming from technological development. A legal person is defined as a natural or corporate entity recognized by the legal system as capable of having rights and duties.

**Arguments for Legal Personhood:** Some researchers suggest granting AI a special legal personality, sometimes called "electronic personhood" or *sui generis*, meaning of its own kind. This proposal stems from the idea that self-learning systems that can make autonomous decisions should be able to bear responsibility for their actions. This solution is seen as a way to fill the "liability gap" that arises when no natural person can be held responsible for the harm caused by AI. This argument clarifies that legal personhood is not exclusive to humans but is a social and legal construct previously used to grant corporations and legal entities rights and duties<sup>7</sup>.

**Arguments Against Legal Personhood:** In contrast, most legal scholars and legislators believe that granting AI legal personhood is currently unacceptable. This rejection is based on the principle that legal personhood is linked to essential human qualities such as consciousness, intent, and the ability to distinguish right from wrong, qualities that current AI systems lack. They argue that considering AI a legal person could diminish the responsibility of developers and operators, leading to legally unsatisfactory outcomes. Current regulatory frameworks, especially in the European Union, have rejected the idea of granting AI legal personhood. This debate is not merely philosophical; it is a direct

---

<sup>7</sup> Nadia Banteka (2024) Legal Personhood and AI: AI Personhood on a Sliding Scale. In: Lim E, Morgan P, eds. *The Cambridge Handbook of Private Law and Artificial Intelligence*. Cambridge Law Handbooks. Cambridge University Press, p. 618-635. <https://doi.org/10.1017/9781108980197.033>

response to the inadequacy of existing legal theories, such as tort and agency law, to sufficiently determine liability for AI-induced harm<sup>8</sup>.

The existence of this debate itself reveals a fundamental crisis in the legal system, as it faces a clash between its human-centric nature and the reality of a new actor that possesses intelligence but is not human. The rejection of this path by most jurisdictions indicates a preference for amending existing laws rather than creating a new "legal type."

## 2.2. Legal Capacity and Agency in the Context of AI

Given the refusal to grant AI legal personhood, some researchers have resorted to qualifying it as a legal "agent" acting on behalf of its human principal. Under this qualification, the principal (the programmer, owner, or user) bears responsibility for the harms caused by the AI, similar to a principal's liability for the actions of their agent. This approach faces significant challenges due to the autonomous and unpredictable nature of AI systems. While a human agent always has some degree of autonomy, their actions remain within the ultimate control of the principal. In the case of self-learning AI systems, they may act in ways that are unpredictable or uncontrollable by the programmer or user<sup>9</sup>. This makes it difficult to prove that the harm was within the human principal's control. The problem is not the lack of human intent but the impossibility of proving foreseeability or control, making the traditional legal solution insufficient.

## 3. The Civil Liability Regime for AI-induced Damages

### 3.1. Challenges to Traditional Civil Liability Frameworks

Traditional civil liability frameworks, which rely on the difficult proof of causality between an action and harm, are entirely unsuitable for dealing with harms caused by AI.

**Inadequacy of Negligence-Based Liability:** Traditional negligence law is inappropriate for determining AI liability because

---

<sup>8</sup> Bart Custers; Henning Lahmann; Benjamyn Scott (2025) From liability gaps to liability overlaps: shared responsibilities and fiduciary duties in AI and other complex technologies. *AI & Soc*, Vol. 40, p. 4035–4050.

<https://doi.org/10.1007/s00146-024-02137-1>

<sup>9</sup> AI Systems and Liability: An Assessment of the Applicability of Strict Liability & A Case for Limited Legal Personhood for AI, *The St Andrews Law Journal*, Vol. 3 No. 1, 2023. <https://doi.org/10.15664/stalj.v3i1.2645>

---

it is based on the "reasonable person" standard. This standard requires proving that a reasonable person should have foreseen the risk of harm and taken reasonable precautions to avoid it. But in the case of autonomous, self-learning systems, it becomes nearly impossible to prove that any person "should have noticed that something was wrong"<sup>10</sup>. This leads to unfair legal outcomes, where victims may be left without compensation, or liability is shifted to the closest party in the chain, even if they were not actually responsible.

**The "Black Box" Problem:** It is the most prominent challenge in civil liability. This problem refers to the fact that complex AI systems, especially those using deep learning, operate in a way that cannot be easily explained or understood, even by the programmers who created them. This makes it extremely difficult to prove a "defect" in the system or to establish "causation" between the system's action and the resulting harm. As a result, the plaintiff faces "excessive difficulties" in providing the technical or scientific evidence needed to prove their case<sup>11</sup>.

### 3.2. Product Liability and the Concept of a "Defect"

Product Liability is one possible legal approach to determine liability for AI harm. This theory, especially under the European Product Liability Directive, faces significant challenges:

- **Definition of "Product":** The European Product Liability Directive focuses on physical products in linear value chains. Software that is not embedded in a physical device does not easily fit this definition, leaving a legal gap<sup>12</sup>.
- **Concept of a "Defect":** It becomes complicated with self-learning systems. The system may cause harm while working "exactly as intended", or it may become "defective" as a result of

---

<sup>10</sup> Baris Soyer; Andrew Tettenborn (2022) AI and civil liability: do we need a new regime?, *International Journal of Law and Information Technology*, Vol. 30, no 4, p. 385–397, <https://doi.org/10.1093/ijlit/eaad001>

<sup>11</sup> Megan Howarth; Katie Chandler; Philipp Behrendt (2025) AI liability: who is accountable when AI malfunctions?, *Taylor Wessing*, accessed 21/9/2025, <https://www.taylorwessing.com/en/insights-and-events/insights/2025/01/ai->

<sup>12</sup> Vibe Ulfbeck (2024) Product Liability Law and AI: Revival or Death of Product Liability Law. In: Lim E, Morgan P, eds. *The Cambridge Handbook of Private Law and Artificial Intelligence*. Cambridge Law Handbooks. Cambridge University Press, p. 206-226. <https://doi.org/10.1017/9781108980197.011>

its continuous learning process after being released<sup>13</sup>.

● **Proposed Legislative Solutions:** To address these issues, the European Union has sought to update its legislative frameworks. The proposed "new Product Liability Directive" aimed to expand the definition of "product" to include software and AI, regardless of how they are supplied<sup>14</sup>. The previously proposed "AI Liability Directive" (which did not achieve political consensus) also introduced "rebuttable presumptions" to help plaintiffs overcome the difficulty of proving defect and causation.

### 3.3. The Role of Insurance and Risk Management

The legal uncertainty in the field of AI liability is not just a problem for victims; it is also a significant barrier to innovation and the adoption of these technologies. Companies and medical institutions, for example, are hesitant to use AI tools due to the unclear legal risks. This is where insurance comes in as a proactive solution. Well-designed insurance policies can mitigate liability risks and provide legal certainty for both developers and users. The existence of an active market for AI liability insurance can encourage the use and development of high-quality technologies because insurance companies will be more willing to underwrite products that are demonstrably safe and effective. This approach reframes liability from a punitive measure to a tool for risk management. The market itself acts as a regulator, pushing developers to build more reliable and safer systems to make them insurable. This creates a "virtuous cycle" where insurance leads to reduced risks for companies, which in turn stimulates innovation and competition, and fosters public trust in beneficial technological advancements<sup>15</sup>.

<sup>13</sup> Mark O'Shaughnessy, Challenges in establishing liability for AI-driven products: the limits of recent reforms, *Dentons*, 14/7/2025, accessed 21/9/2025, <https://www.dentons.com/en/insights/articles/2025/july/14/challenges-in->

<sup>14</sup> Ibid.

<sup>15</sup> Ariel Dora Stern; Avi Goldfarb; Timo Minssen; Nicholson Price (2022) AI Insurance: How Liability Insurance Can Drive the Responsible Adoption of AI in Health Care. *New England Journal of Medicine Catalyst*, Vol. 3, no. 4. <https://doi.org/10.1056/CAT.21.0242>

Liability Theory	Basic Requirements	Applicability to AI	Main Challenges
Negligence	Proof of duty of care, breach, harm, and causation	Highly problematic	Difficulty in proving human negligence or foreseeability
Product Liability	Proof of product defect, harm, and causation	Applicable with modifications	Defining "product" and "defect" in self-learning software systems
Strict Liability	Proof of harm and causation without needing to prove fault	A possible solution in specific cases	May stifle innovation and impose unfair liability on developers
Agency	Proof that the AI was acting as an agent for a human principal	Limited applicability	AI's autonomy may make it act outside the principal's control
Shared Liability	Attributing partial responsibility to each party involved in the system's lifecycle	A new and suitable approach	Requires a flexible legal framework to distribute responsibility

#### 4. The Legal Landscape of Criminal Liability for A.I

##### 4.1. The Principle of Mens Rea and AI

The principle of mens rea (criminal intent) is one of the fundamental pillars of criminal law, as a crime cannot be proven without establishing a culpable state of mind in the perpetrator. This concept, based on intent, knowledge, and negligence, is fundamentally human. The core clash between AI and criminal law

lies in the fact that a machine, by definition, lacks a mind and cannot possess criminal intent<sup>16</sup>.

The most common legal approach is to view AI as merely a "tool" or a "sophisticated gun". Under this qualification, criminal liability falls on the human who used the tool to commit the crime, just as the responsibility for a murder falls on the person who uses a gun, not the gun itself. The self-learning nature of AI and the unpredictable capabilities it can develop make this traditional approach insufficient.

#### 4.2. Attributing Criminal Liability: The Developer, the User, and the System Itself

Attributing criminal liability for harm caused by AI requires a re-evaluation of the traditional roles of responsibility.

- **The User:** In cases where AI is used deliberately to commit a crime, liability falls directly on the user. This includes "malicious interactions" aimed at producing illegal content or facilitating other criminal activities like fraud or information manipulation<sup>17</sup>.
- **The Developer:** Attributing criminal liability to developers is a more complex matter. It is difficult to determine whether a developer could have foreseen the misuse of a self-learning system. While some argue that exempting developers from any criminal liability could lead to "highly negative social consequences", others believe that holding them responsible for predicting all potential harms could stifle innovation unreasonably. Some researchers believe that attributing responsibility to developers is unjustified, especially in the case of strong AI that has the ability for self-learning and conscious, volitional behavior<sup>18</sup>.
- **The AI Itself:** Although this is a controversial proposition, some

<sup>16</sup> Hakan Kan (2024) Criminal liability of AI from the perspective of criminal law: an evaluation in the context of the general theory of crime and fundamental principles, *International Journal of Eurasia Social Sciences*, Vol. 15 no. 55.

<https://doi.org/10.35826/ijoes.4434>

<sup>17</sup> Beatrice Panattoni (2025) Generative AI and criminal law. *Cambridge Forum on AI: Law and Governance*. Cambridge University Press,

<https://doi.org/10.1017/cfl.2024.9>

<sup>18</sup> Roman Dremluga; Natalia Prisekina (2020) The Concept of Culpability in Criminal Law and AI Systems, *Journal of Politics and Law*, Vol. 13, No. 3.

<https://doi.org/10.5539/jpl.v13n3p256>

academic studies suggest that AI may, in the future, be capable of bearing criminal liability<sup>19</sup>. This idea is based on the ability of strong AI to exhibit self-learning and conscious, volitional behavior. These discussions, even if hypothetical, highlight the view of the scientific community that AI's capabilities may exceed being merely a tool.

### 4.3. The Role of AI as a Tool or Agent in Criminal Activities

The involvement of AI in crimes can be categorized into two main groups:

- **Malicious Interactions:** Where AI is deliberately used as a means to commit a crime. This includes fraud, creating illegal content such as deepfakes, and its use in terrorist activities<sup>20</sup>.
- **Dangerous Interactions:** These are unintended harms that may arise from a user's misuse of the system, its automatic behaviors, or overreliance on its decisions<sup>21</sup>.

The legal system's struggle to adapt to crimes committed by AI is, in essence, the old problem of "agency" in new clothes. AI's ability for self-learning and unpredictable automatic behaviors turns this problem from a simple agency issue into a "black box agency" problem. This development poses a new challenge for criminal law: it no longer deals with a simple tool but with an actor that is not a person yet is more than just a tool.

## 5. Legal Protection and Challenges in the Digital Age

### 5.1. Intellectual Property Rights and AI-Generated Content

The intersection of AI with intellectual property (IP) laws represents one of the most dynamic and impactful legal debates.

- **Authorship and Copyright:** The main question is whether content generated by AI can be protected by copyright. The U.S. Copyright Office and courts hold that human authorship is a fundamental requirement for this protection. A court in Washington D.C. affirmed this position in August 2023. The line between human authorship and automated content is still "blurry". If a human provides a "significant creative input," such as editing or arranging, the work may be eligible for protection<sup>22</sup>.

---

<sup>19</sup> Hakan Kan. Op.cit.

<sup>20</sup> Beatrice Panattoni, Op.cit.

<sup>21</sup> Ibid.

<sup>22</sup> Negar Bondari (2025) AI, Copyright, and the Law: The Ongoing Battle Over Intellectual Property Rights, accessed 21/9/2025,

- **AI Training and Copyright Infringement:** Major AI companies face lawsuits alleging that they illegally used copyrighted materials to train their models. This raises a debate about the "fair use" doctrine. Defendants argue that using copyrighted material for training is similar to human learning and falls under "fair use" because it does not result in a direct copy of the original work. In contrast, plaintiffs argue that AI outputs often closely resemble existing copyrighted works, which undermines the "fair use" defense<sup>23</sup>.

This debate reflects a deep economic conflict. AI developers need vast amounts of data, often copyrighted, to train their models. They argue that this use is "transformative" and should be protected under "fair use." In contrast, creators and artists see this as an existential threat to their economic viability.

## 5.2. Privacy and Data Protection in AI Systems

AI systems exacerbate existing privacy risks by enabling mass surveillance and data collection on an unprecedented scale. These systems can infer sensitive information from seemingly harmless datasets, bypassing the need for explicit consent<sup>24</sup>.

- **Algorithmic Bias:** Algorithmic bias is a serious problem, as AI systems tend to perpetuate existing social and racial inequalities due to biases in the training data. This can lead to discriminatory outcomes in fields such as employment, loan applications, and law enforcement. The problem is not a technical glitch but a direct reflection of historical and social inequalities encoded in the technology<sup>25</sup>. Addressing bias in AI forces us to confront and correct our own societal biases.

- **The Role of Regulations:** Regulations like the EU's General Data Protection Regulation (GDPR) and the California Consumer

---

<https://sites.usc.edu/iptls/2025/02/04/ai-copyright-and-the-law-the-ongoing-battle-over-intellectual-property-rights/>

<sup>23</sup> Ibid.

<sup>24</sup> Kalada Nonju; Agent Benjamin Ihua-Maduenyi (2024) The Impact of AI on Privacy Laws, *International Journal of Research and Innovation in Social Science*, p. 2150-2174. <https://dx.doi.org/10.47772/IJRISS.2024.8090178>

<sup>25</sup> Katharine Miller, Privacy in an AI Era: How Do We Protect Our Personal Information?, Stanford HAI, 18/3/2024, accessed 21/9/2025, <https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information>

Privacy Act (CCPA) are essential to balance innovation with privacy protection. These laws impose requirements on how data is collected, processed, and stored, and they compel organizations to ensure their systems comply with these regulations<sup>26</sup>.

### **5.3. Cybersecurity and the Dual-Use Nature of AI**

AI has a dual-use nature, it can be used for both defense and offense in cybersecurity. The offensive capabilities of AI are particularly dangerous, as autonomous systems can adapt and evolve in real-time at a speed that exceeds human control. This raises complex legal issues regarding accountability for autonomous cyberattacks. Due to the blurred line between human and machine decisions, it becomes difficult to attribute responsibility for collateral damage or system failures. Legal frameworks must adapt to address these new risks, including the need for transparency, oversight, and liability mechanisms for AI systems<sup>27</sup>.

### **5.4. The Challenge of Proof and Causation**

The black box problem is a comprehensive legal challenge that is not limited to civil liability. It complicates the ability to prove a defect, determine causation, and attribute accountability in various legal contexts. This difficulty in proof not only hinders civil and criminal liability cases but also adds complexity to cases of intellectual property infringement and challenges of algorithmic bias<sup>28</sup>.

The "black box" problem reveals a deeper epistemological crisis for the law. Legal systems were built on principles of evidence, traceability, and causality. When technology operates in a way that is inherently untraceable and opaque, it challenges the very foundations of how law works. This necessitates a shift in focus from how harm occurred to focusing on the risks the system poses, regardless of its internal workings.

---

<sup>26</sup> Manikanta kumar Kakarala and Sateesh Kumar Rongali (2025) Data Privacy and Security in AI. *World Journal of Advanced Research and Reviews*, Vol. 25, no. 3, p. 555-561. <https://doi.org/10.30574/wjarr.2025.25.3.0555>

<sup>27</sup> Amit Jaiswal; Prakash Chandra Mishra (2024) AI and cybersecurity law: legal issues in ai-driven cyber defense and offense. *ShodhKosh: Journal of Visual and Performing Arts*, Vol. 5, no. 6, p. 555–559.

<https://doi.org/10.29121/shodhkosh.v5.i6.2024.4144>

<sup>28</sup> Mihai Stefanoaia; Mihaela Rus (2025) AI in crime prediction: current trends and challenges, *The Proceedings of World Conference on Security Studies*, Vol. 2 No. 1, <https://doi.org/10.33422/worldsecurityconf.v2i1.1189>

## 6. Global Regulatory Frameworks and Future Directions

### 6.1. Comparative Analysis of National and International Approaches

The global regulatory landscape is diverse, with countries taking different approaches to AI governance.

- **The EU AI Act:** This law is the first comprehensive and binding legal framework for AI governance in any major jurisdiction. The law adopts a "risk-based approach". It prohibits AI systems with "unacceptable risks," such as social scoring, and imposes strict obligations on "high-risk" systems used in critical infrastructure, employment, and justice<sup>29</sup>. This approach is proactive and aims to regulate AI before it causes widespread harm<sup>30</sup>.
- **The United States:** The US approach is described as fragmented and non-binding. While important frameworks exist, such as the "NIST AI Risk Management Framework" (NIST AI RMF) and the "Blueprint for an AI Bill of Rights"<sup>31</sup>, they lack legally binding enforcement mechanisms<sup>32</sup>. This approach focuses more on innovation and self-regulation, providing voluntary guidelines for companies<sup>33</sup>.
- **Other Approaches:** Other countries have adopted different approaches. Italy, for example, passed a comprehensive law that imposes penalties on those who use AI illegally<sup>34</sup>. China, on the

<sup>29</sup> High-level summary of the AI Act, *EU AI Act*, 27/2/2024, p. 1-6. accessed 21/9/2025, <https://artificialintelligenceact.eu/high-level-summary/>

<sup>30</sup> The EU Artificial Intelligence Act: Up-to-date developments and analyses of the EU AI Act, Future of Life Institute, 2025, accessed 21/9/2025, <https://artificialintelligenceact.eu/>

<sup>31</sup> OSTP, Blueprint for an AI Bill of Rights, *The White House*, accessed 21/9/2025, <https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/>

<sup>32</sup> Grace Chintoh; Osinachi Segun-Falade; Chinekwu Odionu; Amazing Ekeh (2024) Legal and Ethical Challenges in AI Governance: A Conceptual Approach to Developing Ethical Compliance Models in the US. *International Journal of Social Science Exceptional Research*, Vol. 3, p.103-109. <https://doi.org/10.54660/IJSSER.2024.3.1.103-109>

<sup>33</sup> Xinbo Huang; Zuryati Mohamed Yusoff; Mohd Zakhiri Bin Md Nor; Mohamad Fateh Labanieh. 2024, The Legal Challenges and Regulatory Responses to AI in China. *Atlantis Highlights in Social Sciences, Education and Humanities*, p. 335-347. [https://doi.org/10.2991/978-94-6463-352-8\\_26](https://doi.org/10.2991/978-94-6463-352-8_26)

<sup>34</sup> Angela Giuffrida (2025) Italy first in EU to pass comprehensive law regulating use of AI, *The Guardian*, accessed 21/9/2025, <https://www.theguardian.com/world/2025/sep/18/italy-first-in-eu-to-pass-comprehensive-law-regulating-ai>

other hand, has taken a more centralized approach, with a Beijing court granting copyright to an AI-generated image for the first time.

•**OECD:** The Organization for Economic Co-operation and Development (OECD) laid the groundwork for global AI governance with its OECD AI Principles in 2019, which focused on values such as transparency, accountability, and fairness<sup>35</sup>.

The global regulatory landscape is characterized by divergence, with the EU choosing a proactive, rights-focused approach, while the US prefers a reactive, flexible model focused on innovation. This disparity poses a challenge for international companies and highlights a philosophical difference on the role of government in regulating technology. Some jurisdictions prioritize safety and rights at the expense of innovation, while others prefer the opposite.

Jurisdiction	Primary Regulator y Principle	Key Legislation / Frameworks	Stance on Liability	Stance on IP and Data
European Union	Risk-based	EU AI Act	Presumptio n of liability for defects with modificatio ns	Strict data protection, proof of training source
United States	Fragment ed and voluntary	NIST RMF	No unified framework	Tradition al protection, ongoing lawsuits over fair use

<sup>35</sup> James Coringrato (2025) Global Approaches to AI Regulation, *The Henry M. Jackson School of International Studies*, College of Arts and Sciences, University of Washington, accessed 21/9/2025, <https://jsis.washington.edu/news/global-approaches-to-artificial-intelligence-regulation/>

China	Centralized and directive	New Generation AI Development Plan	Companies are liable for illegal content	Grants copyright to some AI-generated works
United Kingdom	Principle-based	AI Regulation White Paper	Flexible approach with potential new legislation	Unified, principle-based approach
OECD	Non-binding principles	OECD AI Principles	General guidance for responsible innovation	General guidance for responsible innovation

### Conclusion

This report demonstrates that the core challenge of legal liability for AI lies in the tension between legal principles that are centered on humans and a technology that operates beyond our capacity for prediction and control. While traditional theories of civil and criminal liability have failed to address the "black box" problem and the complexities of causation, the global legal landscape is slowly adapting by adopting proactive, risk-management models.

The future path requires a shift in the legal mindset from a reactive approach that addresses harms after they occur to a proactive model focused on risk management from the design stage. This calls for a combination of international cooperation to establish unified standards, the enactment of flexible and adaptable legislation, and a firm commitment to humanistic principles that ensure AI remains a tool for progress, not a source of unforeseen harm.

## Recommendations for a Progressive Legal Framework

To address the complex legal challenges posed by AI, experts believe a comprehensive and forward-looking approach is necessary.

- **Flexibility and Adaptability:** Laws must be flexible and adaptable to keep pace with the rapid rate of technological development. Legislators should move away from rigid laws in favor of principle-based frameworks that can be applied in different contexts.
- **International Cooperation:** International cooperation is essential to develop consistent standards and harmonize legal frameworks. The absence of a unified framework is one of the biggest challenges in AI governance.
- **Human-Centric Approach:** AI governance should remain human-centric, ensuring human oversight, transparency, and accountability throughout the system's lifecycle.
- **Encouraging Responsible Innovation:** The goal is not to stifle innovation but to guide it toward a responsible path that respects human rights and dignity.

### References:

AI in IoT: Enhancing Connectivity and Efficiency, *Device Authority*, accessed 21/9/2025, <https://deviceauthority.com/artificial-intelligence-in-iot-enhancing-connectivity-and-efficiency/>

AI Systems and Liability: An Assessment of the Applicability of Strict Liability & A Case for Limited Legal Personhood for AI, *The St Andrews Law Journal*, Vol. 3 No. 1, 2023. <https://doi.org/10.15664/stalj.v3i1.2645>

Amit Jaiswal; Prakash Chandra Mishra (2024) AI and cybersecurity law: legal issues in ai-driven cyber defense and offense. *ShodhKosh: Journal of Visual and Performing Arts*, Vol. 5, no. 6, p. 555–559. <https://doi.org/10.29121/shodhkosh.v5.i6.2024.4144>

Angela Giuffrida (2025) Italy first in EU to pass comprehensive law regulating use of AI, *The Guardian*, accessed 21/9/2025, <https://www.theguardian.com/world/2025/sep/18/italy-first-in-eu-to-pass-comprehensive-law-regulating-ai>

Ariel Dora Stern; Avi Goldfarb; Timo Minssen; Nicholson Price (2022) AI Insurance: How Liability Insurance Can Drive the Responsible Adoption of AI in Health Care. *New England Journal of Medicine Catalyst*, Vol. 3, no. 4. <https://doi.org/10.1056/CAT.21.0242>

Baris Soyer; Andrew Tettenborn (2022) AI and civil liability: do we need a new regime?, *International Journal of Law and Information Technology*, Vol. 30, no 4, p. 385–397, <https://doi.org/10.1093/ijlit/eaad001>

Bart Custers; Henning Lahmann; Benjamyn Scott (2025) From liability gaps to liability overlaps: shared responsibilities and fiduciary

duties in AI and other complex technologies. *AI & Soc.*, Vol. 40, p. 4035–4050. <https://doi.org/10.1007/s00146-024-02137-1>

Beatrice Panattoni (2025) Generative AI and criminal law. *Cambridge Forum on AI: Law and Governance*. Cambridge University Press, <https://doi.org/10.1017/cfl.2024.9>

Coursera Staff (2025) What Is AI? Definition, Uses, and Types, Coursera, accessed 21/9/, <https://www.coursera.org/articles/what-is-artificial-intelligence>

Data Privacy and the Legal Implications of Emerging Technologies, *International Journal of Emerging Technologies and Innovative Research*, Vol.10, no 11, Nov. 2023, p. 219-240, accessed 21/9/2025, <http://www.jetir.org/papers/JETIR2311433.pdf>

Grace Chintoh; Osinachi Segun-Falade; Chinekwu Odionu; Amazing Ekeh (2024) Legal and Ethical Challenges in AI Governance: A Conceptual Approach to Developing Ethical Compliance Models in the US. *International Journal of Social Science Exceptional Research*, Vol. 3, p.103-109. <https://doi.org/10.5466/IJSSER.2024.3.1.103-109>

Hakan Kan (2024) Criminal liability of AI from the perspective of criminal law: an evaluation in the context of the general theory of crime and fundamental principles, *International Journal of Eurasia Social Sciences*, Vol. 15 no. 55. <https://doi.org/10.35826/ijoess.4434>

High-level summary of the AI Act, *EU AI Act*, 27/2/2024, p. 1-6. accessed 21/9/2025, <https://artificialintelligenceact.eu/high-level-summary/>

James Coringrato (2025) Global Approaches to AI Regulation, *The Henry M. Jackson School of International Studies*, College of Arts and Sciences, University of Washington, accessed 21/9/2025, <https://jsis.washington.edu/news/global-approaches-to-artificial-intelligence-regulation/>

Kalada Nonju; Agent Benjamin Ihua-Maduenyi (2024) The Impact of AI on Privacy Laws, *International Journal of Research and Innovation in Social Science*, p. 2150-2174. <https://dx.doi.org/10.47772/IJRRISS.2024.8090178>

Katharine Miller, Privacy in an AI Era: How Do We Protect Our Personal Information?, Stanford HAI, 18/3/2024, accessed 21/9/2025, <https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information>

Manikanta kumar Kakarala and Sateesh Kumar Rongali (2025) Data Privacy and Security in AI. *World Journal of Advanced Research and Reviews*, Vol. 25, no. 3, p. 555-561. <https://doi.org/10.30574/wjarr.2025.25.3.0555>

Mark O'Shaughnessy, Challenges in establishing liability for AI-driven products: the limits of recent reforms, *Dentons*, 14/7/2025, accessed 21/9/2025,

<https://www.dentons.com/en/insights/articles/2025/july/14/challenges-in-establishing-liability-for-ai-driven-products>

Megan Howarth; Katie Chandler; Philipp Behrendt (2025) AI liability: who is accountable when AI malfunctions?, *Taylor Wessing*, accessed 21/9/2025, <https://www.taylorwessing.com/en/insights-and-events/insights/2025/01/ai-liability-who-is-accountable-when-artificial-intelligence-malfunctions>

Mihai Stefanoaia; Mihaela Rus (2025) AI in crime prediction: current trends and challenges, *The Proceedings of World Conference on Security Studies*, Vol. 2 No. 1, <https://doi.org/10.33422/worldsecurityconf.v2i1.1189>

Nadia Banteka (2024) Legal Personhood and AI: AI Personhood on a Sliding Scale. In: Lim E, Morgan P, eds. *The Cambridge Handbook of Private Law and Artificial Intelligence*. Cambridge Law Handbooks. Cambridge University Press, p. 618-635. <https://doi.org/10.1017/9781108980197.033>

Negar Bondari (2025) AI, Copyright, and the Law: The Ongoing Battle Over Intellectual Property Rights, accessed 21/9/2025, <https://sites.usc.edu/iptls/2025/02/04/ai-copyright-and-the-law-the-ongoing-battle-over-intellectual-property-rights/>

OSTP, Blueprint for an AI Bill of Rights, *The White House*, accessed 21/9/2025, <https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/>

Roman Dremluga; Natalia Prisekina (2020) The Concept of Culpability in Criminal Law and AI Systems, *Journal of Politics and Law*, Vol. 13, No. 3. <https://doi.org/10.5539/jpl.v13n3p256>

Sinem Sargin; Artificial Intelligence. Smart Applications and Sustainable Consumption: A Theoretical Overview (2024) *Journal of Economics Business and Political Researches (İktisadi İdari Ve Siyasal Araştırmalar Dergisi)*, Vol. 9, no. 25, p. 803-20. <https://doi.org/10.25204/iktisad.1461652>

The EU Artificial Intelligence Act: Up-to-date developments and analyses of the EU AI Act, Future of Life Institute, 2025, accessed 21/9/2025, <https://artificialintelligenceact.eu/>

Tran Anh Tu (2023) The Relationship Between Big Data and IoT. *Journal of Computing and Electronic Information Management*, Vol. 10, no. 3, p. 150-154. <https://doi.org/10.54097/jceim.v10i3.8768>

Vibe Ulfbeck (2024) Product Liability Law and AI: Revival or Death of Product Liability Law. In: Lim E, Morgan P, eds. *The Cambridge Handbook of Private Law and Artificial Intelligence*. Cambridge Law Handbooks. Cambridge University Press, p. 206-226. <https://doi.org/10.1017/9781108980197.011>

What is AI? (2024) *McKinsey*, accessed 21/9/2025, <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-ai>

Xinbo Huang; Zuryati Mohamed Yusoff; Mohd Zakhiri Bin Md Nor; Mohamad Fateh Labanieh. 2024, The Legal Challenges and Regulatory Responses to AI in China. *Atlantis Highlights in Social Sciences, Education and Humanities*, p. 335-347. [https://doi.org/10.2991/978-94-6463-352-8\\_26](https://doi.org/10.2991/978-94-6463-352-8_26)