



الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة طاهزي محمد بشار
كلية الحقوق و العلوم السياسية



شهادة مشاركة

تمنح هذه الشهادة الى الدكتور(ة) عبد الغني حجاب نظير مشاركتهم في الملتقى الدولي
الموسوم بـ "السيادة الرقمية للدولة" المنظم من طرف كلية الحقوق والعلوم السياسية
أيام 11-12-13 نوفمبر 2025 بمداخلة مشتركة عنوانها:
"نماذج مؤسساتية رائدة في تعزيز السيادة الرقمية: دراسة حالة التجربة الأوروبية"

عميد الكلية

أحمد بركات
عميد الكلية
جامعة طاهزي محمد بشار



رئيس الملتقى
أحمد بركات
رئيس الملتقى الدولي
السيادة الرقمية للدولة

جامعة طاهري محمد، بشار

كلية الحقوق والعلوم السياسية



الملتقى الدولي: السيادة الرقمية للدولة، 13/12/11 نوفمبر 2025

مداخلات المحور الأول

الجلسة الأولى: 11 نوفمبر 2025. الساعة 18:00-20:00

رئيس الجلسة: الدكتور بوزيدي بوعلام رابط الجلسة: meet.google.com/oxn-jjhs-pxv

الرقم	المتدخل	عنوان المداخلة	المحور	الجامعة / المؤسسة
1	د. فاضل عائشة	"الجريمة السيبرانية والسيادة الرقمية: التحديات القانونية وآفاق المواجهة"	الأول	جامعة صفاقس. تونس
2	د. مسيكة محمد د. عبد المالك مجادة	إعادة هندسة التنظيم الإداري في ظل السيادة الرقمية: التحول المؤسسي من البيروقراطية التقليدية إلى الحوكمة الذكية	الأول	جامعة بشار
3	د. ضيف الله أسماء د. ضيف الله وفاء	السيادة الرقمية للدولة: واقع وتحديات	الأول	جامعة بشار
4	د. حسين لعريض	Digital Sovereignty: An Examination of Its Dimensions and Challenges	الأول	جامعة قسنطينة 03
5	د. بسدات لحبيب	علاقة الأمن السيبراني بالسيادة الرقمية	الأول	جامعة بشار
6	د. إيمان بودينار	Digital Sovereignty at Risk: Unpacking Political, Security, Health, and Legal Challenges	الأول	جامعة الجزائر 3
7	د. بن عمرواي فهمة	Potential Threats and Risks to State Digital Sovereignty: Challenges and Confronting Current	الأول	جامعة البليدة 2 - على



لوتيسي		Technological Transformations in the Political and Security Spheres	د. عمار عودية	
جامعة الجزائر 3	الأول	السيادة الرقمية في الجزائر - مسارات وتحديات في عالم التكنولوجيا	د. عبد العزيز ضيافي	8
جامعة باتنة 1			د. نسيم سابق	
المركز الجامعي مغنية.	الأول	تأثيرات الذكاء الاصطناعي على السيادة الرقمية - بين حماية الخصوصية والتأثير الأخلاقي والقانوني	عبد الحق عبد النور	9
تلمسان				
جامعة بشار	الأول	الحماية الدستورية للسيادة الرقمية-دراسة مقارنة-	أ.د قوراري مجدوب	10
جامعة بشار	الأول	استراتيجية مكافحة الجريمة السيبرانية لتحقيق السيادة الرقمية	د. عروس كوثر	11
			د. عروس فوزية	
جامعة بشار	الأول	مفهوم السيادة في ظل التحول الرقمي	د. سعيد ياسين	12
جامعة ورقلة	الأول	مهددات السيادة الرقمية مقارنة جيو سياسية. جامعة ورقلة	د. عائشة يدر	13
جامعة بشار	الأول	تداعيات الاجرام المنظم على السيادة الرقمية للدول.	د. بن قرية حفيظ	14
			أ.د عباسي محمد الحبيب	

الجلسة الثانية: الساعة 18:00-20:00

رئيس الجلسة: الدكتور عرابي عبد القادر رابط الجلسة: meet.google.com/gpy-jcml-atn



الرقم	المتدخل	عنوان المداخلة	المحور	الجامعة / المؤسسة
15	د. أمينة بوبصلة	السيادة الرقمية-قراءة تحليلية لأهم التحديات والتهديدات-	الأول	جامعة بومرداس.
16	د. منى طواهرية	السيادة الوطنية في ظل الحتمية الرقمية: هل فقدت الدول سيادتها في الفضاء الرقمي؟	الأول	جامعة برج بوعرييج
17	د. بليو خاري سليم. د. بلوفة وليد	انعكاسات الجرائم السيبرانية على السيادة الرقمية.	الأول	جامعة النعامة جامعة بشار
18	د. جبران سفيان د. غنو أمال	السيادة الرقمية وتأثيراتها الأمنية على الفضاء السيبراني	الأول	جامعة وهران 2
19	د. عبد القادر عرابي	الاعتماد التكنولوجي الخارجي للدول النامية بين حتمية مواكبة الثورة الرقمية ورهن استقلال القرار الوطني	الأول	جامعة بشار
20	أ. علي محمود بديار أ. النوي بن الشيخ	استراتيجيات تعزيز السيادة الرقمية للدول	الأول	المركز الجامعي ميله
21	د. بسام سامية. د. بوعلووط فازية.	مهددات السيادة الرقمية ومواجهتها في الجزائر	الأول	جامعة الجزائر (1)
22	أ.د. علي محمد. د. منيرة لعجال.	مهددات السيادة الرقمية واستراتيجيات مواجهتها	الأول	جامعة أدرار



23	ط.د عبد المالك تلي د. مومني محمد الأمين	السيادة الوطنية في مواجهة تهديدات الفضاء الرقمي	الاول	جامعة ورقلة المركز الجامعي البيض.
24	د. احمد جبار	السيادة الرقمية في وسائل الإعلام: التحديات والاستراتيجيات	الاول	جامعة خميس مليانة
25	د. بوزيان نور الدين د. شكيب أحمد دالي	السيادة الرقمية للدولة في ظل التبعية التكنولوجية - قراءة نقدية في واقع الدول النامية -	الاول	جامعة بشار
26	د. عربي بومدين	مكافحة الإرهاب الرقمي عبر الحدود: المفاهيم الاستراتيجية	الاول	جامعة بشار
27	د. عيدات عيد الغني	السيادة الرقمية في ظل التحول الرقمي اللامتناهي	الاول	

جامعة طاهري محمد. بشار

كلية الحقوق والعلوم السياسية

الملتقى الدولي: السيادة الرقمية للدولة. 11/12/13 نوفمبر 2025.

مداخلات المحور الثاني.

الجلسة الثالثة: 11 نوفمبر 2025. الساعة 18:00-20:00

رابط الجلسة: <https://meet.google.com/wuj-chqr-uge>

رئيس الجلسة: الدكتور ميمي جمال

الرقم	المتدخل	عنوان المداخلة	المحور	الجامعة / المؤسسة
1	د. حشيفة مجذوب	الجهود الدولية والإقليمية للدفاع عن السيادة الرقمية	الثاني	المركز الجامعي النعام
2	د. عرافة زوبيدة د. حسان سعاد	البعد القانوني لجريمة الإرهاب الإلكتروني	الثاني	جامعة بشار
3	د. زوقار عبد القادر	التحري الرقمي في الجرائم السيبرانية	الثاني	جامعة سيدي بلعباس
4	د/ يوسف عبد الهادي	الآليات القانونية لحماية السيادة الرقمية في الجزائر	الثاني	جامعة غليزان
5	د. زبوش عبد الرؤوف. د. زغيثي مصطفى	الإطار القانوني للسيادة الرقمية في الجزائر: بين الحماية والتطوير	الثاني	المركز الجامعي إيليزي
6	د. خالد يعقوبي د. لكحصاسي سيد أحمد	السيادة الرقمية في الصين وروسيا والهند، من منظمة التعاون الاقتصادي والتنمية (NWICO) إلى منظمة شنغهاي للتعاون (SCO) ومجموعة البريكس (BRICS)	الثاني	المركز الجامعي تندوف جامعة أدرار



7	د. سي فضيل الحاج	"متطلبات السيادة الرقمية في ظل قواعد القانون الدولي بين العولمة والحوكمة"	الثاني	جامعة معسكر
8	ط.د. عباسي بن دحمان ط.د. فتح الله علي	السيادة الرقمية للدول بين التشريعات الوطنية والانفتاح الرقمي لتحقيق التوازن الأمثل	الثاني	المركز الجامعي أفلو.
9	د. رحالي سيف الدين ط.د. لكحل نورة	نحو تعزيز الجزائر لسيادتها الرقمية من خلال منظومتها القانونية-قانون 07-18 نموذجاً	الثاني	جامعة بومرداس المركز الجامعي تيبازة
10	د. صباح حمايتي	تفعيل دور السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي كآلية لتعزيز السيادة الرقمية في الجزائر	الثاني	جامعة الوادي
11	د. ميهي جمال	السحابة والتشفير والإطار القانوني آليات تكاملية لتحقيق السيادة الرقمية الوطنية	الثاني	جامعة بشار
12	د. بن يحيى شهبناز	دور الضبط الإداري الإلكتروني في تعزيز السيادة الرقمية للدولة	الثاني	جامعة بشار
13	د. عمراني مصطفى د. بوغازي سماعيل	السيادة الرقمية في مجال الصفقات العمومية في الجزائر	الثاني	جامعة بشار
14	أ.د. غيتاوي عبد القادر د. بحماوي شريف	الأمن الرقمي كأساس للسيادة الرقمية في الجزائر: قراءة في الإطار القانوني والتحديات الوطنية	الثاني	جامعة أدرار
15	د. دريسي يمينة د. دريسي ربيعة	مكانة السيادة الرقمية في التشريعات العربية والوطنية	الثاني	جامعة بشار

جامعة طاهري محمد، بشار

كلية الحقوق والعلوم السياسية



الملتقى الدولي: السيادة الرقمية للدولة. 13/12/11 نوفمبر 2025

مداخلات المحور الثالث.

الساعة: 18:00-20:00

الجلسة الرابعة: 11 نوفمبر 2025.

رابط الجلسة: <https://meet.google.com/axk-pimp-rjw>

رئيس الجلسة : الدكتور بلباقي وهيبة

الرقم	المتدخل	عنوان المداخلة	المحور	الجامعة / المؤسسة
1	د. بلغماري وسيلة	دور السيادة الرقمية في تحقيق التنمية الاقتصادية والتكنولوجية	الثالث	جامعة عين تموشنت
2	د. هشام عليواش	ضوابط نقل البيانات الشخصية خارج الحدود الوطنية في إطار حماية حق الخصوصية في التشريع الجزائري	الثالث	جامعة الأمير عبد القادر للعلوم الإسلامية - قسنطينة
3	د/ قوراري مصطفى	التوازن بين إدماج الذكاء الاصطناعي للتحويل الرقمي وحماية البيانات والمعلومات	الثالث	جامعة بشار
4	د. وافي حاجة	أثر السيادة الرقمية على حقوق الإنسان الرقمية	الثالث	جامعة مستغانم
5	د. حمسي هلاله	"تجليات السيادة الرقمية في الخطاب السياسي الرقمي للأحزاب الجزائرية عبر شبكات التواصل الاجتماعي"	الثالث	جامعة الأمير عبد القادر للعلوم الإسلامية - قسنطينة
6	أ. عثمان غيامي ط. د. عبد الله حماني	السيادة الرقمية ودورها في تعزيز حقوق الإنسان الرقمية	الثالث	جامعة أدرار



7	د. خديجة جديلي د. سليمان حسناوي	الحق في النسيان والسيادة الرقمية: التوازن بين الخصوصية والتحكم في البيانات	الثلث	جامعة تيارت
8	د. حنافي حاج	السيادة الرقمية بين المتطلبات التنظيمية وحماية الحريات العامة	الثلث	جامعة بشار
9	ط.د. كنويزة سعيد	السيادة الرقمية والبيانات الشخصية للمواطن	الثلث	جامعة بشار
10	ركبي محمد الصديقي د. فضلون سميجة	Two-Sided Digital Sovereignty: "Clause Transparency & Governable CTI via LLMs and Visual Analytics.	الثلث	جامعة بشار
11	أ.د. خليفي مريم د. يوسفواي فاطمة	الرقمنة في ظل الإدارة الجبائية	الثلث	جامعة بشار
12	د. رجاوي عبد الرحيم د. الحسن بومسقب	التحديات الاقتصادية للسيادة الرقمية: بين تبعية التكنولوجيا الأجنبية ومخاطر الهيمنة الرقمية على الاقتصاد الوطني	الثلث	جامعة بشار
13	د. قندلي رمضان	مدى تغير مفهوم السيادة في ظل التحول الرقمي	الثلث	جامعة بشار

جامعة طاهري محمد. بشار

كلية الحقوق والعلوم السياسية

الملتقى الدولي: السيادة الرقمية للدولة. 11/12/2025



مداخلات المحور الرابع

الجلسة الخامسة: 11 نوفمبر 2025. الساعة: 18:00-20:00

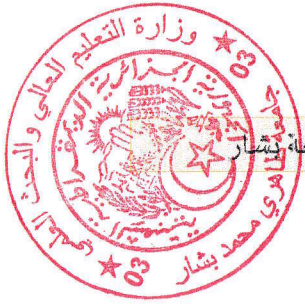
رابط الجلسة: <https://meet.google.com/gyp-rrba-seh>

رئيس الجلسة: الدكتور مسيكة محمد

الرقم	المتدخل	عنوان المداخلة	المحور	الجامعة / المؤسسة
1	أ.د. لعروسي ربيع	الديمقراطية والسيادة الرقمية: قراءة في مشروع جدار الحماية العظيم	الرابع	جامعة الجزائر 3
2	أ.د. ساعد رشيد ط.د. داودي محمد	الأمن الطاقوي والسيادة الرقمية في الجزائر: مقارنة استراتيجية في تحقيق الأمن الوطني والحوكمة السيبرانية.	الرابع	جامعة تيارت جامعة الأغواط
3	د. عبد الغني حجت ب. أ.د. محمد الطاهر عديلة.	نماذج مؤسسية رائدة في تعزيز السيادة الرقمية: دراسة حالة التجربة الأوروبية	الرابع	جامعة المسيلة.
4	أ.د. فاسي عبد الله ط.د. كبداني هبة	التجربة الجزائرية كنموذج لتحقيق السيادة الرقمية.	الرابع	جامعة بشار.
5	أ.د. علوي فاطمة	دور المحافظة السامية للسيادة الرقمية في تجسيد رؤية الجزائر الرقمية 2030	الرابع	جامعة بشار
6	د. بن جراد عبد الرحمن	جهات التصديق الإلكترونية كآلية لتحقيق السيادة الرقمية	الرابع	جامعة أدرار



7	ط.د إبراهيم ولدعلي	الاستراتيجية الجزائرية للسيادة الرقمية، على ضوء التجربة السعودية	الرابع	جامعة الأغواط
8	د. عبد المومن حمودي، أ.د رضا دمدوم	الأطر القانونية والتنظيمية للسيادة الرقمية	الرابع	جامعة قسنطينة
9	د. خديجة بوعامر د. أسماء حمايدية	من السيادة الرقمية إلى السيادة السحابية: تحديات استقلال الدولة في العصر الرقمي) قراءة في تجربة الاتحاد الأوروبي (Gaia-X)	الرابع	جامعة بومرداس
10	موصدق على	السيادة الرقمية والبيانات في الجزائر: نحو استقلالية تكنولوجية وأمن معلوماتي	الرابع	جامعة معسكر
11	د. بلخشي محمد أمين	الاستقلال التكنولوجي: ركيزة أساسية لتعزيز السيادة الرقمية للدولة (دراسة حالة الصين).	الرابع	جامعة الجزائر 3
12	سي العابدي يوسف	التحول الرقمي في خدمة التنمية السياحية المستدامة: تجربة ولاية بشار كنموذج للجنوب الجزائري.	الرابع	مدير السياحة والصناعة التقليدية لولاية بشار
13	كمال منصوري	الرقمنة كأداة لضبط السوق وضمان الشفافية التجارية في ظل التحول الرقمي الوطني.	الرابع	مدير التجارة لولاية بشار
14	طارق علي	من الورق إلى البيانات: تجربة ديوان الترقية والتسيير العقاري لبشار نحو التحول الرقمي الآمن	الرابع	المدير العام لديوان الترقية والتسيير العقاري لولاية بشار
15	بوعافية نسيم	التحول الرقمي في خدمات النقل الحضري: نحو ذكاء حضري مستدام	الرابع	المدير العام للمؤسسة العمومية للنقل الحضري وشبه الحضري. بشار
16	د. عبد المالك مالكي	تحديث الجهود الرقمية للإذاعة الجزائرية -مواكبة التطور والتصدي للمخاطر	الرابع	جامعة بشار
17	د. بلباقي وهيبه	الأطر القانونية لحماية السيادة الرقمية للدولة	الرابع	جامعة بشار
18	د. بيان نور الدين	دور البنوك في تحقيق السيادة الرقمية	الرابع	جامعة بشار



جامعة بغداد

الرابع

الحماية الجنائية العملة الوطنية في المجال الرقمي

د. خليفي بوتخيل

19



جامعة طاهري محمد. بشار

كلية الحقوق والعلوم السياسية

الملتقى الدولي: السيادة الرقمية للدولة. 13/12/11 نوفمبر 2025

مداخلات المحور الخامس.

الساعة 18:00-20:00

الجلسة السادسة: 11 نوفمبر 2025.

رابط الجلسة: <https://meet.google.com/fcv-hsrw-zns>

رئيس الجلسة: الدكتورة لبيدي حنان

الرقم	المتدخل	عنوان المداخلة	المحور	الجامعة / المؤسسة
1	د. العربي عمر	Building a Comprehensive Strategy to Achieve Digital Sovereignty through Artificial Intelligence Models	الخامس	جامعة بشار
2	ط.د. محمد بن سعدة	الاستراتيجية الرقمية للتحويل الرقمي وتحديات تفعيل الحكومة الإلكترونية – المحافظة السامية للرقمنة نموذجاً	الخامس	جامعة الجزائر 3
3	د. صوالحية عماد	مقاربة تكاملية بين الأمن السيبراني وحوكمة البيانات	الخامس	جامعة الوادي
4	د. بوشنة خالد د. رمضاوي سليمان	الآليات القانونية لتعزيز السيادة الرقمية في مواجهة التهديدات السيبرانية: دراسة في ضوء التشريع الجزائري	الخامس	جامعة بشار
5	د. عياش بوشريف	سياسة الأمن القومي الرقمي: طموحات إستراتيجية لتأمين الفضاء الإلكتروني	الخامس	جامعة باتنة 1
6	د. سفير مختارية	نحو سيادة رقمية جزائرية: الآليات القانونية والمؤسسية في المواجهة	الخامس	جامعة وهران 2 أحمد بن أحمد
7	د. العماري يمينه	البنية التحتية لتحقيق السيادة الرقمية في الجزائر	الخامس	جامعة بشار

ط.د. مجدوب كريم			
8	د. نقيش لخطر ط.د. غربي مصطفى	اصلاح المنظومة القانونية كآلية التحقيق السيادة الرقمية في الجزائر. قانون التجارة الالكترونية 18-05 أنموذجا	الخامس المركز الجامعي نور البشير البيض
9	أ.د سي موسى عبد الله. د. تاجر مراد	البيئة الرقمية والبنية الاجتماعية في الجزائر	الخامس جامعة بشار
10	د. لبيدي حنان	نحو مقارنة شاملة لحماية السيادة الرقمية للدولة من تهديدات الإرهاب الالكتروني	الخامس جامعة بشار
11	د. معموري عبيد الله د. مالكي محمد	السيادة الرقمية وريادة الأعمال: بناء مستقبل رقمي مستقل ومبتكر	الخامس جامعة بشار

نماذج مؤسساتية رائدة في تعزيز السيادة الرقمية: دراسة حالة التجربة الأوروبية

Pioneering Institutional Models in Promoting Digital Sovereignty: A Case Study of the European Experience

د. عبد الغني حجاب * . جامعة محمد بوضياف-المسيلة (الجزائر) abdelghani.hadjab@univ-msila.dz
أ.د محمد الطاهر عديلة. جامعة محمد بوضياف-المسيلة (الجزائر) mohamedtahir.adila@univ-msila.dz

ملخص: تستكشف هذه الدراسة النماذج المؤسسية الرائدة لتعزيز السيادة الرقمية من خلال تحليل المبادرات العالمية الناجحة التي تجمع بين الأطر التنظيمية والبنى التحتية التكنولوجية وأنظمة الابتكار. يسلط البحث الضوء على كيفية قيام الدول بتنفيذ استراتيجيات شاملة تشمل سياسات حوكمة البيانات مثل نظام GDPR الأوروبي، وتطوير بنى تحتية رقمية سيادية كمنصة GAIA-X السحابية، وتقليل الاعتماد التكنولوجي عبر نموذج الابتكار المحلي الصيني، وتعزيز النظم البيئية الرقمية المحلية كما في نظام الهوية الرقمية الهندي "أدهار". تُظهر هذه الجهود المتكاملة كيف يمكن للقيادة المؤسسية تحقيق التوازن بين التقدم التكنولوجي وأولويات الأمن القومي في المشهد الرقمي المترابط، مع الحفاظ على الهوية الثقافية والقدرة التنافسية الاقتصادية. يؤكد البحث على أهمية تبني نهج مؤسسي مرن ومكيف لتحقيق سيادة رقمية فاعلة في مختلف السياقات الوطنية.

كلمات مفتاحية: السيادة الرقمية، النماذج المؤسساتية، حماية البيانات، البنية التحتية الرقمية، الاستقلال التكنولوجي.

Abstract: This paper explores pioneering institutional models that strengthen digital sovereignty by analyzing successful global initiatives. It highlights how nations and organizations are establishing control over their digital ecosystems through robust regulatory frameworks, sovereign infrastructure development, and strategic technological autonomy. The study examines key examples, including the EU's GDPR for data governance, China's Great Firewall for digital independence, and India's Aadhaar system for digital identity management. These cases demonstrate diverse approaches to balancing technological advancement with national security priorities. The research underscores the growing importance of institutional capabilities in maintaining digital sovereignty amidst increasing global interconnectivity and technological dependencies. The findings offer valuable insights for policymakers seeking to enhance their nations' digital resilience while navigating complex geopolitical and technological landscapes.

Keywords: Digital Sovereignty, Institutional Models, Data Governance, Digital Infrastructure, Technological Independence.

* المرسل.

مقدمة

أصبحت السيادة الرقمية موضوعاً جوهرياً في ظل التحولات التكنولوجية المتسارعة التي تشهدها المجتمعات الحديثة. وتسعى المؤسسات في مختلف الدول إلى تحقيق استقلاليتها الرقمية الرقمي وحماية بياناتها من التأثيرات الخارجية من خلال تطوير البنية التحتية التكنولوجية، وتعزيز القدرات المحلية، وتقليل الاعتماد على الحلول الرقمية الخارجية.

كما أصبحت تمثل ركيزة أساسية لاستقلال الدول وسيادتها الوطنية. تشير البيانات إلى أن 85% من البنى التحتية الرقمية العالمية تُسيطر عليها شركات من خمس دول فقط، مما يفرض تحديات غير مسبقة على الأمن القومي والخصوصية الرقمية للدول الأخرى. في هذا السياق، برزت نماذج مؤسسية مبتكرة تهدف إلى تحقيق التوازن بين الانفتاح الرقمي والحفاظ على السيادة الوطنية.

الهدف من الدراسة:

تهدف الدراسة إلى:

- ✓ رصد أفضل الممارسات المؤسسية في مجال السيادة الرقمية.
- ✓ تطوير إطار تحليلي لتقييم النماذج المؤسسية.
- ✓ تقديم توصيات عملية للمؤسسات العربية.
- ✓ الإسهام في تطوير الفكر التنموي في مجال الحوكمة الرقمية.

أهمية الموضوع:

تكتسب الدراسة أهميتها من:

- ✓ الحاجة الملحة لمواجهة الاحتكار التكنولوجي العالمي.
- ✓ المخاطر المتنامية على أمن البيانات الوطنية.
- ✓ الفرص الاقتصادية والتنموية المرتبطة بالسيادة الرقمية.
- ✓ ندرة الدراسات العربية التي تتناول النماذج المؤسسية في هذا المجال.

الإشكالية:

تتمحور الإشكالية الرئيسية حول: كيف يمكن للمؤسسات الوطنية بناء نماذج فعالة لتعزيز السيادة الرقمية في ظل هيمنة الشركات العابرة للحدود وتفاوت القدرات التكنولوجية بين الدول؟

الأسئلة البحثية:

- ✓ ما هي أبرز النماذج المؤسسية العالمية الناجحة في تحقيق السيادة الرقمية؟
- ✓ كيف يمكن تقييم فعالية هذه النماذج في مختلف السياقات الوطنية؟

- ✓ ما هي المعوقات الرئيسية التي تواجه المؤسسات في تعزيز سيادتها الرقمية؟
- ✓ كيف يمكن تطوير إطار مؤسسي متكامل للسيادة الرقمية؟

الفرضيات البحثية:

- ✓ توجد علاقة طردية بين قوة الإطار المؤسسي ومستويات تحقيق السيادة الرقمية.
- ✓ تختلف فعالية النماذج المؤسسية باختلاف البيئة التشريعية والبنية التحتية.
- ✓ يمكن للتعاون الإقليمي أن يعزز القدرة المؤسسية على تحقيق السيادة الرقمية.

منهجية الدراسة:

تعتمد الدراسة على:

- ✓ المنهج التحليلي المقارن لدراسة النماذج المؤسسية المختلفة.
- ✓ منهج دراسة الحالة (الاتحاد الأوروبي، الصين، الولايات المتحدة الأمريكية نموذجاً).
- ✓ التحليل الكيفي للسياسات والتشريعات الرقمية.

1. السيادة الرقمية: إطار معرفي ونظري

1.1. مفهوم السيادة الرقمية

السيادة الرقمية (Digital Sovereignty) تعرف بقدرة الدولة أو المؤسسة على التحكم في البيانات والبنى التحتية الرقمية والخدمات الإلكترونية وتطوير حلول تقنية محلية بشكل مستقل لتقليل من التبعية للأنظمة والمنصات الأجنبية، وهي تشمل الجوانب القانونية، التقنية، والسياسات التنظيمية لضمان أمن واستقلالية الفضاء الرقمي. مع ضمان الأمن والحوكمة الرقمية وفقا للقوانين المحلية والقيم الوطنية. تختلف الدول في نهجها لتحقيق هذه السيادة، سواء عبر سياسات حماية البيانات أو تعزيز البنى التحتية المحلية أو تطوير تشريعات رقمية صارمة (Finnemore & Hollis, 2016).

2.1. أهدافها:

تحقيق السيادة الرقمية هو هدف استراتيجي تسعى إليه العديد من المؤسسات والدول في جميع أنحاء العالم. يشير مصطلح "السيادة الرقمية" إلى قدرة المؤسسة أو الدولة على التحكم في بياناتها وبنيتها التحتية الرقمية، وحمايتها من التهديدات الخارجية، وتطوير تكنولوجياتها الخاصة. هناك العديد من التجارب المؤسسية التي تهدف إلى تحقيق السيادة الرقمية، وتشمل:

- ✓ تعزيز الأمن السيبراني: تعتمد المؤسسات على تطوير أنظمة حماية قوية ضد الهجمات الإلكترونية، مثل استخدام تقنيات التشفير المتقدمة وجدران الحماية الذكية.
- ✓ الاعتماد على البنية التحتية المحلية: بعض الدول والمؤسسات تعمل على إنشاء مراكز بيانات محلية وتقليل الاعتماد على الخدمات السحابية الأجنبية لضمان التحكم الكامل في البيانات.
- ✓ تطوير البرمجيات المفتوحة المصدر: استخدام البرمجيات المفتوحة المصدر يساعد المؤسسات على تقليل الاعتماد على الشركات الأجنبية، مما يعزز استقلالها الرقمي.
- ✓ تشجيع الابتكار المحلي: دعم الشركات الناشئة والمطورين المحليين يساهم في بناء منظومة رقمية مستقلة وقوية (Tallberg et al., 2016).

3.1. عوامل تحقيق السيادة الرقمية:

- ✓ يتطلب تحقيق السيادة الرقمية استثمارات كبيرة في البنية التحتية الرقمية، وتطوير القدرات البشرية، ودعم الابتكار الرقمي (Carrapico & Barrinha, 2018).

- ✓ كما يتطلب تعاونا دوليا في مجال الأمن السيبراني، وتبادل الخبرات والمعلومات.
- ✓ وتعتمد أيضا على التشريعات والقوانين التي تحمي البيانات وتكفل السيادة الرقمية.

4.1. تحديات تحقيق السيادة الرقمية:

- ✓ الاعتماد على الشركات الأجنبية في صناعة أشباه الموصلات والتكنولوجيا المتقدمة.
- ✓ التكلفة العالية لتطوير أنظمة رقمية محلية متكاملة ونقص الكفاءات والتهديدات السيبرانية المتزايدة.
- ✓ التحديات القانونية المتعلقة بحرية الإنترنت والتوازن بين الأمن الرقمي والانفتاح التكنولوجي (Flonk et al., 2020).

2. التجارب المؤسسية في تحقيق السيادة الرقمية

هي جهود تقوم بها المؤسسات والمنظمات لتحقيق السيادة الرقمية، والتي تعني القدرة على التحكم في البيانات الرقمية والأنظمة الرقمية التي تؤثر على المجتمع. إليك بعض الأمثلة على التجارب المؤسسية في تحقيق السيادة الرقمية:

1.2. تجارب في القطاع العام (الدول)

تتبنى العديد من الدول استراتيجيات وطنية للسيادة الرقمية، تهدف إلى تعزيز القدرات الرقمية المحلية، وحماية البيانات الحساسة، وتقليل الاعتماد على التكنولوجيات الأجنبية. على سبيل المثال:

1.1.2. التجربة الأوروبية (النموذج التنظيمي) تعزيز السيادة الرقمية عبر التشريعات والبنية التحتية

تبنى الاتحاد الأوروبي استراتيجية شاملة لتعزيز السيادة الرقمية من خلال عدة مبادرات مثل " منصة السحابة الأوروبية "GAIA-X لتقليل الاعتماد على الخدمات السحابية الأمريكية والصينية مثل AWS و Google Cloud. كما اعتمد الاتحاد الأوروبي على تشريعات صارمة مثل اللائحة العامة لحماية البيانات (GDPR) لضمان أمن سيادة البيانات وتشجيع الابتكار المحلي في مجال التكنولوجيا والسيطرة عليها داخل حدود الدول الأوروبية (Tallberg et al., 2020).

2.1.2. التجربة الصينية (النموذج المركزي) تطوير أنظمة محلية بديلة

تظهر الصين نمودجا مختلفا يعتمد على السيطرة الحكومية المركزية من خلال تطوير تقنيات محلية مثل شبكات الجيل الخامس عبر شركات مثل هواوي و Tencent لتعزيز الهيمنة الرقمية العالمية، والاستثمار في التكنولوجيا والذكاء الاصطناعي، تسعى المؤسسات الصينية إلى تقليل الاعتماد على التقنيات الأجنبية. وتتم السيطرة على البيانات عبر تطبيق سياسة "الجدار الناري العظيم Great Firewall" بشكل يمكن الدولة من التحكم في تدفق البيانات وحماية السيادة الرقمية، مما يعزز الأمن القومي والتنافسية الاقتصادية لحجب خدمات أجنبية مثل Google و Facebook.

كما طورت الصين منصاتها المحلية مثل: WeChat و Alibaba Cloud و Baidu للحد من الاعتماد على منصات التكنولوجيا الأمريكية. وفرضت قيودا على الشركات الأجنبية وعززت إنتاج أشباه الموصلات محليا لتقليل التبعية في صناعة التقنية المتقدمة (Carrapico & Farrand, 2021).

3.1.2. التجربة الأمريكية (النموذج الرأسمالي-التكنولوجي) والتي تبرز من خلال:

✓ الهيمنة العالمية: سيادة شركات مثل Google و Amazon و Microsoft على البنى التحتية الرقمية (السحابة، أنظمة التشغيل).

✓ **التشريعات:** قوانين مثل **CLOUD Act** تسمح للحكومة الأمريكية بالوصول إلى بيانات مخزنة خارجيا (Farrell & Newman, 2021).

4.1.2. تجارب ناشئة (روسيا، الهند)

أولاً: روسيا: بناء إنترنت محلي (Runet)

أنشأت روسيا بنية تحتية رقمية تسمح لها بتشغيل شبكة إنترنت مستقلة في حال حدوث أي تهديدات خارجية. وأطلقت نظام تشغيل محلي مثل **Astra Linux** لاستخدامه في المؤسسات الحكومية بدلا من الأنظمة الأجنبية. وأصدرت تشريعات مثل قانون البيانات المحلية (2015) لإجبار الشركات على تخزين بيانات المواطنين داخل البلاد (Fathaigh et al., 2021).

ثانياً: الهند (تعزيز صناعة التكنولوجيا المحلية)

تبنت الهند سياسة **Digital India** لتعزيز تقنيات محلية مثل **Aadhaar** (نظام الهوية الرقمية). وفرضت سياسات لدعم الشركات الناشئة في مجال التكنولوجيا، وأطلقت برامج مثل **"Make in India"** لتعزيز الابتكار المحلي. كما حظرت بعض التطبيقات الأجنبية لدعم بدائل محلية مثل **Jio Platforms** في مجال الاتصالات والتكنولوجيا الرقمية (Fathaigh et al., 2021).

2.2. تجارب في القطاع الخاص (المؤسسات)

تسعى العديد من المؤسسات إلى تحقيق السيادة الرقمية من خلال بناء بنيتها التحتية الرقمية الخاصة، وتطوير برمجياتها الخاصة، وحماية بياناتها من التهديدات الخارجية. على سبيل المثال، تقوم بعض المؤسسات المالية ببناء مراكز بيانات خاصة بها، وتطوير أنظمة أمن معلومات متقدمة، لضمان حماية بيانات عملائها. أيضاً، تتجه العديد من الشركات إلى استخدام الحوسبة السحابية السيادية، وذلك لحماية معلوماتها الشخصية. ومن أمثلة ذلك:

1.2.2. شركة أمازون (Amazon Web Services–AWS):

على الرغم من كونها شركة أمريكية، فإن أمازون تقدم نموذجاً لكيفية دعم السيادة الرقمية لعملائها من المؤسسات. من خلال خدمات الحوسبة السحابية، تتيح **AWS** للمؤسسات اختيار مواقع تخزين البيانات وفقاً للمتطلبات القانونية والتنظيمية المحلية، مما يساعد على تحقيق السيادة الرقمية على مستوى العملاء (Flonk, 2021).

2.2.2. مايكروسوفت وغوغل وبرنامج "السيادة الرقمية"

قامت الشركتان بتقديم برنامج "السيادة الرقمية" الذي يهدف إلى مساعدة الشركات على تحقيق السيادة الرقمية من خلال دعم التكنولوجيا الرقمية والابتكار (Flonk, 2021).

3. دراسة حالة: السعي نحو السيادة الرقمية في الاتحاد الأوروبي

يشير مفهوم السيادة الرقمية بشكل عام إلى قدرة دولة أو منطقة على ممارسة السيطرة على بنيتها التحتية الرقمية واستخدام البيانات والتطورات التكنولوجية بشكل مستقل عن التأثير الخارجي. وقد اكتسبت السيادة الرقمية أهمية متزايدة بالنسبة للاتحاد الأوروبي في المشهد العالمي الحالي، الذي يتميز بالرقمنة السريعة والتوترات الجيوسياسية. ولا يعد تركيز الاتحاد الأوروبي على السيادة الرقمية ظاهرة منعزلة، بل هو استجابة لاتجاهات عالمية أوسع ومخاوف بشأن السيطرة في العصر الرقمي. يهدف هذا التقرير إلى تحليل جهود الاتحاد الأوروبي ودوافعه وتحدياته ونجاحاته في تحقيق السيادة الرقمية، بالاعتماد حصرياً على الأدبيات الأكاديمية التي تمت مراجعتها من قبل النظراء. سيقدم التقرير لمحة موجزة عن أهدافه: تحليل جهود الاتحاد الأوروبي ودوافعه وتحدياته ونجاحاته في تحقيق السيادة الرقمية، بالاعتماد حصرياً على الأدبيات الأكاديمية التي تمت مراجعتها من قبل النظراء. سيسلط التقرير الضوء على هيكله، مشيراً إلى الأقسام التي ستغطي التعاريف والسياسات والدوافع والتحديات والتقييمات والمقارنات العالمية (Novak, et al., 2021).

1.3. تصور السيادة الرقمية في الاتحاد الأوروبي: تعريف أكاديمي

استكشفت العديد من الدراسات الأكاديمية تعريفات مختلفة للسيادة الرقمية ضمن السياق المحدد للاتحاد الأوروبي، مما يشير إلى الغموض والتفسيرات المتنوعة للمفهوم. لا يوجد فهم واحد ومتماثل للسيادة الرقمية داخل الاتحاد الأوروبي، وهو ما يمكن أن يؤدي إلى تحديات في صياغة السياسات وتنفيذها. تسعى جهات فاعلة مختلفة (الدولة، والشركات، والأفراد) إلى تحقيق الاستقلال والاكتفاء الذاتي في المجال الرقمي. ينطوي جوهر السيادة الرقمية على السيطرة على الطبقات المادية والرمزية والمعلوماتية للرقمية. تشمل هذه السيطرة القدرة على التأثير وتقييد تصنيع وتصميم واستخدام وإنتاج التقنيات الرقمية.

حددت الأدبيات الأكاديمية طبقات وأبعاداً مختلفة للسيادة الرقمية، مثل سيادة البيانات، والسيادة التكنولوجية، والسيطرة على البنية التحتية، وسيادة الأمن السيبراني، والسيادة القانونية. تتعلق سيادة البيانات بالسيطرة على جمع البيانات ومعالجتها. تشير السيادة التكنولوجية إلى التطوير المستقل للبنية التحتية التكنولوجية والتحكم فيها. تضمن سيادة الأمن السيبراني حماية البنية التحتية الرقمية من التهديدات. السيادة القانونية هي القدرة على إنشاء وإنفاذ القوانين الرقمية.

يتضمن نهج الاتحاد الأوروبي في تحقيق السيادة الرقمية موازنة استقلالية الدول الأعضاء بالحاجة إلى التعاون والتنظيم على مستوى الاتحاد الأوروبي. يهدف الاتحاد الأوروبي إلى مواءمة التشريعات مع احترام الخصوصية الوطنية. يعد النضال من أجل تحقيق التوازن بين السيطرة والتعاون موضوعاً رئيسياً. يشكل الإطار التنظيمي للاتحاد الأوروبي ويستجيب للسعي لتحقيق السيادة الرقمية (Saurugger & Terpan, 2021).

2.3. السياسات والمبادرات الأوروبية الرئيسية التي تدفع السيادة الرقمية

1.2.3. **اللائحة العامة لحماية البيانات (GDPR)** أحدثت هذه اللائحة تأثيرًا كبيرًا على سيادة البيانات، وأرست معيارًا عالميًا لحماية البيانات وحقوق الأفراد. تعمل اللائحة العامة لحماية البيانات على توحيد كيفية التعامل مع البيانات الشخصية عبر الإنترنت وتمنح المواطنين مزيدًا من التحكم. تحدد اللائحة قواعد صارمة لحماية البيانات وتزيد من مسؤولية مراقبي البيانات. تعد اللائحة العامة لحماية البيانات عنصرًا أساسيًا في استراتيجية الاتحاد الأوروبي للسيادة الرقمية، حيث تعمل على تمكين الأفراد ووضع معيار عالمي لخصوصية البيانات. تمنح اللائحة العامة لحماية البيانات الأفراد التحكم في بياناتهم الشخصية وتقرض متطلبات صارمة على الشركات. كان لها تأثير اقتصادي كبير وتؤثر على التجارة الرقمية العالمية. ومع ذلك، توجد تحديات في التنفيذ والإنفاذ (Bellanova, 2022).

2.2.3. **قانون الخدمات الرقمية (DSA)** يهدف هذا القانون إلى تنظيم المنصات عبر الإنترنت، وزيادة مسؤوليتها عن الإشراف على المحتوى، ومنع انتشار المحتوى غير القانوني والمعلومات المضللة، وحماية المستخدمين. يسعى قانون الخدمات الرقمية إلى تنظيم الاقتصاد الرقمي والتقنيات الناشئة. يحمل المنصات مسؤولية الإشراف على المحتوى وحماية المستخدمين. يعد قانون الخدمات الرقمية أداة تشريعية رئيسية لتعزيز السيادة القانونية للاتحاد الأوروبي في المجال الرقمي من خلال فرض التزامات على المنصات عبر الإنترنت. يزيد قانون الخدمات الرقمية من سيطرة الدول الأعضاء على المنصات عبر الإنترنت. يهدف إلى حماية المواطنين من المخاطر والأضرار عبر الإنترنت. ومع ذلك، لوحظت تحديات في الإنفاذ المنسق والتأثيرات المحتملة على حرية التعبير (Cioffi et al., 2022).

3.2.3. **قانون الأسواق الرقمية (DMA)** يناقش هذا القانون أهدافه المتمثلة في تعزيز المنافسة في الأسواق الرقمية من خلال معالجة الممارسات المحتملة المناهضة للمنافسة من قبل المنصات الكبيرة عبر الإنترنت ("حراس البوابة"). يسعى قانون الأسواق الرقمية إلى تنظيم الاقتصاد الرقمي والتقنيات الناشئة. يقيد سلطة شركات التكنولوجيا الكبيرة غير الأوروبية. يهدف قانون الأسواق الرقمية إلى تعزيز السيادة الاقتصادية للاتحاد الأوروبي في القطاع الرقمي من خلال الحد من سلطة اللاعبين المهيمنين. يستهدف قانون الأسواق الرقمية "حراس البوابة" لضمان المنافسة العادلة. يهدف إلى تسهيل دخول الأسواق الرقمية. المفوضية الأوروبية مسؤولة عن الإنفاذ (De Gregorio & Radu, 2022).

4.2.3. **الاستراتيجية الأوروبية للبيانات**: تحل أهدافها المتمثلة في إنشاء فضاء بيانات أوروبي لضمان إتاحة المزيد من البيانات للاستخدام في الاقتصاد والمجتمع مع إبقاء الشركات والأفراد تحت سيطرتهم على بياناتهم. تهدف الاستراتيجية إلى إنشاء فضاءات بيانات أوروبية لضمان توفر المزيد من البيانات مع الحفاظ على السيطرة. تعد استراتيجية البيانات حاسمة لتعزيز سيادة البيانات في الاتحاد الأوروبي من خلال تشجيع تبادل البيانات ضمن إطار من التحكم والقيم الأوروبية. تهدف الاستراتيجية إلى

تعزيز الابتكار القائم على البيانات مع تحقيق التوازن بين الخصوصية والأمن. تسعى إلى معالجة المخاوف بشأن فقدان السيطرة على البيانات لصالح شركات غير أوروبية. توجد تحديات في تنفيذ وإدارة فضاءات البيانات (Farrand & Carrapico, 2022).

5.2.3. قانون الأمن السيبراني للاتحاد الأوروبي وتوجيهات الشبكات ونظم المعلومات (NIS)
تقيم فعاليتها في تعزيز قدرات الاتحاد الأوروبي في مجال الأمن السيبراني ومرونته. يعزز قانون الأمن السيبراني دور وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA) وينشئ إطاراً للشهادات. تهدف توجيهات الشبكات ونظم المعلومات إلى تحسين قدرات الدول الأعضاء في مجال الأمن السيبراني. تعد هذه الإجراءات التشريعية حيوية لتعزيز سيادة الأمن السيبراني للاتحاد الأوروبي وحماية بنيته التحتية الرقمية من التهديدات. يمنح قانون الأمن السيبراني وكالة الاتحاد الأوروبي للأمن السيبراني ولاية دائمة وينشئ إطاراً للشهادات. تعمل توجيهات الشبكات ونظم المعلومات NIS2 على تعزيز التزامات الأمن السيبراني. ومع ذلك، لوحظت تحديات ونقائص في التنفيذ (Flonk, 2022).

6.2.3. مبادرة GAIA-X: تستكشف طموحها في بناء نظام بيئي أوروبي آمن وشفاف ومتحد
لخدمات الحوسبة السحابية، مما يوفر بديلاً لخدمات الحوسبة السحابية غير الأوروبية ويعزز الاستقلال التكنولوجي. تهدف مبادرة GAIA-X إلى بناء نظام سحابي أوروبي يلتزم بقواعد الخصوصية الأوروبية. إنها مبادرة أوروبية لزيادة السيادة الرقمية. تمثل مبادرة GAIA-X جهداً رئيسياً لتعزيز السيادة التكنولوجية للاتحاد الأوروبي من خلال إنشاء بنية تحتية سحابية بقيادة أوروبية. تهدف GAIA-X إلى ضمان بقاء أوروبا مسيطرة على مستقبلها الرقمي. تسعى إلى ربط العروض الحالية عبر المصادر المفتوحة والمعايير. ومع ذلك، توجد تحديات في التبني والمنافسة مع كبار مزودي الخدمات السحابية (Broeders et al., 2023).

7.2.3. قانون الاتحاد الأوروبي بشأن الذكاء الاصطناعي: يحل نهجه في تنظيم الذكاء الاصطناعي بناءً على نهج قائم على المخاطر، وضمان التقدم التكنولوجي مع حماية الحقوق الأساسية وتعزيز الاستخدام الأخلاقي للذكاء الاصطناعي. يُعد قانون الذكاء الاصطناعي أول إطار قانوني شامل للذكاء الاصطناعي في العالم. يهدف إلى تنظيم أنظمة الذكاء الاصطناعي وفقاً لقواعد وقيم الاتحاد الأوروبي. يُعد قانون الذكاء الاصطناعي خطوة مهمة نحو إرساء السيادة القانونية والأخلاقية للاتحاد الأوروبي في مجال الذكاء الاصطناعي سريع التطور. يهدف قانون الذكاء الاصطناعي إلى وضع معايير عالمية لتنظيم الذكاء الاصطناعي. يؤكد على نهج يركز على حقوق الإنسان. ومع ذلك، لا تزال هناك تحديات في توسيع نطاق الابتكار والمنافسة مع الشركات العملاقة العالمية (Heermann, 2023).

3.3. دوافع وراء تركيز الاتحاد الأوروبي على السيادة الرقمية

1.3.3. **الدوافع الاقتصادية:** يتمثل أحد الدوافع الرئيسية في الرغبة في ضمان الازدهار الاقتصادي والقدرة التنافسية في العصر الرقمي، وتقليل الاعتماد على اللاعبين المهيمنين من خارج الاتحاد الأوروبي. يعتمد الاتحاد الأوروبي بشكل كبير على دول أجنبية في تلبية احتياجاته الرقمية. يُنظر إلى السيادة الرقمية على أنها ضرورية للنمو الاقتصادي والابتكار. الهدف هو تعزيز الصناعات التكنولوجية المحلية (Schmitz & Seidl, 2023).

2.3.3. **الدوافع الأمنية:** يتمثل دافع مهم آخر في حماية البنية التحتية الرقمية والبيانات من التهديدات السيبرانية وضمان الأمن القومي. توجد مخاوف بشأن أمن البيانات الشخصية والبنية التحتية الرقمية. يُنظر إلى الاعتماد على البنية التحتية غير الأوروبية على أنه نقطة ضعف. ترتبط السيادة الرقمية بقدرة الاتحاد الأوروبي على العمل بشكل مستقل في العالم الرقمي (Schmitz & Seidl, 2023).

3.3.3. **الدوافع الاجتماعية والقائمة على القيم:** يهدف الاتحاد الأوروبي إلى ضمان توافق الفضاء الرقمي مع القيم الأوروبية وحماية حقوق المواطنين والعمليات الديمقراطية. يُنظر إلى السيادة الرقمية على أنها أساس لحماية القيم الأوروبية. توجد مخاوف بشأن تأثير الشركات غير الأوروبية التي قد لا تلتزم بالقيم الأوروبية. الحاجة إلى الحماية من المعلومات المضللة والتلاعب هي دافع (Schmitz & Seidl, 2023).

4.3.3. **العوامل الجيوسياسية:** يسعى الاتحاد الأوروبي إلى ترسيخ مكانته كلاعب مستقل في المشهد الرقمي العالمي، وتقليل اعتماده على الولايات المتحدة والصين. توفر التوترات المتزايدة بين الولايات المتحدة والصين حافزاً للاتحاد الأوروبي لتطوير قدراته الرقمية الخاصة. يهدف الاتحاد الأوروبي إلى وضع معايير عالمية للتقنيات الرقمية. تُصوّر السيادة الرقمية على أنها صيغة جيو-اقتصادية رابحة (Schmitz & Seidl, 2023).

4.3. تحديات وعقبات تحقيق السيادة الرقمية في أوروبا

✓ يشكل الاعتماد الكبير على مزودي التكنولوجيا غير الأوروبيين عقبة كبيرة أمام تحقيق سيادة رقمية حقيقية. يعتمد الاتحاد الأوروبي على دول أجنبية في نسبة كبيرة من احتياجاته الرقمية. يخلق هذا الاعتماد مخاطر أمنية واقتصادية. يعد هيمنة مزودي الخدمات السحابية الأمريكيين مصدر قلق رئيسي.

✓ يؤدي تباين المصالح والقدرات والمبادرات السياسية بين الدول الأعضاء إلى إعاقة تطوير استراتيجية موحدة للسيادة الرقمية. تعد مقاومة بعض الدول الأعضاء لتعزيز الاتحاد الأوروبي عاملاً يحد التجزئة داخل السوق الموحدة من قدرة شركات الاتحاد الأوروبي على المنافسة عالمياً. يطرح التوزيع غير المتكافئ للموارد بين الدول الأعضاء تحديات.

✓ يتطلب تحقيق السيادة الرقمية تجاوز التوتر بين السيطرة والانفتاح، بالإضافة إلى الانخراط في تعاون دولي. يسعى الاتحاد الأوروبي إلى تحقيق التوازن بين السيادة الرقمية والانفتاح والترابط. التعاون الدولي ضروري في مجالات مثل حوكمة الذكاء الاصطناعي. يحاول مجلس التجارة والتكنولوجيا بين الاتحاد الأوروبي والولايات المتحدة تضيق الخلافات.

✓ يعد ضمان امتثال شركات التكنولوجيا الكبيرة وإنفاذ اللوائح الجديدة بشكل فعال تحديات مستمرة. قد تجد شركات التكنولوجيا العالمية صعوبة في التكيف مع الأطر القانونية المختلفة. يحتاج الاتحاد الأوروبي إلى ضمان اتخاذ تدابير فعالة وقابلة للإنفاذ ضد المنصات الكبيرة. تواجه سلطة الاتحاد الأوروبي التنظيمية تحديات من هيمنة شركات التكنولوجيا الكبرى (Heermann, 2023).

5.3. تقييم نجاح وتأثير جهود الاتحاد الأوروبي في مجال السيادة الرقمية

✓ تتنوع التقييمات الأكاديمية لنجاح مبادرات الاتحاد الأوروبي في مجال السيادة الرقمية، حيث يقر البعض بالنقد المحرز بينما يسلط آخرون الضوء على القيود. يُنظر إلى اللائحة العامة لحماية البيانات على أنها معيار عالمي ولكنها تواجه تحديات في التنفيذ. يهدف قانون الخدمات الرقمية وقانون الأسواق الرقمية إلى زيادة السيطرة على المنصات وتعزيز المنافسة، لكن تأثيرهما طويل الأجل لا يزال قيد التطور. يهدف قانون الذكاء الاصطناعي إلى تحقيق السيادة الرقمية في مجال الذكاء الاصطناعي ولكنه يواجه تحديات في توسيع نطاق الابتكار.

✓ تعد مبادرة GAIA-X مبادرة مهمة ولكنها تواجه عقبات في تحقيق تبني واسع النطاق والتنافس مع مزودي الخدمات السحابية الراضين. تهدف GAIA-X إلى إنشاء بنية تحتية سحابية أوروبية ذات سيادة. تعزز سيادة البيانات وقابلية التشغيل البيئي. ومع ذلك، يشير النقد إلى تحديات في التطبيق العملي والمنافسة.

✓ أحرز الاتحاد الأوروبي تقدماً في وضع استراتيجية شاملة، لكن تحقيق سيادة رقمية كاملة لا يزال عملية معقدة ومستمرة. وضع الاتحاد الأوروبي استراتيجية شاملة تتضمن تدابير تشريعية وسياسية. ومع ذلك، لا تزال هناك تحديات في الإنفاذ، ومصالح الدول الأعضاء المتنوعة، والتغير التكنولوجي السريع. أثار خطاب الاتحاد الأوروبي بشأن السيادة الرقمية على التغييرات في السياسات (Broeders et al., 2023).

6.3. نهج الاتحاد الأوروبي تجاه السيادة الرقمية في سياق عالمي: تحليل مقارنة

✓ يختلف نهج الاتحاد الأوروبي، الذي غالباً ما يركز على التنظيم وحقوق الإنسان، عن النهج الأكثر توجهاً نحو السوق في الولايات المتحدة والنموذج الذي تسيطر عليه الدولة في الصين. يضع الاتحاد الأوروبي نفسه كلاعب مستقل بإطار تنظيمي خاص به. يؤكد الاتحاد الأوروبي على نهج يركز على

حقوق الإنسان. تتبع الولايات المتحدة نموذجًا أكثر توجهًا نحو السوق، بينما تمتلك الصين نظامًا رقميًا تسيطر عليه الدولة.

✓ بينما تسعى جميع المناطق إلى مزيد من السيطرة في المجال الرقمي، تختلف دوافعها والتحديات المحددة التي تواجهها اختلافًا كبيرًا. تتفق جميع البلدان بشكل عام على الحاجة إلى تعزيز الصناعات التكنولوجية المحلية من أجل الأمن القومي. ومع ذلك، يختلف التوازن بين التنظيم والابتكار، والتركيز على القيم المختلفة، عبر المناطق.

✓ يمكن أن تؤدي النهج المتباينة إلى توترات جيوسياسية وتحديات في مواءمة نماذج الحوكمة الرقمية العالمية، ولكنها تخلق أيضًا فرصًا للتعاون بين الدول ذات التفكير المماثل. زادت المنافسة الجيوسياسية بين الولايات المتحدة والصين والاتحاد الأوروبي. يمثل مجلس التجارة والتكنولوجيا بين الاتحاد الأوروبي والولايات المتحدة محاولة لتضييق الخلافات. يسعى الاتحاد الأوروبي إلى إقامة تحالفات رقمية استراتيجية مع دول ذات تفكير مماثل (Flonk, 2022).

خاتمة

تحقيق السيادة الرقمية ليس مجرد خيار، بل أصبح ضرورة استراتيجية للمؤسسات والدول التي تسعى لحماية بياناتها، وتعزيز أمنها القومي، ودعم نموها الاقتصادي المستدام. وتتطلب هذه الجهود استثمارات كبيرة في البحث والتطوير، وسن تشريعات قوية، وبناء شراكات محلية ودولية لتعزيز الاستقلال الرقمي.

أحرز الاتحاد الأوروبي تقدمًا ملحوظًا في وضع استراتيجية شاملة للسيادة الرقمية من خلال سلسلة من القوانين الهامة والمبادرات السياسية الاستراتيجية. تهدف هذه الجهود إلى خلق بيئة رقمية أكثر أمانًا وعدلاً وتنافسية مع التمسك بالقيم الأوروبية. ومع ذلك، تتطلب التحديات المستمرة التزامًا وتعاونًا وتكيفًا مستمرين لضمان سيادة الاتحاد الأوروبي الرقمية في مواجهة مشهد تكنولوجي عالمي سريع التطور وتحولات جيوسياسية مستمرة. من الضروري تحقيق التوازن بين الأمن والانفتاح، وإمكانية الاتحاد الأوروبي في تشكيل المعايير الرقمية العالمية بناءً على قيمه.

التوصيات

1. تعزيز التشريعات: سن قوانين تحمي البيانات وتنظم عمل الشركات الأجنبية.
2. الاستثمار في البنية التحتية: تطوير شبكات وطنية وشبكات اتصالات محلية.
3. الشراكات الإقليمية: تعاون عربي أو إفريقي لإنشاء منصات رقمية مشتركة.
4. التوعية الرقمية: حث الأفراد والمؤسسات على أهمية حماية البيانات.

المراجع:

1. Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: An introduction. *European Security*, 31(3), 337–355. <https://doi.org/10.1080/09662839.2022.2101887>
2. Broeders, D., Cristiano, F., & Kaminska, M. (2023). In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions. *JCMS: Journal of Common Market Studies*, 61(5), 1261–1280. <https://doi.org/10.1111/jcms.13462>
3. Carrapico, H., & Barrinha, A. (2018). European Union cyber security as an emerging research and policy field. *European Politics and Society*, 19(3), 299–303. <https://doi.org/10.1080/23745118.2018.1430712>
4. Carrapico, H., & Farrand, B. (2021). When trust fades, Facebook is no longer a friend: Shifting privatisation dynamics in the context of cybersecurity as a result of disinformation, populism and political uncertainty. *JCMS: Journal of Common Market Studies*, 59(5), 1160–1176. <https://doi.org/10.1111/jcms.13175>
5. Cioffi, J. W., Kenney, M. F., & Zysman, J. (2022). Platform power and regulatory politics: Polanyi for the twenty-first century. *New Political Economy*, 27(5), 820–836. <https://doi.org/10.1080/13563467.2022.2027355>
6. De Gregorio, G., & Radu, R. (2022). Digital constitutionalism in the new era of internet governance. *International Journal of Law and Information Technology*, 30(1), 68–87. <https://doi.org/10.1093/ijlit/eaac004>
7. Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, 31(3), 435–453. <https://doi.org/10.1080/09662839.2022.2102896>
8. Farrell, H., & Newman, A. L. (2021). The Janus face of the liberal international information order: When global institutions are self-undermining. *International Organization*, 75(2), 333–358. <https://doi.org/10.1017/S0020818320000302>
9. Fathaigh, R. Ó., Helberger, N., & Appelmann, N. (2021). The perils of legally defining disinformation. *Internet Policy Review*, 10(4), 1–15. <https://doi.org/10.14763/2021.4.1584>
10. Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *American Journal of International Law*, 110(3), 425–479. <https://doi.org/10.1017/S0002930000016894>
11. Flonk, D. (2021). Emerging illiberal norms: Russia and China as promoters of internet content control. *International Affairs*, 97(6), 1925–1944. <https://doi.org/10.1093/ia/iab146>
12. Flonk, D. (2022). Content control contestations: How and why internet governance norms emerge and develop. [Hertie School]. <https://doi.org/10.48462/opus4-4203>
13. Flonk, D., Jachtenfuchs, M., & Obendiek, A. S. (2020). Authority conflicts in internet governance: Liberals vs. sovereigntists? *Global Constitutionalism*, 9(2), 364–386. <https://doi.org/10.1017/S2045381720000167>
14. Gorwa, R. (2021). Elections, institutions, and the regulatory politics of platform governance: The case of the German NetzDG. *Telecommunications Policy*, 45(6), Article 102145. <https://doi.org/10.1016/j.telpol.2021.102145>
15. Heermann, M. (2023). Undermining lobbying coalitions: The interest group politics of EU copyright reform. *Journal of European Public Policy*, 1–29. <https://doi.org/10.1080/13501763.2023.2249948>

16. Novak, S., Rozenberg, O., & Bendjaballah, S. (2021). Enduring consensus: why the EU legislative process stays the same. *Journal of European Integration*, 43(4), 475–493. <https://doi.org/10.1080/07036337.2020.1800679>
17. Saurugger, S., & Terpan, F. (2021). Normative transformations in the European union: On hardening and softening law. *West European Politics*, 44(1), 1–20. <https://doi.org/10.1080/01402382.2020.1762440>
18. Schmitz, L., & Seidl, T. (2023). As open as possible, as autonomous as necessary: Understanding the rise of open strategic autonomy in EU trade policy. *JCMS: Journal of Common Market Studies*, 61(3), 834–852. <https://doi.org/10.1111/jcms.13428>
19. Tallberg, J., Lundgren, M., Sommerer, T., & Squatrito, T. (2020). Why international organizations commit to liberal norms. *International Studies Quarterly*, 64(3), 626–640. <https://doi.org/10.1093/isq/sqaa046>
20. Tallberg, J., Sommerer, T., Squatrito, T., & Lundgren, M. (2016). The performance of international organizations: A policy output approach. *Journal of European Public Policy*, 23(7), 1077–1096. <https://doi.org/10.1080/13501763.2016.1162834>