Security Policy Papers
أوراق السياسات الأمنية
https://spp.nauss.edu.sa/index.php/spp
ورقة تحليل سياسات أمنية

نحو سياسات أكثر فاعلية لتعزيز الأمن الوطني في مواجهة التزييف العميق للصوت

Toward More Effective Policies to Strengthen National Security in Countering Audio Deepfakes

المخرجات الرئيسة

- توصيف التزييف العميق للصوت بوصفه تهديدًا رقميًّا متعدِّد الأبعاد، يمتد أثره إلى الأمن المجتمعي والثقة المؤسَّسية.
- تحليل حدود المقاربات الدولية في مواجهة الظاهرة، وبيان إمكانات تكييفها مع السِّياقات الوطنية.
- تحديد بدائل سياسات عملية ترتكز على التكامل بين الأبعاد التشريعية والتقنية والتوعوية والتنظيمية.
- ترجيح المقاربة التكاملية بوصفها الخيار الأكثر فعالية واستدامة لتعزيز الجاهزية والاستجابة المؤسَّسية

المستخلص

تتناول الورقة أحد أخطر التحدِّيات الرقمية النَّاشئة، المتمثِّلة في التزييف العميق للصوت؛ بوصفه تهديدًا متعدِّد الأبعاد يمسُّ الأمن الرقمي والأمن المجتمعي والثقة المؤسَّسية. فقد أسهم التطور المتسارع لتقنيات الذكاء الاصطناعي التوليدي في إتاحة أدوات قادرة على محاكاة الأصوات البشرية بدرجة عالية من الدقة، وهو ما جعل الصوت الذي كان يُعدُّ وسيطًا موثوقًا، عُرضةً للتلاعب والاستغلال في عمليات الاحتيال، والتضليل، والتأثير النفسي ،والإعلامي.

Abstract

This paper addresses one of the most serious emerging digital challenges: deepfakes of voice as a multidimensional threat that affects digital security, societal security, and institutional trust. The rapid development of generative artificial intelligence technologies has made available tools capable of simulating human voices with a high degree of accuracy, rendering voice—once considered a reliable medium—vulnerable to manipulation and exploitation in fraud, disinformation, and psychological and media influence operations.

1658-8886© 2026. SPP. This is an open access article, distributed under the terms of the Creative Commons Attribution-NonCommercial License.

وتنطلق الورقة من تحليل تشخيصي لطبيعة المشكلة وسياقها التقني والاجتماعي والأمني، وتُبرز محدودية السياسات السَّائدة التي لا تزال محكومة بمنطق الاستجابة الجزئية، سواء من حيث بطء التحديث التشريعي، أو تفاوت القدرات التقنية، أو ضعف الوعي المجتمعي ،أو غياب بروتوكولات تحقيق رقمية متخصِّصة. كما تستعرض الورقةُ مقارنةً للتجارب الدولية الرائدة مع استخلاص أبرز نقاط القوة والقصور.

وتقترح الورقة حزمةً من بدائل السياسات العامة، تشمل التحديث التشريعي وبناء القدرات التقنية والمؤسَّسية، وتعزيز التوعية المجتمعية وتنظيم مسؤوليات المنصَّات الرقمية، مع تقييم هذه البدائل وترجيح المقاربة التكاملية الشَّاملة بوصفها الخيار الأكثر فعالية في مواجهة التزييف العميق للصوت.

The paper begins with a diagnostic analysis of the nature of the problem and its technical, social, and security context, highlighting the limitations of prevailing policies that remain governed by a logic of piecemeal responses—whether in terms of slow legislative updates, varying technical capabilities, low public awareness, or the absence of specialized digital forensic protocols. The paper also reviews a comparison of leading international experiences, identifying key strengths and shortcomings.

The paper proposes a set of public policy alternatives, including legislative modernization, technical and institutional capacity-building, promoting public awareness, and regulating the responsibilities of digital platforms, while evaluating these alternatives and favoring a comprehensive, integrated approach as the most effective option for addressing deep voice forgery.

المقدمة

أصبحت التقنيات القائمة على الذكاء الاصطناعي جزءًا رئيسًا من المشهد الرقمي العالمي، وواحدة من أكثر أدواته تأثيرًا في البنية الاجتماعية والأمنية للدول. ومن بين هذه التقنيات يبرز التزييف العميق للصوت بوصفه أحد أخطر مظاهر إساءة استخدام الذكاء الاصطناعي، نظرًا لقدرته على إنتاج مقاطع صوتية تحاكي الأصوات البشرية بدقة عالية، تجعل من الصعب وأحيانًا من المستحيل التمييز بينها وبين المادة الأصلية. وقد أدى توافر هذه البرمجيات وانتشارها السَّريع إلى خلق واقع جديد، أصبحت فيه الأصوات المسموعة، سواء في الفضاء العام أو ضمن قنوات الاتصال الخاصة، قابلةً للتلاعب، وهو ما يفتح المجال أمام أنماط متعدِّدة من المخاطر الأمنية والاجتماعية.

ويُمثِّل التزييف العميق للصوت تهديدًا مباشرًا للأمن الرقمي؛ إذ يُمكن استغلاله في انتحال الهوية أو اختراق الأنظمة الحسَّاسة المعتمِدة على التحقق الصوتي، أو تنفيذ عمليات احتيال مالي ومعلوماتي عبر خلط الحقائق وتوجيه الرسائل الزائفة. ولا يقتصر خطر هذه الظاهرة على الجانب التقني فقط، بل يمتد إلى المجال المجتمعي؛ حيث يمكن لمقاطع صوتية مفبركة أن تُثير الفوضى، وتُعمِّق الانقسامات وتُضعف ثقةَ المواطنين في المؤسَّسات الرسمية والإعلامية، خصوصًا عندما تُستعمل بشكل منهجي في حملات التضليل في إدارة الأزمات المفتعلة.

وتنبع أهمية تناول هذه الظاهرة في إطار ورقة سياسات من أنها لم تعد مجرد مسألة تقنية، بل أصبحت قضية ترتبط بالأمن الوطني وبسلامة المجال العام، ويتطلب التعامل معها استجابة مؤسَّسية شاملة تجمع بين التشريع والتقنية والتوعية والتنسيق بين الجهات المعنية، وتأتي هذه الورقة لتقديم تحليل منهجي لجوانب التزييف العميق للصوت، وتحديد آثاره المباشرة وغير المباشرة، واستعراض الخيارات المتاحة

أمام صانع القرار لتعزيز قدرة الدولة والمجتمع على مواجهة هذا التحدّي المتصاعد، كما تسعى الورقة إلى اقتراح مسارات عملية تُسهم في ترسيخ الأمن الرقمي، ورفع مستوى الوعي المجتمعي، وبناء بيئةٍ مقاوِمةٍ للتضليل الصوتي، بما يحدّ من مخاطره ويحافظ على ثقة المواطنين في مصادر المعلومات الرسمية.

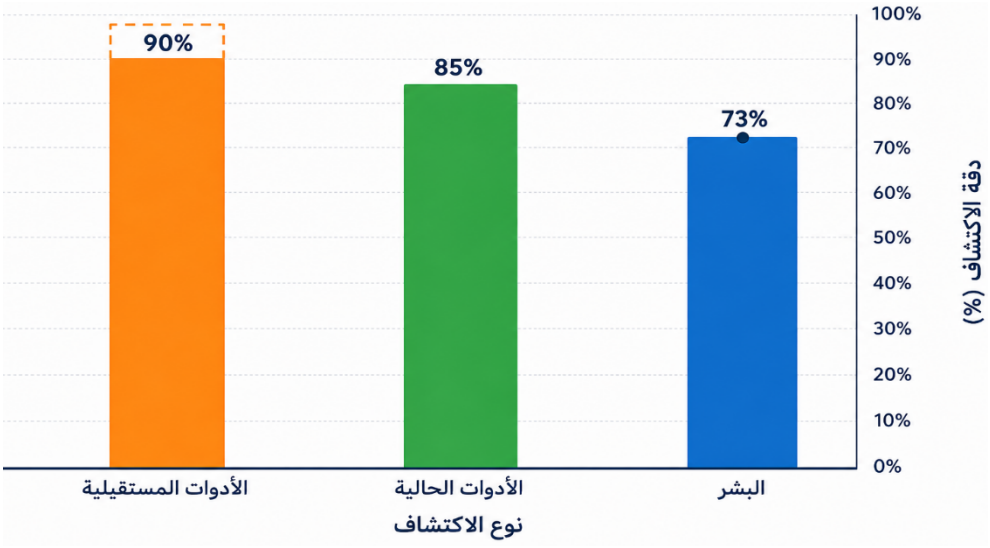
تحليل المشكلة والسياسات المرتبطة بها في ضوء الممارسات الدولية الفضلى

يُشكل التزييف العميق للصوت إحدى القضايا الأمنية النَّاشئة التي فرضت نفسها بقوة خلال السنوات الأخيرة، بعد التطوّر المتسارع في تقنيات الذكاء الاصطناعي التوليدي، وسهولة الحصول على أدوات قادرة على إنتاج مقاطع صوتية عالية الدقة، يصعب التمييز بينها وبين الصوت الحقيقي. وما يضاعف من خطورة هذه الظاهرة أنها لم تعد حكرًا على جهات متقدّمة أو مجموعات تخصُّصية، بل أصبحت في متناول الأفراد العاديين وذوي المهارات التقنية المتوسّطة، الأمر الذي جعل استخدامها في عمليات الاحتيال والهندسة الاجتماعية وتضليل الرأي العام أكثر انتشارًا (Ahma-diadli et al., 2025, p. 1). كما هو موضح في الشكل 1.

وتبرز المشكلة الأساسية في أنَّ التزييف العميق للصوت لا يمسُّ مستوًى واحدًا من الأمن، بل تمتدُّ آثاره إلى الأمن الرقمي والأمن المجتمعي والأمن الاقتصادي، فضلًا عن تأثيره في ثقة المواطنين بالمعلومات الصادرة عبر القنوات الرسمية وشبه الرسمية. ولعل ما يُظهر خطورة هذا الاتجاه ما كشفه تقرير جرائم الإنترنت الصادر عن مكتب التحقيقات الفيدرالي الأمريكي لعام 2025 من

شكل 1

مستوى دقة التعرُّف البشري على المقاطع الصوتية المزيَّفة



المصدر: إعداد الباحث بالاعتماد على: (Stanford University Index Report 2024, pp. 175-178)

رصد أكثر من 22 ألف شكوى مرتبطة بالاحتيال المدعوم بالذكاء الاصطناعي، بخسائر تجاوزت 893 مليون دولار خلال عام واحد، تصدّرتها عمليات استنساخ الصوت (Federal Bureau of Investigation, 2026).

ولتحليل هذه الظاهرة، يمكن الاعتماد على منهجية تحليل السياسات العامة التي تبدأ بإعادة توصيف المشكلة ثم تحليل سياقها وأبعادها، وانتقالًا إلى استعراض السياسات القائمة ونقاط ضعفها وصولًا إلى المقارنة الدولية واستخلاص الممارسات الجيِّدة.

توصيف المشكلة والسِّياق المحيط بها

تتداخل في مشكلة التزييف العميق للصوت مجموعة من العوامل التقنية والاجتماعية والأمنية، فمن الناحية التقنية أصبح بالإمكان تدريب الأنظمة الصوتية على عددٍ محدودٍ من العيِّنات؛ بحيث تُنتج نماذج قادرة على تقليد نبرة الشخص وإيقاع كلامه بدقة كبيرة، وهو ما يجعل الصوت أحد أكثر البيانات عرضة للاستغلال (Bendiab et al., 2025, pp. 12–13). أما من الناحية الاجتماعية، فإنَّ المجتمعات العربية على وجه الخصوص تميل إلى الثقة بالمحتوى الصوتي والتسجيلات الهاتفية أكثر من الثقة بالمنشورات النصِّية، وهو ما يزيد من قابلية الجمهور للتأثر بالمقاطع المفبركة (Alqahs et al., 2023; El-Masri et al., 2022).

ومن الناحية الأمنية، يطرح هذا التحدِّي إشكالات تتجاوز الاحتيال إلى تهديد سلامة الاتصال بين الأفراد والمؤسَّسات، وارتباك الجهات الحكومية عند انتشار تسجيلات غير موثوقة نُسبت لمسؤولين أو مؤسسات رسمية، وقد تستغلها جهات معادية لزعزعة الأمن العام (Security.org, 2025). وتواجه جهود التصدي لهذه المقاطع تحديات تقنية وتشريعية؛ إذ لا تزال أدوات الكشف تواجه صعوبة في مواكبة تقنيات التوليد المتسارعة(Issa, 2026)، بينما أظهرت التطورات المتسارعة في تقنيات التزييف العميق عن تحديات في كفاية الأطر القانونية والتنظيمية القائمة وقابليتها للإنفاذ، ولا سيما تجاه الاستخدامات المستحدثة لهذه التقنيات(Birrer & Just, 2025).

السياسات السَّائدة للتعامل مع المشكلة ومحدوديتها

أدى التسارع الكبير في تطور تقنيات التزييف العميق للصوت، إلى دفع الدول والمؤسَّسات إلى تبنِّي مجموعة من السياسات والإجراءات المتفاوتة في طبيعتها وفعاليتها، تراوحت بين المعالجة التقنية والتدخلات التشريعية والمبادرات التوعوية ذات الطابع الوقائي، غير أنَّ القراءة التحليلية لهذه السياسات تكشف أن معظمها لا يزال محكومًا بمنطق الاستجابة الجزئية، ولم يرتقِ بعد إلى مستوى الإستراتيجية الشَّاملة، القادرة على التعامل مع الظاهرة بوصفها تهديدًا مركبًا للأمن الرقمي والمجتمعي في آن واحد.

بطء التحديث القانوني واتساع الفجوة التشريعية

تُعدُّ التشريعات القانونية إحدى أهم أدوات الدولة في مواجهة المخاطر النَّاشئة في الفضاء الرقمي، غير أنَّ غالبية الأطر القانونية القائمة في عدد كبير من الدول لم تُصمَّم في الأصل للتعامل مع تقنيات الذكاء الاصطناعي التوليدي، ولا سيما التزييف العميق للصوت، فالعديد من قوانين الجرائم الإلكترونية لا تزال تركز على مفاهيم تقليدية، مثل: انتحال الهوية النصِّي، أو الاختراق

التقني المباشر، دون أن تتضمن نصوصًا صريحةً تُجَرِّم إنتاج ونشر وتوظيف المقاطع الصوتية المزَيَّفة المنتجة آليًّا (Zuboff, 2024, pp. 112-113).

ويُفضي هذا القصور إلى نشوء فراغ قانوني تستفيد منه الجهات المضلّلة والإجرامية؛ حيث يصبح من الصعب توصيف الجريمة بدقة، وإثبات القصد الجنائي وتحديد المسؤولية القانونية، خصوصًا في الحالات التي يُستخدم فيها الصوت المزيَّف لأغراض التأثير غير المباشر، مثل: زعزعة الثقة أو إثارة الفوضى، دون تحقيق مكاسب مادية مباشرة، كما أنَّ بطء الإجراءات التشريعية مقارنةً بسرعة تطوّر التقنية، يجعل القوانين غالبًا متأخرة بخطوة أو أكثر عن الواقع التقني المتغيّر.

تفاوت القدرات التقنية بين الدول والمؤسَّسات

على المستوى التقني، أحرزت بعض الدول المتقدمة خطواتٍ مهمةً في تطوير وتبني أدوات متقدِّمة لكشف التزييف الصوتي، تعتمد على تحليل البصمة الصوتية وأنماط التردّد والتناقضات الدقيقة في الإيقاع والنبرة، غير أنَّ هذه القدرات لا تتوافر بشكل متكافئ على المستوى الدولي، ولا حتى داخل الدولة الواحدة بين مختلف مؤسَّساتها (Fire et al., 2025, pp. 2-3).

ففي حين تمتلك بعض الجهات الأمنية والسيبرانية مختبرات رقمية متقدِّمة، لا تزال جهات أخرى تعتمد على أدوات محدودة وتقنيات تقليدية لم تعد قادرة على مجاراة جودة المقاطع المزيَّفة المُنتجة باستخدام نماذج ذكاء اصطناعي متقدمة. ويؤدي هذا التفاوت إلى إضعاف منظومة الاستجابة الشاملة؛ إذ تصبح بعض القطاعات أكثر عرضة للاختراق الصوتي من غيرها، ولا سيما القطاعات المالية والإعلامية والإدارية.

محدودية الوعي المجتمعي وضعف الثقافة الأمنية الرقمية

على الرغم من تزايد الحديث عن مخاطر الأخبار الزائفة عمومًا، فإنَّ الوعي المجتمعي بخطورة التزييف الصوتي تحديدًا لا يزال محدودًا؛ إذ يميل كثير من الأفراد إلى منح التسجيلات الصوتية درجةً عاليةً من المصداقية، انطلاقًا من الاعتقاد السَّائد بأنَّ الصوت يصعب تزويره مقارنةً بالصورة أو النص، ويزداد هذا التأثير حين يُنسب التسجيل إلى شخصية رسمية، أو جهة أمنية، أو مؤسَّسات ذات مكانة اعتبارية (Chesney & Citron, 2019, pp. 853-854).

غياب بروتوكولات تحقيق رقمية متخصِّصة

من أبرز أوجه القصور في السياسات الحالية؛ غياب بروتوكولات موحدة ومتخصِّصة للتحقيق الجنائي الرقمي في قضايا التزييف الصوتي، ففي كثير من الحالات تعتمد الأجهزة الأمنية والقضائية على أساليب تقليدية في فحص التسجيلات الصوتية، تركز على جودة الصوت أو مصدره الظاهري، وهي مقاربات لم تعد كافية في ظل القدرة المتزايدة لتقنيات الذكاء الاصطناعي على محاكاة الأصوات البشرية بدقة عالية (Vaccari & Chadwick, 2020, pp. 6-8).

كما أن نقص التدريب المتخصص وغياب الأدلة الإجرائية المعيارية يمثلان تحديًا أمام فعالية التحقيق في قضايا التزييف العميق للصوت؛ إذ تتطلب هذه القضايا قدرات متخصصة في فحص المحتوى الاصطناعي وتحليل الأدلة الرقمية والتحقق من أصالتها. وقد أكدت المنظمة الدولية للشرطة الجنائية «الإنتربول» أهمية بناء قدرات أجهزة إنفاذ القانون وتدريب العاملين فيها على التعرف

على تحديد الوسائط الاصطناعية وكشفها وتحليلها، وتعزيز القدرات الجنائية والتحقيقية اللازمة للتعامل معها(INTERPOL, 2024). ويكتسب هذا التحدي أهمية أكبر في القضايا العابرة للحدود؛ حيث تتداخل الاختصاصات القانونية، وتتعدَّد مصادر التهديد.

محدودية التنسيق المؤسَّسي وتجزئة الاستجابات

تتَّسم السياسات السَّائدة في كثير من الدول بقدر من التجزئة؛ حيث تعمل الجهات التقنية والأمنية والتشريعية والإعلامية في مسارات متوازية دون إطار تنسيق جامع. ويؤدي هذا الانفصال إلى تكرار الجهود أحيانًا، وإلى وجود فجوات واضحة في الاستجابة، خصوصًا في المراحل الأولى لانتشار المقاطع الصوتية المزيَّفة (Gasser & Almeida, 2021, pp. 12–13). إنَّ غياب التنسيق المؤسسي يُقَلِّل من القدرة على الاستجابة السريعة والمتكاملة، ويحدُّ من الاستفادة القصوى من الموارد المتاحة، سواء أكانت تقنية أم بشرية أم قانونية.

السياق العربي في مواجهة التزييف العميق للصوت

بالرغم من محدودية البيانات العربية المتخصِّصة حول التزييف العميق للصوت بوصفه مجالًا مستقلًّا للرصد والتحليل، فإنَّ المؤشِّرات المرتبطة بتنامي الجرائم الرقمية ومُمارسات الاحتيال القائمة على انتحال الهُويَّة، تُشير إلى أنَّ المنطقة العربية ليست بمنأى عن هذا التهديد (International Telecommunication Union [ITU], 2025). ويكتسب التزييف الصوتي حساسيةً إضافيةً في السِّياقات العربية بالنظر إلى ارتفاع مستويات الثقة الاجتماعية في الرسائل والتسجيلات الصوتية، وما يرتبط بذلك من قابلية أكبر للتأثر بالمحتوى المنسوب إلى شخصيات أو جهات رسمية.

كما أنَّ معظم المقاربات العربية الحالية لا تزال تتعامل مع الظاهرة ضمن الأطر العامة للجرائم المعلوماتية أو الأمن السيبراني، دون تطوير سياسات متخصِّصة أو بروتوكولات وطنية لكشف التزييف الصوتي والتحقيق فيه، وهو ما يسهم في اتساع الفجوة بين سرعة تطوُّر أدوات الذكاء الاصطناعي، وقدرة المنظومة التنظيمية والمؤسَّسية على الاستجابة.

وعليه، فإنَّ الإفادة من الخبرات الدولية في السياق العربي، لا تقتضي استنساخ النماذج القائمة، بقدر ما تتطلب تكييفها بما يتلاءم مع مستويات الجاهزية المؤسَّسية والخصوصيات الاجتماعية والثقافية لكل دولة.

ومن خلال ما سبق، يُمكن القول إنَّ السياسات السَّائدة للتعامل مع التزييف العميق للصوت، على الرغم من أهميتها، لا تزال تعاني قصورًا في شمولية الرؤية، وبطئًا في التكيف، وتفاوتًا في القدرات، وضعفًا في البُعد الوقائي المجتمعي. وهو ما يُبرز الحاجة الملحة إلى الانتقال من سياسات رد الفعل إلى سياسات استباقية متكاملة، تقوم على تحديث التشريعات، وتعزيز القدرات التقنية، وبناء الوعي المجتمعي، وتطوير منظومات التحقيق الرقمي، ضمن إطار وطني منسَّق يعالج هذه الظاهرة بوصفها تحديًا أمنيًّا متعدد الأبعاد.

مقارنة السياسات الدولية في مواجهة التزييف العميق للصوت

تُظهر التجارب الدولية المختلفة أنَّ التعامل مع ظاهرة التزييف العميق للصوت لم يعد مسألةً تقنيةً بحتةً، بل تحول إلى قضية سياسات عامة ذات أبعاد

أمنية وقانونية ومجتمعية متداخلة، فالدول التي أدركت مبكرًا خطورة هذه الظاهرة، سعت إلى تطوير مقاربات شاملة تجمع بين التشريع والتقنية وبناء القدرات والتوعية المجتمعية، في حين لا تزال دول أخرى تعتمد على سياسات جزئية أو ردود أفعال ظرفية لا ترقى إلى مستوى التهديد المتنامي.

وتكمن هنا أهمية المقارنة بين السياسات الدولية في أنها تُبرز بوضوح الفروق في المقاربات الوقائية والاستباقية من جهة، والمقاربات التفاعلية المحدودة من جهة أخرى، كما تُتيح استخلاص أفضل الممارسات القابلة للتكييف مع السّياقات الوطنية المختلفة.

تجربة الاتحاد الأوروبي

يندرج تعامل الاتحاد الأوروبي مع ظاهرة التزييف العميق للصوت ضمن رؤية أوسع لحماية الفضاء المعلوماتي الأوروبي، تقوم على اعتبار الأمن الرقمي جزءًا لا يتجزأ من الأمن المجتمعي. وانطلاقًا من هذه الرؤية، لم يقتصر النهج الأوروبي على ملاحقة الأفراد المتورطين في إنتاج المحتوى المزيَّف أو نشره، بل اتجه في المقام الأول إلى إعادة تنظيم البيئة الرقمية نفسها، ولا سيما المنصات الكبرى التي تمثل القناة الرئيسة لتداول هذا النوع من المحتوى.

ويُشير الجدول 1 أدناه، استنادًا إلى بيانات حديثة وردت في تقارير أوروبية معتمدة على معطيات اليوروبول، إلى أنَّ نحو 49% من الشركات داخل الاتحاد الأوروبي، تعرضت لمحاولات احتيال باستخدام تقنيات التزييف العميق للصوت، في حين تمكنت أجهزة إنفاذ القانون من اعتراض حوالي 7,500 مكالمة هاتفية احتيالية مولَّدة بالذكاء الاصطناعي خلال عام 2024 فقط (Euro-pean Parliamentary Research Service, 2025).

يُعدُّ قانون الخدمات الرقمية (DSA) حجر الزاوية في مقاربة الاتحاد الأوروبي لمواجهة التزييف العميق

جدول 1

مؤشرات حول جرائم التزييف العميق للصوت والاحتيال الرقمي في الاتحاد الأوروبي

المؤشرات	القيمة المسجَّلة	الدلالة الأمنية
نسبة الشركات التي تعرضت لمحاولات احتيال باستخدام التزييف العميق للصوت	49%	يعكس اتساع نطاق استخدام التزييف العميق في الهجمات الاحتيالية الموجهة
عدد مكالمات الاحتيال المعتمدة على تقنيات الذكاء الاصطناعي التي تمَّ اعتراضها من قبل أجهزة إنفاذ القانون	نحو 7,500 مكالمة	يُبرز هذا العدد الدور الوقائي للتدخل الأمني المبكر
أكثر أنماط التزييف استخدامًا	انتحال صوت مسؤولين تنفيذيين أو مؤسَّسات رسمية	يدل المؤشِّر على استهداف الثقة المؤسَّسية
القطاعات الأكثر تضرّرًا	الشركات المتوسطة والكبيرة، القطاع المالي	يشير إلى ارتفاع المخاطر الاقتصادية
أبرز التهديدات المرتبطة بالتزييف الصوتي	الاحتيال المالي، التضليل، الابتزاز	يشكل تهديدًا مباشرًا للأمن الاقتصادي وأمن الاتصالات

المصدر: (European Parliamentary Research Service, 2025)

للصوت؛ إذ يفرض على المنصَّات الرقمية الكبرى التزامات قانونية واضحة، تتعلق برصد المحتوى المضلِّل، بما في ذلك المحتوى المولَّد بواسطة تقنيات الذكاء الاصطناعي، والتعامل معه ضمن أطر زمنية محدَّدة، ولا يكتفي هذا القانون بالمطالبة بالإزالة أو التقييد، بل يشترط كذلك وجود آليات داخلية فعَّالة لتقييم المخاطر والإبلاغ عنها واتخاذ تدابير وقائية قبل تفاقم آثارها (European Commission, 2025a).

ومن الجوانب اللافتة في التجربة الأوروبية اعتمادها مبدأ الشَّفافية بوصفه أداةً أمنيةً؛ حيث ألزمت المنصَّات بالإفصاح عن طبيعة المحتوى المنتج آليًّا، سواء أكان نصًّا أم صورةً أم صوتًا، ويكتسب هذا الإجراء أهمِّية خاصة فيما يتعلق بالتزييف الصوتي؛ إذ يحدُّ من قدرة التسجيلات المزيَّفة على التأثير الخفي في الرأي العام، ويمنح المستخدم العادي فرصة إدراك الطابع الاصطناعي للمحتوى قبل التفاعل معه أو تداوله.

وإلى جانب الإطار التنظيمي، استثمر الاتحاد الأوروبي أيضًا في برامج بحثية وتطويرية متقدِّمة، ركزت على ابتكار أدوات قادرة على كشف التزييف الصوتي، عبر تحليل الخصائص الدقيقة للصوت، مثل: التردُّدات غير الطبيعية، أو أنماط التنفس، أو التفاوت الزمني بين المقاطع، وقد أُنجزت هذه المشاريع في إطار تعاون وثيق بين الجامعات ومراكز الأبحاث والمؤسَّسات الأمنية، وهو ما مَكَّن من ربط المعرفة الأكاديمية بالاحتياجات العملية لأجهزة إنفاذ القانون الأوروبية (European Commission, 2025b, DETECTOR project).

ومع ذلك، لا تخلو المقاربة الأوروبية من تحدِّيات، أبرزها بُطء الإجراءات التنظيمية مقارنةً بسرعة تطوُّر تقنيات التزييف، إضافة إلى تعقيد التنسيق بين الدول الأعضاء، واختلاف مستويات الجاهزية التقنية والقانونية بينها، ومع ذلك تبقى هذه التجربة من أكثر النماذج نضجًا من حيث الربط بين الشفافية والمساءلة المؤسسية.

تجربة الولايات المتحدة الأمريكية

تُشير البيانات الصادرة عن لجنة التجارة الفيدرالية الأمريكية إلى ارتفاع الخسائر المبلغ عنها الناتجة عن جرائم الاحتيال الصوتي في الولايات المتحدة الأمريكية، إلى نحو 12.5 مليار دولار خلال عام 2024، في ظل تنامٍ متسارعٍ لاستخدام تقنيات الذكاء الاصطناعي في هذا المجال (Federal Trade Commission, 2025). وفي استجابة تنظيمية مباشرة لهذه المخاطر، بادرت لجنة الاتصالات الفيدرالية الأمريكية إلى حظر استخدام المكالمات الهاتفية المولَّدة بأصوات ذكاء اصطناعي لأغراض الاحتيال أو التأثير في العمليات الانتخابية، مع تمكين السلطات من فرض غرامات مالية على كل مكالمة مخالفة(Federal Communications Commission, 2024)، وتعدُّ هذه الإجراءات انعكاسًا لتصاعد إدراك المؤسَّسات الأمريكية لخطورة التزييف الصوتي على الأمن الاقتصادي والديمقراطي.

وتعكس التجربة الأمريكية في مواجهة مخاطر التزييف الصوتي، طبيعة النظام الفيدرالي القائم؛ حيث تتوزَّع الصلاحيات بين المستوى الاتحادي ومستوى الولايات، وهو ما أفرز استجابات متعدِّدة المستويات لمواجهة التزييف العميق للصوت، وقد أسهمت حوادث واقعية شملت عمليات احتيال مالي وتسجيلات صوتية مزيَّفة نُسبت إلى مسؤولين وشخصيات عامة، في تسريع وتيرة الاهتمام بهذه الظاهرة (Federal Trade Commission [FTC], 2023)..

وعلى مستوى الولايات، بادرت بعضها، مثل كاليفورنيا وتكساس، إلى سنِّ تشريعات تحظر

استخدام التزييف العميق للصوت في السياقات الانتخابية أو لأغراض التضليل السياسي، خصوصًا خلال الفترات الحسَّاسة التي تسبق الانتخابات (Gold-berg, 2025). وتُعدُّ هذه الخطوة انعكاسًا مباشرًا للقلق من تأثير الأصوات المزيَّفة في توجيه الناخبين أو تشويه صورة المرشحين.

أما على المستوى الاتحادي، فقد اضطلعت وزارة الأمن الداخلي الأمريكية بدورٍ محوريٍّ في تطوير برامج متخصِّصة لرصد التزييف الصوتي، ولا سيَّما ذلك الموجه إلى مؤسَّسات الطوارئ أو البنية التحتية الحيوية أو الجهات الأمنية، وتركز هذه البرامج على بناء قدرات استباقية تعتمد على تحليل الأنماط والإنذار المبكر والتنسيق بين الوكالات المختلفة (U.S. Department of Homeland Security, 2025, p. DHS report).

كما تتميَّز التجربة الأمريكية كذلك بحضور قوي للقطاع الخاص؛ إذ أدَّت شركات التكنولوجيا الكبرى دورًا مهمًّا في تطوير أدوات كشف التزييف الصوتي، سواء بدافع المسؤولية المجتمعية أو لحماية مصداقية منصّاتها، وقد أفرز هذا الوضع نمطًا من الشراكة بين القطاعين العام والخاص، يقوم على تبادل المعرفة والتقنيات. غير أنَّ أبرز نقاط ضعف هذه التجربة تكمن في التفاوت التشريعي بين الولايات وغياب إطار اتحادي موحَّد يعالج الظاهرة بصورة شاملة، وهو ما يؤدي أحيانًا إلى ثغرات قانونية يمكن استغلالها. (FTC, 2024)

تجربة الصين

تنطلق المقاربة الصينية في التعامل مع التزييف العميق للصوت من اعتبارات تتعلق بالأمن المعلوماتي والاستقرار المجتمعي، وقد أصدرت الصين لوائحَ تنظيميةً تُلزم بوسم المحتوى المولَّد بالذكاء الاصطناعي، بما في ذلك المقاطع الصوتية، ومنع تداوله دون الإفصاح الواضح عن طبيعته الاصطناعية (Cyberspace Ad-ministration of China, 2025).

وتفرض السلطات الصينية رقابةً صارمةً على المنصَّات الرقمية، وتُحملها مسؤولية مباشرة عن المحتوى المتداول، مع فرض عقوبات سريعة في حال الإخلال بالضوابط. وتُسهم هذه المقاربة في تقليص الانتشار الواسع للتزييف الصوتي، بفضل الجمع بين القدرات التقنية المتقدمة والتنظيم الصارم. وعلى الرغم من الانتقادات الموجهة إلى هذه التجربة بسبب تشدّدها، فإنها تُظهر فعالية من حيث السيطرة السريعة على المحتوى المضلّل، وتوفير بيئة رقمية أقل عرضة للفوضى المعلوماتية.

تجربة كوريا الجنوبية

على الرغم من غياب إحصاءات رسمية تفصِّل جرائم التزييف العميق للصوت بوصفها فئةً مستقلةً في كوريا الجنوبية، فإنَّ تقارير حكومية وأمنية قد أشارت إلى تزايد استخدام تقنية استنساخ الصوت بالذكاء الاصطناعي في أنماط الاحتيال وانتحال الهوية، خصوصًا في السياقات المالية والهندسة الاجتماعية، وهو ما يعني تحول التزييف الصوتي إلى تهديد أمني صامت، يصعب رصده إحصائيًّا ضمن التصنيفات الجنائية التقليدية (Korea Internet & Security Agency, 2024, pp. 27-29).

وتُعدُّ كوريا الجنوبية من الدول التي تعاملت مع التزييف العميق، بما في ذلك التزييف العميق للصوت، وفق نهج يقوم على الحزم القانوني والجاهزية التقنية، مستفيدةً من تجارب سابقة في مواجهة الجرائم الإلكترونية ذات الأثر المجتمعي الواسع. وقد أقرَّت الحكومة تشريعات

تُجرِّم صراحةً إنتاج أي محتوى مزيف أو تداوله إذا كان يمس الحياة الخاصة أو الأمن العام، مع فرض عقوبات مشددة على المخالفين (Kim, 2025, pp. 532-533).

ويُلاحظ في التجربة الكورية تركيزها الكبير على البعد التقني التطبيقي؛ إذ تمتلك الدولة مختبرات متقدمة تستخدم تقنيات الذكاء الاصطناعي العكسي لتحليل الأصوات، وتحديد مؤشرات التلاعب بدقة عالية (The Korea Times, 2025). ولا يقتصر دور هذه المختبرات على الدعم الفني، بل تُعدُّ جزءًا من منظومة التحقيق الجنائي الرقمي. كما تعتمد كوريا الجنوبية على شراكات وثيقة بين الحكومة والجامعات، تُسهم في تدريب الكوادر الأمنية والقضائية على أحدث تقنيات تحليل الأدلة الصوتية، بما يضمن مواكبة التطور السريع في هذا المجال. ويُعدُّ هذا الاستثمار في العنصر البشري أحد أبرز عناصر القوة في التجربة الكورية.

ويلخص الجدول 2 أدناه أبرز أوجه التفاوت بين المقاربات الدولية في مواجهة التزييف العميق للصوت؛ إذ يركز الاتحاد الأوروبي على التنظيم والحوكمة، مع مستوى تقني متوسط، بينما تعكس تجربة الولايات المتحدة الأمريكية تباينًا في التشريع والتنسيق، مقابل قدرات تحقيقية وتقنية قوية. في حين تعتمد التجربة الصينية نموذجًا رقابيًّا صارمًا، وتقنيات قوية، وتنسيقًا عاليًا، مع ضعف نسبي في البُعد التوعوي. أما كوريا الجنوبية، فتتميز بالحزم القانوني والتفوق التقني، على الرغم من محدودية التوعية.

بدائل السياسات المقترحة لمواجهة التزييف العميق للصوت وتقييمها

تستند بدائل السياسات المقترحة في هذا المحور إلى التحليل المقارن للمقاربات الدولية والمعطيات القانونية والتقنية التي تمَّ استعراضها في المحاور السَّابقة من الورقة، وإلى اجتهاد الباحث في تقييم ومواءمة هذه الخبرات مع الخصوصية الوطنية للدول العربية. وقد اتضح أنَّ مواجهة التزييف العميق للصوت لا يمكن أن تتم من خلال حل أُحادي أو إجراء تقني معزول، بل تتطلب حزمةً متكاملةً من البدائل السياسية القابلة للتكييف مع السياق الوطني، والتي تراعي الطبيعة المركبة لهذا التهديد بوصفه خطرًا رقميًّا وأمنيًّا ومجتمعيًّا في آنٍ واحدٍ.

جدول 2

مقارنة بين المقاربات الدولية في التعامل مع التزييف العميق للصوت

المقاربات الدولية	التشريع	التقنية	التوعية	التحقيق الجنائي	التنسيق
الاتحاد الأوروبي	قوي تنظيمي	متوسطة	متوسطة	متوسط	عالٍ
الولايات المتحدة الأمريكية	متفاوت	قوية	محدودة نوعًا ما	قوي	متفاوت
الصين	تنظيم رقابي صارم	قوية	ضعيفة نسبيًّا	قوي	عالٍ
كوريا الجنوبية	قانون صارم	قوية	محدودة	قوي	متوسط

المصدر: الجدول من إعداد الباحث

تحديث الإطار التشريعي وبناء منظومة قانونية متخصّصة

يتمثَّل هذا البديل في مراجعة وتحديث التشريعات الوطنية ذات الصلة بالجرائم الإلكترونية، بما يضمن إدراج نصوص قانونية صريحة تُجرِّم إنتاج المقاطع الصوتية المفبركة المولدة بتقنيات الذكاء الاصطناعي أو تداولها أو توظيفها، متى ترتب على ذلك المساس بالأمن العام، أو تضليل الرأي العام، أو الإضرار بالأفراد والمؤسسات.

ويتميَّز هذا البديل بكونه يوفر أساسًا قانونيًّا واضحًا يحدُّ من الغموض التشريعي، ويُعزِّز قدرة الأجهزة القضائية والأمنية على توصيف الجريمة، وتحديد المسؤوليات، وإثبات القصد الجنائي. كما يسمح بتدرّج العقوبات وَفْق خطورة الفعل، ويشمل الأفعال التحضيرية، مثل توفير أدوات التزييف والترويج لها.

ويُعدُّ تحديث الإطار التشريعي شرطًا لازمًا لأي سياسة فعَّالة في مواجهة التزييف العميق للصوت؛ لما يوفره من وضوح قانوني، وردع رمزي ومادي. فمن حيث الفعالية، يتيح هذا البديل توصيف الجريمة بشكل أدق، ويغلق جانبًا مهمًّا من الفراغ القانوني الذي تستغله الجهات المضللة، كما يُعزز قدرة الأجهزة القضائية على التحرك بثقة، ويبعث برسالة واضحة تؤكد جدية الدولة في التعامل مع هذا التهديد.

ومع ذلك، يظل هذا البديل، على الرغم من أهميته، محدود الأثر إذا نُفِّذ بمعزل عن غيره؛ لأن القوانين وحدها لا تكفي للحد من الجريمة، ومعالجتها بعد حدوثها. كما أنَّ بُطء المسار التشريعي مقارنةً بسرعة تطور تقنيات الذكاء الاصطناعي قد يجعل النصوص القانونية متأخرة عن الواقع التقني. وعليه، يُمكن القول إنَّ البديل التشريعي يُمثِّل قاعدةً ضروريةً، لكنه لا يكفي بوصفه حلًّا منفردًا.

إنشاء وحدة وطنية متخصِّصة في كشف التزييف الصوتي والتحقيق الجنائي الرقمي

يقترح هذا البديل إحداث وحدة وطنية أو مركز متخصِّص يُعنى برصد المقاطع الصوتية المفبركة وكشفها وتحليلها، ويعمل بوصفه مرجعيةً فنيةً للأجهزة الأمنية والقضائية والإعلامية، وتُجَهَّز هذه الوحدة بأدوات تقنية متقدمة تعتمد على تحليل البصمة الصوتية، والتردّدات الدقيقة، والأنماط غير الطبيعية في النطق والتنفس والإيقاع.

ويتميَّز هذا البديل بقدرته على تعزيز الجاهزية التقنية والمؤسَّسية، وتحسين جودة الأدلة الرقمية وتسريع وتيرة التحقيقات، وتقليص هامش الشَّك في النتائج الفنية أمام القضاء. كما يسمح بتوحيد بروتوكولات التحقيق، وبناء قاعدة بيانات وطنية للأصوات وأنماط التزييف المكتشفة.

غير أنَّ هذا البديل يواجه تحدِّيات تتعلق بالكلفة والاستدامة، نظرًا إلى حاجته إلى توفير القدرات التشغيلية والتقنية والكوادر الكافية للتعامل مع الزيادة المضطردة المتوقعة لحالات التزييف العميق، فضلًا عن ضرورة وجود استثمارات مالية مستمرة، وتحديث دوري للأدوات، وتأهيل متخصِّص للموارد البشرية، كما أنَّ فعاليته القصوى تبقى رهينةً بمدى تكامله مع الأطر القانونية والتنظيمية، حتى لا يتحول إلى جهد تقني معزول يفتقر إلى الغطاء التشريعي والشرعية المؤسَّسية.

اعتماد سياسة وطنية شاملة للتوعية وبناء الثقافة الأمنية الرقمية

ينطلق هذا البديل من فرضية أساسية مفادها أنَّ الوقاية المجتمعية تُمَثِّل خط الدفاع الأول في مواجهة التزييف العميق للصوت، ويقوم على إطلاق برامج توعوية

وطنية مستدامة، تستهدف مختلف فئات المجتمع، وتهدف إلى تعزيز مهارات التحقُّق الرقمي، وترسيخ ثقافة التشكيك الإيجابي قبل تداول المحتوى الصوتي.

وتشمل هذه السياسة إدماج مفاهيم الأمن الرقمي في المناهج التعليمية، وتنظيم حملات إعلامية دورية، وإعداد أدلة إرشادية مبسَّطة، وتدريب الموظفين العموميين والعاملين في القطاعات الحسَّاسة على التعرُّف على مؤشرات التزييف الصوتي.

ويمتاز هذا البديل بكونه الأقل كلفةً مقارنة بحجم أثاره المتوقعة على المدى المتوسط والطويل؛ إذ يُسهم في تحصين المجتمع وتقليص قابلية الأفراد للتأثر بالمقاطع الصوتية المزيَّفة، كما ينسجم مع التحوُّلات الحديثة في الفكر الأمني، التي أصبحت تعترف بدور المواطن بوصفه فاعلًا في منظومة الأمن، وليس مجرد متلقٍّ للحماية.

إلا أنَّ التحدّي الجوهري لهذا البديل يكمن في صعوبة قياس نتائجه بشكل فوري، واعتماده الكبير على الاستمرارية والتراكم الزمني، كما أنَّ فعاليته تظل محدودة في غياب أدوات كشف تقنية وتشريعات رادعة، وهو ما يجعل من هذا البديل عنصرًا مُكمِّلًا أكثر من كونه بديلًا قائمًا بذاته.

تنظيم مسؤوليات المنصّات الرقمية وتعزيز الشراكة مع القطاع الخاص

يقوم هذا البديل على إعادة تنظيم البيئة الرقمية، من خلال تحميل المنصَّات الرقمية مسؤوليات واضحة في رصد المحتوى الصوتي المزيَّف، ووضع آلياتٍ للإبلاغ السريع والوسم الإجباري للمحتوى المولّد آليًّا، بما يُسهم في الحدّ من انتشاره وتأثيره. كما يشمل هذا البديل بناء شراكات إستراتيجية مع شركات التكنولوجيا والاتصالات، للاستفادة من خبرتها في تطوير أدوات كشف التزييف، وتبادل البيانات الفنية وتعزيز الابتكار المحلي في هذا المجال.

ويُمثِّل هذا البديل مدخلًا مهمًّا لمعالجة المشكلة عند نقطة الانتشار الأساسية، وهي المنصَّات الرقمية؛ إذ يُتيح تنظيم مسؤولياتها تقليص سرعة انتشار المحتوى المزيَّف، ورفع مستوى الشَّفافية، وتحميل الفاعلين الرقميين جزءًا من المسؤولية الأمنية.

غير أنَّ هذا البديل يواجه تحديات قانونية وتنظيمية، تتعلق بتباين التشريعات الوطنية، والطابع العابر للحدود للمنصَّات الرقمية، وإشكاليات حرية التعبير، كما تعتمد فعاليته بدرجة كبيرة على مستوى تعاون المنصات، سواء أكان طوعيًا أم قائمًا على الالتزام النظامي، وهو ما قد لا يكون مضمونًا في جميع الحالات.

مقاربة تكاملية تجمع بين البدائل السَّابقة ضمن إستراتيجية وطنية موحدة

يتمثَّل هذا البديل في دمج البدائل الأربعة السَّابقة ضمن إستراتيجية وطنية شاملة لمواجهة التزييف العميق للصوت، تقوم على التنسيق المؤسَّسي، وتوزيع الأدوار، وتكامل الأدوات القانونية والتقنية والتوعوية. ويُعدُّ هذا الخيار الأكثر فعالية على المدى المتوسط والبعيد؛ لأنه يعالج الظاهرة من جذورها، ويحدُّ من انتقالها بين القطاعات، ويُعزِّز مناعة الدولة والمجتمع في مواجهة أشكال التزييف المستقبلية. غير أنَّ نجاح هذا البديل يظل مرهونًا بوجود قيادة مؤسَّسية واضحة، وآليات تنسيق فعَّالة، ونظام متابعة وتقييم دوري لقياس الأداء، وتحديث السياسات وفق المستجدَّات.

وتُظهر بدائل السياسات المقترحة أنَّ الاعتماد على حلٍّ منفردٍ، سواء أكان تشريعيًّا أم تقنيًّا أم توعويًّا، لن يكون كافيًا لمواجهة التزييف العميق للصوت بفعالية،

وعليه، تميل هذه الورقة إلى ترجيح الخيار التكاملي الذي يجمع بين تحديث التشريعات وتعزيز القدرات التقنية، وبناء الوعي المجتمعي، وتنظيم البيئة الرقمية في إطار وطني منسَّق وقابل للتطوير.

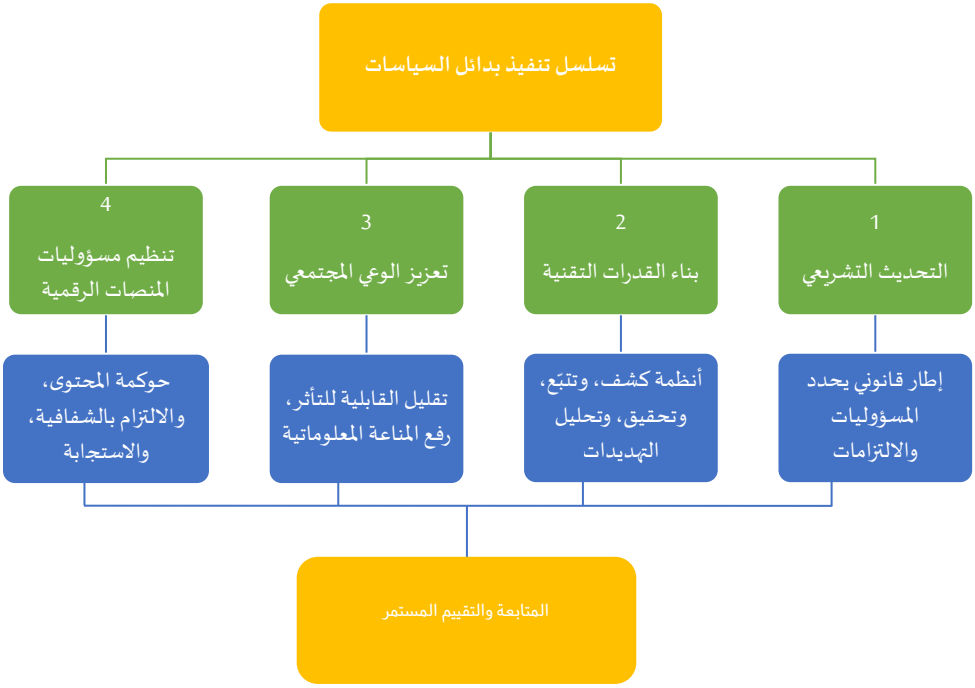
ترجيح السيناريو الأمثل: المقاربة التكاملية الشَّاملة

في ضوء التقييم المقارن للبدائل السَّابقة، يتبيَّن أنَّ المقاربة التكاملية التي تجمع بين التحديث التشريعي، وبناء القدرات التقنية، وتعزيز الوعي المجتمعي، وتنظيم البيئة الرقمية، تُمثِّل السيناريو الأكثر توازنًا وفعالية؛ لأنها لا تعالج مشكلة التزييف العميق للصوت من زاوية واحدة، بل تتعامل معها بوصفها تهديدًا مركبًا يتطلب استجابةً متعدِّدة المستويات.

ويتحقق التكامل بين البدائل المقترحة وفق منهج تتابعي لا تجميعي؛ إذ يبدأ المسار بالتحديث التشريعي بوصفه الإطار المنظم للمسؤوليات، ثم ينتقل إلى بناء القدرات التقنية للكشف والتحقيق، يلي ذلك تعزيز الوعي المجتمعي للحدّ من قابلية الأفراد للتأثر، قبل استكمال المنظومة بتنظيم مسؤوليات المنصَّات الرقمية. وتخضع هذه المراحل لمنظومة متابعة وتقييم دوري، تسمح بتحديث الاستجابة وفق تطوُّر التهديدات، كما في الشكل 2.

شكل 2

تسلسل تنفيذ المقاربة التكاملية



المصدر: من إعداد الباحث

التوصيات

- تُوصي الورقة بالإسراع في تحديث التشريعات الوطنية ذات الصلة بالجرائم الإلكترونية، من خلال إدراج تعريف قانوني دقيق للتزييف العميق للصوت يحدِّد نطاقه وأشكاله والأفعال المجرَّمة المرتبطة به، مع اعتماد مقاربة تشريعية مرنة تضمن مواكبة التطور التقني، وتحقيق التوازن بين متطلَّبات الأمن وحماية الحقوق.
  - الجهة القائدة: وزارة العدل.
  - الجهات الشريكة: الجهات المختصة بالأمن الرقمي.
  - الأفق الزمني: قصير المدى (6 12- شهرًا).
- تُوصي الورقة بإنشاء مركز وطني يكون مرجعيةً وطنيةً فنِّية وتقنية في قضايا التزييف الصوتي، يضطلع بمهام الكشف والتحليل، ودعم التحقيقات الجنائية الرقمية، وتوحيد البروتوكولات الفنية، وبناء قواعد بيانات متخصِّصة، وذلك في إطار شراكات مؤسَّسية مع الجامعات ومراكز الأبحاث؛ لضمان تراكم الخبرة.
  - الجهة القائدة: وزارة الداخلية.
  - الجهات الشريكة: الجامعات، ومراكز الأبحاث، والجهات التقنية المختصة.
  - الأفق الزمني: متوسط المدى (3-1 سنوات).
- تُوصي الورقة بالانتقال من المبادرات التوعوية المحدودة، إلى إستراتيجية وطنية شاملة تهدف إلى رفع الوعي المجتمعي بمخاطر التزييف العميق للصوت، وتعزيز مهارات التحقُّق النقدي، وإدماج مفاهيم الأمن الرقمي في التعليم الأساسي، مع استهداف الفئات الأكثر عرضة، مثل: الإعلاميين، والموظفين العموميين، والقطاعات المالية.
  - الجهة القائدة: وزارة التعليم والقطاع المكلف بالاتصال.
  - الجهات الشريكة: المؤسَّسات الإعلامية والجهات المعنية بالأمن الرقمي.
  - الأفق الزمني: متوسط إلى طويل المدى.
- تُوصي الورقة بوضع أطر تنظيمية تُحمِّل المنصَّات الرقمية مسؤوليات محدَّدة في رصد ووسم المحتوى المولَّد آليًّا، وتوفير آليات إبلاغ فعَّالة، وتعزيز التعاون مع الجهات الوطنية المختصة، مع مراعاة خصوصيات حرية التعبير والطبيعة العابرة للحدود للفضاء الرقمي.
  - الجهة القائدة: الجهة الوطنية المختصة بتنظيم الاتصالات.
  - الجهات الشريكة: المنصَّات الرقمية والجهات التنظيمية ذات الصلة.
  - الأفق الزمني: متوسط المدى (1 - 3 سنوات).
- تُوصي الورقة بتعزيز التعاون مع شركات التكنولوجيا والاتصالات، والجامعات، ومراكز الأبحاث، بهدف تطوير حلول تقنية وطنية لكشف التزييف الصوتي، ونقل المعرفة، ودعم الابتكار في مجال الأمن الرقمي، من أجل تقليص التبعية التقنية الخارجية.
  - الجهة القائدة: الجهة الوطنية المختصة بالبحث والابتكار.
  - الجهات الشريكة: شركات التكنولوجيا، والجامعات، ومراكز الأبحاث.
  - الأفق الزمني: طويل المدى (أكثر من 3 سنوات).
- تُوصي الورقة بإرساء آليات مؤسَّسية منتظمة لمتابعة وتقييم فعالية السياسات المتخذة، من حيث الجاهزية الأمنية، والتنسيق المؤسَّسي،

وتطوُّر التهديدات، والأثر المجتمعي؛ بما يسمح بمراجعة الإستراتيجيات وتحديثها، وضمان استجابتها المستمرة للتحوُّلات التقنية.

- الجهة القائدة: لجنة وطنية مشتركة للمتابعة والتقييم.
- الجهات الشريكة: المؤسسات المعنية بتنفيذ السياسة.
- الأفق الزمني: مراجعة دورية (سنوية).

المراجع

Ahmadiadli, Y., Zhang, X.-P., & Khan, N. (2025). Beyond identity: A generalizable approach for deepfake audio detection. arXiv Preprint arXiv:2505.06766. https://2h.ae/uRgbk

Alqahs, K., Al-Kandari, Y. Y., & Albuloushi, M. S. (2023). Social media users' attitudes toward pervasiveness of fake news in Arab countries and its negative effects: Kuwait as a case study. Journal of Information, Communication and Ethics in Society, 21(3), 322–341. https://doi.org/10.1108/JICES-05-2022-0053

Bendiab, G., Zeltni, K., & Bader El Den, M. (2025). Audio deepfake: Generation methods, legitimate applications and the potential for misuse. University of Portsmouth. https://2h.ae/jnvNr

Birrer, A., & Just, N. (2025). What we know and don't know about deepfakes: An investigation into the state of the research and regulatory landscape. New Media & Society, 27(12), 6819–6838. https://doi.org/10.1177/14614448241253138

Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 111(4).

Cyberspace Administration of China. (2025). Measures for Labeling of AI-Generated Synthetic Content. China Law Translate. https://2h.ae/Xtgvn

El-Masri, A., Riedl, M. J., & Woolley, S. (2022). Audio misinformation on WhatsApp: A case study from Lebanon. Harvard Kennedy School Misinformation Review, 3(4). https://doi.org/10.37016/MR-2020-102

European Commission. (2025a). DETECTOR: Deepfake evidence and technology for forensic content oversight and research (Horizon EU project). CORDIS - European Commission. Retrieved from https://2h.ae/vZVps

European Commission. (2025b). Digital Services Act: ensuring transparency and accountability online. European Union. Retrieved from https://2h.ae/rdbPs

European Parliamentary Research Service. (2025). Scam calls and deepfake threats: AI-generated fraud

Gasser, U., & Almeida, V. A. F. (2021). A layered model for AI governance. IEEE Internet Computing, 25(6). https://2h.ae/ZtzWz

Goldberg, H. (2025). To craft effective state laws on deepfakes and elections, mind the details. TechPolicy.press. https://2h.ae/wPVZI

Issa, E. (2026). AFAD-MSA: Dataset and models for Arabic fake audio detection. Computation, 14(1), 20. https://doi.org/10.3390/computation14010020

INTERPOL. (2024). Beyond illusions: Unmasking the threat of synthetic media for law enforcement. International Criminal Police Organization.

International Telecommunication Union (ITU). (2025). State of digital development and trends in the Arab States region: Challenges and opportunities. Geneva: ITU.

Kim, K. (2025). Deepfakes: Challenges to intellectual property rights in South Korea. *GRUR International, 74(6). https://2h.ae/ydCcg

Korea Internet & Security Agency. (2024). Cyber threat trends report. Seoul, South Korea: Author. Security.org. (2025). 2024 Deepfakes guide and statistics. https://2h.ae/JsOIy

Stanford University. (2024). AI Index Report 2024. Stanford: Human- and its impacts. European Parliament. https://2h.ae/PDvvb

Federal Bureau of Investigation. (2026). 2025 internet crime report. Internet Crime Complaint Center. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

Federal Communications Commission (FCC). (2024). AI-generated voices in robocalls can deceive voters; FCC action to ban them. https://2h.ae/hjJaw

Federal Trade Commission. (2023). Scammers use fake emergencies to steal your money. Consumer Advice. https://consumer.ftc.gov/articles/scammers-use-fake-emergencies-steal-your-money

Federal Trade Commission. (2024). Approaches to address AI-enabled voice cloning. https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/04/approaches-address-ai-enabled-voice-cloning

Federal Trade Commission. (2025). New FTC data show big jump in reported losses to fraud to $12.5 billion in 2024. https://2h.ae/lurzg

Firc, A., Malinka, K., & Hanáček, P. (2025). Evaluation framework for deepfake speech detection: A comparative study of state-of-the-art deepfake speech detectors. Cybersecurity, 8, Article 50. https://2h.ae/ltcpm

Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. Social Media + Society, 6 (1). https://2h.ae/QvGVL

Zuboff, S. (2024). The law and artificial intelligence: Regulation, liability and rights in the age of deepfakes and generative models. Journal of Digital Law, 9(1).

Centered Artificial Intelligence (HAI). https://2h.ae/nzvKY

The Korea Times. (2025, February 2). South Korean police to develop deepfake detection system. Retrieved from https://2h.ae/JBxan

U.S. Department of Homeland Security. (2025). Increasing threats of deepfake identities: Deepfake detection and mitigation efforts (DHS Publication). U.S. Department of Homeland Security. https://2h.ae/LeTsJ

August 2026

أغسطس 2026

Security Research Center

Naif Arab University for Security Sciences, Saudi Arabia, Riyadh

مركز البحوث الأمنية

جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، الرياض

Keywords: security studies, deepfakes, cybersecurity, artificial intelligence, public policy, digital governance

الكلمات المفتاحية: الدراسات الأمنية، التزييف العميق للصوت، الأمن الرقمي، الذكاء الاصطناعي، السياسات العامة، الحوكمة الرقمية

Production and hosting by NAUSS

Email: srcenter@nauss.edu.sa

doi: 10.26735/ZBAC3466