AL-NAHRAIN UNIVERSITY
COLLEGE OF LAW
ISSN:3006- 0605 DOI:10.58255

الحماية الإدارية للبيانات الشخصية من مخاطر التزييف العميق دراسة تحليلية مقارنة –

Administrative protection of personal data from the risks of deep fakes - Comparative analytical study -

م.م.هبة هاشم محمد الفتلاوي
كلية الطب – جامعة القادسية
hiba.hashim@qu.edu.iq
كلية الطب - جامعة القادسية
Hiba Hashim Mohammed
College of Medicine - University of Al-Qadisiyah

المستخلص في ظل التطورالمتسارع لتقنيات الذكاء الأصطناعي أصبحت بيانات ألافراد بمثابة وقود لتلك التقنيات والتي يعد التزييف العميق من أخطرها حيث يتم عن طريقها انشاء محتوى مُفبرك يحاكي الواقع بدقة متناهية حتى يصعب على الكثير التمييز بينما ماهوحقيقي و بين ماهووهمي مما يلحق الافراد من جراء ذلك أضرار بالغة تتعلق بمسائل كالتشهير والابتزاز والاحتيال ليمتد بعدها ليشمل المجتمع ككل مما يقوض الثقة المجتمعية بالهوية الرقمية ففي ظل هذه التهديدات بات التزييف العميق يمثل انتهاكا وجوديا للبيانات الشخصية، فمن خلاله يتم تسخير الشبكات التقنية من اجل انتهاك الحرمات عبر محتوى مزيف ليشوه الحقائق ،وامام هذه التحديات برزت الحماية الإدارية لتلك البيانات من مخاطر التقنيات العميقة ضرورة قانونية كمنهج متكامل يجمع ما بين ايجاد تشريع صارم وانشاء مؤسسات مختصة لحماية البيانات ومع الالتزام بالرقابة التقنية من جانب وفرض الجزاءات من قبل الجهات الادارية لضمان الامتثال والالتزام بقوانين الحماية من جانب اخر ليجسد مبدأ الاشتراك بمسؤولية حماية البيانات الشخصية مابين الجهات المعنية من حكومات ومؤسسات حتى يشمل الافراد عبر نشر ثقافة الوعي ومحو الامية الإعلامي والتثقيف بكيفية الحفاظ على بيانتهم الشخصية فمن خلال هذه الدراسه نسلط الضوء على اليات الحماية الإدارية التي تجمع ما بين الاطر الموضوعية والاجرائية من اجل سد الفجوة ما بين الثوره الرقمية وحق الفرد في حماية بياناته الشخصية ٠

الكلمات المفتاحية : الحماية الإدارية ، البيانات الشخصية ، التزييف العميق – مخاطر – الإجراءات التقنية

Abstract

In light of the rapid development of artificial intelligence technologies, individual data has become the fuel for these technologies, of which deep fakes are among the most dangerous. This is achieved by creating fabricated content that mimics reality with extreme accuracy, making it difficult for many to distinguish between what is real and what is fake. This causes significant harm to individuals, including defamation, blackmail, and fraud, which then extends to society as a whole, undermining societal trust

in digital identity. In light of these threats, deep fakes have become an existential violation of personal data. Through them, technical networks are exploited to violate privacy through fake content that distorts facts. In the face of these challenges, administrative protection of this data from the dangers of deep fakes has emerged as a legal necessity. This approach combines strict legislation and the establishment of specialized institutions to protect data, while adhering to technical oversight on the one hand and imposing penalties by administrative authorities to ensure compliance and adherence to protection laws on the other. This embodies the principle of shared responsibility for protecting personal data among relevant authorities, including governments and institutions, to include individuals by spreading a culture of awareness. And media literacy and education on how to protect their personal data. Through this study, we shed light on administrative protection mechanisms that combine objective and procedural frameworks in order to bridge the gap between the digital revolution and the individual's right to protect his personal data.

المقدمة // في ظل التطور التكنولوجي المتسارع الذي نعيشهُ في الوقت الحاضر شكّلت حماية البيانات الشخصية ركيزة أساسية لسيادة الدول ومدى تحقيقها للامن الرقمي واستقرار مجتمعاتها التي أصبحت تعتمد بصورة كبيرة على تقنيات الذكاء الاصطناعي في تسيير شؤونها حيث لا يمكن للفرد الاستغناء عن تلك التقنيات فالبريد الالكتروني وبطاقات التعريف ووسائل الدفع الالكتروني والتواصل لها من الاهمية الكبيرة في مختلف المجالات التي تعتمد في عملها بشكل أساسي على البيانات الشخصية للافراد ، حيث تشمل هذه البيانات كل ما يؤدي الى التعريف بالفرد او الوصول اليه كالأسم او الصوت او الصورة وغيرها من البيانات الصحية والحيوية (البيومترية) ومع تدفق الكم الهائل من البيانات برزت تحديات خطيرة نتيجة إساءة استخدام تلك التقنيات فأوجدت مخاطر غير مسبوقة والتي يعد التزييف العميق من ابرزها تلك التقنية التي تعمل على انشاء محتوى مزيف شديد الاقناع يصعب على الكثير التميز بين ماهو مفبرك وبين ماهو حقيقي عبر استغلال البيانات الشخصية التي تكون لها بمثابة وقود تتغذى عليه تلك التقنيات مما يلحق بالفرد اضرار بالغة تتعلق بتشويه السمعة والاحتيال والتشهير والابتزاز وبالتالي ينعكس على تقويض ثقة المجتمع بالهوية الرقمية ،ففي هذا السياق تبرز الحماية الإدارية ضروة ملحة كدرع وقائي يستبق تلك المخاطر عن طريق تبني استراتجيات متكاملة تجمع مابين إيجاد تشريع موحد ومؤسسات فاعلة والاليات تقنية متطورة لكشف تلك المخاطر فنسعى في هذا البحث الى تقديم دراسة شاملة لتعزيز الحماية الإدارية للبيانات الشخصية في مواجهة تقنيات التزييف العميق عبر استخلاص افضل التجارب في دول تمثل نماذج متباينة كالنموذج المصري والفرنسي تمهيدا لوضع نظام حماية البيانات إداريا في العراق وتنتهي بتشريعات رادعة عبرالكشف عن موطن القوة والضعف في سبيل مواجهة وباء التزييف العميق من اجل تحويل تلك البيانات من وقود للتزيف العميق الى ذخيرة للحقيقة في عصر باتت فيه حماية البيانات الشخصية للافراد يمثل جوهرالسيادة الرقمية لتلك الدول ٠

إشكالية البحث :- تنطلق إشكالية البحث من التساؤل حول مدى إمكانية الجهات الإدارية من توفير الحماية الازمة للبيانات الشخصية في ظل اتساع الفجوة بين التهديد الخطير من جراء إساءة استخدام تقنيات الذكاء الاصطناعي ولا

سيما تقنية التزييف العميق وبطء الاستجابة التشريعية والمؤسسية في وقت يتطلب مواجهة تلك المخاطر الى اليات استباقية متقدمة فبرزت صعوبات تتعلق بغياب الأطر القانونية والإدارية لحماية تلك البيانات من جانب ومواجهة مخاطر التزييف العميق من جانب اخر، حيث ان عدم وجود تشريع موحد لحماية البيانات اولمواجهة تقنيات التزييف العميق وعدم انشاء هيئات إدارية مختصة تسهر على احترام تنفيذ تلك القوانين قد زاد الامر تعقيدا مما جعل الإدارة في وضع لايسمح لها الاخذ بدورها وأصدار تشريعاتها التنظيمية او اتخاذ إجراءاتها التقنية فضلا عن عدم وجود ضمانات لممارسة تلك الجهات الإدارية من جزاءات تستطيع الإدارة فرضها على المخالف في سبيل ضمان التزامه بتطبيق تلك التشريعات ، حيث شكل هذا التحدي ثغرة تستحق الدراسة **واتضحت كأشكالية جوهرية جمعت بين الجانب القانوني والإداري والتقني مع دراسة مقارنة توضح فيها الاطار المتكامل لجهود حماية البيانات الشخصية من مخاطر التزيف العميق في بيئات تشريعية وإدارية مختلفة كالعراق ومصر وفرنسا ٠**

أهمية البحث تستمد أهمية بحثنا **للحماية الإدارية للبيانات الشخصية من مخاطر التزييف العميق** بما تمثله من ضمانة أساسية لحق الفرد في الحفاظ على بياناته من الاستغلال في الفضاء الرقمي وتعرضها لمخاطر التزييف العميق الذي يمثل انتهاكا صارخا يهدد الامن الفردي (بالانتحال والتشهير والابتزاز) والامن المجتمعي (بتقويض الثقة واثارة الرأي العام وتحقيق غايات إجرامية) وتظهر أهمية البحث في انه يجمع بين التحليل القانوني والتقني كأساليب متطورة لتوفيرالحماية الازمة للبيانات الشخصية كالتشفير والجدر النارية واستخدمات تقنيات بالكشف عن المحتوى المزيف التي تساهم في التصدي للاستخدامات الضارة للتزييف العميق واضافة الى السعي في تقديم دراسة مقارنة لأطر حماية بيانات الافراد إداريا وتشريعا والاستفادة من تجارب الدولة في حماية البيانات ومواجهات هذه التقنيات الخطرة مما يساعد على فهم نقاط القوة وتدارك نقاط الضعف كذلك يساهم البحث في نشرالثقافة ورفع الوعي بأهمية ضرورة حفاظ الفرد على بيانته وبخطورة هذه التقنيات التي تخلق محتوى يصعب تمييزه والذي ينعكس على إيجاد بيئة إدارية تستند الى نظم تشريعية رصينة سعيا لبناء فضاء رقمي يقوم على الثقة والمسؤولية ٠

منهجية البحث سنتبنى في هذا البحث الى اعتماد المنهج التحليلي القائم على تحليل النصوص القانونية ذات الصلة بموضوع بحثنا إضافة الى تحليل تقنية التزييف العميق والمنهج المقارن من اجل تتبع تجارب الدول في هذا المجال والوصول للاشكاليات في ذات الموضوع كونها صلب بحثنا تحديدا بما تمثله التجربة المصرية والفرنسية ولائحة الاتحاد الأوربي التي تعد نموذج رائد في هذا المجال إضافة الى المنهج الوصفي المعتمد على جمع المعلومات والحقائق من مصادر مختلفة تتعلق بحماية البيانات وتقنية التزييف العميق ٠

اهداف البحث يهدف البحث الى تسليط الضوء على موضوع حيوي وحديث يتعلق بمدى تأثير التزييف العميق على حماية البيانات الشخصية وضرورة إيجاد أساليب إدارية وقانونية لمواجهتها هذه التقنيات الخطرة مع بيان اثرها على الفرد والمجتمع واضافة الى البحث في اليات الحماية الإدارية ورصد الفجوات التشريعية التي انعكست على توفر الحماية الإدارية للبيانات الشخصية مع تقديم دراسة للسياسات المتبعة في حماية البيانات في الدول العربية مع بيان

موقف الدول الغربية التي تعد متقدمة بموضوع توفير الحماية إداريا وتشريعيا ومواجهة هذه التقنيات بهدف وضع اطار اداري متكامل ليجمع بين التشريع الرادع والرقابة المؤسسية فاعلة وتقنيات كاشفة للتزيف العميق ٠

خطة البحث انطلاقا من أهمية البحث ولغرض احتواء اشكاليته ارتأينا الى تقسيمه الى مبحثين وعلى النحو الاتي :تضمن المبحث الأول الاطار المفاهيمي للبيانات الشخصية و تقنية التزييف العميق الذي تضمن مطلبين تناول الأول التعريف بمفهوم التعريف البيانات الشخصية وصورها بينما تناول المطلب الثاني التعريف بمفهوم التزييف العميق واثاره على الفرد والمجتمع

اما المبحث الثاني خصص لدراسة اليات الحماية الإدارية لبيانات الشخصية من مخاطر التزييف العميق الذي تضمن مطلبين تناول الأول الحماية الموضوعية للبيانات الشخصية من التزييف العميق بينما خصص الثاني للحماية الإجرائية للبيانات الشخصية من تقنية التزييف العميق

المبحث الأول

الاطار المفاهيمي للبيانات الشخصية و تقنية التزييف العميق

يعتبر الحق في البيانات الشخصية من الحقوق اللصيقة للفرد فما لاشك فيه ان لكل فرد بياناته التي يفضل بقاءها طي الكتمان عن الاخرين وعدم افشاءها لما في ذلك حماية لأمنه او سمعته الى غيرذلك من الاعتبارات وتشمل البيانات الشخصية كل مايمكنه من تعريف الفرد او ربطه به من اسم او صورة الى بياناته الحيوية (البيومترية) او الصحية الى كل تفاصيل حياته الخاصة ٠

في ذات الوقت برزت تحديات جسيمة تهدد هذا الحق وسلامة هوية الفرد الرقمية وفي مقدمة تلك التحديات خطر داهم ومتطور بسرعة هائلة الا وهو التزييف العميق تلك التقنية التي طمست الخطوط الفاصلة بين ماهو حقيقي وماهو محاكى مزيف حيث تم استخدامها لألحاق إضرار جسيمة بالفرد وتعتمد هذه التقنية على الذكاء الاصطناعي التوليدي لتزييف بيانات الفرد من اجل انشاء فيديو او تزييف صورة او مقطع صوتي بحيث يصعب على الشخص العادي التعرف على المحتوى المزيف من الحقيقي ٠لذا نسعى من خلال هذا المبحث تقديم اطار مفاهيمي متكامل يربط بين مفهوم البيانات الشخصية وتقنية التزييف العميق نتطرق في المطلب الأول الى التعريف بمفهوم البيانات الشخصية وصورها وفي المطلب الثاني ننتطرق الى التعريف بمفهوم التزييف العميق واثر هذه التقنية على الفرد والمجتمع ٠

المطلب الأول

التعريف بمفهوم التعريف البيانات الشخصية وصورها

في ظل التحول الرقمي المتسارع برزت البيانات الشخصية أهميتها كونها الوقود الأساسي الذي تتغذى عليه تطبيقات الذكاء الاصطناعي ونظرا لهذه الأهمية يجعلها عرضة للتلاعب و التزييف وتحديداً في بيئة الانترنيت كون تداولها يكون بشكل سريع و دون رقابة كافية مما يستدعي فهما دقيقا للبيانات الشخصية وهذا مانتطرق اليه في الفرع الأول اما الفرع الثاني نستعرض أنواع هذه البيانات ٠

الفرع الأول

مفهوم البيانات الشخصية

لم تكن التشريعات تهتم لموضوعات الخصوصية و حماية بيانات الشخص كما هو في الوقت الحالي فقد اختلف مفهوم البيانات الشخصية باختلاف القوانين الدول المنظمة لها ،حيث يعد مفهوم البيانات الشخصية من الحقوق المرتبطة ارتباط وثيق بحق الخصوصية كما له الدور الأساس في ممارسة الشخص لبقية حقوقه الأخرى كالحق في المساواة و الحق في ابداء الرأي و غيرها من الحقوق ،فقد عرفها المشرع الفرنسي بأنها (أي معلومات تتعلق بشخص طبيعي محدد أو يمكن التعرف عليه بشكل مباشر أو غير مباشر بالإشارة الى رقم التعريفي أو الى نص اخر خاص به) [١]م (٢)من القانون الوطني الفرنسي رقم (٧٨-١٧) الصادر في ٦ يناير ١٩٧٨ (قانون المعلوماتية والحريات) فضلا عن (GDPR) هو مختصر اللائحة الاوربية لحماية البيانات الشخصية المعروفة باسم General Data Protection requlation (التي تعد تشريع اوربي في مجال حماية البيانات الشخصية للأفراد داخل الاتحاد الأوربي (EU) والتي حددت عام ٢٠١٦ وأصبحت نافذة المفعول عام ٢٠١٨ حيث عرف البيانات الشخصية في المادة الرابعة من اللائحة الاوربية (GDPR) [٢]، بأنها أي معلومات تتعلق بالشخص الطبيعي معرف او يمكن تحديد هويتهِ (صاحب البيانات) بشكل مباشر أو غير مباشر و بذلك لم تختلف مفهوم البيانات الشخصية فيها كثيراً عما ورد في التوجيه الأوربي لحماية البيانات الشخصية (EC/95/46)[٣] ،أما المشرع المصري فقد تناول مفهوم (البيانات الشخصية) بأنها أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات واي بيانات أخرى كالاسم أو الصورة أو الصوت أو الرقم التعريفي أو محدد لهوية عبر الانترنت أو أي بيانات تحدد الهوية النفسية او الصحية او الاقتصادية او الثقافية او الاجتماعية [٤]،كما عرفت البيانات الشخصية وذلك حسب ما جاءت بهِ منظمة التعاون الاقتصادي و التنمية بأنها (كل معلومة عائدة لشخص طبيعي معرف أو قابل للتعرف) فهي كل معلومات تتعلق بشخص معين وتؤدي الى تحديد هويتهِ و التعرف عليه [٥]. وبناء على ما تقدم يعد بياناً شخصياً ويخضع للحماية القانونية كل بيان يرتبط بالشخص و يساعد على التعرف على هويته كأسمهِ و لقبه و عنوانه و معلوماته الاسرية وجنسيته ، ويترتب عليه أن البيانات الشخصية هي كل يتوافق مع المعلومات سواء كانت هذه المعلومات عامة أو خاصة أو مهنية أو غيرها تؤدي الى التعرف على الشخص المعني .

---

[١] م (٢) من الائحة العامة لحمايات البيانات ، ترجمة د. مصطفى عبيد ،الاتحاد الأوربي(البرلمان الأوربي والمفوضية الاوربية) اللائحة العامة لحماية البيانات ، موسوعة العلوم القانونية ، مركز البحوث والدراسات متعددة التخصصات ، الطبعة الأولى ، ٢٠١٨ ، ص٤ .

[٢] GDPR تشريع اوربي في مجال حماية البيانات الشخصية للأفراد داخل الاتحاد الأوربي (EU) و التي حددت عام ٢٠١٦ وأصبحت نافذة المفعول عام ٢٠١٨ .

[٣] يعد التوجيه الأوربي لحماية البيانات الشخصية التشريع الذي وضع الأساس لعدة قوانين منها اللائحة الاوربية لعام ٢٠١٨ حيث أدى التطور التكنلوجي الحاجة الى صدور تشريعات جديدة لتعزيز الحماية و فرض العقوبات اقسى على الانتهاكات .

[٤] المادة الأولى (١) من الفصل الأول (التعريفات) من قانون حماية البيانات الشخصية رقم (١٥١ لسنة ٢٠٢٠) .

[٥] منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت، ٢٠١٦، ص ١٠٠ .

الفرع الثاني

أنواع البيانات الشخصية

تصنفت البيانات الشخصية وذلك حسب أهميتها الى :-

أولا / البيانات الشخصية العامة (الغير الحساسة) وهي مجموعة من المعلومات التي بالإمكان الوصول اليها ولا تتطلب مستوى عالي من الحماية ،فهي بيانات تسمح بتحديد هوية الشخص و تميزه عن الغير منها على سبيل المثال (الاسم و تاريخ البطاقة ورقم الهاتف و عنوان البريد الالكتروني)[١] وكذلك من قبيل البيانات الشخصية الحالة الاجتماعية لشخص كونه متزوج أو اعزب أو مطلق ،وكذلك الحال بالنسبة لعنوان منزل الشخص الذي يقيم فيه أو عنوان عملهِ[٢] **وهنا نتساءل عما اذا كان الصوت و الصورة للشخص يتم اعتبارها بياناً شخصياً؟**اعتبرت اللجنة القومية للحريات في فرنسا ان صورة الشخص الطبيعي سواء كانت ثابتة أم متغيرة بياناً شخصياً يخضع للحماية القانونية مستندة بذلك الى ان التكنولوجيا الحديثة قد سمحت بإدخال تعديلات ومعالجات للصوت والصورة ووضعهم بمستوى واحد الى جانب النص مما يؤدي الى معالجتها بصورة منفصلة بالتالي يمكن جعلها بيانات شخصية يوجب توفير الحماية لها ومما لا شك فيه ان اعتبار صوت الانسان و صورتهِ بيان شخصي هو مفهوم حديث للبيانات الشخصية ، ففكرة البيانات الشخصية كانت مقتصرة والى وقت قريب على الاسم و اللقب و العمر و العمل الوظيفي وهذا ما ذهب اليه التوجيه الأوربي الخاص بحماية البيانات الشخصية الصادر عام ١٩٩٥[٣]،فصورة الشخص تتمتع بحماية قانونية باعتبارها ان الحق في الصورة من مظاهر الحق في الحقوقية[٤]،ونحن نؤيد ما ذهب اليه التوجه الحديث باعتبار كلا من الصوت و الصورة بيان شخصي كون ان تطبيقات الذكاء الاصطناعي و برامج الحاسوب قد سمحت بالمعالجة كل منهما بإضافة نص الى صورة او صوت الى نص معين فكل ذلك يؤدي الى اعتبارها من البيانات الشخصية التي بالإمكان ادخال معالجة عليها وبالتالي تكون عرضه للتلاعب والتزييف

ثانيا /البيانات الحساسة وهي صورة من صور البيانات التي ينتج عن معالجتها اثار وأضرار بالغة اذا ما تم مقارنتها بالبيانات الغير حساسة [٥]وذلك لأهميتها البالغة ولأرتباطها بالكشف عن اصل الفرد و معتقداتهِ و توجيهاتهِ السياسية و معلوماتهِ الطبية وهو ما يشكل خطورة على حياة الفرد وحقوقهِ وحرياته الاساسية لهذه الأسباب عمدت اكثر الدول عند

---

[١] بن شهب أسماء ، كلية الحقوق ، حماية البيانات الشخصية للمستخدم في اطار عقود الحوسبة الحسابية ، بحث منشور مجلة الفكر القانوني السياسي ، جامعة الاخوة منتوري – قسطنطينية ، المجلد التاسع ، العدد الأول ، ٢٠٢٥ ، ص ٣٠٢ .

[٢] Joëlle BEDEREDE,Données personnelles dans le cadre dun sit we ,étude disponible sur ,la date de mise en ligne ,2003,p 32

[٣] د. سامح عبد الواحد التهامي ، الحماية القانونية للبيانات الشخصية دراسة في القانون الفرنسي (القسم الأول) بحث منشور ، كلية الحقوق ،جامعة الزقازيق ٢٠١٠ ، ص ٣٩٠ .

[٤] حسام الدين الاهواني ، الحق في الخصوصية (دراسة مقارنة) ، دار النهضة العربية ، دون سنة نشر ، ص ٧٦ .

[٥] سمير سعد رشاد سلطان ، الحماية القانونية للبيانات الحساسة في مجال الاستدلال (دراسة مقارنة) ، بحث منشور ،مجلة البحوث القانونية و الاقتصادية ، عدد ٨٨ ، يونيو ٢٠٢٤ ، ص ١٠٤٣ .

تنظيمها للتشريعات المتعلقة بحماية البيانات الشخصية الى تحديد البيانات الحساسة بقائمة على سبيل الحصر لا المثال عند أدراجها لتلك البيانات ، فقد حدد كلاً المشرع الفرنسي و المصري تلك البيانات على سبيل الحصر ، وقد عرف المشرع المصري البيانات الحساسة بكونها البيانات التي تفصح عن الصحة النفسية و العقلية و البدنية او الجينية او البيانات القياسات الحيوية البايومترية او البيانات المالية او المعتقدات الدينية او الآراء السياسية او الحالة الأمنية وفي جميع الأحوال تعد بيانات الاطفال من البيانات الشخصية الحساسة [١] ،كما عرفتها اللائحة العامة الاوربية بكونها البيانات المتعلقة بالبيانات الشخصية التي تكشف عن الأصل العرقي او الاثني او الآراء السياسية او المعتقدات الدينية او الفلسفية او عضوية النقابات العمالية و معالجة البيانات الجينية و البيانات البايومترية لغرض تحديد هوية الشخص الطبيعي بشكل فردي او البيانات المتعلقة بالصحة او المتعلقة بالتوجه الجنسي للشخص الطبيعي [٢] ،اما المشرع الفرنسي فقد حدد البيانات الشخصية الحساسة بموجب المادة (٨ من القانون رقم ٧٨ – ١٧ لعام ١٩٧٨) المعروف باسم قانون المعلوماتية والحريات الفرنسي حيث ورد هذا التحديد بعد التعديلات التي أدخلت على القانون بموجب قانون رقم (٨٠١ – ٢٠٠٤) الصادر في ٢٠٠٤ الذي تماشى مع التوجيه الأوربي (٩٥/٤٦) حيث نصت المادة (٨) (يحظر معالجة البيانات التي تكشف عن الأحوال العرقية او الاثنية او الآراء السياسية او الفلسفية او الدينية او الانتماءات النقابية او الصحة او الحياة الجنسية او البيانات الجينية او البايومترية) [٣] ،وقد اتجهت تلك اللائحة الى وضع تعريفات لتلك المصطلحات فقد عرفت البيانات الصحية بانها كل البيانات المتعلقة بالصحة الجسدية او العقلية للشخص الطبيعي بما في ذلك تقديم خدمات الرعاية الصحية و التي تكشف عن معلومات حول حالته الصحية [٤] ،اما البيانات الجينية عرفت بانها كل ما يتعلق بالخصائص الجينية الموروثة او المكتسبة للشخص الطبيعي و التي تعطي معلومات فريدة من فسيلوجيا او صحة ذلك الشخص الطبيعي و التي تنتج على وجه الخصوص من تحليل عينة بيولوجية من الشخص المعني فهي بيانات حساسة يجب ان تتمتع بوضع قانوني خاص [٥] .

[١] المادة الأولى من قانون رقم (١٥١ لسنة ٢٠٢٠) قانون حماية البيانات الشخصية .

[٢] سمير سعد رشاد سلطان ، مصدر سابق ، ص ١٠٥٧

[٣] بقيت المادة (٨) نافذة بعد تطبيق اللائحة الاوربي ٢٠١٨ كتعريف للبيانات الحساسة ، يشمل البيانات البايومترية و الجينية بشكل صريح .

[٤] م (١٥) من الائحة العامة لحمايات البيانات ،ترجمة د.مصطفى عبيد ،الاتحاد الأوربي(البرلمان الأوربي والمفوضية الاوربية) اللائحة العامة لحماية البيانات ، مصدر سابق ،ص ٧ .

[٥] د. طارق جمعة السيد راشد ، الحماية القانونية للحق في خصوصية البيانات الجينية (دراسة تحليلية مقارنة)، بحث منشورفي المجلة القانونية ، كلية الحقوق ، جامعة القاهرة ، العدد ١٢ / مجلد ٨ ، لسنة ٢٠٢٠ ، ص ٣٩١٠ .

اما البيانات القياسات الحيوية (البايومترية) فتعد بيانات ناتجة عن معالجة تقنية محددة تتعلق بالخصائص الجسدية او الفسيولوجية او السلوكية للشخص الطبيعي و التي تسمح او تؤكد تحديد هويته بشكل فردي مثل شكل الوجه و بصمة الاصبع [١] ٠

وحسننا فعل المشرع الأوربي بموجب اللائحة المعتمدة في فرنسا عند وضعهِ التعريفات المحددة لدقة تلك المصطلحات الفنية و التي تتطلب تعريفا واضحاً و محدد لبعض البيانات التي جاءت في قائمة البيانات الحساسة ،وهذا على خلاف المشرع المصري الذي لم يضع تعريف محدد للمصطلحات المحددة تحت مفهوم البيانات الحساسة ٠

المطلب الثاني

التعريف بمفهوم التزييف العميق واثاره على الفرد والمجتمع

تعد تقنية التزييف العميق أحدى أهم تقنيات الذكاء الاصطناعي التي شهدت تطوراً متسارعاً في الوقت الحاضر و التي تعتبر من التحديات التي تواجه حماية البيانات الشخصية ،فهذه التقنية هي نتاج احد تطبيقات الذكاء الاصطناعي التي استخدمت لأنشاء محتوى مزيف شديد الاقناع بتزييف الصوت والصورة مستغلة بذلك البيانات الشخصية للأفراد دون علمهم لتحولها الى سلاح رقمي تم تطويره للاحتيال والتشهير بالأشخاص وتقويض الثقة المجتمعية لذا يتطلب لفهم هذه التقنية الى تقسيم المطلب الى فرعين نتطرق الى مفهوم التزييف العميق ومعرفه اساليبه ضمن الفرع الأول منه ونتطرق في الفرع الثاني الى اثر تزييف البيانات الشخصية على الفرد والمجتمع

الفرع الأول

مفهوم التزييف العميق و أنواع المحتوى المزيف

يعتبر التزيف العميق من احد تقنيات الذكاء الاصطناعي وظهرت لأول مرة في ا عام ٢٠١٧ عندما نشر احد مطوري برامج الانترنت موهبته عندما قام بتبديل وجوه المشاهير لهوليود على وجوه فنانين لأفلام اباحية [٢]وأن مصطلح التزييف العميق من كلمتين الأولى deep بمعنى العميق و fake و معنى التزييف ،فالاول يشير الى احدى برنامج الذكاء الاصطناعي (نموذج التعلم العميق) Learng Deep Model و الثاني هو تزيف الحقائق و الوقائع٠

وقد عرف برلمان الاتحاد الأوربي بموجب المادة (٦٠) من قانون الذكاء الاصطناعي (عبارة عن محتوى صوت او صورة او فيديو الذي تم انشائه او التلاعب به بواسطة الذكاء الاصطناعي والذي يشبه الأشخاص او الأشياء او

[١] م (١٤) من الائحة العامة لحمايات البيانات ،ترجمة د٠مصطفى عبيد ،الاتحاد الأوربي(البرلمان الأوربي والمفوضية الاوربية) اللائحة العامة لحماية البيانات ، مصدر سابق ،ص ٦

[٢] د٠ باسم محمد فاضل ،التحديات القانونية لتقنية التزييف العميق (deep fake) ، دراسة تحليلة مقارنة ، الطبعة الأولى ، دار الفكر الجامعي ، مصر ، ٢٠٢٥ص ٢٦

الأماكن او الكيانات او الاحداث الموجودة ويبدو بشكل زائف للشخص على انه اصلي او حقيقي) [١] كما يرى جانب من الفقه الفرنسي ان التزييف العميق يعتمد على استخدام برامج الذكاء الاصطناعي لتزييف الوجه و محتوى الصوت و الفيديو ذلك بإنتاج مقاطع فيدوية مزيفة بأستخدام تقنية التزييف العميق [٢] ٠

وقد عرفه البعض بأنهُ (الفيديو المنتج من خورزميات التعلم العيمق من خلال برامج متاحة يسهل الوصول اليها تتمتع بالقدرة على انتاج وتقديم محتوى محرف يخالف الحقيقة من خلال وضع وجعه شخص مستهدف فوق جسد شخص اخر بدون تمييز) [٣]

وبعد عرض التعريفات نلاحظ تركيزها على الجانب التقني الفني، و بالتالي من الضروري نحتاج الى تعريف قانوني ليبين طبيعة هذه التقنية و يميزها عن غيرها من التقنيات الذكاء الاصطناعي ٠

فقد عرفه البعض (بأنه عبارة عن نسخة متطرفة ملفقة و همية من البيانات السمعية و البصرية التي قد تم التلاعب بها من خلال احدى تطبيقات الذكاء الاصطناعي المعدة لذلك و الذي يقصد في جوهره التقول على شخص بشيء لم يقلهُ بواسطة تقنيات تكنلوجية حديثة [٤] ٠

ويرى الباحث ان التزييف العميق هي احدى تقنيات الذكاء الاصطناعي التي تقوم على أساس انشاء محتوى مزيف رقمي من صور او صوت او فيديو أو كيلهما لشخص او حتى النصوص تحاكي الواقع و تخالف الحقائق ويصعب تمييزها تستخدم لأغراض غير مشروعة بقصد الاضرار بالافراد ٠

ان التكنلوجيا التي تقف وراء انشاء مقاطع مزيفة تتمثل من خلال استخدام تقنيتين الأولى تتمثل بي **تقنية التعلم الالي العميق** وذلك من خلال تغذيتها بمحتوى واسع جداً من الصور و مقاطع الفيديو و الأصوات ، حيث تقوم النظم عبر خوارزميات ذكية بتغيير به وجوه الأشخاص واصواتهم او عمل محاكاة لهم تبدو كأنها واقعية لكنها غير حقيقية على الاطلاق وذلك من خلال شبكة التعليم العميق [٥] ،و التقنية الأخرى (GAN) **شبكة الخصومة التوليدي** Generative Adversarial Net work والتي تنتج من استخدام شبكتين تكملان بعضهما البعض من خلال التنافس بينهما ،الأولى **شبكة المولد** التي تعتمد في عملها على توليد صور و أصوات و بيانات واقعية فتكون اكثر

---

[١] التطورات والتحيلات الحديثة لقانون الذكاء الاصطناعي للاتحاد الأوربي منشور على الموقع الالكتروني /مقال منشور على الموقع الالكتروني https://artificialintelligenceact.eu/article/3/ تم زيارة الموقع ٢٠٢٥/٦/١٥

[2] ٠Mariëtte van Huijstee, pieter van Boheemen,Djurre Das and etai,Tackling deepfakes in Eurpean policy,panel For the Future of science and techlingdeepfakes in Eurpean parliamentary Research Service,SCIENTIFIC Foresight unit (STOA),PE690.039-July ,2021.p.2

[٣] مكافحة التزيف العميق /تقنية البلوك تشين كدلل على صحة الوسائط الرقمية مقال منشور على الموقع الالكتروني https://www.researchgate.net/publication/348467461_Combating_Deepfakes_Multi-LSTM_and_Blockchain_as_Proof_of_Authenticity_for_Digital_Media تم زيارة الموقع ٢٠٢٥/٦/٢٠

[٤] د ٠ محمود سلامة عبد المنعم الشريف ، جريمة الاباحي عبر تقنية التزييف العميق و المسؤولية الجنائية عنها ، بحث منشور في المجلة العلمية لبحوث الصحافة ، جامعة القاهرة ، كلية الاعلام ، العدد ٢٤ ، الجزء الثالث ، يوليو ٢٠٢٢ م ، ص ٣٦٩ ٠

[٥] احمد حازم مصطفى ، تقنية المعلومات ، هيئة المعرفة و التنمية البشرية ، دبي ، ٢٠١٥ ، ص ١٨ ٠

اقناعاً للواقع بالاعتماد على الذكاء الاصطناعي التوليدي ،اما الشبكة الثانية هي Discim inator Network **شبكة التمييز** حيث تعمل هذه الشبكة على التمييز بين البيانات الحقيقية و المزيفة المنتجة من قبل الشبكة التوليدية فيزداد معدل التمييز و التنبؤ الصحيح ويتم انتاج صور اكثر واقعية ويعتمد هذا التنافس بين الشبكتين وصولاً الى خلق محتوى من قبل شبكة المولد يصعب تميزه عن الحقيقة فهذه الشبكة (GAN) تستخدم في صناعة محتوى زائف من ملفات و صور و صوت و فيديوات يصعب تمييزها لدى الأشخاص الذين ليس لهم دراية واسعة بالتكنلوجيا لكن في الوقت الحاضر تم الاستعانة ب بعض التطبيقات التي يمكن ربطها على الهواتف الذكية والتي يمكن من خلال انشاء محتويات مزيفة باستخدام تطبيقات عميقة مثل(Face Mag , face APP)وما الى ذلك [١] ٠

ثانيا / أساليب التزييف العميق

تختلف أساليب تقنية التزييف العميق بأختلاف المحتوى المستخدم والتي منها /

١ – تقنية تزييف الفيديوهات او الصور تتم بإدخال الفيديوهات بدرجة عالية من الدقة واستخدام معين لتكنلوجيا بالإضافة الى توفر الوقت والامدادات المالية [٢]وتستخدم هذه التقنية في انتاج الصور او مقاطع الفيديووذلك بتبديل الوجه او تركيب وجه شخص اخر بعد استخدام خوارزميات التشفير او خوارزميات فك التشفير كالتلاعب بالوجه و تغيير التعابير او مطابقة الشفاه باستخدام خوارزمية التوليد و خوارزمية التمييز [٣] ٠

٢ – تقنية تزييف الأصوات / ويقصد بها تركيب الصوت او تعديله وذلك بإنتاج تسجيل مزيف لشخص يتضمن الحديث عن موضوع معين بصوت نفس الشخص غير انه لم يقوم ذلك في حقيقة الامر او تعديل ذلك الصوت عن طريق التلاعب و التحكم في بنبرة الصوت بحيث يغير من حالة الشخص او شعوره عند نشر الصوت المزيف كان يظهر الشخص في حالة السكر او الحزن [٤] ٠

٣ – تقنية تزييف النصوص / ويتم ذلك باستخدام نماذج اللغة الموجودة بأجهزة الحاسوب لغرض انشاء نصوص مختلفة وهي التي يمكن ان تستغل من اجل عمل دعاية معينة ، كما يمكن للنصوص المزيفة المولدة لتحقيق نفس

[١] سحر فؤاد مجيد االنجار ، المواجهة الجنائية للجرائم الناشئة عن استخدام التزييف العميق ، بحث منشور ، مجلة العلوم القانونية ، جامعة بغداد ،كلية القانون ، المجلد ٣٩ ، العدد الثاني ، ٢٠٢٤ ، ص ٥٨١ ٠

[٢] د٠ سامح محمد محمد السيد إبراهيم ، المخاطر الأمنية و المجتمعية للتزييف العميق و اليات المواجهة ، بحث منشور ، المجلة القانونية (ISSN 2537-0758)، جامعة نايف للعلوم الأمنية ، ص ٣٩٧١ ٠

[٣] د٠ رباب مصطفى عبد المنعم الحكيم ، الجوانب القانونية للتزييف العميق ، بحث منشور ، مجلة البحوث الفقهية و القانونية ، العدد ٤٨ ، اصدار يناير ، ٢٠٢٥ ، ص ٢٦٨٢ ٠

[٤] دليل التزييف العميق ، الصادر من برنامج الوطني للذكاء الاصطناعي ، الامارات العربية المتحدة ، يوليو ٢٠٢١ ، ص ١٠ ٠

الغايات على وسائل التواصل الاجتماعي او التلاعب ببيانات محرك البحث على الانترنت التي تحوي على اخبار مزيفة تطغي على الحقيقة لموضوع او قصة معينة ينظر اليها انا تلحق ضرر او احراج بالخصم [١] ٠

الفرع الثاني

اثر تزييف البيانات الشخصية على الفرد والمجتمع

لا يمكن أنكار الاثار الإيجابية العديدة لأستخدام التكنولوجيا فالسبب ليس بتلك التقنيات وانما بأساءة استخدمها ،حيث يعتبر تداول البيانات الشخصية من صور و صوت و نصوص و فيديوهات و اتاحتها و مشاركتها ارض خصبة للأشخاص للذي يريدون إساءة استخدامها و الحاق ضرر بأصحابها حيث يقوم الشخص المسيء عبر تقنية التزييف العميق بدمج تلك البيانات التي حصل عليها بإنتاج فيديو و صور و تسجيلات جديدة مزيفة تخالف الحقيقة في المحتوى و الموضوع وبعدها يقوم بمشاركة تلك البيانات المزيفة مع الاخرين ، فمصدر الخطر يكمن في توظيفها لأغراض غير مشروعة ،فيكون ذلك الضرر على المستوى الفردي و المستوى الاجتماعي ، فعلى المستوى الفردي من الممكن توظيف هذه التقنية لغرض تشوية سمعة الافراد واثارة النعرات الطائفية و بث الفتنة وكذلك مما يتسبب للفرد بأضرار نفسية بالغة حيث تستخدم المقاطع و الصور المزيفة للتشهيرأوالتنمر او الترهيب[٢] مما يمنح المسيء سلطة على الفرد من اجل دفع مبالغ او تنفيذ ما يطلبه منه من تعليمات وهذه التقنية تفتح امام المسيء الأبواب وتمنحُ العديد من الفرص التي تمكنهُ من تنفيذ مآربه سواء من اجل الانتقام او ابعاد الضحية عن المنافسة او فرص النجاح في الوصول لأهدافه المشروعة وبالتالي الحاق الضرر بالضحية من جراء استخدام التزييف العميق حيث تؤدي الى ضياع او تدمير العلاقة بين الأزواج او الإساءة الى سمعة الشخص او ابتعاد الناس عنه او التعامل معهُ وقد يفقد فرص الترقية او العمل وغيرها من الاثار التي لا يمكن إصلاحها حتى بعد اكتشاف البيانات المزيفة ،إضافة الى تشويه سمعة الفرد يستخدم بعض ضعاف النفوس تقنية التزييف بقصد الابتزاز للحصول على منافع مادية او معنوية [٣] كذلك تستخدم هذه التقنية لصناعة فيدويات للانتقام من بعض الأشخاص او الشريك الاخر و التي تعرف بأسم الانتقام الاباحي وهي جرائم عنف جنسي عبر الانترنيت و يقصد بها نشر صور عارية او مقاطع فيديو جنسية لشخص ما بشكل صريح على الانترنت عادة ما تتم عن طريق شريك جنسي سابق دون موافقة الشخص المعني من اجل ان تسبب لهُ في الضيق و الحرج ، ويعتبر الانتقام الاباحي من أوسع وجوه استغلال تقنية التزييف العميق و

---

[١] سالي يوسف ، كيف نواجة استخدام الذكاء الاصطناعي في التضليل المعلوماتي (استخدام تقنية deep fake لتزييف الفيديوهات)، مقال منشورفي موقع مركز المستقبل للأبحاث و الدراسات المقدمة ، القاهرة ، ٢٠٢٢ ٠https://futureuae.com/ar-AE/Mainpage/Item تاريخ زيارة الموقع ٢٠٢٥/٦/٢٤

[٢] احمد محمد البوشي ، الابتزاز الالكتروني مفهوم جديد في جرائم التهديد المعلوماتية ، دراسة تفصيلية في ضوء قانون العقوبات و قانون مكافحة جرائم تقنية المعلومات رقم ٧٥ لسنة ٢٠١٨ ، دار النهضة العربية ، ٢٠٢٢ ، ص ٢٣

[٣] علاء الدين منصور مغايرة ، جرائم الذكاء الاصطناعي وسبل مواجهتها ، جرائم التزييف العميق نموذجاً ، بحث منشور ، المجلة الدولية للقانون ، جامعة قطر ، المجلد ١٣ / العدد المنتظم الثاني ،٢٠٢٤ ، ص ١٣٦ ٠

يبين تقرير صادر عن المؤسسة الهولندية عام ٢٠١٩ الذي ورد فيه ان اجمالي الفيديويات المزيفة التي عثر عليها خلال عام ٢٠١٨ و أكتوبر ٢٠١٩ هو ١٤٦٧٨ فيديو و تشكل ٩٦% من هذه الفيديوهات اباحية مما يؤكد مدى انتشار هذا النوع من استخدام التقنية و الخطورة الكامنة وراءها ، ومن امثلة ذلك مما دفع الفتاة المصرية الى الانتحار نتيجة قيام احد المجرمين بنشر مقطع اباحي على مواقع التواصل الاجتماعي عام ٢٠٢٢ [١] .

هذا وتستعمل تقنية التزييف العميق بقصد الحاق الضرر بالفرد وذلك عن طريق الاحتيال ، حيث تسمح وسائل التواصل الحديثة من خلال استخدام المواقع الالكترونية كالبيع او الشراء البضائع و عرض الخدمات و المعلومات عن طريقها حيث تعرض تلك السلع في الفضاء الرقمي و بسبب ذلك يتم تبادل بيانات شخصية التي تكون على قدر كبير من الأهمية او بيانات حساسة كوسائل الدفع الالكتروني التي تعتبر المصدر الأخطر نتيجة حركة التعامل المالي عن طريقها يقابل ذلك تهديد لسرعة تلك البيانات الامر الذي يعرض الفرد المتعامل ليصرح ببياناتهِ الشخصية و التي يتم تداولها بين الوسطاء بشكل يسمح الاستيلاء عليها لغرض اجرامي [٢].اما على المستوى الاجتماعي فأن التزييف العميق للبيانات الشخصية يؤدي الى زعزعه الثقة في وسائل الاعلام والمصادر الرسمية ويؤثر على الرأي العام والقرارات السياسية وذلك نتيجه نشر معلومات مضللة عن الناس وتصريحات كاذبة وتعد من امثلة هذه التقنية المزيفة ما نشر من فيديو ذو محتوى مزيف للرئيس الاوكراني فولوديمرزينلسكي عام ٢٠٢٢ وهو يأمر جنوده بالقاء الاسلحة والاستسلام في القتال ضد الغزو الروسي وبعدها نفت الحكومة الاوكرانية ببيان رسمي حذرت فيها الجنود من الفيديوهات المفبركة بتقنية التزييف العميق[٣] كذلك ما ينشر من تسجيلات وفيديوهات بتلك التقنية كان يتضمن مشاهد اعتداء الشرطة على المواطنين بقصد احداث تاثير على الرأي العام ونشوب تظاهرات وشغب وتعدي على الاموال العامة [٤] هذا وان هذه التقنية تعد مصدر قلق على القطاعات الحكومية والاقتصادية التي تعتمد في انظمتها على البيانات البيومترية نتيجه اختراق التزييف العميق للبصمات البيومترية للافراد كتطبيقات التزييف العميق للوجه [٥] ، وهذا ما نراه في الوقت الحاضر من فيديوهات وتسجيلات لأشخاص متوفين منذ سنوات كذلك من اثار البيانات المزيفة على المستوى الاجتماعي هو تقويض الثقة والتشكيك في المصداقية لان عدم قدره الفردعلى التفرقة بين البيانات المزيفة والحقيقية والاشاعة والواقع يؤدي الى احداث جدل داخل المجتمع بسبب انتشار تلك الفيديوهات والتي

---

[١] احمد عبد الموجود زكير ، جريمة التزييف الاباحي ، دراسة مقارنة ، بحث منشور ، المجلة القانونية ،كلية الحقوق، جامعة القاهرة ، فرع الخرطوم ، مجلد ١١ ، عدد٧ ، ٢٠٢٢ ، ص ٢٢٣٤ .

[٢] صبرية جدي ، الحماية القانونية للحق في الخصوصية المعلوماتية ، بحث منشور ، مجلة التواصل في الاقتصاد و الإدارة و القانون ، كلية الحقوق و العلوم السياسية ، جامعة باجي مختار ، عنابة ، المجلد ٢٤ ، العدد ٢ ، اوت ٢٠١٨ ، ص ٦ .

[٣] د٠ محمود سلامة عبد المنعم ، مصدر سابق ، ص ٣٧٠ .

[٤] د٠ ولاء محمد محروس الناغي / د٠ ياسر محمود الناغي ، ادراك مستخدمي التواصل الاجتماعي لتهديدات التزييف العميق وعلاقته باستخدام الامن لتلك المواقع ، بحث منشور ، المجلة العلمية لبحوث الصحافة ، كلية الاعلام ، جامعة القاهرة ، العدد ٢٤ ، الجزء الثالث ، يوليو ، ٢٠٢٢، ص ٣٣٩ .

[٥] د٠ سامح محمد محمد السيد ، مصدر سابق ، ص ٣٩٧٤ .

تكون عادة على شكل معلومات بالمواقع الالكترونية وبالتالي فقدان الثقة في جميع ما ينشر لانه لا يوجد طرق يمكن للفرد من خلالها معرفه مدى صحه الخبر او الفيديو المتلاعب به[١] ، اضف الى ذلك من الاثار الاجتماعيه لتزييف العميق هو استغلال البيانات الشخصية لأغراض اجرامية فقد تستخدم تلك البيانات المزيفة والمسروقة في التخطيط للجرائم والتمويل في المجتمع مما يهدد الامن العام مثالها التلاعب بأدلة الاثبات الرقمية في القانون الجنائي وذلك بأظهار شخص يقتل غيره أويسرق امواله او ان يسب او يشتم وغيرها من الافعال الاجرامية في حين انه لم يرتكبها و انما قام به غيره وذلك بتزييف صوره وفيديواته وتركيب وجه بدل وجه الجاني فيظهر وكأنه ارتكب الفعل الاجرامي[٢] ٠

ومن هنا يتبين اثر البيانات المزيفة على الفرد و المجتمع نتيجة إساءة استخدام تكنولوجيا المعلومات على الرغم من الاعتماد و قواعد البيانات إضافة الى الاعتماد على البيانات الحساسة كما هو الحال في جواز السفر الالكتروني البيومتري و في كثير من النشاطات كالتجارة الالكترونية و الدفع الالكتروني و التصفح على الأنتر نت و تقنيات التتبع و المراقبة التي تقوم بها الكامرات التي باتت أداة مهمة لتحقيق الامن و الرصد لكثير من الجرائم مما يدفعنا الى التساؤل حول ما مدى توفر الحماية لتلك البيانات و تأمينها رغم أهميتها و لسهولة تداولها و نقلها الذي لا يتجاوز بضع الثواني من جهة و مساسها بخصوصية الفرد وبياناته من جهة أخرى هذا ما نحاول ان نبينه في المبحث الثاني

المبحث الثاني

اليات الحماية الإدارية لبيانات الشخصية من مخاطر التزييف العميق

باتت حماية البيانات الشخصية في العصر الحالي من اهم الأصول التي تستوجب توفير الحماية لها نظراً لسهولة تلفها و تعديلها عبر الوسائل التقنية الا ان هذه الحماية تتطلب نهجاً شاملاً يجمع ما بين مجموعة من الاليات القانونية و التدابير الإدارية و الإجراءات الفنية و التقنية في سبيل تحقيق تلك الحماية من اجل الوقوف على الاليات الحماية الإدارية للبيانات الشخصية من تقنية التزييف العميق ٠ نتناول في المطلب الأول منهَ الحماية الموضوعية للبيانات الشخصية من مخاطر التزييف العميق ، بينما نتطرق في المطلب الثاني الى الحماية الاجرائية للبيانات الشخصية ٠

المطلب الأول

الحماية الموضوعية للبيانات الشخصية من التزييف العميق

من اجل توفير حماية متكاملة تعتمدها الجهات الإدارية المعنية بذلك نبغي ان تستند حماية أنظمة الهوية الشخصية الى اطر قانونية تحمي بيانات الأشخاص و خصوصيتهم و حقوقهم من اخطر التهديدات التقنية وعلى رأسها التزييف

[١] د٠ رضا إبراهيم عبد الله البيومي ، الحماية القانونية من مخاطر التزييف العميق ، دراسة تحليلية مقارنة ، بحث منشور ، مجلة ، روح القوانين ، كلية الحقوق ، جامعة طنطا ، عدد خاص ، المؤتمر الدولي الثامن لتكنولوجيا والقانون ، ص ٨٤٣ ٠

[٢] د٠ احمد مصطفى معوض محمد ، استخدامات الذكاء الاصطناعي وتقنية التزييف العميق في قذف الغير انموذجاً دراسة مقارنة معاصرة ، بحث منشور في مجلة البحوث الفقهية و القانونية ، كلية الشريعة و القانون ، دمنهور ، جامعة الازهر ، المجلد ٣٤ ، العدد ٣٩ ، أكتوبر ، ٢٠٢٢ ، ص ٢٥٣٥ ٠

العميق فقد اعتمدت العديد من الدول على خلق اطار متكامل (تشريعي ومؤسسي) لتوفير تلك الحماية عبر قوانين عامة لحماية البيانات ومواجهة هذه التقنيات بأليات رادعة مصممة خصيصا لمواجهتها وعدم التعامل معها كجرائم تقليدية مع الاهتمام بأنشاء مؤسسات مخصصة لتوفير حماية البيانات الشخصية اومراكز لمواجهة تلك التقنيات حفاظا على حق المجتمع في الحقيقية وحق الفرد في الحفاظ على بياناته من اجل ذلك سنقسم هذا المطلب الى فرعين نتطرق في الفرع الأول الى أهمية تطوير البينة التشريعية اما في الفرع الثاني منه نتطرق الى تطوير البنية المؤسسية

الفرع الأول

تطوير البنية التشريعية بأيجاد تشريع صارم موحد

ان تنظيم حماية البيانات الشخصية تشريعيا بات امراً ملحاً لما لذلك من أثر على تحقيق الامن المعلوماتي ففي بعض الدول قد مكنت القوانين في إيجاد حماية شاملة و موثوقة للبيانات الشخصية وذلك تعبيراً عن حق الافراد في حماية بياناتهم من جانب و مكافحة الجرائم المعلومات وتقينة التزييف العميق من جانب اخر ، ففي فرنسا فقد تبنى المشرع حماية البيانات الشخصية بموجب قانون رقم (٧) لسنة ١٩٨٧ الذي تم تعديلهُ بعد صدور قانون (٨٠١) في سنة ٢٠٠٤ والتي حل محلها هذا القانون جزئياً اللائحة الاوربية (GDPR) الصادر ٢٠١٦ الذي اصبح نافذا عام ٢٠١٨ و التي حلت محل القانون الفرنسي جزئياً وأصبحت الاطار الموحد لحماية البيانات الشخصية في الاتحاد الأوربي مع السماح لبقية الدول الأعضاء بإدخال تعديلات وطنية تكميلية تتناسب مع وضع كل دولة [١] ٠ حيث تبنى هذا القانون حماية متكاملة و صارمة لكل صور البيانات الشخصية [٢] ادراكاً منه لمخاطر التكنولوجيا عند الوصول الغير المشروع للبيانات الشخصية والتي تمثل اهداراً لفكرة الحق في الخصوصية فقد نظم المشرع بموجب هذه التشريع المعالجات الالكترونية للبيانات حيث اكد على ان مضمون المادة الأولى منه على ان الخصوصية المعلوماتية يجب ان تكون في خدمة كل مواطن و يجب ان لا تتضمن مساس بهوية الفرد او حقوقه الحياتية الخاصة او الحريات الفردية العامة [٣] و استناداً لهذا الغى المشرع الفرنسي الكثير من الالتزامات على من يقوم بمعالجة البيانات حتى يمكن القول بانها معالجة مشروعة كون الخطوة الأساس تبدأ عند الوصول لتلك البيانات وإدخال المعالجة عليها ولم يكتفي بذلك بل انه القى بعض الالتزامات على عاتق من يقوم بتلك المعالجة حتى تكتمل منظومة حماية البيانات الشخصية منها التزامات يجب ان يتبعها المعالج قبل انشاء نظام المعالجة للالتزامات اجرائية و التزامات موضوعية منها الالتزام بأمن تلك البيانات و الالتزام بعدم افشائها و الالتزام بإبلاغ من يتم معالجة بياناته او ابلاغ اللجنة التي أنشئت هذا الغرض

[١] المركز الأوربي لدراسات ومكافحة الإرهاب و الاستخبارات مقال منشور على https://www.europarabct.com/ تاريخ زيارة الموقع ٢٠٢٥/٧/١

[٢] د٠ سامح عبد الواحد التهامي ،مصدر سابق ، ص ٣٨٥

[٣] م (١) من الائحة العامة لحمايات البيانات ،ترجمة د٠مصطفى عبيد ،الاتحاد الأوربي(البرلمان الأوربي والمفوضية الاوربية) اللائحة العامة لحماية البيانات ، مصدر سابق ،ص ٣ ٠

هذا التعديل لتحقيقاً لمبدأ شفافية معالجة البيانات و عدم نقل تلك البيانات خارج نطاق دول الاتحاد الأوربي [١]، حيث سمح بتوسع نطاق معالجة البيانات ليشمل حتى لم يكن مقيماً داخل الاتحاد الأوربي الا انه فرض قيود و متطلبات جديدة عليه [٢] ،و بموجب هذا القانون و تعديلاته قد فرض عدة التزامات على معالجي البيانات ومن يمكنه الوصول اليها ونص على حقوق أساسية للفرد يتمتع بها ، منها الوصول لبياناتهِ واجراء التصحيح عليها و الحق و الاعتراض على معالجة البيانات لأغراض تسويفية و الموافقة المسبقة خاصة في معالجة ملفات الارتباط [٣] ٠ وبذلك جمع المشرع الفرنسي ما بين التشريعات المحلية و متطلبات اللائحة العامة لحماية البيانات ليظهر باطار قانوني متطور و متوازن بين حماية البيانات الشخصية ومتطلبات العصر الرقمي ٠

اما على مستوى التشريع المصري فقد ادرك المشرع المصري أهمية حماية البيانات الشخصية فعمد الى صدور قانونه رقم ٥١ لسنة ٢٠٢٠ و الذي لا يختلف كثير عن ما ورد في التشريعات الفرنسية ، فقد أصبحت بموجبه كافة الخدمات الرقمية و التكنلوجيا تفرض على المستخدم التزامات منها ضرورة الموافقة على السماح الترخيص بجمع البيانات بواسطة خوارزميات الذكاء الاصطناعي [٤] ،وكذلك من اهم النقاط التي يقوم عليها القانون بعد فرض الالتزامات على المعالج و المتكلم [٥]، كما اعطى القانون للشخص المعني صاحب البيانات بعض الحقوق التي تمكنهُ من المطالبة بتصحيح او تعديل او محو البيانات محل المعالجة و يمكنهُ من الاعتراض عليها اذا ما تعارضت مع حقوقهِ و حرياته الأساسية [٦] ٠

كذلك وعلى خطى المشرع الفرنسي فقد أورد المشرع المصري معالجة خاصة للبيانات الحساسة التي بموجبها فقد فرض القيود الصارمة على مجموعة من البيانات التي وضعتها على انها حساسة فمنها ما يتعلق بالصحة التقنية و القياسات الحيوية و الحالة الأمنية البيانات الجينية و المالية و بيانات الأطفال التي و التي صنفها المشرع على انها بيانات حساسة [٧]٠

---

[١] د٠ سامح عبد الواحد التهامي ،مصدر سابق ، ص ٢٩٢

[٢] قانون ٢٠٢٤ قانون تعديل لائحة الاتحاد الأوربي للبرلمان الأوربي النسخة الالكترونية منشور على موقع الاتحاد الأوربي يورو –ليكس http://data.europa.eu/eli/reg/2024/1468/oj تاريخ زيارة الموقع ٢٠٢٥/٧/٥

[٣] سياسة الخصوصية و حماية الحياة الخاصة مقال منشور على موقع السفارة الفرنسية في البحرين https://bh.ambafrance.org/%D8%B3%D9%8A%D8%A7%D8%B3%D8%A9-%D8%A7%D9%84%D8%AE%D8%B5%D9%88%D8%B5%D9%8A%D8%A9 تاريخ زيارة الموقع ٢٠٢٥/٧/١

[٤] يحيى دهشان ، المسؤولية الجنائية عن جرائم الذكاء الاصطناعي ، مجلة التشريعية والقانون ، الامارات ، مجلد ٣٤ – العدد ٨٢ ، ابريل ، ٢٠٢٠ ص ١٤٤ ٠

[٥] م (٥–٧) من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠ ٠

[٦] م ٣ من قانون حماية البيانات الشخصية المصري رقم ١٥١ في ٢٠٢٠ ٠

[٧] المادة قانون حماية البيانات الشخصية المصري رقم ١٥١ في ٢٠٢٠

الا انه قد أورد استثناء من حماية البيانات عندما يتعلق الامر بمحاضر الضبط القضائي و التحقيقات و الدعاوى القضائية و البيانات الشخصية لدى جهات الامن القومي مما تقدم لاعتبارات أخرى وغيرها من البيانات الواردة على سبيل الحصر في القانون من نطاق الحماية المقررة [١]، وقد احسن المشرع المصري عند تحديده أنواع البيانات الشخصية ٠

اما على المستوى المشرع العراقي فلم يوجد تشريع موحد صدر لحد الان يعتني بحماية البيانات الشخصية رغم التطور التكنلوجي في تطبيقات الذكاء الاصطناعي من جهة وبالرغم مما تمثله هذه البيانات كمحرك أساسي لتلك التطبيقات ،فقد اقتصرت الحماية على تشريعات قطاعية محدودة منها الحماية على قانون البطاقة الوطنية رقم ٣ لسنة ٢٠١٦ الذي نص بموجب المادة (١٥) منه (لا يجوز تداول البيانات و القيود المدنية و المستندات الالكترونية او اجراء أي معاملة الكترونية مع قاعدة البيانات تجري او جرت خارج سيطرة واشراف المديرية العامة او جرت بدون موافقة المدير العام او من يخوله او استخدمت في مجالات خلافاً لأحكام هذا القانون) مقتصراً على كيفية ونقل القيود المدنية من السجلات الورقية الى الصيغة الالكترونية ومنح المواطن بطاقة متضمنة كل بياناتهِ الشخصية و التزامهِ بالتحديث بين الحين و الاخر من الرغم من ذكره للبيانات وتجميعها بصورة الكترونية و معالجتها بموجب المادة (١ فقرة ٢٤) [٢] ٠ الا انه اغفل مسألة في غاية الأهمية وهي في حالة الاعتداء على هذه البيانات وإمكانية قرصنتها او تعرضها للتزييف او الاستحواذ عليها ونشرها من قبل المعتدين عليها وكذلك لم يرد كيفية حمايتها و النصوص العقابية التي تفرض في سبيل توفير الحماية فلم يكن المشرع العراقي موفقاً في هذا التشريع على الرغم من الأهمية الكبيرة للبطاقة الوطنية الموحدة وما تحمله من معلومات حساسة بايومترية تضمنت بصمة العين و الابهام وغيرها من المعلومات الواسعة مما يثير المخاوف من سوء الاستخدام و انتهاكات للخصوصية في ظل غياب قانون حماية للبيانات الشخصية و بشكل مستقل وكذلك الحال فيما يخص المادة (٥٢ / اولاً / ثانياً) من قانون المصارف رقم ٩٤ لسنة ٢٠٠٤ و الذي بموجبه فرض المصرف المركزي العراقي ضوابط لحماية البيانات العملاء في القطاع المالي لكن تلك الحماية غير شاملة و تفتقر الى رقابة مستقلة ، لذا ندعو المشرع العراقي الى اسراع بإصدار قانوني لحماية البيانات الشخصية لما لذلك من أهمية في تحقيق التنمية و الاستقرار المعلوماتي ٠

اما على مستوى مكافحة الجرائم التقنية التزييف العميق فقد اعتمدت الدول في سبيل ذلك اما بتوضيف التشريعات السارية لمكافحة التزييف العميق بشكل فعال لذلك بإدخال تعديلات على قوانينها للجرائم الالكترونية ليواكب التطورات أو العمل على سن قوانين جديدة لمكافحة الظواهر الحديثة بعد ان تتوافق القوانين السارية كافة عن توفير الحماية اللازمة فيها ٠

[١] المادة قانون حماية البيانات الشخصية المصري رقم ١٥١ في ٢٠٢٠

[٢] المادة (١/فقرة ٢٤) من قانون البطاقة الوطنية رقم ٣ لسنة ٢٠١٦ (نظام معالجة المعلومات : النظام الالكتروني او برامج الحاسوب المستخدمة لأنشاء المعلومات او ارسالها او تسلمها او معالجتها او تخزينها الكترونياً٠

ففي فرنسا حيث يعد الاطار القانوني للذكاء الاصطناعي جزء من نظام الاتحاد الأوربي الموحد فعلى مستوى الاتحاد قد اخذ خطوات واضحة في سبيل مكافحة التزييف العميق وذلك على مستوى قانون الذكاء الاصطناعي الذي اقره البرلمان الأوربي في ٢٠٢٤ [١] و الذي بموجبهِ صنف خطورة تقنيات الذكاء الاصطناعي وفقاً لأربعة مستويات فعلى المستوى الأول الخطورة الغير مقبولة وهي نوع من الخطورة التي تهدد سلامة و عيش الفرد و الحقوق المكفولة لمواطني الاتحاد الأوربيوغير أخلاقية بحيث لا يسمح بها ، اما المستوى الثاني فهي عالية المخاطر او الذي بموجبه تخضع المنتجات الذكية الى قواعد صارمة عند التعامل معها والتي لها اثار كبيرة على حقوق الافراد وسلامتهم ،اما المستوى الثالث فهي الخطورة الخطوالمحدودة و الذي بموجبه تخضع منتجات الذكاء الاصطناعي لقواعد محددة و الذي الزم بموجبه بالتصريح بحقيقة المحتوى تقع من ضمنها هذه المنتجات تقنية التزييف العميق ،اما المستوى الرابع فهي منتجات الذكاء الاصطناعي منخفضة الخطورة حيث لا يخضع بموجبهِ المنتجات الذكية لقيود [٢] مثالها الألعاب الالكترونية او الفلاتر التجميلية ووفقا المادة (٥٢) الفقرة الثالثة من قانون الذكاء الاصطناعي الأوربي صنفت تقنية التزييف العميق ضمن المستوى الثالث [٣] و الذي الزم بموجبهِ بضرورة التصريح بالمحتوى المزيف مالم يكن الاستخدام لأغراض مشروعة تخص بالكشف عن الجرائم او التحقيق الجنائي او محاكمة المجرمين ، الا ان يمكن اعتبار التزييف العميق ضمن مستويات الأفعال المحضورة متى ما استخدمت لغرض تشويه سمعة الاخرين او التأثير على مجموعة اشخاص بشكل يؤدي الى اضعاف قدرتهم على على اتخاذ قرار لم يكونو يتخذوه لو لولا ذلك الوضع [٤] .

كذلك فقد واجهة الاتحاد الأوربي تقنية التزييف العميق عن طريق قانون الخدمات الرقمية الذي تناول المحتوى الغير القانوني و الإعلانات الشفافة و التضليل للمحتويات المزيفة وذلك بموجب قانون الخدمات الرقمية عام ٢٠٢٢ .

اما على مستوى التشريع المصري فقد تدارك المشرع خطورة هذه الجرائم ففي الربع الأخير من عام ٢٠١٧ زاد عدد البرامج الخبيثة بشكل واسع بنسبة وصلت الى ٢٥ % بحيث أصبحت مصر من الدول الرقمية الثالثة على مستوى

---

[١] قانون الاتحاد الأوربي للذكاء الاصطناعي رقم ١٦٨٩/ ٢٠٢٤ منشور على الموقع الالكتروني https://share.google/NXZ1kPKgs3Qtg7kRY تم زيارة الموقع ٧/٧/ ٢٠٢٥

[٢] تصنيف المخاطر الأربعة لقانون الذكاء الاصطناعي في الاتحاد الأوربي هل شركتك مستعدة مقال منشور على الموقع الالكتروني https://www.fticonsulting.com/insights/fti-journal/four-risks-eus-artificial-intelligence-act تاريخ زيارة الموقع ٢٠٢٥/٧/١٠

[٣] الذكاء الاصطناعي والتزييف العميق : لوائح الاتحاد الاتحاد الأوربي وإيطاليا مقال منشور على الموقع الالكتروني https://www.jacobacci-law.com/news-and-publications/ai-and-deepfakes-eu-and-italian-regulations تاريخ زيارة الموقع ٢٠٢٥/٧/١٠

[٤] د٠ محمود حسين سيد أبو سيف ، التنظيم القانوني للتزيف العميق في قانون الذكاء الاصطناعي الصادر عن الاتحاد الأوربي ، بحث منشور ، مجلة العلوم القانونية والاقتصادية العدد الأول ، السنة ٦٧، يناير، ٢٠٢٥ ص ١٧٢٦

القارة الافريقية من حيث تعرضها للبرمجيات و الهجمات الالكترونية [١]،فعمد المشرع على اصدار قانون جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ حيث جرم المشرع المصري فعل التزييف العميق في الفصل الثالث في القانون الذي جاء بعنوان الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة و المحتوى المعلوماتي الغير المشروع التي كانت دقيقة جداً في وصف صور التزييف العميق حيث نصت المادة (٢٦) من القانون (كل من تعمد استعمال برنامج معلوماتي او تقنية معلوماتية في معالجة المعطيات الشخصية للغير لربطها بمحتوى منافٍ للآداب العامة او لا ظهارها بطريقة من شأنها المساس بأعتباره او شرفهِ) ، كذلك واجهة المشرع المصري التزييف العميق في قانون حماية الخصوصية للبيانات الشخصية الرقمية رقم (١٥١ لسنة ٢٠٢٠) عند تعريفهِ للبيانات الشخصية حيث عد تصميم تطبيقات بيومترية معقدة تعتمد على عمليات مسح بصمات رقمية و فحوصات التعرف على الصور و تحسين أداء الصوروالكلام أمور في غاية الخطورة وان حماية البيانات الشخصية هي حق من حقوق الانسان في ظل تنامي التقنيات المزيفة عبر الانترنت [٢] .

اما على مستوى التشريعات العراقية يتميز الوضع القانوني بغياب تشريع مخصص لتنظيم تقنيات الذكاء الاصطناعي على خلاف ما وجدنا على مستوى التشريع الفرنسي او وجود تشريع لمكافحة الجرائم الالكترونية و جر ائم التزييف العميق كما هو الحال في مصر على الرغم من ان العراق قد صادق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عام ٢٠١٠ في القاهرة ،الا انه اعتمد على مواجهة التزييف العميق ضمن القوانين القائمة منها قانون العقوبات رقم ١١١ لسنة ١٩٦٩ المعدل حيث يطبق على الأفعال المرتبطة بالتزييف منها احكام المادة ٤٣٠ و ٤٥٢ و الخاصة بتجريم التهديد على وقائع مشابهة مثل جرائم الابتزاز المالي بواسطة التقنيات الذكاء الاصطناعي لحملهم على تسليم أموال بالتهديد الأشخاص بنشر صورهم او تزييف محتوى فيديوي لهم ، كنوع من انتحال الهوية ، كذلك تطبيق المادة ٤٥٦ على جرائم الاحتيال الالكتروني مما تقدم يتبين ان هنالك قصور تشريعي على مستوى حماية البيانات الشخصية من جانب ومكافحة مخاطر التزييفات العميقة من جانب اخر لذا ندعو المشرع الى توفير الحماية التشريعية بالإسراع على اصدار تشريع خاص لحماية البيانات في ظل اتساع التحول الرقمي ومن جانب اخر الإسراع في اصدار قانون لتنظيم تقنيات الذكاء الاصطناعي و الجرائم الالكترونية كون التشريعات لا تواكب التقنيات الحديثة

الفرع الثاني

تطوير البنية المؤسسية بأنشاء جهات مخصصة

من اجل ضمان احترام تطبيق القانون المعني بحماية البيانات الشخصية لابد من وجود جهة مختصة ذات سلطة تضطلع بمهامها لتكون العين الساهرة على ضمان تتمتع جميع الافراد بالحق في حماية بياناتهم الشخصية ومنع

[١] رانيا سليمان أبو المعاطي محمود / نهى محمد إبراهيم الدسوقي / فاتن فائز حميده الصفتي ، سياسة مكافحة الإرهاب الالكتروني ، مصر و السعودية نموذجا ، بحث منشور المركز العربي للبحوث و الدراسات افاق سياسية ، العدد ٥٣ ، ٢٠٢٠ ، ص ٥٢– ٥٣ .

[٢] منة الله كمال موسى ذياب ، سلوك حماية الخصوصية الرقمية البيومترية لدى مستخدمي تطبيقات التوييف العميق ، بحث منشور ، المجلة العربية لبحوث الاعلام و الاتصالات ، كلية الاعلام ، جامعة الكندية ، القاهرة ، العدد ٣٧ ، ابريل ، ٢٠٢٠ ، ص ٢٤ .

الاعتداء عليه ، ففي فرنسا اسند المشرع مهمة حماية البيانات الى الهيئة الوطنية للمعلومات و الحريات (CNIL) مهمتها تراقب الاحتيال على القوانين وذلك طبقاً لنص المادة (١١) من القانون الفرنسي رقم ٧٨ – ١٧ عام ١٩٧٨ والذي جاء متوافق مع اللائحة الاتحاد الأوربي ومنحها المشرع الاستقلال التام وعدم خضوعها الى لأي سلطة باعتبارها سلطة إدارية مستقلة ومنحها العديد من الاختصاصات و السلطات التي تمكنها من ضمان تتمتع الافراد بما قرره المشرع من حقوق لهم [١] .

فهي لا تتلقى أي أوامر من أي جهة او سلطة داخل الدولة ولا تخضع لأي صورة من صور السلطة الرئاسية فلا تدخل ضمن الهيكل التنظيمي لأي وزارة او إدارة وتقدم اللجنة تقريرها السنوي المتضمن أنشطة اللجنة ومهامها لرئيس الجمهورية او الوزير الأول (رئيس الوزراء) و البرلمان [٢]،و تتشكل اللجنة الوطنية للمعلومات و الحريات من ثمان عشر عضو **أربعة** منهم أعضاء برلمان و **عضوين** من الجمعية الوطنية و **عضوين** من مجلس الشيوخ و **ستة** مستشارين (عضوين عاملين سابقين بمجلس الدولة الفرنسي لا تقل درجتهما عن مستشار و اثنين عاملين سابقين من المحكمة المحاسبات لا تقل درجتهما عن مستشار و عضوين من مجلس الاقتصادي و الاجتماعي و البيئي) و **ثلاث** اشخاص ذوي كفاءة و متخصصين في المعلوماتية لديهم دراية بقضايا الحريات و **رئيس** لجنة الولوج الى المستندات الإدارية [٣] .

وتمتلك اللجنة القومية في فرنسا صلاحيات واسعة ابتداء من ضرورة الالتزام بأخطار اللجنة قبل انشاء نظام معالجة البيانات الشخصية ويعتبر ملزم كل من يقوم بأنشاء نظام للمعالجة سواء أ كان جهة عامة او خاصة الهدف منه تمكين اللجنة في فرض سلطتها و العلم باي عملية لمعالجة البيانات ومن ثم فرض رقابتها للتأكد من مدى ملائمتها للقانون [٤]وكذلك من ضمن السلطات الممنوحة للجنة هو الترخيص حيث ان اللجنة تسهرعلى احترام معالجات البيانات الشخصية تلك التي تتعلق بأمن الدولة او الدفاع عنها او منع حدوث الجرائم والاستدلال عليها وذلك طبقاً للمادة (٦) من القانون الفرنسي اومعالجة البيانات التي يكون موضوعها بيومترية او جينية او صحية [٥] هذا وتفرض اللجنة ايضاً رقابتها السابقة على معالجة البيانات التي يتم الحساب الدولة او شخص معنوي عام او خاص حسب المادة (٢٧) من القانون كذلك من صلاحيتها الترخيص بنقل المعطيات و الامر بأجراء التغيرات اللازمة لحماية تلك

[١] طارق جمعة السيد راشد ، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي ، بحث منشور ، مجلة القانون و الاقتصاد ، ملحق خاص ، العدد ٩٢ ، ص ٢٢٩ .

[٢] د. شريف يوسف خاطر، حق الاطلاع على البيانات الشخصية ، بحث منشورفي مجلة كلية القانون الكويتية العالمية ، ص ٣٤٣ .

[٣] د. شريف يوسف خاطر ، حماية الحق في الخصوصية المعلوماتية ، دراسة مقارنة ، دار الفكر و القانون ، جامعة المنصورة ، سنة ٢٠١٥ ، ص ١٥٢ .

[٤] د. سامح عبد الواحد التهامي ،مصدر سابق ، ص٢٢٢

[٥] V.Jean-paul cost Aila tansparence ad Ministrative Regard sur L,actualité sptem ber- octobor – 1998 – p 37 – 40 .

البيانات و الامر بسحبها و اتلافها [١] ،ولها ان تضع اللوائح نموذجية بهدف ضمان امن أنظمة المعالجة ومن أجل ضمان تنفيذ ما تسعى اليه اللجنة الوطنية (CNIL) في تحقيق رقابتها قد مكن المشرع اللجنة من فرض جزاء على المخالفين لقانون حماية البيانات منها الغرامات المالية إضافة الى إمكانية فرض حظر السفر و تجميد الأصول و خصوصا في حالة الجرائم الالكترونية[٢] ،اما على مستوى مكافحة جرائم المعلوماتية و التزييف العميق في فرنسا فأن هذه المهمة تقع من الناحية الإدارية ضمن مسؤوليات جهات الامن السيبراني (ANSSI) إضافة الى تعاونها مع وزارة الداخلية و الهيئة الوطنية لحماية البيانات التي تعمل على فرض الرقابة على المنصات الرقمية ، حيث يكون هناك تنسيق مشترك كحالات انتهاك الشخصيات في الهجمات السبرانية حيث توفر (ANSSI) التحليل التقني بينما تتولى الهيئة الوطنية (CNIL) الجانب القانوني و المخالفات المتعلقة بالبيانات [٣] .

اما في مصر فقد أنشئ قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠[٤] مركز حماية البيانات الشخصية على غرار الهيئة الوطنية في فرنسا ويتبع الى وزارة الاتصالات ويتشكل المركز من مجلس إدارة يقسم الى ممثليتين عن وزارة الداخلية و جهاز المخابرات وهيئة الرقابة الداخلية و ممثل عن هيئة تنمية صناعة تكنلوجيا المعلومات و ممثل عن الجهاز القومي و رئيس تنفيذي للمركز مع ثلاثة أعضاء من ذوي الخبرة يختارهم الوزير شخصياً [٥] ،ويهدف هذا المركزالى حماية البيانات وتنظيم معالجتها ووقايتها من خلال وضع وتطوير سياسات وخطط استراتيجية و برامج لحماية البيانات فضلاً عن توحيد تلك السياسة داخل مصر وضع اطار ارشادي للوائح والسلوك الخاصة لحماية البيانات و التعاون و التنسيق الأجهزة الحكومية و غير الحكومية في ضمان تلك الإجراءات ،ومن اجل ضمان ممارسة هذا المركز لاختصاصات فقد مكنهُ المشرع من عدة سلطات اثناء تحقيق اهدافهِ ومن ابرز سلطاتهِ هو اصدار التراخيص و التصاريح الخاصة عند التحكم و المعالجة للبيانات بما فيها البيانات الحساسة ونقلها عبر الحدود بالإضافة الى تقديم المشورة في مجال حماية البيانات [٦] ،إضافة الى ذلك سلطاتهِ في التفتيش و التحقيق في الشكاوي و المخالفات مع منح موظفي المركز الصلاحيات القانونية لتنفيذ القانون إضافة الى ذلك يسعى المركز في وضع السياسات و الخطط الاستراتيجية وتلقي الشكاوي و البلاغات وحل النزاعات المتعلقة بانتهاك قانون حماية

---

[١] كحلاوي عبد الهادي – بن زيطة عبد الهادي ، السلطة الإدارية المستقلة لحماية البيانات الشخصية ، دراسة مقارنة بين القانونين الفرنسي و الجزائري ، بحث منشور في المجلة الجزائرية العلوم و القانون و السياسة ، المجلد ٥٩ ،العدد ٢،السنة ٢٠٢٢ ، ص ١٢٧

[٢] المركز الأوربي لدراسات مكافحة الإرهاب و الاستخبارات المانيا و هولندا ،مقال منشور م https://www.europarabct.com/?=83399 تم زيارة الموقع ٢٠٢٥/٧/١٥

[٣] الوكالة الوطنية لأمن أنظمة المعلومات سلطة ANSSIعلى الموقع الالكتروني https://www.orsys.fr/orsys-lemag/en/glossary-2/anssi-%F0%9F%9F%A9-authorit

تم زيارة الموقع ٢٠٢٥/٧/١٥

[٤] استنادا للمادة (١٩) من قانون حماية البيانات المصري رقم (١٥١) لسنة ٢٠٢٠ .

[٥] استنادا للمادة (٢٠) من قانون حماية البيانات المصري رقم (١٥١) لسنة ٢٠٢٠ .

[٦] استنادا للمادة (٢٦) من قانون حماية البيانات المصري رقم (١٥١) لسنة ٢٠٢٠ .

البيانات اما على مستوى مكافحة التزييف العميق في مصر يتم ذلك عن طريق الجهاز القومي لتنظيم الاتصالات [١] وكذلك يتم مواجهة التزييف العميق عن طريق وزارة الداخلية عبر إدارة مباحث الانترنت التي تتولى التحقيق في جرائم تقنية معلوماتية بما في ذلك التزييف العميق ٠

بالتالي نرى ان كل من فرنسا و مصر وضعتا قانون ينظم حماية البيانات الشخصية والذي بموجبه قد نصت على انشاء هيئات او جهات إدارية متخصصة لحماية البيانات و مراقبة للامتثال للقوانين و تمتع بصلاحيات تنظيم و تفتيش و ترخيص عند معالجة البيانات وجهات مختصة لمواجهة الجرائم الناشئة من تطبيقات الذكاء الاصطناعي ولاسيما التزييف العميق ، الا انهُ نرى هنالك اختلافات جوهرية منها ما يتعلق بطبيعة الهيئة فاللجنة الفرنسية (CNIL) سلطة مستقلة تماماً عن أي وزارة اما مصر مركز حماية البيانات المصري يتبع الى وزارة الاتصالات ، إضف لذلك تعتبر الإجراءات الفرنسية اشمل و صارمة من حيث تنظيم الإجراءات و التحقيقات و فرض الغرامات في حين المركز المصري يحدد العقوبات الجنائية خلاصة القول تعد فرنسا نموذجاً متقدماً لحماية البيانات الشخصية بفضل استقلالية الهيئة الوطنية (CNIL) واتباعها لأليات تنفيذية صارمة٠

اما في العراق فانه لا توجد جهة مستقلة او هيئة متخصصة لحماية البيانات عند مقارنتها في الهيئات المستقلة كالهيئة (CNIL) في فرنسا و مركز حماية البيانات في مصر، لذا ندعوا الى ضرورة انشاء هيئة متخصصة مستقلة لحماية البيانات (الهيئة الوطنية المستقلة لحماية البيانات الشخصية) وتكون ذات صلاحيات عند اجراء أي معالجة او تعديل على البيانات من اجل حماية حقوق الافراد ، على ان تحدد تلك الصلاحيات بموجب قانون حماية البيانات الشخصية يصدر لهذا الغرض وبذات الوقت ندعو الى انشاء مركز لمكافحة الجرائم الالكترونية و الذكاء الاصطناعي لمواجهة هذا النوع من الجرائم عبر تجريم انشاء او تداول محتوى مزيف Deep Fake وفقاً للقانون ويكون على مستوى من التنسيق بين الوزارات والجهات المعنية كالاتصالات والداخلية والتخطيط والامن الوطني ، فمن اجل خلق منهج كامل لحماية البيانات الشخصية لابد من تطوير البيئة المؤسساتية عبر انشاء هيئة لحماية البيانات من جهة و انشاء مركز لمكافحة تلك التقنيات العميقة من جهة أخرى ٠

المطلب الثاني

الحماية الإجرائية للبيانات الشخصية من تقنية التزييف العميق ٠

نتيجة لما تميزت به البيانات الشخصية من أهمية باعتبارها جزء من مفردات الشخصية الإنسانية ولما لها من دور كبير في تحديد هوية صاحبها بالإضافة الى اعتبارات تتعلق بالسرية الشخصية التي تترتب على انشاءها وعرضها على الاخرين و مشاركتها معهم فعلاً يثير المسؤولية لذا باتت حماية تلك البيانات ضرورة حتمية في مواجهة التهديدات ولاسيما المتطورة منها كالتزييف العميق فبرزت مجموعة من الإجراءات التي يحتم على الإدارة اتخاذها في سبيل توفير تلك الحماية للبيانات واتخاذ كافة التدابير في مواجهة مخاطر التقنيات العميقة حيث تستند ألليات الحماية

[١] استنادا للمادة (١) من قانون الجرائم الالكترونية المصري ، رقم (١٧٥) لسنة ٢٠١٨ ٠

الإدارية في هذا المجال الى إجراءات متعددة لذا سنقسم هذا المطلب الى ثلاث فروع نتطرق في الفرع الأول منه الى الإجراءات الإدارية التقنية ويختص الفرع الثاني بالإجراءات الإدارية التنظيمية بينما نتطرق في الفرع الثالث الى إجراءات الإدارة في فرض الجزاءات التي تمثل ضمانة لتوفير تلك الحماية ٠

الفرع الأول

الإجراءات الإدارية التقنية

تعتمد حماية البيانات الشخصية على مجموعة متكاملة من الأدوات التقنية التي صممت لضمان سرية البيانات و سلامتها من جهة وعلى بالاعتماد على تقنيات لمواجهة التزييف العميق من جهة أخرى و التي تتميز بفاعليتها كونها تتلائم مع الطبيعة التقنية لنظام الحاسبة وشبكة الانترنت بأعتبارها البيئة التي يعمل فيها وذلك لمنع وقوع الاعتداء على اقل تقدير و التقليل من الاضرار التي تلحق نتيجة ذلك الاعتداء فهذه الإجراءات التقنية أو التكنلوجيا تسعى الى الحفاظ على امن المعلومات من خلال تحديد الشخص المستخدم ومدى مشروعية دخولهِ للنظام و التحكم في دخولهِ للشبكة و تحقيق سرية المعلومات و تكاملها ، والتي تتمثل بالتعريف بشخص المستخدم ووسائل التحكم في الدخول للشبكة و مراقبة وتتيح الاستخدام [١] والتي تتعلق بكل مايشمل بأجراءات التخزين والاحتفاظ للحماية الامنة للبيانات الشخصية حيث تتمثل الحماية الإدارية التقنية في هذا المجال بما يلي /

أولا :- التشفير / وهي عملية يتم ضمن عملها تحويل البيانات الشخصية للفرد الى رموز غير مفهومة من خلال استخدام خوارزميات رياضية وذلك بهدف حماية تلك البيانات من الوصول غير المسموح اليها ، فلا يستطيع قراءة محتواه شخص اخر كونه لا يملك مفتاح فك ذلك التشفير [٢]، ويكون التشفير بصورتين **الأولى** يتم باستخدام كل من المرسل و المستخدم ذات المفتاح السري في تشفير الرسالة وفك تشفيرها و يكون كل من الطرفين على معرفة بذات المفتاح (عبارة المرور) و التي يتم استعمالها مستقبلاً ٠ اما **الصورة الثانية** تكون باستخدام مفتاحين اثنين بينهما علاقة لدى الأول المفتاح العام و الاخر المفتاح الخاص [٣] والذي يكون معرفاً لدى اكثر من شخص او جهة وهو الرقم الذي يتم تداوله و نشره بين المستخدمين لتشفير البيانات و المعلومات ، وبعد يأتي دور المفتاح الخاص الذي يعد النصف الاخر و المكمل للمفتاح العام للوصول الى الرقم الأساسي ويكون معرف لدى شخص واحد او جهة واحدة وهو المرسل و الذي يميز كل شخص مستخدم عن غير من المستخدمين [٤] ،تعد خوارزميات تشفير البيانات امراً بالغ الأهمية في حماية البيانات في القطعات الحيوية مثل التمويل و الرعاية الصحية و الحكومية و لضمان

---

[١] د ٠ شريف فتحي الشافعي ، تخطيط و تصميم و تركيب شبكات الحاسب الالي ، دار الكتب العلمية للنشر و التوزيع ، القاهرة ، ٢٠٠٢ ، ص ١٧٤ ٠

[٢] رشيد حمد علي حمد ، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الانترنت ، دراسة مقارنة ، دار النهضة العربية ، القاهرة ، ٢٠١٣ ، ص٢٧٧ ٠

[٣] د ٠ اشرف السعيد احمد ، تكنلوجيا المعلومات في المجال الأمني ، القاهرة ، ٢٠١٣ ، ص ٨٥ ٠

[4] John R , Computer and in formation Security hand book , Second edition , A Msterdam , Elsevier , Morgan , Kaufm mehnn , 2013 , C.p124 .

تطبيق افضل المهارات لتطبيق استراتيجية التشفير من قبل الإدارة يجب ان يكون هنالك تحديث للخوارزميات التشفير وبشكل دوري لضمان بقاءها آمنة ضد أساليب الهجوم إضافة الى ذلك ينبغي استخدام مفاتيح قوية ومعقدة و تجنب استخدام كلمات مرور سهلة أو شائعة او سهولة تخمينها فأن من اهم التحديات التي تواجه هذه التطبيقات هي إدارة المفاتيح فاذا لم يتم ادارتها بشكل صحيح يؤدي الى فقدان الوصول الى تلك البيانات المشفرة او تعرضها للاختراق [١] ٠

ثانيا :- استخدام برمجيات مقاومة وكشف الفيروسات الالكترونية ٠

وهي عبارة برامج تقوم بحماية الأجهزة من الهجمات الفايروسية وتعمل على مكافحتها والتي تكون مصممة لغرض الاضرار بتلك الأجهزة وبالتالي تشكل خطرا و تهديداً للبيانات الشخصية ويتم رصد البرامج الضارة عن طريق القرص الصلب أو المدمج أو بعض الرسائل الالكترونية وتسميتها بمضادات الفايروسات ، وتعمل هذه البرامج سواء بشكل مباشر بمجرد الدخول الى البرامج أو تنزيل الملفات أو ان تعمل عند الطلب وهذا عندما يطلب المستخدم برنامج للكشف عن الفيروسات [٢] ٠

ثالثا:- الجدار الناري / وهو نظام يوفر الحماية عبر ترشيح البيانات المرسلة المستعملة من الشبكة اعتماداً على قواعد قد حددها المستخدم مسبقاً الهدف منه هو منع الاختراق و التسلل للحاسبة و حماية البيانات للمستخدم من الوصول غير المصرح به وذلك بتقليل إزالة وجود الاتصالات الشبكية الغير مرغوب بها و السماح في الوقت ذاتهِ للاتصالات المصرح بها ان تنتقل بحرية وذلك عبر ما يعرف بالخادم الوكيل الذي يعتبر بمثابة جدار او حاجب بين النظام المعلوماتي للحاسبة و شبكة الانترنت [٣]حيث توفر هذه الجدر النارية طبقة أساسية من الحماية التي تندمج مع غيرها لمنع المهاجمين من الوصول للخوادم بطرق احتيالية [٤]،ومن اهم وظائف هذه الجدر النارية هي التدقيق من هوية المستخدم و مراقبة الاستخدام وتتبع سجلات الدخول و الخروج للشبكة و مراقبة المحتوى الوارد الى الشبكة للبحث عن الفيروسات و البرامج الضارة ، الا انه من اجل توفير حماية قصوى للبيانات الشخصية يجب الاكتفاء بنظم التقنية لحماية البيانات الشخصية وانما يجب اتباع أساليب تقنية لمواجة تقنيات التزييف العميق والتي منها

أولا :- استخدام تقنيات الذكاء الاصطناعي كأليات الكشف عن المحتوى المزيف

---

[١] المركز الوطني للامن السيبراني ،الحماية من البرامج الضارة (الربمجيات الخبيثة) مقال على الموقع الالكتروني https://www.ncsc.gov.bh/ar/cyberwiser/general-threats/protecting-against-malware.

تاريخ زيارة الموقع ٢٠٢٥/٧/٢٧ ٠

[٢] Chuck Eattom , Jeff Taylor Computer Crime – investigation an the law Course technology , 2010 , p 145

[٣] بن شهب أسماء ، حماية البيانات الشخصية للمستخدم في اطار عقود الحوسبة السحابية ، بحث منشور ، مجلة الفكر القانوني و السياسي ، كلية الحقوق ، جامعة الاخوة منتوري – قسطنطينية ، المجلد التاسع ، العدد الأول ، ٢٠٢٥ ، ص ٣١٣ ٠

[٤] جدران الحماية / التحكم في مرور البيانات الشركة عبر firewall(الحماية تبدأمن هنا) مقال منشور على الموقع الالكتروني https://my-communication.com/firewall/?utm_ تاريخ زيارة الموقع ٢٠٢٥ /٧/٢٨

يمكن الاعتماد على تقنيات الذكاء الاصطناعي في الكشف عن تقنيات التزييف العميق على الرغم من ان هذه تعتمد ايضاً على أنظمة الذكاء الاصطناعي ويتم ذلك عن طريق تطوير المستخدم لأنظمة تقنية وألية قادرة على التحليل ومراقبة المواقع و المنصات الالكترونية من اجل الكشف المحتوى المزيف [١]،ولعل بين أدوات الكشف عن التزييف الحديثة هي تقنية التعلم العميق و تحليل البيانات التي تعتمد على شبكات عصبية عميقة تعمل على تحليل مكونات الصور و الفيديوهات حيث تركز على حركة العين و الملامح حيث يتم تمرير الصور عن طريق شبكة عصبية وبعدها تقييم تلك الصور ووضع ميزات بسيطة عنها ويتم بعدها فحص تلك الميزات

بحثا عن أي تحريف [٢]،وكذلك عن طريق تقنية التوقيع الرقمي و العلامة المائية التي تساعد في تأكيد اصالة الملف و كشف التزوير او التزييف ، إضافة الى تقنية توليد البيانات و تقنية الكشف عن النص الزائف هذا وقد تطورت بعض البرامج لمكافحة التزييف العميق وغيرها من البرمجيات الخطرة ٠

ثانيا :- مساهمة الشركات العالمية والمؤسسات الاكاديمية في مواجهة التزييف العميق

لم تقتصر اليات مكافحة التزييف من قبل القطاعات العامة و الحكومية وانما امتدت الى إدارة القطاع الخاص ، فقد طورت الشركات التكنلوجيا العملاقة مثل (google) وميتا (Meta) وأكس (x) وتيك توك (TikTok) وغيرها من الشركات المنتجة للذكاء الاصطناعي او مستخدمة من إدارة مكافحة التزييف العميق حيث اتسعت الاليات لمواجهة تلك التقنية والقضاء على نشر المحتوى المزيف حيث يمكن للمستخدم عبر (google) من التحقق من صحة صدور الفيديو اذا كان مريب او مزيف عن طريق التقاط صورة او فيديو او تشغيلهُ عبر البرنامج او منصة البحث العكسي للصور التابعة لجهة خارجية كذلك طور مختبر انتل تقنية fake catcher القادرة على اكتشاف مقاطع المزيفة بمعدل دقة تصل الى ٩٦% وهو برنامج يستطيع كشف المحتوى المزيف بوقت قياسي يبلغ الأجزاء من الثانية اذ يعتمد على العين و ورفة العين وايضاً إشارات تدفق الدم التي تجمع من الوجه الكامل وبالتالي تترجم الى خوارزميات وبما ساعد تقنية التعلم العميق عن كشف تلك الاثارات الى خرائط مكانية او زمانية وتبين فما اذا كان الفيديو حقيقياً او مزيفاً [٣] وبالمقابل وفرت شركة فيس بوك (face book) و كوكل (google) للباحثين قاعدة بيانات ضخمة تحتوي على فيديوهات مزيفة و حقيقية لغرض مساعدة الباحثين في الكشف عن المحتوى المزيف [٤] ٠

الفرع الثاني / الإجراءات الإدارية التنظيمية

---

[١] د٠ صدام فيصل كوكز ، التزييف العميق تقنيات معقدة واشكاليات قانونية ، دار هاتريك للطباعة و النشر و التوزيع ، الطبعة الأولى ، أربيل ، ٢٠٢٥ ، ص ٧٥ ٠

[٢] Aarti Karndikar, Vedtia Deshpande, Sanjann Singh, Sayail Nagbhidkar,Saurabh Agrawal,Deepfake video Detection using convolutional neural Network,International Joural of Advanced trends in computer Science and Engineering ,Volume 9 ,No 2 , March- April 2020 ,p1314

[٣] سامح محمد السيد إبراهيم ، مصدر سابق ، ص ٣٩٩١

[٤] علاء الدين منصور مغايرة ، جرائم الذكاء الاصطناعي وسبل مواجهتها جرائم التزيف العميق انموذجا ، بحث منشور ، كلية القانون ، جامعة قطر ، ٢٠٢٣ ، ص ١٥٣ ٠

تشكل إجراءات الإدارية في هذا المجال في وضع لوائح او تعليمات صارمة لحماية البيانات الشخصية و تدريب الكوادر من الموظفين و نشر الوعي من اجل مواجهة لتهديد التزييف العميق للبيانات فلا يمكن الاكتفاء بالإجراءات التقنية فلابد من وجدود هذه اللوائح التنظيمية ، ففي فرنسا تم اصدار المرسوم 2019–536 الصادر في ٢٩مايو ٢٠١٩ و الذي تم اعتماده لغرض تطبيق قانون حماية البيانات الشخصية الفرنسي و يوضح القواعد الإجرائية للهيئة الفرنسية (CNIL) وتتضمن هذه اللوائح تفاصيل عملية تحدد كيفية تطبيق القانون وتشمل عادة التعريفات الدقيقة و المفاهيم كتوضيح المصطلحات المتعلقة بالبيانات الحساسة ، وتحدد أنواع البيانات الجينية و الحيوية و شروط المعالجة البيانات كالموافقة الصريحة و الغرض من تلك المعالجات و الأغراض المشروعة التي يسمح بها معالجة البيانات كالبحث العلمي و الخدمات الصحية ، إضافة الى بيان واجبات المسؤول بالمعالجة و متطلبات أمن البيانات و شروط نقل البيانات عبر الحدود و إدارة انتهاكات البيانات كإجراءات الإبلاغ و اخطار الافراد المتضررين و حقوق الافراد و اليات الوصول الى بياناتهم وإمكانية تصحيحها و حذفها او نقلها و كذلك تتضمن هذه اللوائح التراخيص و التصاريح بأنواع الأنشطة التي تتطلب ترخيصاً و اليات الرقابة و التفتيش و العقوبات التي ترافق مخالفات تنفيذها ورسوم الترخيص [١]و تتمثل أهمية صدور هذه اللوائح في سد الفراغ التشريعي و تفصيل الاحكام العامة التي قد يترك توضيحها الى صدور لائحة تنظيمية مثالها قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠ الذي أحال اكثر من ١٨ قيد الى اللائحة إضافة لذلك تبرز أهمية هذه اللوائح الى توحيد المعايير الفنية و الإجرائية و تعزيز الحماية للبيانات الحساسة و تفعيل العقوبات و الرقابة إضافة الى التنظيم المؤسسي مثل شروط تعيين مسؤول حماية البيانات و الاطار الترخيصي ورسوم اصدار الترخيص أما الجهات المسؤولة عن إصدارها بالوزارات التي فهي عادةً ماتعنى بالاتصالات او تكنلوجيا المعلومات ٠

بالتالي يتبين لنا ان اصدار هذه اللوائح او التعليمات بأختلاف مسمياتها ليس أجراء بيروقراطي بل هو ضرورة حتمية يضمن الوضوح القانوني وحماية عملية عبر وضعه لمعايير تقنية صارمة ٠

وكذلك تتضمن الحماية الإجرائية بالالتزام بتدريب الكوادر والتوعية ونشر ثقافة ضرورة حماية البيانات وتدريب الكوادروالموظفين على ذلك حيث يمكن للإدارة ان تخلق بيئة يدرك فيها الجميع أهمية الحفاظ على البيانات الشخصية و مواجهة أساليب التزييف العميق التي تلحق بيناتهم اضرار تلحق بهم مخاطر اجتماعية و اقتصادية و أمنية ، ويكونون مستعدين لأ تخاذ الإجراءات الصحيحة للوقاية والاستجابة وبالتالي تعزيز حصانة شاملة لهم من التهديدات المتطورة وذلك عبر التدريب المستمر والمنتظم للكوادر و نشر التوعية و التثقيف بين افراد المجتمع في هذا المجال ، حيث ان غالباً ما تستغل الهجمات الالكترونية ضعف المعلومات لدى الفرد مما يجعل التهديدات الداخلية مصدر قلق كبير فيجعل من الموظفين خط الدفاع الأول ضد المجرمين الالكترونيين [٢] وتبرز أهمية التدريب في توعية الموظفين

[١] مشروع اللائحة التنفيذية ، استناداً لأحكام (٢٦) من قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ وكذلك المرسوم السلطاني رقم (٢) لسنة ٢٠٢٢ والمرسوم الاماراتي بالقانون الاتحادي رقم ٤٥ لسنة ٢٠٢١ على سبيل المثال ٠

[٢] استراتجية حماية البيانات العناصر الرئيسية وافضل الممارسات مقال منشور

بمخاطر تزييف البيانات واهمية استخدام كلمات مرور قوية و السلامة عند تبادل المعلومات عبر الوسائل الالكترونية و الإبلاغ عن الحوادث ٠

كذلك مما يبرز أهمية التدريب انه يساعد على خلق ثقافة مؤسسية تحترم خصوصية الفرد وحقوقهِ في بياناتهِ ويستخدم كأساس لترسيخ حماية البيانات ضمن بيئة العمل [١] ويتم ذلك من خلال تنظيم ورش عمل و ندوات دورية لرفع الوعي بأحدث المتطلبات و المعايير التنظيمية بما يعزز قدرة الموظفين على التعامل مع نظم الحماية البيانات الشخصية [٢]بالإضافة لذلك تلجأ الإدارة في سبيل توفير الحماية لنظم البيانات الشخصية الى نشر الوعي و التثقيف التي تعتبر عامل أساسي في حماية الامن المعلوماتي و الحد من المخاطر المتعلقة بانتهاك البيانات الشخصية هي التوعية المجتمعية ويتم ذلك من خلال تعزيز الوعي العام ومحو الامية الإعلامية بدأ من التعليم المبكر من اجل تزويدالافراد بالمهارات اللازمة للتمييز بين المحتوى الحقيقي و المزيف و تثقيف الجمهور بمخاطر التزييف العميق واهمية الحفاظ على بياناتهم وكيفية اكتشاف التقنيات الخبيثة و تزويدهم بالمعرفة الضرورية للاستدلال و التحقق من صحة تلك المعلومات المشتركة عبر المنصات الالكترونية [٣] ٠

وعادة يقع دور نشر ثقافة الوعي بين افراد المجتمع على عاتق الجهات الإعلامية لمواجهة إساءة استخدام تطبيقات الذكاء الاصطناعي و تظليل البيانات الشخصية فقد لعبت شركات الاعلام العالمية دوراً كبيراً في سبيل مواجهة تقنية التزييف العميق حيث اطلقت شركة الاعلام نيويورك تايمز بالتعاون مع شركة ادوبي (Adobe)و شركة أكس (تويتر سابقاً) مبادرة اصالة المحتوى وكذلك للصحافة دور في مكافحة هذه الظاهرة من خلال قيام الصحفيين بأعتماد معايير موحدة يتم تطبيقها على الصناعة الرقمية للتحقق من اصالة المحتوى ، وذلك من خلال تقديم دليل للمشاهدين على صحة ما ينشرون و تبني أسلوب سيفت (SIFT)وهو عبارة عن اختصار كلمات (توقف – تتحقق – ابحث – اعثر على المصدر)وهذه سلسلة الإجراءات التي تحتم على الصحفي قبل نشرهِ للأخبارمن ينعكس على نشر محتوى صحيح وليس مزيف [٤] ٠

---

https://www.ibm.com/sa-ar/think/insights/data-protection-strategy

تاريخ زيارة الموقع ٢٠٢٥/٨/١٠

[١] دورات ادارة تقنية المعلومات ، التدريب الداخلي للموظفين على نظم حماية البيانات الشخصية متاح على الموقع الالكتروني https://mercury-training.com/ar/%D8%A5%D8%AF%D8%A7%D8%B1%D8%A9-%D8%AA%D9%82%D9%86%D9%8A%D8%A9-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA.html

تاريخ زيارة الموقع ٢٠٢٥/٨/١٢

[٢] الاكاديمية الداخلية للتدريب و التطور دورة متقدمة في حماية البيانات الشخصية https://batdacademy.com/ar/course-details تاريخ زيارة الموقع ٢٠٢٥/٨/١٢

[٣] د ٠ سامح محمد محد ، مصدر سابق ، ص ٣٩٩٣ ٠

[٤] معالجة التزييفات العميقة في الصحافة مقال على الموقع الالكتروني

الفرع الثالث

اجراءات الإدارة في فرض الجزاءات

بعد عرضنا لأليات الحماية التقنية والتنظيمية التي تستعين بها الإدارة في سبيل توفير حماية للبيانات الشخصية لابد من التعرض لسلطة الإدارة في فرض الجزاءات التي تمكنها من فرض الالتزام بقوانين الحماية ففي فرنسا تمتلك اللجنة الوطنية للمعلوماتية و الحرية (CNI) تمتلك أدوات متعددة في سبيل ضمان حماية البيانات ابتداً من اصدار التحذيرات الى الغرامات المالية الكبيرة في حالة تلقيها للشكاوي حول الانتهاكات التي تضر بالبيانات الشخصية والتأكد من ثبوتها و تلزم المؤسسات بضرورة الامتثال للتشريعات ويتم ذلك على شكل انذار مكتوب للمؤسسات لتعديل ممارساتها خلال مدة محددة قبل فرض الغرامة كأمر تصريح فوري بحذف البيانات التي حجبها بشكل غير قانوني **أو** تعليق تلك الأنظمة من اللائحة العامة حماية البيانات [١] كما تلجأ الى فرض غرامات مالية و التي تكون على مستويين **الأول** يصل الى (١٠ ملايين يورو) أو ٢ % من حجم الاعمال السنوي العالمي (أيهما أعلى) وتفرض في حالات كأنتهاك شروط الموافقة المسبقة لمعالجة البيانات أو عدم الإبلاغ عن الخروقات اما المستوى **الثاني** يصل الى (٢٠ مليون يورو) أو ٤ % من حجم الاعمال السنوي (أيهما أعلى) للمخالفات الأشد كما في حالة نقل البيانات الى دول خارج الاتحاد الأوربي دون ضمانات كافية[٢] ،إضافة الى الجزاءات المالية تفرض اللجنة الوطنية الفرنسية (CNIL) جزاءات تبعية حيث لها ان تصدر أمر بوقف معالجة البيانات أو حذفها إضافة الى سلطتها في فرض الجزاءات التكميلية كالنشر العلني للعقوبات حيث تلزم الجهة المخالفة بنشر قرار العقوبة على موقعها الالكتروني أو في وسائل الاعلام وحسب الشهادات و الاعتمادات كجزاء تكميلي اذا ثبت عدم فاعلية شهادات الأمان على سبيل المثال [٣]، وتستند اللجنة الوطنية (CNIL) عند فرض الجزاءات تبعا لخطورة الانتهاك عدد المتضررين القصد من المخالفة ان كان عمدي او اهمال و مدى التعاون مع التحقيقات او الإجراءات الوقائية التي اتبعتها المؤسسات في سبيل توفير الحماية للبيانات من المخاطر ،اما في مصر فان مركز حماية البيانات الشخصية يملك سلطة في فرض الجزاءات الإدارية حسب قانون ١٥١ لسنة ٢٠٢٠ فلهو في سبيل ذلك اصدار انذار كتابي للمخالف بإزالة مخالفتهِ خلال مهلة معينة وفي حال عدم الامتثال لذلك يفرض جزاءاً بتعليق الترخيص جزئياً أو كلياً أو سحب الترخيص و الغاء الاعتماد و يلجأ مركز حماية البيانات المصري الى فرض غرامات مالية بين (١٠٠,٠٠٠ الف

---

https://share.google/zqBBchy1PrTJZliOm تم زيارة الموقع بتاريخ ٢٠٢٥/٨/١٦

[١] م (٥٨) من الائحة العامة لحمايات البيانات ،ترجمة د٠مصطفى عبيد ،الاتحاد الأوربي(البرلمان الأوربي والمفوضية الاوربية) اللائحة العامة لحماية البيانات ، مصدر سابق ،ص ٦٠ ٠

[٢] م (٨٣) من الائحة العامة لحمايات البيانات ،ترجمة د٠مصطفى عبيد ،الاتحاد الأوربي(البرلمان الأوربي والمفوضية الاوربية) اللائحة العامة لحماية البيانات ، مصدر سابق ،ص ٧٦

[٣] الاطار القانويني لحماية البيانات ا في الاتحاد الأوربي

https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data- protection_en

تاريخ زيارة الموقع ٢٠٢٥/٨/٢٠

جنيه – ٥,٠٠٠,٠٠٠ ملايين جنيه) تبعاً لنوع المخالفة وشدتها [١] ، إضافة الى ذلك يملك المركز جزاءات تكميلية كالنشر العلني في وسائل الاعلام وعلى النفقة الخاصة للمخالف وكذلك بإخضاع المخالف لأشراف المركز لضمان الامتثال وعلى نفقة المخالف إضافة الى ذلك يملك المركز سلطة سحب الشهادات و الاعتمادات كجزاء أداري تكميلي يلغي بواسطتهِ الترخيص بمعالجة البيانات الحساسة كالبيانات الصحية و المالية اذا ثبت عدم توافق ذلك مع الإجراءات الأمنية اما في العراق نظراً لعدم وجود قانون مخصص لحماية البيانات الشخصية مما يعني غياب الجزاءات الإدارية وانما يقتصر على الجزاءات الجنائية الواردة في قانون العقوبات رقم ١١١ لسنة ١٩٦٩ الذي يجرم افعالاً مثل افشاء الاسرار او التصنت [٢] ٠

في نهاية المبحث تبين لنا ن الحماية الإدارية للبيانات الشخصية من مخاطر التزييف العميق تتطلب اطارا متكاملا من الاليات يجمع بين وجود تشريع موحد وصارم وهيئة متخصة تضطلع بمهام الحماية الامنة للبيانات الشخصية مع اتباع إجراءات وتدابير تقنية وتنظيمية وصولاً لوضع ضمانات تنفيذ تلك الإجراءات بفرض جزاءات إدارية تستعين بها الإدارة عن وجود مخالفات ،بالرجوع الى التشريع العراقي نظراً لعدم وجود تشريع مخصص لتوفير حماية صارمة للبيانات الشخصية من مخاطر التزييف العميق انعكس سلبا على إمكانية الإدارة في توفير تلك الحماية وضمان الامتثال و احترام القانون على خلاف الدول المقارنة ، لذا ندعو المشرع الى ضرورة توفير حماية للبيانات الشخصية في ظل المخاطر التقنية كالتزييف العميق المتطورة التي تمثل بيانات الافراد بمثابة وقود لها ٠

الخاتمة

في نهاية دراسة بحثنا لموضوع (الحماية الإدارية للبيانات الشخصية من مخاطر التزييف العميق) استبان لنا انه في ظل العصر الرقمي الذي نعيشه فرض على الجهات الإدارية تحديات تتعلق بحماية البيانات الشخصية وأصبحت تلك الحماية ضرورة ملحة في ظل التطور المتسارع لتقنيات الذكاء الاصطناعي ولاسيما تقنية التزييف العميق التي تعد من اخطرها فالتطور المذهل المرتبط بأنشاء محتوى مزيف شديد الاقناع يعتمد أساسا في انشائه على استغلال البيانات الشخصية ليتحول الى أداة للتهديد وتقويض الثقة المجتمعية فقد أظهرت لنا الدراسة ان حماية البيانات تتطلب نهج متكامل مما يقتضي إيجاد منظومة تشريعية وهيئات مختصة ومع إيجاد اليات اليات تقنية وتنظيمية تتكيف لمواكبة التقنيات المتطورة ومن ذلك خلصنا الى مجموعة من الاستنتاجات والمقترحات نعرضها تبعا

أولا :- الاستنتاجات

١- يعد بياناً شخصياً و يخضع للحماية القانونية كل بيان يرتبط بالشخص و يساعد على التعرف على هويته كأسمهِ و لقبه و عنوانه و معلوماته الاسرية وجنسيته ، ويترتب عليه أن البيانات الشخصية هي كل ما يتوافق مع المعلومات سواء كانت هذه المعلومات عامة أو خاصة أو مهنية أو غيرها تؤدي الى التعرف على الشخص المعني ٠

[١] المواد للفصل الرابع عشر من قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ المواد من (٣٥ – ٤٦) ٠

[٢] المادة (٤٣٧) من قانون العقوبات العراقي (يعاقب بالحبس مدة لاتزيد عن سنتين وبغرامة لاتزيد على مائتي دينار او بأحدى هاتين العقوبتين كل من علم بحكم وظيفته او صناعته او فنه او طبيعة عمله بسر فأفشاه في غير الأحوال المصرح بها قانونا ٠٠٠٠)

٢ – تبين لنا المشرع في قوانين حماية البيانات الشخصية قد صنف البيانات الى عامة (غير حساسة) وهي كل مايتعلق بالاسم او الوظيفة او البريد الالكتروني والى البيانات الحساسة وهي كل ما يتعلق بمعلومات الشخصية الصحية او الجينية او البيومترية (الحيوية) ومعتقداته الدينية وتوجهاته السياسية مع اضافة الى ذلك حرص المشرع على توفير حماية خاصة وصارمة عند معالجة البيانات الحساسة والوصول اليها لما تلحق بالفرد من اضرار بالغة عند التلاعب بها او تزييفها مع الإشارة الى تحديد تلك البيانات على سبيل الحصر لا المثال بموجب قوانين حماية البيانات ٠

٣– تقنية التزييف العميق هي احدى تقنيات الذكاء الاصطناعي التي تقوم على أساس انشاء محتوى رقمي مزيف من صور او صوت او فيديو أو كيلهما لشخص او حتى النصوص تحاكي الواقع و تخالف الحقائق في ذات الوقت لأغراض غير مشروعة بقصد الاضرار بهِ ، عبر اعتمادها على شبكتيين في عملها وتعبر البيانات الشخصية وقود لهذه التقنية وتستند تقنية التزييف العميق في عملها أساليب متعددة منها مايتعلق بتزييف المحتوى الفيديوي للشخص او الصوتي او صوره٠

٤ – ينطوي على تزييف البيانات الشخصية اثار على المستوى الفردي وعلى المستوى الاجتماعي فعلى مستوى الفرد بقصد الاضرار بسمعته واثره عليه بعدم حصوله على وظيفة او ترقية عمل او ابتعاد الناس مع التعامل معه او بقصد الاحتيال والابتزاز مقابل الحصول على الأموال او التشهير به عبر نشر مقاطع وصور مزيفة عنه اما على المستوى الاجتماعي يؤدي الى زعزعه الثقة في وسائل الاعلام والمصادر الرسمية ويؤثر على الرأي العام ذلك نتيجة نشر معلومات مضللة عن الناس وتصريحات كاذبة إضافة الى استغلال البيانات المزيفة لأغراض إجرامية ٠

٥– الحماية الموضوعية للبيانات الشخصية وتحصينها من مخاطر التقنيات العميقة تتطلب إيجاد تشريعات موحدة لتوفير الحماية وانشاء هيئات مختصة من جهة وتشريعات لمواجهة خطر تقنية التزييف العميق ومركز مخصصة مزودة بتقنيات عالية وبتنسيق حكومي من جهة أخرى ٠

٦– تبين لنا ان على مستوى التشريع العراقي بعدم وجود تشريع موحد صدر لحد الان مخصص لحماية البيانات الشخصية رغم التطور التكنلوجي في تطبيقات الذكاء الاصطناعي على خلاف ما وجدنا بالدول المقارنة كالتشريع الفرنسي والمصري ٠

٧– تبين لنا عدم وجود هيئة مخصصة لحماية البيانات على غرار االهيئة الوطنية للمعلومات و الحريات (CNIL) في فرنسا والمركز القومي في مصر ٠

٨– ان للإدارة مجموعة من الاجراءات التقنية في سبيل حماية البيانات من التزييف العميق والتي تنوعت مابين حماية البيانات كالتشفير واستخدام تقنيات مقاومة للفيروسات وإجراءات تقنية لمواجهة التقنيات العميقة كالكشف المكبر عن المحتوى المزيف إضافة الى مساهمة الجهات الحكومية والمؤسسات الإعلامية والاكاديمية في سبيل ذلك ٠

٩– ان للإدارة مجموعة من الإجراءات التنظيمية منها اصدار اللوائح بالاستناد الى التشريعات الخاصة بحماية البيانات إضافة الى الاهتمام بالجانب التدريبي للكوادر بأعتبارهم خط الدفاع الأول الى جانب توعية وتثقيف افراد

المجتمع بأهمية حماية البيانات كأعتماد ارقام مرور قوية عند حفظ بيانتهم حتى ويكونون مستعدين لأتخاذ الإجراءات الصحيحة للوقاية والاستجابة وبالتالي تعزيز حصانة شاملة لهم من التهديدات المتطورة

٩- في سبيل توفير حماية للبيانات الشخصية لسلطة الإدارة في فرض الجزاءات التي تمكنها من فرض الالتزام بقوانين الحماية والتي تنوعت مابين فرض الغرامات المالية إضافة الى الجراءات التكميلية كسحب الترخيص والنشر العلني في وسائل الاعلام للمخالف وعلى نفقته الخاصة ٠

ثانيا :- المقترحات

١-لعل او ما نقترح هو ضروة الإسراع بإصدار تشريع موحد خاصة بحماية البيانات الشخصية على غرار التشريعات المقارنة يوضح فيه حقوق والتزامات كل من المعالج وصاحب على وجه الدقة مع الاخذ بالنموذج الفرنسي كونه يمثل اكثر تطورا في هذا المجال ٠

٢- ندعو المشرع الى ضروة اصدار تشريع لمواجهة تقنيات الذكاء الاصطناعي ولاسيما التزييف العميق او الإسراع بأكمال مشروع قانون الجرائم الالكترونية مع ضروة ادخال تعديلات عليه تتضمن مواجهة تقنية التزييف العميق عبر وضع مفهوم موحد وضع إجراءات صارمة للحد من استخدامات هذه التقنية ٠

٣-ضرورة انشاء هيئة متخصصة مستقلة لحماية البيانات (الهيئة الوطنية المستقلة لحماية البيانات الشخصية) وتكون ذات صلاحيات عند اجراء أي معالجة او تعديل على البيانات من اجل حماية حقوق الافراد ، على ان تحدد تلك الصلاحيات بموجب قانون حماية البيانات الشخصية يصدر لهذا الغرض

٤-ندعوالى انشاءمركز لمكافحة الجرائم الالكترونية (المركز الوطني لمكافحة التقنيات والجرائم الالكترونية) لمواجهة هذا النوع من الجرائم عبر تجريم انشاء او تداول محتوى مزيف Deep Fake وفقاً للقانون ويكون على مستوى من التنسيق بين الوزارات والجهات المعنية كالاتصالات والداخلية والتخطيط والامن الوطني ٠ كما هو الحال في الدول المقارنة ٠

٤-ندعو الى ضروة نشر التوعية المجتمعية وتعزيز الوعي العام في محو الامية الإعلامية وذلك عبر وسائل الاعلام ومواقع التواصل الاجتماعي من اجل التمييز بين المحتوى المزيف والحقيقي لمواجهة إساءة استخدام هذه التقنيات ونشر ثقافة حماية البيانات الشخصية مع ضروة الالتزام بالتحقق من المعلومة قبل نشرها لما يلحق بالضحية من اضرار بالغة ٠

المصادر

أولا :- الكتب

١-احمد حازم مصطفى ، تقنية المعلومات ، هيئة المعرفة و التنمية البشرية ، دبي ، ٢٠١٥ ٠

٢- احمد عبد الموجود زكير ، جريمة التزييف الاباحي ، دراسة مقارنة ، بحث منشور ، المجلة القانونية ،كلية الحقوق، جامعة القاهرة ، فرع الخرطوم ، مجلد ١١ ، عدد٧ ، ٢٠٢٢ ٠

٣- احمد محمد البوشي ، الابتزاز الالكتروني مفهوم جديد في جرائم التهديد المعلوماتية ، دراسة تفصيلية في ضوء قانون العقوبات و قانون مكافحة جرائم تقنية المعلومات رقم ٧٥ لسنة ٢٠١٨ ، دار النهضة العربية ، ٢٠٢٢ ٠

٤- د٠ اشرف السعيد احمد ، تكنلوجيا المعلومات في المجال الأمني ، القاهرة ، ٢٠١٣ ٠

٥- د٠ باسم محمد فاضل ،التحديات القانونية لتقنية التزييف العميق (deep fake) ، دراسة تحليلة مقارنة ، الطبعة الأولى ، دار الفكر الجامعي ، مصر ، ٢٠٢٥

٦- حسام الدين الاهواني ، الحق في الخصوصية (دراسة مقارنة) ، دار النهضة العربية ، دون سنة نشر ٠

٧- رشيد حمد علي حمد ، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الانترنت ، دراسة مقارنة ، دار النهضة العربية ، القاهرة ، ٢٠١٣ ٠

٨- د٠شريف فتحي الشافعي ، تخطيط و تصميم و تركيب شبكات الحاسب الالي ، دار الكتب العلمية للنشر و التوزيع ، القاهرة ، ٢٠٠٢ ٠

٩- د٠ شريف يوسف خاطر ، حماية الحق في الخصوصية المعلوماتية ، دراسة مقارنة ، دار الفكر و القانون ، جامعة المنصورة ، سنة ٢٠١٥ ٠

١٠- د٠ صدام فيصل كوكز ، التزييف العميق تقنيات معقدة واشكاليات قانونية ، دار هاتريك للطباعة و النشر و التوزيع ، الطبعة الأولى ، أربيل ، ٢٠٢٥ ٠

١١- د٠ منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت، ٢٠١٦

ثانيا :- البحوث

١- احمد عبد الموجود زكير ، جريمة التزييف الاباحي ، دراسة مقارنة ، بحث منشور ، المجلة القانونية ،كلية الحقوق، جامعة القاهرة ، فرع الخرطوم ، مجلد ١١ ، عدد٧ ، ٢٠٢٢ ٠

٢- د٠ احمد مصطفى معوض محمد ، استخدامات الذكاء الاصطناعي وتقنية التزييف العميق في قذف الغير انموذجاً دراسة مقارنة معاصرة ، بحث منشور في مجلة البحوث الفقهية و القانونية ، كلية الشريعة و القانون ، دمنهور ، جامعة الازهر ، المجلد ٣٤ ، العدد ٣٩ ، أكتوبر ، ٢٠٢٢ ٠

٣- بن شهب أسماء ، حماية البيانات الشخصية للمستخدم في اطار عقود الحوسبة السحابية ، بحث منشور ، مجلة الفكر القانوني و السياسي ، كلية الحقوق ، جامعة الاخوة منتوري – قسطنطينية ، المجلد التاسع ، العدد الأول ، ٢٠٢٥ ٠

٤- رانيا سليمان أبو المعاطي محمود / نهى محمد إبراهيم الدسوقي / فاتن فائز حميده الصفتي ، سياسة مكافحة الإرهاب الالكتروني ، مصر و السعودية نموذجا ، بحث منشور المركز العربي للبحوث و الدراسات افاق سياسية ، العدد ٥٣ ، ٢٠٢٠ ، ص ٥٢- ٥٣ يحيى دهشان ، المسؤولية الجنائية عن جرائم الذكاء الاصطناعي ، مجلة التشريعية والقانون ، الامارات ، مجلد ٣٤ – العدد ٨٢ ، ابريل ، ٢٠٢٠ ٠

٥- د٠رباب مصطفى عبد المنعم الحكيم ، الجوانب القانونية للتزييف العميق ، بحث منشور ، مجلة البحوث الفقهية و القانونية ، العدد ٤٨ ، اصدار يناير ، ٢٠٢٥ ٠

٦- د٠رضا إبراهيم عبد الله البيومي ، الحماية القانونية من مخاطر التزييف العميق ، دراسة تحليلية مقارنة ، بحث منشور ، مجلة ، روح القوانين ، كلية الحقوق ، جامعة طنطا ، عدد خاص ، المؤتمر الدولي الثامن لتكنلوجيا والقانون ٠

٧- د٠سامح عبد الواحد التهامي ،الحماية القانونية للبيانات الشخصية دراسة في القانون الفرنسي (القسم الأول) بحث منشور ، كلية الحقوق ،جامعة الزقازيق ٢٠١٠ ٠

٨- د٠سامح محمد محمد السيد إبراهيم ، المخاطر الأمنية و المجتمعية للتزييف العميق و اليات المواجهة ، بحث منشور ، المجلة القانونية ((ISSN 2537-0758، جامعة نايف للعلوم الأمنية ٠

٩- سحر فؤاد مجيد االنجار ، المواجهة الجنائية للجرائم الناشئة عن استخدام التزييف العميق ، بحث منشور ، مجلة العلوم القانونية ، جامعة بغداد ،كلية القانون ، المجلد ٣٩ ، العدد الثاني ، ٢٠٢٤ ٠

١٠- سمير سعد رشاد سلطان ، الحماية القانونية للبيانات الحساسة في مجال الاستدلال (دراسة مقارنة) ، بحث منشور ،مجلة البحوث القانونية و الاقتصادية ، عدد ٨٨ ، يونيو ٢٠٢٤ ٠

١١- د٠شريف يوسف خاطر، حق الاطلاع على البيانات الشخصية ، بحث منشورفي مجلة كلية القانون الكويتية العالمية ٠

١٢- صبرية جدي ، الحماية القانونية للحق في الخصوصية المعلوماتية ، بحث منشور ، مجلة التواصل في الاقتصاد و الإدارة و القانون ، كلية الحقوق و العلوم السياسية ، جامعة باجي مختار ، عنابة ، المجلد ٢٤ ، العدد ٢ ، اوت ٢٠١٨ ٠

١٣- د٠طارق جمعة السيد راشد ، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي ، بحث منشور ، مجلة القانون و الاقتصاد ، ملحق خاص ، العدد ٩٢ ٠

١٤- د٠طارق جمعة السيد راشد ،الحماية القانونية للحق في خصوصية البيانات الجينية (دراسة تحليلية مقارنة)، بحث منشورفي المجلة القانونية ، كلية الحقوق ، جامعة القاهرة ، العدد ١٢ / مجلد ٨ ، لسنة ٢٠٢٠ ٠

١٥- علاء الدين منصور مغيابيرة ، جرائم الذكاء الاصطناعي وسبل مواجهتها ، جرائم التزييف العميق نموذجاً ، بحث منشور ، المجلة الدولية للقانون ، جامعة قطر ، المجلد ١٣ / العدد المنتظم الثاني ،٢٠٢٤ ٠

١٦- كحلاوي عبد الهادي – بن زيطة عبد الهادي ، السلطة الإدارية المستقلة لحماية البيانات الشخصية ، دراسة مقارنة بين القانونين الفرنسي و الجزائري ، بحث منشور في المجلة الجزائرية العلوم و القانون و السياسة ، المجلد ٥٩ ،العدد ٢،السنة ٢٠٢٢ ، ص ١٢٧

١٧-د٠ محمود حسين سيد أبو سيف ، التنظيم القانوني للتزيف العميق في قانون الذكاء الاصطناعي الصادر عن الاتحاد الأوربي ،بحث منشور ،مجلة العلوم القانونية والاقتصادية العدد الأول ، السنة ٦٧، يناير، ٢٠٢٥

١٨- د٠ محمود سلامة عبد المنعم الشريف ، جريمة الاباحي عبر تقنية التزييف العميق و المسؤولية الجنائية عنها ، بحث منشور في المجلة العلمية لبحوث الصحافة ، جامعة القاهرة ، كلية الاعلام ، العدد ٢٤ ، الجزء الثالث ، يوليو ٢٠٢٢ م ٠

١٩- منة الله كمال موسى ذياب ، سلوك حماية الخصوصية الرقمية البيومترية لدى مستخدمي تطبيقات التويف العميق ، بحث منشور ،المجلة العربية لبحوث الاعلام و الاتصالات ، كلية الاعلام ، جامعة الكندية،القاهرة، العدد ٣٧ ، ابريل ، ٢٠٢٠

٢٠- ولاء محمد محروس الناغي / د٠ ياسر محمود الناغي ، ادراك مستخدمي التواصل الاجتماعي لتهديدات التزييف العميق وعلاقته باستخدام الامن لتلك المواقع ، بحث منشور ، المجلة العلمية لبحوث الصحافة ، كلية الاعلام ، جامعة القاهرة ، العدد ٢٤ ، الجزء الثالث ، يوليو ، ٢٠٢٢ ٠

ثالثا: المقالات والمواقع الالكترونية

١- استراتجية حماية البيانات العناصر الرئيسية وافضل الممارسات مقال منشور

https://www.ibm.com/sa-ar/think/insights/data-protection-strategy

٢- الاطار القانويني لحماية البيانات في الاتحاد الأوربي

https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en

٣- تصنيف المخاطر الأربعة لقانون الذكاء الاصطناعي في الاتحاد الأوربي هل شركتك مستعدة مقال منشور على الموقع الالكتروني https://www.fticonsulting.com/insights/fti-journal/four-risks-eus-artificial-intelligence-act

٤- التطورات والتحيلات الحديثة لقانون الذكاء الاصطناعي للاتحاد الأوربي منشور على الموقع الالكتروني https://artificialintelligenceact.eu/article/3/

٥- دورات ادارة تقنية المعلومات ، التدريب الداخلي للموظفين على نظم حماية البيانات الشخصية متاح على الموقع الالكتروني

https://mercury-training.com/ar/

٦- سالي يوسف ، كيف نواجة استخدام الذكاء الاصطناعي في التضليل المعلوماتي (استخدام تقنية deep fake لتزييف الفيديوهات)، مقال منشورفي موقع مركز المستقبل للأبحاث و الدراسات المقدمة ، القاهرة ، ٢٠٢٢ ، https://futureuae.com/ar-AE/Mainpage/Item

٧- سياسة الخصوصية و حماية الحياة الخاصة مقال منشور على موقع السفارة الفرنسية في البحرين

https://bh.ambafrance.org/

٨- قانون الاتحاد الأوربي للذكاء الاصطناعي رقم ١٦٨٩/ ٢٠٢٤ منشور على الموقع الالكتروني https://share.google/NXZ1kPKgs3Qtg7kRY تم زيارة الموقع ٧/٧/ ٢٠٢٥٨- قانون ٢٠٢٤ قانون تعديل لائحة الاتحاد الأوربي للبرلمان الأوربي النسخة الالكترونية منشور على موقع الاتحاد الأوربي يورو -ليكس http://data.europa.eu/eli/reg/2024/1468/oj

٩- المركزالأوربي لدراسات مكافحة الإرهاب و الاستخبارات المانيا و هولندا

https://www.europarabct.com/?=83399 ١٠-المركزالوطني للامن السيبراني،الحماية من البرامج الضارة(الربمجيات الخبيثة) مقال على الموقع الالكتروني

https://www.ncsc.gov.bh/ar/cyberwiser/general-threats/protecting-against-malware.

١١- الاكاديمية الداخلية للتدريب و التطور دورة متقدمة في حماية البيانات الشخصية https://batdacademy.com/ar/course-details

١٢- الذكاء الاصطناعي والتزييف العميق : لوائح الاتحاد الاتحاد الأوربي وإيطاليا مقال منشور على الموقع الالكتروني https://www.jacobacci-law.com/news-and-publications/ai-and-deepfakes-eu-and-italian-regulations

١٣- مكافحة التزيف العميق /تقنية البلوك تشين كدلل على صحة الوسائط الرقمية مقال منشور على الموقع الالكتروني

http://data.europa.eu/eli/reg/2024/1468/oj

١٤- معالجة التزييفات العميقة في الصحافة مقال على الموقع الالكتروني

https://share.google/zqBBchy1PrTJZliOm

١٥- الوكالة الوطنية لأمن أنظمة المعلومات سلطة ANSSIعلى الموقع الالكتروني

https://www.orsys.fr/orsys-lemag/en/glossary-2/anssi-%F0%9F%9F%A9-authorit

رابعا :- التشريعات

١ - قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل

٢- القانون المعلوماتية والحريات الفرنسي رقم (٧٨-١٧) الصادر في ٦ يناير ١٩٧٨

٣ - قانون البطاقة الوطنية العراقي رقم ٣ لسنة ٢٠١٦

٤ - لائحة الاتحاد الأوربي GDPR لحماية البيانات ٢٠١٦ والنافذة ٢٠١٨

٥- قانون مكافحة جرائم تقنية المعلومات المصري ، رقم (١٧٥) لسنة ٢٠١٨

٦- مشروع قانون مكافحة الجرائم الالكترونية العراقي لسنة ٢٠١٩

٧- قانون حماية البيانات الشخصية المصري رقم ١٥١ في ٢٠٢٠

٨ - قانون ٢٠٢٤ قانون تعديل لائحة الاتحاد الأوربي لعام٢٠١٨

٩- مشروع اللائحة التنفيذية من قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠

١٠- المرسوم الفرنسي رقم ٥٣٦ /٢٠١٩الصادر في ٢٩مايو ٢٠١٩

١١- قانون الاتحاد الأوربي للذكاء الاصطناعي رقم ١٦٨٩/ ٢٠٢٤ الصادر عام ٢٠٢٤

خامسا :- الاتفاقيات والمعاهدات // -الاتفاقية العربية لمكافحة جرائم المعلومات لسنة ٢٠١٠

سادسا :- الكتب المترجمة

-الائحة العامة لحمايات البيانات ، ترجمة د٠ مصطفى عبيد ،الاتحاد الأوربي(البرلمان الأوربي والمفوضية الاوربية) اللائحة العامة لحماية البيانات ، موسوعة العلوم القانونية ، مركز البحوث والدراسات متعددة التخصصات ، الطبعة الأولى ، ٢٠١٨

سابعا:- المصادر الأجنبية

1- Aarti Karndikar, Vedtia Deshpande, Sanjann Singh, Sayail Nagbhidkar,Saurabh Agrawal,Deepfake video Detection using convolutional neural Network,International Joural of Advanced trends in computer Science and Engineering ,Volume 9 ,No 2 , March- April 2020

2-Chuck Eattom,Jeff Taylor Computer Crime–investigation an the law Course technology , 2010

3-Joëlle BEDEREDE,Données personnelles dans le cadre dun sit we ,étude disponible sur ,la date de mise en ligne ,2003

4- John R , Computer and in formation Security hand book , Second edition , A Msterdam , Elsevier , Morgan , Kaufm mehnn , 2013

5-Mariëtte van Huijstee, pieter van Boheemen,Djurre Das and etai,Tackling deepfakes in Eurpean policy,panel For the Future of science and techlingdeepfakes in Eurpean parliamentary Research Service,SCIENTIFIC Foresight unit (STOA),PE690.039-July ,2021

6- V.Jean-paul cost Aila tansparence ad Ministrative Regard sur L,actualitésptem ber- octobor – 1998