مجلة

تعنى بنشر البحوث والدراسات القانونية المتعلقة بتقنية المعلومات والعلوم الحديثة

مجلة علمية محكمة | العدد (10) | السنة الخامسة | رجب 1440 هـ | مارس 2019 م

ISSN 2312-5799

معهد دبي القضائي

العدد - 10 -

تعنى بنشر البحوث والدراسات القانونية المتعلقة بتقنية المعلومات والعلوم الحديثة | السنة السادسة | رجب 1440 هـ | مارس 2019 م | السعر: 30 درهما

الحماية القانونية للبريد الإلكتروني

أ.د. عابد فايد عبد الفتاح فايد

اميرات المراقبة التلفزيونية المغلقة CCTV كوسيلة للمراقبة السابقة على ارتكاب الجريمة لأغراض منع الجريمة وملاحقة مرتكبيها

الأستاذ الدكتور خالد موسى توني

هل ينبغي أن تضع الحكومة اللوائح والقوانين، فيما يتعلق بالذكاء الاصطناعي؟ نعم، هي تفعل ذلك بالفعل

كريستوفر فونزون كيت هينزلمان

هل ينبغي تنظيم الذكاء الاصطناعي؟

البروفيسور ديلاكروس

الاتحاد الأوروبي يناقش تنظيم الذكاء الاصطناعي، والقضايا القانونية المرتبطة به

ديريك دو بريز

www.dji.gov.ae

رؤيتنا

أن نكون مركزاً إقليمياً للتميز القانوني والعدلي

رسالتنا

تزويد أعضاء المجتمع القانوني بأفضل تدريب مهني والتطوير المستمر وإكسابهم المعرفة الحديثة ذات الصلة

معهد دبي القضائي
DUBAI JUDICIAL INSTITUTE

P.O.Box.: 28552 Dubai
United Arab Emirates
Tel.: 00971 4 20 54 112
: 00971 4 20 54 110
Fax: 00971 4 28 2 7071
Web:www.dji.gov.ae
research@dji.gov.ae

www. / DubaiJudicial

Google play App Store

معهد دبي القضائي

مجلة علمية محكمة | العدد (10) | السنة السادسة | رجب 1440هـ | مارس 2019م

رؤيتنا

أن نكون مركزاً إقليمياً للتميز القانوني والعدلي

رسالتنا

تزويد أعضاء المجتمع القانوني بأفضل تدريب مهني
والتطوير المستمر وإكسابهم المعرفة الحديثة ذات الصلة

معهد دبي القضائي
DUBAI JUDICIAL INSTITUTE

صندوق بريد: 28552 دبي
الإمارات العربية المتحدة
هاتف: 00971 4 20 54 112
00971 4 20 54 110
فاكس: 00971 4 28 27071
www.dji.gov.ae
research@dji.gov.ae

عن المجلة

«مجلة معهد دبي القضائي» تعنى بنشر البحوث والدراسات القانونية المتعلقة بتقنية المعلومات والعلوم الحديثة، مجلة علمية محكمة تقبل النشر باللغة العربية، والإنجليزية، والفرنسية. وهي مجلة يلفت مجال اهتمامها إلى طبيعة موضوعاتها حيث أضيفت عبارة تقنية المعلومات والعلوم الحديثة إلى كلمة قانونية بهدف الدلالة على طبيعة الموضوعات المكونة للبنيان الداخلي للمجلة.

وهذه الموضوعات هي المشكلات القانونية المعاصرة التي يتحتم بحثها في ضوء التقدم العلمي بطفرتيه: طفرة التقدم في مجال المعلومات وشبكة الاتصال، وطفرة التقدم في المجال البيولوجي.

إذن فعنوان المجلة جاء من السعة والشمول إلى حد كبير. فحصيلة التطورات العلمية سريعة ومتنوعة، وأبعادها وانعكاساتها على كافة فروع القانون لا فكاك منها.

والمجلة تتضمن الأبواب الآتية:

- البحوث والدراسات القانونية.
- الاجتهادات القضائية وتشمل:
  - التعليق على الأحكام.
  - المبادئ القانونية التي يرسيها القضاء الإماراتي والقضاء المقارن.
- النصوص القانونية المستحدثة.
- التقارير العلمية عن الندوات والمؤتمرات وورش العمل.
- عرض الرسائل الجامعية والكتب.

أولوية وترتيب النشر:

- الموضوعات المرتبطة بدولة الإمارات العربية المتحدة.
- تاريخ وصول البحث إلى مدير تحرير المجلة.
- تنوع موضوعات البحث.
- ترتيب البحوث في المجلة يخضع لاعتبارات فنية.

الأهداف:

1. تعزيز وتكريس ثقافة ومنهجية إجراء البحوث والدراسات القانونية المتعلقة بالعلوم والتقنية المتقدمة.
2. إثراء العمل القضائي بالبحوث والدراسات القانونية التي تعكس التطور التشريعي المواكب للتقدم العلمي، ما يعين القاضي في أداء عمله وتوسيع مداركه وزيادة حصيلته المعلوماتية.
3. العمل على تنشيط الاجتهاد في مجال الفقه والقضاء من خلال نشر الدراسات والبحوث والمقالات المعمقة والتعليقات على الأحكام ذات الصلة بانعكاسات التقدم العلمي.
4. إمداد المحاكم والنيابات العامة بالبحوث والدراسات التي تسهم في تطوير القضاء في إطار تعاون مثمر بين الفقه والقضاء.
5. الاهتمام بالدراسة القانونية المقارنة للقوانين وأحكام القضاء للاطلاع على الخبرات الأجنبية وطريقة معالجتها للمشكلات القانونية الناتجة عن انعكاسات وتأثير التقدم العلمي، مع مراعاة قيم المجتمع ومصالحه.
6. الاهتمام بدراسة التشريعات المكملة التي تعكس تجاوب المشرع مع التقدم العلمي بغرض رفع ما قد يكون من تناقض بين نصوصها أو بينها وبين غيرها من تشريعات، فالتحديث التشريعي لأي قانون يجب أن يكون نتاج تركيب علمي متناسق.
7. قيام المعهد بإحدى مهامه على وجه فعال وسريع في إمداد الدوائر المعنية بنتائج الدراسات والبحوث التي يمكن أن تفيد تلك الدوائر في تشخيص المشكلات التي يعكسها التقدم العلمي وتقديم الحلول المقترحة.. وخاصة في حالات الاستعجال، حيث يلزم سرعة التدخل التشريعي تحت تأثير هذا الاستعجال.
8. إثراء المكتبة القانونية بصفة خاصة والمكتبة العربية بصفة عامة، ليس فقط بالبحوث والدراسات المتعلقة بتقنية المعلومات والعلوم الحديثة، بل وبنتائج وتقويم هذه الدراسات في ضوء ما يسفر عنه التطبيق العملي.

قواعد النشر

النشر بالمجلة يتم وفقاً للقواعد التالية:

1. أن يتسم البحث بالعمق والأصالة والثراء المعرفي.
2. الالتزام بأصول البحث العلمي وقواعده العامة، ومراعاة التوثيق العلمي الدقيق.
3. يجب أن يكون البحث خالياً من الأخطاء اللغوية والنحوية، مع مراعاة الترقيم المتعارف عليه في الأسلوب العربي، وضبط الكلمات التي تحتاج إلى ضبط، وتقوم هيئة التحرير بالمراجعة اللغوية والتعديل بما لا يخل بمحتوى البحث أو مضمونه.
4. أن لا يكون البحث قد سبق نشره على أي نحو كان، أو تم إرساله للنشر في غير المعهد، ويثبت ذلك بإقرار من الباحث.
5. يقدم البحث مطبوعاً في نسختين، ويرفق به نسخة من الوعاء الإلكتروني المطبوع من خلاله.
6. ألا يزيد عدد صفحات البحث أو الدراسة على 40 صفحة من الحجم العادي (A4) ويجوز في بعض الحالات التغاضي عن هذا الشرط إذا كان تقسيم البحث إلى قسمين أو أكثر يؤدي إلى الإخلال بوحدة البحث.
7. يلتزم الباحث بعدم إرسال بحثه لأي جهة أخرى للنشر حتى يصله رد المجلة.
8. يرفق الباحث بحثه بنبذة عن سيرته العلمية، وعنوانه بالتفصيل ورقم الهاتف، والفاكس (إن وجد) والبريد الإلكتروني.
9. تخضع البحوث التي ترد إلى المعهد للتقويم والتحكيم من قبل المختصين للحكم على أصالتها وجديتها وقيمتها وسلامة طريقة عرضها، ومن ثم صلاحيتها للنشر من عدمها.
10. يمنح كل باحث خمس نسخ من العدد المنشور فيه بحثه.
11. يمنح المعهد مكافأة مالية للأبحاث التي تقرر صلاحيتها للنشر ويقوم المعهد بنشرها.
12. تصبح البحوث والدراسات المنشورة ملكاً لمعهد دبي القضائي، ولا يحق للباحث إعادة نشرها في مكان آخر دون الحصول على موافقة كتابية من المعهد.
13. للمعهد الحق في ترجمة البحث أو أجزاء منه وبما لا يخل بمحتوى البحث أو مضمونه متى اقتضت الظروف ذلك، وبما لا يخل بفحوى المادة العلمية.
14. أصول البحوث التي تصل إلى المجلة لا ترد سواء نشرت أو لم تنشر.
15. ترسل البحوث بعنوان مدير تحرير المجلة ص ب 28552 دبي، دولة الإمارات العربية المتحدة، أو على البريد الإلكتروني research@dji.gov.ae .

المحتويات

كشاف أعداد المجلة

م	البحث	اسم الباحث		الصفحات		بيانات النشر	لغة النشر
				من	إلى		
1	المسؤولية المدنية الناشئة عن الجريمة المعلوماتية في القانون الدولي الخاص.	أ.د. أحمد محمد أمين الهواري		16	52	العدد الأول / السنة الأولى / جمادى الآخرة 1433هـ/ مايو 2012	العربية
2	حجية المحررات الإلكترونية في الإثبات : تعليق على باكورة أحكام القضاء الدبوي.	أ.د. محمد محمد محمد أبو زيد		56	100	العدد الأول / السنة الأولى / جمادى الآخرة 1433هـ/ مايو 2012	العربية
3	تعليق على قضاء دبي بشان الاختصاص القضائي بجرائم الإنترنت	د. عبد الرازق الموافي عبد اللطيف		104	137	العدد الأول / السنة الأولى / جمادى الآخرة 1433هـ/ مايو 2012	العربية
4	النصوص القانونية المستحدثة: النصوص القانونية ذات الصلة بانعكاسات التقدم العلمي التي أدخلت على نصوص القوانين الرئيسة.	أ.د. محمد محمد محمد أبو زيد		140	147	العدد الأول / السنة الأولى / جمادى الآخرة 1433هـ/ مايو 2012	العربية
5	دعوة المشرع لرفع التعارض بين ثبوت النسب بالبصمة الوراثية ونفيه باللعان	أ.د. محمد محمد محمد أبو زيد		16	33	العدد الثاني / السنة الأولى / ربيع الثاني 1424هـ/ مارس 2013	العربية
6	عقد إيواء الموقع الإلكتروني دراسة مقارنة	د. طاهر شوقي محمد محمود		35	77	العدد الثاني / السنة الأولى / ربيع الثاني 1424هـ/ مارس 2013	العربية
7	التصويت الإلكتروني وأثره في ممارسة الديمقراطية	د. عبد الكريم محمد محمد السروي		78	137	العدد الثاني / السنة الأولى / ربيع الثاني 1424هـ/ مارس 2013	العربية
8	قراءة في قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة	د. عبد الرازق الموافي عبد اللطيف		139	186	العدد الثاني / السنة الأولى / ربيع الثاني 1424هـ/ مارس 2013	العربية
9	أضواء على نصوص المرسوم بشأن المسؤولية المدنية عن الأضرار النووية	أ.د. محمد محمد محمد أبو زيد		189	219	العدد الثاني / السنة الأولى / ربيع الثاني 1424هـ/ مارس 2013	العربية
10	تأملات في أحكام سند الشحن البحري الإلكتروني (مقال)	المستشار الأمين عثمان إسماعيل		221	230	العدد الثاني / السنة الأولى / ربيع الثاني 1424هـ/ مارس 2013	العربية
11	عقود التجارة الإلكترونية في القانون الدولي الخاص	أ.د. أحمد محمد أمين الهواري		15	72	العدد الثالث/ السنة الثانية / ذي القعدة 1424هـ/ سبتمبر 2013	العربية
12	حماية المستهلك الإلكتروني في العقد الإلكتروني	أ.د. ماجدة شلبي		75	164	العدد الثالث/ السنة الثانية / ذي القعدة 1424هـ/ سبتمبر 2013	العربية
13	الرقابة على محتوى الإنترنت	د. طاهر شوقي مؤمن		167	206	العدد الثالث/ السنة الثانية / ذي القعدة 1424هـ/ سبتمبر 2013	العربية

م	البحث	اسم الباحث		الصفحات من	الصفحات إلى	بيانات النشر	لغة النشر
14	باكورة الأحكام القضائية لمحكمة تمييز دبي في تطبيق تقنيات الإتصالات في قضايا الأحوال الشخصية	أ.د. محمد محمد محمد أبو زيد		209	217	العدد الثالث/ السنة الثانية / ذي القعدة 1424هـ/ سبتمبر 2013	العربية
15	حكم المحكمة الأمريكية العليا : تسريب معلومات سرية للتحايل في سوق الأوراق المالية	إعداد هيئة تحرير المجلة		219	232	العدد الثالث/ السنة الثانية / ذي القعدة 1424هـ/ سبتمبر 2013	العربية
16	المبادئ الرئيسة للمسؤولية المدنية عن الأضرار النووية	د. محمد السيد الدسوقي		18	65	العدد الرابع / السنة الثانية / رمضان 1435 هـ/ يوليو 2014م	العربية
17	الجريمة المعلوماتية: دراسة مقارنة بين القانونيين الليبي والإماراتي	د. رحاب علي عميش		66	103	العدد الرابع / السنة الثانية / رمضان 1435 هـ/ يوليو 2014م	العربية
18	تعليق على حكم محكمة القضاء الإداري المصرية في شأن حجب المواقع الإباحية	المستشار حسن البنا عبد الله عياد		104	145	العدد الرابع / السنة الثانية / رمضان 1435 هـ/ يوليو 2014م	العربية
19	حقوق البث الجزئي لمباريات كرة القدم فيما دون الوقت الكامل للمباراة	المستشار ستيوارت بيبوورث		146	158	العدد الرابع / السنة الثانية / رمضان 1435 هـ/ يوليو 2014م	العربية والإنجليزية
20	التخفي: نظرة متعمقة في شبكة تور (شبكة تخفي) وآثارها على أمن الحاسوب وحرية الرأي والتعبير في العصر الرقمي.	تشيلسي أيه لويس		24	107	العدد الخامس / السنة الثالثة/ جمادى الأولى 1436 هـ / فبراير 2015 م.	العربية والإنجليزية
21	المخاطر القانونية الدولية المتعلقة بالمصادر المفتوحة وحلولها المحتملة.	تشينج يو هو		111	163	العدد الخامس / السنة الثالثة/ جمادى الأولى 1436 هـ / فبراير 2015 م.	العربية والإنجليزية
22	تعليق حول حكم محكمة العدل الأوربية الصادر في 13 مايو 2014 بشأن الحق في اعتبار بعض الوقائع في طي النسيان.	الصالحين محمد العيش		168	178	العدد الخامس / السنة الثالثة/ جمادى الأولى 1436 هـ / فبراير 2015 م.	العربية
23	المسؤولية المدنية عن أضرار المنتجات الطبية المعيبة (دراسة مقارنة بين القانون الإماراتي والقانون الفرنسي).	د. رغيد عبد الحميد فتال د. أحمد سليمان		18	79	العدد السادس / السنة الثالثة/ صفر 1436 هـ / ديسمبر 2015 م.	العربية
24	القانون الواجب التطبيق على العقد الإلكتروني في التشريع الإماراتي.	د. زياد خليف العنزي		80	117	العدد السادس / السنة الثالثة/ صفر 1436 هـ / ديسمبر 2015 م.	العربية
25	شروط الإعلان التجاري عبر الإنترنت	د. طاهر شوقي مؤمن		118	143	العدد السادس / السنة الثالثة/ صفر 1436 هـ / ديسمبر 2015 م.	العربية

م	البحث	اسم الباحث		الصفحات من	الصفحات إلى	بيانات النشر	لغة النشر
26	حكم وقتي بشأن تدابير وقتية وتحفظية، صادر من قبل رئيس لجنة الطعون التابعة لمحكمة التحكيم الرياضية في دعوى التحكيم رقم 3861/أ/ 2014، المنظورة أمام محكمة التحكيم الرياضية.	حكم تحكيم صادر من قبل محكمة التحكيم الرياضية.		144	153	العدد السادس / السنة الثالثة/ صفر 1436 هـ / ديسمبر 2015 م.	العربية
27	دعوى التحكيم رقم 3488 / ت/ 2014 ، محكمة التحكيم الرياضية المرفوعة من قبل الوكالة العالمية لمكافحة المنشطات، ضد السيد / جوها لا لوكا.	حكم تحكيم صادر من قبل محكمة التحكيم الرياضية.		154	193	العدد السادس / السنة الثالثة/ صفر 1436 هـ / ديسمبر 2015 م.	العربية
28	دعاوى التحكيم: 3665 و 3666 و 3667 / ت / 2014 (محكمة التحكيم الرياضية) الدعوى المرفوعة من قبل لويس سواريز ونادي برشلونة لكرة القدم واتحاد أوروجواي لكرة القدم ضد الاتحاد الدولي لكرة القدم، حكم تحكيم صادر من قبل محكمة التحكيم الرياضية.	حكم تحكيم صادر من قبل محكمة التحكيم الرياضية.		194	227	العدد السادس / السنة الثالثة/ صفر 1436 هـ / ديسمبر 2015 م.	العربية
29	تدابير الأمم المتحدة لمكافحة استخدام الإنترنت لأغراض إرهابية: علاج جذري للمشكلة أم مجرد مسكن لها؟	د. ماهر إدريس البنا		18	48	العدد السابع / السنة الرابعة/ شوال 1437هـ/ يوليو 2016م.	العربية والإنجليزية
30	مستقبل حقوق الملكية الفكرية في مجال اللوحات المقتبسة من صور	تشينج يو هو		50	94	العدد السابع / السنة الرابعة/ شوال 1437هـ/ يوليو 2016م.	العربية والإنجليزية
31	حق الولي في إلزام الحاضنة بتمكينه من الرؤية الإلكترونية للمحضون عبر وسائل التواصل الاجتماعي.	أ.د. محمد عبد الرحمن الضويني		96	104	العدد السابع / السنة الرابعة/ شوال 1437هـ/ يوليو 2016م.	العربية
32	التعدي على العلامة التجارية لوي فيتون	حكم صادر من محكمة استئناف الولايات المتحدة الأمريكية - الدائرة التاسعة		106	120	العدد السابع / السنة الرابعة/ شوال 1437هـ/ يوليو 2016م.	العربية والإنجليزية
33	نزاع حول نطاق العلامة التجارية، Taylorgang.Com	مركز الويبو WIPO للتحكيم والوساطة		122	137	العدد السابع / السنة الرابعة/ شوال 1437هـ/ يوليو 2016م.	العربية والإنجليزية

م	البحث	اسم الباحث		الصفحات		بيانات النشر	لغة النشر
				من	إلى		
34	الشكلية الإلكترونية وحماية المستهلك في القانون الإماراتي والمقارن	الأستاذ الدكتور عابد فايد عبد الفتاح فايد		18	51	العدد الثامن/ السنة الخامسة/ ذو الحجة 1438 هـ / يوليو 2018 م	العربية
35	حماية المصنفات الرياضية وفقاً لقانون حقوق المؤلف والحقوق المجاورة الإماراتي رقم (7) لسنة 2002 والاتفاقيات الدولية ذات الصلة	د. عامر محمود الكسواني د. مراد محمود المواجدة		52	97	العدد الثامن/ السنة الخامسة/ ذو الحجة 1438 هـ / يوليو 2018 م	العربية
36	الأبعاد الدستورية للفضاء الإلكتروني: دراسة مقارنة	د. سيمون بدران		99	134	العدد الثامن/ السنة الخامسة/ ذو الحجة 1438 هـ / يوليو 2018 م	العربية
37	نزاع الطماطم	حكم المحكمة العليا بالولايات المتحدة الأمريكية		137	140	العدد الثامن/ السنة الخامسة/ ذو الحجة 1438 هـ / يوليو 2018 م	العربية والإنجليزية
38	الآثار القانونية للإنترنت على سيادة الدول: الاستقلالية الدستورية نموذجاً.	د. سيمون بدران		21	55	العدد التاسع/ السنة السادسة/ ذو الحجة 1439 هـ / سبتمبر 2018 م	العربية
39	في بصمة المخ وبصمة الحامض النووي DNA النظام الجنائي الإسلامي	د. الهاني طايع		57	116	العدد التاسع/ السنة السادسة/ ذو الحجة 1439 هـ / سبتمبر 2018 م	العربية
40	من الأحكام القضائية: حكم محكمة استئناف الولايات المتحدة الأميريكية الدائرة الثانية/ كريستيان لوبوتان إس إيه / ضد / إيف سان لوران أمريكا هولدينج: هل يصلح اللون الأحمر كعلامة تجارية؟.	حكم محكمة استئناف الولايات المتحدة الأميريكية الدائرة الثانية		119	148	العدد التاسع/ السنة السادسة/ ذو الحجة 1439 هـ / سبتمبر 2018 م.	العربية والإنجليزية
41	من الرسائل العلمية الجامعية ملخص مناقشة أطروحة الدكتوراة في القانون الجنائي المعنونة ب الجرائم المرتكبة عبر وسائل التواصل الاجتماعي - دراسة مقارنة -.	د. حوراء موسى		151	166	العدد التاسع/ السنة السادسة/ ذو الحجة 1439 هـ / سبتمبر 2018 م.	العربية

تقديم

بقلم: القاضي الدكتور جمال حسين السميطي
المدير العام رئيس التحرير

عزيزي القارئ.....

عندما يستقر هذا العدد ـ العاشر ـ بين يديك الكريمتين، نتذكر أول إطلالة للمجلة منذ العام 2012م، فقد كان التحدي الأكبر لنا هو مناط اختصاص المجلة، وكانت رؤيتنا المرتبطة بأن تعنى المجلة بالموضوعات "المتعلقة بتقنية المعلومات والعلوم الحديثة"، تحد مشوب بالتخوف من قلة البحوث والدراسات التي تغطي هذا الجانب في شقه القانوني، بينما لازالت هذه العلوم في طورالاكتشافات المتسارعة والمذهلة بنتائجها وإفرازاتها المؤثرة في كل مناحي حياتنا بما فيها الصناعة القانونية، ولا يخفى تأثير ذلك على العاملين بمجال العدالة والقضاء. فهؤلاء المشتغلين المنشغلين بإحقاق الحقوق وتطبيق قيم الشفافية وانتهاج منهج العدالة في كافة قراراتهم راحة لضمائرهم وتأدية للأمانة المكلفون بحملها، وبيان مدى قدرتهم على تطويع الاكتشافات الحديثة في خدمة العدالة.

وبظهورالذكاء الاصطناعي وما أحدثه من أصداءً هامة في جميع أنحاء العالم، وتوقع الخبراء أنْ يؤدي إلى تغييروإعادة تشكيل طريقة حياة البشر اليومية على نحوٍ متزايد، فكان لابد لنا أن نتطور ونطور اهتمامات المجلة لتعنى "بالذكاء الاصطناعي والعلوم المتقدمة" ويستمر التحدي ويشتد مابين جدب الموضوعات المتعلقة بهذا الجانب قانونياً، واختلاط فهم مايعنيه الذكاء الاصطناعي على البعض، وجاءت مبادرتنا الأولى بإعداد وتقديم أول ورقة عمل عن استخدام الذكاء الاصطناعي في المجالات القانونية والقضائية، ألقيت بمؤتمر النيابة العامة الذي نظمته نيابة رأس الخيمة، وارتأينا فيه أن الذكاء الاصطناعي سيؤثر في مجال الصناعة القانونية حتماً؛ مما سيؤدي إلى تحول كبير في تقديم الخدمات القانونية والقدرة على قيادة التغيير الكبير في الحياة العادية والخدمات المتخصصة في المجالات المرتبطة بالعدالة، ولم نشأ أن ننتظر بل قررنا أن نمهد الطريق أمام كل باحث وقارئ وقانوني للاطلاع على المقالات الأجنبية المنشورة والتي استقطبناها وقمنا بترجمتها للغتنا العربية عوناً ومساعدة منا

alsumaitijh@dji.gov.ae

لتشجيع الباحثين والمفكرين وأعضاء السلطة القضائية وكل العائلة القانونية العربية عامة والإماراتية خاصة لولوج هذا اليم والإبحار فيه لتقود دولتنا الحبيبة سفينة هذا العلم إلى شاطئ الأمان، وكما أن قيادتنا الرشيدة - حفظهم الله تعالى - ملهمة وسباقة في هذا المضمار بتخصيص وزارة مستقلة للذكاء الاصطناعي يقودها ابن من أبناء دولتنا الحبيبة، وبسواعد أبناء الإمارات وعقولهم اخترقنا الفضاء صعوداً، وسعينا لقيادة الأرض باستخدام أحدث التقنيات. فكان لابد لصناعة القانون من مواكبة هذا التطور وتسارع الخطى لتكون بين الصفوف الأولى في المجتمع فهماً ومواكبةً وتطبيقاً لكل مخرجات العلم الحديث. فنحن في عصرالبيانات الضخمة (فلله الحمد على نعمة القيادة المؤمنة بالعلم والميسرة في سبيله كل غالٍ ونفيس لمن أراد من أبناء الوطن التميزوالإبداع والنبوغ، ولله الحمد على وطن اتخذ من السعادة والتسامح أسلوب حياة لشعبه ولكل من يقيم على ترابه، ولكل زائر لربوعه.. حفظ الله دولة الإمارات العربية المتحدة، وحفظ حكامها وشعبها من كل شر ومكروه. وأدام عليها نعمة الأمن والأمان.

كلمة العدد

بقلم أسرة التحرير

عزيزي القارئ.

ونحن نقدم لك العدد العاشر من المجلة نطوف معك من خلال إطلالة سريعة على ما تضمه المجلة بين دفتيها من بحوث ومقالات آملين أن تكون مجلتنا هذه عوناً للباحث والقانوني بما تحويه من علم ومعرفة وإضافة له تدفعنا لمزيد من الجهد والتميز، حيث يضم العدد:

أولاً: موضوعاً يتناول، الحماية القانونية للبريد الإلكتروني: دراسة مقارنة بين الفقه الإسلامي والمرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة.

حيث يتسم البحث بالأصالة العلمية والجدة الواضحة، ويظهر ذلك جليًا من حداثة المراجع العلمية وتشريعات دولة الإمارات العربية المتحدة، التى رجع إليها الباحث. ومن ثم، للبحث فائدة واضحة في استجلاء كثير من غوامض المسائل المتعلقة بموضوعه، بحث جدير بالقراءة.

ثانياً: كاميرات المراقبة التلفزيونية المغلقة CCTV كوسيلة للمراقبة السابقة على ارتكاب الجريمة لأغراض منع الجريمة وملاحقة مرتكبيها.

تتناول إشكالية موضوع البحث، غياب التنظيم القانوني الإجرائي لإجراءات تبيح مباشرة المراقبة السابقة على ارتكاب الجريمة، ويقدم الباحث مشروع قانون لاستخدام التقنيات الإلكترونية الحديثة في أغراض الحد من الجريمة والملاحقة الجنائية لها، بحث جدير بالقراءة.

ثالثاً: مقالات ثلاث تتناول الذكاء الاصطناعي، حيث يتسائل البروفيسور ديلا كروس، هل ينبغي تنظيم الذكاء الاصطناعي؟ ويتسائل كريستوفر فونزون وكيت هينزلمان، هل ينبغي أن تضع الحكومة اللوائح والقوانين فيما يتعلق بالذكاء الاصطناعي؟ ويجيبا، نعم هي تفعل ذلك بالفعل.

وأخيراً إطلالة على مناقشات الاتحاد الأوروبي لتنظيم الذكاء الاصطناعي، والقضايا القانونية المرتبطة به، يقدمه لنا ديريك دو بريز.

وختاماً: نرجو أن تجدوا بين دفتي هذا العدد كل الفوائد المرجوة مما يحتويه.

الحماية القانونية للبريد الإلكتروني

دراسة مقارنة بين الفقه الإسلامي والمرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة

أ.د. عابد فايد عبد الفتاح فايد

الحماية القانونية للبريد الإلكتروني

دراسة مقارنة بين الفقه الإسلامي والمرسوم بقانون اتحادي رقم 5 لسنة2012 في شأن مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة

أ.د. عابد فايد عبد الفتاح فايد

دكتوراة في الحقوق من جامعة باريس1 (بانتيون- سوربون)

أستاذ القانون المدني - كلية الحقوق- جامعة حلوان - جمهورية مصر العربية

أستاذ القانون المدني ومدير ماجستير التحكيم - كلية القانون- الجامعة الأمريكية في الإمارات والمحامي أمام المحاكم العليا في جمهورية مصر العربية

المقدمة

موضوع البحث:

نتابع باندهاش كل يوم ما تنتجه الثورة الإلكترونية من إبداعات وابتكارات. ومايدهشنا من هذه الثورة، حتى الآن، ليس سوى نقطة في بحر زاخر، لا يعلم حدوده إلا الله سبحانه وتعالى.

وتفرض هذه الثورة الإلكترونية على الإنسان أن يقوم بضبطها وتوجيهها التوجيه الصحيح، ليستفيد من منافعها ويتجنب أضرارها بقدر الإمكان.

ومن نتاج الثورة الإلكترونية، البريد الإلكتروني وما ينتج عنه من تأثيرات قانونية متعددة. فهل يتصور الإنسان مقدار ماوصلت إليه البشرية في هذا الخصوص، ابتداء من إرسال الرسائل مع رسول والحمام الزاجل، وتنظيم هيئات البريد العادي، والتلغراف والتلكس، الى أن وصلنا الى البريد الإلكتروني.

إن هذا التطور يفرض على علماء القانون الاجتهاد ليجدوا القواعد القانونية المناسبة. ونظراً لتقليدية الحلول الموجودة، كان لزاماً على المشرعين أن يجدوا تنظيمات حديثة لمواجهة هذا القادم الجديد، ومن هؤلاء بالطبع المشرع الإماراتي الذي لم يقف مكتوف

الأيدي، إنمانظم حماية فعّالة لمكافحة جرائم تقنية المعلومات، وهي ماتنسحب بالقطع على الاعتداء على البريد الإلكتروني بمقتضى القانون الاتحادي رقم 5 لسنة 2012.

وحتى لا تكون حلولنا القانونية بلا جذور، يلزم أن تستند إلى ما أقرته شريعتنا الغراء من قواعد لكفالة حماية الأموال والممتلكات والحقوق والمكتسبات، وهذا ما يمثل الجناح الآخر لأحكام الحماية من الاعتداء المتوقع على البريد الإلكتروني.

وهذا المزج بين الأصالة والمعاصرة هو أحد مميزات النظام القانوني في دولة الإمارات العربية المتحدة، الذي يمثل رسالة الإسلام القانونية إلى العالم بين الأنظمة القانونية المعاصرة. ولم يشهد هذا النظام حتى الآن كتابات تبين ثراءه وتفرده بين هذه النظم.

في هذا الإطار نقدم بحثنا هذا حول أحكام حماية البريد الإلكتروني من الاعتداءات التي يمكن أن تقع عليه، آخذين في الحسبان هذا التطور وفقاً لقواعد القانون الحديث، والذي في مواكبته لهذا التطور يكون في الوقت نفسه محكوماً بقيم المجتمع الأساسية ومصالحه الحيوية.

إشكالية البحث وأهميته:

تدور إشكالية هذا البحث حول جوانب الحماية من الاعتداء على البريد الإلكتروني:

1. ما المقصود بالبريد الإلكتروني ومتى نشأ وما أنواعه؟.
2. ملكية البريد الإلكتروني: كيف يحصل الشخص على البريد الإلكتروني وما علاقته به؟.
3. ما هي صور الاعتداء المتوقعة على البريد الإلكتروني، في الفقه الإسلامي وقانون مكافحة جرائم تقنية المعلومات الإماراتي؟.
4. كيفية الوقاية من الاعتداء على البريد الإلكتروني؟.
5. ما هو الجزاء الذي يوقع في حالة الاعتداء على البريد الإلكتروني؟.

أما أهمية البحث فتبرز في إظهار الجوانب النظرية والعملية لحماية البريد الإلكتروني من الاعتداء الذي يمكن أن يقع عليه. كما أن هذا البحث يهدف إلى التعريف بالبريد الإلكتروني واستخداماته المختلفة والصور المتوقعة للاعتداء عليه، بحيث يشكل جانباً من التوعية بهذه الأداة الإلكترونية وبتأثيراتها القانونية في الحياة. فلا يقبل بعد هذه التوعية الجهل بدور البريد الإلكتروني في النظام القانوني الإماراتي. ومن يفعل هذا فإنه يوصم على الأقل بعدم الوعي بالقانون الإماراتي والتطورات الحديثة التي مر بها في العقدين الأخيرين بصفة خاصة، إن لم ينسب له إهدار النصوص القانونية المعنية بهذه التطورات[1]. فلم يعد يقبل بسهولة[2] أن تنص لائحة حديثة على أنه "لا يعتد بالمكاتبات الواردة عن طريق البريد الإلكتروني" [3]، لأن هذا قد يعني عدم إلمام واضع هذه اللائحة بالأحكام القانونية للبريد الإلكتروني، وخاصة بما أضفاه عليه المشرع الإماراتي من قيمة قانونية في الإثبات [4]، ومن

(1) انظر حول جانب من هذه التطورات: أ. د. محمد محمد محمد أبو زيد، النصوص القانونية ذات الصلة بانعكاسات التقدم العلمي التي أدخلت على نصوص القوانين الرئيسة، مجلة معهد دبي القضائي، العدد الأول، مايو 2002، ص 139.

(2) ونقول لم يعد يقبل بسهولة نظراً لأن أحكام البريد الإلكتروني ودوره في الإثبات لا تتعلق بالنظام العام، ومن ثم يمكن استبعادها أو الاتفاق أو النص على خلافها، مع ما يمثله ذلك من إهمال للتطور التقني وتأثيراته القانونية في النظام القانوني الإماراتي.

(3) انظر على سبيل المثال: لائحة غرفة فض المنازعات في اتحاد الإمارات العربية المتحدة لكرة القدم (المادة 11).

(4) راجع قانون الإثبات رقم 10 لسنة 1992 وتعديلاته بمقتضى القانون رقم 36 لسنة 2006. انظر في ذلك على سبيل المثال: م. د. عبد الحميد النجاشي الزهيري، الوجيز في شرح قانون الإثبات الإماراتي، الآفاق المشرقة، 2014، ص95 وما بعدها. وقد استقر القضاء الإماراتي على منح القيمة القانونية (المناسبة) في الإثبات تطبيقاً لنصوص هذا القانون لجميع الوسائل الإلكترونية وإلغاء أحكام محاكم الموضوع التي تخالف هذه المبادئ. انظر في هذا القضاء المستقر على سبيل المثال: نقض، جلسة 11 مارس 2013 (تجاري)، الطعن رقم 317 لسنة 2012 س 7 ق. أ، مجموعة الأحكام والمبادئ القانونية الصادرة عن محكمة النقض المصرية من دوائر المواد المدنية والتجارية والإدارية، السنة القضائية السابعة 2013م، من أول مارس حتى آخر أبريل، المكتب الفني، محكمة النقض، دائرة القضاء، الجزء الثاني، ص 549، وقد جاء فيه: أن التفات الحكم المطعون فيه عن كشف الحساب المستخرج من الحاسب الآلي صادر عن المطعون ضدها يقابله كشف حساب صادر عن الطاعن لبيان أوجه الحق في الدعوى مخالفة للقانون (خطأ في تطبيقه)، وأساس ذلك أن الحكم لم يناقش حجة الطاعنة في إطار حرية الإثبات في الأعمال التجارية وفي إطار النصوص القانونية ودون ندب خبير لتحقيق الدعوى. وانظر أيضاً، نقض جلسة 22 إبريل 2013 (تجاري)، الطعن رقم 658 لسنة 2012، س7 ق.أ، مجموعة الأحكام. ... المرجع السابق، ص 855، حيث جاء فيه: جواز الإثبات في الدعاوى المتصلة بهيئة سوق الإمارات للأوراق المالية والسلع استثناء من أحكام وقواعد الإثبات بجميع طرق الإثبات بما في ذلك الوسائل الإلكترونية"؛ نقض، جلسة 1 مايو 2013 (تجاري)، الطعن رقم 114 لسنة 2013 س7 ق.أ، مجموعة الأحكام والمبادئ القانونية الصادرة عن محكمة النقض من دوائر المواد المدنية والتجارية والإدارية، السنة القضائية السابعة 2013م، من أول مايو حتى آخر يونيو، المكتب الفني، محكمة النقض، دائرة القضاء، الجزء الثالث، ص972، حيث قضت المحكمة بجواز احتجاج التاجر على خصمه التاجر بالبيانات المستقاة من حاسبه الآلي واستثنائها من أحكام المواد (26، 27، 28، 29) من قانون المعاملات التجارية، بشرط أن يكون التاجر ممن يستخدم في تنظيم عملياته التجارية الوسائل الإلكترونية الحديثة وفقا لأحكام قرار وزير المالية والتجارة رقم 74 الصادر في 1994/10/30.

دور قيد الدعوى[1] وفي الإعلان القضائي[2]، وفي غيرها من المجالات القانونية[3].

وأخيراً، يهدف هذا البحث إلى إعلام الكافة - إضافة إلى الإعلام القانوني الذي يهتم بنشر القوانين في الجريدة الرسمية - بأن الاعتداء على البريد الإلكتروني يعد جريمة يعاقب عليها القانون بعقوبات شديدة ورادعة.

المنهج المستخدم:

نستخدم في هذا البحث المنهج التحليلي المقارن. نبدأ أولاً بتحليل الوقائع الموجودة والنصوص القانونية القائمة والتصورات في الفقه الإسلامي، ثم نجري هذا التحليل في إطار مقارن بين أحكام الحماية في الفقه الإسلامي وفي قانون مكافحة جرائم تقنية المعلومات. كل ذلك مع إبراز الجانب التطبيقي وذلك بالاستعانة بالأحكام القضائية والمبادئ القانونية التي أرستها المحاكم العليا في دولة الإمارات العربية المتحدة، وفي بعض الأنظمة المقارنة.

(1) حيث نص قانون الإجراءات المدنية رقم 11 لسنة 1992 وتعديلاته بمقتضى القانون رقم 10 لسنة 2014 والقانون رقم 18 لسنة 2018 في المادة 162 منه على أن "يرفع الاستئناف بصحيفة تودع مكتب إدارة الدعوى في المحكمة الاستئنافية المختصة وتقيد فوراً بالسجل المعد لذلك أو بقيدها إلكترونياً". وقد طبقت محكمة تمييز دبي هذا النص ونقضت حكم محكمة الاستئناف الذي خالفه، وذلك في حكمها الصادر بجلسة 7 فبراير2016 (تجاري)، الطعن رقم709/2015: الموقع الإلكتروني لمحاكم دبي، والذي جاء فيه أن:... الثابت بالأوراق أن الحكم المستأنف صدر بجلسة 26-4- 2015 حضورياً في حق المستأنفة وأنها قد قيدت استئنافها إلكترونياً بتاريخ 26-5-2015م ولما كان العبرة في تقرير تاريخ تقديم الاستئناف في ميعاده القانوني بتاريخ قيده إلكترونياً لدى قلم كتاب محكمة الاستئناف وليس بتاريخ مراجعة قيده وتدقيقه واعتماده بواسطة قلم كتاب المحكمة وسداد رسمه المقرر، وعليه فتكون الطاعنة قد قدمت استئنافها في ميعاده القانوني المنصوص عليه في أحكام المادتين (159/152) من قانون الإجراءات المدنية، وإذ خالف الحكم المطعون فيه هذا النظر وقضى بسقوط حق الطاعنة في الاستئناف المذكور للتقرير به بعد الميعاد القانوني على سند من أن العبرة في تحديد تاريخ تقديم الاستئناف إلكترونياً بتاريخ سداد الرسم في 2-6-2015م وليس بتاريخ قيده إلكترونيا في 26-5-2015م فإنه يكون قد خالف القانون وأخطأ في تطبيقه بما حجبه عن نظر موضوع الاستئناف مما يعيبه ويوجب نقضه".

(2) حيث أجاز قانون الإجراءات المدنية رقم 11 لسنة 1992 وتعديلاته بمقتضى القانون رقم 10 لسنة 2014 والقانون رقم 18 لسنة 2018 م، أن: "الإعلان يمكن أن يكون بالبريد المسجل بعلم الوصول أو البريد الإلكتروني أو ما يقوم مقامها من وسائل التقنية الحديثة التي يصدر بتحديدها قرار من وزير العدل أو بأية وسيلة يتفق عليها الطرفان".

(3) من ذلك القانون الاتحادي رقم 4 لسنة 2013 بشأن تنظيم مهنة الكاتب العدل، حيث جاء فيه أن السجل الإلكتروني هو "سجل أو مستند يتم إنشاؤه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية، على يد وسيط ملموس أو على أي وسيط إلكتروني آخر ويكون قابلاً للاسترجاع بشكل يمكن فهمه" (المادة (1) من قرار مجلس الوزراء رقم 39 لسنة 2014 في شأن اللائحة التنفيذية لقانون تنظيم مهنة الكاتب العدل).

الدراسات السابقة:

قليلة هي الدراسات التي أجريت على البريد الإلكتروني في الفقه العربي بصفة عامة، وفي نطاق القانون الإماراتي بصفة خاصة. ويمكن الإشارة في هذا الخصوص إلى الدراسة الرائدة التي أجراها الزميل الأستاذ الدكتور عبد الهادي العوضي حول " الجوانب القانونية للبريد الإلكتروني" في سنة 2007 [1]، وهي الدراسة التي بُنيت عليها أو استفادت منها جميع الدراسات اللاحقة[2]. وعلى حد علمنا، تعتبر دراستنا هذه من أوائل الدراسات التي تعالج جوانب الحماية القانونية للبريد الإلكتروني في القانون الإماراتي، في ضوء القوانين التي تعالج التجارة الإلكترونية والمعاملات الإلكترونية وقانون مكافحة جرائم تقنية المعلومات رقم 5 لسنة 2012)[3].

خطة البحث:

سوف ندرس أحكام الاعتداء على البريد الإلكتروني من خلال الخطة الآتية.

الفصل التمهيدي: التعريف بالبريد الإلكتروني وأنواعه وتطوره.الفصل الأول: ملكية البريد الإلكتروني.

المبحث الأول: تحديد الملكية مناط حماية البريد الإلكتروني.

المبحث الثاني: نظريات تحديد ملكية البريد الإلكتروني.

(1) د. عبد الهادي العوضي، الجوانب القانونية للبريد الإلكتروني، دار النهضة العربية، القاهرة، 2007. وقد عثرنا على دراسة سابقة على دراسة العوضي ولكنها لم تكن بذات العمومية ولا التأثير الذي كان لدراسة هذا الأخير، وذلك ربما لتميزها بالطابع الدراسي التدريبي واعتمادها على الترجمة عن الإنجليزية دون مراعاة الواقع القانوني السوري أو العربي بصفة عامة : المحامي / عدنان غسان برابو، دراسة عن بعض الجوانب القانونية والتقنية لاستخدام البريد الإلكتروني في المؤسسات، بحث مقدم في مادة تقنيات وأدوات الإدارة واستخداماتها، المعهد العالي للتنمية الإدارية ـــــ قسم ماجستير العلوم الإدارية، جامعة دمشق، العام الدراسي 2004-2005.

(2) انظر على سبيل المثال: عبد الله بن ناصر بن أحمد العمري، الحماية الجنائية للبريد الإلكتروني، دراسة تأصيلية مقارنة، رسالة لاستكمال متطلبات الحصول على درجة الماجستير، قسم العدالة الاجتماعية ـــــ تخصص السياسة الجنائية، جامعة نايف للعلوم الأمنية، الرياض، 1431 هـ ـــــ 2010 م؛ إيمان محمد طاهر، الحماية المدنية لمستخدمي البريد الإلكتروني، مجلة الرافدين للحقوق، كلية الحقوق، جامعة الموصل، العراق، العدد 54، 2012، ص 190-134.

(3) معظم الدراسات التي أجريت حول القانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، كلها تنتمي إلى القانون الجنائي. وتعتبر الدراسة التي أجراها الزميل الدكتور عبد الرازق الموافي من أهم الدراسات التي أجريت حول هذا القانون: د. عبد الرازق الموافي عبد اللطيف، شرح قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة، " المرسوم بالقانون الاتحادي رقم 5 لسنة 2012"، الكتاب الأول، معهد دبي القضائي، سلسلة الدراسات والبحوث القانونية والقضائية العلمية المحكمة، 13، 1435هـ- 2014؛ والكتاب الثاني، معهد دبي القضائي، سلسلة الدراسات والبحوث القانونية والقضائية العلمية المحكمة، 15، 1437 هـ- 2016 م، بالإضافة إلى الدراسات الأخرى التي سنشير إليها في هذا البحث. ولا توجد دراسة مستقلة انصبت على البريد الإلكتروني في ضوء هذا القانون والقوانين التي تعالج المسائل الإلكترونية في القانون الإماراتي.

الفصل التمهيدي
التعريف بالبريد الإلكتروني ونشأته وأنواعه وتطوره

نشأة البريد الإلكتروني ومخترعه: على الرغم من حداثة البريد الإلكتروني، فإن مخترعه لم يعد يتذكر أول رسالة أرسلها عبر الإيميل من جهاز كمبيوتر إلى جهاز كومبيوتر مجاور. والبريد الإلكتروني يسبق في وجوده وجود الإنترنت نفسه.

ففي الحقيقة، يرجع الفضل في ظهور البريد الإلكتروني إلي العالم الأمريكي راي توملينستونRay Tomlinson، والذي يعتبر، وبحق، مخترع البريد الإلكتروني حيث صمم علي شبكة الإنترنت برنامج لكتابة الرسائل يسمى send message، وذلك بغرض تمكين العاملين بالشبكة من تبادل الرسائل فيما بينهم، ثم ما لبث أن اخترع برنامجاً أخر يسمح بنقل الملفات من جهاز كمبيوتر إلي جهاز أخر، ثم قام بدمج البرنامجين في برنامج واحد، ونتج عن هذا الدمج ميلاد البريد الإلكتروني.

ولقد صادفت Ray Tomlinson مشكلة تتمثل في أن الرسالة لا تحمل أي دليل علي مكان مرسلها ففكر في ابتكار رمز لا يستخدمه الأشخاص في أسمائهم، يوضع بين اسم المرسل والمَوقع الذي ترسل منه الرسالة، وكان اختياره للرمز @، وكان ذلك في خريف عام 1971، وبذلك أصبح أول عنوان بريد إلكتروني في التاريخ هو tenexa–Tomlinson@bbn [1].

التعريف بالبريد الإلكتروني:

لم يعرف العرب القدامى البريد الإلكتروني، ومن ثم فلن نجد لديهم بالطبع تعريفاً لهذا النظام. كما أننا لم نجد للبريد الإلكتروني تعريفاً في المرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات. ولكن هذا القانون استخدم اسم " وسيلة تقنية المعلومات"، وعرفها بأنها " أي أداة إلكترونية مغناطيسية، بصرية، كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية وأداء العمليات المنطقية والحسابية، أوالوظائف التخزينية، ويشمل "أي وسيلة موصلة أو مرتبطة بشكل مباشر، تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية أو إيصالها للآخرين". وهذا التعريف يشمل بلا شك البريد الإلكتروني، كوسيلة من وسائل تقنية المعلومات، تهدف إلى تبادل المعلومات بين أجهزة الحاسب الآلي، كما تهدف إلى إمكانية تخزين المعلومات لوقت الحاجة إليها، بمجرد إرسالها، ولو لنفس العنوان. ويكون إرسال المعلومات أو الرسائل إلى عناوين معينة، مثلما يتم إرسال البريد العادي إلى عنوان محدد، وإلا كان مهدداً بعدم الوصول إلى الجهة أو الشخص المقصود.

(1) ومخترع البريد الإلكتروني هو المبرمج الأمريكي راي توملينسون. ولد توملينسون في العام 1941 وتخرج من معهد ماساشوستس للتكنولوجيا (إم آي تي) الشهير، وكتب أول بريد إلكتروني في التاريخ في 1971. وصمم توملينسون البرنامج الذي يتيح إرسال هذه الرسائل حين كان يعمل على شبكة " أربانت" المخصصة للباحثين والعسكريين والتي انبثقت عنها لاحقاً شبكة الإنترنت. وهو صاحب فكرة استخدام علامة@ لفصل هوية الشخص عن الشبكة التي يتصل بها.

انظر حول هذا التاريخ : بي بي سي العربية: وفاة مخترع البريد الإلكتروني راي توملينسون، في 7 مارس 2016
email_inventor_dies_160306/03/http://www.bbc.com/arabic/business/2016

وأيضا: ويكيبيديا، الموسوعة الحرة: راي_توملينسون
/https://ar.wikipedia.org/wiki

أهمية البريد الإلكتروني:

أصبح البريد الإلكتروني ضرورة حياتية ومهنية في حياة الأفراد والمشروعات. ويمتاز البريد الإلكتروني بالسرعة والسهولة والاقتصاد في النفقات. ففي ثوان معدودة، يستطيع الشخص أن يرسل رسالة إلى أبعد مكان على وجه الأرض، محملة بمرفقات كتابية أو مصورة أو صوتية أو مرئية. كما يمكن إرسال الرسالة الى عدة متلقين في نفس الوقت. البريد الإلكتروني أصبح جزءاً من الحياة، إذا فقده الشخص يفقد جزءاً من حياته. ويفضل البريد الإلكتروني التليفون لأنه لا يحتاج إلى الرد الفوري على الرسائل، كما يتفوق في سرعته على البريد العادي[1]. ويستخدم البريد الإلكتروني على مستوى المنظمات والهيئات والشركات والأفراد. وتساعد سرعته وإمكانياته في الإرسال على الإنجاز وسرعة إتخاذ القرار.

والبريد الإلكتروني وسيلة إبرام وإثبات للحقوق والالتزمات[2] ووسيلة للإعلان

(1) د. حسن عماد مكاوي، تكنولوجيا الاتصال الحديثة في عصر المعلومات، الدار المصرية اللبنانية، القاهرة، الطبعة الخامسة، شوال 1430 هـ - أكتوبر 2009م، ص 229.

(2) انظر بصفة خاصة المادة الرابعة والمادة العاشرة من القانون الاتحادي رقم 1 لسنة 2006 في شأن المعاملات والتجارة الإلكترونية:

مادة 4: 1- لا تفقد الرسالة الإلكترونية أثرها القانوني أو قابليتها للتنفيذ لمجرد أنها جاء ت في شكل إلكتروني.

2- لا تفقد المعلومات المثبتة في الرسالة الإلكترونية حجيتها القانونية حتى وإن وردت موجزة، متى كان الاطلاع على تفاصيل تلك المعلومات متاحًا ضمن النظام الإلكتروني الخاص بمنشئها، وتمت الإشارة في الرسالة إلى كيفية الاطلاع عليها.

مادة 10:

1- لا يحول دون قبول الرسالة الإلكترونية أو التوقيع الإلكتروني كدليل إثبات:

(أ) أن تكون الرسالة أو التوقيع قد جاء في شكل إلكتروني.

(ب) أن تكون الرسالة أو التوقيع ليس أصليًا أو في شكله الأصلي، متى كانت هذه الرسالة أو التوقيع الإلكتروني أفضل دليل يتوقع بدرجة معقولة أن يحصل عليه الشخص الذي يستشهد به.

2- في تقدير حجية المعلومات الإلكترونية في الإثبات، تراعى العناصر الآتية:

(أ) مدى إمكانية الاعتداد بالطريقة التي تم بها تنفيذ واحدة أو أكثر من عمليات إدخال المعلومات أو إنشائها أو تجهيزها أو تخزينها أو تقديمها أو إرسالها.

(ب) مدى إمكانية الاعتداد بالطريقة التي استخدمت في المحافظة على سلامة المعلومات.

(ج) مدى إمكانية الاعتداد بمصدر المعلومات إذا كان معروفًا.

(د) مدى إمكانية الاعتداد بالطريقة التي تم بها التأكد من هوية المنشئ.

(هـ) أي عنصر آخر يتصل بالموضوع.

3- ما لم يتم إثبات عكس ذلك، يفترض أن التوقيع الإلكتروني المحمي:

(أ) يمكن الاعتداد به.

(ب) هو توقيع الشخص الذي تكون له صلة به.

(ج) قد وضعه ذلك الشخص بنية توقيع أو اعتماد الرسالة الإلكترونية المنسوب إليه إصدارها.

4- ما لم يتم إثبات عكس ذلك يفترض أن السجل الإلكتروني المحمي:

(أ) لم يتغير منذ أن أنشئ.

القضائي[1]، وفي إعلان القرار الإداري[2]، وفي غير ذلك من مجالات القانون. وقد اعترف القانون له بهذه الوظائف، الأمر الذي يزيد الثقة فيه[3]. وإن كان له من عيب فهو إمكانية استهدافه ومحاولة زعزعة الأمان فيه، ولكن القانون يعالج هذه العيوب بوسائله كما أن التقدم التقني يقدم حماية فعالة في هذا الخصوص.

كما يمكن استخدام البريد الإلكتروني في تحقيق غايات أخرى مثل الدعوة إلى الله أو لنشر أفكار معينة [4].

أنواع البريد الإلكتروني:

تتعدد أنواع البريد الإلكتروني. فهناك البريد الإلكتروني الشخصي (الخاص)، والبريد الإلكتروني المهني لشركة أو مؤسسة معينة، والبريد الإلكتروني الحكومي. ولهذا التقسيم أهميته الكبيرة، خاصة من حيث الأمان التقني للبريد الإلكتروني. ففي الغالب يكون البريد الإلكتروني الحكومي (وأيضاً المهني) أكثر أماناً من البريد الشخصي (أو الخاص). ولهذا قد يتعرض المسؤول الحكومي أو الموظف أو العامل للمساءلة إذا استخدم بريده الإلكتروني الشخصي في المخاطبات الرسمية أو تلك المتعلقة بوظيفته أوعمله، لأن ذلك سيسهل إمكانية التجسس على هذا البريد والسطو عليه من قبل أعداء الدولة أو المؤسسة أو الشركة [5].

(ب) معتد به.

(1) كانت المادة 8 من قانون الإجراءات المدنية رقم 11 لسنة 1992 وتعديلاته بمقتضى القانون رقم 10 لسنة 2014 تجيز " أن يتم الإعلان بالبريد المسجل بعلم الوصول أو البريد الإلكتروني أو ما يقوم مقامها من وسائل التقنية الحديثة التي يصدر بتحديدها قرار من وزير العدل أو بأية وسيلة يتفق عليها الطرفان"، (وقد ألغيت هذه المادة بالمرسوم بقانون اتحادي رقم (10 لسنة 2017)، ونقل حكمها إلى المادة (8) من قرار مجلس الوزراء رقم (57 لسنة 2018) في شأن اللائحة التنظيمية لقانون الإجراءات المدنية الاتحادي رقم (11 لسنة 1992) بشأن قانون الإجراءات المدنية.

(2) انظر بحث الزميل د. علاء محيي الدين مصطفى أبو أحمد، القرار الإداري الإلكتروني، ص 65 وما بعدها.

(3) ومع كل هذه الأهمية، يبدو غريباً أن لائحة غرفة فض المنازعات باتحاد الإمارات العربية المتحدة لكرة القدم نصت على أنه " لا يعتد بالمكاتبات الواردة عن طريق البريد الإلكتروني" (المادة 11). وربما لا نأخذ هذا الحكم على محمل الجد. فهذه اللائحة سارية منذ 2009/8/17، والتي عدلت في 2011/7/30، وتسري التعديلات اعتباراً من 2011/8/31، تبدو صياغتها معيبة، وربما تكون الصياغة قد تمت من غير متخصص. وليس أدل على ذلك من النص في المادة 34/ج منها على أن " يلغى كل نص يتعارض مع نصوص هذه اللائحة"!؟.

(4) انظر على سبيل المثال: د. علي سعيد عثمان محمد، البريد الإلكتروني واستخدامه في الدعوة إلى الله، مجلة الدعوة الإسلامية، كلية الدعوة الإسلامية، جامعة أم درمان الإسلامية، السودان، العدد 5، ديسمبر 2012، ص 162.

(5) مثلما حدث مع هيلاري كلينتون مرشحة الرئاسة الأمريكية، حيث استخدمت – أثناء توليها وزارة الخارجية الأمريكية - بريدها الإلكتروني الشخصي في المخاطبات والمكاتبات الرسمية للوزارة. حول قضية إيميل هيلاري كلينتون انظر:
https://en.wikipedia.org/wiki/Hillary_Clinton_email_controversy

كذلك يمكن تصنيف البريد الإلكتروني إلى بريد إلكتروني خارجي – Webmail – مثل Gmail Hotmail، Yahoo وبريد إلكتروني داخلي مثل البريد الإلكتروني الداخلي للمؤسسات والهيئات بالنسبة للعاملين بها، أو البريد الإلكتروني الذي يربط فروع البنك أوفروع الشركة بالفرع الرئيس.

ويمكن تصنيف البريد الإلكتروني من حيث المقابل المالي، إلى بريد إلكتروني مجاني وبريد إلكتروني مدفوع. ومثال الأول البريد الإلكتروني الشخصي غالبا ما يكون مجانياً، ومثال الثاني البريد الإلكتروني المهني أوالمخصص للأعمال، وفي الغالب يكون مدفوعاً. وتكمن أهمية هذا التمييز في أن مسؤولية الشركة مقدمة خدمة البريد الإلكتروني تكون أشد في حالة البريد الإلكتروني المدفوع منها في حالة البريد الإلكتروني المجاني.

تطور البريد الإلكتروني:

لقد تطور البريد الإلكتروني، ومازال، ويقطع خطوات متقدمة في سبيل إنجاز وظائفه وتحقيق أمن المراسلات. من البريد التزامني إلى البريد غير المتزامن قفز البريد الإلكتروني قفزة هامة. ففي بداياته كانت المراسلة بالبريد الإلكتروني تقتضي دخول كل من الراسل والمرسل إليه إلي الشبكة في الوقت ذاته لتنتقل الرسالة بينهما بشكل آني، غير أنه فيما بعد أصبح البريد الإلكتروني لديه القدرة على التخزين، بحيث تخزن الرسائل الواردة في صندوق بريد المستخدم ليطلع عليها في الوقت الذي يريده [1]. كما تطور نظام وطريقة عمل البريد الإلكتروني وكذلك أمن البريد الإلكتروني من وقت لآخر، وما زالت البحوث مستمرة من أجل تحقيق درجة أمان أعلى للرسائل الإلكترونية، حفاظا على سرية هذه المراسلات وعلى سلامتها من التزوير والاعتداءات الأخرى التي يمكن أن تقع عليها[2].

emails/, Posted on-clintons-to-guide-a/07/E. Kiely, A Guide to Clinton's Emails, http://www.factcheck.org/2016 July 5, 2016.

(1) انظر: بريد إلكتروني https://ar.wikipedia.org/wiki

(2) المرجع السابق.

الفصل الأول
ملكية البريد الإلكتروني (*)

من أولى نقاط الانطلاق في حماية البريد الإلكتروني ضد الاعتداء الواقع عليه مسألة تحديد ملكية البريد الإلكتروني. فتحديد الملكية هو مناط حماية البريد الإلكتروني (المبحث الأول). ولكن هذه المسألة ليست بالوضوح الكافي، الأمر الذي يستلزم عرض النظريات والآراء التي قيلت في هذا الصدد (المبحث الثاني).

المبحث الأول
تحديد الملكية مناط حماية البريد الإلكتروني

يحمي القانون الملكيات والمصالح، ومن ثم يجب تحديد العلاقة بين الشخص وبين محل الاعتداء حتى يمكن لهذا الشخص أن يتمتع بالحماية وأن يتمكن من التصرف في محل ملكيته أو مصلحته. فالقانون يحمي الحقوق وأحيانا المصالح حتى وإن لم تبلغ مرتبة الحقوق.

والبريد الإلكتروني لا يثير فقط مشكلة ملكيته لصاحبه بما فيه من أسرار وممتلكات، بل أكثر من ذلك بكثير، حيث يمتزج بشخص صاحبه. ولا مشكلة في أمر الملكية إذا كانت محتويات البريد الإلكتروني أوراقاً مالية أو شيكات إلكترونية أو أي محتويات لها قيمة مالية في نظر الشرع والقانون، ولكن تبدو المشكلة في حالة وجود معلومات أو رسائل شخصية لا تدخل في مفهوم المال، ومن ثم لا تشكل عنصراً من الذمة المالية لصاحب البريد الإلكتروني.

وقد أثيرت مسألة ملكية المعلومات في تسعينيات القرن الماضي، خاصة على إثر الثورة المعلوماتية. فبين منكر ومعترف بمالية المعلومات، أقر القضاء والقانون الحماية القانونية

للمعلومات، سواء من الناحية الجنائية[1] أو من الناحية المدنية[2]. بل أصبح الحديث حالياً يجري حول الحماية القانونية للحق في ملكية المعلومات، وهذا يمثل الاتجاه الحديث في الفقه والقضاء [3]. وبالنسبة لموقف الفقه الإسلامي، فإنه يعتبر من أرحب الأنظمة القانونية بصدد طبيعة المعلومات، حيث جعل الحقوق المالية هي التي تتعلق بالأموال والمنافع، ووضع معايير للمال هي : أن يميل إليه طبع الإنسان، ويمكن إحرازه بتعيينه وتحديده عيناً أو منفعةً، وأن يكون مما يبذل ويمنع، وأن تكون قابلية الشيء للانتفاع به متحققة في حال الاختيار، فإذا تم تطبيق هذه المعايير على المعلومات، وجب القول بأنها مال، ولها قيمة تباع بها، وهي لصاحبها لأنها تعلقت بها مصلحة خاصة له، وهي حق مالي متقوم باعتبارها منفعة مالية،

(1) (*) نقصد بالملكية هنا علاقة مستخدم البريد الإلكتروني بالبريد الإلكتروني، وهي لا تكون دائما علاقة ملكية بالمعنى الدقيق، ولكنها تبين المركز القانوني لمستخدم البريد الإلكتروني أو "ما يملكه" هذا المستخدم من سلطات على البريد ومحتوياته.

() انظر بصفة عامة في الجرائم الواقعة على الحق في المعلومات والحق على المعلومات: د. أيمن عبد الله فكري، الجرائم المعلوماتية، دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، الرياض، ط1، 1436 هـ- 2015 م.

(2) كان الخلاف على أشده بين الفقهاء حول حقيقة المعلومة المالية، هل تعد المعلومة مالا وبالتالي، تدخل في الذمة المالية للشخص أم لا تعد مالا وبالتالي لا تدخل في الذمة المالية. انظر في هذا:

Ch. GALLOUX, « Ébauche d'une définition juridique de l'information », D., 1994, chr.229 ; P. CATALA, « La -Jpropriété de l'information », Mélanges P. RAYNAUD, Dalloz -Sirey, 1985, p.113.

ولقد قضت محكمة النقض الفرنسية، الدائرة الجنائية، بأن المعلومات لا تعد شيئا، يمكن تملكه، وفقا للقانون الجنائي:

Cass. crim., 3 Avril 1995, Bull. crim., n°142, p.397, Cass. crim., 2 may 1983, Bull. crim., n°122, p.285.

ولقد دفع هذا الموقف أحد الكتاب إلى القول بأنه " أيا كان موقف الفقه أو القضاء الجنائي الفرنسي، فيما يتعلق بالنظام القانوني للمعلومة ومدى قابليتها للتملك من عدمه، فانه في مجال التأمين على المعلومات يكون البحث فيما إذا كانت الذاكرة أو البرنامجlogiciel هي مال أم لا دون جدوى. فحسب قانون الملكية الفكرية ليس بالضرورة أن يكون المال أو الشيء محسوسا ماديا، فضلا عن أنه ليس هناك تخوف من مطابقة الموقف الاقتصادي بالموقف القانوني، فيمكن أن تكون أشياء، أو إذا فضلنا أموال: عقار، أو براءة اختراع، أو برنامج " ذاكرة"، أو مجموعة بيانات. فهي أشياء لها قيمة تجارية، أو إذا شئنا تدخل في تقدير الذمة المالية. وبالتالي ليس هناك ما يمنع الكلام عن تأمين الأشياء في مجال المعلوماتية": د. محمود خيال، التأمين على المعلومات،1999، ص 23 وما بعدها.

(3) يرى الاتجاه الحديث في الفقه والقضاء أن المعلومات مجموعة من القيم الاقتصادية ذات القيمة المالية، وتدخل فيما يمكن تسميته " المال المعلوماتي"، الذي يمكن أن يكون محلا للحق في الملكية. انظر في عرض هذا الاتجاه: د. رشدي محمد علي محمد عيد، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، 2013، ص 31 وما بعدها؛ د. وانظر أيضا: أيمن عبد الله فكري، الجرائم المعلوماتية، المرجع السابق، ص 608 وما بعدها، حيث عرض بدقة وأمانة المفهوم الحديث للملكية المعلوماتية، وانتهى الى القول بأنه لا يمكن تعميم مفهوم المال على جميع أنواع المعلومات على الرغم من استقرار المعاملة الجنائية بالنسبة لها، وأن تطبيق النصوص الحمائية على المعلومات يقتضي النظر إلى طبيعة كل جريمة وما يتفق معها، فقد تقع الجريمة على المعلومات ذات القيمة المالية (مثل البرامج)، وقد تقع على معلومات غير مالية (مثل الحقوق اللصيقة بالشخصية) (ص 806). وقد ذهبت دراسات حديثة إلى القول بأن الحماية القانونية للمعلومات هي حماية لحق الملكية على المعلومات. انظر في هذا:

G. BEAUSSONIE, « La protection pénale de la propriété sur l'information », Droit pénal, 2008, n°9 ; M. COMBE, La protection pénale de l'information, thèse, Nice, 2012.

وبناء على هذا النظر، طبقت محكمة النقض الفرنسية نصوص جريمة السرقة على سرقة المعلومات. انظر على سبيل المثال:

Cass.crim., 20 mai 2015, Bull. crim.,, n° 119.

ويجوز الاعتياض عنها بمال[1]. وبهذا يتلاقى الفقه الإسلامي والاتجاه الحديث في الفقه القانوني والقضاء.

وبناء على ذلك، يعتبر الاعتداء على البريد الإلكتروني ــ وكما سنرى بالتفصيل فيما بعد ــ اعتداء على ملك الغير وانتهاكاً لحرمة أسراره. وهذا مكمن الخطورة ومناط الحماية، فالشخص الذي يعتدي على البريد الإلكتروني لشخص آخر ويستعمله يعتدي على ملكيات، وينتهك أسرار، وكأنه يستولى على " شخص صاحب البريد" وانتحاله واستخدامه باسمه. كل ذلك يبرر ــ بلا شك ــ إقرار حماية فعالة للبريد الإلكتروني ليس فقط حفاظاً على الممتلكات ولكن أيضاً حماية لما هو أغلى من الممتلكات.

المبحث الثاني
نظريات تحديد ملكية البريد الإلكتروني

غير أن مسألة ملكية البريد الإلكتروني ليست بالوضوح الكامل، الأمر الذي يبدو أثر على الحماية المقررة للبريد الإلكتروني. فالأفكار والنظريات التي قيلت في شأن " المركز القانوني لمستخدم البريد الإلكتروني" لم تظهر للوجود مرة واحدة، ومن ثم لا تتمتع بالنضج الضروري، ونشعر أحياناً بأنها تصادر على المطلوب عندما تقترح الحل، بدلاً من أن توصف الواقع أولاً لإسباغ التكييف القانوني الملائم عليه.

واتباعاً لمنهج يتدرج من الحقيقة الواقعية وصولاً إلى الفكرة القانونية التي تتناسب معها، نبدأ أولاً بعرض وتفريد العناصر وصولاً للنظريات التي تحكمها.

ويمكننا في هذا الصدد أن نميز بين ثلاثة عناصر لموضوع ملكية البريد الإلكتروني:

الأول: علاقة الشخص بالبريد الإلكتروني، وهو ما يثير علاقته القانونية مع الشركة منشئة البريد الإلكتروني (المطلب الأول).

الثاني: علاقة الشخص بمحتويات البريد الإلكتروني، وهو ما يثير طبيعة السلطات والمكنات التي يتمتع بها الشخص على ما يحويه بريده الإلكتروني من مواد (المطلب الثاني).

الثالث: وهو مترتب على الثاني، وهو يتعلق بمدى دخول محتويات البريد الإلكتروني في الذمة المالية للشخص، الأمر الذي يجعل هذه المحتويات عنصرا من عناصر تركته بعد وفاته، أم أن الأمر لا يدخل في الذمة المالية ومع ذلك يحتاج إلى حماية قانونية بعد وفاة صاحب البريد الإلكتروني وأخيراً هل " تموت" محتويات البريد الإلكتروني مع وفاة صاحبه؟ (المطلب الثالث).

المطلب الأول
كيفية اكتساب الشخص للبريد الإلكتروني
(العقد بين الشركة منشئة البريد الإلكتروني والشخص المستفيد منه)

يحدد العقد بين الشخص طالب الحصول على البريد الإلكتروني والشركة مقدمة الخدمة طبيعة العلاقة بين الطرفين، وطبيعة حق المستفيد من خدمات البريد الإلكتروني. وهنا يمكن تصور عدة فروض:

الفرض الأول: وفيه تقدم الشركة خدمة البريد الإلكتروني مجاناً وبلا مقابل، وهنا يمكن أن تحكم العلاقة أحكام عقد العارية أو عقد هبة الانتفاع بالبريد الإلكتروني.

الفرض الثاني: وفيه تقدم الشركة خدمات البريد الإلكتروني في مقابل مادي يدفعه لها المستفيد من هذه الخدمات، وهنا يمكن أن تحكم العلاقة أحكام عقد الإيجار أو أحكام عقد المقاولة.

الفرض الثالث: وفيه تنقل الشركة ملكية البريد الإلكتروني إلى طالب البريد الإلكتروني في مقابل ثمن يدفعه، وهنا يمكن أن تحكم هذه العلاقة أحكام عقد البيع.

(1) انظر في هذا: عبير علي محمد النجار، جرائم الحاسب الآلي في الفقه الإسلامي، رسالة ماجستير، الجامعة الإسلامية، غزة، 1430 هـ- 2009 م، ص 58 والمراجع المشار إليها في هوامش هذه الصفحة؛ د. إسماعيل عبد النبي شاهين، أمن المعلومات في الإنترنت بين الشريعة والقانون، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 1-3 مايو 2000، ص971- 992، وبصفة خاصة ص 987.

ولا يخفى ما في تكييف العقد بين طالب البريد الإلكتروني والشركة المقدمة من صعوبة، ومن ثم يصعب إخضاعه للقواعد القانونية المعروفة.

ونرى أن العلاقة بين الطرفين يحكمها عقد غير مسمى هو " عقد إنشاء بريد إلكتروني" أو" عقد تقديم خدمة البريد الإلكتروني "وينتمي هذا العقد إلى طائفة" عقود الخدمات الإلكترونية"، وهي العقود التي تتعلق بتجهيز وتقديم خدمات الإنترنت وكيفية الاستفادة منها. وتبرم هذه العقود بين القائمين على تقديم خدمات شبكات الإنترنت والمستفيدين منها. وهي تشمل، فضلاً عن عقد تقديم خدمة البريد الإلكتروني، عقد الدخول إلى شبكة الإنترنت، وتقديم المساعدة الفنية، وعقد الإيواء، وعقد الاشتراك في بنوك المعلومات،....الخ[1].

ويرى اتجاه فقهي أن هذه العقود من حيث الطبيعة القانونية تعد بمثابة عقود مقاولة وتخضع لأحكامها فيما لم يتم تنظيمه من بنودها بالاتفاق[2].

ونرى أن عقد الحصول على البريد الإلكتروني، كعقد غير مسمى، يخضع للشروط الواردة فيه، وفي حالة عدم وجود شرط يخضع لأحكام أقرب عقد مسمى له، وفقاً لأحكامه الواردة فيه على النحو الذي بيناه في الفروض التي يتصور أن تحكم العلاقة بين الشركة مقدمة خدمة البريد الإلكتروني والمستفيد من هذه الخدمة، ما يمكن أن يحدث في الواقع العملي[3]. وأياً كان الأمر، يكون المستفيد من خدمة البريد الإلكتروني مسئولاً عن أية مسؤولية قانونية تنتج عن استخدامه للبريد الإكتروني.

(1) د. محمد حسين منصور، المسئولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2003، ص 34؛ د. أيمن عبد الله فكري، المرجع السابق، ص 701.

(2) د. محمد حسين منصور، المرجع السابق، ص 34؛ د. أيمن عبد الله فكري، المرجع السابق، ص 701. وانظر في نفس الرأي بخصوص عقد الاستفادة من المعلومات الموجودة في بنك المعلومات أو قاعدة البيانات: د. مدحت محمد محمود عبد العال، برامج المعلومات، طبيعتها القانونية والعقود الواردة عليها، دراسة مقارنة للقوانين المصرية والإماراتية والفرنسية، معهد دبي القضائي، سلسلة الدراسات القانونية والقضائية،(11) الطبعة الأولى، 1434 هـ- 2013م، ص 137 وما بعدها.

(3) يمكن أن نتصور بخصوص تكييف العقد في الواقع العملي، وجود تكييفات مستبعدة وأخرى ممكنة. بالنسبة للتكييفات المستبعدة تكييف العقد على أنه عقد بيع لأن ملكية البريد الإلكتروني تظل للشركة مقدمة خدمة البريد الإلكتروني ولا يمكن أن تتنازل عنها أبداً، كما أن هذا التكييف يفترض وجود " ثمن" مقابل خدمة البريد الإلكتروني، وهذا ما لا يتوافر في أحيان كثيرة. أما التكييفات الممكنة والواقعية، فتكييف العقد على أنه عقد عارية أو هبة انتفاع أو إيجار أو مقاولة، بحسب الأحوال. انظر في مدى واقعية وإمكانية هذه التكييفات بخصوص عقد الاستفادة من معلومات بنك المعلومات: د. مدحت محمد محمود عبد العال، المرجع السابق، ص 137 وما بعدها.

المطلب الثاني
ملكية الشخص لمحتويات البريد الإلكتروني

ليس لدينا أي شك في أن المستفيد من خدمة البريد الإلكتروني يملك محتويات هذا البريد، سواء كانت لها قيمة مالية أو ليس لها سوى قيمة أدبية فقط. فهو يملك الأوراق والمستندات ذات القيمة المالية وتشكل جزءاً من ذمته المالية. أما مجرد الخطابات أو المعلومات، فهي تتصل بالجانب الشخصي لصاحب البريد، فهي وإن لم يكن لها قيمة مالية في ذاتها، إلا أن استخدامها بشكل معين أو الاعتداء عليها أو إفشاءها قد تترتب عليه آثار مالية.

وإذا كانت محتويات البريد الإلكتروني ملكاً للمستفيد من خدمة البريد الإلكتروني، فإنه يتمتع عليها بكافة سلطات المالك على ملكه من استعمال واستغلال وتصرف، بمقابل أو بدون مقابل، حال حياته[1]. أما بعد وفاته فإنها تنتقل أيضاً إلى ورثته، على التفصيل التالي.

المطلب الثالث
مدى انتقال محتويات البريد الإلكتروني إلى الورثة

فيما يتعلق بمدى انتقال محتويات البريد الإلكتروني إلى ورثة المستفيد من البريد الإلكتروني، يقترح بعض المؤلفين إيراد شرط في عقد إنشاء البريد الإلكتروني بين المستفيد من الخدمة والشركة مقدمة الخدمة يحدد مصير محتويات البريد الإلكتروني[2]. وهذا الاقتراح لا يقدم حلاً في الحقيقة، ولكنه رأياً وصائياً يجد مجال تطبيقه في إرادة الأطراف.

أما الحل وفقا لقواعد الشرع والقانون، فيلزم التفرقة بين محتويات البريد الإلكتروني ذات القيمة المالية وتلك التي لا تتمتع سوى بقيمة أدبية أو وجدانية أو عاطفية.

فالأولى تدخل في الذمة المالية للمستفيد من خدمة البريد الإلكتروني وتنتقل إلى

(1) قارن: د. عبد الهادي العوضي، المرجع السابق، ص 48 وما بعدها، حيث يقرر بصفة عامة " ليس من شك في أن البريد الإلكتروني يكون ملكاً لصاحب العنوان البريدي سواء أكان شخصا طبيعيا أم اعتباريا. فهذا الأخير وفقا لعقد الاشتراك contrat d'abonnement مع مورد خدمة منافذ الدخول لمستخدم البريد الإلكتروني تحت مسؤوليته".

(2) أشار اليه د. عبد الهادي العوضي، المرجع السابق، ص 53.

ورثته كاملة بعد وفاته في شقيها الملكية والدفاع، بحيث يملكها الورثة مادياً ويستطيعون الدفاع عنها قانونياً. ويسري على هذه المحتويات ما يسري على أموال التركة من أحكام، وتؤول إلى الورثة كل بحسب نصيبه الشرعي في الميراث (انظر المواد 1242 وما بعدها من قانون المعاملات المدنية).

أما الثانية فلا تنتقل للورثة إلا في جانبها الدفاعي فقط، حيث يملك الورثة سلطة الدفاع عنها بالوسائل القانونية في حال الاعتداء عليها بأي شكل يمس بمورثهم أو ذكراه.

ولم يرد في قانون المعاملات المدنية الإماراتي نص يحدد كيفية قسمة الأوراق العائلية أو الأشياء التي تتصل بعاطفة الورثة نحو المورث. ويمكن هنا تطبيق حكم المادة 905 من التقنين المدني المصري التي تنص على أنه " إذا لم يتفق الورثة علي قسمة الأوراق العائلية أو الأشياء التي تتصل بعاطفة الورثة نحو المورث، أمرت المحكمة إما ببيع هذه الأشياء أو بإعطائها لأحد الورثة مع استنزال قيمتها من نصيبه في الميراث أو دون استنزال، ويراعى في ذلك ما جرى عليه العرف وما يحيط بالورثة من ظروف شخصية".

ونقول بهذا الحكم استناداً إلى أن البريد الإلكتروني" يشكل عنصراً خاصاً من عناصر التركة ينتقل بالوفاة إلى الورثة"، فإنه يمكن قياسه على الأوراق العائلية والأشياء التي تتصل بعاطفة الورثة نحو المورث[1]،" كمذكراته وشهاداته وأوسمته وملابسه الرسمية وصوره الفوتوغرافية وما تركه من ذكريات مادية كالأسلحة وأصول المؤلفات والمكتب الذي كان يقعد عليه والقلم الذي كان يكتب به وما إلى ذلك" [2].

هذا ويجب على الشركة مقدمة خدمة البريد الإلكتروني أن تسمح لورثة المستفيد من خدمة البريد الإلكتروني بالدخول إلى الحساب البريدي للمتوفى، على أن يقدم الورثة ما يثبت صلة القرابة بينهم وبين المتوفى. وهذا ما فعلته بعض الشركات مقدمة خدمة البريد الإلكتروني، مثل شركة America Online [3].

(1) د. عبد الهادي العوضي، الجوانب القانونية للبريد الإلكتروني، رقم 24، ص 54.

(2) د. عبد الرزاق أحمد السنهوري، الوسيط في شرح القانون المدني، الجزء التاسع، أسباب كسب الملكية، مع الحقوق العينية الأصلية المتفرعة عن الملكية، تنقيح المستشار/ أحمد مدحت المراغي، الناشر: منشأة المعارف بالإسكندرية، 2004، رقم 65، ص 165 وما بعدها.

(3) انظر د. عبد الهادي العوضي، الجوانب القانونية للبريد الإلكتروني، رقم 23، ص 53.

الفصل الثاني
صور الاعتداء على البريد الإلكتروني

نعرض هنا لصور الاعتداء على البريد الإلكتروني في ضوء حماية الفقه الإسلامي للممتلكات(المبحث الأول)، وفي القانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات (المبحث الثاني).

المبحث الأول
صور الاعتداء على البريد الإلكتروني
في ضوء حماية الفقه الإسلامي للممتلكات

لقد أشاد الفقه الإسلامي ـ استناداً إلى مصادره من القرآن والسنة والإجماع والقياس وغيرها من المصادر ـ نظاماً محكماً لحماية الأموال والحقوق والممتلكات[1]، يحرم بمقتضاه الاعتداء، كما وضع أسس الاستغلال الحسن لهذه العناصر، بحيث يقرر الأول التجريم والضمان[2]، ويواجه الثاني الاستثمار المشروع للأموال والتحذير من الطرق غير المشروعة.

وفي ضوء هذا النظام الدقيق، يمكن دراسة صور الاعتداء على البريد الإلكتروني في الفقه الإسلامي على النحو التالي[3]:

إتلاف البريد الإلكتروني: أول صورة للاعتداء على البريد الإلكتروني نعرض لها في

(1) محمد لافي، حفظ المال في المفهوم الإسلامي، مقال متاح على شبكة الإنترنت في 1436/8/20 هـ:
http://www.almoslim.net/node/234913

(2) انظر في فكرة الضمان: د. وهبة الزحيلي، نظرية الضمان أو أحكام المسئولية المدنية والجنائية في الفقه الإسلامي، دراسة مقارنة، دار الفكر، دمشق- سوريا،1998.

(3) انظر: عبد الله بن ناصر بن أحمد العمري، الحماية الجنائية للبريد الإلكتروني، المرجع السابق ص152 وما بعدها. وبصفة عامة انظر: د. محمد عبيدلي، جرائم الأموال الإلكترونية وعقوبتها، دراسة مقارنة بين الفقه الاسلامي وقانون دولة الامارات العربية المتحدة، 2013؛ د. الشحات إبراهيم محمد منصور، الجرائم الإلكترونية في الشريعة الاسلامية والقوانين الوضعية، بحث فقهي مقارن، دار الفكر الجامعي، الإسكندرية،2011.

الفقه الإسلامي هي إتلاف البريد الإلكتروني. وهو من أسباب الضمان بشرط أن يكون واقعاً على مال متقوم من وجهة نظر الشرع الإسلامي. والإتلاف قد يقع على العين ذاتها، مثل إتلاف جهاز الحاسب الآلي بكسره أو بحرقه، وقد يقع الإتلاف على المنفعة، مثل إتلاف منفعة البريد الإلكتروني، عن طريق تعطيل أجهزة الشركة مقدمة الخدمة أو إتلاف البريد الإلكتروني عن طريق الفيروسات أو تعبئة السعة التخزينية للبريد الإلكتروني عن طريق الرسائل غير المرغوب فيها (الرسائل الإقتحامية الضارة بالبريد الإلكتروني). وسواء وقع الإتلاف مباشرة أو بالتسبب، فإنه يوجب الضمان، كما سنرى فيما بعد عند التعرض للجزاء المدني. ويشترط للضمان في هذه الحالة أن يكون المتلف مالا متقوما، فإن لم يكن مالا أو كان مالا ولكن غير متقوم فلا ضمان.

غصب البريد الإلكتروني: يقصد بالغصب أخذ الشيء ظلما أو بغير حق من صاحبه وإزالة يده عنه والظهور عليه بمظهر المالك له. والغصب محرم في الشرع الإسلامي بنص الكتاب والسنة والإجماع. وقد يقع الغصب على العقار وقد يقع على المنقول، وفي جميع الأحوال يلزم رد المال المغصوب إلى صاحبه ـ أصله وما حصل فيه من زيادة ـ ، وهذا هو ضمان الغاصب الذي اعتدى على مال الغير. ويعتبر اختراق البريد الإلكتروني والاستيلاء عليه غصباً له، ويلتزم المغتصب بالضمان، بأن يرد البريد الإلكتروني إلى صاحبه وتعويضه عن الأضرار التي أصابته نتيجة الغصب.

التجسس على البريد الإلكتروني: يقصد بالتجسس تتبع الأخبار وعورات الناس وكشفها بعد أن كانت مختبئة. والتجسس محرّم بالقرآن والسنة. فقد حرّم القرآن الكريم والسنة الشريفة تتبع عورات الناس وكشف أسرارهم. والتجسس جريمة يعاقب من يقوم بها تعزيراً من قبل القاضي. ومن التجسس المحرّم؛ التجسس على البريد الإلكتروني وتتبع أخبار وأسرار صاحبه والكشف عنها للناس، بغير حق. وهذا يعني أن التجسس لو كان واقعاً على البريد الإلكتروني للمجرمين واللصوص وأعداء الأمة، فلا شيء فيه ولا يعاقب فاعله.

التزوير بواسطة البريد الإلكتروني: يقصد بالتزوير إظهار الأمر على غير حقيقته بتحسينه وتجميله بالكذب. والتزوير محرّم في الشرع الإسلامي بالكتاب والسنة. ومن أكثر الجرائم التي ترتكب عن طريق البريد الإلكتروني والإنترنت عموماً هي جريمة التزوير، بل أنها تدخل أو مشتقاتها في كل الجرائم الإلكترونية تقريباً، مثل استخدام تقنية أو شفرة

معينة للوصول إلى تغيير الحقيقة، أو عمل عناوين بريد إلكترونية لشركات أو لشخصيات معينة. ويضمن المزور ما سببه من ضرر لمستخدم البريد الإلكتروني نتيجة هذا التزوير.

الاحتيال والنصب عن طريق البريد الإلكتروني: يقصد بالاحتيال أو النصب استخدام وسائل غير مشروعة للوصول إلى غاية غير مشروعة. كمن يكذب لإقناع الناس بشيء معين توصلاً للحصول على أموالهم. والاحتيال والنصب حرام في الشرع الإسلامي. ويمكن استخدام البريد الإلكتروني في النصب والاحتيال من أجل أكل أموال الناس بالباطل. مثال ذلك إرسال بعض الرسائل الإلكترونية لمستخدمي البريد الإلكتروني عن بنك أو خدمة أو شركة وهمية، من أجل الاستيلاء على أموالهم، ومثل من يرسل رسالة بأنه سوف يقدم للمستخدم في قرعة معينة، مثل قرعة الجرين كارد، أو ترتيب الهجرة إلى بلد معين، من أجل الحصول على أموال مستخدم البريد الإلكتروني دون أن يقدم له خدمة حقيقية، وهكذا.

المبحث الثاني
صور الاعتداء على البريد الإلكتروني في القانون رقم 5 لسنة 2012

لم يذكر المشرع الإماراتي في القانون الاتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات – ومن قبله القانون رقم 2 لسنة 2006– البريد الإلكتروني ضمن وسائل تقنية المعلومات في المادة الأولى المخصصة للتعريفات، ومع ذلك تنطبق أحكام هذا القانون على تقنية البريد الإلكتروني[1]، بوصفه نظام معلومات إلكتروني أو وسيلة تقنية معلومات (المطلب الأول) [2]، ولكن ذكر البريد الإلكتروني في المادة العاشرة فقرة ثالثة منه، وهي تنظم ما يمكن تسميته " الجرائم الواقعة على البريد الإلكتروني" (المطلب الثاني) [3].

(1) عبد الله بن ناصر بن أحمد العمري، الحماية الجنائية للبريد الإلكتروني، المرجع السابق، ص106 وما بعدها، حيث طبق المؤلف أحكام القانون رقم 2 لسنة 2006 على الاعتداء الذي يقع على البريد الإلكتروني.

(2) ويثير هذا الاجتهاد مبدأ الشرعية في مجال جرائم تقنية المعلومات. وهنا يمكن القول بأن مبدأ الشرعية يحظر اللجوء إلى القياس ولكنه لم يشترط أن يكون التفسير ضيقاً، فالشرعية الجنائية لا تستلزم بالضرورة التفسير الضيق، وذلك لأن مثل هذا التفسير سيجعل القانون عاجزاً عن مواجهة التطورات الحديثة، كما سيوصم هذا الأمر بعدم المعقولية: هل من المعقول أن تنطوي عبارة النص على حصر أو إشارة لكل الحالات الضارة في المجتمع؟ انظر في هذا المعني: م. د. فتحي محمد أنور عزت، جرائم العصر الحديث، الطبعة الأولى، دار الفكر والقانون، المنصورة، 2010، ص 641.

(3) انظر حول سياسة المشرع الإماراتي في مواجهة جرائم تقنية المعلومات: د. أحمد عبد المجيد الحاج، المسؤولية الجنائية لجرائم النشر

المطلب الأول
صور الاعتداء على البريد الإلكتروني باعتباره نظام معلومات إلكتروني أو وسيلة تقنية معلومات

البريد الإلكتروني هو نظام معلومات إلكتروني، وأيضاً وسيلة تقنية المعلومات، ومن ثم يكون محمياً بالنصوص الجزائية التي وردت في قانون مكافحة تقنية المعلومات. وهذا تطبيقاً لما ورد في المادة الأولى من هذا القانون المخصصة للتعريفات، حيث عرّفت " نظام المعلومات الإلكتروني" بأنه " مجموعة برامج معلوماتية ووسائل تقنية المعلومات المعدة لمعالجة وإدارة وتخزين المعلومات الإلكترونية أو ما شابه ذلك". كما عرفت " وسيلة تقنية المعلومات" بأنها " أي أداة إلكترونية مغناطيسية، بصرية، كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية وأداء العمليات المنطقية والحسابية، أوالوظائف التخزينية، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر، تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية أوإيصالها للغير".

وقد طبق القضاء الإماراتي على جرائم الاعتداء على البريد الإلكتروني ـ قبل صدور القانون رقم 5 لسنة2012 واستحداثه جريمة الاعتداء على البريد الإلكتروني ـ نصوص قانون العقوبات الاتحادي رقم 3 لسنة 1987 المعدل بالقانون الاتحادي رقم 34 لسنة 2005، ومواد القانون الاتحادي رقم 2 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات[1].

وتطبيقاً لهذا النظر، يمكن أن يتخذ الاعتداء على البريد الإلكتروني ـ وفقاً للقانون رقم 5 لسنة 2012 ـ إحدى الصور الآتية:

1- دخول البريد الإلكتروني بدون ترخيص أوتجاوز حدود الترخيص أو البقاء فيه بصورة غير مشروعة (م 2).

الإلكتروني في ضوء قانون مكافحة جرائم تقنية المعلومات الإماراتي، دورية الفكر الشرطي، العدد 85، ابريل 2013، ص 167؛ عقيد د. عبيد صالح حسن، سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، دورية الفكر الشرطي، العدد 95، أكتوبر 2015، ص 21. وانظر أيضاً: د. عبد الرازق الموافي عبد اللطيف، قراءة في قانون مكافحة جرائم تقنية المعلومات الإماراتي الجديد " المرسوم بقانون اتحادي رقم 5 لسنة 2012، مجلة معهد دبي القضائي، السنة الأولى، العدد 2، ربيع الثاني 1434هـ- مارس 2013 م، ص 139.

(1) انظر على سبيل المثال: حكم محكمة تمييز دبي، جلسة 31-8-2008، الطعن رقم 249/2008 جزاء، الموقع الإلكتروني لمحاكم دبي، وانظر في التعليق على هذا الحكم: د. عبد الرازق الموافي عبد اللطيف، تعليق على قضاء دبي بشأن الاختصاص القضائي بجرائم الإنترنت، مجلة معهد دبي القضائي، العدد1، السنة الأولى، جمادى الآخرة 1433ـــ مايو 2012م، ص 107 وما بعدها.

في هذه الصورة من الاعتداء، يتمثل الركن المادي للجريمة في دخول الشخص إلى نظام معلومات إلكتروني أو وسيلة تقنية معلومات وهي هنا البريد الإلكتروني بدون ترخيص له بهذا الدخول. كما قد يتمثل الركن المادي أيضاً في تجاوز حدود الترخيص، ويتعلق ذلك في حالة الترخيص للشخص بالدخول إلى البريد الإلكتروني والاستفادة من خدماته خلال فترة معينة أو بعدد معين من الخدمات، فيظل داخل البريد الإلكتروني بعد فوات الفترة الزمنية أو النطاق المحدد للخدمات[1].

وتثير هذه الصورة من الاعتداء مسألة الدخول التلقائي والدخول غير الإرادي للبريد الإلكتروني، فمن يدخل إلى البريد الإلكتروني بدون إرادة منه، يتوجب عليه الخروج فور علمه واكتشافه ذلك، أما إذا استمر في البقاء فإن هذا يعد بقاء غير مشروع في البريد الإلكتروني.

أما الركن المعنوي للجريمة فيتمثل في قصد الدخول بدون ترخيص أو تجاوز حدود الترخيص أو البقاء بصورة غير مشروعة. ويتضح من هذا أن الاعتداء على البريد الإلكتروني يتخذ هنا صورة العمد. غير أن هذا مجرد استنتاج تقتضيه طبيعة الجريمة، حيث أن المشرع لم يحدد صورة الركن المعنوي، ولكنه اجتهاد يخالف صريح نص المادة 43 من قانون العقوبات الاتحادي الذي جاء فيها أنه " يسأل الجاني عن الجريمة سواء ارتكبها عمداً أم خطأ ما لم يشترط العمد صراحةً". وبناء على ذلك يكون الاعتداء على البريد الإلكتروني مجرماً سواء وقع عمداً أم عن طريق الخطأ[2]. وهذا وضع يخالف نظرية القصد الجنائي، بل يطيح بها ـ على حد تعبير البعض ـ لأنها تشترط للعقاب معاصرة القصد مع النشاط الإجرامي[3].

(1) انظر في هذا المعنى بصفة عامة: د. عبد الرازق الموافي عبد اللطيف، شرح قانون مكافحة تقنية المعلومات لدولة الإمارات العربية المتحدة، " المرسوم بالقانون الاتحادي رقم 5 لسنة 2012"، الكتاب الأول: الجرائم المتعلقة بدخول أو إعاقة الوصول إلى المواقع والشبكات، والتزوير الإلكتروني، والبيانات الطبية، والبرامج الضارة، والاحتيال الإلكتروني، ووسائل الدفع الإلكتروني، والأرقام السرية، والشفرات، والاتصالات، والتهديد والابتزاز، والمواد الإباحية والقمار والآداب العامة. معهد دبي القضائي، سلسلة الدراسات والبحوث القانونية والقضائية العلمية المحكمة،(13)، ص 24.

(2) ويخالف هذا النص الأصول العامة في قانون العقوبات التي تقضي بأن الأصل في الجرائم أنها عمدية ولا عقاب على غير العمد إلا بنص خاص. انظر في ذلك:عبد الرازق الموافي عبد اللطيف، شرح قانون مكافحة تقنية المعلومات لدولة الإمارات العربية المتحدة،" المرسوم بالقانون الاتحادي رقم 5 لسنة 2012، ص 25، والمراجع التي أشار إليها في هوامش الصفحة ذاتها. وفي عرض الاتجاهات التشريعية في القصد الجنائي عموماً انظر: د. محمود نجيب حسني، النظرية العامة للقصد الجنائي، دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، الطبعة الثالثة، دار النهضة العربية، القاهرة، 1988، وبصفة خاصة ص 16 وما بعدها.

(3) د. محمد حماد مرهج الهيتي، الجريمة المعلوماتية، دار الكتب القانونية، مصر ـــــ الإمارات، 2014، ص 325.

2- الدخول بغير ترخيص إلى بريد إلكتروني بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية (م 4).

ويتمثل السلوك الإجرامي في الدخول بغير ترخيص إلى نظام معلوماتي إلكتروني أو وسيلة تقنية معلومات (وهو هنا بريد إلكتروني)، وهذا يشكل الركن المادي للجريمة. أما الركن المعنوي فيتمثل في أن هذا الدخول يكون بقصد الحصول على بيانات حكومية (سرية أو غير سرية) أو معلومات سرية خاصة بمنشأة مالية أوتجارية أو اقتصادية[1].

ويقصد بالبيانات الحكومية: البيانات أو المعلومات الإلكترونية الخاصة أو العائدة إلى الحكومة الاتحادية أو الحكومات المحلية لإمارات الدولة أوالهيئات العامة أو المؤسسات العامة الاتحادية أوالمحلية (م1). والمعلومات السرية: هي أي معلومات أو بيانات غير مصرح للغير بالاطلاع عليها أو بإفشائها إلا بإذن مسبق ممن يملك هذا الإذن(م1). أماالمنشأة المالية أوالتجاريةأوالاقتصادية فهي أي منشأة تكتسب وصفها المالي أو التجاري أو الاقتصادي بموجب الترخيص الصادر لها من جهة الاختصاص بالدولة (م 1).

3- حصول أو تعديل أو إتلاف أو إفشاء بغير تصريح بيانات أو معلومات يتضمنها البريد الإلكتروني وكانت هذه البيانات أو المعلومات تتعلق بفحوصات طبية أو تشخيص طبي أو علاج أو رعاية طبية أو سجلات طبية (م7). في هذه الصورة من الاعتداء التي يحمي المشرع فيها "الخصوصية المعلوماتية" [2]، يتكون الركن المادي للجريمة من السلوك الإجرامي المتمثل في الحصول أو الاستحواز أوالتعديل أوالإتلاف أوالإفشاء للبيانات أوالمعلومات الطبية التي يتضمنها البريد الإلكتروني عن طريق استعمال الشبكة المعلوماتية أو موقع إلكتروني أو نظام معلومات إلكتروني أو وسيلة تقنية معلومات، أما الركن المعنوي فيها فيتكون من القصد الجنائي العام الذي يتكون من العلم والإرادة، العلم بأنه يقوم بسلوك من شأنه الاعتداء على معلومات طبية تخص المجني عليه، وأن يقوم بهذا السلوك بإرادته وليس مرغماً أو جاهلاً

(1) وسوف نرى أن المشرع قد شدد العقوبة إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر. هذا وسوف نرى أيضا أن المشرع لم يتعرض لحالة دخول الجاني بقصد الإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر للبيانات أو المعلومات الحكومية أو السرية الخاصة بمنشأة مالية أو تجارية أو اقتصادية. انظر ما يلي ص

(2) في هذا المعنى، انظر: د. أيمن عبد الله فكري، الجرائم المعلوماتية، المرجع السابق، ص 918.

بأثره. وعلى ذلك، إذا انتفى العلم أو انعدمت الإرادة ينتفي القصد الجنائي [1].

4- تعطيل أو إعاقة الوصول إلى البريد الإلكتروني(م8). يعاقب المشرع " كل من أعاق أو عطل الوصول إلى شبكة معلوماتية أو موقع إلكتروني أو نظام معلومات إلكتروني"، بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين. وفي هذه الصورة من الاعتداء، يتمثل الركن المادي للجريمة في ارتكاب الفاعل إعاقة أو تعطيل الوصول إلى إلى نظام معلومات إلكتروني وهو هنا البريد الإلكتروني، بما يؤدي إلى النتيجة التي يريدها الجاني وهي هنا إعاقة أو تعطيل الوصول إلى البريد الإلكتروني بالفعل. أما الركن المعنوي في هذه الجريمة فهو القصد الجنائي العام الذي يتكون من العلم والإرادة.

5- إتلاف أو مسح أو تغيير أو تدمير أو تعطيل البريد الإلكتروني أو البيانات أو المعلومات الموجودة به عن طريق إدخال برنامج معلومات بدون ترخيص (م10 فقرة 1 وفقرة 2). يعاقب المشرع " كل من أدخل عمداً وبدون تصريح برنامج معلوماتي إلى الشبكة المعلوماتية أو نظام معلوماتي إلكتروني أو إحدى وسائل تقنية المعلومات وأدى ذلك إلى إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرنامج أو النظام أو الموقع الإلكتروني أو البيانات أو المعلومات" م 1/10). وكذلك يعاقب المشرع الشروع في هذه الجريمة في حالة إذا لم تتحقق النتيجة (م 2/10). ويتمثل الركن المادي لهذه الجريمة في إدخال الجاني وبدون تصريح برنامج معلوماتي في الشبكة المعلوماتية أو نظام معلوماتي إلكتروني أو إحدى وسائل تقنية المعلومات، وأن يؤدي هذا الإدخال (في حالة الجريمة الكاملة) إلى إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرنامج أو النظام أو الموقع الإلكتروني أو البيانات أو المعلومات، أولا يؤدي إلى هذه النتيجة في حالة الشروع في هذه الجريمة. أما الركن المعنوي في هذه الجريمة يأخذ صورة القصد الجنائي العام بعنصريه العلم والإرادة، وهو تعمد ارتكاب الجريمة كاملة فتتحقق كاملة في الفرض الأول، وتخيب أولا تتحقق النتيجة بسبب لا يد له فيه.

(1) قارن : د. عبد الرازق موافي عبد اللطيف، شرح قانون مكافحة تقنية المعلومات لدولة الإمارات العربية المتحدة، " المرسوم بالقانون الاتحادي رقم 5 لسنة 2012، الكتاب الأول، ص 99 وما بعدها: " ففي الاتلاف على سبيل المثال ينتفي العلم في حالة استعمال الجاني قرص مرن أو إسطوانة بها فيروسات دون علمه باصابتها بفيروسات تضر بالمعلومات أو البيانات الطبية (...) وفي حالة انعدام الإرادة ينتفي القصد الجنائي، كأن يحدث فعل الحصول او الاستحواذ او التعديل او الاتلاف او الافشاء للبيانات وللمعلومات الطبية دون أن تتجه إرادة الجاني إلى ذلك".

6- الحصول على رقم سري أو شفرة أو كلمة مرور أو أي وسيلة أخرى للدخول إلى البريد الإلكتروني بدون تصريح (م 14 فقرة 1). عاقب المشرع هنا " كل من حصل بدون تصريح على رقم سري أو شفرة أو كلمة مرور أو أي وسيلة أخرى للدخول إلى وسيلة تقنية معلومات أو موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلوماتية أو معلومات إلكترونية". ويتكون الركن المادي لهذه الجريمة من أي فعل يؤدي إلى الحصول على رقم سري أو شفرة أو كلمة مرور أو أي وسيلة أخرى للدخول إلى وسيلة تقنية معلومات أو موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلوماتية أو معلومات إلكترونية، وأن يتم ذلك الفعل بدون تصريح ممن يملك التصريح، أما الركن المعنوي فيتكون من القصد الجنائي العام بعنصريه العلم والإرادة.

المطلب الثاني
صور الاعتداء على البريد الإلكتروني تطبيقاً للنص الخاص بجريمة "الاعتداء على البريد الإلكتروني"

على الرغم من عدم ذكر البريد الإلكتروني في المادة الأولى منه المتعلقة بالتعريفات، إلا أن قانون مكافحة جرائم تقنية المعلومات قد ذكر البريد الإلكتروني في الفقرة الثالثة من المادة العاشرة منه.

فقد عاقبت الفقرة الثالثة من المادة العاشرة من المرسوم بقانون بشأن مكافحة جرائم تقنية المعلومات بالحبس والغرامة أو بإحدى هاتين العقوبتين " أي فعل عمدي يقصد به إغراق البريد الإلكتروني بالرسائل وإيقافه عن العمل أو تعطيله أو إتلاف محتوياته". وكانت هذه هي المناسبة الوحيدة التي ذكر فيها ـ صراحةً ـ قانون مكافحة جرائم تقنية المعلومات الاعتداء على البريد الإلكتروني. أما بقية صور الاعتداء على البريد الإلكتروني فتنطبق عليه باعتباره " نظام معلومات إلكتروني" أو " وسيلة تقنية معلومات"، كما رأينا.

ويمكن أن يتخذ الاعتداء على البريد الإلكتروني ـ تطبيقاً للمادة 3/10 من القانون رقم 5 لسنة 2012 ـ إحدى الصور الآتية[1]:

1. إغراق البريد الإلكتروني بالرسائل: ويكون الإغراق عن طريق إرسال عدد كبير من الرسائل التي تؤدي إلى امتلاء مساحة البريد الإلكتروني، الأمر الذي اعتبره المشرع اعتداء على البريد الإلكتروني. وهذه الرسائل قد تكون رسائل إعلانية أو إقحامية وهي ما يعرف بالرسائل غير المرغوب فيها، وقد تكون رسائل عادية ولكنها كثيرة لدرجة تقلل كفاءة البريد الإلكتروني.

2. ايقاف البريد الإلكتروني عن العمل: ويكون ذلك عن طريق استخدام برنامج معلوماتي أو فيروسات أو نقل معلومات معينة تؤدي إلى إيقاف البريد الإلكتروني عن العمل. وأخطر هذه الوسائل الفيروسات، وهي متعددة الأشكال، وتؤدي إلى إيقاف البريد الإلكتروني.

3. تعطيل البريد الإلكتروني: والعطل يرادف الإيقاف عن العمل، ويقصد منه المشرع إحكام الحماية على البريد الإلكتروني ضد أي فعل يؤدي إلى إيقافه عن العمل أو تعطيله.

4. إتلاف محتويات البريد الإلكتروني: ويكون ذلك باستخدام وسائل معينة لتدمير وإتلاف ما يحويه البريد الإلكتروني من بيانات ومعلومات.

5. ويتكون الركن المادي لجريمة الاعتداء على البريد الإلكتروني من أي فعل من أفعال الاعتداء السابقة، أما الركن المعنوي فهو القصد الجنائي العام بعنصريه العلم والإرادة.

6. هذا وقد وضع المشرع الإماراتي في قانون مكافحة جرائم تقنية المعلومات عقوبات رادعة على الاعتداء على البريد الإلكتروني في جميع صور الاعتداء سالفة البيان[2].

(1) انظر في هذه الصور دراسة ل " جريمة الاعتداء على البريد الإلكتروني" : د. عبد الرازق الموافي عبد اللطيف، شرح قانون مكافحة جرائم تقنية المعلومات...، الكتاب الأول، المرجع السابق، ص 116 وما بعدها

(2) انظر ما يلي ص

الفصل الثالث
الوقاية من الاعتداء على البريد الإلكتروني

الوسائل الوقائية من الاعتداء على البريد الإلكتروني قد تكون تقنية أو فنية (المبحث الأول)، وقد تكون ذات طبيعة قانونية (المبحث الثاني). ونتناول هذه الوسائل تباعا.

المبحث الأول
الوقاية التقنية

تستخدم وسائل تقنية معينة من أجل منع التلاعب والتعديل في البيانات أو المعلومات المحفوظة في البريد الإلكتروني. مثال ذلك التشفير والتوثيق والتوقيع الإلكتروني والجدار الناري وغيرها.

ويقصد بالتشفير استخدام أرقام سرية لا يعرفها إلا المرسل والمستقبل، أما التوثيق فيقصد به اللجوء إلى طرف ثالث غير المرسل والمستقبل يمكن أن يطلق عليه وكالات الإثبات. أما التوقيع الإلكتروني فيعني اختصاص الشخص بتوقيع يميزه عن غيره في المجال الإلكتروني. وسنقتصر على التشفير والتصديق باعتبارهما أهم الوسائل التقنية:

أولا: التشفير La cryptologie [1]، وهي كلمة تجد جذورها في الكلمة اليونانية kruptos وهي تعني الشيء المخبأ Caché، هو مجموعة من التقنيات تسمح بحماية الاتصال وذلك عن طريق استخدام كتابة سرية. بالنظر إلى ذلك، يعني التشفير استخدام كود رقمي من أجل ترميز أو تعمية المعلومات حتى لا تدرك من قبل الغير.

(1) Sur la cryptologie voir: E. CAPRIOLI, " Le nouveau régime juridique de la cryptologie", Droit & Patrimoine, n° 67, janvier 1999, p.34 ; F. FORTIN, " Cryptologie : le tournant libéral du gouvernement", Droit & Patrimoine, n° 69, mars 1999, p.20 et voir aussi la fiche technique: la cryptologie, p.21; I. RENARD, Vive la signature électronique, Dalloz, Coll. DELMAS expresse, 2002, p.19 et s.; E. BARBARY, " Des décrets tant attendus: quel droit pour la cryptologie?" JCP, 1998, I, 124.

ويهدف التشفير إلى تحقيق وظيفتين: تحديد ماهية الشخص المتدخل في الاتصال عن بعد، والتأكد من أن الوثيقة المستقبلة هي ذات الوثيقة التي التزم بناء عليها هذا الشخص.

وتستند النظم التشفيرية على زوج من المفاتيح: المفتاح العام clé publique والمفتاح الخاص clé privée (ويسمى أيضا المفتاح السري clé secrète). فكل شخص يملك مفتاحا خاصا، معروف من جانبه فقط، عن طريقه يشترك في مفتاح عام، يستطيع الجميع الدخول إليه، فهو متاح للجميع.

ويتكون المفتاح العام والمفتاح الخاص، عمليا، من متواليات من الأرقام المتولدة في الوقت نفسه من لوغاريتم حسابي Algorithme mathématique [1]. ويرتبط المفتاحان حسابيا ببعضها البعض ولكن معرفة أحدهما لا تعني معرفة الآخر.

فكل مفتاح يسمح بعملية معينة يستطيع الآخر أن يأتي بعكسها. بعبارة أخرى، معرفة المفتاح العام لا تسمح بأية حال بمعرفة المفتاح الخاص، ولكن تسمح بفك شفرة الرسالة المشفرة بهذا المفتاح الخاص.

ويعتبر المفتاح الخاص أو السري (ويعرف بالتشفير المتماثل) وسيلة لتحديد الهوية رقميا، ويمكن إدخاله عن طريق دعامات متعددة مرتبطة بالكومبيوتر: برنامج logiciel، أو كارت ممغنط Carte à puce، أو قارئ للبصمة الرقمية أو iris، الذي يحول بيانا أو معطى معينا مرتبط بالكومبيوتر إلى ملف رقمي fichier numérique. وتعرف هذه الوسائل الأخيرة بالخواص الذاتية biométriques [2].

وينتمي المفتاح الخاص إلى التوقيع الرقمي للشخص. غير أنه على خلاف التوقيع اليدوي، الذي يصدر مباشرة عن الشخص، فالتوقيع الرقمي ينقل بواسطة دعامة إلكترونية.

(1) algorithme هو نظام العد العربي الذي اخترعه الخوارزمي.

(2) تعني الخواص الذاتية لفظة إنجليزية anglicisme تحدد مقاس العناصر المورفولوجية morphologiques للبشر، وهو يعادل المصطلح الفرنسي anthropométrie. فالبيومتري هو إذن نظام أوتوماتيكي للقياس يعتمد على معرفة الخصائص الجسدية أو السلوكية للفرد:

I. RENARD, Vive la signature électronique, Dalloz, coll. Delmas Express, 2002, p.20 et s.

بالإضافة إلى ذلك، قد يكون من السهل تقليد التوقيع الرقمي إذا وقع البرنامج أو الكارت الممغنط في يد شخص أخر بسبب عدم الإهمال في الحفاظ عليه من جانب صاحبه. غير أنه في حالة التوقيع بالخواص الذاتية يقل هذا الخطر بدرجة كبيرة.

أما المفتاح العام (ويعرف بالتشفير اللامتماثل) فيوضع على محرر أو مستند ينتمي إلى كارت التحديد الرقمي لهوية الشخص. هذا الكارت يرسل مع هذا المحرر أو المستند الرقمي الموقع عليه بواسطة تقنية المفتاح الخاص.

ويستطيع مستقبل الرسالة، عن طريق استخدام وسائل فنية مناسبة، أن يستخدم المفتاح لكي يتأكد أو يستوثق من أن التوقيع الموجود على المحرر هو بالفعل توقيع محرره. ويوضع المفتاح العام على شهادة التوقيع الإلكتروني للشخص.

ونظرا لأهمية هذه التقنية في حماية أمن المعاملات الإلكترونية، فقد تعهد القوانين بالتشفير إلى هيئة معتمدة، تسمى بالطرف الثالث محل الثقة، تقوم بتقديم مفاتيح فك شفرة رسائل البريد الإلكتروني[1]. وهذا ما فعله المشرع الإماراتي، حيث عهد بمهمة توثيق المعاملات الإلكترونية إلى هيئة اتصالات الإمارات. وعلى خلاف بعض القوانين كالقانون المصري[2]، لم يرد في القانون رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات أية

(1) انظر د. عبد الهادي العوضي، الجوانب القانونية للبريد الإلكتروني، ص 186.

(2) فقد قرر قانون التوقيع الإلكتروني رقم 15 لسنة 2004 أن التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية تتمتع بذات الحجية في الإثبات إذا ما توافرت فيها الشروط الآتية:

أ-

ب-

ج- إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني (م 18).

وأحال القانون إلى اللائحة التنفيذية لبيان هذه المسألة. وتقرر اللائحة التنفيذية في هذا الخصوص أنه " يتم من الناحية الفنية والتقنية، كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني الموقع إلكترونيا باستخدام تقنية شفرة المفتاحين العام والخاص وبمضاهاة شهادة التصديق الإلكتروني بأصل هذه الشهادة وتلك البيانات أو بأي وسيلة مشابهة" (م 11).

وقد بينت اللائحة التنفيذية أيضا المقصود بكل من التشفير ومفاتيحه المختلفة:

التشفير: منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيا بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة (م9/1).

تقنية شفرة المفتاحين العام والخاص (المعروفة باسم تقنية شفرة المفتاح العام): منظومة تسمح لكل شخص طبيعي أو معنوي بأن يكون لديه مفتاحين متفردين أحدهما عام متاح إلكترونيا، والثاني خاص يحتفظ به الشخص ويحفظه على درجة عالية من السرية (م10/1).

المفتاح الشفري العام: أداة إلكترونية متاحة للكافة، تنشأ بواسطة عملية حسابية خاصة، وتستخدم في التحقق من شخصية الموقع على

إشارة لتقنية التشفير. وكذلك لم يرد ذكر هذه التقنية في القانون الاتحادي رقم 1 لسنة 2006 في شأن المعاملات والتجارة الإلكترونية، ولا في القانون رقم 36 لسنة 2006 بتعديل قانون الإثبات الاتحادي رقم 10 لسنة 1992. بل عهد القانون رقم 1 لسنة 2006 بهذه المهمة إلى جهة معينة تقوم بمهمة توثيق المعاملات الإلكترونية.

ثانيا: التصديق أو التوثيق: Certification وهو يعني اللجوء إلى طرف ثالث محايد ومستقل عن الأطراف (سواء كان فردا عاديا أو شركة أو جهة من الجهات) من أجل توثيق المعاملات الإلكترونية للأشخاص[1]. وبهذا يتحدد وضع الموثق أو المصدق بأنه وسيط بين المتعاملين، يلجأ إليه بغرض منح الثقة في محرراتهم حتى يمكنهم أن يستخدموها لإثبات ما تتضمنه من تصرفات قانونية. ولهذا السبب يطلق عليهم البعض " وكلاء الإثبات: agents de preuve ".

التصديق هي عملية يتأكد بها من صحة المعاملات الإلكترونية يقوم بها طرف محايد، وهو في الغالب، طرف ثالث أجنبي عن المتعاقدين أطراف التعاقد الإلكتروني. ويسمى هذا الطرف الثالث في أوربا " مقدم خدمات التصديق" Prestataire de services de certification، ويسمى مزود خدمات التصديق، في الإمارات العربية المتحدة، وفي مصر يسمى جهة التصديق، وهكذا تختلف التسمية التي تطلق عليه في النظم القانونية المختلفة.

المحرر الإلكتروني، والتأكد من صحة وسلامة محتوى المحرر الإلكتروني الأصلي (م 11/1).

المفتاح الشفري الخاص: أداة إلكترونية خاصة بصاحبها، تنشأ بواسطة عملية حسابية خاصة وتستخدم في وضع التوقيع الإلكتروني على المحررات الإلكترونية، ويتم الاحتفاظ بها على بطاقة ذكية مؤمنة() (م12/1).

المفتاح الشفري الجذري: أداة إلكترونية تنشأ بواسطة عملية حسابية خاصة وتستخدمها جهات التصديق الإلكتروني لإنشاء شهادات التصديق الإلكتروني وبيانات إنشاء التوقيع الإلكتروني (م13/1).

(1) للمزيد من التفاصيل حول التصديق وما يرتبط به من خدمات انظر:

A. BENSOUSSAN, " Centre certificateur, authentification, preuve et contrôle", PA, 29 mai 1996, p.28; E. CAPRILI, " Sécurité et confiance dans le commerce électronique, signature numérique et autorité de certification", JCP, 1998, I, 123; B. POIDEVIN," De cadre juridique de la certification", juriscom.net, le 1er septembre 2002; D. GOBERT, " Commerce électronique : vers un cadre juridique général pour le tiers de confiance", Revue du droit des technologies de l'information", n°18, avril 2004, p.33.

د. إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية، مجلس النشر العلمي، جامعة الكويت، 2003، ص 143 وما بعدها.

أما عن طبيعة عملية التصديق، فيقول البعض [1]: إن منح شخص ثالث سلطة توثيق التوقيع يقرب مهمة الجهات القائمة على هذا الأمر من مهمة الموثق في النظام الفرنسي أي التأكد من شخص المتعاقد ومن مضمون التصرف المراد توثيقه. انطلاقا من هذا القول، عالج بعض الفقهاء موضوع سلطات التصديق الإلكتروني تحت اسم فكرة الموثق الإلكتروني Cyber notaire أو notaire électronique [2]. ومع ذلك يبقى فرق جوهري بين سلطات التصديق الإلكتروني والموثق يتمثل في أن هذه السلطات لا تملك أو ليس من مهمتها أن تتدخل في إنشاء وتأريخ وحفظ المحررات القانونية طبقا للإجراءات المنصوص عليها في القانون[3].

فمهمة جهة التصديق تقتصر على فحص التصرفات القانونية الإلكترونية وإعطاء ذوي الشأن شهادة بهذا المعنى تسمى شهادة التصديق الإلكتروني. ومع ذلك تشترك جهات التصديق مع الموثق في التحمل ببعض الالتزامات[4].

أما عن آلية التصديق الإلكتروني في مجال خدمات البريد الإلكتروني فهي تتلخص في أمرين أساسين[5]: وجود شخص من الغير محل ثقة يتوسط بين المرسل والمستقبل للبريد الإلكتروني ويعمل على تحديد هوية الطرفين وتحديد تاريخ الرسالة وحمايتها من الإختراق وغيره من الاعتداءات، النص على قرينة إفتراض صحة البريد الإلكتروني، متى استوفى ضوابط فنية وتقنية معينة.

(1) E. CAPRIOLI, “ Sécurité et confiance dans le commerce électronique, signature numérique et autorité de certification”, JCP, 1998, I, 123, n°29.

(2) Voir. A. GOBIN, “ Pour une problématique notaire des autoroutes de l’information”, JCPN, 1995, n°50, 51, p.1749, cité par E. CAPRIOLI, art. précité, n°29, à la marge 73.

وانظر في الموضوع تفصيلا: الدراسة القيمة للزميل الأستاذ الدكتور مصطفى أبو مندور موسى، الجوانب القانونية لخدمات التوثيق الإلكتروني، دراسة مقارنة، دار النهضة العربية، القاهرة، دون سنة نشر.

(3) E. CAPRIOLI, art. précité, n°29.

(4) حول مهمة الموثق والالتزامات الملقاة عليه انظر: د. عبد الحميد عثمان الحفني، المسئولية المدنية للموثق، دراسة مقارنة بين القانون المصري والفرنسي، مجلة البحوث القانونية والاقتصادية، كلية الحقوق- جامعة المنصورة، العدد الثاني عشر، أكتوبر 1992، ص 2؛ د. محمد محيى سليم، ذاتية مسئولية الموثق، دون ناشر ولا دار نشر، ولا سنة نشر.

(5) انظر في تفصيل ذلك: د. مصطفى أبو مندور موسى، الجوانب القانونية لخدمات التوثيق الإلكتروني، المرجع السابق، ص 74 وما بعدها.

1: وجود شخص ثالث محل ثقة يتوسط بين طرفي البريد الإلكتروني:

ويقوم بهذا الدور في القانون الإماراتي، كما مر بنا، مزود خدمات التصديق الإلكتروني. وقد عرف القانون الاتحادي رقم 1 لسنة 2006 في شأن المعاملات والتجارة الإلكترونية بدولة الإمارات العربية المتحدة [1] بالمادة الأولى منه " مزود خدمات التصديق" بأنه " أي شخص أو جهة معتمدة أو معترف بها تقوم بإصدار شهادات تصديق إلكترونية أو أي خدمات أو مهمات متعلقة بها وبالتوقيعات الإلكترونية والمنظمة بموجب أحكام هذا القانون" [2].

ومن التعريف المتقدم لجهة التصديق الإلكتروني يتحدد الدور الذي تضطلع به هذه الأخيرة، وهو يتمثل بصفة أساسية في إصدار شهادات التصديق الإلكتروني (البسيطة والمعتمدة)، وفي تقديم بعض الخدمات الأخرى.

كما نص القانون رقم 1 لسنة 2006 في المادة 20 على أنه: " لأغراض هذا القانون يعين بقرار من مجلس الوزراء جهة لمراقبة خدمات التصديق وعلى وجه الخصوص لأغراض ترخيص وتصديق ومراقبة أنشطة مزودي خدمات التصديق والإشراف عليها". وتنفيذا لهذا النص تم تعيين هيئة اتصالات الإمارات كجهة مراقبة لخدمات التصديق الإلكتروني[3].

كما نظم القانون المذكور في المواد 21 وما بعدها واجبات مزود خدمات التصديق وتنظيم عمل مزودي خدمات التصديق والاعتراف بشهادات المصادقة الإلكترونية والتوقيعات الإلكترونية الأجنبية[4].

(1) الجريدة الرسمية العدد 442 السنة السادسة والثلاثون محرم 1427 هـ يناير 2006 م.

(2) وهو نفس التعريف الذي أوردته المادة الثانية من قانون إمارة دبي رقم 2 لسنة 2002 بشأن المعاملات والتجارة الإلكترونية.

(3) في فرنسا، تختص الإدارة المركزية لسلامة نظم المعلومات بالتصديق على التوقيع الإلكتروني، ولها أن تمنح ترخيصا لمزاولة نشاط خدمات التصديق الإلكتروني لبعض الهيئات التي تستوفي الشروط التي تراها، كما أنها تختص باعتماد الهيئات الأجنبية المختصة بإصدار شهادات التصديق الإلكتروني (المرسوم الصادر من مجلس الدولة في 18 إبريل 2002).

أما في مصر، فإن هيئة تنمية صناعة تكنولوجيا المعلومات هي سلطة التصديق الإلكتروني العليا، ولها أن ترخص في مزاولة نشاط خدمات التصديق الإلكتروني وفقا للشروط والإجراءات المنصوص عليها في قانون التوقيع الإلكتروني ولائحته التنفيذية، كما أنها تختص باعتماد الجهات الأجنبية المختصة بإصدار شهادات التصديق الإلكتروني.

(4) المادة 21:

أولا: يجب على مزود خدمات التصديق:

أ- أن يتصرف وفقا للبيانات التي يقدمها بشأن ممارسته لنشاطه.

ب- أن يمارس عناية معقولة لضمان دقة واكتمال كل ما يقدمه من بيانات جوهرية ذات صلة بشهادة المصادقة الإلكترونية أو مدرجة

فيها طيلة سريانها.
ج- أن يوفر وسائل يكون من المعقول الوصول إليها وتمكن الطرف الذي يعتمد على خدماته من التأكد من الآتي:
1- هوية مزود خدمات التصديق.
2- أن الشخص المعينة هويته في شهادة المصادقة الإلكترونية, لديه السيطرة في الوقت المعني على أداة التوقيع المشار إليها في هذه الشهادة.
3- الطريقة المستخدمة في تعيين هوية الموقع.
4- وجود أية قيود على الغرض أو القيمة التي يجوز أن تستخدم من أجلها أداة التوقيع.
5- ما إذا كانت أداة التوقيع صحيحة ولم تتعرض لما يثير الشبهة.
6- ما إذا كان للموقع وسيلة لإعطاء إخطار بموجب هذا القانون.
7- ما إذا كان هناك وسيلة مناسبة للإبلاغ عن إلغاء التوقيع.
د- أن يوفر وسيلة للموقعين تمكنهم من تقديم إخطار بأن أداة التوقيع قد تعرضت لما يثير الشبهة، وأن يضمن توافر خدمة إلغاء للتوقيع يمكن استخدامها في الوقت المناسب.
هـ- أن يستخدم في أداء خدماته نظماً وإجراءات وموارد بشرية جديرة بالثقة.
و- أن يكون مرخصاً من مراقب خدمات التصديق إذا كان يعمل في الدولة.
ثانيا: لتقرير ما إذا كانت أية نظم أو إجراءات أو موارد بشرية جديرة بالثقة, لأغراض الفقرة (1/هـ) السابقة, يتعين الأخذ بالاعتبارات الآتية:
أ- الموارد المالية والبشرية بما في ذلك توافر الموجودات داخل منطقة الاختصاص.
ب- مدى الثقة في برامج وأجهزة الحاسب الآلي.
ج- إجراءات معالجة وإصدار شهادات المصادقة الإلكترونية وطلبات الحصول على هذه الشهادات والاحتفاظ بالسجلات.
د- توفر المعلومات الخاصة بالموقعين المحددين في شهادات المصادقة الإلكترونية, وكذلك توفير المعلومات للأطراف المعتمدة على خدمات التصديق.
هـ- انتظام ومدى مراجعة الحسابات من جانب جهة مستقلة.
و- وجود إعلان من الدولة أو من جهة اعتماد, أو من مزود خدمات التصديق بشأن وجود ما ذكره أو الالتزام به.
ل- مدى خضوع مزود خدمات التصديق للاختصاص القضائي لمحاكم الدولة.
ح- مدى التناقض بين القانون المطبق على أعمال مزود خدمات التصديق وقوانين الدولة.
ثالثا: يجب أن تحدد شهادة المصادقة الإلكترونية ما يأتي:
أ- هوية مزود خدمات التصديق.
ب- أن الشخص المعينة هويته في شهادة المصادقة الإلكترونية لديه السيطرة في الوقت المعني على أداة التوقيع المشار إليها في هذه الشهادة.
ج- أن أداة التوقيع كانت سارية المفعول في أو قبل تاريخ إصدار شهادة المصادقة الإلكترونية.
د- ما إذا كانت هناك أية قيود على الغرض أو القيمة التي يجوز أن تستخدم من أجلها أداة التوقيع أو شهادة المصادقة الإلكترونية.
هـ- ما إذا كانت هناك أية قيود على نطاق أو مدى المسؤولية التي قبلها مزود خدمات التصديق تجاه أي شخص.
رابعا: إذا حدثت أية أضرار نتيجة لعدم صحة شهادة المصادقة الإلكترونية أو نتيجة لأي عيب فيها, يكون مزود خدمات التصديق مسئولاً عن الخسائر التي يتكبدها:
أ- كل طرف تعاقد مع مزود خدمات التصديق حول تقديم شهادة المصادقة الإلكترونية.
ب- أي شخص اعتمد بصورة معقولة على شهادة المصادقة الإلكترونية التي أصدرها مزود خدمات التصديق.
خامسا: لا يكون مزود خدمات التصديق مسئولاً عن أي ضرر في الحالتين الآتيتين:
أ- إذا أدرج في شهادة المصادقة الإلكترونية بياناً يقيد نطاق ومدى مسؤوليته تجاه أي شخص ذي صلة, وفقا للائحة التي تصدر في هذا الشأن.
ب- إذا أثبت أنه لم يرتكب أي خطأ أو إهمال, أو أن الضرر قد نشأ عن سبب أجنبي لا يد له فيه.
المادة 22:

يصدر الوزير بناء على اقتراح المراقب اللوائح الخاصة بتنظيم وترخيص عمل مزودي خدمات التصديق الذين يعملون في الدولة, بما في ذلك ما يأتي:
1- ترخيص وتجديد ترخيص مزودي خدمات التصديق وممثليهم المفوضين وتجديد هذه التراخيص والمسائل المتعلقة بها.
2- أنشطة مزودي خدمات التصديق, ويشمل ذلك طريقة ومكان وأسلوب الحصول على أعمالهم وجذب الجمهور لها.
3- المعايير والقواعد التي يتعين على مزودي خدمات التصديق المحافظة عليها واتباعها في أعمالهم.
4- تحديد المعايير المناسبة فيما يتعلق بمؤهلات وخبرة مزودي خدمات التصديق وتدريب موظفيهم.
5- تحديد شروط إدارة الأعمال التي يقوم بها مزود خدمات التصديق.
6- تحديد محتويات وتوزيع المواد والإعلانات المكتوبة أو المطبوعة أو المرئية والتي يجوز أن يوزعها أو يستخدمها أي شخص فيما يتعلق بأية شهادة مصادقة إلكترونية أو مفتاح رقمي.
7- تحديد شكل ومحتوى أية شهادة مصادقة إلكترونية أو مفتاح رقمي.
8 ـــــ تحديد التفاصيل التي يجب تدوينها في الحسابات التي يحتفظ بها مزودو خدمات التصديق.
9- المؤهلات الواجب توافرها في مدققي حسابات مزودي خدمات التصديق.
10- وضع القواعد اللازمة لتنظيم التفتيش والتدقيق على أعمال مزودي خدمات التصديق.
11- شروط إنشاء وتنظيم أي نظام إلكتروني بواسطة مزود خدمات التصديق، سواء بمفرده أوبالاشتراك مع مزودي خدمات تصديق آخرين، وفرض وتغيير تلك الشروط أو القيود وفقا لاقتراح المراقب وبالتنسيق مع الجهات ذات الاختصاص.
12- الطريقة التي يدير بها الحاصل على الترخيص معاملاته مع عملائه، وكذلك عند تعارض مصالحه مع مصالحهم، وواجباته تجاههم فيما يتصل بشهادات المصادقة الإلكترونية الرقمية.
13- اقتراح الرسوم التي يجب استيفاؤها فيما يتصل بأي أمر مطلوب بموجب أحكام هذه المادة ويصدر بهذه الرسوم قرار من مجلس الوزراء.
14- وضع أية نماذج لأغراض تطبيق هذه المادة.
15- الغرامات المالية والجزاءات المقررة على مخالفة قواعد ترخي وتنظيم عمل مزودي خدمات التصديق.
المادة 23:
1- لتقرير ما إذا كانت شهادة المصادقة الإلكترونية أو التوقيع الإلكتروني نافذا قانوناً, لا يؤخذ في الاعتبار المكان الذي صدرت فيها هذه الشهادة أو التوقيع الإلكتروني، ولا بالاختصاص القضائي الذي يوجد فيه مقر عمل الجهة التي أصدرت هذه الشهادة أو التوقيع الإلكتروني.
2- تعتبر شهادة المصادقة الإلكترونية التي يصدرها مزودو خدمات التصديق الأجانب، كشهادة مصادقة إلكترونية صادرة من مزودي خدمات التصديق الذين يعملون بموجب هذا القانون، إذا كانت ممارسات مزودي خدمات التصديق الأجانب ذات مستوى من الوثوق يوازي على الأقل المستوى الذي تتطلبه المادة (20) من مزودي خدمات التصديق العاملين بموجب هذا القانون, ومع الأخذ في الاعتبار المعايير الدولية المعترف بها.
3- يجوز الاعتراف بالتوقيعات التي تستوفي شروط القوانين الخاصة بدولة أخرى، واعتبارها في مستوى التوقيعات الصادرة وفقاً لأحكام هذا القانون، إذا اشترطت قوانين الدولة الأخرى مستوى من الاعتماد على التوقيعات يوازي على الأقل المستوى الذي يشترطه هذا القانون لتلك التوقيعات.
4- يتعين بشأن الاعتراف بشهادات المصادقة الإلكترونية والتوقيعات الإلكترونية الأجنبية المنصوص عليه في الفقرتين (2) و(3) السابقتين، النظر إلى العوامل الواردة في الفقرة (2) من المادة (21) من هذا القانون.
5- لتقرير ما إذا كان التوقيع الإلكتروني أو شهادة المصادقة الإلكترونية نافذة قانونيا, يتعين أن يؤخذ بالاعتبار أي اتفاق بين الطرفين حول المعاملة التي يستخدم فيها ذلك التوقيع أو الشهادة.
6- استثناء من أحكام الفقرتين (2), (3) السابقتين:
أ- يجوز للأطراف في المعاملات التجارية والمعاملات الأخرى أن يتفقوا على استخدام مزودي خدمات تصديق معينين أو فئة معينة منهم أو فئة معينة من شهادات المصادقة الإلكترونية وذلك فيما يتصل بالرسائل أو التوقيعات الإلكترونية المقدمة لهم.
ب- وفي الحالات التي يتفق فيها الأطراف فيما بينهم على استخدام أنواع معينة من التوقيعات أو شهادات المصادقة الإلكترونية فإن هذا الاتفاق يعتبر كافيا لأغراض الاعتراف المتبادل بالاختصاصات القضائية للدول التي تتبعها هذه الأطراف، شريطة ألا يكون مثل هذا الاتفاق

ويلتزم مزود خدمات التصديق ببعض الالتزامات[1]: منها ضرورة الحصول على ترخيص بمزاولة النشاط من هيئة اتصالات الإمـارات، وضـرورة عدم التوقف عن النشاط إلا بعد الحصول على موافقة كتابية من الهيئة، والالتزام بعدم إفشاء سرية البيانات الإلكترونية، والالتزام باعتماد شهادات التصديق من الهيئة، سواء كانت هذه الشهادات صادرة عن جهات تصديق وطنية أو جهات تصديق أجنبية. كما ألزم المشرع جهة التصديق الإلكتروني بضرورة توفير نظم خاصة بتأمين المعلومات وحماية البيانات وبإصدار الشهادات وإدارة المفاتيح والشفرات، وفقا للمعايير الفنية والتقنية المتعارف عليها.

كما الزم القانون جهة التصديق الإلكتروني بضرورة التأكد من صحة البيانات المقدمة من طالب الترخيص مع التقيد بالبيانات المقدمة من هذا الأخير وعدم إضافة بيانات أخرى دون موافقة منه.

وأخيراً تلتزم جهة التصديق بضرورة التحديث المستمر لشهادات التصديق الإلكتروني، بما يضمن بث الثقة لدى المتعاملين معها.

2- النص على قرينة إفتراض صحة البريد الإلكتروني، متى استوفى ضوابط فنية وتقنية معينة:

وتقوم هذه القرينة على افتراض صحة البريد الإلكتروني، وبصفة خاصة البريد الإلكتروني الموصى عليه، متى استوفى الشروط الفنية والتقنية المطلوبة قانوناً. ويشترط لقيام هذه القرينة : أن يكون البريد الإلكتروني عبر مزود خدمة معتمد أي يخضع لتطبيق نظام التوثيق الإلكتروني، وأن يملك مقدم خدمة البريد الإلكتروني الضمانات الفنية والتقنية المتطلبة قانوناً، وبصفة خاصة التوقيع الإلكتروني وشهادة المصادقة الإلكترونية [2].

غير مشروع وفقا لأحكام القوانين المطبقة في الدولة.

(1) انظر في التزامات مقدم خدمات التصديق الإلكتروني بالتفصيل:د. سعيد السيد قنديل، التوقيع الإلكتروني، ماهيته- صوره- حجيته في الإثبات، بين التدويل والاقتباس، دار الجامعة الجديدة للنشر، الإسكندرية، 2004، ص 87 وما بعدها؛ د. خالد مصطفى فهمي، النظام القانوني للتوقيع الإلكتروني في ضوء التشريعات العربية والاتفاقيات الدولية، دار الجامعة الجديدة للنشر، الإسكندرية، 2007، ص 152 وما بعدها.

(2) د. مصطفى أبو مندور موسى، الجوانب القانونية لخدمات التوثيق الإلكتروني، المرجع السابق، ص77. ومن الجدير بالذكر أمرين: الأول: أن هذه القرينة قرينة بسيطة يجوز إثبات عكسها، والثاني: أنه في حالة إثبات عكس هذه القرينة، فلا يعني ذلك عدم مسؤولية مقدم الخدمة ولكن تنعقد مسؤوليته وفقا للقواعد العامة في المسؤولية المدنية. (المرجع السابق ص 76 في الهامش، وص 77).

المبحث الثاني
الوقاية القانونية

إلى جانب الوقاية التقنية لمنع الاعتداء على البريد الإلكتروني، توجد وسائل قانونية وقائية للحد أيضاً من مثل هذا الاعتداء. غير أننا نلاحظ أنه إذا كان الأمر محدداً فيما يتعلق بالوسائل التقنية، فإن الأمر ليس كذلك بالنسبة للوسائل القانونية. ويمكن الاجتهاد في هذا الصدد.

أولى الوسائل القانونية للوقاية من الاعتداء على البريد الإلكتروني هي حرمة وكفالة سرية المراسلات التي تتم عبر البريد الإلكتروني، حيث أضفى القانون بل والدستور الصفة الخصوصية عليها، ولا يجوز مراقبة هذه المراسلات إلا لضرورات قانونية أو أمنية، وأن يتم ذلك بقرار قضائي[1].

ثاني الوسائل القانونية الوقائية وقف الاعتداء أو الفعل غير المشروع، وهي وسيلة ذات طبيعة مدنية تقوم بها المسؤولية المدنية كإحدى وظائفها ربما غير المعروفة وغير المشهورة[2]. وتعطي القوانين، لمن وقع اعتداء على حق من حقوقه اللصيقة بشخصيته، وقف هذا الاعتداء مع التعويض عن الضرر الذي يصيبه من جراء هذا الاعتداء[3]. وهذا ما ينص عليه قانون المعاملات المدنية الإماراتي في المادة 90 من أن " لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر".

وثالث الوسائل القانونية الوقائية هي النص على جزاء جنائي على الاعتداء على البريد الإلكتروني، وهو الأمر الذي يحقق الردع لكل من تسول له نفسه الاعتداء على خصوصية

(1) انظر: د. عبد الهادي العوضي، الجوانب القانونية للبريد الإلكتروني، ص 124 وما بعدها، وص 137 وما بعدها.

(2) انظر في هذه الوسيلة:

C. BLOCH, La cessation de l'illicite, rechercher sur une fonction méconnue de la responsabilité civile extracontractuelle, Dalloz, Paris,2008.

(3) انظر: المادة 50 من القانون المدني المصري، والمادة 9/ 2 مدني فرنسي، والمادة 1/809 إجراءات مدنية فرنسي (جديد).

الآخرين والعبث برسائلهم الإلكترونية أو إتلافها أو الاستيلاء عليها. وهذا ما سنراه عند دراسة الجزاء الجنائي على الاعتداء على البريد الإلكتروني، على اعتبار أنه " نظام معلوماتي إلكتروني" أو " وسيلة تقنية معلومات".

ومن الوسائل القانونية أيضاً ما نقترحه من ضرورة إبرام عقد تأمين ضد الأضرار التي تلحق البريد الإلكتروني[1]، وهو وسيلة وقائية وعلاجية، وسيلة وقائية حيث تشترط شركات التأمين أماناً معيناً أو اتخاذ إجراءات محددة لمنع أو تقليل وقوع الأضرار، كما أن عبئها النهائي يقع على فاعل الضرر، وهي وسيلة علاجية أيضا حيث يحصل المضرور على تعويض الضرر الذي حدث لبريده الإلكتروني من شركة التأمين، ثم ترجع الشركة على فاعل الضرر.

الفصل الرابع
جزاء الاعتداء على البريد الإلكتروني

ونبدأ أولاً بنتناول الجزاء الجنائي على الاعتداء على البريد الإلكتروني (المبحث الأول)، ونعقبه بدراسة الجزاء المدني على هذا الاعتداء (الجزاء المدني).

المبحث الأول
الجزاء الجنائي

شهد الجزاء الجنائي – فيما يتعلق بالمواد الإلكترونية – تطوراً ملحوظاً. فقد بدأ بالاستهانة في بداية الظاهرة ولذلك لم يقرر سوى عقوبة الغرامة في الغالب. ولكن عندما استفحل خطر الاعتداءات الإلكترونية لفتت نظر المشرع فقرر لها عقوبات تتناسب مع خطورتها.

(1) حول تأمين مخاطر الإنترنت عموما، انظر: د. طاهر شوقي مؤمن، التأمين ضد مخاطر استخدام الإنترنت، المؤتمر الثاني والعشرون، الجوانب القانونية للتأمين واتجاهاته المعاصرة، كلية القانون –جامعة الإمارات العربية المتحدة، 13-14 مايو 2014، ص 81.

وهذا ما أخذ به المشرع الإماراتي في المرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

أولا- جريمة دخول البريد الإلكتروني بدون ترخيص أوتجاوز حدود الترخيص أو البقاء فيه بصورة غير مشروعة:

فقد نص المرسوم بقانون في المادة الثانية منه في فقرتها الأولى على عقوبة الحبس والغرامة على جريمة دخول البريد الإلكتروني بدون ترخيص أوتجاوز حدود الترخيص أو البقاء فيه بصورة غير مشروعة. وفي حين لم يحدد المرسوم مدة الحبس ولكن ترك أمر تحديدها للقاضي وفقا للقواعد العامة المنصوص عليها في المادة(69) من قانون العقوبات الاتحادي (من شهر إلى ثلاث سنوات)، فإنه قد حدد مقدار الغرامة كحد أدنى مائة ألف درهم وحد أقصى ثلاثمائة ألف درهم. وللقاضي أن يجمع بين الحبس والغرامة أو يكتفي بإحدى العقوبتين فقط.

وأضاف المشرع في الفقرتين الثانية والثالثة من المادة الثانية ظروفاً مشددة للعقوبة على النحو التالي:

تكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسون ألف درهم أو بإحدى هاتين العقوبتين إذا ترتب على أي فعل من الأفعال المنصوص عليها بالفقرة 1 من هذه المادة إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات.

تكون العقوبة الحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين إذا كانت البيانات أو المعلومات محل الأفعال الواردة في الفقرة 2 من هذه المادة شخصية.

ويلاحظ أن المشرع لم يتعرض لحالة دخول الجاني (البريد الإلكتروني) بقصد الإلغاء أو الحذف أو التدمير أو الإفشاء أو الإتلاف أو التغيير أو النسخ أو إعادة النشر بالنسبة للبيانات أو المعلومات. وكنا نأمل ـ مع البعض من الفقه ـ أن يتعرض القانون لهذه الحالة ويخضعها لعقوبة مغلظة [1].

(1) انظر: د. عبد الرازق الموافي عبد اللطيف، قراءة في قانون مكافحة جرائم تقنية المعلومات، مرجع سابق ذكره، ص 143.

ثانيا- جريمة الدخول بغير ترخيص إلى بريد إلكتروني بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية:

عاقب المرسوم بقانون رقم 5 لسنة 2012 في المادة الرابعة منه بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون وخمسمائة ألف درهم " كل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول، بقصد الحصول على بيانات حكومية،أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أواقتصادية".

وتكون العقوبة السجن مدة لا تقل عن خمس(5) سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز 2 مليون درهم، إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر.

ولم يتعرض المرسوم هنا لحالة دخول الجاني (البريد الإلكتروني) بقصد إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو نسخ أو نشر أو إعادة نشر البيانات أو المعلومات المذكورة في النص، وكان من الواجب عليه أن يتعرض لهذه الحالة بشكل مستقل ويخضعها لعقوبة شديدة[1]، ولا يكتفي فقط بجعلها نتيجة للدخول بغير ترخيص للبريد الإلكتروني.

ثالثا- جريمة حصول أو تعديل أو إتلاف أو إفشاء بغير تصريح بيانات أو معلومات يتضمنها البريد الإلكتروني وكانت هذه البيانات أو المعلومات تتعلق بفحوصات طبية أو تشخيص طبي أو علاج أو رعاية طبية أو سجلات طبية:

"يعاقب بالسجن المؤقت كل من حصل أو استحوذ أو عدل أو أتلف أو أفشى بغير تصريح بيانات أي مستند إلكتروني أو معلومات إلكترونية عن طريق الشبكة المعلوماتية أو موقع إلكتروني أو نظام المعلومات الإلكتروني أو وسيلة تقنية معلومات وكانت هذه البيانات أو المعلومات تتعلق بفحوصات طبية أو تشخيص طبي، أو علاج أو رعاية طبية أو سجلات طبية" (المادة السابعة من المرسوم).

(1) انظر: د. عبد الرازق الموافي عبد اللطيف، قراءة في قانون مكافحة جرائم تقنية المعلومات، مرجع سابق ذكره، ص 146.

رابعاً: جريمة تعطيل أو إعاقة الوصول إلى البريد الإلكتروني:

"يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من أعاق أوعطل الوصول إلى شبكة معلوماتية أوموقع إلكتروني أو نظام معلومات إلكتروني" (المادة الثامنة من المرسوم).

خامسا: جريمة إتلاف أو مسح أو تغيير أو تدمير أو تعطيل البريد الإلكتروني أو البيانات أو المعلومات الموجودة به عن طريق ادخال برنامج معلومات بدون ترخيص:

نص المرسوم بقانون رقم 5 لسنة 2012 في المادة 10 منه على أن: " يعاقب بالسجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز ثلاثة ملايين درهم أو بإحدى هاتين العقوبتين كل من أدخل عمداً وبدون تصريح برنامج معلوماتي إلى الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات، وأدى ذلك إلى إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرنامج أو النظام أو الموقع الإلكتروني أو البيانات أو المعلومات.

وتكون العقوبة السجن والغرامة التي لا تجاوز خمسمائة ألف درهم أو إحدى هاتين العقوبتين إذا لم تتحقق النتيجة. وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين عن أي فعل عمدي يقصد به إغراق البريد الإلكتروني بالرسائل وإيقافه عن العمل أو تعطيله أو إتلاف محتوياته".

سادساً: جريمة الحصول على رقم سري أو شفرة أو كلمة مرور أو أي وسيلة أخرى للدخول إلى البريد الإلكتروني بدون تصريح:

نص المرسوم بقانون رقم 5 لسنة 2012 في المادة 14 على أن : "يعاقب بالحبس والغرامة التي لا تقل عن مائتي ألف درهم ولا تزيد على خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من حصل، بدون تصريح، على رقم سري أو شفرة أو كلمة مرور أو أي وسيلة أخرى للدخول إلى وسيلة تقنية معلومات، أو موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو معلومات إلكترونية".

ويعاقب بذات العقوبة كل من أعد أو صمم أو أنتج أو باع أو اشترى أو استورد أو عرض للبيع أو أتاح أي برنامج معلوماتي أو أي وسيلة تقنية معلومات، أو روج بأي طريقة روابط

لمواقع إلكترونية أو برنامج معلوماتي، أو أي وسيلة تقنية معلومات مصممة لأغراض ارتكاب أو تسهيل أو التحريض على ارتكاب الجرائم المنصوص عليها في هذا المرسوم بقانون.

المبحث الثاني
الجزاء المدني

يمكن تصور الجزاء المدني للاعتداء على البريد الإلكتروني في صورتين: المسؤولية العقدية في حالة الإخلال بالتزام عقدي من جانب الشركة مقدمة الخدمة (أولاً) والمسؤولية التقصيرية في حالة الإخلال بواجب أو التزام قانوني من جانب شخص لا تربطه بالمستفيد من البريد الإلكتروني رابطة عقدية (ثانياً).

أولا- مسؤولية الشركة مقدمة خدمة البريد الإلكتروني وتابعيها:

رأينا فيما سبق أن الحصول على البريد الإلكتروني يتم بمقتضى " عقد إنشاء البريد الإلكتروني" أو " عقد تقديم خدمة البريد الإلكتروني" المبرم بين المستفيد من خدمة البريد الإلكتروني والشركة مقدمة خدمة البريد الإلكتروني.

ويرتب هذا العقد التزامات متبادلة على عاتق طرفيه. تلتزم الشركة مقدمة خدمة البريد الإلكتروني بالتزامات منها : الالتزام بأن تضع إمكانياتها الفنية أمام المستفيد من الخدمة ليتمكن من إرسال وتلقي الرسائل البريدية عبر البريد الإلكتروني، والالتزام بالحفاظ على سرية المراسلات وخصوصية محتويات الرسائل الإلكترونية.

وفي حالة إخلال الشركة بهذه الالتزامات، تنعقد مسؤوليتها العقدية تجاه المستفيد عن الأضرار التي تلحق به نتيجة هذا الإخلال.

غير أن هذه المسؤولية العقدية يمكن التقليص منها عن طريق اتفاقات الإعفاء من المسؤولية. ففي الغالب ينص في العقد على عدم مسؤولية الشركة مقدمة خدمة البريد الإلكتروني عن الأضرار التي قد تلحق بمستخدم البريد نتيجة محتوى الرسائل الواردة فيه[1].

(1) في حدود صحة اتفاقات المسؤولية، انظر: د.محمود جمال الدين زكي، مشكلات المسؤولية المدنية، الجزء 2، مطبعة جامعة القاهرة، 1990.

ثانياً- مسؤولية الغير عن الاعتداء على البريد الإلكتروني:

يسأل الغير المعتدي على البريد الإلكتروني مسؤولية تقصيرية في القانون الإماراتي، وهي ذات الضمان الذي قرره الفقه الإسلامي في حالة الاعتداء على أموال الناس وممتلكاتهم.

فقد قرر الفقه الإسلامي المبدأ العام في عدم الإضرار بالغير استناداً إلى حديث الرسول صلى الله عليه وسلم الذي قال فيه : " لا ضرر ولا ضرار"، في صورة قاعدة فقهية. كما قرر الفقه الإسلامي أيضا قاعدة فقهية أخرى تقول بأن : " الضرر يزال".

وتطبيقاً لهاتين القاعدتين، لا يجوز لأحد أن يضر غيره في ماله أو في حق من حقوقه، واذا حدث هذا الإضرار يلتزم فاعل الضرر بإزالته عيناً أو نقداً.

وفي ضمان الضرر، يفرق الفقه الإسلامي بين الإضرار الذي يحدث مباشرة والإضرار الذي يحدث بالتسبب، ويقصد بالأول أن الفعل الضار (الإضرار) قد أدى إلى وقوع الضرر مباشرة ودون واسطة بين الأمرين، أما الثاني فيقصد به الفعل الضار (الإضرار) الذي يؤدي إلى وقوع الضرر ولكن عن طريق واسطة بين الفعل والضرر.

ويلتزم فاعل الضرر بضمانه دون شرط لا تعدي ولا غيره إذا كان حدث مباشرة، ويلتزم بضمانه ولكن بشرط التعدي أو التعمد أو أن يكون الفعل الضار مفضياً إلى الضرر أي توجد علاقة سببية بين الفعل والضرر الذي وقع.

وقد تبنى قانون المعاملات المدنية الإماراتي هذه الأحكام في نصوصه، حيث نص على القواعد الفقهية في المادة 42 منه التي تقرر بأن " 1ـ لا ضرر ولا ضرار، 2 ـ الضرر يزال، 3 ـ الضرر لا يزال بمثله" [1]، كما نص على أن " كل إضرار بالغير يلزم فاعله ولو غير مميز بضمان الضرر" (المادة 282)، كما كرس التفرقة بين الإضرار بالمباشرة والإضرار بالتسبب، حيث نص في المادة 283 على أن: " 1 ـ يكون الإضرار بالمباشرة أو التسبب، 2 ـ فإن كان بالمباشرة

(1) انظر: القواعد الفقهية في قانون المعاملات المدنية: د. جاسم علي سالم الشامسي، " شرح القواعد الفقهية التي نص عليها قانون المعاملات المدنية وتطبيقاتها القضائية والفقهية" (ص 26):
Colloque : Les dénominateurs communs entre les principes généraux du droit musulman et des droits des pays Beyrouth, octobre 2001 - arabes et les principes généraux du droit français

لزم الضمان ولا شرط له وإذا وقع بالتسبب فيشترط التعدي أو التعمد أو أن يكون الفعل مفضياً إلى الضرر"[1].

وليس الاعتداء على البريد الإلكتروني سوى مجرد تطبيق عادي للضمان في الفقه الإسلامي وفي قانون المعاملات المدنية الإماراتي.

وبناء على ذلك، يسأل المعتدى على البريد الإلكتروني، بأي شكل من الأشكال، عن الأضرار التي تحدث للمستفيد من خدمة البريد الإلكتروني.

ولا يمكن التنصل من هذه المسؤولية أو التقليل منها عن طريق الاتفاق على الإعفاء منها، حيث أن المسؤولية عن الفعل الضار تتعلق بالنظام العام، ومن ثم لا يجوز الاتفاق على الإعفاء أو التخفيف منها[2]. وبناء على ذلك، لا قيمة للعبارات التي توضع أسفل الصفحة أو أسفل الرسالة تقرر عدم مسؤولية مرسل الرسالة عن الأضرار التي تحدث للمستفيد من البريد الإلكتروني نتيجة محتوى الرسالة[3].

وقد نظم المشرع الإماراتي مجموعة من التطبيقات القانونية لفعل الإضرار[4]، يمكن أن تنطبق على الاعتداءات الواقعة على البريد الإلكتروني، مثل التغرير بالغير، وإتلاف مال الغير، والغصب والتعدي على مال الغير.

(1) انظر حول فكرتي المباشرة والتسبب وتطبيقاتهما في القانون المدني بالمقارنة بأصلهما في الفقه الإسلامي: د. محمد يوسف الزغبي، مسؤولية المباشر والمتسبب في القانون المدني، مؤتة للبحوث والدراسات(26 الأردن، مجلد 2، عدد 1، 1987، ص161-212؛ د. عماد أحمد أبو صد، مسؤولية المباشر والمتسبب، دراسة مقارنة بين الشريعة الإسلامية والقانون المدني، دار الثقافة للنشروالتوزيع، عمان-الأردن، 1432هـ- 2011 م.

(2) في هذا انظر: د.محمود جمال الدين زكي، مشكلات المسؤولية المدنية، الجزء 2، مطبعة جامعة القاهرة، 1990.

(3) في هذا المعنى: المحامي عدنان غسان برانبو، دراسة عن بعض الجوانب القانونية والتقنية لاستخدام البريد الإلكتروني في المؤسسات، المرجع السابق، ص 33.

(4) انظر في التطبيقات القانونية للإضرار في قانون المعاملات المدنية الإماراتي: د. بشار طلال المومني، د. إياد محمد إبراهيم جاد الحق، د. قيس عبد الستار، شرح مصادر الالتزام غير الإرادية في قانون المعاملات المدنية الإماراتي، الطبعة الأولى، مكتبة الجامعة بالشارقة، 2015، ص 59 وما بعدها. وفي القانون المدني الأردني والقانون المدني المصري، انظر: د. عماد أحمد أبو صد، مسؤولية المباشر والمتسبب، المرجع السابق، ص 226 وما بعدها.

التغرير بالغير: وقد نصت على التغرير بالغير المادة 285 من قانون المعاملات المدنية بقولها: " إذا غرر أحد بآخر ضمن القدر المترتب على ذلك الغرر". وفي بيان ذلك قضت محكمة النقض بأن" النص في المواد 185، 186، 187، 191 من قانون المعاملات المدنية على أن الغرر هو أن يخدع أحد المتعاقدين المتعاقد الآخر بوسائل احتيالية قولية أو فعلية تحمله على الرضا بما لم يكن ليرضى به بغيرها، ويعتبر السكوت عمداً عن واقعة أو ملابسة تغريراً إذا ثبت أن من غرر به ما كان ليبرم العقد لو علم بتلك الواقعة أو هذه الملابسة، يدل على أن الغش المفسد للرضاء، يجب أن يكون وليد إجراءات احتيالية أو وسائل من شأنها التغرير بالمتعاقد بحيث تشوب إرادته ولا تجعله قادراً على الحكم على الأمور حكماً سليما"[1].

إتلاف مال الغير: وفقا للمادة 300 من قانون المعاملات المدنية، " من أتلف مال غيره أو أفسده ضمن مثله إن كان مثليا وقيمته إن كان قيميا، وذلك مع مراعاة الأحكام العامة للتضمين"[2]. ويشترط لضمان المال المتلف أن يكون هذا المال مملوكا للغير أو مملوكا للمتلف وتعلق به حق للغير مثل إتلاف المال المرهون أو إنقاص قيمته [3][4]. ويضمن المتلف من ما أتلفه سواء كان مميزاً أو غير مميز (م. 303 ق. م. أ.). وعلى ذلك لو أتلف صبي البريد الإلكتروني (أو محتوياته) لغيره، فإنه يلزمه الضمان من ماله هو سواء كان مميزاً أو غير مميز، تطبيقا للنص المتقدم.

الغصب والتعدي على مال الغير: عالج المشرع الإماراتي الغصب والتعدي على مال الغير في المواد من 304 إلى 312 من قانون المعاملات المدنية[5].

(1) نقض تجاري، 17 ديسمبر 2013، الطعن رقم 673 لسنة 2013، مجلة الفقه والقضاء والقانون، دائرة القضاء، السنة الثانية، العدد الثالث، مارس 2014، ص 324، مشار إليه في المرجع السابق، ص 60، هامش رقم 1.

(2) انظر : د. وهبة الزحيلي، نظرية الضمان أو أحكام المسؤولية المدنية والجنائية في الفقه الإسلامي، دراسة مقارنة، دار الفكر، دمشق-سوريا، 1998، وبصفة خاصة ص 22 وما بعدها.

(3) انظر : المذكرة الإيضاحية لقانون المعاملات المدنية الصادر بالقانون الاتحادي رقم(5) لسنة 1985 المعدل، وزارة العدل، 1987، ص 301، حبث تشير إلى قول الحنابلة بإيجاب الضمان على من أتلف الأضحية، ولو كان صاحبها، لما في إتلافها من الإضرار بحق الفقراء.

(4) تنص المادة 302 من قانون المعاملات المدنية على أن " 1- إذا أتلف أحد مالاً لغيره على زعم أنه ماله ضمن ما أتلف. 2- وإذا أتلف مال غيره بإذن مالكه فلا يضمن".

(5) انظر في دراسة الغصب والتعدي على مال الغير، على سبيل المثال: د. الشهابي إبراهيم الشرقاوي، مصادر الالتزام غير الإرادية في قانون المعاملات المدنية الإماراتي، الطبعة الثانية، الآفاق المشرقة، 1434 هـ - 2013 م، ص 70 وما بعدها.

وتطبيقاً لأحكام هذه المواد، من غصب مال غيره وجب عليه رده بحالته التي كان عليها عند الغصب وفي مكان غصبه. فإن استهلكه أو أتلفه أو ضاع منه بتعديه أو بدون تعديه فعليه مثله أو قيمته يوم الغصب وفي مكان الغصب. ويضمن أيضا منافعه وزوائده.

وإذا أتلف أحد المال المغصوب في يد الغاصب، فالمغصوب منه بالخيار إن شاء ضمن الغاصب ولهذا أن يرجع على المتلف، وإن شاء ضمن المتلف وليس للمتلف الرجوع على الغاصب.

وإذا تصرف الغاصب في المال المغصوب معاوضة أو تبرعاً، وتلف المغصوب كله أو بعضه في يد من تصرف له الغاصب، كان للمغصوب منه الخيار في تضمين من شاء منهما، فإن ضمن الغاصب صح تصرفه وإن ضمن من تصرف له الغاصب كان له الرجوع على الغاصب وفقا لأحكام القانون.

وغاصب الغاصب حكمه حكم الغاصب. وإذا تغير المغصوب بنفسه يخير المغصوب منه بين استرداد المغصوب او البدل على حسب الاحوال. الى اخر الاحكام التي اوردها المشرع للغصب والتعدي على مال الغير.

وقد أورد المشرع الإماراتي حكماً في غاية الأهمية وهو ما نصت عليه المادة 312 معاملات مدنية من أن " حكم كل ما هو مساو للغصب كحكم الغصب"، كما أن المادة 308 معاملات مدنية أعطت للقاضي في جميع الأحوال الحكم على الغاصب بالتعويض الذي يراه مناسباً إن رأى مبرراً لذلك.

ولاشك لدينا في إنطباق أحكام الغصب والتعدي على مال الغير على البريد الإلكتروني، إذا توافرت شروطه.

الخاتمة

في هذا البحث الذي انصب على بيان جوانب الحماية القانونية من الاعتداء على البريد الإلكتروني، وفقاً للفقه الإسلامي والمرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، تناولنا في فصل تمهيدي التعريف بالبريد الإلكتروني ونشأته وأهميته وأنواعه وتطوره، وفي الفصل الأول درسنا ملكية البريد الإلكتروني، ورأينا أن تحديد الملكية أو السلطات التي يملكها مستخدم البريد الإلكتروني هي مناط حماية البريد الإلكتروني، فالقانون يحمي الحقوق والممتلكات، وقد تناولنا بعد ذلك، تحديد ملكية البريد الإلكتروني أو العلاقات القانونية الناشئة عن الاستفادة ببريد الكتروني، ورأينا أن الشخص يكتسب البريد الإلكتروني عن طريق إبرام عقد مع الشركة منشئة البريد الإلكتروني، وهو عقد غير مسمى في القانون، يطلق عليه في العمل " عقد إنشاء البريد الإلكتروني" أو " عقد تقديم خدمة البريد الإلكتروني"، يخضع للأحكام الواردة فيه، فإن لم توجد يخضع لأحكام أقرب عقد مسمى له. هذا وقد رأينا أن الشخص المستفيد من خدمة البريد الإلكتروني، يملك محتويات البريد الإلكتروني، ويتمتع بكافة سلطات الملكية عليها، وتكون عنصراً من ذمته المالية، ومن ثم تنتقل إلى الورثة بعد وفاة المستفيد.

وبعد بيان المركز القانوني لمستخدم البريد الإلكتروني وبيان علاقته به والسلطات التي يتمتع بها عليه، تناولنا في الفصل الثاني صور الاعتداء على البريد الإلكتروني في الفقه الإسلامي، وفي قانون مكافحة جرائم تقنية المعلومات، ووجدنا تقارباً في صور الحماية من الاعتداء على البريد الإلكتروني في النظامين. وفي الحقيقة لم نصل إلى بيان حصري للاعتداءات الواقعة على البريد الإلكتروني وفقاً للفقه الإسلامي وقانون مكافحة جرائم تقنية المعلومات، ولكنّا اجتهدنا في تطبيق أحكام الفقه الإسلامي وقانون مكافحة جرائم تقنية المعلومات على ما أمكن تصوره منها.

وفي الفصل الثالث، تعرضنا للوقاية من الاعتداء على البريد الإلكتروني، وذلك عن طريق وسائل تقنية مثل التشفير والتصديق للرسائل الإلكترونية بل والمعاملات الإلكترونية بصفة عامة، ووسائل قانونية مثل حرمة الرسائل البريدية الإلكترونية وسريتها، ووقف الاعتداء غير المشروع الواقع على الحقوق اللصيقة بالشخصية بالوسائل القانونية، والردع العام الناتج عن إقرار عقوبات رادعة على الاعتداء على البريد الإلكتروني، وإبرام عقد تأمين،. ..الخ.

وأخيرا، درسنا في الفصل الرابع الجزاء الذي يوقع على الاعتداء على البريد الإلكتروني، سواء من الناحية المدنية أو من الناحية الجنائية، ورأينا تقارب بل ربما وحدة الجزاءات القانونية والشرعية، وذلك لأن القانون الإماراتي يستمد أحكامه من الفقه الإسلامي، كما في القواعد المدنية في قانون المعاملات المدنية، أو ينص على عدم الإخلال بالأحكام المقررة في الشريعة الإسلامية، ويحرص على عدم مخالفة هذه الأحكام، كما في قانون مكافحة جرائم تقنية المعلومات، أو في قانون العقوبات بصفة عامة.

ومن أجل إحكام الحماية من الاعتداء الواقع على البريد الإلكتروني، نوصي المشرع بالآتي:

1. النص صراحةً على البريد الإلكتروني كنظام معلومات إلكتروني أو وسيلة تقنية معلومات في قانون مكافحة جرائم تقنية المعلومات في المادة الأولى الخاصة في التعريفات.

2. النص على الجرائم التي تقع على البريد الإلكتروني، كما فعل المشرع في المادة 10 من المرسوم بقانون رقم 5 لسنة 2012، مع ضرورة عدم الإخلال بالبناء الفني والصياغة للنصوص.

3. أن يتعرض المشرع في المادة الثانية من المرسوم بقانون رقم 5 لسنة 2012 لحالة دخول الجاني (البريد الإلكتروني) بقصد الإلغاء أو الحذف أو التدمير أو الإفشاء أو الإتلاف أو التغيير أو النسخ أو إعادة النشر بالنسبة للبيانات أو المعلومات ويخضعها لعقوبة مغلظة.

4. أن يتعرض المرسوم في المادة الرابعة منه لحالة دخول الجاني (البريد الإلكتروني) بقصد إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو نسخ أو نشر أو إعادة نشر البيانات أو المعلومات المذكورة في النص، بشكل مستقل ويخضعها لعقوبة شديدة، ولا يكتفي فقط بجعلها نتيجة للدخول بغير ترخيص للبريد الإلكتروني.

5. النص على قرينة افتراض صحة البريد الإلكتروني، متى استوفى ضوابط فنية وتقنية معينة.

6. النص على إبرام عقد تأمين على المعاملات الإلكترونية وأن يكون هذا التأمين إجبارياً.

7. ضرورة استقاء أحكام الحماية من الاعتداء على البريد الإلكتروني من الفقه الإسلامي الذي يتعرض تقريبا لكل الصور التي يمكن أن يتخذها هذا الاعتداء.

8. تقوية ضمانات مستخدمي البريد الإلكتروني من الناحية التقنية، عن طريق أدوات التشفير والتصديق والتوقيع الإلكتروني والجدار الناري وغيرها.

9. إزالة كل ما يوجد في التشريعات القائمة (قوانين ولوائح) ولا يتوائم مع المعاملات الإلكترونية أو ينكر البريد الإلكتروني. وبذلك يواكب المشرع الإماراتي التطورات الموجودة في الأنظمة القانونية المقارنة.

هذا والله المستعان، وهو الهادي إلى سواء السبيل،،،،،

قائمة المراجع

أولا- المراجع باللغة العربية:

1- الكتب والأبحاث والمقالات:

د. إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية، مجلس النشر العلمي، جامعة الكويت، 2003.

د. أحمد عبد المجيد الحاج، المسؤولية الجنائية لجرائم النشر الإلكتروني في ضوء قانون مكافحة جرائم تقنية المعلومات الإماراتي، دورية الفكر الشرطي، العدد 85، ابريل 2013، ص 167.

د. إسماعيل عبد النبي شاهين، أمن المعلومات في الإنترنت بين الشريعة والقانون، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة، 1-3 مايو 2000، ص971- 992.

د. الشحات إبراهيم محمد منصور، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، بحث فقهي مقارن، دار الفكر الجامعي، الإسكندرية، 2011.

د. الشهابي إبراهيم الشرقاوي، مصادر الالتزام غير الإرادية في قانون المعاملات المدنية الإماراتي، الطبعة الثانية، الآفاق المشرقة ناشرون، 1434 هـ- 2013 م.

المذكرة الايضاحية لقانون المعاملات المدنية الصادر بالقانون الاتحادي رقم(5) لسنة 1985 المعدل، وزارة العدل، 1987.

إيمان محمد طاهر، الحماية المدنية لمستخدمي البريد الإلكتروني، مجلة الرافدين للحقوق، كلية الحقوق، جامعة الموصل، العراق، العدد 54، 2012، ص 190-134.

د. أيمن عبد الله فكري، الجرائم المعلوماتية، دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، الطبعة الأولى، الرياض، 1436هـ -2015 م.

د. بشار طلال المومني، د. إياد محمد إبراهيم جاد الحق، د. قيس عبد الستار، شرح مصادر الالتزام غير الإرادية في قانون المعاملات المدنية الإماراتي، الطبعة الأولى، مكتبة الجامعة بالشارقة، 2015.

د. وهبة الزحيلي، نظرية الضمان أو أحكام المسؤولية المدنية والجنائية في الفقه الإسلامي، دراسة مقارنة، دار الفكر، دمشق- سوريا، 1998.

بي بي سي العربية: وفاة مخترع البريد الإلكتروني راي توملينسون، في 7 مارس 2016.

email__inventor__dies__160306/03/http://www.bbc.com/arabic/business/2016

د. جاسم علي سالم الشامسي، " شرح القواعد الفقهية التي نص عليها قانون المعاملات المدنية وتطبيقاتها القضائية والفقهية" (صفحة 26).

Colloque : Les dénominateurs communs entre les principes généraux du droit musulman et des droits des pays arabes et les principes généraux du droit français – Beyrouth، octobre 2001.

د. جمال عبد الرحمن محمد علي، الحجية القانونية للمستندات الإلكترونية، 2004، بدون ناشر.

د. حسن عماد مكاوي، تكنولوجيا الاتصال الحديثة في عصر المعلومات، الدار المصرية اللبنانية، القاهرة، الطبعة الخامسة، شوال 1430 هـ - أكتوبر 2009م.

د. خالد مصطفى فهمي، النظام القانوني للتوقيع الإلكتروني في ضوء التشريعات العربية والاتفاقيات الدولية، دار الجامعة الجديدة للنشر، الإسكندرية، 2007.

د. رشدي محمد علي محمد عيد، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، 2013.

د. سعيد السيد قنديل، التوقيع الإلكتروني، ماهيته- صوره- حجيته في الإثبات، بين التدويل والاقتباس، دار الجامعة الجديدة للنشر، الإسكندرية، 2004.

د. طاهر شوقي مؤمن، التأمين ضد مخاطر استخدام الإنترنت، المؤتمر الثاني والعشرون، الجوانب القانونية للتأمين واتجاهاته المعاصرة، كلية القانون -جامعة الإمارات العربية المتحدة، 13-14 مايو 2014، ص 81.

د. عبد الحميد عثمان الحفني، المسؤولية المدنية للموثق، دراسة مقارنة بين القانون المصري والفرنسي، مجلة البحوث القانونية والاقتصادية، كلية الحقوق- جامعة المنصورة، العدد الثاني عشر، أكتوبر 1992، ص 2.

م. د. عبد الحميد النجاشي الزهيري، الوجيز في شرح قانون الإثبات الإماراتي، الآفاق المشرقة، 2014.

د. عبد الرازق الموافي عبد اللطيف، قراءة في قانون مكافحة جرائم تقنية المعلومات الإماراتي الجديد " المرسوم بقانون إتحادي رقم 5 لسنة 2012، مجلة معهد دبي القضائي، السنة الأولى، العدد 2، ربيع الثاني 1434هـ- مارس 2013 م، ص 139.

.....، تعليق على قضاء دبي بشأن الاختصاص القضائي بجرائم الإنترنت، مجلة معهد دبي القضائي، العدد1، السنة الأولى، جمادى الاخرة 1433 هـ- مايو 2012 م، ص 107 وما بعدها.

.....، شرح قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة، "المرسوم بالقانون الاتحادي رقم 5 لسنة 2012"، الكتاب الأول، معهد دبي القضائي، سلسلة الدراسات والبحوث القانونية والقضائية العلمية المحكمة، العدد 13، 1435 هـ-2014 م والكتاب الثاني، معهد دبي القضائي، سلسلة الدراسات والبحوث القانونية والقضائية العلمية المحكمة، العدد 15، 1437هـ- 2016 م.

د. عبد الرزاق أحمد السنهوري، الوسيط في شرح القانون المدني، الجزء التاسع، أسباب كسب الملكية، مع الحقوق العينية الأصلية المتفرعة عن الملكية، تنقيح المستشار/ أحمد مدحت المراغي، الناشر : منشأة المعارف بالإسكندرية، 2004.

د.عبد الهادي العوضي، الجوانب القانونية للبريد الإلكتروني، دار النهضة العربية، القاهرة، 2007.

المحامي / عدنان غسان برابو، دراسة عن بعض الجوانب القانونية والتقنية لاستخدام البريد الإلكتروني في المؤسسات، بحث مقدم في مادة تقنيات وأدوات الإدارة واستخداماتها، المعهد العالي للتنمية الإدارية- قسم ماجستير العلوم الإدارية، جامعة دمشق، العام الدراسي 2004-2005.

عبد الله بن ناصر بن أحمد العمري، الحماية الجنائية للبريد الإلكتروني، دراسة تأصيلية مقارنة، رسالة لاستكمال متطلبات الحصول على درجة الماجستير، قسم العدالة الاجتماعية- تخصص السياسة الجنائية، جامعة نايف للعلوم الأمنية، الرياض، 1431 هـ - 2010 م.

عقيد د. عبيد صالح حسن، سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، دورية الفكر الشرطي، العدد 95، أكتوبر 2015، ص 21.

عبير علي محمد النجار، جرائم الحاسب الآلي في الفقه الإسلامي، رسالة ماجستير، الجامعة الإسلامية، غزة، 1430 هـ- 2009 م.

د. علاء محيي الدين مصطفى أبو أحمد، القرار الإداري الإلكتروني، دون ناشر أو سنة نشر أو مكان نشر.

د. علي سعيد عثمان محمد، البريد الإلكتروني واستخدامه في الدعوة إلى الله، مجلة الدعوة الإسلامية، كلية الدعوة الإسلامية، جامعة أم درمان الإسلامية، السودان، العدد 5، ديسمبر 2012، ص 162.

د. عماد أحمد أبو صد، مسؤولية المباشر والمتسبب، دراسة مقارنة بين الشريعة الإسلامية والقانون المدني، دار الثقافة للنشر والتوزيع، عمان-الأردن، 1432هـ- 2011 م.

م. د. فتحي محمد أنور عزت، جرائم العصر الحديث، الطبعة الأولى، دار الفكر والقانون، المنصورة، 2010.

د. محمد حماد مرهج الهيتي، الجريمة المعلوماتية، دار الكتب القانونية، مصر - الإمارات، 2014.

محمد لافي، حفظ المال في المفهوم الإسلامي، مقال متاح على شبكة الإنترنت في 1436/8/20 هـ: http://www.almoslim.net/node/234913

د. محمد محمد محمد أبو زيد، النصوص القانونية ذات الصلة بانعكاسات التقدم العلمي التي أدخلت على نصوص القوانين الرئيسة، مجلة معهد دبي القضائي، العدد الأول، مايو 2002، ص 139.

د. محمد محيى سليم، ذاتية مسؤولية الموثق، دون تاريخ نشر ودون ناشر ودون سنة نشر.

د. محمد يوسف الزغبي، مسؤولية المباشر والمتسبب في القانون المدني، مؤتة للبحوث والدراسات - الأردن، مجلد 2، عدد 1، 1987، ص161-212.

د.محمود جمال الدين زكي، مشكلات المسؤولية المدنية، الجزء 2، مطبعة جامعة القاهرة، 1990.

د. محمود خيال، التأمين على المعلومات،1999، بدون ناشر، ص 23 وما بعدها.

د. محمود نجيب حسني، النظرية العامة للقصد الجنائي، دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، الطبعة الثالثة، دار النهضة العربية، القاهرة، 1988.

د. مدحت محمد محمود عبد العال، برامج المعلومات، طبيعتها القانونية والعقود الواردة عليها، دراسة مقارنة للقوانين المصرية والإماراتية والفرنسية، معهد دبي القضائي، سلسلة الدراسات القانونية والقضائية، العدد 11، الطبعة الأولى، 1434 هـ- 2013م

د. مصطفى أبو مندور موسى، الجوانب القانونية لخدمات التوثيق الإلكتروني، دراسة مقارنة، دار النهضة العربية، القاهرة، دون سنة نشر.

د. وهبة الزحيلي، نظرية الضمان أوأحكام المسؤولية المدنية والجنائية في الفقه الإسلامي، دراسة مقارنة، دار الفكر، دمشق- سوريا،1998.

ويكيبيديا، الموسوعة الحرة: راي __ توملينسون
https://ar.wikipedia.org/wiki/

ويكيبيديا، الموسوعة الحرة : بريد الكتروني https://ar.wikipedia.org/wiki

2- القوانين واللوائح والقرارات والأحكام القضائية:

القانون الاتحادي رقم 10 لسنة 1992 وتعديلاته بشأن الإثبات في المعاملات المدنية والتجارية.

القانون الاتحادي رقم 36 لسنة 2006 بتعديل بعض أحكام قانون الإثبات في المعاملات المدنية والتجارية.

القانون الاتحادي رقم 11 لسنة 1992 وتعديلاته بشأن الإجراءات المدنية والتجارية والإدارية.

القانون الاتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات.

القانون الاتحادي رقم 10 لسنة 2014 بتعديل بعض أحكام قانون الإجراءات المدنية والتجارية والإدارية.

القانون الإتحادي رقم 18 لسنة 2018 بتعديل بعض أحكام قانون الإجراءات المدنية رقم 11 لسنة 1992.

القانون الاتحادي رقم 4 لسنة 2013 بشأن تنظيم مهنة الكاتب العدل

قرار مجلس الوزراء رقم 39 لسنة 2014 في شأن اللائحة التنفيذية لقانون تنظيم مهنة الكاتب العدل

قانون إمارة دبي رقم 2 لسنة 2002 بشأن المعاملات والتجارة الإلكترونية.

لائحة غرفة فض المنازعات في اتحاد الإمارات العربية المتحدة لكرة القدم.

نقض، جلسة 11 مارس 2013 (تجاري)، الطعن رقم 317 لسنة 2012 س 7 ق. أ، مجموعة الأحكام والمبادئ القانونية الصادرة عن محكمة النقض من دوائر المواد المدنية والتجارية

والادارية، السنة القضائية السابعة 2013م، من أول مارس حتى آخر أبريل، المكتب الفني، محكمة النقض، دائرة القضاء، الجزء الثاني، ص 549

نقض، جلسة 22 أبريل 2013 (تجاري)، الطعن رقم 658 لسنة 2012، س7 ق.أ، مجموعة الأحكام والمبادئ القانونية الصادرة عن محكمة النقض من دوائر المواد المدنية والتجارية والإدارية، السنة القضائية السابعة 2013م، من أول مارس حتى آخر ابريل، المكتب الفني، محكمة النقض، دائرة القضاء، الجزء الثاني، ص 855

نقض،جلسة 1 مايو 2013 (تجاري)، الطعن رقم 114 لسنة 2013 س7 ق.أ، مجموعة الأحكام والمبادئ القانونية الصادرة عن محكمة النقض من دوائر المواد المدنية والتجارية والإدارية، السنة القضائية السابعة 2013م، من أول مايو حتى آخر يونيو، المكتب الفني، محكمة النقض، دائرة القضاء، الجزء الثالث، ص972.

حكم محكمة تمييز دبي، جلسة 31-8-2008، الطعن رقم 249/2008 جزاء، الموقع الإلكتروني لمحاكم دبي.

حكم محكمة تمييز دبي، جلسة 7 فبراير 2016 (تجاري)، الطعن رقم709/2015: الموقع الإلكتروني لمحاكم دبي.

ثانيا: المراجع باللغة الفرنسية:

1- الكتب والأبحاث والمقالات:

BARBARY (E.), " Des décrets tant attendus: quel droit pour la cryptologie?" JCP, 1998, I, 124.

BEAUSSONIE (G.), « La protection pénale de la propriété sur l'information », Droit pénal, 2008, n°9.

BENSOUSSAN (A.), " Centre certificateur, authentification, preuve et contrôle", PA, 29 mai 1996, p.28.

BLOCH (C.), La cessation de l'illicite, rechercher sur une fonction méconnue de la responsabilité civile extracontractuelle, Dalloz, Paris, 2008.

CAPRIOLI (E.), " Le nouveau régime juridique de la cryptologie", Droit & Patrimoine, n° 67, janvier 1999, p.34.

..... " Sécurité et confiance dans le commerce électronique, signature numérique et autorité de certification", JCP, 1998, I, 123.

CATALA (P.), « La propriété de l'information », Mélanges P. RAYNAUD, Dalloz- Sirey, 1985, p.113.

COMBE (M.), La protection pénale de l'information, thèse, Nice, 2012.

FORTIN (F.), " Cryptologie : le tournant libéral du gouvernement", Droit & Patrimoine, n° 69, mars 1999, p.20.

GALLOUX (J.- Ch.), « Ébauche d'une définition juridique de l'information », D., 1994, chr.229.

GOBERT (D.), " Commerce électronique : vers un cadre juridique général pour le tiers de confiance", Revue du droit des technologies de l'information", n°18, avril 2004, p.33.

POIDEVIN (B.)," De cadre juridique de la certification", juriscom.net, le 1er septembre 2002.

RENARD (I.), Vive la signature électronique, Dalloz, Coll. DELMAS expresse, 2002.

2- الأحكام القضائية:

Cass. crim., 3 avril 1995, Bull. crim., n°142, p.397

Cass. crim., 2 mai 1983, Bull. crim., n°122, p.285.

Cass.crim., 20 mai 2015, Bull. crim.,, n° 119.

ثالثا: المراجع باللغة الأنجليزية:

https://en.wikipedia.org/wiki/Hillary_Clinton_email_controversy

Kiely (E.), “A Guide to Clinton’s Emails”, http://www.factcheck.org/2016/07/a-guide-to-clintons-emails/, Posted on July 5, 2016.

تم بحمد الله وتوفيقه

كاميرات المراقبة التلفزيونية المغلقة CCTV كوسيلة للمراقبة السابقة على ارتكاب الجريمة لأغراض منع الجريمة وملاحقة مرتكبيها

الأستاذ الدكتور
خالد موسى توني

كاميرات المراقبة التلفزيونية المغلقة CCTV كوسيلة للمراقبة السابقة على ارتكاب الجريمة لأغراض منع الجريمة وملاحقة مرتكبيها

الأستاذ الدكتور
خالد موسى توني
أستاذ ورئيس قسم القانون الجنائي
أكاديمية شرطة دبي

مقدمة

تسعى التشريعات الوطنية والمقارنة في مختلف دول العالم نحو تحقيق قدر كبير من التوازن بين اعتبارات مكافحة الجريمة وصون الحقوق والحريات الفردية، فوظيفة القانون الرئيسة هي تنظيم المجتمع؛ بغية الحفاظ على حريات ومصالح الأفراد الخاصة، مع حفظ كيان المجتمع وتحقيق الاستقرار والحفاظ على النظام العام[1].

ويأتي هذا الدور تلبية للتكليف الدستوري بصون الحقوق والحريات وكفالة احترامها من قبل جميع سلطات الدولة والأفراد على حد سواء، إلا أن هذا الالتزام الدستوري لم يعد من الميسور على الدول المختلفة الوفاء المطلق به، إذ ترتب على تزايد أخطار الظاهرة الإجرامية بشكل عام والإجرام المنظم والإرهاب بشكل خاص أن أضحت النظم والقواعد الإجرائية التقليدية غير قادرة أو فاعلة في مواجهة هذه الظواهر الإجرامية ذات الخطورة المتنامية واللامحدودة، ولعل هذا الأمر، هو ما دفع المشرعين في النظم الإجرائية المقارنة في العديد من دول العالم إلى التقييد من نطاق بعض الحريات والحقوق الدستورية الفردية، وذلك بقيود غير تقليدية.

(1) د. فتوح الشاذلي: المساواة في الإجراءات الجنائية، دار المطبوعات الجامعية، 1990م، ص3.
د. أحمد شوقي أبو خطوة، المساواة في القانون الجنائي، دار النهضة العربية، 1991م، ص 34.

حيث، أدخلت دول عدة على نظمها القانونية العديد من النصوص الإجرائية المستحدثة التي خولت جهات إنفاذ القانون عامة، وجهات الضبط الإداري خاصة، العديد من الصلاحيات التي تسمح لها بالقيام بانتهاك بعض الحقوق الخاصة للأفراد، لاسيما حقهم في خصوصية المكالمات الهاتفية، والحق في الصورة، ليس فقط تحقيقاً لأغراض التحقيق في الجرائم والوصول للأدلة التي تسمح بإدانة مرتكبيها، بل وقننت أيضاً قواعد جديدة تسمح باللجوء لبعض الإجراءات الاستثنائية التي تبيح استخدام الوسائل التكنولوجية الحديثة في المراقبة السابقة على ارتكاب الجريمة، تحقيقاً لبعض الأغراض الوقائية التي يأتي في مقدمتها الحيلولة دون ارتكاب الجرائم الإرهابية، وجرائم الاعتداء على الأمن القومي، وغيرها من صور الإجرام المنظم.

ويمثل التوجه الإجرائي السابق تغيراً ملحوظاً على مستوى السياسة الجنائية الإجرائية التي أصبح ميلها نحو التوسع في السلطات والصلاحيات التي قد تملكها جهات غير سلطتي التحقيق والاتهام في سبيل الحد من الجرائم ومكافحتها أحد أبرز معالمها ومظاهر تطورها في العصر الحديث.

ولعل التطور السابق هو ما يقودنا للتساؤل حول ماهية وطبيعة إجراء المراقبة التكنولوجية السابقة على ارتكاب الجريمة من ناحية، وعن مدى مشروعية هذه المراقبة ومبرراتها القانونية التي يمكن أن تسوغ خضوع الأفراد لصورة أو أكثر من صور انتهاك حرمة الحياة الخاصة في مرحلة سابقة على ارتكاب الجريمة من ناحية أخرى، فإذا انتهينا لإباحة هذه الطائفة من الإجراءات، فإن هذا يدفعنا لطرح تساؤل آخر، حول ما هي القيمة القانونية لنتائج هذه المراقبة السابقة أمام سلطات التحقيق والحكم؟.

ولعل الإجابة عن الأسئلة السابقة يمكن تقصيها من خلال تناول التنظيم القانوني لهذه المراقبة التكنولوجية السابقة على ارتكاب الجريمة في النظم الإجرائية المقارنة التي أقرت بجوازها، ووضعت لها الأطر القانونية المنظمة لجوانبها المختلفة، عسى أن يكون في هذا التناول ما قد يُسهم في الانتهاء لمشروع قانون يسمح بإدراج هذه الإجراءات الاستثنائية المستحدثة ضمن نظامنا التشريعي بما يسمح بكفاءة وفاعلية أفضل لنظامنا الإجرائي في مواجهة مختلف صور الإجرام، وفي ذات الوقت يحقق التوازن المنشود بين ضمان الحد المعقول من احترام سلطات إنفاذ القانون للحقوق والحريات الفردية من ناحية، وبين تمكينها

من أداء دورها الوقائي في منع الجرائم الخطيرة بما يكفل حماية الأمن القومي ويحافظ على أمن واستقرار المجتمع من ناحية أخرى.

وفي هذا الإطار تُعد الدوائر التليفزيونية المغلقة (CCTV Closed Circuit Television) الوسيلة الأكثر انتشاراً واستخداماً في مباشرة هذه الصورة من المراقبة، وقد أثارت مسألة استخدام كاميرات المراقبة التلفزيونية في أغراض المراقبة العامة للصورة والنشاط الخاص بالأفراد، وذلك في مرحلة سابقة على ارتكاب الجريمة، العديد من التساؤلات حول مشروعية هذه الوسيلة ومدى قبول العمل بها، خاصة في ضوء ما يكفله الحق في احترام الخصوصية من ضمانات تفرض عدم التعرض لنشاط الأفراد والاطلاع عليه بحال من الأحوال إلا في الأحوال الاستثنائية المبررة قانوناً.

إشكالية موضوع البحث:

تبرز إشكالية موضوع البحث في غياب التنظيم القانوني الإجرائي على المستوى الوطني لمثل هذه الإجراءات التي تبيح مباشرة المراقبة السابقة على ارتكاب الجريمة، خاصة في ظل تعارضها مع بعض الحقوق الفردية الأساسية، كالحق في الخصوصية، والحق في الصورة، مما دعا لدراسة هذا الموضوع لبيان مدى مشروعية اللجوء لبعض الإجراءات الاستثنائية التي قد تمس بهذه الحقوق الأساسية للفرد لأغراض مكافحة الجرائم وكشف وملاحقة مرتكبيها.

كما تظهر في ذات السياق إشكالية أخرى بسبب ما قد تمثله هذه الإجراءات من انتهاك لأسس البحث والتحري وقواعد الإثبات الجنائي التي تنهض جميعها على قرينة أو مبدأ أن المتهم برئ إلى أن تثبت إدانته بموجب حكم قضائي، والذي ترتب عليه مبدأ هام يحكم العلاقة بين المتهم وسلطات البحث والتحري من جهة، والتحقيق والاتهام من جهة أخرى، وهو ضرورة تحقيق التوازن الإجرائي بين المتهم وسلطات إنفاذ القانون، بحيث لا تتيح القواعد الإجرائية التقليدية المساس بهذه الحقوق إلا لأغراض البحث والتحري والتحقيق في جرائم وقعت بالفعل، سعياً للوصول لدليل، أو تعضيداً لآخر قائم بالفعل في الدعوى، وهي مفترضات لا تتحقق أو تتوافر في حالة اللجوء لبعض الإجراءات الجنائية الإدارية ذات الطبيعة القضائية لأغراض الوقائية من الجرائم الخطيرة في مرحلة سابقة على ارتكاب الجريمة، أو اكتشافها، أو الوصول لبعض الدلائل ضد الأشخاص الخاضعين لهذه الإجراءات.

ومن الملائم في هذا الصدد تقييم سبل المواجهة التشريعية لهذه الجرائم الخطيرة من زوايا عدة، فعلى المستوى الموضوعي يلاحظ أن المشرع قد واجه هذه الطائفة من الجرائم من خلال سياسة تجريم وعقاب تتسم بتعظيم الغرض الوقائي على حساب الغرض العقابي، وهو ما دفع المشرعين في مختلف النظم الجنائية المقارنة لخلق طائفة جديدة من الجرائم اصطلح الفقه على تسميتها بالجرائم العاقة أو المانعة، وهو ما يمكن أن نطلق عليه وبحق تجريم وقائي ينهض على مواجهة خطر الأفعال التي تهدد أمن وسلامة واستقرار المجتمعات بتجريمها في مراحل سابقة على الشروع المعاقب عليه، وذلك كتجريمها في مراحل العزم والتفكير في بعض الأحيان، وفي مرحلة الأعمال التحضيرية في أحيان أخرى، وذلك كحل وقائي يحول دون ارتكاب أفعال تلحق الضرر بالفعل بالمصالح السابقة[1].

ومن هنا تبرز أهمية تناول موضوع الدراسة، فإذا كان المشرع على المستوى الموضوعي لجأ إلى سياسة عقابية استثنائية عظم فيها من قيمة الوقاية والمنع، فهل يمكن أن يقابل هذه السياسة الموضوعية سياسة مماثلة على المستوى الإجرائي، بحيث تعظم من الدور الوقائي للإجراءات الجنائية على حساب أغراض التحقيق والحكم، من خلال نظم إجرائية استثنائية تتيح مباشرة بعض الإجراءات الماسة بحرمة الحياة الخاصة، أوالتي تتعارض مع أصل البراءة والتي يمكن مباشرتها دون سبق ارتكاب جريمة، أو قبل اكتشافها من قبل السلطات المختصة ضد أشخاص لا توجد دلائل أو أدلة كافية تقرر تورطهم فيها، وذلك تحقيقاً لذات الغرض الوقائي.

وهنا يمكننا القول بأنه وإن كانت التشريعات الجنائية الإجرائية المقارنة قد حرصت على تحقيق موازنة موضوعية وإجرائية في مكافحة الجرائم من خلال تطبيق ذات النهج الموضوعي على المستوى الإجرائي بتبنيها لإجراءات استثنائية يمكن من خلالها تعظيم الغرض الوقائي على حساب الغرض العقابي، إلا أن تشريعاتنا الإجرائية باتت لا تسير في ذات الاتجاه، بحيث أضحى البون شاسعاً بين الأفكار والقيم القانونية الحاكمة للسياسة الجنائية على المستوى الموضوعي، وبين تلك التي مازالت حاكمة للسياسة الجنائية على المستوى الإجرائي.

(1) انظر في تفاصيل هذه السياسة العقابية: أستاذنا الدكتور: مأمون محمد سلامة، الأحكام الخاصة بالجرائم الماسة بأمن الدولة، دار الفكر العربي، طبعة 1997، ص 34 وما بعدها، د. محمد عبدالكريم نافع: الجرائم الماسة بأمن الدولة من الداخل والخارج، بدون ناشر، ومن أمثلة التدخل التشريعي بالتجريم في حالة التفكير والعزم على ارتكاب الجريمة في مرحلة سابقة على مباشرة أي عمل مادي.

منهج البحث وخطته:

ومن مجموع ما سبق، فإنه يمكننا القول بأن تناول هذا الموضوع يقتضي استخدام المنهج الوصفي والتحليلي والمقارن من خلال تناول التنظيم القانوني للمراقبة السابقة على ارتكاب الجريمة في التشريعات الإجرائية المقارنة بالوصف والتحليل المناسب، وعلى ذلك فقد تم تقسيم موضوع البحث على النحو التالي: -

فصل التمهيدي: التعريف بالدوائر التلفزيونية المغلقة (CCTV).

المبحث الأول: أوجه الاستخدام الأمني لكاميرات المراقبة التلفزيونية المغلقة(CCTV).

المبحث الثاني: مدى تعارض المراقبة التكنولوجية السابقة على ارتكاب الجريمة مع الحق في الصورة

المبحث الثالث: أحكام المراقبة التكنولوجية السابقة على ارتكاب الجريمة للصوت والصورة في التشريعات الإجرائية المقارنة.

المبحث الرابع: القيمة القانونية لتسجيلات كاميرات المراقبة التلفزيونية المغلقة CCTV.

الخاتمة والنتائج والتوصيات.

المبحث التمهيدي
التعريف بالدوائر التليفزيونية المغلقة (CCTV)

الدوائر التليفزيونية المغلقة عبارة عن «نظام من الكاميرات – يتضمن أو لا يتضمن أداة للتسجيل – يرسل الصور إلى مجموعة من أجهزة الرصد أو المراقبة، ولا تخضع هذه الصور للبث العام»[1].

حيث تقوم هذه الدوائر التلفزيونية برصد صور تلفزيونية عبر دائرة مغلقة عند حدوث حركة ضمن الأماكن المرصودة، ويمكن وضع هذه الكاميرات باستخدام تشكيلة من عدسات المراقبة المخفية، كما يمكن إخفاء العدسات في نقاط التغذية بالتيار الكهربائي أو على هيئة مرشات مقاومة الحريق أو فتحات التهوية وما إلى ذلك[2].

(1) Herman Kruegle; CCTV surveillance: analog and digital video pratical and techonology, Butterworth – Heineman, 2007, p.354.

caint- paul) (Saint- paul) Jean – christophe; délit d' atteinte à L'intimité de La vie privée exige- t- iL …. Une) atteinte effective à L'intimité de La vie privée? D. 1999. p. 152 .

(2) حسن جلال زايد: عمليات الشرطة، الجزء الأول، أكاديمية شرطة دبي، 2010م، ص 220.

ومن الملاحظ التزايد العام في استخدام أنظمة المراقبة التليفزيونية CCTV على المستوى الوطني لدى الكثير من الدول، وذلك لمواجهة التحديات الأمنية المتزايدة، ففي المملكة المتحدة يمكن القول بأن التزايد الملحوظ في استخدام كاميرات الدوائر التلفزيونية المغلقة لم يكن حتميًا[1]. والحقيقة أن الشرطة كانت عازفة عن استخدام مثل هذه التقنيات أو تشجيع استخدامها لخشيتها من النظر إليها باعتبارها «الأخ الأكبر» Big Brother، أو بسبب القيود القانونية المحتملة. وعلى النقيض من ذلك، كانت السلطات المحلية أسرع في اقتناعها بمزايا هذه التقنيات الحديثة، ومن ثم استخدامها لأغراض منع الجريمة وغيرها من الأغراض المحلية الأخرى[2]، ويمكن القول بأن كاميرات المراقبة أو كما يطلق عليها أنظمة التصوير والتسجيل المغلق CCTVقد أصبحت من أنماط التطبيقات التكنولوجية الشائعة الاستخدام، وذلك دون حاجة إلى تبرير معين غير الحفاظ على الأمن وضمان وكفالة قدر من التغطية الرقابية لأماكن تواجده بما يحمل الأفراد على الخضوع للقانون واللوائح والالتزام بهما.

أما في اليابان، فلا يتم استخدام مصطلح الدوائر التليفزيونية المغلقة. وبدلاً عن ذلك، يتم استخدام طائفتين مستقلتين من الكاميرات تتمثلان فيما يلي[3].

- كاميرات منع الجريمة: crime prévention cameras) Bouhan Camera) حيث يتم تسجيل الصور، ولكن لا تخضع للمراقبة الفورية.
- كاميرات المراقبة surveillance cameras) Kanshi Camera) حيث يتم تسجيل الصور، ومراقبتها مراقبة فورية بواسطة مشغل بشري[4]، ويلاحظ أن اليابان تستخدم، بصفة عامة، أنظمة منع الجريمة.

(1) Goold, CCTV and Policing: Public Area Surveillance and Police Practices in Britain, 69.

(2) Ibid., 83.

(3) Nagoya Crime Prevention Camera Centre Blog: The difference between crime prevention cameras' and surveillance cameras' (Bouhan cameras (crime prevention cameras) are used to prevent crime and their images are recorded for play back at a later time. On the other hand, kanshi cameras (surveillance cameras) are normally monitored live and the cameras can be moved by operators when necessary.

(4) Kanshi systems were often classified as Bouhan systems by the operators due to the purpose of the system: if a systems' purpose was only to prevent and deter crime, and not to follow suspicious people or activities, then it was classified as a Bouhan system, even if an operator was constantly monitoring images from the cameras.

المبحث الأول
مظاهر الاستخدام الأمني لكاميرات المراقبة التلفزيونية المغلقة (CCTV)

في فرنسا يمكن القول بأنه في مجال البحث والتنقيب عن الجريمة يكون لمأموري الضبط القضائي أن يتخذوا الإجراءات التي تسهل عليهم ذلك البحث من أجل الوصول إلى معرفة مرتكب الجريمة، وبما أن مصلحة المجتمع تحتم السماح للسلطة العامة استخدام الطرق التي تمكنهم من القبض على الجناة، فيكون من المنطقي إضفاء صفة المشروعية على الوسائل التي تمكنهم من التقاط صور المشتبه فيهم.

وقد بدأ جهاز الشرطة الفرنسي منذ مطلع الستينات من القرن الماضي في الاعتماد على أسلوب المراقبة عن طريق الدوائر التلفزيونية المغلقة (CCTV) التي تركب عدساتها بمواقع مختارة في الميادين والطرق العامة بالمدن لمراقبة حركة المارة والسيارات وأماكن التجمعات، فضلاً عن تصوير المسيرات والمظاهراتMarches and Manifestation ، وذلك لمعرفة منظميها ومثيري الشغب وتقدير الأساليب لمواجهتها، ويعد ذلك الأسلوب المتبع من قبل الشرطة وسيلة فاعلة لمنع الجرائم، ودليلاً قطعيًا على وقوع الجريمة متى خلت الصورة والتسجيلات المقدمة من التحريف والخداع وعمليات المونتاج[1].

ويرى جانب من الفقه أن استخدام مثل هذه الأساليب كوسيلة إثبات أثناء البحث والتنقيب عن الجرائم، فإنها تكون ذات أثر إيجابي، وتسمح بإمكانية الوصول إلى الحقيقة في أسرع وقت ممكن[2].

ومن المدن الفرنسية التي استخدمت ذلك الأسلوب مدينة مارسيليا Marseille حيث أصدر المجلس المحلي للمدينة قراره في 16 أكتوبر 1972م بالموافقة على إنشاء دائرة مركزية للمراقبة التلفزيونية لحركة المرور، ويعمل هذا النظام في وسط المدينة[3].

(1) Grossen : Rapport sur La protection de La personnalité en droit privée société Suisse des jurists, 1960 , p. 58. ets.

(2) Grossen : op . cit, p. 58 .

(3) le conseil municipal de **la ville fe** Marseille a approuvé (850.4/Par décision du 16 Octobre 1972 (Rapport 72 le prohect de realization d'un poste central du sur reillance de la circulation routiéve par television ce systéme Fonctionne à L'heur actuelle dans Le centre de La ville.

وتعد هذه الوسائل من الإجراءات الوقائية التي تتبعها الشرطة من أجل الحفاظ على النظام العام والآداب، أما إذا أثيرت الشكوك حول شخص ما بشأن ارتكابه لجريمة معينة، فإنه يكون لمأمور الضبط القضائي اتخاذ كافة الإجراءات المشروعة في مرحلة جمع الاستدلال، وذلك من أجل الوصول للجناة، إلا أن مشروعية هذه الإجراءات يرتبط بضرورة ألا يكون في مباشرتها ما يمثل مساسًا بحرية الأفراد في المجتمع، أو انتهاكاً لحرمة حياتهم الخاصة.

ويرى بعض الفقه أن هذه القاعدة أصبحت هي الحاكمة في نطاق بحث مدى جواز تصوير الأشخاص بواسطة الأجهزة التقنينية الحديثة، ككاميرات المراقبة التلفزيونية المغلقة CCTV وذلك منذ صدور القانون الخاص بحماية الحياة الخاصة في 18 يوليه 1970م، حيث أصبح منذ ذلك الوقت من غير الجائز تصوير الأشخاص في الأماكن الخاصة حتى ولو كان ذلك بواسطة جهاز موجود في مكان عام[1].

وتجدر الإشارة إلى أن المشرع الإماراتي يعتبر أول مشرع عربي يقرر تنظيم استخدام كاميرات المراقبة في أغراض المراقبة الأمنية، وذلك بمقتضى القانون رقم 24 لسنة 2008 بشأن مقدمي الخدمات الأمنية ومستخدميها والمعدل بالقانون رقم 10 لسنة 2014، ثم أعقبه في ذلك المشرع القطري بإصداره القانون رقم 9 لسنة 2011 بشأن تنظيم استخدام كاميرات وأجهزة المراقبة الأمنية، هذا وقد عرفت المادة الأولى من هذا القانون كاميرات وأجهزة المراقبة بأنها «كل جهاز معد لنقل وتسجيل الصورة، بهدف مراقبة وملاحظة الحالة الأمنية».

(1) انظر في هذا الشأن:
Contrucci marseille L'oeil de la circulation est en place Journal.. le soir du 24 septembre 1975.
Levasseur (B) ; Les Méthodes scientifiques de recherché de La verité colloque d'abidijan 10 – 16- Janvier 1972, Rev. inter Dr. pen. Paris, 1972, p. 345 .

المبحث الثاني
مدى تعارض استخدام كاميرات المراقبة التلفزيونية المغلقة CCTV مع الحق في الصورة

يمكن القول بأنه من المتفق عليه في مجال البحث والتحري عن الجرائم أنه يمكن لمأموري الضبط القضائي أن يتخذوا بعض الإجراءات التي تسهل عليهم ذلك البحث من أجل الوصول لمعرفة مرتكب الجريمة، وبما أن مصلحة المجتمع تحتم السماح للسلطة العامة باستخدام الطرق التي تمكنهم من القبض على الجناة فيكون من المنطقي إضفاء صفة المشروعية على رسم صورة للمتهم أو التقاط صورة له تسهل على المجني عليه أو غيره من الشهود التعرف عليه[1].

ولا غرو أن اعتماد جهاز الشرطة على أسلوب المراقبة عن طريق الدوائر التلفزيونية المغلقة التي تم تركيب عدساتها في مواقع مختارة وذلك لمراقبة الحركة العامة وأماكن التجمعات فضلاً عن تصوير المسيرات والمظاهرات Marches and Manifestation وذلك لمعرفة منظميها ومثيري الشغب وتقدير أنسب الأساليب لمواجهتها[2] أدى إلى إثارة التساؤل حول مدى مشروعية هذه التسجيلات وما إذا كانت تتعارض مع حق الفرد في الصورة أم لا؟ خاصة إذا تمت هذه التسجيلات دون استئذان الشخص الخاضع لها أو إعلامه بها؟.

المطلب الأول
مدى تعارض استخدام كاميرات المراقبة التلفزيونية في التصوير والتسجيل لأغراض المراقبة مع حق الفرد في الصورة

تعود نشأة الحق في الصورة للقضاء الفرنسي Le droit à L'image وذلك منذ النصف الثاني من القرن التاسع عشر، وذلك رغبة منه في توفير الحماية اللازمة للأشخاص ضد التقاط صورهم أو نشرها بغير رضاءهم، ثم تم تقنين هذه الحماية بنصوص محدودة بموجب قانون

(1) Ravans: liberté d'éxpression et protection de droits de la personnalité , Dalloz, 2000, chron. p. 459. p. 149 .

(2) Ravans; op. cit, p. 150 .

grossen; Rapport sur la protection de la personnalité en droit privée société Suisse des jurists, 1960, p. 58 ets .

الصحافة الصادر في 29 يوليو 1881 الذي يعتبر أول قانون يجرم التقاط الصورة ونشرها[1].

وإن كان نطاق التجريم قاصر فقط على صور رئيس الجمهورية وغيره من رؤساء الدول الأجنبية وحكوماتها ووزراءها[2].

وتجدر الإشارة إلى أن القضاء الفرنسي قد أكد على أن مضمون الحق في الصورة يقرر لصاحبه سلطة الاعتراض على التقاط الصورة بغير رضاه[3].

ويتجه بعض الفقه إلى القول بأن الحق في الصورة يعد امتدادًا طبيعيًا لحق الإنسان في الملكية الذي يؤدي إلى اعتبار الإنسان مالكًا لصورته[4]، في حين يتجه البعض الآخر إلى أن

(1) Ravanas . La protection des personnes contre la realization et la publication de leur image preface de Pierre kayser , paris , 1978 , p. 181 . p. 414 .

(2) وتجدر الإشارة إلى أن حماية الحق في الصورة قد بدأت في نطاق القانون الفرنسي من خلال الحماية المدنية، حيث لم يكن هناك أي نص عقابي أو إجرائي يمنع التقاط الصورة لأشخاص دون رضاءهم أو علمهم، ولعل عدم كفاية هذه الجزاءات المدنية وعدم قدرتها على تحقيق الردع هو ما دعا للمناداة بتجريم الاعتداء على الحق في الصورة تحقيقا للردع المطلوب. انظر في ذلك:

Kayser. Les droit de la personnalité , aspects theoriques et pratiques, Rev. trim . dr . civ. 1971, No 42 p. 506.

Gassin : vie privée (atteinte à la) encyclopédie , Dalloz, droit penal , Dalloz , 1976, No . 10

Decocq; Rapport sur le secret de la vie privée en droit Francais Journées libanaise de L' Association H capitan travaux de L'association H capitan, T. 25, paris, Dolloz, 1971, p. 4071.

ومن الأحكام القضائية التي أقرت الحق في حماية الصورة الشخصية حكم محكمة Seine المدنية الصادر في 16 يونيه 1858 حيث جاء في هذا الحكم أنه "من حق الشخص الاعتراض على نشر صورته وأن هذا الحق مطلقًا للشخص".

3 – 62-Trib – civ- seine 16 Juin 1858, Dalloz 1858 .

وكذلك حكم محكمة استئناف باريس الصادر في 8 يوليو 1887م .

Cour d'appel de paris 8 Juillet 1887, Gaz, Pal. 1888 , 1 sem . p.

(3) حيث قضت محكمة Paris الابتدائية في 30 مايو 1975 بتعويض السيدة Francois marette وذلك لقيام إحدى المجلات بنشر صورة تمثلها أثناء اشتراكها بمظاهرة بالطريق العام نظمتها حركة تحرير المرأة وجاء في حيثيات الحكم أن المدعية لم توافق صراحة أو ضمنًا على التقاط صورتها أو نشرها.Trib . gr , inst paris 30 mai 1975.

كما قضت أيضًا محكمة السين Seine في قضية برجيت باردو بتعويضها عن التقاط صورة ونشرها لجهاز تصوير وهي داخل منزلها.

Trib . gr . inst 24 Novembre 196 Gaz pal . 1966, p. 30

كما قضت محكمة جنايات باريس في 21 أكتوبر 1980 برفض الطعن المقدم من مدير مجلةparis – Match في الحكم الصادر ضده من محكمة باريس بتغريمه 6000 فرنك مع نشر الحكم الصادر ضده لقيامه بنشر صورة الممثل Jean chbon وهو على فراش الموت دون إذن منه لوقوعه تحت طائلة المواد 368 و 269 و -37 من قانون العقوبات الفرنسي القديم. انظر:

Levasseur : Charonique de Juris prudence, Rev.S.C. paris 1981, p. 878 .

(4) Ravanas : La protection des personnes contre La realization et la public de leur image …. op . cit, p. 41 .

Edelman ; esquisse d'une Théorie du sujet L'homme et son image , Dalloz , 1970, chrornis 129 et 121 .

الحق في الصورة حق من الحقوق العفوية التي ترتبك بالذمة المالية، فهو أشبه في هذه الحالة بحق المؤلف[1].

بينما يذهب الرأي الراجح وبحق إلى اعتبار الحق في الصورة من عناصر الحياة الخاصة وترتيبًا على ذلك يعد الحق في الصورة من الحقوق اللصيقة بالشخصية[2].

هذا وقد انتقد بعض الفقه والقضاء اعتبار الحق في الصورة كعنصر من عناصر الحياة الخاصة، ذلك أن الحياة الخاصة تنتهي عندما تبدأ الحياة العامة، وبالتالي من المتصور أن يحدث اعتداء مبرر على الحق في الصورة في نطاق الحياة العامة (1)، كما أن تخويل الشخص الحق في الاعتراض على التقاط صورته أثناء ممارسته لحياته العامة دون رضاه لما فيه من اعتداء على خصوصيته لا يعني أن يندرج الحق في الصورة ضمن الحق في الحياة الخاصة[3].

وهذا الاتجاه الأخير أيدته بعض أحكام القضاء الفرنسي التي قررت أن الحق في الصورة مستقل عن الحق في حماية الحياة الخاصة، ويمكن أن يقع عليه اعتداءات أثناء الحياة العامة للشخص حتى ولو لم يكن هناك سر يجب المحافظة عليه[4] ، كما أقرت محكمة باريس الابتدائية في حكم آخر لها أن لكل شخص حق مانع على صورته ويمكنه أن يعترض على التقاطها ونشرها حتى لو لم ينطو ذلك على مساس بحياته الخاصة[5]،كما أقرت محكمة

وهذا الاتجاه هو ما ذهب إليه حكم محكمة السين الصادر في 15 فبراير 1882.

(1) Martin; le secret de la vie privee , Rev. Dr. Civ. 1959, p. 242.

وهذا هو ما ذهبت إليه محكمة السين في حكم آخر لها صادر في 24 يوليو 1966.

Trib . gr . inst 24 Novembre 1966, Gaz. pal . 1966, p. 30

(2) Decocq : Rapport sur Le Secret de La vie rrivée … op. cit, p. 483 .

Ravanas ; La protection des personnes , op. cit. P.422.

هذا وقد أيدت العديد من الأحكام هذا الاتجاه وقررت أن الحق في الصورة هو مظهر من مظاهر الحياة الخاصة، ومن ذلك ما قررته محكمة باريس في حكمها الصادر في 13 مارس 1965 من أن تصوير الشخص بغير رضاه واستغلال هذه الصورة يعد من قبيل المساس بالحياة الخاصة، كما أوردت ذات المحكمة أمثلة لعناصر الحياة الخاصة من بينها الحق في الصورة.

Paris Référe 13 mars 1965 . J. C. P. 1965 - 11- 14223 .

Paris 15 mai 1970 , Dalloz, 1970 – 466 .

(3) Nersson : distinction du droit à L'image et du choit au respect de la vie privée , Rev trim . dr civ, P. 364 , 365 .

(4) Trib. Gr. Inst . Grasse Refére 27 Février 1971 , J. C. P. 1971 – 16734, Note. Lindon .

(5) Trib . gr . inst, paris 3 juillet 1974 J. C. P, 1974 – 11- 17873 2espece Note. Lindon.

مارسيليا Marseille الابتدائية بأن الحق في الصورة لا يختلط بالحق في احترام الحياة الخاصة ويمكن أن يتعرض للمساس حال ظروف ترتبط بالحياة العامة للشخص[1].

رأينا الخاص في طبيعة الحق في الصورة:

ومن جانبنا فإننا نرى أن الحق في الصورة يدخل في نطاق الحق في الحياة الخاصة إذ لا يمكن الركون لفكرة جواز المساس بهذا الحق متى انتقل صاحبه لمباشرة حياته العامة كأساس للقول بخروجه عن نطاق هذا الحق، ذلك أن إباحة المساس بالحق في الصورة أثناء مباشرة الحياة العامة ما هو إلا استثناء من الأصل العام الذي يضفي على هذا الحق حماية هي أقرب في جوهرها للحماية المقررة للحق في الحياة الخاصة ، وترتيباً على أن الحق في الحياة الخاصة حقاً نسبيا؛ فإن الحق في الصورة تمتد إليه هذه الخاصية وبالتالي يظل متمتعاً بالحماية القانونية المقررة له إلى أن يدخل هذا الحق بفعل ممارسة صاحبه أو وضعه الاجتماعي أو ضرورات الحياة العامة في نطاق الإباحة التي تبيح المساس به لأغراض معينة.

ويتوافق هذا الرأي مع ما ذهب إليه كل من المشرع الاتحادي الذي اعتبر صورة الشخص من الأمور التي تدخل في نطاق الحياة الخاصة، ولذلك يعد الاعتداء الذي يقع على الحق في الصورة من قبيل الاعتداء على الحق في الحياة الخاصة.

حيث نصت المادة 378 من قانون العقوبات الاتحادي في بندها الثاني على الاعتداء على الحق في الصورة بقولها: « يعاقب بالحبس والغرامة كل من اعتدى على حرمة الحياة الخاصة أو العائلية للأفراد وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه:

أ ـ .....

ب ـ التقط أو نقل بجهاز من الأجهزة أيًا كان نوعه صورة شخص في مكان خاص».

والأمر ذاته هو ما ذهب إليه المشرع الفرنسي بموجب قانون 17 يوليو 1970 الذي جرم الاعتداء على الحق في الصورة وذلك بمقتضى المادتين 368 و369 والتي تم تنظيمها مرة

(1) Trib. Gr. Inst Marseille Reféve 18 Janvier 1974 Gaz Pal des 15 et 16 Avril 1974 p. 8.

Paris 10 December 1976.Gaz. Pall, des 11 et 12 mai 1977m p. 14.

أخرى عند صدور قانون العقوبات الفرنسي الجديد في عام 1992 الذي شدد العقوبات المقررة لهذه الجريمة بمقتضى المادتين 1/226، 2/226 منه.

وتجدر الإشارة إلى أن المادة 368 من قانون العقوبات الفرنسي القديم كانت تعاقب على فعل الالتقاط La Fixation والثاني هو النقل La Transmission [1]، ثم أضاف بمقتضى نص المادة 1/226 من قانون العقوبات الفرنسي الجديد فعل التسجيل enregistrant الذي يقصد به حفظ صورة الشخص على مادة معدة لذلك لمشاهدتها فيما بعد[2].

والملاحظ أن كل من القانونين الإماراتي والفرنسي قد اشترطا لوقوع جريمة التقاط الصور أو تسجيل نشاط الأفراد أن يتم ذلك في مكان خاص ودون رضاء صاحب الشأن، وهو ما يعني بمفهوم المخالفة إباحة هذا الالتقاط أو التسجيل متى وقع في مكان عام أو برضا صاحب الشأن.

ومن هنا يثار التساؤل حول مدى مشروعية استخدام كاميرات المراقبة التلفزيونية المغلقة CCTV في تصوير الأشخاص وتسجيل نشاطهم في كل من الأماكن العامة والأماكن الخاصة؟

(1) Isabelle Lo lies ; La protection de La vie privée universite de droit d'economie et des seiences d' Aix Marseille, 1999, p. 104 .

(2) د. إبراهيم عيد نايل: الحماية الجنائية لحرمة الحياة الخاصة من قانون العقوبات الفرنسي، الحماية الجنائية للحديث والصورة ، ط 2000، دار النهضة العربية، ص 159.

وتجدر الإشارة إلى أن المشرع الفرنسي قد وسع من نطاق الحماية المقررة للحق في الصورة، بموجب نص المادة 1/226، حيث كانت المادة 368 الملغاة تقتضي أن يتم الالتقاط والتسجيل بوسيلة معينة ثم عدل عن ذلك فأجاز أن يتم الالتقاط بأي جهاز من الأجهزة وبأي وسيلة معينة. راجع في ذلك:

Isabelle Lo lies , op . cit . p. 104 et 105.

المطلب الثاني
مدى مشروعية استخدام كاميرات المراقبة التلفزيونية CCTV في تصوير وتسجيل النشاط العام للأفراد في الأماكن الخاصة

جرم المشرع الاتحادي بمقتضى المادة 378 عقوبات اتحادي والتي تقابل نص المادة 226 – 1 من قانون العقوبات الفرنسي، التقاط صور الأفراد وتسجيلها متى وقع ذلك في مكان خاص، وعلى ذلك يعد المكان في هذه الحالة عنصراً من عناصر التجريم وبدونه فلا مجال لقيام هذه الجريمة، وترتيباً على ذلك يعد تسجيل نشاط الأفراد العام أو التقاط صورهم أمراً مشروعاً ويخرج عن نطاق الحماية الجنائية المقررة قانوناً متى كان الشخص متواجداً في مكان عام[1].

وتطبيقًا لذلك فلا يبسط القانون حمايته لمن يتواجد في مكان عام إذا ما تم تصويره أو نقلت صورته؛ لأن المعيار هنا هو وجود المجني عليه في مكان خاص، حتى ولو كان في وضع طبيعي فلا يجوز نقل صورته آنذاك، كمن يجلس بكامل ملابسه في وضع طبيعي، ورغم ذلك تقوم الجريمة أيضًا لأن الأساس هو التقاط الصورة أو نقلها للشخص وهو في مكان خاص لا يجوز دخوله إلا بإذنه[2].

معيار التمييز بين المكان العام والمكان الخاص:

لا شك أنه بتحديد مدلول المكان الخاص يترتب عليه بالتبعية أن يعد ما عداه مكانًا عامًا، وفي هذه الاتجاه يمكن التمييز بين اتجاهين في تحديد مدلول المكان الخاص إحداهما موضوعي يرتبط بطبيعة المكان ذاته، والآخر شخصي لا يعول بشكل أساسي على طبيعة المكان بقدر ما يعول على هيئة الشخص وحالته أثناء مباشرته لنشاطه العام.

الاتجاه الموضوعي في تحديد المكان الخاص :

وقوام هذا الاتجاه تحديد الأماكن الخاصة بصورة موضوعية مطلقة من خلال تعداد هذه الأماكن دون نظر لهيئة الأشخاص أو حالتهم أثناء مباشرة نشاطهم التام فيها، ويرى أنصار

(1) Bécourt: La protection de la vie privée et limites communication écrite pour la troisieme collque international sur la convention Europpéenee de droit de l'homme bruxelles 30 Sep. 3 Octonre, 1970, p. 142 .

Stoufflet : Le droit de la personne sur son image cquelques remarques sur la protection de la personnalité, J. C. - P. 1957 – 1- 1374, No. 10.

(2) د. هشام محمد فريد رستم: المرجع السابق، رقم 49، ص 92.

هذا الاتجاه أن المكان الخاص هو كل مكان خلافًا للشوارع والطرقات والحدائق والميادين والملاعب وغيرها من الأماكن العامة بطبيعتها[1].

وتطبيقًا لذلك عرف بعض الفقه المكان العام بأنه «المكان العام هو الذي يباح فيه لكل شخص ارتياده دون حاجة إلى إذن خاص سواء كان هذا المكان مفتوح مطلقًا للجمهور أم بشروط خاصة[2].

وقد أيد القضاء الفرنسي في بادئ الأمر هذا الاتجاه ، حيث قضت محكمة باريس، برفض دعوى أقاماتها فتاة فرنسية ضد إحدى الصحف تأسيسًا على ما تحظره وتجرمه المادة 368 من قانون العقوبات، لقيام هذه الجريدة بنشر صورة لها وهي عارية الصدر أثناء تناولها للإفطار مع أصدقاءها على شاطئ Saint – Tropes وقد أسست المحكمة رفضها للدعوى بأنه "لما كان من الثابت أن ثمة عددًا كبيرًا من المصطافين العراة وشبه العراة متواجدون على الشاطئ دون أن يهتموا بسائر المصطافين أو يتأذوا من نظرات الآخرين، فإن صورة المدعية وهي عارية الصدر أثناء تناولها إفطارها على هذا الشاطئ لا يكون من شأنه أن يجعل التقاط الصورة قد تم في مكان خاص بالمعنى الوارد في المادة 368 عقوبات[3]، كما قرر أحد الفقهاء أن شاطئ البحر مكان عام لا يتطلب الدلوف إليه الحصول على إذن أو تصريح[4].

وعلى ذلك فالمكان الخاص هو كل مكان مسور لا تنفذ إليه نظرات الناس من الخارج

(1) Badinter: la protection de la vie privée contre L'écoute éléctronique clamdestine, J . C. P. 1971- 1- Doct, No. 2435.
د. ممدوح خليل البحر: حماية الحياة الخاصة في القانون الجنائي، دراسة مقارنة، رسالة دكتوراة، جامعة القاهرة، 1983، ص 319، د. محمد محمد الدسوقي: الحماية الجنائية لحرية الحياة الخاصة، رسالة دكتوراة، كلية الحقوق، جامعة القاهرة، ص 201 وما بعدها.
كما قضت محكمة جنحAix-enprovence في حكم لها ببراءة المتهم في واقعة تتلخص في قيام أحد الأشخاص بتصوير فتاتين أثناء تواجدهما بأحد شوارع باريس ثم قام بنشرها دون رضاهما ، مقررة في حكمها بأنه لا توجد ثمة انتهاك لحرمة الحياة الخاصة وفقًا للمادة 368 عقوبات لعدم توافر أحد العناصر المكونة للجريمة وهي المكان الخاص.
Trib- Corr Aix– en province `6 Octobre 1973, J. C. P. 1974 -11- No. 17623 note. Lindon, Rev. SC. Crim. 1976, obs. levasseur, p. 119.
وأيضًا:
Cour d'appel de toulouse 26 Février 1974. J. C. P. 1975 -11- 17903. Note. Lindon.
(2) Decocqe: Rapport sur Le secret de la vie privée en droit francais Journées Libanaises de L'Assocéation H. capitant, t. 25éd Dalloz, paris 1974, P. 476.
(3) Trib. Gr. Inst paris 18 Mars 1971 Gaz. Pal, 1972- 1 sem P. 59. Note. Pierre Frémond, J.C.P. 1971 – 11- 16875.
(4) Piganiol; Note sous La decision du 18 mars 1971, J. C. P. 1971, p. 448. ج

ويتوقف دخوله على إذن يمنحه في نطاق محدود من له ملكية المكان أو استعماله أو الانتفاع به[1]، كما عرفه البعض أنه المكان الذي يتوقف الدخول فيه على رضاء الشخص الذي يشغله[2].

الاتجاه الشخصي في تحديد مدلول المكان الخاص:

قوام هذا الاتجاه هو الركون إلى حالة الخصوصية التي يسبغها الأفراد على نشاطهم بغض النظر عن طبيعة مكان مباشرة هذا النشاط، وما إذا كان بحسب طبيعته مكان عام أم مكان خاص، وعلى ذلك فقد عرفه بعض الفقه بأنه المكان الذي يستخدم كإطار للحياة الخاصة، ولا يكون في مقدور الغير دخوله إلا برضاء صاحب الشأن[3].

وعلى هذا الأساس فقد عرف البعض المكان الخاص بأنه المكان الذي يكون دخوله متوقفاً على إذن مالكه أو المستغل أو المنتفع، ويكون بمثابة دائرة خاصة أو محددة للمتواجدين به[4].

وتطبيقًا لذلك قضت إحدى المحاكم الفرنسية بقيام جريمة التنصت في حق مستخدم لقيامه بوضع جهاز تنصت بمكتب مخدومه لمعرفة مكالماته مع محاميه، وقد انتهت المحكمة إلى أن مكتب رب العمل يعتبر مكانًا خاصًا، لأنه لا يستطيع أحد الدلوف داخله دون إذن صاحبه[5].

وتجدر الإشارة إلى أن القضاء قد اعتنق المفهوم الشخصي لتحديد مفهوم المكان الخاص معتمداً في ذلك على معيار الرضا الصادر عن ذوي الشأن بالولوج لهذا المكان ولو بالنظر،

(1) Bécourt: Réfléxions sur le project de loi relatife a La protection de la vie privée Gaz. Pal. 1970 – 1 er Sem, doct. P. 202.
(2) Ravanas: La Protection des personnes contre La réalosation La publication de leur image, 1978, p. 521.
(3) Chavanne: La protection de la vie privée dans la loi du 17 Juillet 1970, Rev. Sc. Crim. 1971, p. 613.
(4) Bécourt (D); Réfléxions sur Le project de loi relative a la protection de la vie privée, Gaz. Pal 1970 1 er sem, doctrin, P. 202.
- Isabelle Lolies; La protection p»nale de la vie privée, op. cit. p. 115.
- Ravanas; La protection des personnes contre la realization et la publication de leur image 1978, p. 522.
(5) Arret de La cour de Cassation du 8 dec. 1983, Gaz. pal. 1984, 11- p.8.
Cass. crim, 6 oct 1984m Gaz.Pal, 1985, p.394.

وتطبيقًا لذلك قضت محكمة استئناف باريس Paris بتوافر صفة الخصوصية بالنسبة لليخت الخاص في عرض البحر، حيث قررت صفة المكان الخاص إذا كان في عرض البحر ولو على غير مقربة من شاطئ أو ميناء لأن لكل شخص على متن قارب أن يعتقد إذا لم تكن ثمة قوارب تسير على مقربة منه أنه بمأمن من نظرات الغير[1].

في حين ذهب جانب آخر من الفقه والقضاء إلى اعتناق المفهوم الشخصي لتحديد فكرة المكان الخاص إلى التعويل على معيار استخدام المكان L'utilisation du lieu، وعلى ذلك يعتبر المكان خاصاً إذا كان يخفي جانب من الحياة الخاصة حتى ولو كان عاماً بطبيعته وهذا هو الرأي الذي سارت عليه أحكام القضاء.

وخلاصة القول أن الفقه والقضاء والتشريع سواء في فرنسا أو في مصر يجمع على أن التقاط الصور الخاصة بالأفراد وتسجيل نشاطهم العام يكون مباحاً ولا تقع به جريمة متى تم ذلك في مكان عام يمكن ارتياده من قبل الجمهور سواء كان ذلك بمقابل أو بدون مقابل، وسواء كان الدخول منوطًا بشرط أم لا، وسواء كان هذا المكان عاماً بطبيعته أم كان عاماً بالتخصيص أو بالمصادفة[2].

(1) انظر تفاصيل هذا الحكم والتعليق عليه لدى:
.Levasseur ; in chronique de Jurisprudence , Rev. SC. Crim, 1980 , p. 714

(2) انظر في ذلك:
Ravanas; La protection des personnes contre la realization et la publication de leur image, op. cit. p. 520
وتجدر الإشارة إلى أن محكمة النقض المصرية قد قضت فيما يتصل بالمكان العام بالمصادفة بأنه "المكان العام بالمصادفة هو بحسب الأصل مكان خاص مقصورًا على أفراد وطوائف معينة ولكنه يكتسب صفة المكان العام في الوقت الذي يوجد فيه عدد من الأفراد بطريق المصادفة أو الاتفاق أما في غير هذا الوقت فإنه يأخذ حكم الأماكن الخاصة. نقض 14 أكتوبر 1973م، مجموعة أحكام النقض س 224 رقم 175، ص 847.

المطلب الثالث
مدى مشروعية استخدام كاميرات المراقبة التلفزيونية CCTV في تصوير صورة ونشاط الأفراد في الأماكن العامة

يثار التساؤل حول ما إذا كان تواجد الشخص في مكان عام يبيح تصوير صورته أو هيئته ونشاطه الفردي أو الجماعي على اعتبار أنه أصبح جزء من المكان العام، وما إذا كان حظر تصوير الأشخاص بدون إذن يسري سواء كان الشخص في مكان عام أم في مكان خاص؟.

وفي سياق الإجابة على هذا التساؤل يمكن القول بأن الفقه لم يتفق في هذا الشأن على رأي واحد إذ انقسم في هذا الصدد إلى اتجاهين:

الاتجاه الأول: إباحة تسجيل نشاط الأفراد بواسطة كاميرات المراقبة التلفزيونية CCTV في الأماكن العامة:

هذا الاتجاه يرى أن الأفراد بخروجهم للأماكن العامة قد أصبحوا جزء منها، كما أنه يعني بالضرورة توافر الرضا بالتعرض لنظرات الناس، وهو ما لا يمثل انتهاكًا لحقه في الخصوصية الذي خرج عن نطاقه بدخوله المكان العام، وتسجيل النشاط الفردي في هذه الحالة بواسطة كاميرات المراقبة التلفزيونية CCTV لا يعدو أن يكون تثبيتًا لأحداث مباح للكافة رؤيتها في الأماكن العامة باعتبارها جزء من المكان العام[1].

ولعل ما يدعم هذا القول؛ إن إباحة تسجيل هذه الأحداث يقف عند حد التسجيل فقط، دون أن يمتد الأمر لإباحة نشرها أو استخدامها إلا في الأحوال المحددة قانونًا[2].

هذا وقد انتُقد هذا الاتجاه تأسيسًا على أن مجرد الرؤية العادية العارضة تختلف عن التصوير أو التسجيل وبالتالي لا يجوز قياس جواز التصوير أو التسجيل على جواز رؤية

(1) Nerson: Les droits extra – parti moniaux, these, lyon 1939, p. 384.
Stoufflet: Le droit de la personne sar son image (quelques remarques sur la protection de la personnalite) J.C.P, -1957- 1– 1374. No. 10.

(2) Fougerol: La figure humaine et le droit, Thése. paris, 1913, p. 63 .

الأشخاص في الأماكن العامة[1].

كما أنه لا فائدة وفقًا للرأي السابق من إباحة التقاط الصور وتسجيل النشاط دون إباحة استخدامها إلا برضاء صاحبها، كما أنه ليس من المقبول أن يباح الاحتفاظ بتسجيلات وصور للغير دون رضاءه ولو كان الالتقاط أو التسجيل قد تم أو وقع في مكان عام[2].

الاتجاه الثاني: التفرقة في الإباحة بين ما إذا كانت صورة أو هيئة، ونشاط الأفراد هي الموضوع الأساسي أم أنها تظهر بصورة عارضة:

ويعول أنصار هذا الاتجاه على وضع الشخص في المكان العام أثناء التسجيل La position de la personnel وفرقوا بين الفروض التالية:

1 - إذا كان محل التصوير هو المكان العام ذاته ويظهر فيه الأشخاص بشكل عارض:

وفي هذا الفرض يكون ظهور الأشخاص أثناء مباشرتهم لأنشطتهم قد تم بصورة عارضة غير مقصودة، وهو ما يبرر إباحة التصوير أو التسجيل دون حاجة لإذن مبدئي من هؤلاء الأشخاص، فالتسجيل هنا ليس محله النشاط الفردي للأشخاص تحديدًا، إذ ينصب التسجيل هنا على مشاهد للحياة العامة بما فيها من تفاصيل يشكل مجموعها هذه الحياة[3].

هذا، وقد اتجه القضاء الفرنسي إلى إباحة تصوير الأشخاص في الأماكن العامة عندما لا تكون قسمات الشخص وأوصافه هي المحل الرئيس لهذا التصوير، وهو ما عبر عنه القضاء الفرنسي بحرية التقاط الصور أو تسجيل الأحداث في الأماكن العامة دون حاجة لإذن من الأشخاص المتواجدين فيه[4].

(1) د. حسام الأهواني: الحق في احترام الحياة الخاصة، المرجع السابق، ص 114.

(2) Kayser: Le droit dit à L'image mélanges 11, éd Dalloz et Siry, Paris 1961, p. 79, No. 8.

وتجدر الإشارة إلى أن النقد الموجه للرأي السابق قد وجد أساساً له في مظاهر التقدم العلمي الحديث الذي ترتب عليه أن تندمج عمليات التصوير والنشر معاً وتتمان في لحظة واحدة كما يحدث في حالة الإرسال التلفزيوني المباشر، فكيف يباح للشخص في مثل هذا الفرض أن يعترض بعد التصوير وقبل البث أو النشر!. انظر في ذلك: هبة أحمد حسانين: المرجع السابق، ص 553.

(3) Fougerol : La Figure humain, op . cit, p. 63 .

(4) Ravanas : La protection des personnes contre le realization et la publication de leur image , p. 143 .

وتجدر الإشارة إلى أن إباحة الالتقاط والتسجيل في الأحوال السابقة لا تمتد إلى إباحة نشر هذه الصور أو التسجيلات إلا بعد طمس معالم

2 - إذا كان محل التصوير أو التسجيل هو الأشخاص ونشاطهم:

ويذهب أنصار هذا الرأي إلى القول بعدم إباحة تصوير الأفراد تسجيل نشاطهم العام عندما يكون المحل الرئيس لهذه التسجيلات هو الشخص ونشاطه العام ذاته، بحيث لا يعدو المكان العام سوى أن يكون خلفية لا قيمة لها، وذلك على سند من القول بأن إباحة تصوير الأماكن العامة ومن فيها من أشخاص وما يدور فيها من أحداث تحقيقًا لمصلحة عامة هو أمر استثنائي أملته بعض الضرورات كحفظ الأمن وغيرها، وعلى ذلك وجب التقيد بحدود هذا الاستثناء وعدم إباحة التصوير إلا إذا كان محله المكان العام ذاته لا الأشخاص المتواجدين فيه[1].

ولعل الرأي السابق هو ما يحقق قدراً كبيراً من التوازن بين الحق في احترام خصوصية نشاط الأفراد وبين حماية الأماكن العامة التي قد يترتب عليها اللجوء لاستخدام بعض التقنيات التكنولوجية في مراقبة احترام المكان العام وقواعد الانضباط السلوكي فيه ولو امتد ذلك لتصوير وتسجيل أحداث تقع في هذه الأماكن يكون محورها نشاط فردي للأشخاص فرادى أو جماعات شريطة ألا يكون الغرض الرئيسي هو ترقب الأشخاص ذواتهم فيما يقومون به من نشاط.

3 - حكم تصوير وتسجيل اجتماعات الأفراد الخاصة في الأماكن العامة:

إذا كنا قد انتهينا فيما سلف إلى إباحة تصوير وتسجيل النشاط الفردي للأشخاص حال تواجدهم عرضاً في الأماكن العامة، إلا أنه ثمة تساؤل آخر يثار في هذا الشأن حول ما إذا كان نطاق إباحة تسجيل النشاط الفردي للأشخاص حال تواجدهم في مكان عام يمتد ليشمل تسجيل وتصوير الاجتماعات الخاصة التي تتم في أماكن عامة؟

ومثال ذلك تصوير الأشخاص أثناء اجتماعهم في احتفالية أو مهرجان أو مشاركتهم في مظاهرة أو تواجدهم في المقاهي والمطاعم ودور الاحتفالات المختلفة.

الأشخاص الموجودين فيها ما لم يحصل على رضاء منهم بالنشر، فإذا قام المصور بنشر الأحداث أو التسجيلات واعترض صاحب الشأن كان من الواجب محو هذه الصور والتسجيلات وإلا انعقدت مسؤولية المصور عن النشر بدون إذن أو رضاء. انظر في ذلك:

. Fougerol : La Figure humaine, op. cit, p. 64

(1) د. سعيد جبر: الحق في الصورة، دار النهضة العربية، القاهرة 1986م، ص 82، د. هدى أحمد حسانين: المرجع السابق، ص 556.

وفي هذا الصدد يذهب الفقه إلى القول بجواز تصوير وتسجيل نشاط الأفراد وصورهم أثناء مشاركتهم في الاجتماعات العامة التي يباح لأي فرد المشاركة فيها كالاحتفالات العامة والمهرجانات نظراً لطبيعتها العامة وعدم حاجتها لإذن لإباحة التصوير والتسجيل لأحداثها، فقد جرى العرف على إباحة تصوير هذه الأحداث والمشاركين فيها، إذ أن تواجد الشخص فيها ومشاركته في أحداثها تعني نزوله عن حقه في الاعتراض على التصوير أو التسجيل[1].

أما الاجتماعات الخاصة: Une Cérémonie privée فهي بطبيعتها لا يسمح للمشاركة فيها إلا للأشخاص المعنيين، وعلى ذلك فلا يجوز تصوير أو تسجيل هذه الاجتماعات إلا بناء على إذن من الأشخاص المعنيين[2]، وتطبيقًا لذلك رفضت محكمة باريس Paris الابتدائية إدانة مجلة Paris Match عندما قامت بتصوير إحدى المتظاهرات المشاركات في مظاهرة نسائية.

ومن جانبنا فإننا نرى أن هذه الاجتماعات الخاصة التي تجري وقائعها في أماكن عامة يجب التمييز بصددها بين أمرين؛ الأول وهو تصوير وتسجيل وقائع وأحداث هذه الاجتماعات الخاصة، والأمر الثاني هو نشر هذه الأحداث أو الوقائع، إذ أن الأمر الأول وهو تصوير وتسجيل أحداثها ووقائعها التي تدور في مكان عام يندرج من وجهة نظرنا في نطاق الإباحة الخاصة بجواز تصوير نشاط الأفراد والجماعات الذي يدور في المكان العام بدون إذن خاص منهم متى لم يكن هذا الاجتماع هو المحل الرئيس لهذا التسجيل أو التصوير، إذ لافارق هنا بين تسجيل الأحداث الفردية وتسجيل الأحداث الجماعية متى تمت في ذات المكان العام، فضابط المشروعية هنا يعود لكون التصوير لا يستهدف هذا الاجتماع الخاص بذاته وإنما تم تصويره عرضًا حال تغطية كاميرات المراقبة للمكان العام لأغراض حفظ الأمن والنظام، وعلى ذلك نرى أن تصوير جلسات ولقاءات الأفراد في المطاعم والمقاهي وغيرها من الطرق والشوارع والمناطق العامة مع ما تتضمنه من تفاصيل أمر مشروع إلا أن مشروعيته تقف عند حد التصوير والتسجيل دون نشر هذه التسجيلات وإتاحتها للكافة إلا بإذن من الأفراد ما لم يتم إخفاء معالم شخصيتهم حتى لا يتعرف عليهم الغير[3].

(1) Fougerol : La Figure humaine., op. cit, p.69 .
Ravanas : op. cit, p. 144 .
(2) Fougerol : La Figure humaine., op. cit, p.69 .
Ravanas : op. cit, p. 144 .
(3) تجدر الإشارة إلى أن الاحتفالات الدينية سواء العامة أم الخاصة قد ثار الخلاف حول مدى جواز تسجيل وقائعها وتصوير الأفراد

المطلب الرابع
دور الرضا وأثره في إباحة تصوير وتسجيل نشاط الأفراد بواسطة كاميرات المراقبة التلفزيونية CCTV

اتفق كل من المشرع الإماراتي والفرنسي على أن التصوير والتسجيل غير المشروع الذي تنعقد به المسؤولية الجنائية لمرتكبه وفقًا للمادة378 من قانون العقوبات الاتحادي والمادة 226-1، 226-2 من قانون العقوبات الفرنسي يقتضي أن تقع الأفعال السابقة دون رضاء المجني عليه[1].

وعلى ذلك فالرضا بالتصوير أو التسجيل يعد سببًا كافيًا لإباحة استخدام كاميرات المراقبة التلفزيونية المغلقة CCTV في تصوير وتسجيل النشاط العام للأفراد.

وعلى ذلك فإذا كان الرضا سببًا في إباحة هذا الفعل حتى قبل صدور قانون 17 يوليو 1970، واستقر القضاء على إعمال مقتضاه وإنتاج أثره[2]، إلا أن ثمة تساؤل يثار في هذا الصدد حول مشكل هذا الرضا ووسائل التعبير عنه ومدى افتراضه عند استخدام هذه الكاميرات في إكمال التصوير والتسجيل؟.

وفي هذا الصدد يمكن القول بأنه من المتفق عليه أنه يستوي القول بتوافر الرضا أن يعبر عنه صاحبه بأي وسيلة سواء أكانت كتابةً أو شفاهةً كما أنه يستوي أن يكون صريحًا أو ضمنيًا[3].

المشاركين فيها، وفي هذا الإطار قضى قاضي الأمور المستعجلة بمحكمة باريس الابتدائية؛ بإلغاء عرض فيلم سينمائي تعرض بالكشف عن حقيقة احتفال ديني لقبيلة حيث ظهر في ذلك الفيلم مشهد كاشف لشخصية بعض الحاضرين بهذا الاحتفال.
- Trib. gr . Inst Paris référés 6 Juin 1974, Dalloz, 1975 – J. P. 95, Note. Reymond Lindon.
(1) Gassin : vie privée " Atteintes à La :Encylopédie Dalloz No. 53.
- Ravanas : La protection des personnes contre la realization … , op. cit, p. 253.
(2) Paris 10 Avril. 1955, Dalloz 1955. p. 295.
(3) Ravanas : La protection des personnes contre la realization et la publication de leur image, p. 250
وتجدر الإشارة إلى أن الموافقة على التقاط الصورة أو تسجيل النشاط لا يعني الموافقة على نشرها، فقد أذن الشخص للغير بالتقاط الصورة دون أن يمتد هذا الرضا لإباحة نشرها، ما لم تدل ظروف الحال وملابساته على توافر الموافقة الضمنية على هذا النشر. انظر:
Rennes 23 Novembre 1903, S . 1904 11- 111 Dalloz, 1905 – 2 – 29.

وفيما يتصل بافتراض توافر الرضا بالتصوير والتسجيل باستخدام كاميرات المراقبة التلفزيونية المغلقة CCTV، فقد ذهب الفقه إلى القول؛ إن هذا الرضا يكون مفترضًا بقوة القانون في الحالة التي نصت عليها المادة 39 مكرر من قانون العقوبات المصري، والمادة 226 1- من قانون العقوبات الفرنسي وذلك إذا ما وقعت أفعال التصوير والتسجيل أثناء اجتماع على مسمع ومرأى من الحاضرين إذ يعد رضاهم في هذه الحالة مفترضًا[1].

كما قضت محكمة النقض الفرنسية في هذا الصدد بأن هناك بعض الفئات التي تفرض طبيعة عملهم وحرفتهم توافر قرينة ضمنية بالرضا بتصوير وتسجيل نشاطهم المهني الخاص بهم[2].

مدى جواز تصوير وتسجيل نشاط الأفراد في الأماكن الخاصة ؟:

لم يشر المشرع الإجرائي صراحةً إلى جواز قيام مأمور الضبط القضائي بالأمر بتسجيل الوقائع التي تدور في مكان خاص أسوة بما فعله بالنسبة لتقنية التنصت وتسجيل أحاديث تجري في مكان خاص وإضفاء المشروعية على ذلك الفعل طبقاً لما هو وارد بنص المادة 75 إجراءات جزائية، حيث أعطت المادة 75 للنيابة العامة بعد موافقة النائب العام سلطة الأمر بمراقبة المكالمات السلكية واللاسلكية أو إجراء تسجيل لأحاديث جرت في مكان خاص متى كان لذلك فائدة في تحقيق قائم.

ويلاحظ أن المشرع على الرغم من تجريمه لأفعال تسجيل الأحاديث والتقاط الصور في نص المادة 378 عقوبات اتحادي، وهو ما يعني التسوية في التجريم والعقاب بين التنصت السمعي والتنصت البصري، إلا أن المشرع الإجرائي قد فرق بينهما من حيث إجازة تسجيل الأحاديث التي تجري في مكان خاص بمعرفة قاضي التحقيق أو النيابة العامة وعدم الإشارة صراحةً إلى جواز والتقاط الصور أو التسجيل البصري للأحداث التي تدور في مكان خاص.

ولما كان صمت المشرع عن النص على جواز التقاط صور لوقائع تدور في مكان خاص سواء كان التصوير يتم عن طريق أجهزة التصوير التقليدية أم المستحدثة فإنه لا يجوز

(1) د/ حسام الأهواني: المرجع السابق، ص 207، د. سعيد جبر: المرجع السابق، ص55.

(2) Cass. Civ. 6 Janr. 1971. Dalloz 1976 . 263 .

تفسير صمت المشرع على أن قبول إباحة التصوير والتسجيل للأحداث التي تجري في مكان خاص من أجل الكشف عن الجريمة وتعقب مرتكبيها وذلك بالقياس على إباحة التسجيل لأحاديث تجرى في مكان خاص، الأمر الذي يعد استثناء تمليه ضرورة تحقيق المصلحة العامة.

إذ أن الاستثناء لا يجوز التوسع فيه أو القياس عليه، ومن ثم فإن التصوير لوقائع وأحداث تدور في مكان خاص هو إجراء غير مشروع ومن ثم يقع تحت طائلة قانون العقوبات لأن النص عام يستوي أن يكون مرتكب فعل الالتقاط شخصاً عاديًا أو موظفاً عامًا ممثل في قاضي تحقيق أو كممثل للنيابة العامة.

وترتيبًا على ذلك إذا ما جرى تصوير لوقائع تدور في مكان خاص سواء في مرحلة الاستدلال أو التحقيق الابتدائي وأسفر ذلك التصوير عن دليل، فإن الدليل المستمد من هذه التسجيلات المرئية يتسم بعدم المشروعية وبالتالي يكون باطلاً والبطلان في هذه الحالة متعلق بالنظام العام، ومن ثم يجوز إبداؤه والتمسك به في أي مرحلة تكون عليها الدعوى.

أما التصوير في مكان عام فهو على العكس من ذلك، إذ أن تواجد الشخص في مكان عام إنما يعد تنازلاً عن حقه في الاعتراض على الالتقاط وبالتالي لا يعد في تصويره مساساً بحرمة حياته الخاصة.

المبحث الثالث
التنظيم القانوني لاستخدام كاميرات المراقبة التليفزيونية في المراقبة الوقائية السابقة على ارتكاب الجريمة لأغراض منع الجريمة وملاحقة مرتكبيها

مَثَل استخدام كاميرات المراقبة التلفزيونية أحد مظاهر توظيف المعطيات التكنولوجية الحديثة في أغراض منع الجريمة والحد منها، فضلاً عن دورها الملموس في الآونة الأخيرة في تمكين سلطات البحث والتحري من الوصول لمرتكبي الجرائم بسهولة ويسر من خلال تعقب بصمة الوجه أو الحركة الجسدية، وأدى تعاظم الاستخدام الأمني والقانوني لهذه الكاميرات إلى قيام المشرعون في العديد من دول العالم إلى تبني تنظيمات قانونية تقنن الاستخدام القانوني لهذه التكنولوجيا في تحقيق أغراض الملاحقة الجنائية للجرائم ومرتكبيها، وفيما يلي سنتناول التنظيم القانوني لاستخدام كاميرات المراقبة التلفزيونية في أغراض المراقبة الوقائية السابقة على ارتكاب الجريمة في التشريعات المقارنة، وهو ما يقتضي تقسيم هذا المبحث لعدة مطالب على النحو التالي:

المطلب الأول: موقف التشريعات الوطنية والمقارنة من استخدام كاميرات المراقبة التليفزيونية في المراقبة التكنولوجية السابقة على ارتكاب الجريمة.

المطلب الثاني: شروط وإجراءات استخدام كاميرات المراقبة التليفزيونية في المراقبة التكنولوجية السابقة على ارتكاب الجريمة.

المطلب الأول
موقف التشريعات الوطنية والمقارنة من استخدام كاميرات المراقبة التليفزيونية في أغراض المراقبة التكنولوجية السابقة على ارتكاب الجريمة

فيما يتعلق بالمراقبة التليفزيونية، تبدو الأنظمة القانونية الثلاثة محل الدراسة متشابهة تمامًا. ومما ينبغي ملاحظته في هذا السياق أن المراقبة التليفزيونية قد بدأ استخدامها، في الأنظمة القانونية الثلاثة، من جانب المواطنين والشركات الخاصة، ثم اتسع نطاق المستخدمين لها ليشمل السلطات العامة (لاسيما السلطات المحلية)، من أجل أغراض تتعلق بوقاية النظام العام. وقد أدى استخدام هذه الوسيلة التكنولوجية من وسائل المراقبة إلى إثارة التساؤل بشأن ما إذا كان يمكن – وكيف يتم ذلك – استخدام مقاطع الفيديو المسجلة والصور الملتقطة بهذه الطريقة لأغراض التحقيق وأغراض الملاحقة الجنائية.

موقف المشرع الفرنسي:

ففي فرنسا، يُطلق على النظام القانوني الحالي للمراقبة التليفزيونية «حماية الفيديو» vidéo protection [1]. ويرد هذا النظام القانوني، بصورة أساسية، في تقنين الأمن الداخلي Code de la Sécurité Intérieure[2].

(1) Seee.g. Le Monde, 'Quand la 'vidé protection' remplace la'vidéo surveillance", 16 February 2010. Then, the Law 2011/LOPPSI 267 imposes the use of this term.

(2) E.g. E. Heilmann and P. Melchior, Vidéo - surveillance ou vidéo-protection?, Le choc des idées, Le Muscadier (Paris, 2012); A. Bauer and F. Freynet, Vidéosurveillance et vidéo protection, Que sais-je?,PUF (Paris, 2012); A. Bauer and C. Soullez, Les politiques publiques de sécurité, Que sais-je? PUF(Paris 2011); F. Ocqueteau, 'A comment on video - surveillance in France: regulation and impact on crime' (2001) 25(1 International journal (2/of comparative and applied criminal justice 103; N.C.Ahl, 'La vidéo -surveillance en trompe-l'oeil', Le Monde (29 October 2011); E. Heilmann, 'La vidéo surveillance, un mirage technologique et politique' in L. Mucchielli, La frénésie sécuritaire, La découverte (Paris, 2008); N. Le Blanc, 'Le bel avenir de la vidéosurveillance de voie publique' (2010)2(62) Mouvements 32; T Le Goff, 'Politique de securité: les chiffres et les images', (2010) 3 Esprit 90;C. Laval, 'Surveiller et prévenir' (2012) 2 Revue du MAUSS 47. Seealso the reports of the CNIL (Commission Nationale de l'Informatique et des Libertés).

ويوجد قسم بهذا التقنين يركز على حماية الفيديو عمومًا[1]. كما يوجد قسم آخر مخصص للحرب في مواجهة الإرهاب[2]. والحقيقة أنه منذ أن تم تبني هذه الوسيلة من وسائل المراقبة في النظام القانوني الفرنسي، بموجب القانون (1995/73) [3]، أضحت المراقبة التليفزيونية تكتسب أهمية خاصة، لاسيما لأغراض مواجهة الإرهاب باعتبارها وسيلة لجمع الأدلة في أعقاب ارتكاب الجريمة بالفعل[4].

كما سمح القانون رقم 2006/64 الصادر في 23 يناير 2006 بالمادة الأولى منه للعامة من أجل التأمين ضد الهجمات الإرهابية والحماية المباشرة للمباني الخاصة والشركات بوضع كاميرات للمراقبة تقوم بتسجيل الصورة والحدث ضد الهجمات الإرهابية والتفجيرات الناتجة عنها، وهذا الإجراء للأماكن المفتوحة للعامة لتأمين الأشخاص والأملاك التي تتعرض للسرقة والتفجيرات الإرهابية، وتوضع الكاميرات الخاصة بالمباني الخاصة خارج المبنى[5].

موقف المشرع الإيطالي:

وفي إيطاليا، أدت الحرب في مواجهة الإرهاب إلى إعادة تعريف وترتيب الأولويات والأهداف والأدوات من جانب السلطات العامة التي شجعت استخدام الوسائل التكنولوجية الحديثة. وقد أسفر ذلك عن استخدام واسع النطاق لأنظمة المراقبة التليفزيونية video sorveglianza لأغراض الوقاية من الجرائم بصفة عامة والجرائم الإرهابية بصفة خاصة. وقد جاءت هذه التطورات كرد فعل على القلق المتنامي لدى المواطنين وحاجتهم إلى الشعور بالأمن في مواجهة التهديدات الإرهابية المتصاعدة[6].

(1) (Articles L251(1) to L255(1.

(2) (Articles L223(1) to L223(9.

(3) 1995/Law 73.

(4) J. Pradel, Procédure pénale, 16th ed., Cujas (Paris 2011), p. 407.

(5) du 21 janvier 1995 D orientionet de programmation relative a la securite 73-Loi no 95.

وقد أضيفت المادة السابقة بمقتضى القانون:

L.n 2006 – 64 du 23 janv 2006, art 1er.

انظر في تناول هذه الإجراءات الاستثنائية التي أقرها هذا القانون:

(6) I sistemi di video sorveglianza 2, Video sorveglianza e privacy: quadronormativo, casistica e aspettitecnici, (Transcrime, Inforsicurezza (4 May 2006.

ولا يُسمح باستخدام أسلوب المراقبة التليفزيونية إلا في ظل توافر شروط معينة، وفي هذا السياق، يشار إلى أن استخدام المراقبة التليفزيونية في المجال العام، تحكمه قواعد خاصة لحماية البيانات تفصلها المادة (34) من تقنين حماية البيانات[1]، وكذلك قرار السلطة الإيطالية لحماية البيانات الصادر في 8 أبريل 2010[2]).

موقف المشرع الإنجليزي:

وفي المملكة المتحدة، يلاحظ اتجاه متزايد بوتيرة متسارعة نحو استخدام وسائل المراقبة التكنولوجية خلال الربع قرن الأخير. وليس من قبيل المبالغة القول إن المملكة المتحدة تعد رائدة على مستوى العالم في استخدام هذه الوسائل الحديثة[3]. وقد أدى الاستخدام الواسع للمراقبة عن طريق كاميرات الدوائر التليفزيونية المغلقة (Closed Circuit Television(CCTV)) في الأماكن العامة، لاسيما في لندن، إلى إثارة العديد من الأسئلة بشأن مدى انتهاك هذه الوسيلة للحق في الخصوصية. ولا توجد سوى قيود محدودة على استخدام هذه الكاميرات في الأماكن العامة[4]. ومما هو جدير بالملاحظة أنه لا يوجد نص تشريعي يتعلق بتنظيم المراقبة التليفزيونية، ولكن فقط مدونة للسلوك غير ملزمة a non-binding CCTV code of practice صادرة عن مكتب مفوض المعلومات the Information Commissioner's Office[5]). ومن ثم، فإن النصوص التي تتضمنها هذه المدونة لا تعد أن

(1) bearing the adoption of the Codice in material di protezione dei datipersonali 2003/Legislative Decree 196.

(2) Garante per la protezionedeidatipersonali, Provvedimento in material di video sorveglianza, G.U.99 (29 April 2010).

(3) EFUS, Citizens, Cities and video-surveillance, Towards a democratic and responsible use of CCTV, EFUS press (Paris, 2010) p. 14.

(4) On the United Kingdom regime, on CCTV cameras in relation to terrorism prevention: see e.g.Q.A.M. Eijkman and D. Weggemans, 'Visual surveillance and the prevention of terrorism: What about the checks and balances?', D. Fenwick, 'Terrorism, CCTV and the Freedom Bill 2011:Achieving compatibility with Article 8 ECHR?' and B. Sheldon, 'Camera surveillance within the UK: Enhancing public safety or a social threat?' in H. Fenwick, Developments in Counter-Terrorist Measures and Uses of Technology, Routledge (New York, 2012); D. Giannoulopoulos, 'La vidéo surveillance au Royaume-Uni. La camera omniprésente' (2010) 1 Archives de politique criminnelle 245.

(5) The Protection of Freedoms Act 2012 specifically requires the Secretary of State to prepare a code of practice containing guidance on the development of surveillance camera systems and the use of processing of images or other information obtained by virtue of such system. It also appoints a person as the Surveillance Camera Commissioner in order to encourage compliance with the surveillance camera code, review its operation and

تكون مجرد توصيات، وليست قواعد ملزمة قانوناً.

ولا تحتاج عمليات المراقبة التليفزيونية العامة General video-surveillance، التي تتم بطريقة كاميرات الدوائر التليفزيونية المغلقة، ترخيصاً أو إذناً للقيام بها في ظل قانون تنظيم سلطة التحقيق الصادر عام 2000. ومع ذلك، فإن عمليات المراقبة السرية والمخطط لها، التي تستهدف أشخاصاً معينين لأغراض التحري – عن طريق كاميرات الدوائر التليفزيونية المغلقة، تتطلب إذنًا للقيام بها. ومن ثم، فإن الجمهور يجب أن يكون على علم بأن مثل هذه الأنظمة مستخدمة، وأن استخدامها يخضع لقانون حماية البيانات الصادر عام 1998 the Data Protection Act ومدونة كاميرات الدوائر التليفزيونية المغلقة the CCTV Code of Practice.

موقف التشريعات العربية:

وفيما يتعلق بموقف التشريعات العربية فمن الملاحظ ندرة التنظيمات القانونية العربية فيما يتصل بتنظيم استخدام كاميرات المراقبة في المراقبة الوقائية لأغراض منع ارتكاب الجرائم، اللهم إلا تشريعين اثنين فقط، هما التشريع القطري رقم (9) لسنة 2011 بتنظيم استخدام كاميرات وأجهزة المراقبة الأمنية، والتشريع المحلي لإمارة دبي رقم 24 لسنة 2008 بشأن مقدمي الخدمات الأمنية ومستخدميها المعدل بالتشريع رقم 10 لسنة 2014، والذي ألزم جميع ملاك المجمعات السكنية بتركيب أنظمة مراقبة أمنية[1].

ومن جانبنا نرى عدم كفاية هذه التشريعات المحلية التي تم صياغتها في إطار أهداف مختلفة عن أعمال البحث والتحري واستقصاء الجرائم والبحث عن مرتكبيها. ولذا، نرى أنه من الأهمية بمكان قيام المشرع الوطني الاتحادي بإصدار قانون مستقل ينظم الاستخدام الأمني والقضائي لكاميرات المراقبة التلفزيونية المغلقة بما يحقق الاستفادة المثالية منها في أعمال البحث والتحري من ناحية وفي الملاحقة القضائية لمرتكبي الجريمة من ناحية أخرى.

(provide advice about the code (including changes to or breaches of its provisions.

(1) وتجدر الإشارة إلى أن إدارة نظم الحماية في شرطة دبي، قررت إنه تم حصر المباني التي سينطبق عليها القانون في دبي وبلغ عددها 25 ألف مبنى سكني، وأن دبي تتفوق على لندن، المعروف أنها من أكثر المدن إدارة للكاميرات على مستوى العالم.

المطلب الثاني
التنظيم القانوني لاستخدام المراقبة التليفزيونية في المراقبة السابقة على ارتكاب الجريمة

أغراض الوقاية من الجريمة :

فيما يتعلق بأسلوب المراقبة التليفزيونية بطريق كاميرات الدوائر التليفزيونية المغلقة، توجد عناصر ثلاثة تحتاج إلى إلقاء الضوء عليها لإظهار أوجه التشابه والاختلاف بين الأنظمة القانونية الثلاثة محل الدراسة. وتتمثل هذه العناصر في الجهات المسؤولة عن استخدام هذه الوسيلة الحديثة من وسائل المراقبة (الفرع الأول)، ونطاق استخدامها (الفرع الثاني)، والمدى الزمني لاستخدامها (الفرع الثالث).

الفرع الأول
الجهات ذات الصلة باستخدام أسلوب المراقبة التليفزيونية

في كل من فرنسا والمملكة المتحدة، يُناط الإذن بتركيب واستخدام كاميرات المراقبة التليفزيونية بسلطة إدارية. ويبدو هذا الوضع على النقيض مما هو مأخوذ به في إيطاليا.

أولاً: الجهات ذات الصلة باستخدام المراقبة التليفزيونية في النظام الإجرائي الفرنسي:

في فرنسا، يمكن الترخيص باستخدام أسلوب المراقبة التليفزيونية، أوما يُطلق عليها حماية الفيديو لضمان الأمن، لاسيما عندما تتعرض الأماكن والمنشآت لمخاطرالاعتداء والسرقة، وذلك شريطة ألا تسجل هذه الكاميرات التليفزيونية مابداخل المنشآت والمباني الخاصة، ولا مداخل هذه المنشآت والمباني[1]. فإذا ما أتاحت مقاطع الفيديو أو الصور التي التقطتها هذه الكاميرات التعرف على شخص معين، فإن استخدام هذه الصور يجب أن يكون متسقًا مع نصوص القانون رقم (1978/17) (وهو القانون الخاص بحماية قواعد البيانات).

(1) Article L251(3) CSI.

ويتطلب الإجراء السابق صدور إذن من المحافظ Préfet. وله أن يصدر هذا الإذن بقرار arrêté préfectoral في أي وقت، بعد استشارة اللجنة الإقليمية Commission départementale التي يُناط بها حماية البيانات الشخصية بما يتفق مع الحق في الخصوصية[1]. وتأمر هذه اللجنة باتخاذ كل الاحتياطات الضرورية، لاسيما فيما يتعلق بالأشخاص الذين يتاح لهم استغلال نظام حماية الفيديو أو المراقبة التليفزيونية أو الاطلاع على الصور الناتجة عن استخدام هذا الأسلوب[2].

وتجدر الإشارة إلى أن الإذن بالمراقبة التليفزيونية يُمنح لطوائف معينة من الأشخاص – محددة بالنسبة لكل حالة معينة – وهم عمال الشرطة ورجال الدرك gendarmerie. ويجب أن يتضمن الترخيص تحديداً لطريقة نقل الصور ومدة الاحتفاظ بها. وتعطي اللجنة الوطنية لحماية الفيديو رأيها بشأن استخدام مثل هذه الوسيلة التكنولوجية، إذا كانت هذه الكاميرات تُستخدم في مراقبة وتسجيل الطرق العامة أو الأماكن أو المباني المفتوحة للعامة[3].

ومع ذلك، يمكن لممثل الدولة على المستوى المحلي ومحافظ البوليس Préfet de Policeعلى مستوى باريس أن يأمروا، لأغراض منع الأعمال الإرهابية، بتطبيق أنظمة حماية الفيديو، وأن يأذنوا، أيضاً، لطائفة أوسع من الأفراد أن يطلعوا ويستخدموا الصور الناتجة عن المراقبة بهذه الوسيلة[4].

وفي الحالات العاجلة، وبصفة خاصة في ظل مخاطر التعرض للأعمال الإرهابية، يمكن لممثل الدولة على المستوى المحلي ومحافظ البوليس على مستوى باريس أن يصدرا دون إخطار مسبق للجنة الوطنية لحماية الفيديو Commission départementale de vidéo protection، ترخيصاً أوإذناً مؤقتاً بتركيب أنظمة الحماية عن طريق الفيديو a video-protection system. وبعد ذلك، يتم إخطار رئيس اللجنة المذكورة بهذا الترخيص، ومن ثم

(1) Article L252(2) and L 252(3) CSI.

(2) Article L 252(1).

(3) has a mission of 267/Article L 251(4) CSI; the Commission nationale de video protection created by Law 2011 advice and evaluation of the effectiveness of video-protection at the level of the Ministry of Interior.

(4) Article L 223(2) CSI;seealso J.-P. Courtois and C. Gautier, Rapport d'information sur la vidéo surveillance, Sénat, n° 131, 10 December 2008.

يمكن للجنة أن تبدي رأيها بشأن هذا الترخيص[1]. وهنا يجب ملاحظة أنه على الرغم من وجود التزام بفك وإزالة أدوات المراقبة التليفزيونية في أعقاب إصدار اللجنة لرأي سلبي بشأن هذه المراقبة[2]، فليس ثمة نص قانوني يلزم بالإتلاف التلقائي للبيانات التي تم جمعها أثناء فترة المراقبة. ومن ثم، فإن تدمير أو إتلاف البيانات التي تم جمعها غير ممكن إلا بناءً على طلب من الطرف أو الأطراف المتأثرة بهذه البيانات، وبعد صدور قرار قضائي بهذا المعنى[3].

ومن أجل التوفيق بين الاعتبارات الأمنية والحق في الخصوصية، اقتُرح إنشاء لجان للأخلاقيات ethics committees. وقد أنشئت هيئة خصيصاً لتحقيق هذا الغرض يُناط بها الإشراف على أنظمة الحماية بطريقة الفيديو في بعض المدن الفرنسية مثل Lyon، Le Havre. والهدف الأساسي لمثل هذه اللجنة هو ضمان احترام الحريات[4].

ولأغراض التحقيق، يمكن لضابط الشرطة أن يحصل على إذن بالوصول إلى المعلومات التي تم جمعها بطريق حماية الفيديو من خلال أمر قضائي عادي من جهة الادعاء أو من القاضي استنادًا إلى نصوص خاصة. ومعنى ذلك، فإن المعلومات التي تم جمعها في بادئ الأمر في ظل ترخيص إداري ودون خضوع لأي رقابة يمكن، بعد ذلك، الاستعانة بها لأغراض التحقيق استنادًا إلى مجرد طلب قضائي عادي دون مزيد من الفحص بشأن كيفية جمع مثل هذه المعلومات، فهل يبدو هذا الوضع مقبولاً؟.

ثانياً: الجهات ذات الصلة باستخدام المراقبة التليفزيونية في النظام الإجرائي الإنجليزي:

وفي المملكة المتحدة، استخدمت كاميرات المراقبة عن طريق الدوائر التليفزيونية المغلقة بهدف مواجهة الجرائم التي تحدث في الشوارع ومحلات التسوق الكبيرة (المولات). وهذه الوسيلة من وسائل المراقبة، التي استخدمت في بادئ الأمر على المستوى المحلي، أضحت مع مرور الوقت سياسة وطنية. ومن ثم، ظهرت الحاجة للتنسيق بين الأنشطة

(1) Article L223(4) and L223(5) CSI.

(2) Article L 223(4) and also 253(6) CSI.

(3) Article L 253(5) CSI.

(4) EFUS, Citizens, Cities and video surveillance, pp.141–142.

الوطنية في هذا المجال وتشجيع المشاركة في المعلومات[1]. ولم يُنظر إلى كاميرات المراقبة التليفزيونية باعتبارها من وسائل المراقبة السرية. ومن ثم، فإن هذه الوسيلة من وسائل المراقبة لم تُعامل باعتبارها تشكل تدخلاً، ولا مراقبة موجهة (directed surveillance[2])، وذلك ما لم ينصب تركيز هذه الكاميرات على مجموعة معينة من الناس أو على فرد بعينه، ومن ثم تسجل حركة وأنشطة فرد خاص. واستناداً إلى النظرة السابقة إلى كاميرات المراقبة التليفزيونية، فإن استخدامها بالضوابط السابقة لا يحتاج إلى ترخيص أو إذن في ظل الفصل الثاني من قانون تنظيم سلطة التحقيق الصادر في عام 2000.

وفي حالة استخدام كاميرات المراقبة التليفزيونية كأداة من أدوات تطبيق القانون أو كوسيلة من وسائل جمع الأدلة، فيجب الحصول على ترخيص أو إذن مسبق بهذا الاستخدام[3]. ويجب أن يتضمن مثل هذا الإذن تحديدًا دقيقًا لما هو مأذون به، وكيفية إجراء المراقبة (على سبيل المثال تحديد أي نوع من الكاميرات سيتم استخدامه) وتحديداً للنشاط الذي سيخضع للمراقبة، ومن ثم تسجيله على الأشرطة. ويجب أن يأخذ الضباط المأذون لهم بإجراء هذه المراقبة في اعتبارهم عدم المساس أو التدخل في خصوصية أشخاص آخرين غير خاضعين للتحقيق والتحري.

ثالثاً: الجهات ذات الصلة باستخدام المراقبة التليفزيونية في النظام الإجرائي الإيطالي:

في إيطاليا، يمكن للسلطات المحلية، منذ دخول القانون (2009/38) حيز النفاذ استخدام أنظمة المراقبة التليفزيونية من أجل ضمان الأمن في الأماكن العامة[4]، لأغراض وقاية النظام العام.

ويُناط بالشرطة المحلية تركيب كاميرات المراقبة التليفزيونية، مستعينة في ذلك بفنيين من شركات خاصة، وبمشورة الشرطة الوطنية. وتسهر الشرطة الوطنية والشرطة

(1) Ibid., pp. 184–185.

(2) S. 26(2)(a)/1(2)(a) RIPA 2000, defining directed surveillance.

(3) This authorisation is given by the organisation operating the CCTV system. They have discretion to refuse any request unless there is an overriding legal obligation such as a court order or information access rights. See ICO, CCTV code of conduct, Data protection, 2008, p. 13.

(4) Law 38 (2009/Article 6(7).

المحلية والشرطة شبه العسكرية Carabinieri على التحكم في هذه الكاميرات. وعندما يتم إرسال الصور إلى المراكز الرئيسة للشرطة الوطنية، فإنه يكون بمقدورهم الاطلاع على الصور المرسلة من جميع الكاميرات، وكذلك التحكم في هذه الكاميرات عن بعد. ويقصر القانون اختيار مشغلي هذه الكاميرات على ضباط الشرطة القضائية.

وفي مركز العمليات الرئيسي للمراقبة التليفزيونية التابع للشرطة المحلية، ينهض بالعمل ثلاثة من الضباط لفترات ثلاثة متتابعة لضمان استمرار المتابعة لمدة 24 ساعة في كل يوم. وفي المراكز الرئيسة للشرطة الوطنية، يتواجد على مدار الأربع وعشرين ساعة في كل يوم أحد مفتشي الشرطة الوطنية واثنان من المساعدين.

ويبين، مما سبق، أن الصور التي يتم التقاطها بطريقة المراقبة التليفزيونية يتم إرسالها، بصورة متزامنة، إلى المراكز الرئيسة للشرطة الوطنية والشرطة المحلية على حد سواء. وبعد ذلك، يمكن للمراكز الرئيسة للشرطة الوطنية أن ترسل الصور إلى السلطات القضائية باعتبارها من قبيل الأدلة. وبإيجاز، يمكن القول أن إثنا عشر فردًا من المشتغلين من الشرطة الوطنية والشرطة المحلية والشرطة شبه العسكرية Carabinieri بمقدورهم الاطلاع على الصور، ولا يمكن مشاركة هذه الصور، في ذات الوقت، مع الجهات الأخرى. وليس بمقدور أحد، سوى العاملين بالشرطة القضائية، الوصول إلى أو الاطلاع على الصور المخزنة. وحتى هؤلاء العاملين بالشرطة القضائية لا يجوز لهم الاطلاع على هذه الصور المخزنة إلا بناءً على إذن يصدر من القاضي. وللاطلاع على هذه الصور، يُتطلب، ليس فقط الحصول على إذن من القاضي، ولكن أيضًا مفتاح. ولا يستطيع الدخول على المواد المسجلة سوى مدير النظام، ومن خلال استخدام مفتاح معين مخصص لهذا الغرض.

الفرع الثاني
النطاق الموضوعي لاستخدام المراقبة التليفزيونية

يمكن القول أن نطاق استخدام الوسائل التكنولوجية للمراقبة التليفزيونية، في الدول الثلاث محل الدراسة، هو منع الجريمة، وإن كانت هذه التشريعات لا تمانع كقاعدة من استخدام نتائجها فيما بعد في إجراءات الملاحقة الجنائية.

أولاً: النطاق الموضوعي لاستخدام المراقبة التليفزيونية في النظام الإجرائي الفرنسي:

في فرنسا، تم تصميم نظام الحماية بطريق الفيديو أو المراقبة التليفزيونية لتسجيل ما يحدث في الأماكن العامة بغرض أساسي يتمثل في منع الجرائم، سواء أكانت هذه الجرائم من الجرائم الخطيرة أو الجرائم الأقل خطورة[1]. كما تُستخدم هذه الوسيلة أيضًا لجمع التحريات عن أي نوع من أنواع الجرائم، سواء أكانت خطيرة أو غير خطيرة.

وقد أعلنت الحكومة الفرنسية أن نظام حماية الفيديو أوالمراقبة التليفزيونية مكون أساسي في سياسات الأمن في المدن. وإذا كان نظام حماية الفيديو قد طُور، بحسب الأصل، لمواجهة الجرائم العادية[2]، فإن السياقات الحديثة لمكافحة الإرهاب قد قدمت مسوغات إضافية لزيادة استخدام هذا الأسلوب الحديث من أساليب المراقبة. وقد تقدم القول بأنه توجد نصوص خاصة، بل في الحقيقة قسم مستقل يتعلق بالمراقبة التليفزيونية من أجل منع الجرائم الإرهابية والتحري عنها بعد وقوعها. ويلاحظ أن هذه النصوص الاستثنائية تمنح مزيدًا من السلطات وهامشًا أوسع من السلطة التقديرية[3]، سواء للسلطات المختصة بمنح الإذن باستخدام هذه الوسيلة أو السلطات التنفيذية المختصة بمباشرتها – والحقيقة أنه توجد ظروف كثيرة تسوغ تركيب واستخدام عدد متزايد من كاميرات المراقبة التليفزيونية مع مرور الوقت.

وينتقد بعض الكتاب عدم وجود نص يحدد جرائم معنية تسوغ اللجوء إلى هذا الأسلوب من أساليب المراقبة. وقد تقدم القول بأن نقل وتسجيل الصور المجمعة من خلال هذه الوسيلة يختلف تبعاً لعدد من الظروف بما في ذلك السياق الجنائي. كما أن مستوى السلطات المخولة للجهات ذات الصلة بالمراقبة التليفزيونية يعتمد على نوع الجرائم المراد منعها أو التحري عنها. ويقدم الإرهاب مسوغًا لتوسيع المجال الخاضع للمراقبة ليشمل النطاق المباشر المحيط بالأبنية والأماكن التي يُحتمل تعرضها لمخاطر الأنشطة الإرهابية[4].

(1) 125 Law 1995/as amended by Ordonnance 351 2012.

(2) 73 Law 1995/Art.4 .Priority tasks of the police are for example the fight against urban violence and the control of public order.

(3) E.g. the Préfet may authorise an installation before the commission has given its opinion.

(4) Article L223–1 and Article 223–2 CSI.

ويبين، من ذلك، أن المراقبة التليفزيونية يمكن استخدامها في الظروف الاستثنائية، وفي ظل توافر شروط مشددة.

ثانياً: النطاق الموضوعي لاستخدام المراقبة التليفزيونية في النظام الإجرائي الإيطالي:

وفي إيطاليا، يستهدف استخدام الكاميرات التليفزيونية أغراضًا متعددة. ويمكن تصنيف هذه الكاميرات إلى طوائف مختلفة تتمثل فيما يلي:

1. حماية تكامل الأفراد بما في ذلك الأمن في المدن، والنظام العام، ووقاية الهيئات العامة، وللكشف عن الجرائم أو منعها، وتيسير وتحسين الخدمات المتاحة للجمهور من أجل تعزيز أمن المستخدمين أو المنتفعين.
2. حماية الملكية.
3. كشف ومنع ومراقبة المخالفات القانونية.
4. جمع الأدلة[1].

وكما هو الحال في الدول الأخرى، انتشر استخدام أسلوب المراقبة التليفزيونية انتشارًا سريعاً في وسائل النقل في المدن[2]، وذلك لمواجهة التهديدات الإرهابية المتصاعدة[3]. وإذا كان الهدف الأساسي لوضع كاميرات المراقبة التليفزيونية هو منع الجرائم الصغيرة، فقد اتسع هذا الهدف في الوقت الحاضر ليشمل جمع المعلومات بغرض الوقاية من الجرائم الأكثر خطورة، بما في ذلك الجرائم الإرهابية[4].

ويبدو الجانب الوقائي لأسلوب المراقبة التليفزيونية أقل وضوحاً. ومع ذلك، فإن رضا المواطنين عن هذا الأسلوب يبدو مرتفعاً، حتى وإن كان هذا النظام لا يحقق جميع التوقعات المعقودة عليه، وتفسير ذلك، أن المراقبة التليفزيونية تولد شعورًا لدى المواطنين بأنهم يحظون بدرجة أعلى من الحماية، وأن استخدام هذا الأسلوب سيعزز احتمال الاستجابة

(1) (Garante per la Protezione dei datipersonali, Video surveillance, Decision (8 April 2010.

(2) وتجدر الإشارة إلى أن وسائل المراقبة التليفزيونية تم تركيبها في بادئ الأمر في وسائل الموصلات العامة.

(3) I sistemi di videosorveglianza 2, p. 49.

(4) F. Caprioli, 'Nuovamente al vagliodella Corte Costituzionale l'usoinvestigati vedeglistrumenti diripresavisiva' (2008) 3 Giur Cost 1832.

السريعة من جانب الشرطة. وتشير بعض الدراسات إلى أن الرسالة التي يحملها أسلوب المراقبة التليفزيونية هي أن رقابة تليفزيونية أكبر تقود إلى مستوى أعلى من منع الجرائم، ومن ثم تخفيض مستوى الظاهرة الإجرامية 'video-surveillance = + prevention of offences = -criminality'[1].

ثالثاً: النطاق الموضوعي لاستخدام المراقبة التليفزيونية في النظام الإجرائي الانجليزي:

وفي المملكة المتحدة، يُستخدم أسلوب المراقبة التليفزيونية لتحقيق أغراض متعددة أبرزها الأغراض الرقابية، لاسيما تلك المتعلقة بالاعتبارات الأمنية. ويسود الشعور بأن التطور السريع لكاميرات المراقبة التليفزيونية يمثل تقدماً كبيراً في مجال الوقاية من الجرائم. ويشكل هذا الأسلوب الرقابي جزءًا مهمًا من استراتيجية منع الجرائم في المملكة المتحدة، كما تستخدم المعلومات الناتجة عن استخدام هذا الأسلوب كدليل في المحاكمات وفي التعرف على هوية المتهمين[2].

كما يمكن أن تكون لهذا الأسلوب فوائد أخرى تتعلق بالردع والأمان، وإن كانت هذه الفوائد محل جدل بين الكتاب[3]. ومع ذلك، فإن التنافس السريع لاستخدام هذه الكاميرات، والاستخدام الواسع للمعلومات التي يتم جمعها بهذه الطريقة في أغراض التحري والتحقيق يمثلان تآكلاً للحريات المدنية.

الفرع الثالث
النطاق الزمني لاستخدام كاميرات المراقبة التليفزيونية
ثمة مسألتان على درجة كبيرة من الأهمية في هذا السياق.

الأولى: ما هي المدة التي يستمر خلالها الترخيص أو الإذن الصادر من السلطة المختصة باستخدام أسلوب المراقبة التليفزيونية؟.

(1) See I sistemi di video sorveglianza 2, p. 11.

(2) Unlike the interception of telecommunications, which can not beused as evidenceat trial.

(3) See e.g. A. Bauer and F. Freynet, Vidéosurveillance et vidéo protection PUF (Paris, 2008); V. Carli,'Assessing CCTV as an effective safety and management tool for crime-solving, prevention and reduction', International Centre for the Prevention of Crime (Montreal, December 2008); CCTV,Politics.co.uk: www.politics.co.uk/reference/cctv (accessed on 5 August 2013).

والثانية: ما هي المدة التي يمكن خلالها الاحتفاظ بالمعلومات التي تم جمعها من خلال هذا الطريق؟.

وفيما يتعلق بمدة تركيب أو استخدام كاميرات المراقبة التليفزيونية، في فرنسا، تستمر مدة تركيب أو استخدام كاميرات المراقبة التليفزيونية لفترة زمنية محددة. وتتمثل هذه المدة في خمس سنوات قابلة للتجديد. وعلى النقيض من ذلك، لا يوجد في إيطاليا والمملكة المتحدة أي قيد زمني على مدة تركيب أو استخدام هذه الكاميرات. ومعنى ذلك، أنه ليس ثمة حاجة لتقديم طلب لتجديد الترخيص أو الإذن باستخدام هذا الأسلوب.

وفيما يتعلق بالمدة التي يمكن الاحتفاظ خلالها بالمعلومات التي يتم جمعها من خلال كاميرات المراقبة التليفزيونية، فإن الأمر يتفاوت تفاوتًا كبيرًا بين الدول الأعضاء في الاتحاد الأوربي. ففي الدول الثلاث مدخل الدراسة، يمكن الاحتفاظ بهذه المعلومات إلى أن يصبح ذلك غير ضروري. بيد أن هذا المعيار يبدو غامضاً إلى درجة كبيرة. ولذلك، تفضل دول أخرى تحديد فترات زمنية محددة.

وفي فرنسا، يحدد الترخيص أو الإذن مدة حيازة الصور بشهر واحد في أعقاب نقل هذه الصور أو الاطلاع عليها، وذلك بغض النظر عن مدى ضرورة الاحتفاظ بها لأغراض الإجراءات الجنائية[1]. وفيما عدا حالة التحقيق في الجريمة المتلبس بها flagrante delicto، والتحقيق الابتدائي a preliminary investigation، والمعلومات القضائية Information judiciaire لا يجوز أن يتجاوز الاحتفاظ بالصور مدة الشهر[2]. وفي حالة ما إذا كانت شروط الاستعجال والتعرض لمخاطر الأعمال الإرهابية، متوافرة، فإن تركيب كاميرات المراقبة التليفزيونية (نظام حماية الفيديو) يكون لأربعة أشهر[3]. وهذه المدة قابلة للتجديد بعد استشارة اللجنة الإقليمية لحماية الفيديو[4] (Commission départementale de vidéo protection).

وفي إيطاليا، فيما يتعلق بكاميرات المراقبة التليفزيونية التي تقوم السلطات المحلية

(1) Article L252-3 CSI.

(2) Article L252-5 CSI.

(3) Article L223-4 CSI.

(4) Article L223-5 CSI.

بتركيبها لأغراض النظام العام، فإن الشرطة المحلية والوطنية بمقدورها الاطلاع على الصور المشفرة والاحتفاظ بها لمدة سبعة أيام حتى إتلافها، وذلك ما لم تكن ثمة حاجة للمعلومات الموجودة في هذه الصور، مما يبرر تخزينها لمدة أطول[1]. ومع ذلك، فإن هذه المدة يمكن مدها في الأماكن التي تكون عرضة بصورة خاصة للتهديدات الإرهابية، حتى ثلاثين يومًا[2]. أما في الحالة التي يتم فيها تركيب كاميرات المراقبة التليفزيونية بمعرفة جهات خاصة، كالأفراد والشركات، لأغراض أخرى لا تتعلق بالنظام العام، فإن الصور لا يمكن الاحتفاظ بها لمدة تجاوز أربعًا وعشرين ساعة.

وأخيراً، في المملكة المتحدة لم ترد إشارة إلى المدة التي يمكن الاحتفاظ بالصور خلالها سوى في أداة غير تشريعية (مدونة للسلوك a code of practice). ومن ثم، فإن هذه الأداة ليس لها قوة قانونية ملزمة، ولا تعدو أن تكون مجرد توصية. ومع ذلك، فإن الإشارة إلى المدة في هذه التوصية تبدو بالغة الغموض: «لا يجوز لك الاحتفاظ بالصور لمدة تجاوز ما هو ضروري، بصورة صارمة، لتحقيق أغراضك من تسجيل هذه الصورة. وفي حالة ما إذا كانت هناك ثمة حاجة للاحتفاظ بهذه الصور لمدة تزيد على ذلك...»[3]. وثمة إشارة أخرى إلى المدة التي يمكن خلالها الاحتفاظ بالصور: «الصور التي يتم الحصول عليها عن طريق نظام مركز المدينة يمكن الاحتفاظ بها للوقت الكافي بما يسمح للجرائم أن تظهر إلى دائرة الضوء، لمدة شهر على سبيل المثال، وفي جميع الأحوال، فإن المدة التي يُحتفظ بالصور خلالها يجب أن تكون، أقصر ما يمكن، وذلك استنادًا إلى خبرتك»[4]. غير أنه بالنظر إلى أثر الاحتفاظ بالبيانات الشخصية – لاسيما الاحتفاظ بالصور – على الحق في الخصوصية، فإن عدم وجود نص تشريعي ملزم يحدد المدة التي يمكن الاحتفاظ بالصور خلالها يبدو غير مقبول على الإطلاق.

(1) 2009/Article 6(8), Law 38.

(2) Garante per la protezione dei datipersnali, Prescrizioni per la video sorveglianza presso i sitidiinteresse culturale maggiormenteesposti alla minacciaterroristica(12 March 2009).

(3) ”y]ou should not keep images for longer than strictly necessary to meet your own purposes for recording] them. On occasion, you may need to retain images for a longer period, where a law enforcement body is investi gating a crime, to give them opportunity to view the images as part of an active investigation”.CCTV code of practice, Data protection, Information Commissioner’s Office (revised. 2008), p. 14.

(4) Ibid.

المبحث الرابع
القيمة القانونية لتسجيلات كاميرات المراقبة التلفزيونية المغلقة (CCTV)

يثار التساؤل حول القيمة القانونية للتسجيلات التي تتم بواسطة كاميرات المراقبة التلفزيونية المغلقة CCTV، وما مدى مشروعية استخدامها في الإثبات الجنائي، وهل من الممكن الاستناد إليها كدليل إثبات في مرحلتي التحقيق والاتهام والمحاكمة أم أنها لا ترقى لمرتبة الدليل، وتقتصر مجالات الاستفادة منها على الأغراض الأمنية فقط دون غيرها من أغراض الملاحقة الجنائية؟.

وتجدر الإشارة في هذا المقام إلى أنه لا خلاف حول جواز الاستناد لنتائج المراقبة السابقة على ارتكاب الجريمة بواسطة كاميرات المراقبة التلفزيونية المغلقة، حيث أجازت التشريعات الإجرائية المقارنة التي نظمت استخدام كاميرات المراقبة التلفزيونية في أعمال الوقاية والحد من الجريمة وحماية الأشخاص والأموال والممتلكات، استخدام نتائجها في الإثبات الجنائي، وهو أيضاً ما اتجه إليه القضاء المصري في هذا الشأن[1]، وعلى ذلك فالمشكلة تتلخص في مدى جواز استخدام نتائج المراقبة السابقة على ارتكاب الجريمة للمكالمات والمحادثات والشخصية في إجراءات الملاحقة الجنائية القضائية للمتهمين.

وننوه في هذا الصدد أنه لا يقصد هنا بمشروعية الإثبات بنتائج المراقبة السابقة على ارتكاب الجريمة أن يكون الدليل الناتج عنها منصوصاً عليه قانوناً كما هو الحال في نظام الأدلة القانونية، فليس المقصود حقيقة أن مبدأ الشرعية الجنائية يقتصر على مجرد التوافق مع أحكام القاعدة القانونية المكتوبة[2]، وإنما المقصود من الناحية الفعلية هو شرعية الإثبات (Licéité de la preuve[3]،

(1) انظر على سبيل المثال حكم محكمة جنايات القاهرة في الجناية رقم..... وكذلك حكم محكمة النقض في الطعن رقم - قضية مقتل السيدة سوزان تميم- حيث استندت المحكمة في التدليل على إدانتها للمتهم على التسجيلات الناتجة عن كاميرات المراقبة التلفزيونية.

(2) د. محمد نعيم فرحات: النظرية العامة لعذر تجاوز حق الدفاع الشرعي، رسالة دكتوراه، 1981، ص 155 وما بعدها.

(3) انظر حول مشروعية الدليل في المواد الجنائية بصفة عامة: د. أحمد ضياء الدين محمد خليل: مشروعية الدليل في المواد الجنائية، دراسة تحليلية مقارنة لنظريتي الإثبات والمشروعية في مجال الإجراءات الجنائية، دار النهضة العربية، 2010.

وهذا المبدأ يعني أن تتم إدارة الأدلة (L'administration des preuves[1])بالبحث عنها والحصول عليها بطريقة مشروعة أي مطابقة للقواعد القانونية، فيجب طبقاً لمبدأ مشروعية الإثبات أن يتفق الإجراء الذي تم في إطاره الحصول على الدليل مع القواعد القانونية والأنظمة الثابتة في وجدان المجتمع المتحضر[2]، وذلك لأن القانون هو الذي يحدد القواعد التي تحكم الحصول على الدليل، ومن أهم هذه القواعد احترام الحياة الخاصة بكل عناصرها، احترام الحرية، وعدم تجاوز القواعد القانونية فيما يخص القيام ببعض الإجراءات القانونية من الناحية الفنية كالإجراءات الخاصة بالقبض والتفتيش، كما يجب مراعاة إعلانات حقوق الإنسان والمواثيق والاتفاقات الدولية وقواعد النظام العام وحسن الآداب السائدة في المجتمع، بالإضافة إلى المبادئ التي استقرت عليها محكمة النقض. فهذه القواعد هي التي تسمح للقاضي باستبعاد الأدلة التي يتم الحصول عليها بالمخالفة لقواعد القانون الموضوعية أو الإجرائية[3].

MERLE R. et VITU A., Traité de droit criminel, t. II, Procédure pénale, Cujas, 5e éd. 2001, n° 168, p. 211 ; J. (1) PRADEL, Procédure pénale, op. cit., n° 408. – S. GUINCHARD et J. BUISSON, Procédure pénale, Litec, 6e éd. .2010, n° 551

(2) د. أحمد فتحي سرور: الشرعية والإجراءات الجنائية، دار النهضة العربية، 1977، ص 105-106، وتجدر الإشارة إلى أن لقاعدة استبعاد الأدلة غير المشروعة في الفقه المقارن أهمية متفاوتة: ففي الوقت الذي أكد فيه تيار فقهي على أهمية المشروعية والنزاهة في تحصيل الدليل من حيث المبدأ، إلا أنه لا يتوقف كثيراً عند المبررات النظرية والعملية التي تقف وراء استبعاد الأدلة المتحصلة بالمخالفة لذلك المبدأ ، في حين يذهب رأي أخر إلى تحديد موقفه من القاعدة في ضوء ما يعتنقه من أفكار تدعم الاستبعاد أو تناهضه. انظر في ذلك تفصيلاً: د. أحمد عوض بلال: قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، دار النهضة العربية، الطبعة الثالثة 2013، ص 153. ويرى سيادته أن الجدل الفقهي في هذا الصدد يكشف بدوره عن تباين النظرة إلى وظيفة المحكمة الجنائية، فمن ناحية، ثمة رأي ينظر إلى المحكمة الجنائية باعتبارها هادفة فحسب إلى التحقق من التهمة المنسوبة، وعلى ذلك فإن قبول الدليل أو استبعاده يتعين أن يكون محكوماً بهذا الاعتبار وحده: فكل ما يلزم لقبول الدليل هو ما إذا كان بلغ درجة كافية من الجدية للتعويل عليه reliable ومن أجل هذا يندرج ذلك التحليل تحت ما يعرف بمبدأ كفاية التعويل .reliability principleومن ناحية ثانية، ثمة تحليل آخر يطلق عليه مبدأ الوظيفة التأديبية disciplinary principle ، ومؤداه أنه يتعين على المحكمة استبعاد الأدلة المتحصلة بطرق غير مشروعة حتى ولو كان التعويل عليها متحققاً، لأن من وظائف المحكمة استعمال سلطتها من أجل محاربة الوسائل غير المشروعة في الكشف عن الجرائم. ومن ناحية ثالثة، ثمة تحليل توفيقي يطلق عليه مبدأ الحماية protective principle لا يقوم على حتمية استبعاد كافة الأدلة المتحصلة بطرق غير مشروعة: فهذا النوع من الاستبعاد ليس سوى صورة واحدة من أربع تحقق الحماية بدرجات متفاوتة، والصور الأخرى هي؛ استحداث دفع بعدم المسؤولية، استبعاد الدليل وفقاً للسلطة التقديرية للمحكمة، وتخفيف العقاب. ويقوم هذا التحليل على أن الاستبعاد التقديري هو أفضل تلك الوسائل قاطبة في تحقيق الحماية.

(3) وتجدر الإشارة إلى أن مبدأ مشروعية الإثبات هو مبدأ مقرر في المسائل المدنية كما هو بالنسبة للمسائل الجنائية. ومما هو جدير بالذكر أن المشروعية ليست بشرط واجب في دليل البراءة، ذلك لأنه من المبادئ الأساسية في الإجراءات الجنائية أن كل متهم يتمتع بقرينة البراءة إلى أن يحكم بإدانته بحكم نهائي، وهذا ما أكدته محكمة النقض المصرية بقولها «من المقرر أنه وإن كان يشترط في أدلة الإدانة أن تكون مشروعة، إذا لا يجوز أن تبنى إدانة صحيحة على دليل باطل قانوناً، إلا أن المشروعية ليست بشرط واجب في دليل البراءة، ذلك أنه من المبادئ الأساسية في الإجراءات الجنائية، أن كل متهم يتمتع بقرينة البراءة إلى أن يحكم بإدانته بحكم نهائي وأنه إلى أن يصدر هذا الحكم، له الحرية الكاملة في اختيار وسائل دفاعه بقدر ما يسعفه مركزه في الدعوى وما يحيط به من عوامل الخوف والحرص والحذر

ولا تقتصر مشروعية دليل الإدانة على مجرد الاتفاق مع القاعدة القانونية المكتوبة أو المنصوص عليها، وإنما يجب أن يتعدى ذلك إلى النظام القانوني في مجمله بما يشمل مبدأ الأمانة (Le Principe de la loyauté[1])، وهذا يعني أن أي دليل يتم الحصول عليه بطريقة غير مشروعة أو بوسيلة مخالفة للقانون لا تكون له قيمة في الإثبات. فلا يجوز للقاضي أن يستند على دليل تم الحصول عليه من استجواب جرى بطريقة مخالفة للقانون، أو دليل استمد من محرر مسروق، أو عن طريق استراق السمع، أو عن طريق تسجيل الحديث خلسة. كما لا يجوز للقاضي أن يؤسس عقيدته على دليل تم ضبطه نتيجة قبض غير مشروع، أو كان وليد إجراء تفتيش باطل، أو اعتراف باطل أو وليد إكراه، أو كان نتيجة خلق لحالة تلبس من قبل مأمور الضبط القضائي.

وعلى ذلك يقتضي الوقوف على القيمة القانونية لنتائج المراقبة السابقة على ارتكاب الجريمة استعراض موقف كل من النظام الإجرائي المصري من نتائج هذه المراقبة ثم استعراض قيمتها في النظم الإجرائية المقارنة.

وغيرها من العوارض الطبيعية التي تعتري النفس البشرية، وقد قام على هدي هذه المبادئ حق المتهم في الدفاع عن نفسه وأصبح حقاً مقدساً يعلو على حقوق الهيئة الاجتماعية التي لا يضيرها تبرئة مذنب بقدر ما يؤذيها ويؤذي العدالة معاً إدانة برئ»، وحق المتهم في الصمت Droit de silence دون أن يفسر ذلك كدليل ضده. راجع في هذا الصدد؛ نقض 31 يناير 1967، مجموعة أحكام محكمة النقض، س 18، رقم 24، ص 128؛ نقض 15 فبراير 1984، مجموعة أحكام محكمة النقض، س 35، رقم 31، ص 153؛ نقض 2 نوفمبر 1989، مجموعة أحكام محكمة النقض، س 40، رقم 138، ص 819. وقد أثار هذا الموقف من محكمة النقض خلافاً في الفقه بين مؤيد ومعارض، انظر في عرض هذا الخلاف: د. هلالي عبد اللاه أحمد: النظرية العامة للإثبات في المواد الجنائية، المرجع السابق، ص 456 وما بعدها والمراجع المشار إليها لديه.

(1) فيجب أن يتم الحصول على الدليل بالإضافة إلى ما سبق في المتن وفقاً لمبدأ الأمانة Le Principe de la loyauté وهذا ما سار عليه الفقه والقضاء الفرنسي: انظر:

PERROCHEAU, Des fluctuations du principe de loyauté dans la recherche des preuves, Petites affiches, 17 mai 2002, p. 6; LEBORGNE A, L'impact de la loyauté sur la manifestation de la vérité ou le double visage d'un grand principe, RTD civ. 1996, p. 535, spéc. p. 547. ; Crim, 12 juin 1952 , J.C.P. , 1952, II, 7241, note Brouchot ; RASSAT M.-L, note sous Cass. crim. 6 avr. 1993, JCP 1993, II, 22144, et autres références citées infra, n° 29, note 52 ; Cass. .crim. 15 juin 1993, D. 1994, Jur. p. 613, note MASCALA C.; Cass. 2e civ., 7 oct. 2004 : Bull. civ. 2004, II, n° 447

الخاتمة

تناولنا فيما سلف موضوعاً يحتاج إلى معالجة تشريعية خاصة تتصل بتنظيم استخدام من استخدامات التكنولوجيا الحديثة في أعمال البحث والتحري عن الجرائم وفي هذا الصدد ننوه إلى جملة من النتائج نعقبها بمشروع مقترح لقانون ينظم استخدام تقنية كاميرات المراقبة المغلقة في أعمال البحث والتحري وهي على النحو التالي:

تقنين استخدام كاميرات المراقبة التلفزيونية في أغراض الحد من الجريمة والوقاية منها، وكذلك حماية الأشخاص والممتلكات والأموال، بحيث يكون اللجوء لاستخدامها من خلال ضوابط قانونية تحقق التوازن بين هذه الأغراض واحترام الحق في الخصوصية.

أن يتم وضع ضوابط فنية مناسبة عند اللجوء لاستخدام كاميرات المراقبة في كل قطاع مهني بما يحقق فائدة عملية حقيقية نظراً للتنوع الفني والتقني في هذه الكاميرات وأنظمتها.

أن يتم وضع ضوابط قانونية واضحة محددة للتعامل مع ما تقوم هذه الكاميرات بتسجيله من بيانات ومعلومات أمام الجهات الإدارية والقضائية المختلفة.

وضع عقوبات مناسبة لأحوال الخروج على الضوابط القانونية المنظمة لاستخدام كاميرات المراقبة التلفزيونية.

ونقترح في هذا الصدد أن تكون نصوص هذا القانون على التفصيل التالي:

مشروع قانون استخدام التقنيات التكنولوجية الحديثة في أغراض الحد من الجريمة والملاحقة الجنائية لها

(المادة الأولى)

يجوز لأغراض الحد من الجريمة والملاحقة الجنائية لمرتكبيها استخدام التقنيات التكنولوجية الحديثة في أعمال المراقبة السابقة على ارتكاب الجريمة، وتشمل هذه التقنيات؛ تقنيات مراقبة المكالمات والمحادثات والمراسلات أيا كان شكلها أو طبيعتها أو وسيلتها، وتقنيات المراقبة باستخدام كاميرات المراقبة التلفزيونية المغلقة.

(المادة الأولى)

يجوز لأصحاب المصلحة طلب الإذن باستخدام كاميرات المراقبة التلفزيونية لأغراض الحماية الخاصة للأشخاص والممتلكات والأموال، وتصدر الموافقة على ذلك من وزارة الداخلية.

(المادة الثانية)

تلتزم كافة الأشخاص ـ الاعتبارية العامة والخاصة ـ بتركيب كاميرات مراقبة تلفزيونية في الأماكن العامة التي تخضعها لرقابتها وإشرافها، وعليها في كل الأحوال وضع إشارات كاشفة عن وجود هذه الكاميرات في مكان واضح، وفي كل الأحوال لا يجوز تركيب هذه الكاميرات في الأماكن الخاصة، أو مد نطاق عملها لتصل إلى أماكن خاصة.

(المادة الثالثة)

على مستخدمي أنظمة المراقبة التلفزيونية الصادر ترخيص لهم باستخدامها الالتزام بالحفاظ على سرية التسجيلات الناتجة عن هذه المراقبة وعدم إطلاع الغير عليها أو إفشاءها، أو استخدامها بأي حال من الأحوال في أغراض خاصة خلافاً لأغراض الحماية والتأمين.

ويعاقب كل من يخالف هذا الالتزام بالحبس مدة لا تقل عن ثلاثة أشهر وبالغرامة التي لا تقل عن (20000)عشرين ألف درهم ولا تزيد عن (100000) مائة ألف درهم. وتكون العقوبة

هي السجن مدة لا تقل عن ثلاثة سنوات ولا تزيد عن خمس سنوات إذا استخدمت هذه النتائج في أفعال ابتزاز مادي أو معنوي أو أفعال إساءة لسمعة الأشخاص أو أعراضهم.

(المادة الرابعة)

يلتزم مستخدمو أنظمة المراقبة التلفزيونية بتسليم التسجيلات الناتجة عنها للجهات المختصة عند طلبها، وفي كل الأحوال يجب على هؤلاء تسليم هذه التسجيلات بدون طلب لجهات إنفاذ القانون في كل الأحوال التي تكون لها فائدة في إظهار الحقيقية بشأن أي جريمة وقعت بالفعل أو يشتبه في ارتكابها.

يعاقب كل من يخالف هذا الالتزام بالحبس مدة لا تقل عن ثلاثة أشهر وبالغرامة التي لا تقل عن (20000)عشرين ألف درهم ولا تزيد عن(50000) خمسين ألف درهم.

(المادة الخامسة)

تكون لنتائج المراقبة التلفزيونية الحجية القانونية الكاملة أمام جهات التحقيق والمحاكمة، ويجوز الاستناد إليها في إجراءات الملاحقة الجنائية أمام الجهات القضائية المختلفة.

(المادة السادسة)

على المرخص له باستخدام كاميرات المراقبة التلفزيونية إتلاف التسجيلات الناشئة عن المراقبة التكنولوجية بنوعيها بعد انقضاء أربعة أشهر من تاريخ انتهاء أعمال المراقبة، ما لم تكن هذه النتائج محل استخدام قضائي، وفي الأحوال التي يتم استخدامها في أغراض الملاحقة الجنائية يكون التخلص منها بمعرفة النيابة العامة بعد صدور الحكم البات في الدعوى و انقضاءها.

ويعاقب كل من يخالف هذا الالتزام بالحبس مدة لا تقل عن ستة أشهر وبالغرامة التي لا تقل عن (50000) خمسين ألف درهم ولا تزيد عن(100000) مائة ألف درهم.

(المادة السابعة)

تحدد اللائحة التنفيذية لهذا القانون والقرارات الصادرة تنفيذاً له، الجهة المختصة بتلقي طلبات استخدام تقنيات المراقبة التلفزيونية وإجراءاته، وكذلك المواصفات الفنية الواجب توافرها في كاميرات المراقبة التلفزيونية التي يتم استخدامها في كل قطاع، وعلى مستخدميها التقيد بهذه المواصفات.

يعاقب كل من يقوم باستخدام أنظمة المراقبة التلفزيونية دون الحصول على الترخيص اللازم لذلك، وكذلك كل من يخالف شروط هذا الترخيص بالغرامة التي لا تقل عن(50000) خمسين ألف درهم ولا تزيد عن(100000) مائة ألف درهم.

قائمة المراجع

- أولاً:المراجع العربية:
- المؤلفات العامة:
- أحمد فتحي سرور: الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1985.
- أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، المجلد الأول، دار النهضة العربية 1981.
- عوض محمد، قانون الإجراءات الجنائية، دار النهضة العربية، ج1، 1990.
- عوض محمد عوض: المبادئ العامة في الإجراءات الجنائية، دار المطبوعات الجامعية، 1999م.
- فوزية عبد الستار: شرح قانون الإجراءات الجنائية، دار النهضة العربية، 1986.
- فوزية عبد الستار: شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، الطبعة الثالثة، 1990.
- محمد زكي أبو عامر: شرح قانون الإجراءات الجنائية، منشأة المعارف، الإسكندرية، 1994.
- محمد زكي أبو عامر: الحماية الجنائية للحريات الشخصية، منشأة المعارف، الإسكندرية، 1979.
- محمد زكي أبو عامر: قانون العقوبات، القسم الخاص، دار الجامعة الجديدة للنشر، طبعة 2005.
- محمود نجيب حسني: شرح قانون العقوبات القسم الخاص، دار النهضة العربية، القاهرة، 1992.
-
- -المؤلفات المتخصصة:
- إبراهيم عيد نايل: الحماية الجنائية لحرمة الحياة الخاصة من قانون العقوبات الفرنسي، الحماية الجنائية للحديث والصورة، دار النهضة العربية، القاهرة، 2000.
- أحمد شوقي أبو خطوة، المساواة في القانون الجنائي، دار النهضة العربية، القاهرة، 1991.
- أحمد ضياء الدين محمد خليل: مشروعية الدليل في المواد الجنائية، دراسة تحليلية

مقارنة لنظريتي الإثبات والمشروعية في مجال الإجراءات الجنائية، دار النهضة العربية، القاهرة، 2010.
- أحمد عبد الظاهر: استيقاف الأشخاص في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة الأولى، 2006.
- أحمد فتحي سرور: الشرعية الدستورية وحقوق الإنسان في الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1993.
- أحمد فتحي سرور: الشرعية والإجراءات الجنائية، دار النهضة العربية، القاهرة، 1977.
- حسام الدين الأهواني: الحق في احترام الحياة الخاصة، الحق في الخصوصية، دار النهضة العربية، القاهرة، 1987م.
- حسن جلال زايد: عمليات الشرطة، الجزء الأول، أكاديمية شرطة دبي، 2010.
- حسن صادق المرصفاوي: المحقق الجنائي، منشأة المعارف، الإسكندرية، الطبعة الأولى، 1990.
- حلمي الدقدوقي: رقابة القضاء على المشروعية الداخلية لأعمال الضبط الإداري، دراسة مقارنة، دار المطبوعات الجامعية، 1989.
- سعيد جبر: الحق في الصورة، دار النهضة العربية، القاهرة 1986م.
- طارق أحمد فتحي سرور: دروس في جرائم النشر، دار النهضة العربية، الطبعة الأولى، 1997.
- عبد الرءوف مهدي: الجوانب الإجرائية لحماية الحق في الحياة الخاصة، بحث مقدم إلى مؤتمر "الحق في الحياة الخاصة"، كلية الحقوق جامعة الإسكندرية، 1987م.
- فتوح الشاذلي: المساواة في الإجراءات الجنائية، دار المطبوعات الجامعية، 1990.
- مأمون محمد سلامة، الأحكام الخاصة بالجرائم الماسة بأمن الدولة، دار الفكر العربي، طبعة 1997.
- محمد عبد الكريم نافع: الجرائم الماسة بأمن الدولة من الداخل والخارج، بدون ناشر.
- محمد نعيم فرحات: النظرية العامة لعذر تجاوز حق الدفاع الشرعي، دكتوراة، 1981.
- محمود أحمد طه: التعدي على حق الإنسان في حرمة اتصالاته الشخصية، 1990.
- مصطفى أحمد عبد الجواد حجازي: الحياة الخاصة ومسؤولية الصحفي، دار الفكر العربي، 2000.
- هلالي عبد اللاه أحمد: النظرية العامة للإثبات الجنائي، دار النهضة العربية، القاهرة، 1998.

- – المقالات والدوريات:
- أحمد رفعت خفاجي: مدى حجية الدليل المستمد من مراقبة المحادثات التليفونية، مجلة روح القوانين، كلية الحقوق جامعة طنطا، العدد الأول، سنة 1989.
- أحمد فتحي سرور: مراقبة المكالمات التليفونية، المجلة الجنائية القومية، العدد الأول 1963.
- رءوف عبيد: القبض على المتهمين واستيفائهم، مجلة العلوم القانونية والاقتصادية، يناير 1962.
- رمسيس بهنام: نطاق الحق في حرمة الحياة الخاصة، بحث مقدم إلى مؤتمر الحق في حرمة الحياة الخاصة، المنعقد في كلية الحقوق، جامعة الإسكندرية، في الفترة من 4– 6 يونيه 1987.
- زين العابدين سليم، د. محمد إبراهيم زيد: الأساليب الحديثة في مكافحة الجريمة، المجلة العربية للدفاع الاجتماعي، العدد 15 يناير 1983.
- محمود نجيب حسني: الحماية الجنائية لحرمة الحياة الخاصة، مجلة القضاة، يوليو 1987م العدد السادس.
- نعيم عطية: حق الأفراد في حياتهم الخاصة، مجلة إدارة قضايا الحكومة. العدد الرابع – السنة الحادية والعشرون. ديسمبر 1977م.
- هشام محمد فريد رستم: الحماية الجنائية لحق الإنسان في صورته، مجلة الدراسات القانونية كلية الحقوق جامعة أسيوط 1986م.
- وليد محمد الشناوي: مبدأ التناسب في مجال إجراءات مواجهة الإرهاب، دراسة مقارنة، مجلة العلوم القانونية الصادرة عن كلية الحقوق جامعة المنصورة، 2014، العدد الثاني.
- – الرسائل العلمية:
- أحمد ضياء الدين خليل، مشروعية الدليل في المواد الجنائية رسالة دكتوراة جامعة عين شمس 1982م.
- آدم عبد البديع آدم: الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي رسالة دكتوراة، كلية الحقوق، جامعة القاهرة 2000م.
- حسن محمد ربيع: حماية حقوق الإنسان والوسائل المستحدثة للتحقيق الجنائي، رسالة دكتوراة، كلية الحقوق جامعة الإسكندرية، 1985م.
- حسين محمود إبراهيم: الوسائل العلمية الحديثة في الإثبات الجنائي، رسالة دكتوراة، جامعة القاهرة، 1981.
- عبد الله محمد حسين خير الله: الحرية الشخصية في مصر، رسالة دكتوراة، كلية الحقوق، جامعة الإسكندرية، بدون تاريخ.
- عصام زكريا عبد العزيز: دور الشرطة في حماية حقوق الإنسان في مجال الضبط القضائي، رسالة دكتوراة، أكاديمية الشرطة، القاهرة، 2001.
- محمد رشاد إبراهيم: الحماية الجنائية للحق في حرمة الاتصالات الشخصية، رسالة دكتوراة، كلية الحقوق، جامعة الإسكندرية، 2009.
- محمد عبد العظيم محمد: حرمة الحياة الخاصة في ظل التطور العلمي الحديث، دراسة مقارنة، رسالة دكتوراة، كلية الحقوق، جامعة القاهرة، 1988.
- محمد عصام عبد المنعم: حماية حقوق الإنسان في حالة الطوارئ، دراسة مقارنة، رسالة دكتوراة، كلية الحقوق، جامعة عين شمس، 2012.
- محمد محمد الدسوقي الشهاوي: الحماية الجنائية لحرمة الحياة الخاصة، رسالة دكتوراة، كلية الحقوق، جامعة القاهرة.
- ممدوح خليل البحر: حماية الحياة الخاصة في القانون الجنائي، دراسة مقارنة، رسالة دكتوراة، جامعة القاهرة، 1983.

هل ينبغي أن تضع الحكومة اللوائح والقوانين، فيما يتعلق بالذكاء الاصطناعي؟ نعم، هي تفعل ذلك بالفعل

مقال مترجم من موقع ذا هيل.

بقلم كريستوفر فونزون وكيت هينزلمان،

هل ينبغي أن تضع الحكومة اللوائح والقوانين، فيما يتعلق بالذكاء الاصطناعي؟ نعم، هي تفعل ذلك بالفعل

مقال مترجم من موقع ذا هيل.

بقلم كريستوفر فونزون وكيت هينزلمان،

تقريبًا، تأتي كل يوم أخبار إضافية حول كيفية تأثير الذكاء الاصطناعي في الطريقة التي نعيش بها، حيث نشأ جدل ساخن حول ما ينبغي للولايات المتحدة فعله حيال هذا الأمر. من ناحية أخرى، يناقش محبو إيلون مسك وستيفن هوكينج، فكرة وجوب وضع لوائح وقوانين الآن، لإبطاء المبادئ الحاكمة لتطور الذكاء الاصطناعي وتنميتها، وذلك بسبب احتمالية تسببها في تشويش اقتصادي ضخم، بل وحتى تدمير الحضارة الإنسانية.

ومن ناحية أخرى، يجادل مؤيدو الذكاء الاصطناعي بقولهم: إنه لا يوجد إجماع حول ماهية الذكاء الاصطناعي؛ ناهيك عما يمكن للذكاء الاصطناعي فعله من الأساس. ويزعم هؤلاء المؤيدون بأن وضع اللوائح والقوانين لتنظيم الذكاء الاصطناعي في تلك الظروف، سوف يكبت-ببساطة- الابتكار، ويتنازل للدول الأخرى عن المبادرة التكنولوجية التي قدمت الكثير لتقوية اقتصاد الولايات المتحدة.

ورغم ذلك، يهدد التركيز المكثف على هذه الأسئلة التأسيسية بالتشويش على نقطة رئيسية، وهي أن الذكاء الاصطناعي بالفعل يخضع للوائح والقوانين بطرق عدة، ومع هذا يستمر الجدل الكبير حول الذكاء الاصطناعي، ومن المؤكد أن يتبعها إصدار اللوائح والقوانين الإضافية. وهذه اللوائح ليست من نوع المبادئ العامة التي يجادل بها مسك وهوكينج، ويخشاها مؤيدو الذكاء الاصطناعي: «لا يوجد شيء مذكور في الكتب على نحو مثير بأن «الروبوت قد يجرح الإنسان أو يسمح بتعرض الإنسان للضرر عبر التقاعس عن العمل.» هذه أول ثلاثة قوانين مشهورة لإسحاق أزيموف فيما يتعلق بعلم الروبوتات.»

حتى الآن، معظم القواعد ليست مخصصة للذكاء الاصطناعي على الإطلاق. فضلًا عن ذلك، فقواعد الخصوصية طويلة المدى والأمن السيبراني والأفعال والممارسات التجارية غير المنصفة والمضللة والإجراءات القانونية العادلة وقواعد الصحة والسلامة القائمة أو التي تكون أحيانًا طويلة الأجل، التي تغطي التقنيات التي تحدث الآن، يُعتقد أنها تغطي «الذكاء الاصطناعي». وتتضمن تلك القواعد القضايا ذات الصلة بالاحتفاظ بالبيانات الشخصية واستخدامها وحمايتها، والإرشادات الخاصة بكيفية إدارة المخاطر التي تتسبب فيها الخوارزميات المالية وعمليات الحماية ضد التمييز.

ولا ريب من خضوع العديد من تلك القواعد لموضوعات نقاش مركزة، على سبيل المثال، ما إذا كانت تحمي المستهلكين على نحو كاف أم لا. إن تطبيق تلك الأطر القانونية القائمة والمخططات التنظيمية ذات الصلة بالذكاء الاصطناعي، يمكن أن يطرح أسئلةً صعبة. على سبيل المثال، كيف تنطبق المفاهيم التي ترتكز على البشر مثل النية على الروبوتات؟ حتى إن أحدث القوانين التي لم تخاطب على وجه التحديد الذكاء الاصطناعي، مثل العديد من قوانين الدولة التي تحكم المركبات ذاتية القيادة، تتجنب التصريحات العامة حول تكنولوجيا الذكاء الاصطناعي، بدلًا من اختيار مخاطر محددة، تسببت فيها تطبيقات معينة.

ويبدو هذا -أيضًا- هو الاتجاه الذي يتجه إليه الكونجرس. وبمجرد انطلاق الذكاء الاصطناعي، تراجع الكابيتول هيل إلى حد كبير، على الأقل حتى النصف الثاني من عام 2017، عندما قدّم الأعضاء ثلاثة تشريعات منفصلة ذات صلة بالذكاء الاصطناعي: قانون القيادة الذاتية الذي مرره الكونجرس، الذي يتناول مسألة سلامة المركبات المؤتمتة، وقانون تشغيل المركبات المؤتمتة، الذي يتناول على نحو مشابه السيارات بلا سائق، وهو مشروع قانون من مجلس الشيوخ ممثّل من الحزبين، وقانون مستقبل الذكاء الاصطناعي، وهو مشروع قانون من مجلس الشيوخ ممثّل من الحزبين، الذي قد يُنشئ لجنة استشارية حول القضايا المتعلقة بالذكاء الاصطناعي.

وعلى الرغم من إقرار كل تلك القوانين بعمليات التشويش المحتمل، التي تقوّي مخاوف مسك وهوكينج، تتجنب كل من مسك وهوكينج الإعلان عن ذلك، فيما يتعلق بالذكاء الاصطناعي عمومًا؛ بغرض إجراء دراسة أكثر تعمقًا حول المسألة، والتركيز على الإجابة عن أسئلة قطاعات محددة، حيثما تنشأ. وبالتأكيد، قد ينشئ القانون الأكثر عموميةً -قانون

مستقبل الذكاء الاصطناعي- ببساطةٍ كيان متعدد الكفاءات لإجراء الدراسات وتقديم النصح حول قضايا الذكاء الاصطناعي.

وعلى النقيض، يضع القانونان الآخران الأحكام التشريعية مع التأثير الفوري من خلال الاستعانة ببعض قوانين الدولة لضمان وضوح المسار أمام الابتكار دون وجود تعقيدات تسببت فيها اللوائح والقوانين المختلفة للدولة. تركز هذه القوانين، التي تتعلق بالمسؤولية الفعلية، فقط على القطاع الذي بدأت فيه الولايات بلعب دور نشط، وحيث توازنت التكنولوجيا بالفعل؛ ليكون لها تأثير قريب المدى وأثر عالمي واقعي يتمثل في تكنولوجيا المركبات المؤتمتة.

ومن المغري أن ننظر إلى هذه التطورات، ونخلُص إلى أن الصناعة والمبتكرين قد يكونون في أمان باستمرار عند الامتثال لتلك القوانين التي تؤثر فيهم اليوم، في حين ننتظر لنرى ما يفعله الكونجرس، إذا قرر أو عندما يقرر التركيز على نوع معين يُعدونه من تكنولوجيا الذكاء الاصطناعي. وبمعنى آخر، عندما يخضع هذا القطاع للتشريعات، مثل حال تكنولوجيا المركبات ذاتية القيادة اليوم، لكن مثل هذا النهج من شأنه أن يكون مضللًا.

إن النظر في القوانين التي ناقشها الكونجرس أعلاه، توضح أن المشرعين يتفهمون القضايا العديدة التي نشأت عن التطور السريع لتكنولوجيا الذكاء الاصطناعي. في حين يتخذ الكونجرس خطوات إضافية في الوقت الراهن، قد يكون للعمليات التي تضعها هذه القوانين آثار طويلة الأجل. حتى لو لم تؤثر هذه القوانين فورًا أو مباشرةً في قطاع الشركات، فإنه يمكن أن يكون لها آثار في تحديد معالم الطريق.

قد يكون للقرارات التي تُتخذ اليوم آثار جوهرية غير مقصودة؛ حيث يمكن للمشرعين فقدها بسهولة مستقبلًا، أثناء رحلة تطوير تكنولوجيا الذكاء الاصطناعي. من كان يتصور الآثار الكاملة للقسم رقم 230 من قانون آداب الاتصالات عندما سُن في عام 1996؟ أو من كان يتخيل تأثير متطلبات ضمان قانون خصوصية التواصل الإلكتروني لرسائل البريد الإلكتروني الأقل من 180 يومًا عام 1986؟ تميل القوانين التشريعية الأولى حول التقنيات الحديثة للاستمرار.

قد يكون للمفردات ذاتها التي بدأ يستخدمها واضعو اللوائح والقوانين في مشروعات

القوانين تلك، تأثيرٌ دائمٌ على الطريقة التي يرى ويتعامل بها واضعو اللوائح والقوانين مع تقنيات الذكاء الاصطناعي بصورة أكثر عمومية. فعلى سبيل المثال، إذا كانت الشركات لا تنشئ معجمًا للذكاء الاصطناعي يساعد المشرعين أو واضعي اللوائح والقوانين على فهم التقنيات، التي ينبغي تنظيمها على نحوٍ مختلف، ووصفها على نحوٍ ذو معنى، والتمييز بينها، فقد يضع هؤلاء المشرعون وواضعو اللوائح مثل هذا المعجم بأنفسهم، وعلى نحوٍ جيد. وبالمثل، إذا لم تُبق الشركات المشرعين أو واضعي اللوائح والقوانين على درايةٍ بأفضل الممارسات والسياسات النموذجية أو مدونات قواعد السلوك ذات الصلة بالصناعة الخاصة بهم، فلن تكون هناك فرصة لتلك الممارسات في أن تكون بمثابة دليل يبحث عنه المشرعون؛ ليكون نموذجًا يُحتذى به في العمل.

إلى الحد الذي تؤثر به الأنظمة القانونية القائمة في ابتكارات الذكاء الاصطناعي والأطر التي يجري تطويرها خلالها، فليس هناك وقت أفضل من الوقت الحاضر لجذب الطرق التي تكون عليها تلك الأطر القائمة من حيث عملها أو عدم عملها إلى انتباه واضعي اللوائح والقوانين. قد توضع الأجندة التنظيمية للذكاء الاصطناعي في وقتٍ مبكر، وينبغي لمجتمع الذكاء الاصطناعي الانتباه، حيث لن يتم وضع اللوائح والقوانين فحسب، بل هي موجودة بالفعل.

هل ينبغي تنظيم الذكاء الاصطناعي؟

مقال مترجم من موقع تومسون رويترز

البروفيسور ديلاكروس

هل ينبغي تنظيم الذكاء الاصطناعي؟

مقال مترجم من موقع تومسون رويترز
البروفيسور ديلاكروس

أحدث الذكاء الاصطناعي أصداءً هامة في جميع أنحاء العالم، مع توقع الخبراء أنْ يؤدي إلى تغيير وإعادة تشكيل طريقة حياة البشر اليومية على نحوٍ متزايد، كما سيعمل الذكاء الاصطناعي أيضًا على إحداث هزة في مجال الصناعة القانونية؛ مما سيؤدي إلى تحول عميق في تقديم الخدمات القانونية. ومع هذه الإمكانية والقدرة على قيادة التغيير الكبير في الحياة العادية والخدمات المتخصصة، أثير بعض الجدل حول ما إذا كان ينبغي تنظيم الذكاء الاصطناعي أم لا.

أجابت البروفيسور سيلفي ديلاكروس (من جامعة برمنغهام) على أسئلة طومسون (من وكالة رويترز للآراء القانونية في المملكة المتحدة وأيرلندا) حول رأيها في الذكاء الاصطناعي والدعوة إلى تنظيمه.

ما أهمية الذكاء الاصطناعي، ودوره في المجتمع؟

إن أهم تطور يحدث اليوم هو معرفة مدى قدرتنا على جمع واستغلال البيانات لتطوير أنواع جديدة من المعرفة التي تحول -بشكل جذري- الطريقة التي نعيش بها للأفضل أو للأسوأ. أعتقد أن مصطلح «الذكاء الاصطناعي» يمكن أن يكون مضللًا إلى حد ما، فقد تجد في صدر العناوين التي نشرت مؤخرًا-بداية من السيارات ذاتية القيادة إلى أدوات التشخيص الآلي- التطبيقات التي تستخلص البيانات عن بعد اعتمادًا على الخوارزميات المرتبطة بالسعي لتطوير الآلات التي تحاكي وتتجاوز الذكاء البشري.

لقد ذكرتْ من قبل أن هناك حاجة لتنظيم الذكاء الاصطناعي، لماذا تعتقدين أن تنظيم الذكاء الاصطناعي مهم؟

سوف يكون التنظيم جزءًا صغيرًا فقط، غير أنه مهم في الإجابة على هذا التساؤل. نظرًا للسرعة التي تحوِّلُ بها الأدوات والممارسات معاني الأشياء مثل الخصوصية أو الرضا،

فالمناهج المنطلقة من القاعدة ضرورية، وقد تكون هذه المناهج ذات توجهات صناعية (مثل الشراكة في الذكاء الاصطناعي) أو ذات توجه مجتمعي (انظر -على سبيل المثال- المناقشات حول فكرة «الأساس» الذي تنبني عليه موثوقية البيانات).

وكي يكون التنظيم كافيًا وناجحًا، علينا -أولًا- العمل، معًا كمجتمع، لتحديد حجم الاهتمام وسببه بأشكال معينة من الخصوصية والرضا، أو الممارسات المهنية. إذا كنا -مثلًا- قادرين على تطوير برنامج افتراضي للعلاج الآلي لتوفير الخدمات الطبية بموثوقية عالية، فهل ينبغي علينا أن نتوقف وننظر في القيم التي لا يمكن أن تتواجد في الاستشارة الافتراضية الآلية، إن وجدت؟ نعم ينبغي علينا ذلك، إذا كنا غير معتادين على القيام بذلك. تعتبر جميع الابتكارات التكنولوجية في كثير من الأحيان مرغوبة، إذا توفرت فيها أسس التكلفة، السلامة، الجودة وخاصية لفت الانتباه. فإذا وجد أن هذه الابتكارات في وقت لاحق قد أدت إلى اختراق أو تباين كبير، فلا يمكن للتنظيم تغيير هذه النتيجة. واليوم، تأتي الجهود التنظيمية -على سبيل المثال- لمعالجة التباين بين أدوات التحكم في البيانات ومواضيع البيانات.

ما هي التعقيدات القانونية التي ترتبت على ظهور الذكاء الاصطناعي؟

قد أولي اهتمام كبير لتحدي المسؤولية القانونية المتعلق بالسيارات ذاتية القيادة: في كثير من الأحيان، أعتقد أن هذه إحدى المشكلات سهلة الحل بسبب وجود حل واقعي إلزامي خالٍ من الأخطاء. في المقابل، نجد أن تطوير طرق الحفاظ على الرضا و/أو الخصوصية في اقتصادٍ قائم على المعلومات لبيع المنتجات والخدمات الشخصية، تحدٍ شائك.

ماذا يمكن أن يفعل المحامون الآن للتعامل مع الطبيعة المتطورة للذكاء الاصطناعي والاحتياجات التنظيمية المتوقعة؟

أولًا، وقبل كل شيء، يجب على المحامين إخراج رؤوسهم من الرمال وتثقيف أنفسهم. فمن المؤسف أن يحظى معظم الطلاب المتخرجين من كلية الحقوق اليوم بقليل من الفهم للبيانات التي يتم تسريبها يوميًا -سواء أكان ذلك عبر وسائل التواصل الاجتماعي أو التسوق عبر الإنترنت- وما يستخدم فيها يمكن وضعه في (أنواع مختلفة من الخوارزميات)، والحقوق المحدودة التي لديها بموجب تنظيم حماية البيانات الحالية والتي ستنضوي تحت تنظيم حماية البيانات العامة الذي سيدخل حيز التنفيذ في 25 مايو 2018.

ما هو تصورك حول تغيير الذكاء الاصطناعي مهنة المحاماة في السنوات الـ 10 القادمة؟

لدى أنظمة دعم القرار القدرة على تعزيز مهنة المحاماة، خاصة قدرتها على الارتقاء إلى مستوى مسؤولياتها الاجتماعية والأخلاقية. ومن أجل تجسيد تلك القدرة، تحتاج مهنة المحاماة للتفكير في القيم التي تخدمها والمشاركة الاستباقية مع مصممي تلك النظم.

تم الإعلان في ميزانية الحكومة في الخريف عن نية إنشاء أول مجلس استشاري وطني للذكاء الاصطناعي لوضع معايير الاستخدام وأخلاقيات الذكاء الاصطناعي والبيانات، ما هو رأيك في هذه الخطوة؟

إنها مبادرة مهمة، ومن المهم أن تدعم جميع القطاعات (وخبراء الحاسوب، والمتخصصين من جميع المجالات، والأكاديميين، والمواطنين بصفة عامة) وتشارك في عمل هذا المجلس الاستشاري المهم بنشاط.

الاتحاد الأوروبي يناقش تنظيم الذكاء الاصطناعي، والقضايا القانونية المرتبطة به

مقال مترجم من موقع ديجينوميكا.

بقلم: ديريك دو بريز.

الاتحاد الأوروبي يناقش تنظيم الذكاء الاصطناعي، والقضايا القانونية المرتبطة به

مقال مترجم من موقع ديجينوميكا.

بقلم: ديريك دو بريز.

ملخص: سينظر الاتحاد الأوروبي في إنشاء إطار عمل، استنادًا إلى آراء الخبراء بشأن القضايا الأخلاقية والقانونية الشائكة المتعلقة بالذكاء الاصطناعي.

مع استمرار بائعي البرمجيات في الولايات المتحدة في ضخ استثمارات كبيرة في الذكاء الاصطناعي وأنظمة التعلم الآلي، بالإضافة إلى ميزانيات التسويق الخاصة بهذه المشاريع، توصلت المفوضية الأوروبية بعد مناقشة هذا الموضوع إلى حقيقة، تفيد بوجود حاجة ملحة لإصدار لوائح وأطر عمل جديدة تضمن عمل شركات الذكاء الاصطناعي بأمان وتقدمها، وفقًا للمبادئ الأساسية للاتحاد الأوروبي.

وفي بيان جديد مقدم من المجموعة الأوروبية للأخلاقيات، ذُكر أن الشركات الأمريكية تعمل الآن على تطوير أنظمة الذكاء الاصطناعي بمعدلات سريعة، وهناك مخاوف بشأن الفجوة بين الإجراءات التنظيمية وقدرات هذه الأنظمة الجديدة. ويسلط البيان أيضًا الضوء على الطبيعة المبهمة لعملية تطوير هذه الأنظمة.

ستحتاج الشركات الأمريكية التي ترغب في العمل في الاتحاد الأوروبي وبيع برمجيات الذكاء الاصطناعي إلى أن تكون على دراية باللوائح المستقبلية المطروحة للنقاش.

ستُنشئ المفوضية الأوروبية مجموعة من شأنها مناقشة التحديات المرتبطة بعالم الذكاء الاصطناعي سريع التطور؛ على أمل أن يبدأ الاتحاد الأوروبي في تقديم إجابات على بعض الأسئلة الأخلاقية والقانونية والمجتمعية الصعبة التي تثيرها التكنولوجيا.

ذكرت المجموعة الأوروبية للأخلاقيات في بيان لها أن الذكاء الاصطناعي يمكن أن يحقق كثيرًا من الفوائد للعمال والحكومات والمواطنين، لكن البيان أضاف أيضًا أن الطبيعة المبهمة للتكنولوجيا، والسرعة التي تتطور بها، تثير بعض الأسئلة الأخلاقية الملحة.

دعا البيان لإطلاق عملية من شأنها أن تُمهد الطريق لوضع «إطار عمل أخلاقي وقانوني مشترك ومعترف به دوليًا لتصميم وإنتاج واستخدام وحوكمة الذكاء الاصطناعي والروبوتات والأنظمة الذاتية».

كما يقترح البيان مجموعة من المبادئ الأخلاقية الأساسية، استنادًا إلى القيم المنصوص عليها في معاهدات الاتحاد الأوروبي وميثاق الحقوق الأساسية للاتحاد الأوروبي.

ذكر البيان أنه بينما يتزايد الوعي بشأن الحاجة لمناقشة المسائل الأخلاقية والقانونية المتعلقة بالذكاء الاصطناعي، يتم تطوير التكنولوجيا نفسها في كثير من الأحيان بسرعة أكبر من عملية إيجاد الإجابات المطلوبة في هذا الشأن. وأضاف البيان:

تمثل الجهود الحالية خليطا من مبادرات مختلفة. وهناك حاجة واضحة لإطلاق عملية جماعية واسعة النطاق وشاملة، من شأنها تمهيد الطريق لوضع إطار عمل أخلاقي مشترك ومعترف به دوليًا لتصميم، وإنتاج، واستخدام، وحوكمة الذكاء الاصطناعي والروبوتات والأنظمة الذاتية.

أطلقت المفوضية الأوروبية تطبيقات لضم مجموعة من الخبراء في مجال الذكاء الاصطناعي لتنفيذ الآتي:

- تقديم المشورة للمفوضية بشأن كيفية بناء مجتمع واسع ومتنوع من الجهات المعنية المشاركة في «التحالف الأوروبي للذكاء الاصطناعي».
- دعم تنفيذ المبادرة الأوروبية المقبلة بشأن الذكاء الاصطناعي (أبريل 2018).
- بحلول نهاية العام، إعداد مسودة المبادئ التوجيهية للتطوير والاستخدام الأخلاقي للذكاء الاصطناعي بناءً على ميثاق الحقوق الأساسية للاتحاد الأوروبي. وأثناء تنفيذ

ذلك، سيتم النظر في قضايا مثل العدالة والسلامة والشفافية، ومستقبل العمل والديمقراطية، وتأثير ذلك على تطبيق ميثاق الحقوق الأساسية على نطاق أوسع.

الأولويات

تذكر المجموعة الأوروبية للأخلاقيات في بيانها، أنه من المؤسف أن بعض أقوى أدوات الذكاء الاصطناعي وأكثرها فعالية، هي في نفس الوقت الأكثر غموضًا. وأضاف البيان أن جزءًا كبيرًا من القدرات المتقدمة تعود إلى جهات القطاع الخاص، والقدر الأكبر منها مسجل الملكية.

ويشير البيان إلى حقيقة أن أنظمة الذكاء الاصطناعي لم تعد مبرمجة من قبل البشر بطريقة خطية. على سبيل المثال، يُطور جوجل برين ذكاءً اصطناعيًا، يُعتقد أنه يستطيع بناء أنظمة ذكاء اصطناعي أفضل وأسرع من البشر. أو ما يُثار حول أن برنامج AlphaZero يستطيع في أربع ساعات فقط تعلم قواعد الشطرنج من البداية حتى الوصول إلى مستوى بطل العالم. وهذا يعني وفقًا للمجموعة الأوروبية للأخلاقيات الآتي:

في هذا الإطار، لم تعد أفعال تلك التطبيقات الناتجة عن الذكاء الاصطناعي واضحة في كثير من الأحيان، ولم تعد المراقبة البشرية لما تقوم به متوفرة. هذا هو الحال لأنه، أولًا، من المستحيل تحديد كيفية الوصول إلى النتائج خارج نطاق الخوارزميات الأولية. ثانيًا، يستند أداء أنظمة الذكاء الاصطناعي إلى البيانات التي تم استخدامها أثناء عملية التعلم، والتي قد لا تكون متوفرة أو يمكن الوصول إليها. وهكذا، التحيزات والأخطاء المدخلة في النظام في الماضي تصبح متأصلة ومتجذرة فيه.

وضعت المجموعة الأوروبية للأخلاقيات المبادئ الأخلاقية والشروط الأساسية الديمقراطية للاتحاد الأوروبي بشأن دراسة دور الذكاء الاصطناعي في المستقبل. وتعد هذه المبادئ متأصلة على نحو راسخ ضمن المبادئ الأساسية للاتحاد الأوروبي. وتشمل:

- **الكرامة الإنسانية:** ويُفهم منه الاعتراف بالصفة البشرية المتأصلة في الإنسان والنابعة من كونه كائنًا جديرًا بالاحترام، ولا يجب المساس به بسبب تأثيرات التقنيات ذاتية التشغيل.

- **ذاتية التصرف:** ينطوي مبدأ ذاتية التصرف في مضمونه على حرية الإنسان، ويترجم ذلك إلى المسؤولية البشرية عن الأنظمة الذاتية وما يتضمنه ذلك من مراقبة لهذه الأنظمة ودراية بها، ووضع معايير وقواعد خاصة والعيش وفقًا لها، بما يساعد على عدم المساس بحرية الإنسان.

- **المسؤولية:** يجب تطوير الأنظمة الذاتية واستخدامها بالطرق التي تحقق المنافع الاجتماعية والبيئية على مستوى العالم، على النحو الذي تحدده نتائج العمليات الديمقراطية التداولية.

- **العدل والمساواة والتكافل:** ينبغي أن يُسهم الذكاء الاصطناعي في العدالة العالمية وتكافؤ الفرص في الحصول على الفوائد والمزايا التي يمكن أن تقدمها أنظمة الذكاء الاصطناعي والروبوتات والأنظمة الذاتية. ويجب منع الأفعال التي تنطوي على تمييز أو تحيز عند إدخال مجموعات البيانات التي تستخدم لتدريب وتشغيل أنظمة الذكاء الاصطناعي، أو الكشف عنها وتحييدها في مرحلة مبكرة.

- **الديمقراطية:** يجب أن تكون القرارات الرئيسية بشأن تنظيم عملية تطوير وتطبيق الذكاء الاصطناعي نتاجًا لنقاش ديمقراطي ومشاركة عامة. وستضمن روح التعاون العالمي والحوار العام بشأن هذه القضية والتعامل معها بطريقة شاملة وحكيمة ومبنية على المعلومات.

- **سيادة القانون ومسؤولية المحاسبة:** توفر سيادة القانون والوصول إلى العدالة وحق التقاضي والمحاكمة العادلة الإطار اللازم لضمان احترام معايير حقوق الإنسان ولوائح الذكاء الاصطناعي المحتملة. وهذا يشمل الحماية ضد المخاطر الناتجة عن الأنظمة الذاتية التي يمكن أن تنتهك حقوق الإنسان، مثل السلامة والخصوصية.

- **الأمن والأمان والسلامة العقلية والجسدية:** سلامة وأمن الأنظمة الذاتية يتحقق في ثلاث صور: (1) السلامة الخارجية لبيئاتها والمستخدمين، (2) الموثوقية والثبات الداخلي، على سبيل المثال مقاومة القرصنة، و(3) السلامة العاطفية فيما يتعلق بالتفاعل بين الإنسان والآلة. يجب مراعاة جميع أبعاد السلامة من قبل المطورين.

- **حماية البيانات والخصوصية:** في العصر الذي يشهد الجمع واسع النطاق والضخم للبيانات من خلال تقنيات الاتصال الرقمية، يصبح الحق في حماية المعلومات الشخصية والحق في احترام الخصوصية تحديات هامة للغاية وحساسة. ويجب أن تمتثل روبوتات الذكاء الاصطناعي المادية التي تعمل كجزء من إنترنت الأشياء، والروبوتات المعرفية أو البرمجية التي تعمل عبر الشبكة العنكبوتية العالمية إلى لوائح حماية البيانات، ولا يجوز جمع ونشر بيانات أو تشغيل الأنظمة باستخدام مجموعات البيانات، دون الحصول على موافقة مستنيرة بشأن استخدام هذه البيانات ونشرها.

- **الاستدامة:** يجب أن تكون تكنولوجيا الذكاء الاصطناعي متوافقة مع المسؤولية البشرية لضمان تلبية الشروط الأساسية للحياة على كوكبنا، والازدهار المستمر للجنس البشري والحفاظ على بيئة جيدة للأجيال القادمة.

وتعليقًا على هذا البيان، قال نائب الرئيس المسؤول عن السوق الرقمية الموحدة، أندروس أنسيب:

خطوة خطوة، ننشئ البيئة المناسبة لأوروبا التي تمكنها من الاستفادة القصوى مما يمكن أن يقدمه الذكاء الاصطناعي. وتُعد البيانات وأجهزة الحاسوب العملاقة والاستثمارات الجريئة ضرورية لتطوير الذكاء الاصطناعي، جنبًا إلى جنب مع إجراء مناقشة عامة واسعة النطاق بالإضافة إلى احترام المبادئ الأخلاقية، فيما يتعلق باستخدامها. وكما هو الحال دائمًا مع استخدام التقنيات، تعد الثقة أمرًا لابد منه.

رأي الكاتب

هناك الكثير من الأمور على المحك فيما يتعلق بهذا الشأن، فكما تعد التقنيات الذاتية بتوفير السهولة والراحة -لا ينبغي أن يكون الأمر مقبولًا إذا كانت هناك مخاطر على الحقوق الأساسية، أو ما قد يؤدي إلى حدوث تمييز أو تحيز و/أو وقوع أي أفعال لا يقبلها المجتمع. ويتعين على الاتحاد الأوروبي أن يعمل بسرعة وبذكاء لتطبيق إطار العمل المذكور سلفًا؛ لأن هذه الأدوات تتطور بإيقاع سريع. وبمجرد إنشاء هذا الإطار، ينبغي تطبيقه بصرامة وتقديم المساعدات المطلوبة لتوفير المراقبة المستمرة لهذه الأنظمة.